

# XenApp 和 XenDesktop 7.6 Long Term Service 版本

Feb 06, 2018

## 新增功能

[累积更新 6 \(CU6\)](#)

[累积更新 5 \(CU5\)](#)

[累积更新 4 \(CU4\)](#)

[累积更新 3 \(CU3\)](#)

[累积更新 2 \(CU2\)](#)

[累积更新 1 \(CU1\)](#)

[Long Term Service Release \(LTSR\)](#)

[本版本中不提供的功能](#)

[已知问题](#)

## 系统要求

## 技术概述

[Concepts and components](#)

[Active Directory](#)

[Fault tolerance](#)

[Delivery methods](#)

[Reference Architectures](#)

[Design Guides](#)

[Implementation Guides](#)

## 新建部署

[Prepare to install](#)

[Prepare the virtualization environment: VMware](#)

[Prepare the virtualization environment: Microsoft System Center Virtual Machine Manager](#)

[Prepare for using Microsoft System Center Configuration Manager](#)

[Install using the graphical interface](#)

[Install using the command line](#)

[Create a Site](#)

[Install or remove Virtual Delivery Agents using scripts](#)

Machine catalogs  
Delivery groups  
XenApp published apps and desktops  
VM hosted apps  
VDI desktops  
Remote PC Access  
App-V  
Local App Access and URL redirection  
Server VDI  
Remove components

## 升级和迁移

Upgrade a deployment  
Migrate XenApp 6.x  
Migrate XenDesktop 4

## 安全性

Getting Started with Citrix XenApp and XenDesktop Security  
Security best practices and considerations  
Delegated Administration  
Smart cards  
SSL

## 策略

Work with policies  
Policy templates  
Create policies  
Compare, prioritize, model, and troubleshoot policies  
Default policy settings  
Policy settings reference

## 打印

Printing configuration example  
Best practices, security considerations, and default operations  
Print policies and preferences

Provision printers

Maintain the printing environment

许可

连接和资源

连接租用

虚拟 IP 和虚拟环回

辅助数据库位置

Delivery Controller 环境

添加、删除或移动 Controller 或者移动 VDA

基于 Active Directory OU 的控制器发现

会话管理

在 Studio 中使用搜索

IPv4/IPv6 支持

客户端文件夹重定向

个人虚拟磁盘（不包括在 LTSR 中）

安装和升级

配置与管理

工具

显示、消息和故障排除

用户配置文件

HDX

Thinwire 兼容模式

HDX 3D Pro

Flash 重定向

主机到客户端重定向

适用于 Windows 桌面操作系统的 GPU 加速

Windows Server 操作系统 GPU 加速

[OpenGL Software Accelerator](#)

[音频功能](#)

[网络流量优先级](#)

[USB 和客户端设备注意事项](#)

## [监视](#)

[Director](#)

[Session Recording](#)

[Personal vDisk](#)

[Configuration Logging](#)

[Monitor Service OData API](#)

## [SDK](#)

[Understanding the XenDesktop Administration Model](#)

[Get started with the SDK](#)

[PowerShell cmdlet help](#)

[针对 XenApp and XenDesktop 7.6 LTSR 的 Citrix VDI 最佳实践](#)

## [FIPS 示例部署](#)

## [第三方声明](#)

[Citrix SCOM Management Pack for XenApp and XenDesktop](#)

[Citrix SCOM Management Pack for License Server](#)

# 新增功能

Aug 15, 2018

XenApp 和 XenDesktop 7.6 的长期服务版本 (LTSR) 计划可为 XenApp/XenDesktop 7.6 版本提供稳定性和长期支持。

LTSR 的最新更新是[累积更新 6 \(CU6\)](#)。Citrix 建议将您的部署中的 LTSR 组件更新到 CU6。

如果您是 LTSR 程序的新用户，并且未部署原始 XenApp/XenDesktop 7.6 LTSR 版本，则无需在此时安装。相反，Citrix 建议您跳过 7.6 LTSR 版本，并开始使用 CU6。整个 7.6 LTSR 发行版的文档可[在此处](#)获取。

此外，Citrix 还建议您使用特定版本的 Citrix Receiver 及其他组件。升级到这些组件的当前版本可确保进一步简化维护过程以及确保您的部署中最新修复的可用性，但这并非是 LTSR 合规性的必需条件。

下载

[7.6 LTSR CU6 \(XenApp\)](#)

[7.6 LTSR CU6 \(XenDesktop\)](#)

文档

[7.6 LTSR 累积更新 6](#)

[7.6 LTSR 累积更新 5](#)

[7.6 LTSR 累积更新 4](#)

[7.6 LTSR 累积更新 3](#)

[7.6 LTSR 累积更新 2](#)

[7.6 LTSR 累积更新 1](#)

[7.6 LTSR](#)

有用链接

- [Citrix 支持包](#)

支持包是一组由 Citrix 工程师编写、用于帮助诊断和解决 XenDesktop/XenApp 产品故障的常用工具。这些工具按功能和组件编目，因此很方便查找和使用。该包的早期版本用作相应产品的基础...

- [Citrix LTSR 助手](#)

LTSR 助手会扫描 XenApp 和 XenDesktop 7.6 的组件以确定其是否符合长期服务版本 (LTSR)。要扫描的组件可驻留于虚拟机或...

- [LTSR 常见问题解答 \(FAQ\)](#)

Citrix Windows 应用程序交付团队一直在快速发布针对 XenApp 和 XenDesktop 产品线的创新功能和增强功能。在 2015 年，每季度都会提供新产品版本。这样的快速创新步伐增强了 XenApp 的用例和 ...

- [XenApp 和 XenDesktop 服务方案](#)

灵活的服务方案实现了可预测的支持。Citrix 经常为 XenApp 和 XenDesktop 提供新的特性和功能，使企业能够保持竞争力、简化 IT 运营、提高数据安全性，并确保员工可在任何地点访问其业务资源。...

- **产品生命周期日期**

请参阅此表了解产品生命周期日期。下方的产品列表提供了其产品生命周期受**生命周期阶段**限制的 Citrix 产品。产品**生命周期里程碑**中包括状态更改通知 (NSC)、销售结束 (EOS)、维护结束 (EOM) 和生命周期结束 (EOL)。...

- **面向 Receiver for Windows 的 LTSR 计划**

对于 Citrix Receiver for Windows、Citrix Receiver for Mac、Citrix Receiver for Linux、Citrix Receiver for HTML5、Citrix Receiver for Java 或 Citrix Receiver for WinCE 的每个主要版本（例如 v3.0），客户将收到最短 4 年的生命周期。生命周期由至少前三年的主要维护阶段后跟扩展维护阶段组成。

# 累积更新 6 (CU6)

Aug 15, 2018

发布日期：2018 年 8 月

累积更新 6 (CU6) 是 XenApp 和 XenDesktop 7.6 长期服务版本 (LTSR) 的最新累积更新。它提供原始 7.6 LTSR 的 7 个**基础组件**的更新。

[自 XenApp 和 XenDesktop 7.6 LTSR CU5 起已修复的问题](#)

[此版本中的已知问题](#)

[下载](#)

[下载 LTSR CU6 \(XenApp\)](#)

[下载 LTSR CU6 \(XenDesktop\)](#)

## 新建部署

如何从头开始部署 CU6？

可以使用 CU6 metainstaller 在 CU6 的基础上设置一个全新的 XenApp 或 XenDesktop 环境。\* 开始执行该操作之前，我们建议您熟悉以下产品：

请仔细阅读 [XenApp 和 XenDesktop 7.6 长期服务版本](#) 文档，并特别注意 [技术概述](#)、[新建部署](#) 和 [安全](#) 部分，然后再开始规划您的部署。请确保您的设置满足所有组件的 [系统要求](#)。按照 [新建部署](#) 中的部署说明进行操作。

\* 注意：Provisioning Services 和 Session Recording 作为单独的下载和安装程序提供。

## 现有部署

如何更新？

CU6 提供 7.6 LTSR 的 7 个**基础组件**的更新。请记住：Citrix 建议您将您的部署中的所有 LTSR 组件更新到 CU6。例如：如果 LTSR 部署中包含 Provisioning Services，请将 Provisioning Services 组件更新到 CU6。如果 Provisioning Services 不属于您的部署的一部分，则不需要安装或更新该组件。

自 7.6 LTSR 版本起，添加了一个 Metainstaller，允许您从单个统一界面中更新 LTSR 环境的现有组件。按照 [升级说明](#) 中的指示，使用 Metainstaller 更新您的部署中的 LTSR 组件。

### 注意

下面是 CU6 版本特定的信息。有关 [LTSR 基础版本](#)、[CU1](#)、[CU2](#)、[CU3](#)、[CU4](#) 或 [CU5](#) 的同类信息，请参阅各自的文档。

LTSR 基础组件	版本	注意
VDA for Desktop OS	7.6.6000	适用于 Windows 10 的特殊规则。请参阅 <a href="#">CU6 兼容的组件和平台</a> 。
VDA for Server OS	7.6.6000	
Delivery Controller	7.6.6000	
Citrix Studio	7.6.6000	
Citrix Director	7.6.6000	
组策略管理体验	2.5.6000	
StoreFront	3.0.6000.1	
Provisioning Services	7.6.7	适用于 Windows 10 的特殊规则。请参阅 <a href="#">CU6 兼容的组件和平台</a> 。
通用打印服务器	7.6.6000	仅支持 Windows 2008 R2 SP1 Windows 2012 Windows 2012 R2
会话录制	7.6.6000	仅限 Platinum Edition

## LTSR CU6 兼容的组件

建议您在 7.6 LTSR CU6 环境中使用以下组件。这些组件无权享有 LTSR 的优势（扩展的生命周期以及仅用于修复的累积更新）。Citrix 可能会要求您在 7.6 LTSR 环境中升级到这些组件的较新版本。

**Windows 10 注意事项：** Windows 10 无法享有 7.6 LTSR 的所有优势。对于包括 Windows 10 计算机的部署，Citrix 建议您使用 VDA for Desktop OS 和 Provisioning Services 的最新 7.15 LTSR 版本。

有关详细信息，请参阅 [Adding Windows 10 Compatibility to XenApp and XenDesktop 7.6 LTSR](#) (向 XenApp 和 XenDesktop 7.6 LTSR 添加 Windows 10 兼容性) 和 [XenApp and XenDesktop Servicing Options \(LTSR\) FAQ](#) (XenApp 和 XenDesktop 服务选项 (LTSR) 常见问题解答)。

LTSR CU6 兼容的组件和平台	版本
Profile Management	7.15.2001

AppDNA	7.14
许可证服务器	11.15.0.0 Build 24100
HDX RealTime Optimization Pack	2.4.1000
Windows 10	VDA 和 Provisioning Services： 最新 7.15 LTSR CU

## Citrix Receiver 的兼容版本

为简化维护过程以及确保实现最佳性能，Citrix 建议您在最新版本的 Citrix Receiver 可用时随时升级到相应版本。可以从 <https://www.citrix.com/downloads/citrix-receiver.html> 下载最新版本。为方便起见，请考虑订阅 [Citrix Receiver RSS 源](#) 以在新版本的 Citrix Receiver 可用时接收通知。

请注意，Citrix Receiver 无法享有 XenApp 和 XenDesktop LTSR 的优势（扩展的生命周期和仅用于修复的累积更新）。Citrix 可能会要求您在 7.6 LTSR 环境中升级到 Citrix Receiver 的较新版本。如果使用的是 Citrix Receiver for Windows，Citrix 已公布特殊的 LTSR 计划。可以从 [Citrix Receiver 的生命周期里程碑](#) 页面获取有关该计划的详细信息。

特别需要指出的是，LTSR 支持以下版本的 Citrix Receiver 以及之后的所有版本：

LTSR Compatible Versions of Citrix Receiver	Version
Citrix Receiver for Android	3.13.9
Citrix Receiver for Chrome	2.6.9
Citrix Receiver for HTML5	2.6.9
Citrix Receiver for iOS	7.5.6
Citrix Receiver for Mac	12.9.1
Citrix Receiver for Linux	13.10
Citrix Receiver for UWP (通用 Windows 平台)	1.0.5
Citrix Receiver for Windows	4.9.3000

## 需注意的 LTSR 排除项目

以下功能、组件和平台无法享有 LTSR 的生命周期里程碑和优势。需要特别指出的是，累积更新和扩展生命周期优势被排除在外。可以通过常规的最新版本获取扩展功能和组件的更新。

### 排除的功能

本地应用程序访问

Framehawk

排除的组件

Linux VDA

Personal vDisk

排除的 Windows 平台\*

Windows 2008 32 位（面向通用打印服务器）

\* Citrix 保留根据第三方供应商的生命周期里程碑更新平台支持的权利。

## 安装和升级分析

当您使用完整产品安装程序部署或升级 XenApp 或 XenDesktop 组件时，将在安装/升级组件的计算机上收集和存储有关安装过程的匿名信息。这些数据用于帮助 Citrix 改善其客户的安装体验。有关详细信息，请参阅 <http://more.citrix.com/XD-INSTALLER>。

## XenApp 6.5 迁移

XenApp 6.5 迁移过程有助于高效快速地从 XenApp 6.5 场过渡到运行 XenApp 7.6（或支持的更高版本）的站点。这在部署中包含大量应用程序和 Citrix 组策略时很有用，可以降低手动将应用程序和 Citrix 组策略移至新 XenApp 站点时意外引入错误的风险。

安装 XenApp 7.6 核心组件并创建站点后，迁移过程按照以下顺序进行：

- 在每个 XenApp 6.5 工作进程上运行 XenApp 7.6 安装程序，将其自动升级到新 Virtual Delivery Agent for Windows Server OS 以便在新站点中使用。
- 在 XenApp 6.5 Controller 上运行 PowerShell 导出 cmdlet，以将应用程序和 Citrix 策略设置导出至 XML 文件。
- 编辑 XML 文件（如果需要），以细化要导入到新站点的内容。通过自定义这些文件，可以将策略和应用程序设置分阶段导入到 XenApp 7.6 站点：即一些现在导入，其他稍后导入。
- 在新 XenApp 7.6 Controller 上运行 PowerShell 导入 cmdlet，以将 XML 文件中的设置导入新 XenApp 站点。
- 根据需要重新配置新站点，然后对其进行测试。

有关详细信息，请参阅[迁移 XenApp 6.x](#)。

# 已修复的问题

Aug 15, 2018

XenApp/XenDesktop 7.6 LTSR 累积更新 6 包含 XenApp 和 XenDesktop 7.6 LTSR、[累积更新 1](#)、[累积更新 2](#)、[累积更新 3](#)、[累积更新 4](#) 和[累积更新 5](#) 中的所有修复以及以下新修复：

## Citrix Director 7.6.6000

- 在将用户分配到计算机时尝试搜索用户可能会失败。选定的用户显示为空。[#LC8395]

## Citrix Studio 7.6.6000

- 升级使用 XenApp 许可证版本的站点时，许可证版本可能会意外从 XenApp 变为 XenDesktop。[LC6981]

## Controller 7.6.6000

- 升级使用 XenApp 许可证版本的站点时，许可证版本可能会意外从 XenApp 变为 XenDesktop。[LC6981]
- 重新启动为 **AlwaysOn 可用性** 配置的 SQL Server 时，许可证功能可能会丢失。[LC8449]
- 在 XenDesktop 7.6 上，映像部署可能会失败。从 Delivery Controller 发送到 Hyper-V 的刷新命令导致过载进而导致超时时会出现该问题。[LC8639]
- 如果虚拟机使用升级或导入的分布式端口组，则尝试使用这些虚拟机创建或更新计算机目录时，可能会显示以下错误消息：**Exception...Current node not found...type = 'network'**（异常...未找到当前节点...类型 =“网络”）[LC8657]
- 在多 Delivery Controller 环境中升级单个 Delivery Controller 时，站点测试报告可能包含不匹配的数据库版本。[LD0073]

## Provisioning Services 7.6.7

### 控制台问题

- 使用不同的域帐户登录 Provisioning Services 控制台时，可能无法访问场。此时将显示以下错误消息：“域/用户没有场的访问权限。” [LC8150]
- Provisioning Services 控制台和配置向导在复杂的 Active Directory 环境中运行时可能会较慢。因此，Provisioning Services 控制台会超时。利用此增强功能，可以在首选域中进行搜索，而不是在所有域中搜索所有组。如果找到正确的组，则可以停止搜索。可以将以下注册表设置为使用不同的搜索选项：  
HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ProvisioningServices  
名称：DomainSelectOption  
类型：DWORD  
值：设置以下值（十进制）表示不同的搜索方法  
0 = Approach-0（默认值）在用户域和 PVS 管理员组所在域（以及加入白名单的其他域（如果已配置））中搜索。

- 1 = Approach-1。使用 Approach-0 进行搜索，然后在用户所在域的其他可信域中搜索。
- 2 = 已弃用
- 3 = 使用 Approach-0 进行搜索，在父域上进一步枚举发现的组。用于特殊的 Active Directory 环境。
- 4 = 使用 Approach-1 进行搜索，在父域上进一步枚举发现的组。用于特殊的 Active Directory 环境。
- 5 = Approach-2。在用户域和 PVS 管理员组所在域（以及加入白名单的其他域（如果已配置））中使用“用户”属性进行“一步式”搜索。用于特殊的 Active Directory 环境。
- 6 = 使用 Approach-2 进行搜索，然后在用户所在域的其他可信域中搜索。[LC9065]

- 默认 Active Directory 搜索选项可能无法在特殊的 Active Directory 环境中查找某些用户的 Provisioning Services 管理员成员身份。此问题与在父域和子域上通过组关联组成员身份的方式有关。[LC9800]

## 服务器问题

- 使用不同的域帐户登录 Provisioning Services 控制台时，可能无法访问场。此时将显示此错误消息：“域/用户没有场的访问权限。” [LC8150]
- Provisioning Services 控制台和配置向导在复杂的 Active Directory 环境中运行时可能会较慢。因此，Provisioning Services 控制台会超时。利用此增强功能，可以在首选域中进行搜索，而不是在所有域中搜索所有组。如果找到正确的组，则可以停止搜索。可以将以下注册表设置为使用不同的搜索选项：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ProvisioningServices

名称：DomainSelectOption

类型：DWORD

值：设置以下值（十进制）表示不同的搜索方法

0 = Approach-0（默认值）在用户域和 PVS 管理员组所在域（以及加入白名单的其他域（如果已配置））中搜索。

1 = Approach-1。使用 Approach-0 进行搜索，然后在用户所在域的其他可信域中搜索。

2 = 已弃用

3 = 使用 Approach-0 进行搜索，在父域上进一步枚举发现的组。用于特殊的 Active Directory 环境。

4 = 使用 Approach-1 进行搜索，在父域上进一步枚举发现的组。用于特殊的 Active Directory 环境。

5 = Approach-2。在用户域和 PVS 管理员组所在域（以及加入白名单的其他域（如果已配置））中使用“用户”属性进行“一步式”搜索。用于特殊的 Active Directory 环境。

6 = 使用 Approach-2 进行搜索，然后在用户所在域的其他可信域中搜索。[LC9065]

- 同时合并两个或更多虚拟磁盘时，MgmtDaemon.exe 进程可能会意外退出。[LC9123]
- 默认 Active Directory 搜索选项可能无法在特殊的 Active Directory 环境中查找某些用户的 Provisioning Services 管理员成员身份。此问题与在父域和子域上通过组关联组成员身份的方式有关。[LC9800]

## 目标设备问题

- 目标设备可能会变得无响应。[LC8897]

## StoreFront 3.0.6000.1

- StoreFront 服务器上可能会出现身份验证失败问题。该问题是由于 TCP 动态端口耗尽所致。[LC8795]
- 在非英语版本的 Microsoft Windows 操作系统中，**DetectReceiver** 字符串可能无法显示在 StoreFront Web 页面上的按钮

上。[LC9713]

# VDA for Desktop OS 7.6.6000

## 键盘

- 在 Android 设备上启动应用程序时，如果您的光标在文本字段中，可能不会自动显示键盘。此外，必须始终触摸键盘按钮进行打开或关闭。[LC8936]

## 会话/连接

- 在将多个可执行文件添加到注册表项 **HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\CtxHook** 下的 **ExcludedImageNames** 时，禁用 Citrix 挂钩可能无法生效。[LC8614]
- 在使用 H 配置的多显示器环境中可能会出现不一致的鼠标移动。启动 Microsoft Skype for Business 会话，然后开始与其他用户共享屏幕。Citrix 图形驱动程序从操作系统收到的鼠标位置不正确。

要启用此修复，请设置以下注册表项：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ICA  
名称：DisableAppendMouse  
值：DWORD  
类型：00000001

但是，在设置该注册表项后使用 HDX 会话时，以编程方式设置鼠标指针位置的某些功能可能无法按预期方式工作。这些功能包括：

- 鼠标对齐功能。
- 在使用 GotoMeeting 屏幕共享的用户之间同步鼠标位置的功能。
- 在使用 Skype for Business 屏幕共享的用户之间同步鼠标位置的功能。[LC8976]
- 当您尝试在会话中访问映射的客户端驱动器且未响应 Citrix Workspace 安全警告对话框时，其他用户的会话可能会变得无响应。[LC9070]
- Citrix Audio Service 可能会意外退出，并再次重新启动。当您从第二个端点（瘦客户端）重新连接到同一个会话时，新设备并不会正确映射到会话。[LC9381]

## 系统异常

- 服务器上的 picadmsys 可能发生致命异常，并显示蓝屏和错误检测代码 0x22。[LC6177]
- 此修复解决了会导致服务器意外退出的 wdica.sys 文件存在的内存问题。[LC7666]
- 服务器上的 picadmsys 可能遇到致命异常，并显示蓝屏和错误检测代码 0x22 (FILE\_SYSTEM)。[LC7726]
- 服务器上的 vdtw30.dll 可能会遇到致命异常，并显示蓝屏和停止代码 SYSTEM\_SERVICE\_EXCEPTION (3b)。[LC8087]
- VDA 上的 picadmsys 可能遇到致命异常，并显示蓝屏和错误检测代码 0x22。[LC8749]
- VDA for Server OS 上的 picadmsys 可能会遇到致命异常，并显示蓝屏和错误检测代码 0x00000050。[LC8753]
- 服务器上的 picadmsys 可能遇到致命异常，并显示蓝屏和错误检测代码

0x000000D1(DRIVER\_IRQL\_NOT\_LESS\_OR\_EQUAL)。[LC8830]

- VDA for Server OS 上的 wdica.sys 可能会遇到致命异常，并显示蓝屏。[LC9695]

## VDA for Server OS 7.6.6000

### 键盘

- 在 Android 设备上启动应用程序时，如果您的光标在文本字段中，可能不会自动显示键盘。此外，必须始终触摸键盘按钮进行打开或关闭。[LC8936]

### 服务器/站点管理

- 通过 Web Interface 或 StoreFront 启动应用程序时，可能会向子域用户显示以下错误消息：

未授予您访问此已发布的应用程序所需的权限。[LC7566]

### 会话/连接

- 在将多个可执行文件添加到注册表项 **HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\CtxHook** 下的 **ExcludedImageNames** 时，禁用 Citrix 挂钩可能无法生效。[LC8614]
- 远程桌面会话断开连接并重新连接时，可能会在 VDA for Server OS 上创建虚假的 XenApp 会话。[LC8706]
- 升级到 XenApp 7.6 长期服务版本 (LTSR) 累积更新 4 后，登录已发布的应用程序时可能会有五秒延迟。[LC8894]
- 在使用 H 配置的多显示器环境中可能会出现不一致的鼠标移动。启动 Microsoft Skype for Business 会话，然后开始与其他用户共享屏幕。Citrix 图形驱动程序从操作系统收到的鼠标位置不正确。

要启用此修复，请设置以下注册表项：

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ICA**

名称：DisableAppendMouse

值：DWORD

类型：00000001

但是，在设置该注册表项后使用 HDX 会话时，以编程方式设置鼠标指针位置的某些功能可能无法按预期方式工作。这些功能包括：

- 鼠标对齐功能。
- 在使用 GotoMeeting 屏幕共享的用户之间同步鼠标位置的功能。
- 在使用 Skype for Business 屏幕共享的用户之间同步鼠标位置的功能。[LC8976]
- 当您尝试在会话中访问映射的客户端驱动器且未响应 Citrix Workspace 安全警告对话框时，其他用户的会话可能会变得无响应。[LC9070]
- Citrix Audio Service 可能会意外退出，并再次重新启动。当您从第二个端点（瘦客户端）重新连接到同一个会话时，新设备并不会正确映射到会话。[LC9381]

### 系统异常

- 服务器上的 picadm.sys 可能发生致命异常，并显示蓝屏和错误检测代码 0x22。[LC6177]

- 此修复解决了会导致服务器意外退出的 wdica.sys 文件存在的内存问题。[LC7666]
- 服务主机 (svchost.exe) 进程可能会遇到访问冲突并意外退出。icaendpoint.dll 模块出错导致出现此问题。[LC7694]
- 服务器上的 picadm.sys 可能遇到致命异常，并显示蓝屏和错误检测代码 0x22 (FILE\_SYSTEM)。[LC7726]
- 服务器上的 vdtw30.dll 可能会遇到致命异常，并显示蓝屏和停止代码 SYSTEM\_SERVICE\_EXCEPTION (3b)。[LC8087]
- VDA 上的 picadm.sys 可能遇到致命异常，并显示蓝屏和错误检测代码 0x22。[LC8749]
- VDA for Server OS 上的 picadm.sys 可能会遇到致命异常，并显示蓝屏和错误检测代码 0x00000050。[LC8753]
- 服务器上的 picadm.sys 可能遇到致命异常，并显示蓝屏和错误检测代码 0x000000D1(DRIVER\_IRQL\_NOT\_LESS\_OR\_EQUAL)。[LC8830]
- VDA for Server OS 上的 wdica.sys 可能会遇到致命异常，并显示蓝屏。[LC9695]

## 用户体验

- 在 VDA for Server OS 上，鼠标光标可能会从会话中消失。光标变为文本选择光标并且背景色与文本选择光标的颜色相同时会出现此问题。Microsoft Windows 中的可编辑区域的默认背景色为白色，而默认文本选择光标颜色也是白色。因此，光标可能不再可见。[LC8807]
- 将屏幕分辨率显示调整为中或较大后，可能会显示两个鼠标指针，导致出现模糊的指针体验。在 VDA 端而不是 Citrix Workspace 端呈现光标时会出现该问题。[LC9373]

# 累积更新 5 (CU5)

Feb 06, 2018

发布日期：2018 年 2 月

累积更新 5 (CU5) 是 XenApp 和 XenDesktop 7.6 长期服务版本 (LTSR) 的最新累积更新。CU5 提供原始 7.6 LTSR 的 10 个基础组件的更新。

[自 XenApp 和 XenDesktop 7.6 LTSR CU4 起已修复的问题](#)

[此版本中的已知问题](#)

[下载](#)

[下载 LTSR CU5 \(XenApp\)](#)

[下载 LTSR CU5 \(XenDesktop\)](#)

## 新建部署

如何从头开始部署 CU5？

可以使用 CU5 metainstaller 在 CU5 的基础上设置一个全新的 XenApp 或 XenDesktop 环境。\* 开始执行该操作之前，我们建议您熟悉以下产品：

请仔细阅读 [XenApp 和 XenDesktop 7.6 长期服务版本](#) 文档，并特别注意[技术概述](#)、[新建部署](#)和[安全](#)部分，然后再开始规划您的部署。请确保您的设置满足所有组件的[系统要求](#)。按照[新建部署](#)中的部署说明进行操作。

\* 注意：Provisioning Services 和 Session Recording 作为单独的下载和安装程序提供。

## 现有部署

如何更新？

CU5 提供 7.6 LTSR 的 10 个基础组件的更新。请记住：Citrix 建议您将您的部署中的所有 LTSR 组件更新到 CU5。例如：如果 LTSR 部署中包含 Provisioning Services，请将 Provisioning Services 组件更新到 CU5。如果 Provisioning Services 不属于您的部署的一部分，则不需要安装或更新该组件。

自 7.6 LTSR 版本起，添加了一个 Metainstaller，允许您从单个统一界面中更新 LTSR 环境的现有组件。按照[升级说明](#)中的指示，使用 Metainstaller 更新您的部署中的 LTSR 组件。

### 注意

下面是 CU5 版本特定的信息。有关 [LTSR 基础版本](#)、[CU1](#)、[CU2](#)、[CU3](#) 或 [CU4](#) 的同类信息，请参阅各自的文档。

LTSR 基础组件	版本	注意
VDA for Desktop OS	7.6.5000	适用于 Windows 10 的特殊规则。请参阅 <a href="#">CU5 兼容的组件和平台</a> 。
VDA for Server OS	7.6.5000	
Delivery Controller	7.6.5000	
Citrix Studio	7.6.5000	
Citrix Director	7.6.5000	
组策略管理体验	2.5.5000	
StoreFront	3.0.5000.1	
Provisioning Services	7.6.6	适用于 Windows 10 的特殊规则。请参阅 <a href="#">CU5 兼容的组件和平台</a> 。
通用打印服务器	7.6.5000	仅支持 Windows 2008 R2 SP1 Windows 2012 Windows 2012 R2
会话录制	7.6.5000	仅限 Platinum Edition

## LTSR CU5 兼容的组件

建议您在 7.6 LTSR CU5 环境中使用以下组件。这些组件无权享有 LTSR 的优势（扩展的生命周期以及仅用于修复的累积更新）。Citrix 可能会要求您在 7.6 LTSR 环境中升级到这些组件的较新版本。

**Windows 10 注意事项：** Windows 10 无法享有 7.6 LTSR 的所有优势。对于包括 Windows 10 计算机的部署，Citrix 建议您使用 VDA for Desktop OS 和 Provisioning Services 的最新 7.15 LTSR 版本。

有关详细信息，请参阅 [Adding Windows 10 Compatibility to XenApp and XenDesktop 7.6 LTSR](#) (向 XenApp 和 XenDesktop 7.6 LTSR 添加 Windows 10 兼容性) 和 [XenApp and XenDesktop Servicing Options \(LTSR\) FAQ](#) (XenApp 和 XenDesktop 服务选项 (LTSR) 常见问题解答)。

LTSR CU5 兼容的组件和平台	版本
Profile Management	7.15.1000

AppDNA	7.14
许可证服务器	11.14.0.1 Build 22103
HDX RealTime Optimization Pack	2.4
Windows 10	VDA 和 Provisioning Services： 最新 7.15 LTSR CU

## Citrix Receiver 的兼容版本

为简化维护过程以及确保实现最佳性能，Citrix 建议您在最新版本的 Citrix Receiver 可用时随时升级到相应版本。可以从 <https://www.citrix.com/downloads/citrix-receiver.html> 下载最新版本。为方便起见，请考虑订阅 [Citrix Receiver RSS 源](#) 以在新版本的 Citrix Receiver 可用时接收通知。

请注意，Citrix Receiver 无法享有 XenApp 和 XenDesktop LTSR 的优势（扩展的生命周期和仅用于修复的累积更新）。Citrix 可能会要求您在 7.6 LTSR 环境中升级到 Citrix Receiver 的较新版本。如果使用的是 Citrix Receiver for Windows，Citrix 已公布特殊的 LTSR 计划。可以从 [Citrix Receiver 的生命周期里程碑](#) 页面获取有关该计划的详细信息。

特别需要指出的是，LTSR 支持以下版本的 Citrix Receiver 以及之后的所有版本：

LTSR Compatible Versions of Citrix Receiver	Version
Citrix Receiver for Android	3.13.2
Citrix Receiver for Chrome	2.6.2
Citrix Receiver for HTML5	2.6.2
Citrix Receiver for iOS	7.5
Citrix Receiver for Mac	12.8.1
Citrix Receiver for Linux	13.8
Citrix Receiver for UWP (通用 Windows 平台)	1.0.5
Citrix Receiver for Windows	4.9

## 需注意的 LTSR 排除项目

以下功能、组件和平台无法享有 LTSR 的生命周期里程碑和优势。需要特别指出的是，累积更新和扩展生命周期优势被排除在外。可以通过常规的最新版本获取扩展功能和组件的更新。

排除的功能

本地应用程序访问

Framehawk

排除的组件

Linux VDA

Personal vDisk

排除的 Windows 平台\*

Windows 2008 32 位（面向通用打印服务器）

\* Citrix 保留根据第三方供应商的生命周期里程碑更新平台支持的权利。

## 安装和升级分析

当您使用完整产品安装程序部署或升级 XenApp 或 XenDesktop 组件时，将在安装/升级组件的计算机上收集和存储有关安装过程的匿名信息。这些数据用于帮助 Citrix 改善其客户的安装体验。有关详细信息，请参阅 <http://more.citrix.com/XD-INSTALLER>。

## XenApp 6.5 迁移

XenApp 6.5 迁移过程有助于高效快速地从 XenApp 6.5 场过渡到运行 XenApp 7.6（或支持的更高版本）的站点。这在部署中包含大量应用程序和 Citrix 组策略时很有用，可以降低手动将应用程序和 Citrix 组策略移至新 XenApp 站点时意外引入错误的风险。

安装 XenApp 7.6 核心组件并创建站点后，迁移过程按照以下顺序进行：

- 在每个 XenApp 6.5 工作进程上运行 XenApp 7.6 安装程序，将其自动升级到新 Virtual Delivery Agent for Windows Server OS 以便在新站点中使用。
- 在 XenApp 6.5 Controller 上运行 PowerShell 导出 cmdlet，以将应用程序和 Citrix 策略设置导出至 XML 文件。
- 编辑 XML 文件（如果需要），以细化要导入到新站点的内容。通过自定义这些文件，可以将策略和应用程序设置分阶段导入到 XenApp 7.6 站点：即一些现在导入，其他稍后导入。
- 在新 XenApp 7.6 Controller 上运行 PowerShell 导入 cmdlet，以将 XML 文件中的设置导入新 XenApp 站点。
- 根据需要重新配置新站点，然后对其进行测试。

有关详细信息，请参阅[迁移 XenApp 6.x](#)。

# 已修复的问题

Feb 06, 2018

XenApp/XenDesktop 7.6 LTSR 累积更新 5 包含 XenApp 和 XenDesktop 7.6 LTSR、[累积更新 1](#)、[累积更新 2](#)、[累积更新 3](#) 和[累积更新 4](#) 中的所有修复以及以下新修复：

## Citrix Director

- 您（即自定义管理员）无法从计算机目录中获取 Remote PC 设置时可能会出现异常。您有权管理计算机目录，但作用域不包含特定的目录时会出现此问题。[#LC8170]

## Citrix 策略

- 可能无法执行同时包含 Citrix 和 Microsoft 设置的组策略对象。列表中的扩展单元包含两个以上的 GUID 时会出现此问题。[#LC7533]
- 打开组策略编辑器 (gpedit.msc) 的第二个实例时，“Citrix 策略”节点将不打开，并且可能会显示以下错误消息：“Unhandled exception in managed code.”（托管代码管理单元中出现未处理的异常。）[#LC7600]
- 本地策略缓存文件夹 (%ProgramData%/CitrixCseCache) 中的文件设置为“只读”时，可能无法成功应用策略设置。[#LC8750]

## Citrix Studio

- 尝试为用户关联使用“NETBIOS”名称向交付组中添加计算机可能会失败。相反，域名可能会显示。NETBIOS 名称使用错误的 URL 时会出现此问题。[#LC7830]

## Controller

- 尝试为用户关联使用“NETBIOS”名称向交付组中添加计算机可能会失败。相反，域名可能会显示。NETBIOS 名称使用错误的 URL 时会出现此问题。[#LC7830]
- 此问题的症状可能各不相同，并且会观察到以下影响：
  - PowerShell 查询在大型（5000 多个 VDA）站点中可能会超时。
  - 站点的大小导致 Citrix Studio 搜索请求可能会非常缓慢或超时。
  - 查询长时间运行时，可能会在 Delivery Controller 中记录事件 ID 1201“Connection to the database has been lost – Exception Timeout expired”（与数据库的连接已断开 - 异常超时已过期）。[#LC7833]
- 面向服务器操作系统中的会话的 **AllowRestart** 策略不允许您从断开连接的会话中注销。重新启动断开连接的会话时，该会话将重新连接到以前的会话，而非启动新会话。[#LC8090]
- 由于 SQL 数据库中存在死锁，Delivery Controller 与 SQL Server 之间的连接可能会间歇性断开。[#LC8477]
- 在大型 XenApp 和 XenDesktop 环境中，如果监视数据库的大小非常大，监视数据库整理的存储过程将无法正确运行。

## 安装程序

- 读取和写入权限（仅限遍历权限）限制到包含安装介质的文件夹的父文件夹时，尝试从共享文件夹安装 VDA 软件可能会失败。显示以下错误消息：

“A non-recoverable error occurred during a database lookup.” (数据库查询过程中出现不可恢复的错误。) [#LC6520]

## Provisioning Services

### 控制台问题

- 创建模板虚拟机后，XenDesktop 设置向导可能会失败。[# LC8018]

### 服务器问题

- 为 DHCP 发现、提供、请求和确认 (DORA) 过程配置了 Boot Device Manager (BDM) 时，该过程可能无法完成。DHCP 中继发送“OFFER”数据包作为 UNICAST 数据包时会出现此问题。[#LC8130]
- 使用“MCLI Add DiskLocator”命令添加现有虚拟磁盘时，将同一磁盘标识符错误地分配给位于不同存储中的虚拟磁盘。[# LC8281]

### 目标问题

- 目标设备可能会变得无响应。[# LC7911]

## Session Recording (Agent)

- user1 启动 VDA1 提供的正在录制的会话，但不关闭 session1 中的通知消息时，通知消息将不在 VDA1 提供的 session2 中显示。如果在 user1 手动关闭 session1 中的通知消息之前会话由 user2 启动，则会出现此问题。[#LC8132]

## StoreFront

- 升级 StoreFront 之后，尝试登录其中一个服务器会导致该服务器不显示用户的应用程序订阅数据。出现此问题是因为 Microsoft 对等网格限制，由于存在该限制，其中一个对等机在尝试执行第一次网格操作之前可能检测不到自身。[#LC1454]
- 在启用了自动启动桌面设置的情况下，**Multiple launch prevention**（多次启动保护）选项可能不起作用。因此，后续启动相同的桌面实例的请求将失败。[#LC7430]
- 升级非默认驱动器上安装的 StoreFront 2.6 后，可能不会保留用户的应用程序订阅数据。[#LC8046]
- 尝试查看桌面的详细信息时，可能会显示查看过的桌面的详细信息。[#LC8062]
- 在启用了套接字池的情况下，如果站点数据库连接不一致，则当您连续登录并注销时，StoreFront 中的套接字可能会用尽。

# VDA for Desktop OS

## HDX MediaStream Flash 重定向

- 尝试保存 Microsoft Office 文件（例如在启用了 HDX 无缝应用程序中运行的 Microsoft Excel 电子表格）会导致文件意外退出。[#LC8572]

## 打印

- 已发布的应用程序等待 Citrix Print Manager Service (cpsvc.exe) 中的 mutex 对象时，尝试启动该应用程序可能会失败。[#LC6829]
- 通过在已发布的应用程序中选择“首选项”保存打印机属性后，当您注销并重新登录到会话时，这些设置可能无法恢复。从用户设备重定向的网络打印机上会出现此问题。[#LC7770]

## 服务器/站点管理

- 对视觉效果下的高级系统设置所做的更改应用于当前 VDA for Desktop OS 会话，但可能不会保留到后续会话中。为了永久保持此类更改，请设置以下注册表项：

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix

名称：EnableVisualEffect

类型：DWORD

值：1 [#LC8049]

## 会话/连接

- 启动用于视频会议的具有灵活分辨率的某些第三方应用程序时，该应用程序可能会意外退出。[#LC6994]
- 建立 Skype for Business 视频通话时，与第三方应用程序的窗口相交后可能会显示一个蓝色的窗口边框。[#LC7773]
- 使用旧图形模式时，VDA for Desktop OS 上运行的会话可能会变得无响应。出现此问题时，您可能无法更新 Desktop Viewer 上的任何内容，但 Desktop Viewer 不处于无响应状态。此外，30-60 分钟后，以前无响应的会话将恢复。[#LC7777]
- 在启用了本地应用程序访问的情况下，使用交互式登录免责声明策略可能会导致出现黑屏或灰屏。[#LC7798]
- 在版本 7.9 VDA 上运行的两个 Microsoft Excel 2010 工作表之间执行插入操作时，Excel 窗口可能会变得无响应。[#LC7912]
- 在某些情况下，无缝应用程序可能不会在无缝模式下显示，或者某些功能可能不起作用。[#LC8030]
- 多次最大化并还原已发布的应用程序之后，鼠标光标可能显示不正确，并且该应用程序无法垂直和水平扩展。此外，该应用程序不覆盖整个屏幕，并且显示黑色边框。[#LC8988]

## 智能卡

- 使用智能卡登录某个会话时，该会话可能会变得无响应，直至您断开并重新连接会话。[#LC8036]
- Citrix Smart Card Service 可能在 VDA 上意外退出。[#LC8386]

## 系统异常

- wfshell.exe 进程可能会意外退出，指向任务栏分组模块。[#LC6968]
- 在安装了 Hotfix Rollup Pack 7 的系统上，服务器上的 picadmsys 可能发生致命异常，并显示蓝屏和错误检测代码 0x00000050 (PAGE\_FAULT\_IN\_NONPAGED\_AREA)。[#LC6985]
- 服务器上的 picadmsys 可能发生致命异常，并显示蓝屏和错误检测代码 0x22。[#LC7574]
- 在 vdtw30.dll 上服务器可能会遇到致命异常，显示蓝屏和停止代码 0xc0000006。[#LC7608]
- 在 tdica.sys 上 VDA 可能会遇到致命异常，显示蓝屏和缺陷检查代码。[#LC7632]
- VDA 可能会遇到致命异常，显示蓝屏和错误检测代码 0x7E。将 VDA 会话保持空闲状态一段时间时会出现此问题。[#LC8045]

## 用户体验

- Windows Media Player 可能会将 Microsoft AVI (.avi) 文件格式显示为垂直翻转。[#LC8308]
- 尝试登录以前锁定的会话之后，带登录提示的屏幕可能无法刷新。[#LC8774]

# VDA for Server OS

## HDX MediaStream Flash 重定向

- 尝试保存 Microsoft Office 文件（例如在启用了 HDX 无缝应用程序中运行的 Microsoft Excel 电子表格）会导致文件意外退出。[#LC8572]

## 打印

- 已发布的应用程序等待 Citrix Print Manager Service (cpsvc.exe) 中的 mutex 对象时，尝试启动该应用程序可能会失败。[#LC6829]
- 通过在已发布的应用程序中选择“首选项”保存打印机属性后，当您注销并重新登录到会话时，这些设置可能无法恢复。从用户设备重定向的网络打印机上会出现此问题。[#LC7770]

## 服务器/站点管理

- 对视觉效果下的高级系统设置所做的更改应用于当前 VDA for Desktop OS 会话，但可能不会保留到后续会话中。为了永久保持此类更改，请设置以下注册表项：

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix

名称：EnableVisualEffect

类型：DWORD

值：1 [#LC8049]

## 会话/连接

- 尝试重新连接到会话可能会间歇性失败，并导致 VDA for Server OS 进入“正在初始化”状态。在 Delivery Controller 中再次注册 VDA 时会出现此问题。[#LC6647]

- 在会话启动的进度条上单击“取消”时，错误的会话信息可能会保留在 Delivery Controller 中。因此，将不在 VDA 上创建实际的会话，并且您可能无法启动新会话。[#LC6779]
- 在取消停靠便携式计算机后，会话共享可能会失败。在客户端自动重新连接期间触发无序通知时，VDA 向 Delivery Controller 重新注册，此时会出现此问题。[#LC7450]
- 即使在将客户端麦克风重定向策略值设置为禁止时，也可能会在用户会话中间歇性重定向麦克风。

此修复解决了该问题。但是，如果您仍遇到该问题，请在配有麦克风的设备上应用以下注册表项：

- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\ica-tcp\AudioConfig  
名称：MaxPolicyAge  
类型：DWORD  
值：允许上次策略评估时间与端点激活时间之间间隔的最长时间（秒）。默认值为 30 秒。
- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\ica-tcp\AudioConfig  
名称：PolicyTimeout  
类型：DWORD  
值：确定策略非最新后系统等待策略的最长时间（单位为毫秒）。默认为 4,000 毫秒。出现超时时，系统将读取策略并继续进行初始化。将此值设置为 (0) 将跳过 Active Directory 策略检查并立即处理策略。[#LC7495]
- 建立 Skype for Business 视频通话时，与第三方应用程序的窗口相交后可能会显示一个蓝色的窗口边框。[#LC7773]
- 使用旧图形模式时，VDA for Desktop OS 上运行的会话可能会变得无响应。出现此问题时，您可能无法更新 Desktop Viewer 上的任何内容，但 Desktop Viewer 不处于无响应状态。此外，30-60 分钟后，以前无响应的会话将恢复。[#LC7777]
- 在 VDA for Server OS 上，远程桌面会话接管控制台会话时，可能会在 Citrix Studio 中显示一个虚假的 XenApp 会话。[#LC7826]
- 在版本 7.9 VDA 上运行的两个 Microsoft Excel 2010 工作表之间执行插入操作时，Excel 窗口可能会变得无响应。[#LC7912]
- 在某些情况下，无缝应用程序可能不会在无缝模式下显示，或者某些功能可能不起作用。[#LC8030]
- 服务器上的 RPM.dll 可能会变得无响应，并显示以下错误消息：  
“错误 ID 1009，picadm: 等待来自客户端的响应消息超时”[#LC8339]
- 多次最大化并还原已发布的应用程序之后，鼠标光标可能显示不正确，并且该应用程序无法垂直和水平扩展。此外，该应用程序不覆盖整个屏幕，并且显示黑色边框。[#LC8988]

## 智能卡

- 使用智能卡登录某个会话时，该会话可能会变得无响应，直至您断开并重新连接会话。[#LC8036]
- Citrix Smart Card Service 可能在 VDA 上意外退出。[#LC8386]

## 系统异常

- wfshell.exe 进程可能会意外退出，指向任务栏分组模块。[#LC6968]
- 在安装了 Hotfix Rollup Pack 7 的系统上，服务器上的 picadmsys 可能发生致命异常，并显示蓝屏和错误检测代码 0x00000050 (PAGE\_FAULT\_IN\_NONPAGED\_AREA)。[#LC6985]
- 服务器上的 picadmsys 可能发生致命异常，并显示蓝屏和错误检测代码 0x22。[#LC7574]

- 在 vdtw30.dll 上服务器可能会遇到致命异常，显示蓝屏和停止代码 0xc0000006。[#LC7608]
- 在 tdica.sys 上 VDA 可能会遇到致命异常，显示蓝屏和缺陷检查代码。[#LC7632]
- 服务主机 (svchost.exe) 进程可能会遇到访问冲突并意外退出。icaendpoint.dll 模块出错导致出现此问题。[#LC7900]
- 服务器上的 icardd.dll 可能会遇到致命异常，并显示蓝屏和错误检测代码 0x0000003B。[#LC8492]
- 服务器上的 icardd.dll 可能会遇到致命异常，并显示蓝屏和错误检测代码 0x0000003B。[#LC8732]

## 用户体验

- Windows Media Player 可能会将 Microsoft AVI (.avi) 文件格式显示为垂直翻转。[#LC8308]

## 用户界面

- 尝试从 Microsoft Windows Server 2008 R2 桌面会话中注销时，可能不会显示注销屏幕。您可能无法从会话中注销，但会话将显示为好像已意外断开连接。[#LC8016]

# 虚拟桌面组件 - 其他

- 使用连接组时，位于虚拟文件系统 (VFS) 服务器外部或者网络驱动器上的 App-V 应用程序可能无法正确运行。[#LC6837]

# 累积更新 4 (CU4)

Jun 19, 2017

发布日期：2017 年 6 月

累积更新 4 (CU4) 是 XenApp 和 XenDesktop 7.6 长期服务版本 (LTSR) 的最新累积更新。CU4 提供原始 7.6 LTSR 的 10 个[基础组件](#)的更新。

[自 XenApp 和 XenDesktop 7.6 LTSR CU3 起已修复的问题](#)

[此版本中的已知问题](#)

[下载](#)

[下载 LTSR CU4 \(XenApp\)](#)

[下载 LTSR CU4 \(XenDesktop\)](#)

## 新建部署

如何从头开始部署 CU4？

可以使用 CU4 Metainstaller 在 CU4 的基础上设置一个全新的 XenApp 或 XenDesktop 环境。<sup>\*</sup> 开始执行该操作之前，我们建议您熟悉以下产品：

请仔细阅读 [XenApp 和 XenDesktop 7.6 长期服务版本文档](#)，并特别注意[技术概述](#)、[新建部署](#)和[安全部分](#)，然后再开始规划您的部署。请确保您的设置满足所有组件的[系统要求](#)。按照[新建部署](#)中的部署说明进行操作。

<sup>\*</sup> 注意：Provisioning Services 和 Session Recording 作为单独的下载和安装程序提供。

## 现有部署

如何更新？

CU4 提供 7.6 LTSR 的 10 个[基础组件](#)的更新。请记住：Citrix 建议您将您的部署中的所有 LTSR 组件更新到 CU4。例如：如果 LTSR 部署中包含 Provisioning Services，则将 Provisioning Services 组件更新到 CU4。如果 Provisioning Services 不属于您的部署的一部分，则不需要安装或更新该组件。

自 7.6 LTSR 版本起，添加了一个 Metainstaller，允许您从单个统一界面中更新 LTSR 环境的现有组件。按照[升级说明](#)中的指示，使用 Metainstaller 更新您的部署中的 LTSR 组件。

### 注意

下面是 CU4 版本特定的信息。有关[LTSR 基础版本](#)、[CU1](#)、[CU2](#) 或 [CU3](#) 的此类信息，请参阅各自的文档。

LTSR 基础组件	版本	注意
VDA for Desktop OS	7.6.4000	适用于 Windows 10 的特殊规则。请参阅 <a href="#">CU4 兼容的组件和平台</a> 。
VDA for Server OS	7.6.4000	
Delivery Controller	7.6.4000	
Citrix Studio	7.6.4000	
Citrix Director	7.6.4000	
组策略管理体验	2.5.4000	
StoreFront	3.0.4000	
Provisioning Services	7.6.5	适用于 Windows 10 的特殊规则。请参阅 <a href="#">CU4 兼容的组件和平台</a> 。
通用打印服务器	7.6.4000	仅支持 Windows 2008 R2 SP1 Windows 2012 Windows 2012 R2
会话录制	7.6.4000	仅限 Platinum Edition

## LTSR CU4 兼容的组件

建议您在 7.6 LTSR CU4 环境中使用以下组件。这些组件无权享有 LTSR 的优势（扩展的生命周期以及仅用于修复的累积更新）。Citrix 可能会要求您在 7.6 LTSR 环境中升级到这些组件的较新版本。

**Windows 10 注意事项：**可以通过当前版本路径获取对 Windows 10 的常规支持。Windows 10 无法享有 7.6 LTSR 的所有优势。对于包括 Windows 10 计算机的部署，Citrix 建议您使用 [VDA for Desktop OS](#) 和 [Provisioning Services](#) 的当前发布版本 7.9 或更高版本。

有关详细信息，请参阅 [Adding Windows 10 Compatibility to XenApp and XenDesktop 7.6 LTSR](#)（向 XenApp 和 XenDesktop 7.6 LTSR 添加 Windows 10 兼容性）和 [XenApp and XenDesktop Servicing Options \(LTSR\) FAQ](#)（XenApp 和 XenDesktop 服务选项 (LTSR) 常见问题解答）。

LTSR CU4 兼容的组件和平台	版本
Profile Management	5.8

AppDNA	7.14
许可证服务器	11.14.0 Build 20101
HDX RealTime Optimization Pack	2.2.100
Windows 10	VDA: 7.9 或更高的版本 Provisioning Services : 7.9 或更高版本

## Citrix Receiver 的兼容版本

为简化维护过程以及确保实现最佳性能，Citrix 建议您在最新版本的 Citrix Receiver 可用时随时升级到相应版本。可以从 <https://www.citrix.com/downloads/citrix-receiver.html> 下载最新版本。为方便起见，请考虑订阅 [Citrix Receiver RSS 源](#) 以便在新版本的 Citrix Receiver 可用时接收通知。

请注意，Citrix Receiver 无法享有 XenApp 和 XenDesktop LTSR 的优势（扩展的生命周期和仅用于修复的累积更新）。Citrix 可能会要求您在 7.6 LTSR 环境中升级到 Citrix Receiver 的较新版本。如果使用的是 Citrix Receiver for Windows，Citrix 已公布特殊的 LTSR 计划。可以从 [Citrix Receiver 的生命周期里程碑](#) 页面获取有关该计划的详细信息。

特别需要指出的是，LTSR 支持以下版本的 Citrix Receiver 以及之后的所有版本：

Citrix Receiver 的 LTSR 兼容版本	版本
Citrix Receiver for Windows	4.4 或更高版本
Citrix Receiver for Linux	13.5 或更高版本
Citrix Receiver for Mac	12.5 或更高版本
Citrix Receiver for Chrome	2.4 或更高版本
Citrix Receiver for HTML5	2.4 或更高版本
Citrix Receiver for iOS	7.2 或更高版本
Citrix Receiver for Android	3.11.1 或更高版本

## 需注意的 LTSR 排除项目

以下功能、组件和平台无法享有 LTSR 的生命周期里程碑和优势。需要特别指出的是，累积更新和扩展生命周期优势被排除在外。可以通过常规的最新版本获取扩展功能和组件的更新。

排除的功能

本地应用程序访问

Framehawk

排除的组件

Linux VDA

Personal vDisk

排除的 Windows 平台\*

Windows 2008 32 位（面向通用打印服务器）

\* Citrix 保留根据第三方供应商的生命周期里程碑更新平台支持的权利。

## 安装和升级分析

当您使用完整产品安装程序部署或升级 XenApp 或 XenDesktop 组件时，将在安装/升级组件的计算机上收集和存储有关安装过程的匿名信息。这些数据用于帮助 Citrix 改善其客户的安装体验。有关详细信息，请参阅 <http://more.citrix.com/XD-INSTALLER>。

## XenApp 6.5 迁移

XenApp 6.5 迁移过程有助于高效快速地从 XenApp 6.5 场过渡到运行 XenApp 7.6（或支持的更高版本）的站点。这在部署中包含大量应用程序和 Citrix 组策略时很有用，可以降低手动将应用程序和 Citrix 组策略移至新 XenApp 站点时意外引入错误的风险。

安装 XenApp 7.6 核心组件并创建站点后，迁移过程按照以下顺序进行：

- 在每个 XenApp 6.5 工作进程上运行 XenApp 7.6 安装程序，将其自动升级到新 Virtual Delivery Agent for Windows Server OS 以便在新站点中使用。
- 在 XenApp 6.5 Controller 上运行 PowerShell 导出 cmdlet，以将应用程序和 Citrix 策略设置导出至 XML 文件。
- 编辑 XML 文件（如果需要），以细化要导入到新站点的内容。通过自定义这些文件，可以将策略和应用程序设置分阶段导入到 XenApp 7.6 站点：即一些现在导入，其他稍后导入。
- 在新 XenApp 7.6 Controller 上运行 PowerShell 导入 cmdlet，以将 XML 文件中的设置导入新 XenApp 站点。
- 根据需要重新配置新站点，然后对其进行测试。

有关详细信息，请参阅[迁移 XenApp 6.x](#)。



# 已修复的问题

Jun 19, 2017

XenApp/XenDesktop 7.6 LTSR 累积更新 4 包含 XenApp 和 XenDesktop 7.6 LTSR、[累积更新 1](#)、[累积更新 2](#) 和[累积更新 3](#) 中的所有修复以及以下新修复：

## Citrix Director

- 尝试使用 Citrix Director 重置 Citrix 用户配置文件可能会失败，导致出现以下错误消息：

“无法启动重置进程。”

Citrix Director 仅发送用户名而不是与域名一起发送用户名时会出现此问题。因此，Citrix Broker Service 无法在 DDC 域中找到用户。

[#LC6681]

## Citrix Studio

- Microsoft 管理控制台在将计算机添加到目录时可能变得不再响应。

[#LC5334]

- 尝试发布包含具有多个文件类型关联的特定第三方应用程序的 App-V 包可能会失败，导致出现以下错误消息：

“Cannot validate argument on parameter 'ExtensionName'. The character length of the 28 argument is too long. Shorten the character length of the argument so it is fewer than or equal to "16" characters, and then try the command again.” (无法验证参数“ExtensionName”中的参数。参数的 28 个字符长度太长。请缩短参数的字符长度，使其不超过 16 个字符，然后重新尝试该命令。)

尝试向 Citrix Studio 添加 App-V 包时会出现此问题。

[#LC6507]

- 在访问策略“IncludedClientIPFilterEnabled”设置为启用的情况下，在 Citrix Studio 中单击“编辑交付组”时，可能会显示以下错误消息：

“用户配置已手动修改，无法通过 Studio 更改。”

[#LC6620]

- 尝试在 Citrix Studio 中向 Citrix Provisioning Services 目录添加虚拟机时，可能会出现以下错误消息：

“计算机“虚拟机名称”已在计算机目录中存在。”

[#LC6944]

## Controller

- Configuration Logging Service 可能会占用过多内存，导致 Delivery Controller 无响应。  
[#LC6480]
- 尝试删除由 Machine Creation Services 创建的虚拟机会导致 Citrix Studio 无响应。  
[#LC6581]
- 在访问策略“IncludedClientIPFilterEnabled”设置为启用的情况下，在 Citrix Studio 中单击“编辑交付组”时，可能会显示以下错误消息：  
“用户配置已手动修改，无法通过 Studio 更改。”  
[#LC6620]
- 成功从 MCS 目录中删除某个计算机后，Citrix Studio 的“日志记录”选项卡上将显示以下失败任务通知：  
正在锁定池 catalog\_name  
[#LC6653]
- Citrix Studio 中的“计算机目录”节点在选中后需要几分钟时间才能显示其内容。  
[#LC6756]
- 尝试在 Citrix Studio 中向 Citrix Provisioning Services 目录添加虚拟机时，可能会出现以下错误消息：  
“计算机“虚拟机名称”已在计算机目录中存在。”  
[#LC6944]
- 对于可以选择以接受新计算机的多个存储，尝试向现有 Machine Creation Services 目录中添加计算机可能不会遵循轮询方法。  
[#LC7456]

## HDX MediaStream Flash 重定向

- 配置了兼容性列表策略后，在客户端上 Flash 内容可能无法正确重定向。  
[#LC6892]
- Qumu.com 上的 Flash 内容无法加载，且 Web 站点被动态加入黑名单，会出现以下错误消息：“客户端的 Flash Player 无法直接从客户端设备提取 Flash 内容。浏览器页面将刷新，如果服务器端 Flash 呈现功能可用，将使用该功能。”  
[#LC6934]
- 在 Microsoft Internet Explorer 中启用了兼容性视图的情况下，某些具有 Flash 内容的第三方 Web 站点可能无法运行。  
[#LC7513]

## Provisioning Services

## 服务器

- 使用 SQL Server 的默认实例时，尝试使用 Provisioning Services 配置向导通过“加入现有场”选项配置 Provisioning Server 可能会失败。

[#LC6579]

## 目标设备

- Provisioning Services 目标设备可能会遇到致命异常，显示蓝屏。

[#LC6604]

- 尝试从 Provisioning Services 控制台重新启动或关闭目标设备可能会失败。

[#LC6814]

- Provisioning Services 目标设备可能会遇到致命异常，显示蓝屏和停止代码 0x000000f。

[#LC6990]

- 此修复解决了 Provisioning Services 目标设备中的内存泄漏问题。

[#LC7409]

## 会话录制

### 管理

- 您可能会在以下两种情况下收到安装失败错误消息。可以忽略此消息，但要避免收到此消息，请在重新安装 Session Recording 组件前重新启动计算机。[#544579]

- 卸载 Session Recording 组件，然后在未重新启动计算机的情况下重新安装。
- 安装失败并发生回滚，然后尝试在未重新启动计算机的情况下重新安装 Session Recording 组件。

[#LC6979]

## StoreFront

- 尝试启动会话可能会失败并显示以下错误消息：

The ICA file contains an invalid unsigned parameter. (ICA 文件包含无效的未分配参数。)

升级或替换新的 ADMX 文件之前，请将与 ICA 文件签名有关的策略“启用 ICA 文件签名”设置为“未配置”。

注意：修复 #LC5338 适用于 StoreFront 3.0.4000、StoreFront 3.9 及更高版本。

[#LC5338]

- 缓存的域控制器处于脱机状态时，用户无法登录 StoreFront，即使另一个域控制器可用也是如此。

[#LC6358]

- Citrix Receiver for Windows 的图标颜色在修改 StoreFront 主题后不发生变化。

[#LC6435]

- 如果某个 XML Broker 无法正确运行，用户在登录后将看不到应用程序和桌面，即使存在多个正常运行的 XML Broker 时亦如此。此时将显示以下错误消息。

当前没有您可以使用的应用程序或桌面。

[#LC6928]

- 尝试通过在 StoreFront 控制台上选择“传播更改”向服务器组传播更改可能会失败，并显示以下错误消息：“在一台或多台服务器上传播失败。”

[#LC7428]

- 此修复解决了一个与 Firefox 相关的问题。有关详细信息，请参阅知识中心文章 [CTX221551](#)。

[#LC7473]

## 通用打印服务器

### 客户端

- 打印后台处理程序服务可能无响应，从而导致通用打印无法正常工作。等待来自处理程序服务的事务响应时，如果达到超时时间，会出现该问题。

[#LC5209]

## VDA for Desktop OS

### HDX 3D Pro

- 如果 VDA 上使用 HDX 3D Pro 代理，启动新的桌面会话时，可能会缺少两行像素。

[#LC6409]

### 打印

- 打印机重定向可能会间歇性地失败。

[#LC5320]

### 安全问题

- 此修复更新了内部 VDA 组件。

[#LC6904]

### 会话/连接

- 登录没有用户配置文件的 VDA 时，在 Windows 欢迎屏幕显示了一段时间后登录完成前，可能会显示黑屏。  
[#LC2397]
- 尝试通过 Citrix Receiver for Mac 使用网络摄像机在 Cisco WebEx 会议中发送视频时，可能会意外退出 Cisco WebEx 会议。  
[#LC5518]
- 从映射的客户端驱动器读取文件时，如果在客户端会话之外更改了旧的缓存文件长度，则可能会返回该文件长度。此外，对于删除的任何字符，会插入空字符。

要启用此修复，请将以下注册表值设置为“0”：

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\picadm\Parameters

名称：CacheTimeout

类型：REG\_DWORD

值：默认值为 60 秒。如果 CacheTimeout 设置为“0”，则会立即重新加载文件长度，否则会在定义的超时之后进行加载。

[#LC6314]

- 在启用了本地应用程序访问的情况下，使用交互登录免责声明策略可能导致出现黑屏或灰屏并持续 45 秒。  
[#LC6518]
- 对于启用了多点触控功能的 iOS 设备，服务器空闲计时器不重置。  
[#LC6743]

- 虚拟通道数超过 32 时，End User Experience Monitoring 会停止收集指标。

注意：应用此修复后，会删除为虚拟通道设置的限制。

[#LC6768]

- 为交付组配置了“应用程序延迟”的情况下，重新连接会话时，已发布的应用程序有时无法显示。  
[#LC7405]
- 重新连接到已发布的桌面会话并使用多个显示器时，可能不会保留窗口位置。  
[#LC7644]

## 智能卡

- 有时，删除智能卡读卡器可能不会触发用户会话被锁定，即使智能卡删除已配置为锁定用户会话也是如此。  
[#LC7411]

## 系统异常

- VDA 上的 tdica.sys 可能发生致命异常，并显示蓝屏和错误检测代码 0x7E。  
[#LC6553]
- VDA 上的 vd3dk.sys 可能发生致命异常，并显示蓝屏和错误检测代码 0X00000050。

[#LC6833]

- VDA 上的 wdica.sys 会发生致命异常，并显示蓝屏。

[#LC6883]

- VDA 上的 picadm.sys 可能发生致命异常，并显示蓝屏和错误检测代码 0x7F，同时关闭会话。

[#LC7545]

- 服务主机 (svchost.exe) 进程可能会遇到访问冲突并意外退出。scardhook64.dll 模块出错导致出现该问题。

[#LC7580]

## 用户体验

- 此修复在使用高质量音频时改进了对播放一小段时间的声音的支持。

注意：

- 此修复在 Windows Server 2008 R2 上运行的会话中不生效。
- 要使此修复生效，必须使用适用于 Windows 长期服务版本 (LTSR) CU5 或更高版本的 Citrix Receiver 4.4 以及 XenApp 和 XenDesktop 7.6 LTSR CU4 或更高版本的 VDA 版本。

[#LC5842]

- 在 VDA 7.6.300 版本上重定向设备时，USB 设备实例路径的路径名称结尾处可能有额外字符。为了更改此行为，请将产品 ID (PID) 或供应商 ID (VID) 添加到以下注册表项：

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\icausb\Parameters

名称：DeviceInstanceIDOption

类型：REG\_DWORD

值：0 (默认值)、1、2。

- 如果“DeviceInstanceIDOption”配置为“0” (0 为默认值)，则 VID/PID 对配置为“UsingSerialNumberDevices”的设备使用序列号作为实例 ID。其他设备使用“serial\_number+Bus\_number+port\_number”作为实例 ID。
- 如果“DeviceInstanceIDOption”配置为“1”，则 VID/PID 对配置为“UsingSerialNumberDevices”的设备使用“serial\_number+Bus\_number+port\_number”作为实例 ID。其他设备使用序列号作为实例 ID。
- 如果“DeviceInstanceIDOption”配置为“2”，则所有设备都使用序列号作为实例 ID。
- 所有其他值都无效，并被视为“0”。

[#LC6212]

- 在 Web 浏览器中播放视频时，会话可能无响应。

[#LC6259]

- 在多显示器环境中，将外部显示器定义为 Windows 的“主显示”，并在控制面板的显示设置中将其放置在辅助便携式计算机或平板电脑显示器右侧。启动在外部显示器上显示的已发布的应用程序，并将此应用程序移至连接至外部显示器的平板电脑显示器或便携式计算机时，打开或关闭平板电脑或便携式计算机的盖会导致已发布的应用程序变为黑色。

要启用此项修复，必须在 VDA 上设置以下注册表项值：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\Ica\Thinwire

名称 : EnableDrvTw2NotifyMonitorOrigin

类型 : REG\_DWORD

值 : 1 (启用) 和 0 (禁用 ; 0 为默认值)。默认情况下 , 缺少注册表值。

[#LC7760]

## 用户界面

- 存在未保存数据的情况下 , 使用连接中心从无缝会话注销 , 会显示黑色窗口和以下消息 :

“Programs still need to close” (程序仍需关闭) - 包含两个选项 - “Force Logoff” (强制注销) 或“Cancel” (取消) 。  
“Cancel” (取消) 选项不起作用。

安装此修复后 , “Cancel” (取消) 选项可按预期工作。

[#LC6075]

- 使用经过触控优化的桌面时 , URL 快捷方式图标可能显示为空白。

[#LC6663]

## 其他

- 尝试重新连接到断开连接的会话可能会失败。

[#LC6677]

- 在无缝会话中执行时 , 具有“ABM\_GETSTATE”消息的 SHAppBarMessage API 可能无法返回正确值。

[#LC7579]

# VDA for Server OS

## 打印

- 打印机重定向可能会间歇性地失败。

[#LC5320]

## 会话/连接

- 登录没有用户配置文件的 VDA 时 , 在 Windows 欢迎屏幕显示了一段时间后登录完成前 , 可能会显示黑屏。

[#LC2397]

- 尝试通过 Citrix Receiver for Mac 使用网络摄像机在 Cisco WebEx 会议中发送视频时 , 可能会意外退出 Cisco WebEx 会议。

[#LC5518]

- 在登录过程中 , VDA for Server OS 可能在显示“欢迎”屏幕时无响应大约两分钟。通过 Active Directory 组策略对象 (GPO) 配置了最新的交互登录信息时会出现该问题。

[#LC5709]

- 重新连接到会话时，可能会打开另一个已发布的应用程序窗口。

[#LC5786]

- VDA for Server OS 可能无响应。因此，用户会话可能无法注销。

[#LC6117]

- 从映射的客户端驱动器读取文件时，如果在客户端会话之外更改了旧的缓存文件长度，则可能会返回该文件长度。此外，对于删除的任何字符，会插入空字符。

要启用此修复，请将以下注册表值设置为“0”：

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\picadm\Parameters

名称：CacheTimeout

类型：REG\_DWORD

值：默认值为 60 秒。如果 CacheTimeout 设置为“0”，则会立即重新加载文件长度，否则会在定义的超时之后进行加载。

[#LC6314]

- Microsoft Internet Explorer 11 可能无法使用分配给相应会话的虚拟 IP 环回地址。

[#LC6622]

- 对于启用了多点触控功能的 iOS 设备，服务器空闲计时器不重置。

[#LC6743]

- 虚拟通道数超过 32 时，End User Experience Monitoring 会停止收集指标。

注意：应用此修复后，会删除为虚拟通道设置的限制。

[#LC6768]

- Delivery Controller 失去连接时，在 XenApp 服务器上，活动会话可能会被断开连接。VDA 无法跟踪从“预启动”正确变为“活动”状态的会话的状态时会出现该问题。因此，重新启动 Delivery Controller 时，它会尝试从 VDA 中清除资源，且处于预启动的会话会被断开连接或注销，虽然应用程序正在使用中。

[#LC6819]

- 在已发布的桌面上以窗口模式启动会话且该桌面覆盖六个或六个以上显示器时，任务栏或屏幕可能变为灰色。

[#LC6862]

- 将 Google Chrome 设置为默认浏览器后，在应用程序中单击 URL 时，Microsoft Internet Explorer 可能会继续作为默认浏览器。

[#LC6948]

- 在启用了 Electrolysis (e10s) 功能的情况下，64 位版本的 Mozilla Firefox 可能会意外退出。有关详细信息，请参阅知识中心文章 [CTX224067](#)。

[#LC6982]

- 为交付组配置了“应用程序延迟”的情况下，重新连接会话时，已发布的应用程序有时无法显示。

[#LC7405]

## 系统异常

- 某些第三方应用程序可能无法在 RDP 会话中启动。

[#LC4141]

- 托管终端服务的服务主机进程 (svchost.exe) 可能会意外退出。RPM.dll 模块出错导致出现此问题。

[#LC6277]

- VDA 上的 tdica.sys 可能发生致命异常，并显示蓝屏和错误检测代码 0x7E。

[#LC6553]

- VDA 上的 wdica.sys 会发生致命异常，并显示蓝屏。

[#LC6883]

- VDA 上的 picadmsys 可能发生致命异常，并显示蓝屏和错误检测代码 0x7F，同时关闭会话。

[#LC7545]

- 服务主机 (svchost.exe) 进程可能会遇到访问冲突并意外退出。scardhook64.dll 模块出错导致出现该问题。

[#LC7580]

## 用户体验

- 此修复在使用高质量音频时改进了对播放一小段时间的声音的支持。

### 注意：

- 此修复在 Windows Server 2008 R2 上运行的会话中不生效。

- 要使此修复生效，必须使用适用于 Windows 长期服务版本 (LTSR) CU5 或更高版本的 Citrix Receiver 4.4 以及 XenApp 和 XenDesktop 7.6 LTSR CU4 或更高版本的 VDA 版本。

[#LC5842]

- 在 VDA 7.6.300 版本上重定向设备时，USB 设备实例路径的路径名称结尾处可能有额外字符。为了更改此行为，请将产品 ID (PID) 或供应商 ID (VID) 添加到以下注册表项：

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\icausb\Parameters

名称：DeviceInstanceIDOption

类型：REG\_DWORD

值：0（默认值）、1、2。

- 如果“DeviceInstanceIDOption”配置为“0”（0 为默认值），则 VID/PID 对配置为“UsingSerialNumberDevices”的设备使用序列号作为实例 ID。其他设备使用“serial\_number+Bus\_number+port\_number”作为实例 ID。
- 如果“DeviceInstanceIDOption”配置为“1”，则 VID/PID 对配置为“UsingSerialNumberDevices”的设备使用“serial\_number+Bus\_number+port\_number”作为实例 ID。其他设备使用序列号作为实例 ID。

- 如果“DeviceInstanceIDOption”配置为“2”，则所有设备都使用序列号作为实例 ID。
- 所有其他值都无效，并被视为“0”。

[#LC6212]

- 在 Web 浏览器中播放视频时，会话可能无响应。

[#LC6259]

- 在多显示器环境中，将外部显示器定义为 Windows 的“主显示”，并在控制面板的显示设置中将其放置在辅助便携式计算机或平板电脑显示器右侧。启动在外部显示器上显示的已发布的应用程序，并将此应用程序移至连接至外部显示器的平板电脑显示器或便携式计算机时，打开或关闭平板电脑或便携式计算机的盖会导致已发布的应用程序变为黑色。

要启用此项修复，必须在 VDA 上设置以下注册表项值：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\Ica\Thinwire

名称：EnableDrvTw2NotifyMonitorOrigin

类型：REG\_DWORD

值：1 (启用) 和 0 (禁用；0 为默认值)。默认情况下，缺少注册表值。

[#LC7760]

## 用户界面

- 存在未保存数据的情况下，使用连接中心从无缝会话注销，会显示黑色窗口和以下消息：

“Programs still need to close” (程序仍需关闭) - 包含两个选项 - “Force Logoff” (强制注销) 或“Cancel” (取消)。  
“Cancel” (取消) 选项不起作用。

安装此修复后，“Cancel” (取消) 选项可按预期工作。

[#LC6075]

- 使用经过触控优化的桌面时，URL 快捷方式图标可能显示为空白。

[#LC6663]

## 其他

- 在无缝会话中执行时，具有“ABM\_GETSTATE”消息的 SHAppBarMessage API 可能无法返回正确值。

[#LC7579]

# 累积更新 3 (CU3)

Jan 27, 2017

发布日期：2017 年 1 月

累积更新 3 (CU3) 提供原始 7.6 LTSR 的 10 个[基础组件](#)的更新。

自 XenApp 和 XenDesktop 7.6 LTSR CU2 起已修复的问题

此版本中的已知问题

下载

[下载 LTSR CU3 \(XenApp\)](#)

[下载 LTSR CU3 \(XenDesktop\)](#)

## 新建部署

如何从头开始部署 CU3？

可以使用 CU3 metainstaller 在 CU3 的基础上设置一个全新的 XenApp 或 XenDesktop 环境。\* 开始执行该操作之前，我们建议您熟悉以下产品：

请仔细阅读 [XenApp 和 XenDesktop 7.6 长期服务版本](#) 文档，并特别注意[技术概述](#)、[新建部署](#)和[安全](#)部分，然后再开始规划您的部署。请确保您的设置满足所有组件的[系统要求](#)。按照[新建部署](#)中的部署说明进行操作。

\* 注意：Provisioning Services 和 Session Recording 作为单独的下载和安装程序提供。

## 现有部署

如何更新？

CU3 提供 7.6 LTSR 的 10 个[基础组件](#)的更新。请记住：Citrix 建议您将您的部署中的所有 LTSR 组件更新到 CU3。例如：如果 LTSR 部署中包含 Provisioning Services，则将 Provisioning Services 更新到 CU3。如果 Provisioning Services 不属于您的部署的一部分，则不需要安装或更新该组件。

自 7.6 LTSR 版本起，添加了一个 Metainstaller，允许您从单个统一界面中更新 LTSR 环境的现有组件。按照[升级说明](#)中的指示，使用 Metainstaller 更新您的部署中的 LTSR 组件。

### 注意

下面是 CU3 版本特定的信息。有关 [LTSR 基础版本](#)、[CU1](#) 或 [CU2](#) 的此类信息，请参阅各自的文档。

LTSR 基础组件	版本	注意
-----------	----	----

VDA for Desktop OS	7.6.3000	适用于 Windows 10 的特殊规则。请参阅 <a href="#">CU3 兼容的组件和平台</a> 。
VDA for Server OS	7.6.3000	
Delivery Controller	7.6.3000	
Citrix Studio	7.6.3000	
Citrix Director	7.6.3000	
组策略管理体验	2.5.3000	
StoreFront	3.0.3000	
Provisioning Services	7.6.4	适用于 Windows 10 的特殊规则。请参阅 <a href="#">CU3 兼容的组件和平台</a> 。
通用打印服务器	7.6.3000	仅支持 Windows 2008 R2 SP1 Windows 2012 Windows 2012 R2
会话录制	7.6.3000	仅限 Platinum Edition

## LTSR CU3 兼容的组件

建议您在 7.6 LTSR CU3 环境中使用以下组件。这些组件无权享有 LTSR 的优势（扩展的生命周期以及仅用于修复的累积更新）。Citrix 可能会要求您在 7.6 LTSR 环境中升级到这些组件的较新版本。

**Windows 10 注意事项：**可以通过当前版本路径获取对 Windows 10 的常规支持。Windows 10 无法享有 7.6 LTSR 的所有优势。对于包括 Windows 10 计算机的部署，Citrix 建议您使用 [VDA for Desktop OS](#) 和 [Provisioning Services](#) 的当前发布版本 7.9 或更高版本。

有关详细信息，请参阅 [Adding Windows 10 Compatibility to XenApp and XenDesktop 7.6 LTSR](#)（向 XenApp 和 XenDesktop 7.6 LTSR 添加 Windows 10 兼容性）和 [XenApp and XenDesktop Servicing Options \(LTSR\) FAQ](#)（XenApp 和 XenDesktop 服务选项 (LTSR) 常见问题解答）。

LTSR CU3 兼容的组件和平台	版本
Profile Management	5.6
AppDNA	7.12

许可证服务器	11.14.0 Build 18001
HDX RealTime Optimization Pack	2.2
Windows 10	VDA: 7.9 或更高的版本 Provisioning Services : 7.9 或更高版本

## Citrix Receiver 的兼容版本

为简化维护过程以及确保实现最佳性能，Citrix 建议您在最新版本的 Citrix Receiver 可用时随时升级到相应版本。可以从 <https://www.citrix.com/downloads/citrix-receiver.html> 下载最新版本。为方便起见，请考虑订阅 [Citrix Receiver RSS 源](#) 以便在新版本的 Citrix Receiver 可用时接收通知。

请注意，Citrix Receiver 无法享有 XenApp 和 XenDesktop LSTR 的优势（扩展的生命周期和仅用于修复的累积更新）。Citrix 可能会要求您在 7.6 LSTR 环境中升级到 Citrix Receiver 的较新版本。如果使用的是 Citrix Receiver for Windows，Citrix 已公布特殊的 LSTR 计划。可以从 [Citrix Receiver 的生命周期里程碑](#) 页面获取有关该计划的详细信息。

特别需要指出的是，LSTR 支持以下版本的 Citrix Receiver 以及之后的所有版本：

Citrix Receiver 的 LSTR 兼容版本	版本
<a href="#">Citrix Receiver for Windows</a>	4.4 或更高版本
<a href="#">Citrix Receiver for Linux</a>	13.4 或更高版本
<a href="#">Citrix Receiver for Mac</a>	12.4 或更高版本
<a href="#">Citrix Receiver for Chrome</a>	2.2 或更高版本
<a href="#">Citrix Receiver for HTML5</a>	2.2 或更高版本
<a href="#">Citrix Receiver for iOS</a>	7.1.2 或更高版本
<a href="#">Citrix Receiver for Android</a>	3.9.3 或更高版本

## 需注意的 LSTR 排除项目

以下功能、组件和平台无法享有 LSTR 的生命周期里程碑和优势。需要特别指出的是，累积更新和扩展生命周期优势被排除在外。可以通过常规的最新版本获取扩展功能和组件的更新。

### 排除的功能

本地应用程序访问

Framehawk

排除的组件

Linux VDA

Personal vDisk

排除的 Windows 平台\*

Windows 2008 32 位（面向通用打印服务器）

\* Citrix 保留根据第三方供应商的生命周期里程碑更新平台支持的权利。

## 安装和升级分析

当您使用完整产品安装程序部署或升级 XenApp 或 XenDesktop 组件时，将在安装/升级组件的计算机上收集和存储有关安装过程的匿名信息。这些数据用于帮助 Citrix 改善其客户的安装体验。有关详细信息，请参阅 <http://more.citrix.com/XD-INSTALLER>。

## XenApp 6.5 迁移

XenApp 6.5 迁移过程有助于高效快速地从 XenApp 6.5 场过渡到运行 XenApp 7.6（或支持的更高版本）的站点。这在部署中包含大量应用程序和 Citrix 组策略时很有用，可以降低手动将应用程序和 Citrix 组策略移至新 XenApp 站点时意外引入错误的风险。

安装 XenApp 7.6 核心组件并创建站点后，迁移过程按照以下顺序进行：

- 在每个 XenApp 6.5 工作进程上运行 XenApp 7.6 安装程序，将其自动升级到新 Virtual Delivery Agent for Windows Server OS 以便在新站点中使用。
- 在 XenApp 6.5 Controller 上运行 PowerShell 导出 cmdlet，以将应用程序和 Citrix 策略设置导出至 XML 文件。
- 编辑 XML 文件（如果需要），以细化要导入到新站点的内容。通过自定义这些文件，可以将策略和应用程序设置分阶段导入到 XenApp 7.6 站点：即一些现在导入，其他稍后导入。
- 在新 XenApp 7.6 Controller 上运行 PowerShell 导入 cmdlet，以将 XML 文件中的设置导入新 XenApp 站点。
- 根据需要重新配置新站点，然后对其进行测试。

有关详细信息，请参阅[迁移 XenApp 6.x](#)。

# Issues fixed in XenApp and XenDesktop 7.6 LTSR Cumulative Update 3

May 09, 2017

XenApp/XenDesktop 7.6 LTSR 累积更新 3 包含 XenApp 和 XenDesktop 7.6 LTSR、[累积更新 1](#) 和 [累积更新 2](#) 中的所有修复以及以下新修复：

## Citrix Director

- 在 Citrix Director 中执行用户名搜索可能会返回 Citrix Director 中列出但与搜索无关的用户列表。

[#LC5415]

- 使用 Firefox 41 或更高版本时，显示的用户名中将包含一个百分比编码的空格（即 User%20Name）。

[#LC6240]

## Citrix Studio

- 如果用户在启动后 30 秒内登录到物理远程 PC 控制台，“当前用户”在 Citrix Studio 中将变为一个短划线，并且该用户无法连接到远程 PC ICA 会话。

[#LC5408]

- XenDesktop 控制台搜索用户时占用大量 CPU。

[#LC5691]

## Controller

- 尝试创建包含管道符号（“|”）的网络资源时，连接到虚拟机管理程序可能会失败，并显示以下错误消息：

无法连接到服务器

[#LC4933]

- 如果向 Machine Creation Services 虚拟机复制时存储库发生任何故障，尽管复制失败，复制仍显示为成功。

[#LC5430]

- Machine Creation Services 在设置过程中无法识别“Allow migration to a Virtual Machine Host with a different processor version”（允许迁移到配备了其他处理器版本的虚拟机主机）设置。

[#LC5885]

- 重新启动 DDC 后，VDA 可能会卡在正在初始化状态。

[#LC6264]

- 监视数据清理总是在 0:00 UTC 开始。应用此修复后，监视数据清理将于本地时间 0:00 开始。

[#LC6275]

- 当大量匿名用户尝试同时启动应用程序/VDA 时，Broker Service 将断开与数据库服务器的连接。

[#LC6320]

- 为已发布的应用程序设置工作目录时，该设置可能不会反映在“连接租用”模式下启动的已发布应用程序中。

[#LC6397]

- 负载很高时，SQL 数据库连接可能会在 Controller 上超时。在 SQL Server 上观察到极端阻止，并且站点可能会变得无法访问。

[#LC6616]

## Provisioning Services

### 控制台

- 通过虚拟机从使用 SCVMM 群集的模板预配虚拟机时，单击“完成”后向导无法创建虚拟机。

[#LC5871]

- XenDesktop 设置向导可能不执行完全权限检查，导致出现权限错误。

[#LC6190]

### 服务器

- PVS 服务器有时在“复制状态”窗口中显示状态“Server Unreachable”（无法访问服务器）。

[#LC5683]

- 通过虚拟机从使用 SCVMM 群集的模板预配虚拟机时，单击“完成”后向导无法创建虚拟机。

[#LC5871]

- 当目标设备的 boot.iso 代码收到随广播目标发送的 ARP 请求时，目标设备的 boot.iso 代码会发送无效的 ARP 答复。

[#LC6099]

- XenDesktop 设置向导可能不执行完全权限检查，导致出现权限错误。

[#LC6190]

- 使用过程中，Soapserver 占用的 RAM 可能会超过 13 GB。

[#LC6199]

## 目标设备

- 此修复解决了一个安全漏洞。有关详细信息，请参阅知识中心文章 [CTX219580](#)。

[#LC6200、#LC6201、#LC6202、#LC6203、#LC6204]

- 与 PVS 服务器的连接断开时，事件 ID 为 85 的 bnistack 错误 “[MIoWorkerThread] I/O Stream Socket UNAVAILABLE - not counting retry” ([MIoWorkerThread] I/O 流套接字不可用 - 请勿重试) 将在事件查看器中以红色显示。

[#LC6449]

## Session Recording (Player)

- 尝试使用版本高于 Session Recording 的版本的 Citrix Receiver 播放录制件时，将显示一条消息，指出无法播放该文件。应用此修复后，即使是通过较新版本的 Citrix Receiver 录制的文件也能播放。

[#LC6503]

## StoreFront

- StoreFront 无法识别正确的客户端 IP 地址，即使代理服务器在请求中发送“x-forwarded-for”头亦如此。

[#LC5797]

- 使用 Microsoft 浏览器时，在浏览器中输入搜索词时可能会出现延迟。

[#LC6324]

- 安装 StoreFront 3.0.1000 或 3.0.2000 后，管理控制台无法启动并显示以下错误消息：The Management console is unavailable because of a root certificate missing, go to verisign and download the certificate - Verisign class primary CA - G5. (由于缺少根证书，管理控制台不可用，请转至 Verisign 并下载证书 - Verisign 类主 CA - G5。) 有关详细信息，请参阅知识中心文章 [CTX218815](#)。

[#LC6471]

- 将 StoreFront 从版本 2.5 升级到版本 3.0.2000 失败，错误为 1603。有关详细信息，请参阅知识中心文章 [CTX220411](#)。

[#LC6816]

## 通用打印服务器

- 使用 Citrix 通用打印驱动程序时，尝试从 Microsoft Internet Explorer 打印可能会失败，并提示以下错误消息：

"There was an internal error and Internet Explorer is unable to print this document" (存在内部错误，Internet Explorer 无法打印此文档)。

[#LC4472]

# VDA for Desktop OS

## 打印

- Citrix Printer Manager Service (Cpsvc.exe) 可能异常退出并显示访问冲突错误。

[#LC4665]

- XenApp 会话打印机可能未正确映射。例如，使用相同的名称在打印服务器上创建两个打印机，并在其中任一打印机名称后面额外添加一个字符。如果您创建了一条针对这两个打印机的会话打印机策略并登录到 VDA，可能仅映射一个打印机。

[#LC6385]

## 无缝窗口

- 如果启用了 Excelhook，则在最小化后还原 Excel 工作簿时，可能导致 Excel 窗口丢失焦点。

[#LC6637]

## 服务器/站点管理

- 指向 32 位系统的 VDA for Desktop OS 上的 \Device\MUP 的链接可能会丢失。因此，充当微型驱动程序的防病毒软件可能无法扫描映射的驱动器上的文件。

[#LC6041]

## 会话/连接

- 如果具有只写权限的用户打开某个映射的客户端驱动器上的文件，则在尝试向该文件附加数据时可能会失败。在第二次运行 PowerShell 命令“get-process | out-file -filepath “\\client\c\$\temp\proclist.txt” -Append”时会发生此问题。

[#LC3895]

- 如果另一个进程与 picadm.sys 占用相同的锁，用户无法从会话注销，会话保持在断开连接状态。

[#LC4415]

- 在远程 PC 上将用户会话切换到控制台会话时，某些连接属性可能不会更新。

[#LC5139]

- 应用程序尝试枚举文件时，客户端驱动器映射返回损坏的文件路径信息。

[#LC5163]

- 通过 Cisco WAAS Gateway 连接的会话尝试传输较大文件时，由于 VDA 端发生缓冲区溢出，VDA 可能会意外退出。

[#LC5371]

- 如果客户端 USB 设备重定向规则策略包含的字符数超过 1000，所有 USB 驱动器都会重定向，即使存在设备的拒绝规则也是

如此。

[#LC5457]

- 存在被覆盖的开放句柄时，尝试打开文件可能会失败。因此，该文件将被进程锁定。

[#LC5657]

- 在多个已发布的无缝应用程序中在全屏模式与窗口模式之间切换时，如果其中任一应用程序处于无响应状态，这些应用程序可能会无响应。

[#LC5774]

- 如果在用户会话中对远程计算机关闭电源或强制重新启动，可能会在重启完成时禁用所有音频驱动程序。

[#LC6009]

- Citrix 策略“客户端自动重新连接”设置为“禁止”时，尝试启动 VM 托管应用程序可能会失败。

[#LC6103]

- 在升级到 XenApp 和 XenDesktop 7.6 长期服务版本后，可能无法使用复制和粘贴功能。

[#LC6114]

- 当您尝试使用 Citrix Receiver for HTML5 下载文件时，下载窗口可能不会正确聚焦。因此，无法选择要下载的文件。解决方法：将主应用程序窗口最小化，以查看来自 Citrix Receiver for HTML5 的下载窗口。

[#LC6167]

- 此增强功能使 Citrix Device Redirector Service 能够写入与 USB 规则和活动有关的事件日志。

[#LC6243]

- 如果在用户会话中对远程计算机关闭电源或强制重新启动，可能会在重启完成时禁用所有音频驱动程序。

[#LC6322]

## 智能卡

- 在 Citrix Receiver for iOS 用于启动到远程 PC 的桌面会话的配置中，当您使用显式用户名和密码登录到 StoreFront，然后尝试在本地使用智能卡登录到物理远程 PC 时，登录尝试可能会失败，具体表现为以下两种方式之一：

- Microsoft Windows 确认存在智能卡登录选项，但是，即使正确插入了智能卡，“插入智能卡”选项仍不消失。
- Microsoft Windows 不列出智能卡登录选项，即使连接了智能卡读卡器并正确插入了智能卡亦如此。

[#LC5997]

## 系统异常

- XenApp 服务器可能会遇到致命异常，显示一个带有停止检查代码 0x0000000A 的蓝色屏幕。

[#LC5917]

- VDA 上的 wdica.sys 会发生致命异常，并显示蓝屏。

[#LC5938]

- Citrix Audio Service (CtxAudioService.exe) 可能会意外退出。

[#LC6323]

## 用户体验

- 尝试使用 OneNote 录制视频时，网络摄像机重定向失败，从而导致录制失败。

[#LC5205]

## 用户界面

- 如果您在用户会话中从 IME 语言栏中删除 Microsoft 拼音服务器输入法编辑器 (IME)，然后注销，拼音 IME 仍在服务器 IME 语言栏中显示。

[#LC6517]

# VDA for Server OS

## 打印

- Citrix Printer Manager Service (Cpsvc.exe) 可能异常退出并显示访问冲突错误。

[#LC4665]

- XenApp 会话打印机可能未正确映射。例如，使用相同的名称在打印服务器上创建两个打印机，并在其中任一打印机名称后面额外添加一个字符。如果您创建了一条针对这两个打印机的会话打印机策略并登录到 VDA，可能仅映射一个打印机。

[#LC6385]

## 无缝窗口

- 如果启用了 Excelhook，则在最小化后还原 Excel 工作簿时，可能导致 Excel 窗口丢失焦点。

[#LC6637]

## 会话/连接

- 此修复解决了从发布的桌面中处理命令行参数不正确的问题，如以下示例中所示：

如果运行 "C:\Program Files (x86)\Citrix\system32\iexplore.exe" -noframemerging http://www.google.com，则 Internet Explorer 错误解释参数，并将 URL 解析为 http://-noframemerging%20http://www.google.com。

[#LC3660]

- 如果具有只写权限的用户打开某个映射的客户端驱动器上的文件，则在尝试向该文件附加数据时可能会失败。在第二次运行 PowerShell 命令“get-process | out-file -filepath "\\\client\c\$\temp\proclist.txt" -Append”时会发生此问题。

[#LC3895]

- 在 XenApp 7.6.300 中，对多林环境中的应用程序具有有限可见性的用户可能无法启动应用程序。

[#LC4374]

- 如果另一个进程与 picadmsys 占用相同的锁，用户无法从会话注销，会话保持在断开连接状态。

[#LC4415]

- 应用程序尝试枚举文件时，客户端驱动器映射返回损坏的文件路径信息。

[#LC5163]

- 尝试重新连接到会话可能会间歇性失败，并导致 VDA for Server OS 进入“正在初始化”状态。

[#LC5250]

- 在注册表中禁用了组策略计算时，COM 端口映射在重新连接过程中会间歇性失败。

[#LC5274]

- 通过 Cisco WAAS Gateway 连接的会话尝试传输较大文件时，由于 VDA 端发生缓冲区溢出，VDA 可能会意外退出。

[#LC5371]

- 如果客户端 USB 设备重定向规则策略包含的字符数超过 1000，所有 USB 驱动器都会重定向，即使存在设备的拒绝规则也是如此。

[#LC5457]

- VDA for Server OS 可能会显示 VDA 状态为“正在初始化”，而非“已注册”。在此期间，不会为该 VDA 代理任何新会话。

[#LC5621]

- 存在被覆盖的开放句柄时，尝试打开文件可能会失败。因此，该文件将被进程锁定。

[#LC5657]

- 在多个已发布的无缝应用程序中在全屏模式与窗口模式之间切换时，如果其中任一应用程序处于无响应状态，这些应用程序可能会无响应。

[#LC5774]

- 升级到 Hotfix Rollup Pack 7 后，复制并粘贴功能可能不起作用。

[#LC6114]

- 当您尝试使用 Citrix Receiver for HTML5 下载文件时，下载窗口可能不会正确聚焦。因此，无法选择要下载的文件。解决方法：将主应用程序窗口最小化，以查看来自 Citrix Receiver for HTML5 的下载窗口。

[#LC6167]

- 此增强功能使 Citrix Device Redirector Service 能够写入与 USB 规则和活动有关的事件日志。

[#LC6243]

- 启动 XenApp 7.6 长期服务版本累积更新 2 VDA for Server OS 或早期版本时，以下警告消息可能会在系统事件日志中显示：

尝试连接 SemsService 失败，错误代码为 0x2。

[#LC6311]

- 升级到 XenApp 7.6 长期服务版本累积更新 1 或累积更新 2 之后，App-V 应用程序的 /appwe 开关可能会不起作用。

[#LC6398]

## 系统异常

- 访问无效地址位置时，在终端服务中注册的服务主机 (svchost.exe) 进程可能会在 RPM.dll 上意外退出。

[#LC5696]

- XenApp 服务器可能会遇到致命异常，显示一个带有停止检查代码 0x0000000A 的蓝色屏幕。

[#LC5917]

- VDA 上的 wdica.sys 会发生致命异常，并显示蓝屏。

[#LC5938]

- 在终端服务中注册的服务主机 (svchost.exe) 进程可能会在 RPM.dll 上意外退出。

[#LC6461]

## 用户体验

- 尝试使用 OneNote 录制视频时，网络摄像机重定向失败，从而导致录制失败。

[#LC5205]

## 用户界面

- 如果您在用户会话中从 IME 语言栏中删除 Microsoft 拼音服务器输入法编辑器 (IME)，然后注销，拼音 IME 仍在服务器 IME 语言栏中显示。

[#LC6517]

# 虚拟桌面组件 - 其他

- 预配的计算机可能会丢失其 AD 信任关系，并且 VDA 无法注册。使用与创建目录时所使用的主映像或虚拟机不同的主映像或虚拟机更新通过 Machine Creation Services 创建的 Microsoft Windows 8 (及更高版本) 计算机目录后会出现此问题。

[#LC3874]

- Machine Creation Services (MCS) 创建的计算机没有计算机帐户密码 GPO，从而导致 MCS 计算机上的密码未重置。

[#LC4440]

- Director 中的 Activity Manager 可能无法显示为部分用户运行的某些应用程序。

[#LC6235]

# 累积更新 2 (CU2)

Jan 25, 2017

发布日期：2016 年 9 月 30 日

累积更新 2 (CU2) 提供原始 7.6 LTSR 的 10 个[基础组件](#)的更新。

自 XenApp 和 XenDesktop 7.6 LTSR CU1 起已修复的问题

此版本中的已知问题

下载

[下载 LTSR CU2 \(XenApp\)](#)

[下载 LTSR CU2 \(XenDesktop\)](#)

新建部署

如何从头开始部署 CU2？

可以使用 CU2 metainstaller 在 CU2 的基础上设置一个全新的 XenApp 或 XenDesktop 环境。\* 开始执行该操作之前，我们建议您熟悉以下产品：

请仔细阅读 [XenApp 和 XenDesktop 7.6 长期服务版本](#)文档，并特别注意[技术概述](#)、[新建部署](#)和[安全](#)部分，然后再开始规划您的部署。请确保您的设置满足所有组件的[系统要求](#)。按照[新建部署](#)中的部署说明进行操作。

\* 注意：Provisioning Services 和 Session Recording 作为单独的下载和安装程序提供。

现有部署

如何更新？

CU2 提供 7.6 LTSR 的 10 个[基础组件](#)的更新。请记住：Citrix 建议您将您的部署中的所有 LTSR 组件更新到 CU2。例如：如果 LTSR 部署中包含 Provisioning Services，则将 Provisioning Services 组件更新到 CU2。如果 Provisioning Services 不属于您的部署的一部分，则不需要安装或更新该组件。

自 7.6 LTSR 版本起，添加了一个 Metainstaller，允许您从单个统一界面中更新 LTSR 环境的现有组件。按照[升级说明](#)中的指示，使用 Metainstaller 更新您的部署中的 LTSR 组件。

## 注意

下面是 CU2 版本特定的信息。有关[LTSR 基础版本](#)或[CU1](#) 的此类信息，请参阅各自的文档。

LTSR 基础组件	版本	注意
VDA for Desktop OS	7.6.2000	适用于 Windows 10 的特殊规则。请参阅 <a href="#">CU2 兼容的组件和平台</a> 。

VDA for Server OS	7.6.2000	
Delivery Controller	7.6.2000	
Citrix Studio	7.6.2000	
Citrix Director	7.6.2000	
组策略管理体验	2.5.2000	
StoreFront	3.0.2000	
Provisioning Services	7.6.3	适用于 Windows 10 的特殊规则。请参阅 <a href="#">CU2 兼容的组件和平台</a> 。
通用打印服务器	7.6.2000	仅支持 Windows 2008 R2 SP1 Windows 2012 Windows 2012 R2
会话录制	7.6.1000	仅限 Platinum Edition

## CU2 兼容的组件

建议您在 7.6 LTSR CU2 环境中使用以下组件。这些组件无权享有 LTSR 的优势（扩展的生命周期以及仅用于修复的累积更新）。Citrix 可能会要求您在 7.6 LTSR 环境中升级到这些组件的较新版本。

**Windows 10 注意事项：**可以通过当前版本路径获取对 Windows 10 的常规支持。Windows 10 无法享有 7.6 LTSR 的所有优势。对于包括 Windows 10 计算机的部署，Citrix 建议您使用 [VDA for Desktop OS](#) 和 [Provisioning Services](#) 的当前发布版本 7.9 或更高版本。

有关详细信息，请参阅 [Adding Windows 10 Compatibility to XenApp and XenDesktop 7.6 LTSR](#)（向 XenApp 和 XenDesktop 7.6 LTSR 添加 Windows 10 兼容性）和 [XenApp and XenDesktop Servicing Options \(LTSR\) FAQ](#)（XenApp 和 XenDesktop 服务选项 (LTSR) 常见问题解答）。

LTSR CU2 兼容的组件和平台	版本
Profile Management	5.5
AppDNA	7.6.5
许可证服务器	11.14.0 Build 17005

HDX RealTime Optimization Pack	2.1.1
Windows 10	VDA: 7.9 或更高的版本 Provisioning Services : 7.9 或更高版本

## Citrix Receiver 的兼容版本

为简化维护过程以及确保实现最佳性能，Citrix 建议您在最新版本的 Citrix Receiver 可用时随时升级到相应版本。可以从 <https://www.citrix.com/downloads/citrix-receiver.html> 下载最新版本。为方便起见，请考虑订阅 [Citrix Receiver RSS 源](#) 以便在新版本的 Citrix Receiver 可用时接收通知。

请注意，Citrix Receiver 无法享有 XenApp 和 XenDesktop LTSR 的优势（扩展的生命周期和仅用于修复的累积更新）。Citrix 可能会要求您在 7.6 LTSR 环境中升级到 Citrix Receiver 的较新版本。如果使用的是 Citrix Receiver for Windows，Citrix 已公布特殊的 LTSR 计划。可以从 [Citrix Receiver 的生命周期里程碑](#) 页面获取有关该计划的详细信息。

特别需要指出的是，LTSR 支持以下版本的 Citrix Receiver 以及之后的所有版本：

Citrix Receiver 的 LTSR 兼容版本	版本
<a href="#">Citrix Receiver for Windows</a>	4.4 或更高版本
<a href="#">Citrix Receiver for Linux</a>	13.4 或更高版本
<a href="#">Citrix Receiver for Mac</a>	12.3 或更高版本
<a href="#">Citrix Receiver for Chrome</a>	2.1 或更高版本
<a href="#">Citrix Receiver for HTML5</a>	2.1 或更高版本
<a href="#">Citrix Receiver for iOS</a>	7.1.1 或更高版本
<a href="#">Citrix Receiver for Android</a>	3.9 或更高版本

## 需注意的 LTSR 排除项目

以下功能、组件和平台无法享有 LTSR 的生命周期里程碑和优势。需要特别指出的是，累积更新和扩展生命周期优势被排除在外。可以通过常规的最新版本获取扩展功能和组件的更新。

排除的功能
本地应用程序访问

排除的组件

Linux VDA

Personal vDisk

排除的 Windows 平台\*

Windows 2008 32 位（面向通用打印服务器）

\* Citrix 保留根据第三方供应商的生命周期里程碑更新平台支持的权利。

### XenApp 6.5 迁移

XenApp 6.5 迁移过程有助于高效快速地从 XenApp 6.5 场过渡到运行 XenApp 7.6（或支持的更高版本）的站点。这在部署中包含大量应用程序和 Citrix 组策略时很有用，可以降低手动将应用程序和 Citrix 组策略移至新 XenApp 站点时意外引入错误的风险。

安装 XenApp 7.6 核心组件并创建站点后，迁移过程按照以下顺序进行：

- 在每个 XenApp 6.5 工作进程上运行 XenApp 7.6 安装程序，将其自动升级到新 Virtual Delivery Agent for Windows Server OS 以便在新站点中使用。
- 在 XenApp 6.5 Controller 上运行 PowerShell 导出 cmdlet，以将应用程序和 Citrix 策略设置导出至 XML 文件。
- 编辑 XML 文件（如果需要），以细化要导入到新站点的内容。通过自定义这些文件，可以将策略和应用程序设置分阶段导入到 XenApp 7.6 站点：即一些现在导入，其他稍后导入。
- 在新 XenApp 7.6 Controller 上运行 PowerShell 导入 cmdlet，以将 XML 文件中的设置导入新 XenApp 站点。
- 根据需要重新配置新站点，然后对其进行测试。

有关详细信息，请参阅[迁移 XenApp 6.x](#)。

### 支持 Citrix Connector 7.5

Citrix Connector 7.5 在 Microsoft System Center Configuration Manager 与 XenApp 或 XenDesktop 之间搭建了一条桥梁，使您可以将 Configuration Manager 的用途扩展到 Citrix 环境。对 Citrix Connector 7.5 的支持现在包括 XenApp 7.6 和 XenDesktop 7.6 Platinum Edition。

有关信息，请参阅[Citrix Connector 7.5 for System Center Configuration Manager 2012](#)。

# XenApp 和 XenDesktop 7.6 LTSR Cumulative Update 2 中已修复的问题

May 10, 2017

XenApp/XenDesktop 7.6 LTSR 累积更新 2 包含 XenApp 和 XenDesktop 7.6 LTSR 及[累积更新 1](#) 中的所有修复以及以下新修复：

## Citrix Director

- 在 Citrix Director 的 HDX 面板中查看用户会话时，可能会错误显示有关音频虚拟通道的优先级警告。

[#LC5564]

## Citrix 策略

- w3wp.exe 进程会占用 100% 的 CPU。  
[#LC4355]
- Citrix Studio 可能允许只读管理员进行策略过滤器编辑。  
[#LC4801]
- 会在下一次刷新 GPO 或运行 GPUUpdate /Force 时从计算机中删除存储在 Active Directory 中的 Citrix 组策略。VDA 7.6.300 及更高版本中会出现此问题。  
[#LC5204]
- 打开 Citrix Studio 并选择策略节点时显示以下错误消息：

"Changes made to policies outside of this console, such as in PowerShell or management tools from previous versions, resulted in a discrepancy between policies. The assigned objects of policy must match. Object Delivery Group has assignments in the "user" component and in the "computer" component." (在此控制台外所做的策略更改，如在 PowerShell 或先前版本的管理工具中的更改，会导致策略之间出现不一致。<策略名称> 策略的已分配对象必须匹配。对象交付组的“用户”组件中有分配 <分配名称>，“计算机”组件中有分配 <分配名称>。)

[#LC5510]

## Citrix Studio

- 尝试检索大量数据时，尽管是在日志记录节点中，Citrix Studio 并不接收日志记录条目。  
[#LC5292]
- 在 FlexCast Management Architecture 服务已停止或不可用时 Citrix Studio 可能会显示一条有关站点升级的错误消息或提示。  
[#LC5319]

## Controller

- 短时间内启动大量会话时，Director 可能需要很长时间才能显示会话信息。  
[#LC1617]
- 使用 VMware ESXi 5.x 或 6.0 创建 MCS 计算机时，计算机部署会偶尔合并和克隆为密集预配磁盘。  
[#LC4655]
- 当 VDA 处于维护模式下时，Get-BrokerSession cmdlet 可能返回交付组的维护模式状态，而不是单个计算机。  
[#LC4840]
- Citrix Studio 启动时有时会显示以下错误消息：“Could not connect to broker service.” (无法连接到 Broker Service。)  
[#LC4854]
- 该修复程序解决了一个问题，该问题会导致 Machine Creation Services 预配功能无法在 Amazon Web Services 中工作（当控制器通过 Web 代理方式与 Amazon 的公共 API 端点相独立时）。  
[#LC5109]
- 在 FlexCast Management Architecture 服务已停止或不可用时 Citrix Studio 可能会显示一条有关站点升级的错误消息或提示。  
[#LC5319]

## HDX MediaStream Flash 重定向

- 在启用了 HDX MediaStream Flash 重定向的情况下，Microsoft Internet Explorer 在运行 pseudoserverinproc2.dll 时可能会意外关闭。

要启用此修复，请创建以下注册表项：

- 在 Windows 32 位系统上：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer

- 名称 : AllowCOMObjectTrack  
 类型 : DWORD  
 值 : 0
- 在 Windows 64 位系统上 :
 

HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer  
 名称 : AllowCOMObjectTrack  
 类型 : DWORD  
 值 : 0  
 [#LC1885]
  - 在启用 HDX MediaStream Windows Media 重定向的情况下，某些第三方播放器可能会在运行于 Windows 10 上的 VDA 中显示文件时意外退出。  
 [#LC5110]

## 许可

- 在选择“使用现有许可证”时，可能无法继续进行 Citrix Studio 中的站点设置。解决方法：在许可证服务器上重新启动 Citrix Web Services for Licensing 服务来完成其配置。  
 [#630814]

## Provisioning Services

控制台

目标设备

服务器

### 控制台

- 在扩展站点时，PVS 控制台偶尔会超时。  
 [#LC4737]

- 创建目标时，XenDesktop 设置向导不使用模板启动属性。要启用此修复，请创建以下注册表项：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ProvisioningServices  
 名称 : UseTemplateBootOrder  
 类型 : REG\_DWORD  
 数据 : 1

[#LC5237]

### 服务器

- 在丢失数据库连接并恢复后，Provisioning Services 控制台上显示的目标设备数可能低于实际值。  
 [#LC4275]

- Boot Device Manager 目标设备无法获取 IP 地址，而 PXE 目标设备可以成功获取 IP 地址。发生这种情况是因为 Boot Device Manager 发送的 DHCP 发现请求将“Seconds Elapsed”（已用秒数）值设置为 0。然后该请求会由 IP Helper 丢弃。“Seconds Elapsed”（已用秒数）值现在设置为 4 可避免此问题。  
 [#LC4369]

- 如果将 MTU 大小值更改为小于 1500 字节，则引导程序文件无法下载，并且目标设备无法使用 Boot Device Manager (BDM) 进行启动。借助此增强功能，可通过设置以下注册表项来将 MTU 大小值设置为小于 1500 字节。默认情况下已禁用此增强功能：

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\PVSTSB\Parameters  
 名称 : AllowMTUAdjust  
 类型 : DWORD  
 值 : 1

[#LC4531]

- 在扩展站点时，PVS 控制台偶尔会超时。  
 [#LC4737]

- 当尝试导入 VHDX 文件的新虚拟磁盘版本时，导入操作会失败，并出现一条错误消息，指出清单文件无效。  
 [#LC4985]

- Provisioning Server 日志中可能会显示目标设备的错误 IP 地址。  
 [#LC5323]

- 在 Provisioning Server 的事件查看器中可能会显示以下数据库访问错误：

“DBAccess error:<-31749>.” (DBAccess 错误:<无法添加记录 -- 字段与现有记录相同><-31749>。)

多个 Provisioning Server 同步调用特定的存储过程，从而导致对存储过程的调用之间发生冲突，这时会发生该问题。因此，可能会发生两次尝试插入具有相同键值的记录。

[#LC5364]

- 尝试重新启动预配的目标可能会由于数据库超时错误而间歇性地失败。此时可能会显示以下错误消息：“Timeout expired. The timeout period elapsed prior to completion of the operation or the server is not responding.”（超时已过期。在完成操作或服务器未响应之前，已过超时期限。）  
[#LC5511]
- 支持目标设备从网络启动的 BNPXE 服务器绑定到 IP 地址 127.0.0.1。这会阻止目标设备启动。BNPXE 枚举网络接口，但操作系统并未发现所有接口且仅返回 127.0.0.1，这时可能会发生此问题。  
[#LC5916]
- 使用 HP Moonshot 系统时，尝试启动目标设备可能会失败。  
[#LC6024]

## 目标设备

- 创建个人虚拟磁盘时，启动计算机后，显示“Personal vDisk cannot start”（个人虚拟磁盘无法启动）错误对话框，已格式化的磁盘由于“unknown format”（未知格式）错误导致无法使用。  
[#LC5935]

## StoreFront

- 使用 Windows Server 2008 R2 时，如果尝试在“Stores”（应用商店）菜单中选择“Set Unified Experience as Default”（将统一体验设置为默认值），Citrix StoreFront MMC 可能会意外退出。  
[#LC3614]
- 此修复解决了从远程组向本地同步以及往回同步更改的订阅项的相关问题。  
[#LC4690]
- 将 Citrix Receiver for Web 的“Session Timeout”（会话超时）设置为 24 天以上时，会导致登录后立即显示会话超时警告。  
[#LC4787]
- 如果应用商店使用资源聚合，桌面设备站点将不启动所分配的桌面。  
[#LC4838]
- 在 StoreFront 3.0.1 中，工作区控制功能在使用聚合时可能不起作用。  
[#LC5042]
- 使用 PowerShell 脚本命令时，有时不应用 AllFailedBypassDuration 设置。  
[#LC5500]
- 如果通过“Set-BrokerAccessPolicyRule”命令启用了“IncludedClientIPFilter”或“ExcludedClientIPFilter”选项，您可能无法在 StoreFront 上查看资源（例如，共享资源、已发布的桌面或已发布的应用程序）。  
[#LC6058]

## 通用打印服务器

**客户端** **服务器**

### 客户端

- 尝试打印到通用打印服务器时，NextGen 应用程序偶尔会失败。  
[#LC4246]

### 服务器

- Citrix XTE Server 服务 (XTE.exe) 可能会异常退出。  
[#LC0759]

## VDA for Desktop OS

Desktop Studio	会话/连接
HDX 3D Pro	智能卡
HDX MediaStream Windows Media 重定向	系统异常
安装、卸载、升级	用户体验
键盘	用户界面
打印	

[打印](#)

[打印](#)

#### Desktop Studio

- 已注销的 RDP 会话在 Citrix Studio 中可能显示为“已断开连接”，且无法用于重新连接。

[#LC5427]

#### HDX 3D Pro

- 最大化窗口时，上下文菜单可能不会正确显示在桌面上。

[#LC5263]

#### HDX MediaStream Windows Media 重定向

- 在启用 HDX MediaStream Windows Media 重定向的情况下，某些第三方播放器可能会在运行于 Windows 10 上的 VDA 中显示文件时意外退出。

[#LC5110]

#### 安装、卸载、升级

- 尝试从具有不同分辨率的端点重新连接到会话时会导致 VDA 意外退出，且可能导致出现黑窗或白窗。

[#LC4606]

#### 键盘

- 从 5.4.400 版升级到 7.6.300 版时，ICA Service\System32 目录会丢失，且键盘/鼠标输入无法在 Mac 客户端上注册。

[#LC4681]

#### 打印

- 未设置默认打印机时，会话中所有映射的打印机可能会失败。

[#LC4354]

- 在启用旧版打印机名称的情况下，当在一台服务器上为同一用户建立多个会话时，已发布的应用程序可能无法用于自动创建的打印机。

[#LC4517]

- “自动创建客户端打印机”策略可能无法在已发布的应用程序中正确设置默认打印机，且 Microsoft XPS 文档编写器被设置为默认打印机。

[#LC4696]

- SAP 生成的 Excel 电子表格无法在使用通用打印驱动程序 EMF 驱动程序重定向的打印机上打印。

[#LC4853]

- 用户注销并重新登录后，连接到会话的打印机可能无法访问。

[#LC5188]

- Citrix 通用打印驱动程序中的客户端选项上的打印预览会显示给本地端点。

[#LC5404]

#### 会话/连接

- 在同时应用不允许会话墙纸的 Citrix 策略和指定了墙纸的 Microsoft 组策略的情况下，调整重新连接的会话时，不应用 Citrix 策略。

[#LC0115]

- VDA 进入屏幕保护或节能模式后，屏幕上的信息仍可见，直到用户提供将会话更新为黑色屏幕的输入（鼠标或键盘）。通过 DWORD 值 HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\Graphics\SetDisplayRequiredMode = 0 在会话中启用屏幕保护或节能选项时会出现此问题。

[#LC1650]

- 在安装了修补程序 ICAWS760WX86022 的系统中，在重新启动 Citrix ICA 服务时，尝试重新连接到用户会话可能会失败。

[#LC3714]

- 具有此增强功能时，在会话中重定向 USB 设备时，会有一个条目写入 Windows 事件日志。

[#LC3996]

- 登录到使用 UPN 凭据为单点登录而配置的 Web 界面时，会话窗口可能会短暂显示，然后意外退出。

[#LC4035]

- 在使用已发布的 Microsoft Internet Explorer 实例的情况下，从 Web 站点下载文件并将其保存到一个映射的客户端驱动器（“另存为...”）的尝试可能会失败。

[#LC4300]

- 通过 Citrix Receiver for Mac 或 Chromebook 连接时，音频文件可能无法在 VDA 会话中播放。

[#LC4596]

- 当 VDA 和 Citrix Receiver 之间的网络中断后，您无法在 Windows Media Player 上播放 .avi 文件。

[#LC4670]

- 在启用了传统图形模式的情况下，在窗口化的模式和全屏模式间切换会话时，运行在 VDA 上的应用程序窗口可能无法维持最大化状态。

[#LC4693]

- 从 5.6.300 版升级 VDA 后，VDA 可能会变为不响应。

[#LC4851]

- 在运行于 iOS 设备上的用户会话中，时区重定向可能无法工作。

[#LC4869]

- 使用远程桌面协议后，ICA 会话可能在重新连接到 VM 时显示灰屏。此问题仅发生在使用 /NOCITRIXWDDM 安装的 VDA 上。

[#LC4970]

- USB 设备在重定向到 7.6.300 版的 VDA 后可能无法工作。设备的实例 ID 与序列号不同时，会发生该问题。

为了能够完成此修复，请将产品 ID 或供应商 ID 对添加到以下注册表项：

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\icausb\Parameters

名称：UsingSerialNumberDevices

类型：REG\_MULTI\_SZ

值：  
注意：请在备注字符串旁边，添加 vid=xxxx 和 pid=xxxx 对。（值的语法是不区分大小写规则的排序列表，其中“#”是行注释，每个规则都是一个排序的 vid 和 pid 对。例如，vid=#-number 和 pid=#-number。vid/pid 的最大十六进制值是 FFFF。如果 vid/pid 十六进制值小于 4，则用零 (0) 配对数字。例如，如果 vid 是 12，pid 是 13，则 vid/pid 对应该是 vid=0012, pid=0013。每个规则都有固定长度：17，规则的开头或结尾没有空格。示例：#vid=FFFF,#pid=FFFF #vid=0012,#pid=0013。）>

[#LC5035]

- svchost.exe 进程会占用 100% 的 CPU。

[#LC5041]

- 如果启用了 Excelhook，在应用了修补程序 ICATS760WX64028 后，单击任务栏上的 Excel 图标时，Excel 窗口不会最小化。

[#LC5060]

- 当用户正在登录或注销同时激活了证书传播的情况下，svchost.exe 进程可能会在 SCardHook64.dll 处出现间歇性失败。

[#LC5083]

- 此修复程序解决了一个问题，该问题会导致针对基于 DirectShow 的应用程序的客户端提取操作失败，使得无法显示视频。

[#LC5098]

- 操作系统中的 picadd.sys 出现错误，并显示蓝屏和错误检测代码 0xd5。

[#LC5134]

- 作为映射的客户端驱动器映射到会话中的外部 USB DVD 驱动器可能会导致会话性能降低。

[#LC5231]

- COM 端口映射可能会间歇性地失败。

[#LC5235]

- 以下位于性能监视器中的计数器可能会显示不一致。

- \ICA 会话\输入会话带宽

- \ICA 会话\输出会话带宽

此问题仅在计数值很高的情况下出现。

[#LC5262]

- 操作系统中的 picadd.sys 出现错误，并显示蓝屏和错误检测代码 0x3b。

[#LC5299]

- 由于 picadmsys 上的死锁，VDA 可能在出现“欢迎”屏幕后无响应。

[#LC5326]

- 尝试向 Chromebook 设备保存已发布的 Microsoft Excel 电子表格可能会失败。该问题是由于文件扩展名不存在导致。

[#LC6001]

## 智能卡

- 在运行于 Windows 10 Build 10586 及更高版本的 VDA 7.6.300 版及更高版本中不显示登录选项。因此，无法执行智能卡登录。

[#LC4778]

- 当您允许您的 ICA 会话通过空闲的会话计时器断开连接，然后从控制台登录 Remote PC 时，智能卡登录无法正常工作。有时，查看智能卡磁贴的选项会缺失，或者未检测到卡。  
[#LC5187]
- XenDesktop 智能卡会话可能会随机断开连接。  
[#LC5265]
- 通过使用特定的智能卡尝试登录时可能会导致出现以下错误消息：  
“No valid certificates were found on this smart card.  
Please try another smart card or contact your administrator.” (在此智能卡中找不到有效证书。请尝试使用另一个智能卡或联系您的管理员。)  
[#LC5456]

#### 系统异常

- 当 Adobe Shockwave 插件安装在连接至 PVD 的计算机目录上时，Microsoft Internet Explorer 可能在某个用户会话中意外退出。  
[#LC4027]
- 操作系统中的 picadmsys 出现错误，并显示蓝屏和错误检测代码 0x50。  
[#LC4529]
- 操作系统中的 picadmsys 出现错误，并显示蓝屏。  
[#LC4567]
- 从 USB 设备复制未处理的异常可能导致操作系统产生错误，并显示蓝屏。  
[#LC4782]
- 已发布的应用程序可能会意外退出，并在 MobileDesktopHook64.dll 中发生“c000041d”异常。  
[#LC4821]
- 通过远程桌面登录 Windows Server 2008 R2 上运行的 VDA 并启动某些第三方应用程序时，这些应用程序可能会意外退出。  
[#LC5891]

#### 用户体验

- 当您从一个已发布的触控优化桌面切换到正规发布的桌面时，“开始”按钮将：
  - 将鼠标悬停在其上时不会突出显示
  - 打开本地桌面而非已发布的桌面  
[#LC3466]
- 某些 .wmv 文件可能无法以正确的宽高比播放。  
[#LC4695]
- 适用于 3Dconnexion SpaceMouse 的自定义功能可能在某个 VDA 会话中无法工作。  
[#LC4797]
- 在 ICA 会话过程中连接到音频录制/听写软件可能会导致软件意外退出。  
[#LC5407]

#### 用户界面

- 在发布无缝应用程序后，可能会在任务栏上显示通用 Citrix Receiver 图标而非已发布的应用程序图标。  
[#LC4757]

## VDA for Server OS

### HDX MediaStream Windows Media 重定向

[键盘](#)  
[打印](#)  
[服务器/站点管理](#)  
[会话/连接](#)

### 智能卡

[系统异常](#)  
[用户体验](#)  
[用户界面](#)

### HDX MediaStream Windows Media 重定向

- 在启用 HDX MediaStream Windows Media 重定向的情况下，某些第三方播放器可能会在运行于 Windows 10 上的 VDA 中显示文件时意外退出。  
[#LC5110]

#### 键盘

- 从 5.4.400 版升级到 7.6.300 版时，ICA Service\System32 目录会丢失，且键盘/鼠标输入无法在 Mac 客户端上注册。

[#LC4681]

- 无法在 VDA 会话中映射 Bloomberg 键盘，即使策略允许也是如此。

[#LC5360]

## 打印

- 未设置默认打印机时，会话中所有映射的打印机可能会失败。

[#LC4354]

- 在启用旧版打印机名称的情况下，当在一台服务器上为同一用户建立多个会话时，已发布的应用程序可能无法用于自动创建的打印机。

[#LC4517]

- “自动创建客户端打印机”策略可能无法在已发布的应用程序中正确设置默认打印机，且 Microsoft XPS 文档编写器被设置为默认打印机。

[#LC4696]

- SAP 生成的 Excel 电子表格无法在使用通用打印驱动程序 EMF 驱动程序重定向的打印机上打印。

[#LC4853]

- 用户注销并重新登录后，连接到会话的打印机可能无法访问。

[#LC5188]

- Citrix 通用打印驱动程序中的客户端选项上的打印预览会显示给本地端点。

[#LC5404]

## 服务器/站点管理

- 在注销期间，对由 WfShell.exe 进程创建的 "HKEY\_CURRENT\_USER\Software\Microsoft\Internet Explorer>Main" 注册表项所做的更改或添加的值可能无法保留。

[#LC4648]

## 会话/连接

- 在同时应用不允许会话墙纸的 Citrix 策略和指定了墙纸的 Microsoft 组策略的情况下，调整重新连接的会话时，不应用 Citrix 策略。

[#LC0115]

- 退出 64bit ThinAPP 打包的应用程序时，应用程序可能会在 sfrhook64.dll 上遇到意外异常。

要防止出现这种情况，请创建以下服务器端注册表项以解决此问题：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\CtxHook\ApplInit\_Dlls\SfrHook

名称：SkipUnloadOnProcessExit

类型：DWORD

数据：任意值

[#LC3484]

- 在安装了修复程序 ICAWS760WX86022 的系统中，在重新启动 Citrix ICA 服务时，尝试重新连接到用户会话可能会失败。

[#LC3714]

- 具有此增强功能时，在会话中重定向 USB 设备时，会有一个条目写入 Windows 事件日志。

[#LC3996]

- 在使用已发布的 Microsoft Internet Explorer 实例的情况下，从 Web 站点下载文件并将其保存到一个映射的客户端驱动器（“另存为...”）的尝试可能会失败。

[#LC4300]

- 在安装了修复程序 #LC1155 的系统上的会话中，如果手动调整窗口大小，自定义应用程序中的图像显示区域并不正确调整大小。

[#LC4319]

- 通过 Citrix Receiver for Mac 或 Chromebook 连接时，音频文件可能无法在 VDA 会话中播放。

[#LC4596]

- 当 VDA 和 Citrix Receiver 之间的网络中断后，您无法在 Windows Media Player 上播放 .avi 文件。

[#LC4670]

- 在运行于 iOS 设备上的用户会话中，时区重定向可能无法工作。

[#LC4869]

- 使用远程桌面协议后，ICA 会话可能在重新连接到 VM 时显示灰屏。此问题仅发生在使用 /NOCITRIXWDDM 安装的 VDA 上。

[#LC4970]

- USB 设备在重定向到 7.6.300 版的 VDA 后可能无法工作。设备的实例 ID 与序列号不同时，会发生该问题。

为了能够完成此修复，请将产品 ID 或供应商 ID 对添加到以下注册表项：

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\icausb\Parameters

名称：UsingSerialNumberDevices

类型：REG\_MULTI\_SZ

值：`<注意：请在备注字符串旁边，添加 vid=xxxx 和 pid=xxxx 对。（值的语法是不区分大小写规则的排序列表，其中“#”是行注释，每个规则都是一个排序的 vid 和 pid 对。例如，vid=#-number 和 pid=#-number。vid/pid 的最大十六进制值是 FFFF。如果 vid/pid 十六进制值小于 4，则用零 (0) 配对数字。例如，如果 vid 是 12，pid 是 13，则 vid/pid 对应该是 vid=0012, pid=0013。）>`

[#LC5035]

- svchost.exe 进程会占用 100% 的 CPU。

[#LC5041]

- 如果启用了 Excelhook，在应用了修补程序 ICATS760WX64028 后，单击任务栏上的 Excel 图标时，Excel 窗口不会最小化。

[#LC5060]

- 当用户正在登录或注销同时激活了证书传播的情况下，svchost.exe 进程可能会在 SCardHook64.dll 处出现间歇性失败。

[#LC5083]

- 此修复程序解决了一个问题，该问题会导致针对基于 DirectShow 的应用程序的客户端提取操作失败，使得无法显示视频。

[#LC5098]

- 会话可能无法断开连接，导致出现随机 VDA 重新注册。

[#LC5122]

- 操作系统中的 picadd.sys 出现错误，并显示蓝屏和错误检测代码 0xd5。

[#LC5134]

- 作为映射的客户端驱动器映射到会话中的外部 USB DVD 驱动器可能会导致会话性能降低。

[#LC5231]

- COM 端口映射可能会间歇性地失败。

[#LC5235]

- 以下位于性能监视器中的计数器可能会显示不一致。

- \ICA 会话\输入会话带宽

- \ICA 会话\输出会话带宽

此问题仅在计数值很高的情况下出现。

[#LC5262]

- 操作系统中的 picadd.sys 出现错误，并显示蓝屏和错误检测代码 0x3b。

[#LC5299]

- 由于 picadmsys 上的死锁，VDA 可能会在出现“欢迎”屏幕后无响应。

[#LC5326]

- 启用了“特殊文件夹重定向”的情况下，已发布的应用程序可能无法启动，并显示以下错误消息：

“The Citrix server is unable to process your request to start this published application.” (Citrix 服务器无法处理您启动此已发布的应用程序的请求。)

[#LC5593]

- 将 VDA 从 7.6.300 版升级到 7.6 版 LTSR 累积更新 1 后，应用程序的启动可能会较慢或失败。

[#LC5661]

- 尝试向 Chromebook 设备保存已发布的 Microsoft Excel 电子表格可能会失败。该问题是由于文件扩展名不存在导致。

[#LC6001]

## 智能卡

- 在运行于 Windows 10 Build 10586 及更高版本的 VDA 7.6.300 版及更高版本中不显示登录选项。因此，无法执行智能卡登录。

[#LC4778]

- XenDesktop 智能卡会话可能会随机断开连接。

[#LC5265]

- 通过使用特定的智能卡尝试登录时可能会导致出现以下错误消息：

“No valid certificates were found on this smart card.

Please try another smart card or contact your administrator.” (在此智能卡中找不到有效证书。请尝试使用另一个智能卡或联系您的管理员。)

[#LC5456]

## 系统异常

- 操作系统中的 picadmsys 出现错误，并显示蓝屏和错误检测代码 0x50。  
[#LC4529]
- 操作系统中的 picadmsys 出现错误，并显示蓝屏。  
[#LC4567]
- 从 USB 设备复制未处理的异常可能会导致操作系统产生错误，并显示蓝屏。  
[#LC4782]
- 已发布的应用程序可能会意外退出，并在 MobileDesktopHook64.dll 中发生“c000041d”异常。  
[#LC4821]
- 通过远程桌面登录 Windows Server 2008 R2 上运行的 VDA 并启动某些第三方应用程序时，这些应用程序可能会意外退出。  
[#LC5891]

## 用户体验

- 当您从一个已发布的触控优化桌面切换到正规发布的桌面时，“开始”按钮将：
  - 将鼠标悬停在其上时不会突出显示
  - 打开本地桌面而非已发布的桌面  
[#LC3466]
- 某些 .wmv 文件可能无法以正确的宽高比播放。  
[#LC4695]
- 在 ICA 会话过程中连接到音频录制/听写软件可能会导致软件意外退出。  
[#LC5407]

## 用户界面

- 在发布无缝应用程序后，可能会在任务栏上显示通用 Citrix Receiver 图标而非已发布的应用程序图标。  
[#LC4757]

# 累积更新 1 (CU1)

Feb 02, 2017

发布日期：2016 年 5 月 26 日

XenApp 和 XenDesktop 7.6 LTSR 累积更新 1 (CU1)：

- 大约修复了自 7.6 LTSR 起报告的 200 个问题，而自 XenApp 和 XenDesktop 7.6 版本发布以来总共报告了 330 多个问题
- 提供了一个 Metainstaller，允许您从单个统一界面中安装大多数组件  
注意：Provisioning Services 和 Session Recording 作为单独的下载和安装程序提供

[自 XenApp 和 XenDesktop 7.6 LTSR 起已修复的问题](#)

[自 XenApp 和 XenDesktop 7.6 起已修复的问题](#)

[此版本中的已知问题](#)

[新建部署](#)

如何从头开始部署 CU1？

您可以设置基于 CU1 的全新 XenApp/XenDesktop 环境（通过使用 CU1 Metainstaller）。在此之前，建议您熟悉产品：

请仔细阅读 [XenApp 和 XenDesktop 7.6 长期服务版本](#)部分，并特别注意[技术概述](#)、[新建部署](#)和[安全](#)部分，然后再开始计划部署。请确保您的设置满足所有组件的[系统要求](#)。按照[新建部署](#)中的部署说明进行操作。

[现有部署](#)

如何更新？

CU1 提供 7.6 LTSR 的 10 个[基础组件](#)的更新。请记住：Citrix 建议您将您的部署中的所有 LTSR 组件更新到 CU1。例如：如果 LTSR 部署中包含 Provisioning Services，则将 Provisioning Services 组件更新到 CU1。如果 Provisioning Services 不属于您的部署的一部分，则不需要安装或更新该组件。

自 7.6 LTSR 版本起，添加了一个 Metainstaller，允许您从单个统一界面中更新 LTSR 环境的现有组件。按照[升级说明](#)中的指示，使用 Metainstaller 更新您的部署中的 LTSR 组件。

## 注意

下面是 CU1 版本特定的信息。有关 [LTSR 基础版本](#)或 [CU2](#) 的此类信息，请参阅各自的文档。

LTSR 基础组件	版本	注意
VDA for Desktop OS	7.6.1000	适用于 Windows 10 的特殊规则。请参阅 <a href="#">CU1 兼容的组件和平台</a> 。
VDA for Server OS	7.6.1000	

Delivery Controller	7.6.1000	
Citrix Studio	7.6.1000	
Citrix Director	7.6.1000	
组策略管理体验	2.5.1000	
StoreFront	3.0.1000	
Provisioning Services	7.6.2	适用于 Windows 10 的特殊规则。请参阅 <a href="#">CU1 兼容的组件和平台</a> 。
通用打印服务器	7.6.1000	仅支持 Windows 2008 R2 SP1 Windows 2012 Windows 2012 R2
会话录制	7.6.1000	仅限 Platinum Edition

## CU1 兼容的组件

建议您在 7.6 LTSR CU1 环境中使用以下组件。这些组件无权享有 LTSR 的优势（扩展的生命周期以及仅用于修复的累积更新）。Citrix 可能会要求您在 7.6 LTSR 环境中升级到这些组件的较新版本。

**Windows 10 注意事项：**可以通过当前版本路径获取对 Windows 10 的常规支持。Windows 10 无法享有 7.6 LTSR 的所有优势。对于包括 Windows 10 计算机的部署，Citrix 建议您使用 VDA for Desktop OS 7.9 和 Provisioning Services 7.9。

有关详细信息，请参阅 [Adding Windows 10 Compatibility to XenApp and XenDesktop 7.6 LTSR](#) (向 XenApp 和 XenDesktop 7.6 LTSR 添加 Windows 10 兼容性) 和 [XenApp and XenDesktop Servicing Options \(LTSR\) FAQ](#) (XenApp 和 XenDesktop 服务选项 (LTSR) 常见问题解答)。

LTSR CU1 兼容的组件和平台	版本
Profile Management	5.4
AppDNA	7.6.5
许可证服务器	11.13.1
HDX RealTime Optimization Pack	2.0

## Citrix Receiver 的兼容版本

为简化维护过程以及确保实现最佳性能，Citrix 建议您在最新版本的 Citrix Receiver 可用时随时升级到相应版本。可以从 <https://www.citrix.com/downloads/citrix-receiver.html> 下载最新版本。为方便起见，请考虑订阅 [Citrix Receiver RSS 源](#) 以便在新版本的 Citrix Receiver 可用时接收通知。

请注意，Citrix Receiver 无法享有 XenApp 和 XenDesktop LTSR 的优势（扩展的生命周期和仅用于修复的累积更新）。Citrix 可能会要求您在 7.6 LTSR 环境中升级到 Citrix Receiver 的较新版本。如果使用的是 Citrix Receiver for Windows，Citrix 已公布特殊的 LTSR 计划。可以从 [Citrix Receiver 的生命周期里程碑](#) 页面获取有关该计划的详细信息。

特别需要指出的是，LTSR 支持以下版本的 Citrix Receiver 以及之后的所有版本：

Citrix Receiver 的 LTSR 兼容版本	版本
Citrix Receiver for Windows	4.4 或更高版本
Citrix Receiver for Linux	13.2.1 或更高版本
Citrix Receiver for Mac	12.1 或更高版本
Citrix Receiver for Chrome	1.8 或更高版本
Citrix Receiver for HTML5	1.8 或更高版本
Citrix Receiver for iOS	6.1.1 或更高版本
Citrix Receiver for Android	3.8 或更高版本

## 需注意的 LTSR 排除项目

以下功能、组件和平台无法享有 LTSR 的生命周期里程碑和优势。需要特别指出的是，累积更新和扩展生命周期优势被排除在外。可以通过常规的最新版本获取扩展功能和组件的更新。

排除的功能
本地应用程序访问
Framehawk

## 排除的组件

Linux VDA

Personal vDisk

## 排除的 Windows 平台\*

Windows 2008 32 位（面向通用打印服务器）

\* Citrix 保留根据第三方供应商的生命周期里程碑更新平台支持的权利。

## XenApp 6.5 迁移

XenApp 6.5 迁移过程有助于高效快速地从 XenApp 6.5 场过渡到运行 XenApp 7.6（或支持的更高版本）的站点。这在部署中包含大量应用程序和 Citrix 组策略时很有用，可以降低手动将应用程序和 Citrix 组策略移至新 XenApp 站点时意外引入错误的风险。

安装 XenApp 7.6 核心组件并创建站点后，迁移过程按照以下顺序进行：

- 在每个 XenApp 6.5 工作进程上运行 XenApp 7.6 安装程序，将其自动升级到新 Virtual Delivery Agent for Windows Server OS 以便在新站点中使用。
- 在 XenApp 6.5 Controller 上运行 PowerShell 导出 cmdlet，以将应用程序和 Citrix 策略设置导出至 XML 文件。
- 编辑 XML 文件（如果需要），以细化要导入到新站点的内容。通过自定义这些文件，可以将策略和应用程序设置分阶段导入到 XenApp 7.6 站点：即一些现在导入，其他稍后导入。
- 在新 XenApp 7.6 Controller 上运行 PowerShell 导入 cmdlet，以将 XML 文件中的设置导入新 XenApp 站点。
- 根据需要重新配置新站点，然后对其进行测试。

有关详细信息，请参阅[迁移 XenApp 6.x](#)。

## 支持 Citrix Connector 7.5

Citrix Connector 7.5 在 Microsoft System Center Configuration Manager 与 XenApp 或 XenDesktop 之间搭建了一条桥梁，使您可以将 Configuration Manager 的用途扩展到 Citrix 环境。对 Citrix Connector 7.5 的支持现在包括 XenApp 7.6 和 XenDesktop 7.6 Platinum Edition。

有关信息，请参阅[Citrix Connector 7.5 for System Center Configuration Manager 2012](#)。

# 自 XenApp 和 XenDesktop 7.6 LTSR 起已修复的问题

May 10, 2017

XenApp/XenDesktop 7.6 LTSR 累积更新 1 解决了自 XenApp 和 XenDesktop 7.6 LTSR 版本发布以来报告的下列问题。

有关自 XenApp 和 XenDesktop 7.6 版本发布以来已修复的所有问题的列表，请参阅[自 XenApp 和 XenDesktop 7.6 起已修复的问题](#)。

## Citrix Director

- Director 中的用户名搜索操作可能会遇到最多两分钟的随机延迟。

[#LC1250]

- 当尝试将大量数据导出为 PDF 格式时，服务器的 CPU 和内存消耗可达 100%，并出现以下错误消息：

“操作失败。数据源未响应或报告了一个错误。请查看服务器事件日志了解更多信息。”

此修复程序引入了针对 PDF 导出操作的一个可配置的限值，由此，至少可以获得报告的一部分。

安装此修复程序后，必须按如下所示在 wwwroot\Director 文件夹中配置 web.config 文件：

向“appSettings”部分中添加以下行：

该限值取决于服务器的功能（如内存大小），其值指定了 PDF 报告中的行数。

[#LC4108]

- 以任何文件格式导出报告的尝试可能会失败，并出现以下错误消息：

“操作失败。意外的服务器错误。请查看服务器事件日志了解更多信息。”

[#LC4281]

- 如果 XenApp 服务器具有两个 IP 地址且 DNS 服务器无法解析第一个 IP 地址，则管理员可能无法登录到 Citrix Director，并出现以下错误消息：

“系统当前不可用。请稍后重试或联系管理员。”

[#LC4411]

- 尝试以 CSV 格式导出大量数据时，可能会超时，并且导出操作可能会失败，并出现以下错误消息：

“操作失败。数据源未响应或报告了一个错误。请查看 Director 服务器事件日志了解更多信息。”

此修复程序允许您配置针对数据导出操作的超时值。

安装此修复程序后，必须按如下所示配置 wwwroot\Director 文件夹中的 web.config 文件：

向“appSettings”部分添加以下行：

< add key="Connector.DataSourceContext.Timeout" value="3600" />，其中 value 指定超时时间（秒）。

[#LC4467]

- 如果选择一个用户以显示该用户的会话详细信息，可导致该用户的名称在左上角显示为“NULL”。

[#LC4589]

- 如果 NetBios 域名中包含 & 符号，则可能无法从 Citrix Director 控制台执行重影操作。这是因为 & 符号字符是 XML 中的保留字符，并可能导致针对当前登录的解析操作失败。

[#LC4633]

## Citrix 策略

- 如果关闭 Desktop Studio 时未在导航窗格中选择“控制台根节点”，Microsoft 管理控制台 (MMC) 会失败。

[#LC1314]

- Citrix 策略引擎可能导致服务器无响应。如果发生此问题，Citrix Receiver 和 RDP 的连接请求将失败。

[#LC1817]

- 借助此增强功能，通过 Citrix“组策略建模”向导创建的建模报告将出现在 Citrix Studio 的中间窗格中。

[#LC2189]

- 在 Citrix Studio 中添加或创建 Citrix 管理员时，如果使用的用户或组的名称中包含下划线，如 get\dl\_lab\_group，第一个下划线不显示在管理员列表的详细信息中。此名称将显示为 dllab\_group。

[#LC2284]

- 以域用户身份在 AppCenter 的策略节点上运行组策略建模向导时，可能无法显示所应用的用户和计算机策略。

[#LC3284]

- Citrix Director 管理员可能无法在会话详细信息中查看 Citrix 策略。

[#LC3941]

- 尝试在“打印机分配”窗口下向一组用户设备添加多个会话打印机时，无法展开并显示滚动条。由此，向一组用户设备添加多个会话打印机的尝试可能会失败。

[#LC4658]

## Citrix Studio

- 此修复解决了一个安全漏洞。有关详细信息，请参阅知识中心文章 [CTX213045](#)。

注意：为了能够完成此修复，必须使用 7.6 LTSR 累积更新 1 更新 Citrix Studio 和 Controller 组件。

[#LC0559]

- 该修复程序解决了一个问题，此问题导致无法将成员（如果其与 Citrix Studio 不属于同一个域）添加到交付组。

[#LC0955]

- 使用 App-V 集成的应用程序可能无法使用正确的工作目录。

[#LC1623]

- 在升级到 App-V 5.0 Service Pack 3 后，通过 Citrix Receiver 启动 App-V 应用程序的尝试可能会失败。

[#LC1762]

- 在 Citrix Studio 中运行保存时带有“为空”运算符的查询时，此运算符被替换为默认运算符。

[#LC1940]

- 您将具有相同专享升级服务过期日期的 XenApp 和 XenDesktop 许可证合并为一个许可证文件时，Studio 中显示的许可证信息中可能会缺失某些 XenApp 许可证。

**注意：**为了能够完成此修复，必须使用 7.6 LTSR 累积更新 1 更新 Citrix Studio 和 Controller 组件。

[#LC2350]

- 此项修复解决了运行 App-V 应用程序发现时 Citrix Studio 出现内存泄漏的问题。

[#LC2559]

- 当使用 Machine Creation Service 为 VDA for Server OS 编制目录时，个人虚拟磁盘存储的不可用性可能会错误地将目录的“CleanOnBoot”属性设置为“False”。因此，目录可能无法更新。

[#LC2959]

- 当两个应用程序具有相同的 ApplicationID 时，如果刷新 App-V 应用程序，可能导致 Citrix Studio 错误地设置 App-V 包名称。

**注意：**为了能够完成此修复，必须使用 7.6 LTSR 累积更新 1 更新 Citrix Studio 和 Controller 组件。

[#LC2969]

- 关闭 PowerShell 资源时，Citrix Studio 可能无响应。

[#LC3612]

- 在 Citrix Studio 中为交付组下的多个文件夹创建多个应用程序可能会导致很大的文件夹结构。当您首次打开 Citrix Studio 并单击文件夹或应用程序时，可能会拖动而不是选中文件夹或应用程序。这会移动选定对象，并使文件夹或应用程序的结构发生变化。

[#LC3705]

- Add-XDController cmdlet 不向 Controller 分配完全自定义数据库连接字符串。

**注意：**为了能够完成此修复，必须使用 7.6 LTSR 累积更新 1 更新 Citrix Studio 和 Controller 组件。

[#LC3860]

- 如果不属于数据库管理员用户组的用户打开 Citrix Studio，可能会导致 SQL Server 发生权限错误。

注意：为了能够完成此修复，必须使用 7.6 LTSR 累积更新 1 更新 Citrix Studio 和 Controller 组件。

[#LC4127]

- 如果某个服务项目包含两个或更多的租户，则在尝试通过 App Orchestration 2.6 为该服务项目预配更多资源时，可能会失败。

注意：为了能够完成此修复，必须使用 7.6 LTSR 累积更新 1 更新 Citrix Studio 和 Controller 组件。

[#LC4170]

- 当多个 Citrix Studio 会话打开时，在一个会话上执行的策略更改可能会丢失并被其他会话上执行的策略更改覆盖。

注意：为了能够完成此修复，必须使用 7.6 LTSR 累积更新 1 更新 Citrix Studio 和 Controller 组件。

[#LC4487]

## Controller

- 此修复解决了一个安全漏洞。有关详细信息，请参阅知识中心文章 [CTX213045](#)。

注意：为了能够完成此修复，必须使用 7.6 LTSR 累积更新 1 更新 Citrix Studio 和 Controller 组件。

[#LC0559]

- 事件日志中记录了事件 ID 3012 的两个或更多个实例时，事件 ID 3020 和 3021 也出现在日志中，并且消息不正确。应用此修复后，如果记录了事件 ID 3012 的两个或更多个实例，事件 ID 3010 和 3011 正确显示在日志中。

[#LC1425]

- 在事件日志中，事件 ID 1110 和 1111 的错误消息不正确。应用此修复后，事件日志中会显示以下正确消息：

- EventID:1110: 为避免事件日志记录过量，此服务将暂时阻止相关消息(事件 ID: 1100-1109、1112-1116)。
- EventID:1111: 此服务不再阻止相关消息(事件 ID: 1100-1109、1112-1116)。

[#LC1485]

- 如果 NetBios 域名包含 & 符号，尝试启动 Citrix Studio 失败并显示代码为 XDD5:72182E6B 的错误“您无权执行此操作”。

[#LC1646]

- 在某些 Active Directory 组织单位 (OU) 中，如果 OU 名称中包含特殊字符，XenDesktop 的核心服务（如 AD Identity Service 或 Broker Service）可能无法绑定到 OU。这可能会导致 CPU 使用率高于正常水平。此外，服务可能会意外关闭，可能导致 Citrix Studio 无法访问。

[#LC1979]

- 在对已发布的应用程序使用通过关键字执行的过滤时，工作区控制功能可能无法正常工作。

[#LC2025]

- 您将具有相同专享升级服务过期日期的 XenApp 和 XenDesktop 许可证合并为一个许可证文件时，Studio 中显示的许可证信息中可能会缺失某些 XenApp 许可证。

注意：为了能够完成此修复，必须使用 7.6 LTSR 累积更新 1 更新 Citrix Studio 和 Controller 组件。

[#LC2350]

- 包含后导空格的已发布应用程序名称会导致多个问题。从已截断包含后导空格名称的已发布应用程序名称生成浏览器名称时会出现这些问题。

[#LC2897]

- 当两个应用程序具有相同的 ApplicationID 时，如果刷新 App-V 应用程序，可能导致 Citrix Studio 错误地设置 App-V 包名称。

注意：为了能够完成此修复，必须使用 7.6 LTSR 累积更新 1 更新 Citrix Studio 和 Controller 组件。

[#LC2969]

- 执行 Set-BrokerDBConnection 以及相关命令时，Citrix Studio 中的相关配置日志记录条目会列出相应的“主要任务”，并且其状态为“正在进行”，任务完成后，此状态不会更新。

[#LC3479]

- 使用本地系统帐户（通常由 SCCM 等电子软件分发使用）执行到 XenDesktop 7.6 的升级后，Analytics Service 可能无法启动。

[#LC3493]

- 对已连接到 VMware Vsphere 虚拟机管理程序的 VDA 执行计划的重新启动时，可能会导致服务器关闭并处于断电状态。

- 要启用此修复，请设置以下注册表项：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\DesktopServer\RebootSchedule

名称：ShutdownTimeoutRecovery

类型：DWORD

值：1

- 要禁用此修复，请设置以下注册表项：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\DesktopServer\RebootSchedule

名称：ShutdownTimeoutRecovery

类型：DWORD

值：0

在设置值后，必须重新启动 Broker Service。

[#LC3807]

- Add-XDController cmdlet 不向 Controller 分配完全自定义数据库连接字符串。

注意：为了能够完成此修复，必须使用 7.6 LTSR 累积更新 1 更新 Citrix Studio 和 Controller 组件。

[#LC3860]

- 如果不属于数据库管理员用户组的用户打开 Citrix Studio，可能会导致 SQL Server 发生权限错误。

注意：为了能够完成此修复，必须使用 7.6 LTSR 累积更新 1 更新 Citrix Studio 和 Controller 组件。

[#LC4127]

- 如果某个服务项目包含两个或更多的租户，则在尝试通过 App Orchestration 2.6 为该服务项目预配更多资源时，可能会失败。

注意：为了能够完成此修复，必须使用 7.6 LTSR 累积更新 1 更新 Citrix Studio 和 Controller 组件。

[#LC4170]

- 当在控制器上启用“SupportMultipleForest”设置以允许 NTLM 身份验证时，Linux VDA 可能无法完成注册过程，因为可能无法在 Windows Communication Foundation (WCF) 的 EndpointReference 中设置其服务主体名称 (SPN)。

[#LC4235]

- 如果创建由 VMware 虚拟机管理程序托管的虚拟机 (VM)，则在首次尝试从 Citrix Studio 更新或删除这些虚拟机时，操作可能会失败，并显示“错误 ID XDDS:B125B84A”，但后续尝试将成功。

[#LC4436]

- 当多个 Citrix Studio 会话打开时，在一个会话上执行的策略更改可能会丢失并被其他会话上执行的策略更改覆盖。

注意：为了能够完成此修复，必须使用 7.6 LTSR 累积更新 1 更新 Citrix Studio 和 Controller 组件。

[#LC4487]

- 当其中包括用于从/自夏令时切换的开关的日期范围运行 PowerShell 命令“Get-LogSummary”时，将出现以下错误消息：“已添加具有相同键的项”。

当夏令时导致模糊的当地日期或时间时会出现问题。因此，会在 HashMap 中创建重复的条目，并发生异常。

此修复程序引入了一条消息，用于通知用户分别为夏令时的开始或结束时间点将时间跨度拆分到帐户。

[#LC4612]

- 在 Amazon Web Services (AWS) 环境中更新机目录的操作可间歇性失败。要启用此修复程序，必须为将在计算机目录更新期间跳过的映像准备阶段运行命令“Set-ProvServiceConfigurationData –Name ImageManagementPrep\_DoImagePreparation –Value \$false”。

[#LC4709]

- 当存在大量正在运行的应用程序和 VDA 进程时，控制器偶尔会断开与数据库的连接。当发生这种情况时，VDA 保持处于初始化状态，并且应用程序不可用。

[#LC4848]

- 当存在过多的虚拟机管理程序警报时，SQL 数据库服务器的 CPU 使用率可达到 100%。

[#LC5277]

- 在高使用率情况下（超过 5,000 个用户并发地在许多 VDA for Server OS 上启动许多应用程序），SQL 数据库服务器的 CPU

使用率可达到 100% , 从而导致中断且应用程序无法启动。

[#LC5315]

## HDX MediaStream Flash 重定向

- 如果启用了 HDX MediaStream Flash 重定向 , 在 Internet Explorer 中打开和关闭多个含 Flash 内容的选项卡会导致 Internet Explorer 意外退出。

[#LC0375]

- 在启用了 HDX MediaStream for Flash 的情况下 , 在 Internet Explorer 中打开和关闭多个选项卡会导致 Internet Explorer 意外关闭。

[#LC1141]

- 在启用 HDX MediaStream for Flash 重定向的情况下浏览 Web 站点时 , 如果 HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\ApplInit\_DLLs 注册表值设置为“mfaphook.dll”或“mfaphook64.dll”而非“mfaphook.dll”或“mfaphook64.dll”的完整路径 , 则 Flash 重定向功能会失败。

[#LC4388]

## 安装程序

- 如果从命令行安装 VDA 7.6.300 , /noreboot 开关 (具体取决于此开关在开关字符串中的位置) 不会被接受。因此 , VDA 将在安装完成后重新启动。

[#LC4046]

- 安装 VDA 时 , 可能会安装用于提高性能的某些注册表项 , 即使您在安装过程中禁用了“优化性能”选项也是如此。

[#LC4330]

## 许可

- 在设置为法语系统区域设置的许可证服务器上 , Citrix Studio 以西班牙语显示许可模式。

[#LC3450]

## Provisioning Services

控制台

目标设备

服务器

## 控制台

- 安装 Provisioning Services 控制台 7.1.3 后，Windows Server 2008 R2 和 Windows 7 上多个 .NET 应用程序无法启动。

[#LC1838]

- VMware ESX 主机处于维护模式时，XenDesktop 设置向导可能无法创建计算机。

[#LC3401]

- XenDesktop 设置向导可能不在托管单元的 Personal vDisk 存储上使用“被取代”标志。

[#LC3573]

- “流 VM 设置向导”运行过程中，枚举包含多个主机的数据存储的 VMware ESX 群集上的模板需要很长时间才能完成。

[#LC3674]

- 装载和卸载虚拟磁盘时，SOAP Service 可能无响应，并且 Provisioning Services 控制台可能无法启动。

[#LC3723]

- 使用流 VM 设置向导创建计算机时会显示以下错误消息：

对象引用未设置为某个对象的实例。

[#LC3811]

- 技术支持管理员通过 XenDesktop 设置向导从独立的 Provisioning Services 控制台创建新虚拟机 (VM) 时，尝试从 BDM 分区启动目标设备失败，并导致登录服务器显示错误的 IP 地址。

[#LC3911]

- 安装 Provisioning Services 控制台会将以下注册表项设置为 1。这会导致其他 .NET 应用程序尝试使用版本不正确的 Framework，因此可能会失败：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\.NETFramework

名称：OnlyUseLatestCLR

类型：REG\_DWORD

数据：1

[#LC4197]

- 在 Microsoft System Center Virtual Machine Manager (SCVMM) 环境中，尝试使用 XenDesktop 设置向导或流 VM 设置向导创建虚拟机 (VM) 可能会失败。应用此修复后，将在命令中使用主机的完全限定域名 (FQDN) 而非短名称。

[#LC4230]

- 在 System Center Virtual Machine Manager (SCVMM) 2012 环境中，XenDesktop 设置向导可能无法创建 Provisioning Services 目标设备。

[#LC4256]

- 如果用户 1 和用户 2 配置为使用不同的端口，尝试使用流 VM 设置向导或 XenDesktop 设置向导连接到 VMware Vsphere

Hypervisor 5.1 将失败。

要使用不同的端口连接到 VMware ESX 服务器，必须创建以下注册表项：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ProvisioningServices\PlatformEsx

名称：Port

类型：DWORD

值：

[#LC4283]

- XenDesktop 设置向导与 XenServer 之间的 SSL 连接失败。

[#LC4377]

- 这是用于辅助执行 NIC 成组的增强功能，通过 HP Moonshot 系统中使用的最新 Mellanox NIC 和固件实现。

[#LC4646]

- 如果在 System Center Virtual Machine Manager (SCVMM) 中创建的模板具有位于两个不同网络上的 NIC（例如，网络 xxx 上的 NIC1 和网络 yyy 上的 NIC2），则 XenDesktop 设置向导的默认行为是将这两个 NIC 均更改为主机记录的网络（网络 zzz）。要使 NIC2 网络保持不变，请在安装此修复后设置以下注册表项：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ProvisioningServices\PlatformScvmm

名称：RequireMatchingNetworks

类型：REG\_DWORD

值：1

[#LC4650]

- 如果在未选择任何产品的情况下按“Ctrl+C”，Provisioning Services 控制台可能会意外退出并显示以下错误消息：

“MMC has detected an error in a snap-in and will unload it.” (MMC 在管理单元中检测到错误，并且会将其卸载。)

此外，如果某些第三方软件自动注入“Ctrl+C”组合键，也可能会出现此问题。

[#LC4909]

## 服务器

- 使用 BDM 分区时，如果列表中最上面的服务器无法访问，VMware 上运行的目标设备将不尝试登录列表中的所有服务器。

[#LC3805]

- 尝试在 Provisioning Server 上装载虚拟机磁盘失败，除非服务器对虚拟磁盘具有逻辑访问权限。

[#LC3835]

- 技术支持管理员通过 XenDesktop 设置向导从独立的 Provisioning Services 控制台创建新虚拟机 (VM) 时，尝试从 BDM 分区启动目标设备失败，并导致登录服务器显示错误的 IP 地址。

[#LC3911]

- 当导出通过运行 PowerShell 命令“Mcli-Run ExportDisk -p DiskLocatorName="DISK\_NAME",

StoreName="STORE\_NAME", SiteName="SITE\_NAME""导出虚拟磁盘时，可能会创建其中包含对应于每个虚拟磁盘版本的多个条目的清单文件。当多个站点中存在同名的虚拟磁盘时，会出现此问题。每个版本的重复条目数量对应于具有虚拟磁盘的站点的数目。

[#LC4225]

- 在 SCVMM 环境中，如果 VM 存储路径末尾存在尾随反斜杠 (\)，通过 XenDesktop 设置向导创建计算机将失败。

[#LC4418]

- 这是用于辅助执行 NIC 成组的增强功能，通过 HP Moonshot 系统中使用的最新 Mellanox NIC 和固件实现。

[#LC4646]

- 如果在 System Center Virtual Machine Manager (SCVMM) 中创建的模板具有位于两个不同网络上的 NIC (例如，网络 xxx 上的 NIC1 和网络 yyy 上的 NIC2) ，则 XenDesktop 设置向导的默认行为是将这两个 NIC 均更改为主机记录的网络 (网络 zzz) 。要使 NIC2 网络保持不变，请在安装此修复后设置以下注册表项：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ProvisioningServices\PlatformScvmm

名称：RequireMatchingNetworks

类型：REG\_DWORD

值：1

[#LC4650]

## 目标设备

- 在带有 ESX VMXNET3 NIC 的系统上安装 Provisioning Services 目标设备时需安装 Microsoft 修补程序 <https://support.microsoft.com/en-us/kb/2550978> 或替代修补程序。通过此修补程序，将不会明确要求安装 KB2550978，而会显示一条警告消息，通知管理员确保安装 KB2550978 或替代修补程序。

[#LC3016]

- 服务登录帐户设置为“本地系统”(默认值)时，PVS Device Service (BNDevice.exe) 可能无法成功启动。

[#LC3209]

- 与 Active Directory 密码更改相关的某些严重错误日志的日志记录级别可能未正确设置，因此，这些日志不会发送到服务器以便 Citrix Diagnostic Facility 进行跟踪。

[#LC3803]

- 在启用了 PvD 的虚拟磁盘上，自动虚拟磁盘更新功能不运行清单更新。

[#LC3997]

- 使用 VMXnet3 网络驱动程序的 ESX 目标设备会遇到致命问题，在使用 Jumbo 帧 (每个帧的负载超过 1500 字节) 时显示蓝屏。

[#LC4238]

- 预配的目标设备具有 96 小时的许可宽限期，在此之后，如果没有有效的可用许可证，目标设备将关闭。通过此增强功能，目标设备的许可宽限期延长至 30 天 (720 小时)。

[#LC4645]

# 会话录制

代理

播放器

## 代理

- 在 Session Recording Agent 属性中启用“Allow third party applications to record custom data on this VDA machine”（允许第三方应用程序在此 VDA 计算机上记录自定义数据）的情况下，在日语版本的 Windows 操作系统上运行的 Session Recording Agent Service 可能无法启动，并且无法记录客户端会话。

[#LC3861]

## 播放器

- Microsoft 画图会话的录制件无法在 Session Recording Player 中正确播放。

[#LC4389]

- 播放在多显示器用户设备上录制的会话时出现错误。

[#LC4391]

# StoreFront

- 此修复解决了管理控制台用户界面中术语“Classic”的日语翻译不一致的问题。

[#LC3607]

- 单击启动第二个或后续的应用程序时，可能会启动所启动的第一个应用程序的一个或多个实例。如果配置了多站点聚合，则在使用除 Citrix Receiver for Web 以外的 Receiver 版本时会出现此问题。第一个应用程序的另外一个实例可能会从每个聚合的站点启动。

[#LC4278]

- 在 default.ica 文件中为已发布的桌面所做的自定义设置可能不会被接受。例如，您可能无法查看某些桌面内部的连接栏，即使已设置“ConnectionBar = 1”也是如此。

[#LC4688]

- 在某些情况下，StoreFront 会生成包含重复资源的枚举响应。这可能会导致 Receiver for Web 报告故障，并且应用程序可能无法显示。在下列一种或多种情况下会出现此问题：

- 场由多站点配置中的多个 UserFarmMapping 引用。
- 用户属于已应用多个 UserFarmMapping 的 Active Directory 组。
- 其中包含场的 EquivalentFarmSets 没有聚合组，或者存在其中包含针对用户的多个分配的交付组。

# 通用打印服务器

客户端

服务器

## 客户端

- 可能无法在 VDA for Server OS 上的 Microsoft 打印管理控制台中管理远程打印服务器上的端口或打印机，并出现以下错误消息：“Failed to complete the operation. This operation is not supported.”（无法完成此操作。此操作不受支持。）此外，在导航到“端口”选项卡时，可能不会列出端口。

此外，当您右键单击任何打印机并选择“Open Printer Queue”（打开打印机队列）时，可能会出现以下错误消息：

“Windows can't find the printer. Make sure the network is working and you've entered the name of the printer and print server correctly.”（Windows 找不到打印机。请确保网络正常工作，并且您已正确输入打印机和打印服务器的名称。）

要解决此问题，请在 VDA 的注册表中删除注册表

项“HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Print\Providers\Universal Printer”，然后重新启动打印后台处理程序服务。这些端口将在 Microsoft 打印管理控制台中正确枚举，并且您可以配置端口和打印机。

[#LC3740]

## 服务器

- 通过使用 Microsoft GDI Print API 进行的批量打印可能失败，无法打印到最后一页，并出现以下错误消息：

“Dispatch::CDriverTripSummary::PrintReport, Error Occured While Printing....Check  
Printer”（Dispatch::CDriverTripSummary::Print Report，打印时出现错误....请检查打印机）

[#LC3920]

- 此修复程序支持适用于通用打印服务器 7.6.300 的 Citrix UPS Print Driver Certification Tool。有关详细信息，请参阅知识中心文章 [CTX142119](#)。

[#LC4265]

# VDA for Desktop OS

内容重定向

打印

HDX 3D Pro

无缝窗口

HDX MediaStream Flash 重定向

服务器/站点管理

HDX MediaStream Windows Media 重定向

会话/连接

[安装、卸载、升级](#)

[智能卡](#)

[键盘](#)

[系统异常](#)

[登录/身份验证](#)

## 内容重定向

- 在为 Mailto 链接启用内容重定向的情况下，其中含有逗号的 Mailto 链接无法启动，并出现以下错误消息：

“Could not perform this operation because the default mail client is not properly installed”（因为默认邮件客户端未正确安装，无法执行此操作。）

该问题不会在控制台或远程桌面会话中发生。

[#LC3701]

## HDX 3D Pro

- 在 HDX 3D Pro 双显示器配置中，在一个显示器上锁定 Windows 可能不会使第二个显示器屏幕显示空白。如果与一个双显示器客户端会话断开连接后，从一个显示器客户端重新连接，然后从该会话中断开连接，再从该双显示器客户端重新连接，则会发生此问题。

[#LC3934]

- 将鼠标放置在 Microsoft Notepad 应用程序窗口边缘时，鼠标指针可能无法呈现正确的形状。

要启用此项修复，必须设置以下注册表项：

- 在 32 位 Windows 上：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\HDX3D

名称：EnableUnknownCursorHandling

类型：REG\_DWORD

值：1

- 在 64 位 Windows 上：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\HDX3D

名称：EnableUnknownCursorHandling

类型：REG\_DWORD

值：1

[#LC4160]

- 尝试调整会话屏幕分辨率可能会间歇性失败，从而使 DesktopViewer 窗口灰显。

[#LC4261]

- 在启用 HDX 3D Pro 的情况下，用于呈现应用程序的 3D 图形中的自定义鼠标指针可能无法正确显示。

[#LC4713]

## HDX MediaStream Flash 重定向

- 如果启用了 HDX MediaStream Flash 重定向，在 Internet Explorer 中打开和关闭多个含 Flash 内容的选项卡会导致

Internet Explorer 意外退出。

[#LC0375]

- 在启用了 HDX MediaStream for Flash 的情况下，在 Internet Explorer 中打开和关闭多个选项卡会导致 Internet Explorer 意外关闭。

[#LC1141]

- 在启用 HDX MediaStream for Flash 重定向的情况下浏览 Web 站点时，如果 HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\ApplInit\_DLLs 注册表值设置为“mfaphook.dll”或“mfaphook64.dll”而非“mfaphook.dll”或“mfaphook64.dll”的完整路径，则 Flash 重定向功能会失败。

[#LC4388]

### HDX MediaStream Windows Media 重定向

- 在 Receiver 会话中，如果在播放 .MOD、ac3 和 mpeg 文件期间在 Windows Media Player 中向前搜寻，可能会导致播放视频但不播放音频。

[#LC2768]

- 如果您在 ICA 会话（或已发布的桌面会话）中使用 Windows Media Player 播放 .avi 文件，然后在不停止第一个 .avi 文件的情况下开始播放另一个 .avi 文件，则视频帧可能无法正确定向到用户设备。由此，mmvdhost.exe 进程的 CPU 使用率可高于正常使用率，并且视频可能无法在用户设备上正常显示。

[#LC4260]

### 安装、卸载、升级

- 在安装以下一个或多个 Microsoft 安全更新后，登录正在运行 Windows 10 的 XenDesktop VDA 7.6.300 或 7.7 的尝试会失败。有关详细信息，请参阅知识中心文章 [CTX205398](#)。

	安全更新	发行日期
<b>Windows 10 RTM (LTSB)</b>	<a href="#">KB3124266</a>	2016 年 1 月
	<a href="#">KB3135174</a>	2016 年 2 月
	<a href="#">KB3140745</a>	2016 年 3 月
	<a href="#">KB3147461</a>	2016 年 4 月
	<a href="#">KB3156387</a>	2016 年 5 月
<b>Windows 10 版本 1511 (当前业务分支)</b>	<a href="#">KB3124263</a>	2016 年 1 月
	<a href="#">KB3124262</a>	2016 年 1 月

	<a href="#">KB3135173</a>	2016 年 2 月
	<a href="#">KB3140768</a>	2016 年 3 月
	<a href="#">KB3147458</a>	2016 年 4 月
	<a href="#">KB3156421</a>	2016 年 5 月
<b>Windows 10 版本 1511</b>  (2016 年 2 月更新)	其中包含 2016 年 2 月的所有更新的累积映像	2016 年 3 月

**注意：如果您已安装上述任何 Microsoft 安全更新：**

如果您已经在 Windows 10 RTM (Build 10240) VDA 或 Windows 10 版本 1511 (Build 10586.36) VDA 上安装任何上述 Microsoft 安全更新，并需要应用此更新，请执行以下操作：

1. 重新启动并使用安全模式登录到 Windows 10 VDA。
2. 卸载上述 Microsoft 安全更新，然后重新启动。
3. 安装此更新并重新启动。
4. 安装任何适用的 Microsoft 安全更新。

对于在 Windows 10 (RTM/版本 1511/版本 1511 (在 2016 年 2 月更新)) 上新部署的 7.6.300 VDA，请执行以下操作：

1. 准备 Windows 10 (RTM/版本 1511/版本 1511 (在 2016 年 2 月更新)) 映像。

**警告：**在下一步中安装 VDA 和重新引导系统可使计算机进入无法恢复的状态。无需在安装 VDA 后执行重新启动。

2. 安装 7.6.300 VDA 并选择不重新启动。
3. 安装此更新并重新启动。

[来自 DesktopVDACoreWX86\_7\_6\_305、DesktopVDACoreWX64\_7\_6\_305][#LC4604]

## 键盘

- 如果您在 VDA 会话中运行 Citrix GoToMeeting 并被设置为演示者，则您的鼠标指针可能会开始闪烁。如果会话禁用了“旧图形模式”策略设置，则会发生此问题。

[#LC3033]

## 登录/身份验证

- 如果“Windows 远程桌面会话主机配置”策略设置“始终在连接时提示输入密码”已启用，则当用户使用 ICA 协议登录到 VDA 7.x 时，系统会提示用户重新输入凭据。

要启用此修复，请设置以下注册表项：

HKEY\_LOCAL\_MACHINE\Software\Citrix\Portica  
名称：AutoLogon

类型 : DWORD

数据 : 0x00000001 (值必须介于 0 到 2147483647 之间)

注意 : 如果多次尝试运行 MSP 文件 , 可标记 Citrix Display Drive 以进行删除。这将导致无法安装修补程序。此外 , VDA 的显示分辨率可能不正常。要使其正常 , 请重新启动 VDA , 然后再安装修补程序。

[来自 DesktopVDACoreWX86\_7\_6\_301、DesktopVDACoreWX64\_7\_6\_301][#LC1180]

- 安装 Microsoft 修补程序 KB3124266 (对于 Windows 10) 或 KB3124263 (对于 Windows 10 1511) 后 , 尝试登录到 Windows 10 上运行的 XenDesktop VDA 7.6.300 或 7.7 可能会失败。有关详细信息 , 请参阅知识中心文章 [CTX205398](#)。

注意 : 如果您已安装 KB3124266 或 KB3124263 , 并希望应用此更新 , 请执行以下操作 :

- 重新启动并使用安全模式登录到 Windows 10 计算机 , 然后卸载 KB3124266 或 KB3124263
- 重新启动 Windows 10 计算机 , 然后安装此更新。
- 重新安装 KB3124266 或 KB3124263。

[来自 DesktopVDACoreWX86\_7\_6\_304、DesktopVDACoreWX64\_7\_6\_304][#LC4540]

## 打印

- Citrix 打印后台处理程序服务可能会意外退出。

[来自 DesktopVDACoreWX86\_7\_6\_307、DesktopVDACoreWX64\_7\_6\_307][#LC4180]

## 无缝窗口

- 无缝应用程序可能无响应 , 它在 Windows 任务栏中的图标将还原为通用 Citrix Receiver 图标。

[#LC3783]

- 关闭一个无缝已发布应用程序后 , 焦点将转到另一个已发布应用程序 , 而不是典型 [Windows Z 顺序](#) 中的窗口。

[#LC4009]

## 服务器/站点管理

- 在管理员尝试从 Hyper-V 控制台访问虚拟机时 , 如果某个会话已断开连接 , 但处于活动状态 , 则会显示黑屏。在使用 XPDM 驱动程序的部署环境中会发生此问题。

[#LC3536]

- VDA 可能不再接受连接。启动“旧图形模式”策略后 , VDA 将再次开始接受连接。

[#LC3749]

- 当启动 VM 托管的应用程序时 , 可能在应用程序完全启动之前显示 Windows 登录屏幕。此修复程序将提供 15 秒的宽限期 , 然后欢迎屏幕才会出现。它还支持以下注册表项 , 使您可以自定义宽限期的持续时间。

注意 : 在宽限期内 , 不会向用户显示信息以指出应用程序正在启动。如果配置过高的宽限期 , 可能使应用程序启动延迟 , 并导致用户无意中启动应用程序多次。

要更改宽限期的持续时间 , 请设置以下注册表项 :

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI

名称 : LogonUIHideTimeout

类型 : DWORD

值 : 任何大于零值 , 以毫秒为单位 (例如 , 20000 毫秒对应于 20 秒)

[#LC3828]

- 尝试使用 attrib 命令更改已映射客户端驱动器上的文件的文件属性可能会失败。

[#LC3958]

- “输出会话带宽性能监控”计数器可能会在很长一段时间内在记录时报告不一致的值。

[#LC4151]

- 如果您使用显式凭据 (用户名/密码) 登录到 7.6.300 VDA 版本 , 并且已启用用户帐户控制 (UAC) , 则在尝试使用智能卡对正在会话中运行的应用程序进行身份验证时 , 可能会出现以下错误消息 :

“An authentication error has occurred. No credentials are available in the security package.” (发生身份验证错误。安全包中没有可用的凭据。)

[#LC4486]

## 会话/连接

- 当端点安装有多个网络摄像机或视频捕捉设备时 , 只会将其中一个设备映射到客户端会话。此外 , 设备将映射为 Citrix HDX 网络摄像机 , 而不会留下关于所映射设备的任何明显迹象。

[#LC1919]

- 在已启用本地应用程序访问的会话中 , 无法激活屏幕保护程序。

[#LC3182]

- Citrix 策略“拖动时查看窗口内容”无法正常工作。

[#LC3552]

- 已断开的会话可能会在物理计算机上保持打开 , 即使已经过在“断开会话计时器时间间隔”中指定的时间后也是如此。

要启用此修复 , 请设置以下注册表项 :

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\Portica

名称 : ForceDisableRemotePC

类型 : DWORD

值 : 任何大于零的值

[#LC3650]

- 如果端点在几分钟里丢失网络连接 , 则重新连接尝试可能会失败 , 直至 VDA 重新启动。

[来自 DesktopVDACoreWX86\_7\_6\_301、DesktopVDACoreWX64\_7\_6\_301][#LC3700]

- 当在 VDA 长时间处于空闲状态后登录到 VDA 时 , 在重新连接时可能不会自动将凭据传递给登录屏幕 , 并且登录屏幕上会提示输入密码。

[来自 DesktopVDACoreWX86\_7\_6\_309、DesktopVDACoreWX64\_7\_6\_309][#LC3720]

- 即使相关已发布应用程序关闭了文件，WFICA32.exe 进程也仍会使该文件保持锁定状态。因此，在一段时间内无法编辑该文件。

[#LC3724]

- 某些第三方发布的应用程序可能无法在 XenApp 服务器上启动。由此，wfshell.exe 进程可能会意外关闭。发生此错误时，不<sup>会在用户设备上显示任何表明会话正在启动的信息，也不会显示错误消息。</sup>

[#LC3766]

- 移除多显示器会话中的 Thomson Reuters Eikon 工具栏后，会话不回收该工具栏占用的空间。

在其中的主显示器不位于阵列左上角的显示器配置中，您还必须安装修复程序 #LC1599（此修复程序在 Receiver for Windows 4.4 及更高版本中提供）。

[#LC3773]

- 当在会话主机上启用 App-V 配置设置“EnablePublishingRefreshUI”并且已启用“Session Lingering”时，如果尝试在 iOS 设备上关闭应用程序，可能会导致设备屏幕上显示黑色窗口。

[#LC3800]

- 启用 Citrix Windows XP 显示驱动程序模型 (XPDM) 显示驱动程序后，鼠标阴影设置将始终处于启用状态，即使在控制面板中将其禁用也是如此。

[来自 DesktopVDACoreWX86\_7\_6\_302、DesktopVDACoreWX64\_7\_6\_302][#LC3806]

- 如果启用了 Excelhook，则在最小化后还原 Excel 工作簿时，可能导致 Excel 窗口丢失焦点。

[#LC3873]

- 对于使用 Citrix Receiver for Android 的会话，“限制会话剪贴板写入”和“限制客户端剪贴板写入”策略无法正常工作。由此，用户可在会话和用户设备之间复制并粘贴内容，而不管这两个策略的配置如何。

[#LC3894]

- 当您尝试重新连接到已断开的会话时，会出现 Windows 锁屏界面，其中包含一组键，但没有用于输入密码的选项。当单击“其他凭据”时，会显示第二个凭据图标，可用于输入密码并解锁会话。

[来自 DesktopVDACoreWX86\_7\_6\_306、DesktopVDACoreWX64\_7\_6\_306][#LC4053]

- 如果在 ICA 会话中关闭电源或强制重新启动远程计算机，可能会在远程 PC 重启完成时禁用所有音频驱动程序。

[#LC4071]

- 如果在相关已发布应用程序正在运行时向用户设备文件夹添加文件，然后尝试从该应用程序中打开该文件，则该应用程序的“打开文件”对话框可能无法显示该文件，即使单击刷新按钮也是如此。

[#LC4073]

- 由于 picadm.sys 上的死锁，VDA 可能在出现“欢迎”屏幕后无响应。

[来自 DesktopVDACoreWX86\_7\_6\_308、DesktopVDACoreWX64\_7\_6\_308][#LC4195]

- 启用通用 USB 重定向功能后，每当在会话中与通用重定向的 USB 设备断开物理连接并重新连接时，该设备都会被视为新设备。因此，每次重新连接这种 USB 设备时，系统都会为其另外创建一个 GUID。

[来自 DesktopVDACoreWX86\_7\_6\_303、DesktopVDACoreWX86\_7\_6\_303][#LC4259]

- 如果满足所有三个下列条件，则 Citrix Receiver for Chrome 和 VDA 之间的 TLS 连接会失败：

- 已在 VDA 上安装修复程序 #LC2179（修补程序 ICAWS760WX64032 或其替代项）
- 连接已配置为使用 SSL
- Citrix Gateway Protocol (CGP) 已禁用

[#LC4405]

- 在安装修补程序 ICAWS760WX64032 和启用 SSL 后，重新连接到 VDA 的尝试可能会间歇性失败。如果 Citrix ICA 服务因为 SSL 倾听器故障而意外退出或无响应，将出现该问题。

[#LC4438]

- 当在用户设备之间漫游会话时，在 VDA for Desktop OS 7.6.300 版本（已安装 RES Workspace Manager）上运行的会话可能不响应。

[#LC4570]

## 智能卡

- 在 Microsoft Internet Explorer 中，某些 Web 站点的智能卡登录用户界面可能间歇性不可用。

[#LC3988]

## 系统异常

- 在登录或更改显示分辨率时，Ctxgfx.exe 进程可能进入死锁状态，并导致会话挂起。

[#LC2410]

- 操作系统中的 picadm.sys 出现错误，并显示蓝屏和停止代码 0x20。

[#LC3473]

- 操作系统中的 picadm.sys 出现错误，并显示蓝屏和停止代码 0x00000050。

[#LC3921]

- 操作系统中的 ctxad.sys 出现错误，并显示蓝屏和错误检测代码 0xD1。

[#LC4007]

- 在将 VDA for Desktop OS 或 Server OS 升级到 7.6.300 版后，Citrix Print Manager Service (CpSvc.exe) 可能会在注销时意外退出。

[来自 DesktopVDACoreWX86\_7\_6\_307、DesktopVDACoreWX64\_7\_6\_307][#LC4102]

- 操作系统中的 picadm.sys 出现错误，并显示蓝屏和停止代码 0x000000C1。

[#LC4334]

- 当您在 Windows Media Player 上重复播放 .avi 文件时，wfica32.exe 进程消耗的内存可能会持续增加，直到此进程意外退出。

[#LC4335]

- 在从 Citrix Receiver 会话注销时，VDA 可能在 picadd.sys 中遇到严重异常，并显示蓝屏。

[#LC4360]

- VDA 可能在 ctxdvcs.sys 中的错误检测代码 0x00000044 处遇到严重异常，并显示蓝屏。

[#LC4505]

- 如果已定义注册表项 HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ICA\Thinwire\DisableOssForProcesses，则在尝试重新启动 VDA 和启动已发布的桌面时可导致蓝屏。

[#LC4597]

## VDA for Server OS

### 内容重定向

#### HDX MediaStream Windows Media 重定向

#### 键盘

#### 打印

#### 无缝窗口

### 服务器/站点管理

#### 会话/连接

#### 智能卡

#### 系统异常

#### 用户体验

### 内容重定向

- 在除运行 Windows Server 2008 R2 的 VDA 外的其他 VDA 上，从服务器到客户端的内容重定向会失败。因此，当您单击 VDA 会话中的 URL 时，链接将在运行于会话中的浏览器中打开，而不是在本地浏览器中打开。

[#LC2221]

- 在为 Mailto 链接启用内容重定向的情况下，其中含有逗号的 Mailto 链接无法启动，并出现以下错误消息：

“Could not perform this operation because the default mail client is not properly installed”（因为默认邮件客户端未正确安装，无法执行此操作。）

该问题不会在控制台或远程桌面会话中发生。

[#LC3701]

### HDX MediaStream Windows Media 重定向

- 在 Receiver 会话中，如果在播放 .MOD、ac3 和 mpeg 文件期间在 Windows Media Player 中向前搜寻，可能会导致播放视频但不播放音频。

[#LC2768]

- 如果您在 ICA 会话（或已发布的桌面会话）中使用 Windows Media Player 播放 .avi 文件，然后在不停止第一个 .avi 文件的情况下开始播放另一个 .avi 文件，则视频帧可能无法正确定向到用户设备。由此，mmvdhost.exe 进程的 CPU 使用率可高于正常使用率，并且视频可能无法在用户设备上正常显示。

[#LC4260]

## 键盘

- 如果您在 VDA 会话中运行 Citrix GoToMeeting 并被设置为演示者，则您的鼠标指针可能会开始闪烁。如果会话禁用了“旧图形模式”策略设置，则会发生此问题。

[#LC3033]

## 打印

- Citrix 打印后台处理程序服务可能会意外退出。

[来自 ServerVDACoreWX64\_7\_6\_304] [#LC4180]

## 无缝窗口

- 无缝应用程序可能无响应，它在 Windows 任务栏中的图标将还原为通用 Citrix Receiver 图标。  
[#LC3783]
- 关闭一个无缝已发布应用程序后，焦点将转到另一个已发布应用程序，而不是典型 Windows Z 顺序中的窗口。  
[#LC4009]

## 服务器/站点管理

- 当启动 VM 托管的应用程序时，可能会在应用程序完全启动之前显示 Windows 登录屏幕。此修复程序将提供 15 秒的宽限期，然后欢迎屏幕才会出现。它还支持以下注册表项，使您可以自定义宽限期的持续时间。

注意：在宽限期内，不会向用户显示信息以指出应用程序正在启动。如果配置过高的宽限期，可能使应用程序启动延迟，并导致用户无意中启动应用程序多次。

要更改宽限期的持续时间，请设置以下注册表项：

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI

名称：LogonUIHideTimeout

类型：DWORD

值：任何大于零值，以毫秒为单位（例如，20000 毫秒对应于 20 秒）

[#LC3828]

- 尝试使用 attrib 命令更改已映射客户端驱动器上的文件的文件属性可能会失败。  
[#LC3958]
- 从单独用户设备建立与 VDA 的远程桌面 (RDP) 连接的多个并行尝试可能导致 VDA 取消注册。  
[#LC4014]

- “输出会话带宽性能监控”计数器可能会在很长一段时间内在记录时报告不一致的值。

[#LC4151]

- 当 VDA for Server OS 未注册或 Citrix Desktop Service 被禁用时，即使是域管理员也无法通过远程桌面 (RDP) 连接登录到 VDA。然而该行为是为非管理员角色设计的，管理员应能够进行登录。

[#LC4290]

- 如果您使用显式凭据（用户名/密码）登录到 7.6.300 VDA 版本，并且已启用用户帐户控制 (UAC)，则在尝试使用智能卡对正在会话中运行的应用程序进行身份验证时，可能会出现以下错误消息：

“An authentication error has occurred. No credentials are available in the security package.” (发生身份验证错误。安全包中没有可用的凭据。)

[#LC4486]

- 无法在 Excel 电子表格中进行实时滚动（翻页和滚动的同步状态）。VDA 7.6.300 版本中引入了修复程序 #LC2965，用于解决此问题。但是，修复程序 #LC2965 无法在所有情况下完全解决此问题。修复程序 #LC4579 可确保更正此问题，即使在修复程序 #LC2965 不起作用的系统中也是如此。

根据 #LC2965 的说明：

无法在 Excel 电子表格中进行实时滚动（翻页和滚动的同步状态）。之所以发生此问题，是因为在用户每次登录 VDA 时，VDA 上的注册表位置 HKEY\_CURRENT\_USER\Control Panel\Desktop\UserPreferencesMask 中的注册表项和值被 wfshell.exe 进程重写。要阻止此问题，请在 VDA 上创建以下注册表项，并将值设置为 1：

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix

名称：EnableVisualEffect

类型：REG\_DWORD

值：1

[#LC4579]

- 安装修补程序 ICATS760WX64022（或其替代项）之后，注册表项 HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\Graphics\下的任何新自定义注册表配置在重新启动系统后可能无法保留。

[#LC4931]

## 会话/连接

- “源网络地址”在服务器的 Windows 安全日志中为远程用户设备显示不正确的 IP 地址（事件 ID 为 4624）。

[#LC1352]

- 在禁用“客户端音频重定向”或“Windows Media 重定向”策略的情况下，已发布的桌面会话的通知区域中的音量控制（扬声器）图标可能显示不正确的音频状态。

[#LC2538]

- 在 Citrix Receiver for Android 发布的桌面会话中，打开 Microsoft Outlook 日历邀请的尝试可能会失败，并出现以下错误消息：

“Cannot open item”（无法打开项目）

此问题发生于其他用户所创建的日历邀请；由相同用户创建的邀请不受影响。

[#LC2828]

- 在某些情况下，在登录或重新连接到已断开的会话时，客户端打印机重定向和 Citrix 组策略访问控制过滤器可能无法工作。

[#LC3083]

- 在已启用本地应用程序访问的会话中，无法激活屏幕保护程序。

[#LC3182]

- 即使相关已发布应用程序关闭了文件，WFICA32.exe 进程也仍会使该文件保持锁定状态。因此，在一段时间内无法编辑该文件。

[#LC3724]

- 某些第三方发布的应用程序可能无法在 XenApp 服务器上启动。由此，wfshell.exe 进程可能会意外关闭。发生此错误时，不会在用户设备上显示任何表明会话正在启动的信息，也不会显示错误消息。

[#LC3766]

- 移除多显示器会话中的 Thomson Reuters Eikon 工具栏后，会话不回收该工具栏占用的空间。

在其中的主显示器不位于阵列左上角的显示器配置中，您还必须安装修复程序 #LC1599（此修复程序在 Receiver for Windows 4.4 及更高版本中提供）。

[#LC3773]

- 当在会话主机上启用 App-V 配置设置“EnablePublishingRefreshUI”并且已启用“Session Lingering”时，如果尝试在 iOS 设备上关闭应用程序，可能会导致设备屏幕上显示黑色窗口。

[#LC3800]

- 在通过 RDP 会话连接到服务器时，在终端服务 (TermService) 中注册的服务主机 (svchost.exe) 进程可能会在 RPM.dll 上意外关闭。

[#LC3808]

- 如果启用了 Excelhook，则在最小化后还原 Excel 工作簿时，可能导致 Excel 窗口丢失焦点。

[#LC3873]

- 即使在已启用客户端音频重定向策略的情况下，音频 (.wav) 文件仍可能无法播放。在重复使用会话 ID 且已为上一个会话禁用客户端音频重定向策略的情况下，会出现此问题。

[#LC3882]

- 对于使用 Citrix Receiver for Android 的会话，“限制会话剪贴板写入”和“限制客户端剪贴板写入”策略无法正常工作。由此，用户可在会话和用户设备之间复制并粘贴内容，而不管这两个策略的配置如何。

[#LC3894]

- 当因为许可证错误而导致 Windows Server 2008 R2 VDA 的连接失败时，无法显示错误消息“由于没有可用的许可证，无法访问此会话。”。

[#LC4026]

- 如果在相关已发布应用程序正在运行时向用户设备文件夹添加文件，然后尝试从该应用程序中打开该文件，则该应用程序的“打开文件”对话框可能无法显示该文件，即使单击刷新按钮也是如此。

[#LC4073]

- 在注销新安装的 Feature Pack 3 VDA for Server OS (7.6.300) 后，Citrix Studio 可能会将 VDA 的状态显示为“正在初始化”而不是“已注册”。在此期间，将不会为该 VDA 代理任何新会话。

[#LC4188]

- 由于 picadm.sys 上的死锁，VDA 可能在出现“欢迎”屏幕后无响应。

[来自 ServerVDACoreWX64\_7\_6\_305][#LC4195]

- 启用通用 USB 重定向功能后，每当在会话中与通用重定向的 USB 设备断开物理连接并重新连接时，该设备都会被视为新设备。因此，每次重新连接这种 USB 设备时，系统都会为其另外创建一个 GUID。

[来自 ServerVDACoreWX64\_7\_6\_303][#LC4259]

- COM 端口映射可能会间歇性地失败。

[#LC4267]

- 在启用“应用程序预启动”功能的情况下，可能会在用户设备上临时显示一个黑色窗口。当在不启动应用程序的情况下启动 Citrix Receiver 时，可能会出现此问题。

[#LC4280]

- Citrix 策略“拖动时查看窗口内容”无法在已发布的桌面上正常工作。当您登录到 VDA 时，窗口内容会正确显示。但是，在重新连接已断开的会话后，将不再显示窗口内容。

[#LC4301]

- 如果满足所有三个下列条件，则 Citrix Receiver for Chrome 和 VDA 之间的 TLS 连接会失败：

- 已在 VDA 上安装修复程序 #LC2179 (修补程序 ICATS760WX64032 或其替代项)
- 连接已配置为使用 SSL
- Citrix Gateway Protocol (CGP) 已禁用

[#LC4405]

- 在 VDA 7.6.300 会话中启动应用程序时，在应用程序启动之前，会显示含以下消息的进度条几分钟：“Please wait for Local Session Manager” (请等待 Local Session Manager)。在此期间，应用程序看上去无响应，即使它已正确启动也是如此。

[#LC4406]

- 用户会话中的某些应用程序可能默认使用不正确的输入法。可通过在各控制面板中清除“允许我为每个应用窗口设置不同的输入法”复选框来更正此行为。但是，当您重新连接到会话时，设置会恢复为错误的默认设置。

要使设置不恢复，请设置以下注册表项：

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix

名称 : ClientDataOption

类型 : DWORD

数据 : 2 (可以更改输入方法设置)

[#LC4416]

- 当通过 NetScaler Gateway 连接时 , SmartAccess Control 过滤器可能无法正确应用。

[来自 ServerVDACoreWX64\_7\_6\_307][#LC4503]

- 已发布的应用程序路径中的非 ASCII 字符导致应用程序无法启动。

[#LC4595]

- 在启用“客户端自动重新连接”策略的情况下 , 重新连接到会话的尝试可间歇性地失败 , 并导致 VDA 重新注册。将出现以下警告消息 :

“Event 1048, Citrix Desktop Service (Warning)

The Citrix Desktop Service is re-registering with the DDC: "NotificationManager:NotificationServiceThread: WCF failure or rejection by broker (*DDC NAME>*)" (事件 1048 , Citrix Desktop Service (警告) Citrix Desktop Service 正在重新注册 , DDC : “NotificationManager:NotificationServiceThread: WCF 发生故障或被 Broker 拒绝 ()”)

[#LC4767]

## 智能卡

- 在 Microsoft Internet Explorer 中 , 某些 Web 站点的智能卡登录用户界面可能间歇性不可用。

[#LC3988]

## 系统异常

- 操作系统中的 picadm.sys 出现错误 , 并显示蓝屏和停止代码 0x20。

[#LC3473]

- 操作系统中的 picadm.sys 出现错误 , 并显示蓝屏和停止代码 0x00000050。

[#LC3921]

- 在将 VDA for Desktop OS 或 Server OS 升级到 7.6.300 版后 , Citrix Print Manager Service (CpSvc.exe) 可能会在注销时意外退出。

[来自 ServerVDACoreWX64\_7\_6\_304][#LC4102]

- 在终端服务 (TermService) 中注册的服务主机 (svchost.exe) 进程可能会意外退出。

[#LC4150]

- 操作系统中的 picadm.sys 出现错误 , 并显示蓝屏和停止代码 0x000000C1。

[#LC4334]

- 当您在 Windows Media Player 上重复播放 .avi 文件时，wfica32.exe 进程消耗的内存可能会持续增加，直到此进程意外退出。

[#LC4335]

- 在从 Citrix Receiver 会话注销时，VDA 可能在 picadd.sys 中遇到严重异常，并显示蓝屏。

[#LC4360]

- VDA 可能在 ctxdvcs.sys 中的错误检测代码 0x00000044 处遇到严重异常，并显示蓝屏。

[#LC4505]

- 如果已定义注册表项 HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ICA\Thinwire\DisableOssForProcesses，则在尝试重新启动 VDA 和启动已发布的桌面时可导致蓝屏。

[#LC4597]

## 用户体验

- 当尝试在无缝的双显示器会话中移动 Microsoft Excel 窗口时，该窗口可能会在重绘新位置时发生延迟。

[#LC4441]

## 虚拟桌面组件 - 其他

- 在升级到 App-V 5.0 Service Pack 3 后，通过 Citrix Receiver 启动 App-V 应用程序的尝试可能会失败。

[#LC1762]

- 每次启动 Citrix Monitor Service 时，应用程序日志中可能会错误地记录以下错误消息，即使此服务运行正常也是如此：

“Error querying the Broker via GetBrokerObjects to obtain 'Controller Machine Details'”（通过 GetBrokerObjects 查询 Broker 以获取“Controller 计算机详细信息”时出错）。

[#LC2239]

- 尝试注册设为土耳其语系统区域设置的 VDA 时可能会失败，并生成 1048 错误。

[#LC2704]

- 如果站点数据存储不可用，则即使控制器处于租用连接模式，尝试重新连接时也可能失败。

[来自 BrokerAgentWX86\_7\_6\_301、BrokerAgentWX64\_7\_6\_301][#LC4077]

- 对于使用非永久配置文件的用户来说，在安装了 PowerShell 3.0 或更高版本的计算机上可能需要很长时间才能启动已发布的 App-V 应用程序。

[#LC4147]

- 尝试从 Citrix Director 终止用户会话中运行的进程时，可能显示以下错误信息：

“操作失败。数据源未响应或报告了一个错误。请查看服务器事件日志了解更多信息。”

[#LC4384]

- 如果已配置的工作目录不存在，则采用了 App-V 集成的应用程序可能无法启动。

[#LC4839]

# 自 XenApp 和 XenDesktop 7.6 起已修复的问题

Aug 19, 2016

XenApp/XenDesktop 7.6 LTSR 累积更新 1 解决了自 XenApp 和 XenDesktop 7.6 版本发布以来报告的下列问题。

有关自 7.6 LTSR 版本发布以来已修复的所有问题的列表，请参阅[自 7.6 LTSR 起已修复的问题](#)。

## Citrix Director

- Director 中的用户名搜索操作可能会遇到最多两分钟的随机延迟。

[#LC1250]

- 当尝试将大量数据导出为 PDF 格式时，服务器的 CPU 和内存消耗可达 100%，并出现以下错误消息：

“操作失败。数据源未响应或报告了一个错误。请查看服务器事件日志了解更多信息。”

此修复程序引入了针对 PDF 导出操作的一个可配置的限值，由此，至少可以获得报告的一部分。

安装此修复程序后，必须按如下所示在 wwwroot\Director 文件夹中配置 web.config 文件：

向“appSettings”部分中添加以下行：

该限值取决于服务器的功能（如内存大小），其值指定了 PDF 报告中的行数。

[#LC4108]

- 以任何文件格式导出报告的尝试可能会失败，并出现以下错误消息：

“操作失败。意外的服务器错误。请查看服务器事件日志了解更多信息。”

[#LC4281]

- 如果 XenApp 服务器具有两个 IP 地址且 DNS 服务器无法解析第一个 IP 地址，则管理员可能无法登录到 Citrix Director，并出现以下错误消息：

“系统当前不可用。请稍后重试或联系管理员。”

[#LC4411]

- 尝试以 CSV 格式导出大量数据时，可能会超时，并且导出操作可能会失败，并出现以下错误消息：

“操作失败。数据源未响应或报告了一个错误。请查看 Director 服务器事件日志了解更多信息。”

此修复程序允许您配置针对数据导出操作的超时值。

安装此修复程序后，必须按如下所示配置 wwwroot\Director 文件夹中的 web.config 文件：

向“appSettings”部分添加以下行：

<add key="ConnectorDataServiceContext.Timeout" value="3600" />，其中 value 指定超时时间（秒）。

[#LC4467]

- 如果选择一个用户以显示该用户的会话详细信息，可导致该用户的名称在左上角显示为“NULL”。  
[#LC4589]
- 如果 NetBios 域名中包含 & 符号，则可能无法从 Citrix Director 控制台执行重影操作。这是因为 & 符号字符是 XML 中的保留字符，并可能导致针对当前登录的解析操作失败。  
[#LC4633]

## Citrix 策略

- 如果关闭 Desktop Studio 时未在导航窗格中选择“控制台根节点”，Microsoft 管理控制台 (MMC) 会失败。  
[#LC1314]
- Citrix 策略引擎可能导致服务器无响应。如果发生此问题，Citrix Receiver 和 RDP 的连接请求将失败。  
[#LC1817]
- 借助此增强功能，通过 Citrix“组策略建模”向导创建的建模报告将出现在 Citrix Studio 的中间窗格中。  
[#LC2189]
- 在 Citrix Studio 中添加或创建 Citrix 管理员时，如果使用的用户或组的名称中包含下划线，如 get\dl\_lab\_group，第一个下划线不显示在管理员列表的详细信息中。此名称将显示为 dllab\_group。  
[#LC2284]
- 以域用户身份在 AppCenter 的策略节点上运行组策略建模向导时，可能无法显示所应用的用户和计算机策略。  
[#LC3284]
- Citrix Director 管理员可能无法在会话详细信息中查看 Citrix 策略。  
[#LC3941]
- 尝试在“打印机分配”窗口下向一组用户设备添加多个会话打印机时，无法展开并显示滚动条。由此，向一组用户设备添加多个会话打印机的尝试可能会失败。  
[#LC4658]

## Citrix Studio

- 在 Desktop Studio 中单击计算机目录时，可能需要很长时间才会显示目录。此外，托管信息也需要很长时间才能显示。  
[#LC0237]
- 此修复解决了一个安全漏洞。有关详细信息，请参阅知识中心文章 [CTX213045](#)。

注意：为了能够完成此修复，必须使用 7.6 LTSR 累积更新 1 更新 Citrix Studio 和 Controller 组件。

[#LC0559]

- Citrix Studio 可能无法识别 Citrix 服务提供商许可证并显示以下错误消息：

“找不到有效的许可证”

[#LC0813]

- 利用此增强功能，从 Active Directory (AD) 域中的多个站点添加用户时，Citrix Studio 显示正确的用户分配数据。

[#LC0889]

- 该修复程序解决了一个问题，此问题导致无法将成员（如果其与 Citrix Studio 不属于同一个域）添加到交付组。

[#LC0955]

- 如果关闭 Desktop Studio 时未在导航窗格中选择“控制台根节点”，Microsoft 管理控制台 (MMC) 会失败。

[#LC1314]

- 如果在“应用程序”窗口中更改应用程序的属性，交付组的优先级可能会变为零。

[#LC1489]

- 更改 Web Interface 端口号后，Desktop Studio 可能错误地打开许可证升级提示。

[#LC1575]

- 在未配置许可的情况下，尝试使用 XenDesktop 高级 Powershell SDK 命令“New-XDSite”配置新站点，然后尝试运行命令“Get-XDSite”失败。显示错误消息“The site has upgrade steps remaining. Run Get-XDUpgradeStatus to find out the remaining steps”（站点有未执行的升级步骤。请运行 Get-XDUpgradeStatus 以了解剩余步骤）。

[#LC1612]

- 使用 App-V 集成的应用程序可能无法使用正确的工作目录。

[#LC1623]

- 如果用户在 Citrix Studio 中配置预启动和延迟会话，“MaxTimeBeforeDisconnect”属性将设置为零分钟，而不是默认值 15 分钟。

[#LC1706]

- 在升级到 App-V 5.0 Service Pack 3 后，通过 Citrix Receiver 启动 App-V 应用程序的尝试可能会失败。

[#LC1762]

- 升级到 XenDesktop 7.6 之后，Desktop Studio 可能需要三分钟或四分钟才能显示目录或托管信息。

[#LC1851]

- Delivery Controller 脱机或以其他方式变为不可用时，Citrix Studio 可能运行缓慢。

[#LC1891]

- 尝试运行“创建目录”向导可能会失败。当其中一个已连接虚拟机管理程序处于维护模式时会出现此问题。

[#LC1916]

- 在 Citrix Studio 中运行保存时带有“为空”运算符的查询时，此运算符被替换为默认运算符。

[#LC1940]

- 尝试将站点自动从 XenDesktop 7.5 升级到 XenDesktop 7.6 可能会由于检查时没有在新实例和已有实例之间正确地比较 Broker Service 中的“绑定”属性而失败。这可能会导致出现“service instance already registered”（服务实例已注册）错误。尝试在未取消注册现有端点的情况下注册服务端点时会出现此问题。

[#LC2043]

- 将 XenDesktop 从版本 5.x 或 7.x 成功升级到版本 7.6 之后，启动 Studio 时可能会出现以下错误消息：

“升级其余的 Delivery Controller”。

此错误消息的详细信息指出许可证服务器名称，尽管 Delivery Controller 并未安装在许可证服务器上。

[#LC2044]

- 尝试将站点升级到最新的产品版本可能失败。当“Set-ConfigSite”命令无法获取升级后的newValue 时，会出现此问题。

[#LC2047]

- 在 Citrix Studio 中添加或创建 Citrix 管理员时，如果使用的用户或组的名称中包含下划线，如 get\dl\_lab\_group，第一个下划线不显示在管理员列表的详细信息中。此名称将显示为 dllab\_group。

[#LC2284]

- 在交付组中，尝试创建包含“Applications”（应用程序）一词的应用程序文件夹会阻止创建子文件夹。

[#LC2349]

- 您将具有相同专享升级服务过期日期的 XenApp 和 XenDesktop 许可证合并为一个许可证文件时，Studio 中显示的许可证信息中可能会缺失某些 XenApp 许可证。

注意：为了能够完成此修复，必须使用 7.6 LTSR 累积更新 1 更新 Citrix Studio 和 Controller 组件。

[#LC2350]

- 此项修复解决了运行 App-V 应用程序发现时 Citrix Studio 出现内存泄漏的问题。

[#LC2559]

- 为管理员创建自定义角色时，创建角色后会显示以下错误消息“The Given key was not present in the dictionary”（给定的键在字典中不存在）。此外，使用管理员帐户首次启动 Desktop Studio 时，也会显示相同的错误消息。

[#LC2680]

- 如果数据库所有者是 Active Directory 中的组，尝试从站点删除 XenDesktop 控制器可能会失败。

[#LC2912]

- 安装修补程序 DStudio760WX86001 后，尝试限制某些应用程序对用户的可见性时，可能会显示“访问被拒绝”错误。

此问题仅存在于域之间具有单向信任关系的环境中。

[#LC2956]

- 使用命令或在 Studio 中尝试更新具有多个桌面的交付组失败，并显示以下错误消息：

- Object reference not set to an instance of an object.
- Error Id: XDDS:0E01FE12 (对象引用未设置为对象的实例。错误 ID: XDDS:0E01FE12)

[#LC2958]

- 当使用 Machine Creation Service 为 VDA for Server OS 编制目录时，个人虚拟磁盘存储的不可用性可能会错误地将目录的“CleanOnBoot”属性设置为“False”。因此，目录可能无法更新。

[#LC2959]

- 当两个应用程序具有相同的 ApplicationID 时，如果刷新 App-V 应用程序，可能导致 Citrix Studio 错误地设置 App-V 包名称。

**注意**：为了能够完成此修复，必须使用 7.6 LTSR 累积更新 1 更新 Citrix Studio 和 Controller 组件。

[#LC2969]

- 在“编辑交付组”中的“计算机分配”页面上编辑“用户”部分后，现有用户设置被删除。此问题出现在手动添加用户时或从 Microsoft Excel CSV 文件导入用户列表时。

[#LC3267]

- 利用此增强功能，“托管服务器名称”字段在 Desktop Studio 的“桌面操作系统计算机”和“服务器操作系统计算机”的“搜索”视图中可用。

[#LC3343]

- 关闭 PowerShell 资源时，Citrix Studio 可能无响应。

[#LC3612]

- 在 Citrix Studio 中为交付组下的多个文件夹创建多个应用程序可能会导致很大的文件夹结构。当您首次打开 Citrix Studio 并单击文件夹或应用程序时，可能会拖动而不是选中文件夹或应用程序。这会移动选定对象，并使文件夹或应用程序的结构发生变化。

[#LC3705]

- Add-XDController cmdlet 不向 Controller 分配完全自定义数据库连接字符串。

**注意**：为了能够完成此修复，必须使用 7.6 LTSR 累积更新 1 更新 Citrix Studio 和 Controller 组件。

[#LC3860]

- 如果不属于数据库管理员用户组的用户打开 Citrix Studio，可能会导致 SQL Server 发生权限错误。

**注意**：为了能够完成此修复，必须使用 7.6 LTSR 累积更新 1 更新 Citrix Studio 和 Controller 组件。

[#LC4127]

- 如果某个服务项目包含两个或更多的租户，则在尝试通过 App Orchestration 2.6 为该服务项目预配更多资源时，可能会失

败。

**注意**：为了能够完成此修复，必须使用 7.6 LTSR 累积更新 1 更新 Citrix Studio 和 Controller 组件。

[#LC4170]

- 当多个 Citrix Studio 会话打开时，在一个会话上执行的策略更改可能会丢失并被其他会话上执行的策略更改覆盖。

**注意**：为了能够完成此修复，必须使用 7.6 LTSR 累积更新 1 更新 Citrix Studio 和 Controller 组件。

[#LC4487]

## Controller

- 在 Desktop Studio 中单击计算机目录时，可能需要很长时间才会显示目录。此外，托管信息也需要很长时间才能显示。

[#LC0237]

- 用户更新目录时，配置日志记录报告“更新计算机目录”成功，但是“任务详细信息”视图中的其中一项任务显示消息“发布预配方案”失败。

[#LC0518]

- 此修复解决了一个安全漏洞。有关详细信息，请参阅知识中心文章 [CTX213045](#)。

**注意**：为了能够完成此修复，必须使用 7.6 LTSR 累积更新 1 更新 Citrix Studio 和 Controller 组件。

[#LC0559]

- 利用此增强功能，从 Active Directory (AD) 域中的多个站点添加用户时，Citrix Studio 显示正确的用户分配数据。

[#LC0889]

- 如果 XenServer 参数“TimeOffset”存在于主映像虚拟机 (VM) 上，创建 Machine Creation Services (MCS) 目录失败。要检查是否存在此参数，请在 XenServer 控制台上运行命令“xe vm-list uuid= params=other-config”。要解决此问题，请应用此修补程序，或通过运行 XenServer 命令“xe vm-param-remove uuid= param-name=other-config param-key=timeoffset”手动删除该参数。

[#LC1071]

- Monitoring Service 在 7 天而非默认的 90 天后，过早删除应用程序实例历史记录。此问题出现在具有 Platinum Edition 许可的 XenDesktop 和 XenApp 部署中。

[#LC1129]

- 在 Desktop Director 中的“趋势 > 托管应用程序使用情况”选项卡上，各应用程序的总数不等于所有应用程序的总和。此问题出现在运行七天或更长时间的环境中。

[#LC1130]

- 如果通过使用 Machine Creation Services 的 Desktop Studio 创建虚拟机 (VM)，并且 VM 托管在 VMware 虚拟机管理程序上，尝试更新属于计算机目录的虚拟机会失败。出现此问题时，计算机创建日志中会显示错误消息，表示虚拟磁盘不存在，

但数据存储中的目录存在。

[#LC1201]

- 在某些 Amazon Web Services 环境中，使用 Machine Creation Services (MCS) 预配桌面可能会失败并显示错误“No facility for disk upload”（没有用于磁盘上载的设备），即使环境配置正确也是如此。

[#LC1295]

- 使用 Machine Creation Service 预配 VDA 时，VDA 的主 DNS 后缀改变。

[#LC1300]

- 如果关闭 Desktop Studio 时未在导航窗格中选择“控制台根节点”，Microsoft 管理控制台 (MMC) 会失败。

[#LC1314]

- 事件日志中记录了事件 ID 3012 的两个或更多个实例时，事件 ID 3020 和 3021 也出现在日志中，并且消息不正确。应用此修复后，如果记录了事件 ID 3012 的两个或更多个实例，事件 ID 3010 和 3011 正确显示在日志中。

[#LC1425]

- 在事件日志中，事件 ID 1110 和 1111 的错误消息不正确。应用此修复后，事件日志中会显示以下正确消息：

- EventID:1110: 为避免事件日志记录过量，此服务将暂时阻止相关消息(事件 ID: 1100-1109、1112-1116)。
- EventID:1111: 此服务不再阻止相关消息(事件 ID: 1100-1109、1112-1116)。

[#LC1485]

- 如果共享交付组中的某个 VDA 带有标记并且标记用作策略过滤器的一部分，这些策略将不会应用于交付组中的其他 VDA。

[#LC1506]

- 更改 Web Interface 端口号后，Desktop Studio 可能错误地打开许可证升级提示。

[#LC1575]

- 升级到 XenDesktop 7.6 后，如果主 VM 映像包含在 VMware vSphere 5.1 上启用的嵌套式硬件虚拟化属性，创建新目录会失败。

[#LC1586]

- 在未配置许可的情况下，尝试使用 XenDesktop 高级 Powershell SDK 命令“New-XDSite”配置新站点，然后尝试运行命令“Get-XDSite”失败。显示错误消息“The site has upgrade steps remaining. Run Get-XDUpgradeStatus to find out the remaining steps”（站点有未执行的升级步骤。请运行 Get-XDUpgradeStatus 以了解剩余步骤）。

[#LC1612]

- 如果 NetBios 域名包含 & 符号，尝试启动 Citrix Studio 失败并显示代码为 XDD5:72182E6B 的错误“您无权执行此操作”。

[#LC1646]

- 如果用户在 Citrix Studio 中配置预启动和延迟会话，“MaxTimeBeforeDisconnect”属性将设置为零分钟，而不是默认值 15 分钟。

[#LC1706]

- 在含 System Center Virtual Machine Manager 的 Hyper-V 环境中，BrokerService.exe 进程可消耗 100% 的系统内存，导致虚拟桌面无法成功地代理。

[#LC1730]

- 升级到 XenDesktop 7.6 之后，Desktop Studio 可能需要三分钟或四分钟才能显示目录或托管信息。

[#LC1851]

- Delivery Controller 脱机或以其他方式变为不可用时，Citrix Studio 可能运行缓慢。

[#LC1891]

- 尝试运行“创建目录”向导可能会失败。当其中一个已连接虚拟机管理程序处于维护模式时会出现此问题。

[#LC1916]

- 在某些 Active Directory 组织单位 (OU) 中，如果 OU 名称中包含特殊字符，XenDesktop 的核心服务（如 AD Identity Service 或 Broker Service）可能无法绑定到 OU。这可能会导致 CPU 使用率高于正常水平。此外，服务可能会意外关闭，可能导致 Citrix Studio 无法访问。

[#LC1979]

- 在对已发布的应用程序使用通过关键字执行的过滤时，工作区控制功能可能无法正常工作。

[#LC2025]

- Desktop Director 中的“趋势”页面和“过滤器选项”页面中的选项卡可能无法显示数据并显示错误消息。

[#LC2035]

- 尝试将站点自动从 XenDesktop 7.5 升级到 XenDesktop 7.6 可能会由于检查时没有在新实例和已有实例之间正确地比较 Broker Service 中的“绑定”属性而失败。这可能会导致出现“service instance already registered”（服务实例已注册）错误。尝试在未取消注册现有端点的情况下注册服务端点时会出现此问题。

[#LC2043]

- 将 XenDesktop 从版本 5.x 或 7.x 成功升级到版本 7.6 之后，启动 Studio 时可能会出现以下错误消息：  
“升级其余的 Delivery Controller”。

此错误消息的详细信息指出许可证服务器名称，尽管 Delivery Controller 并未安装在许可证服务器上。

[#LC2044]

- 尝试将站点升级到最新的产品版本可能失败。当“Set-ConfigSite”命令无法获取升级后的newValue 时，会出现此问题。

[#LC2047]

- 本版本向 `Set-XDLogging -AdminAddress $ControllerName -AllowDisconnectedDatabase $true` 命令中添加了 `-enabled` 标志。

[#LC2162]

- 在 Powershell 管理单元中，运行命令 Get-Help set-MonitorConfiguration -detailed 返回错误消息 - "GroomApplicationInstanceRetentionDays FIXME"。

[#LC2176]
  - 每次启动 Citrix Monitor Service 时，应用程序日志中可能会错误地记录以下错误消息，即使此服务运行正常也是如此：“Error querying the Broker via GetBrokerObjects to obtain 'Controller Machine Details'”（通过 GetBrokerObjects 查询 Broker 以获取“Controller 计算机详细信息”时出错）。

[#LC2239]
  - 如果委派管理员帐户启用了用户访问控制，Delivery Controller 的更新错误地安装到默认位置。默认位置为“%systemroot%\Program Files\Citrix”，此位置可能与最初安装 Delivery Controller 的位置不同。

[#LC2252]
  - 在 Citrix Studio 中添加或创建 Citrix 管理员时，如果使用的用户或组的名称中包含下划线，如 get\dl\_lab\_group，第一个下划线不显示在管理员列表的详细信息中。此名称将显示为 dllab\_group。

[#LC2284]
  - 如果在具有 GRID 板的 VMware vSphere 6 中的 VM 主映像中启用虚拟图形处理器 (VGPU)，计算机创建过程会失败。

[#LC2326]
  - 您将具有相同专享升级服务过期日期的 XenApp 和 XenDesktop 许可证合并为一个许可证文件时，Studio 中显示的许可证信息中可能会缺失某些 XenApp 许可证。
- 注意：为了能够完成此修复，必须使用 7.6 LTSR 累积更新 1 更新 Citrix Studio 和 Controller 组件。
- [#LC2350]
- 用户从会话注销时，数据库中的“结束日期”更新错误，包括在会话内运行的所有应用程序实例和在会话结束前已经关闭的应用程序。
- [#LC2435]
- 为管理员创建自定义角色时，创建角色后会显示以下错误消息“The Given key was not present in the dictionary”（给定的键在字典中不存在）。此外，使用管理员帐户首次启动 Desktop Studio 时，也会显示相同的错误消息。
- [#LC2680]
- 通过集成 Hyper-V 预配的 VDA 在成功订阅后显示为已取消注册。
- [#LC2722]
- 将 Desktop Controller 从 7.x 版升级到 7.6 版以后，如果运行 PowerShell 命令“Set-MonitorConfiguration”，则会显示以下错误消息：“A database operation failed and cannot be recovered.”（数据库操作失败且无法恢复。）
- [#LC2745]
- 尝试向单个目录添加超过 999 个虚拟机 (VM) 可能会失败。

[#LC2873]

- 包含后导空格的已发布应用程序名称会导致多个问题。从已截断包含后导空格名称的已发布应用程序名称生成浏览器名称时会出现这些问题。

[#LC2897]

- 如果数据库所有者是 Active Directory 中的组，尝试从站点删除 XenDesktop 控制器可能会失败。

[#LC2912]

- 安装修补程序 DSstudio760WX86001 后，尝试限制某些应用程序对用户的可见性时，可能会显示“访问被拒绝”错误。

此问题仅存在于域之间具有单向信任关系的环境中。

[#LC2956]

- 使用命令或在 Studio 中尝试更新具有多个桌面的交付组失败，并显示以下错误消息：

- Object reference not set to an instance of an object.
- Error Id: XDDS:0E01FE12 (对象引用未设置为对象的实例。错误 ID: XDDS:0E01FE12)

[#LC2958]

- 当两个应用程序具有相同的 ApplicationID 时，如果刷新 App-V 应用程序，可能导致 Citrix Studio 错误地设置 App-V 包名称。

注意：为了能够完成此修复，必须使用 7.6 LTSR 累积更新 1 更新 Citrix Studio 和 Controller 组件。

[#LC2969]

- 应用此修复可以解决以下问题：

- 在配置与 US-East-1e 区域的主机连接后，可以建立 Amazon Web Services (AWS) 连接，但可能无法创建计算机。
- 尝试添加 AWS 主机连接以使用 EU-Central-1 时，主机连接创建可能会失败，同时生成身份验证错误。

[#LC3239]

- Machine Creation Services (MCS) 可能不支持 System Center Virtual Machine Manager (SCVMM) 2012 主机上的“AvailableForPlacement”标志。结果导致，如果选择的主机包含的资源不足，计算机创建操作可能会失败。

[#LC3426]

- 执行 Set-BrokerDBConnection 以及相关命令时，Citrix Studio 中的相关配置日志记录条目会列出相应的“主要任务”，并且其状态为“正在进行”，任务完成后，此状态不会更新。

[#LC3479]

- 使用本地系统帐户（通常由 SCCM 等电子软件分发使用）执行到 XenDesktop 7.6 的升级后，Analytics Service 可能无法启动。

[#LC3493]

- 对已连接到 VMware Vsphere 虚拟机管理程序的 VDA 执行计划的重新启动时，可能会导致服务器关闭并处于断电状态。

- 要启用此修复，请设置以下注册表项：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\DesktopServer\RebootSchedule

名称：ShutdownTimeoutRecovery

类型：DWORD

值：1

- 要禁用此修复，请设置以下注册表项：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\DesktopServer\RebootSchedule

名称：ShutdownTimeoutRecovery

类型：DWORD

值：0

在设置值后，必须重新启动 Broker Service。

[#LC3807]

- 在安装适用于 System Center Virtual Machine Manager (SCVMM) 的 Hotfix Rollup Pack 7 后，可能无法通过 Machine Creation Services (MCS) 创建目录。

[#LC3822]

- Add-XDController cmdlet 不向 Controller 分配完全自定义数据库连接字符串。

注意：为了能够完成此修复，必须使用 7.6 LTSR 累积更新 1 更新 Citrix Studio 和 Controller 组件。

[#LC3860]

- 如果不属于数据库管理员用户组的用户打开 Citrix Studio，可能会导致 SQL Server 发生权限错误。

注意：为了能够完成此修复，必须使用 7.6 LTSR 累积更新 1 更新 Citrix Studio 和 Controller 组件。

[#LC4127]

- 如果某个服务项目包含两个或更多的租户，则在尝试通过 App Orchestration 2.6 为该服务项目预配更多资源时，可能会失败。

注意：为了能够完成此修复，必须使用 7.6 LTSR 累积更新 1 更新 Citrix Studio 和 Controller 组件。

[#LC4170]

- 当在控制器上启用“SupportMultipleForest”设置以允许 NTLM 身份验证时，Linux VDA 可能无法完成注册过程，因为可能无法在 Windows Communication Foundation (WCF) 的 EndpointReference 中设置其服务主体名称 (SPN)。

[#LC4235]

- 如果创建由 VMware 虚拟机管理程序托管的虚拟机 (VM)，则在首次尝试从 Citrix Studio 更新或删除这些虚拟机时，操作可能会失败，并显示“错误 ID XDDDS:B125B84A”，但后续尝试将成功。

[#LC4436]

- 当多个 Citrix Studio 会话打开时，在一个会话上执行的策略更改可能会丢失并被其他会话上执行的策略更改覆盖。

注意：为了能够完成此修复，必须使用 7.6 LTSR 累积更新 1 更新 Citrix Studio 和 Controller 组件。

[#LC4487]

- 当为其中包括用于从/自夏令时切换的开关的日期范围运行 PowerShell 命令“Get-LogSummary”时，将出现以下错误消息：“已添加具有相同键的项”。

当夏令时导致模糊的当地日期或时间时会出现问题。因此，会在 HashMap 中创建重复的条目，并发生异常。

此修复程序引入了一条消息，用于通知用户分别为夏令时的开始或结束时间点将时间跨度拆分到帐户。

[#LC4612]

- 在 Amazon Web Services (AWS) 环境中更新机目录的操作可间歇性失败。要启用此修复程序，必须为将在计算机目录更新期间跳过的映像准备阶段运行命令“Set-ProvServiceConfigurationData –Name ImageManagementPrep\_DoImagePreparation –Value \$false”。

[#LC4709]

- 当存在大量正在运行的应用程序和 VDA 进程时，控制器偶尔会断开与数据库的连接。当发生这种情况时，VDA 保持处于初始化状态，并且应用程序不可用。

[#LC4848]

- 当存在过多的虚拟机管理程序警报时，SQL 数据库服务器的 CPU 使用率可达到 100%。

[#LC5277]

- 在高使用率情况下（超过 5,000 个用户并发地在许多 VDA for Server OS 上启动许多应用程序），SQL 数据库服务器的 CPU 使用率可达到 100%，从而导致中断且应用程序无法启动。

[#LC5315]

## HDX MediaStream Flash 重定向

- 如果启用了 HDX MediaStream Flash 重定向，在 Internet Explorer 中打开和关闭多个含 Flash 内容的选项卡会导致 Internet Explorer 意外退出。

[#LC0375]

- 在启用了 HDX MediaStream for Flash 的情况下，在 Internet Explorer 中打开和关闭多个选项卡会导致 Internet Explorer 意外关闭。

[#LC1141]

- 在启用 HDX MediaStream for Flash 重定向的情况下浏览 Web 站点时，如果 HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\AppInit\_DLLs 注册表值设置为“mfaphook.dll”或“mfaphook64.dll”而非“mfaphook.dll”或“mfaphook64.dll”的完整路径，则 Flash 重定向功能会失败。

[#LC4388]

## 安装程序

- 如果从命令行安装 VDA 7.6.300，/noreboot 开关（具体取决于此开关在开关字符串中的位置）不会被接受。因此，VDA 将在安装完成后重新启动。

[#LC4046]

- 安装 VDA 时，可能会安装用于提高性能的某些注册表项，即使您在安装过程中禁用了“优化性能”选项也是如此。

[#LC4330]

## 许可

- 在设置为法语系统区域设置的许可证服务器上，Citrix Studio 以西班牙语显示许可模式。

[#LC3450]

## Provisioning Services

控制台

目标

服务器

### 控制台

- 创建 XenServer 虚拟机时，XenDesktop 设置向导设置了一个无效的“默认”代 ID。

[#LA5924]

- 完成 XenDesktop 向导后，Studio 中的计算机目录将为空，并错误地显示流 IP 地址，而非显示管理 IP 地址。要使用管理 IP 地址，请设置以下注册表项：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ProvisioningServices

名称：UseManagementIpInCatalog

类型：DWORD

值：1

[#LC0125]

- 运行“流 VM 设置向导”以向设备集合中添加 VM 时，如果托管项使用不同的案例格式，则会显示以下错误消息：

为避免创建重复键，取消了添加或设置命令

详细信息:-

不能在具有唯一索引“IDX\_VirtualHostingPoolSiteIdName”的对象“dbo.VirtualHostingPool”中插入重复键的行。重复键值为 (18df503c-c745-452a-89aa-3bbf431c7b33, livsvm01.livdc.local)。

语句已终止。

[#LC0348]

- 创建目标时，XenDesktop 设置向导不使用模板启动属性。要修复此问题，请创建以下注册表项：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ProvisioningServices

名称 : UseTemplateBootOrder

类型 : REG\_DWORD

数据 : 1

[#LC0382]

- 运行“流 VM 设置向导”时，如果 OU 名称包含特殊字符，某些 Active Directory 组织单位 (OU) 可能不在向导中显示。

[#LC0393]

- 尝试使用 MCLI.exe 或命令“mcli-runwithreturn mapdisk -p disklocatorName=MyDiskLocatorName, sitename=MySiteName, storeName=MyStoreName”在 Provisioning Services 服务器上映射磁盘失败，并显示以下错误消息：

Object Reference not set to an instance of an object (对象引用未设置为对象的实例) (MCLI 命令)

尝试运行命令“mcli-run unmapdisk”失败，并显示错误消息“发生意外的 MAPI 错误”。

[#LC0786]

- 尝试使用 XenDesktop 设置向导创建计算机时，硬盘驱动器和虚拟 DVD 驱动器将被放置在不同的存储卷中，即使托管单元只能访问一个卷也是如此。

[#LC0918]

- 如果 Desktop Delivery Controller 的统一资源标识符 (URI) 中包含端口号，则当 XenDesktop 设置向导运行时，Microsoft 管理控制台 (MMC) 将停止响应。

[#LC1248]

- 其中一个群集共享卷不包含 StorageDisk 位置时，XenDesktop 设置向导将失败。

[#LC1807]

- 安装 Provisioning Services 控制台 7.1.3 后，Windows Server 2008 R2 和 Windows 7 上多个 .NET 应用程序无法启动。

[#LC1838]

- 在某些环境中，使用 Provisioning Services 7.x 引导程序文件时，需要很长时间才能同时启动多个目标设备。

注意：不存在高负载的情况下，也会出现此问题。

[#LC1839]

- 如果用于登录 Provisioning Services 控制台的帐户与用于安装 Provisioning Services 的帐户不同，运行 XenDesktop 设置向导将失败并显示以下错误消息：

无法连接 XenDesktop 控制器: <地址>。无法转换部分或全部身份引用。

[#LC1952]

- 在 Microsoft SCVMM 环境中，当模板中的 MAC 地址类型为静态时，XenDesktop 设置向导不向非流网络适配器分配静态 MAC 地址。

[#LC2459]

- 运行 XenDesktop 设置向导时，如果标准存储和 PvD 存储的数量不相等，则不创建所有虚拟机。

[#LC2496]

- XenDesktop 设置向导在一个存储中创建 ESX 虚拟机元数据，而非通过为虚拟机创建的不同磁盘来分发元数据。

[#LC2549]

- 在 XenServer 中使用 XenDesktop 设置向导创建虚拟机时，可能不保留分配有 GPU 的模板设置。

[#LC2859]

- 通过 XenDesktop 设置向导创建的计算机不添加到 XenDesktop 计算机目录中，并显示以下错误消息：

没有与提供的模式匹配的项

[#LC2923]

- VMware ESX 主机处于维护模式时，XenDesktop 设置向导可能无法创建计算机。

[#LC3401]

- XenDesktop 设置向导可能不在托管单元的 Personal vDisk 存储上使用“被取代”标志。

[#LC3573]

- “流 VM 设置向导”运行过程中，枚举包含多个主机的数据存储的 VMware ESX 群集上的模板需要很长时间才能完成。

[#LC3674]

- 装载和卸载虚拟磁盘时，SOAP Service 可能无响应，并且 Provisioning Services 控制台可能无法启动。

[#LC3723]

- 使用流 VM 设置向导创建计算机时会显示以下错误消息：

对象引用未设置为某个对象的实例。

[#LC3811]

- 技术支持管理员通过 XenDesktop 设置向导从独立的 Provisioning Services 控制台创建新虚拟机 (VM) 时，尝试从 BDM 分区启动目标设备失败，并导致登录服务器显示错误的 IP 地址。

[#LC3911]

- 安装 Provisioning Services 控制台会将以下注册表项设置为 1。这会导致其他 .NET 应用程序尝试使用版本不正确的 Framework，因此可能会失败：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\.NETFramework

名称：OnlyUseLatestCLR

类型：REG\_DWORD

数据：1

[#LC4197]

- 在 Microsoft System Center Virtual Machine Manager (SCVMM) 环境中，尝试使用 XenDesktop 设置向导或流 VM 设置向导创建虚拟机 (VM) 可能会失败。应用此修复后，将在命令中使用主机的完全限定域名 (FQDN) 而非短名称。

[#LC4230]

- 在 System Center Virtual Machine Manager (SCVMM) 2012 环境中，XenDesktop 设置向导可能无法创建 Provisioning Services 目标设备。

[#LC4256]

- 如果用户 1 和用户 2 配置为使用不同的端口，尝试使用流 VM 设置向导或 XenDesktop 设置向导连接到 VMware Vsphere Hypervisor 5.1 将失败。

要使用不同的端口连接到 VMware ESX 服务器，必须创建以下注册表项：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ProvisioningServices\PlatformEsx

名称：Port

类型：DWORD

值：

[#LC4283]

- XenDesktop 设置向导与 XenServer 之间的 SSL 连接失败。

[#LC4377]

- 这是用于辅助执行 NIC 成组的增强功能，通过 HP Moonshot 系统中使用的最新 Mellanox NIC 和固件实现。

[#LC4646]

- 如果在 System Center Virtual Machine Manager (SCVMM) 中创建的模板具有位于两个不同网络上的 NIC（例如，网络 xxx 上的 NIC1 和网络 yyy 上的 NIC2），则 XenDesktop 设置向导的默认行为是将这两个 NIC 均更改为主机记录的网络（网络 zzz）。要使 NIC2 网络保持不变，请在安装此修复后设置以下注册表项：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ProvisioningServices\PlatformScvmm

名称：RequireMatchingNetworks

类型：REG\_DWORD

值：1

[#LC4650]

- 如果在未选择任何产品的情况下按“Ctrl+C”，Provisioning Services 控制台可能会意外退出并显示以下错误消息：

“MMC has detected an error in a snap-in and will unload it.” (MMC 在管理单元中检测到错误，并且会将其卸载。)

此外，如果某些第三方软件自动注入“Ctrl+C”组合键，也可能会出现此问题。

[#LC4909]

## 服务器

- 将虚拟磁盘许可模式更改为密钥管理服务 (KMS) 过程中，SOAP Service 可能会意外退出。

[#LC0265]

- 在 Provisioning Services 7.1 中，如果将引导程序配置为使用网关/DHCP 设置在运行时设置子网掩码值，尝试设置子网掩码 0.0.0.0 将失败，并显示以下错误消息：

Invalid Subnet mask (子网掩码无效)。

[#LC0312]

- 引导过程中，目标设备可能会返回广播的 ARP 回复数据包，导致网络流量过量。

[#LC0451]

- 如果有五个或更多网络适配器连接到服务器，则会显示以下错误消息：

- 消息处理器超时。错误号 0XE0070003。
- 成功发送但未收到响应。错误号 0xA0070002。

[#LC0455]

- 多个目标在遇到网络问题后尝试重新连接时，由于多次重新尝试向目标设备发送数据包，流进程 (StreamProcess.exe) 可能会意外关闭。

[#LC0488]

- 在引导程序配置中使用 DHCP 的网络设置时，DHCP 中的“路由器”选项未配置，Provisioning Services 目标设备中可能会显示错误的默认网关 IP 地址。

[#LC0688]

- 在 Citrix 许可证服务器上安装 XenApp Enterprise 和 PVS 数据中心许可证，并从虚拟磁盘启动 XenApp 目标设备时，许可证管理控制台中不占用 PVS 数据中心许可证。

[#LC0707]

- 在本版本中，vhdUtil 工具可以重命名虚拟磁盘链，并准备要导入以用作新磁盘的链。重命名过程中，发生以下操作：

- 更新磁盘标头、页脚和时间戳。
- 重命名 PVP 文件（如果存在）。
- 基于重命名的链创建 XML 文件，该文件允许 Provisioning Services 控制台导入重命名的磁盘。

[#LC0722]

- 尝试使用 MCLI.exe 或命令“mcli-runwithreturn mapdisk -p disklocatorName=MyDiskLocatorName, sitename=MySiteName, storeName=MyStoreName”在 Provisioning Services 服务器上映射磁盘失败，并显示以下错误消息：

Object Reference not set to an instance of an object (对象引用未设置为对象的实例) (MCLI 命令)

尝试运行命令“mcli-run unmapdisk”失败，并显示错误消息“发生意外的 MAPI 错误”。

[#LC0786]

- 升级到 Provisioning Services 7.1 后，如果存在大量 VDA，则需要四到五个小时才能重新启动所有 VDA。

[#LC0941]

- 将 Provisioning Services 从版本 7.1 升级到 7.6 时，如果运行随 Provisioning Services 提供的、用于创建 SQL 脚本以升级 Provisioning Services 数据库版本的 dbscript.exe 生成器，则将显示一条错误消息，并且生成的脚本被截断。

[#LC1087]

- Notifier.exe 进程可能会遇到访问冲突并随机意外退出。

[#LC1199]

- 目标设备显示正确的重试次数，但 Provisioning Services 控制台始终显示零次重试。

[#LC1427]

- 向存储中添加动态虚拟磁盘时，服务器在向第二个存储中添加动态虚拟磁盘后报告不正确的复制状态。

[#LC1428]

- 在两个虚拟磁盘之间复制并粘贴属性时，在第二个磁盘上不粘贴负载平衡设置。

[#LC1498]

- 关闭系统过程中，预配的虚拟机 (VM) 可能随机无响应。

[#LC1573]

- 启动和停止服务时，Stream Service 失败。

[#LC1664]

- Powershell MCLI 命令“Mcli-Get DeviceInfo”在“状态”字段中返回空值。

[#LC1790]

- 安装 Provisioning Services 控制台 7.1.3 后，Windows Server 2008 R2 和 Windows 7 上多个 .NET 应用程序无法启动。

[#LC1838]

- 在某些环境中，使用 Provisioning Services 7.x 引导程序文件时，需要很长时间才能同时启动多个目标设备。

注意：不存在高负载的情况下，也会出现此问题。

[#LC1839]

- 配置适用于 vCenter 的 VMware PXE Manager 时，如果默认网关 IP 地址未作为 DHCP 选项的一部分提供，引导程序协议会错误地将网关 IP 地址 (GIADDR) 设置为中继代理 IP 地址。

[#LC1966]

- 在磁盘菜单中按下任意键时，目标设备在 Microsoft Hyper-V 上会遇到延迟。

[#LC1997]

- Microsoft Hyper-V 上的目标设备数量增加时，在“启动 Windows”屏幕上，某些目标将无法启动并停止响应。

[#LC2011]

- 多个目标设备关闭时，Stream Service 进程有时会停止响应。

[#LC2141]

- 如果存在无响应的线程，Stream Service 进程将无法在自动重启后恢复。

[#LC2227]

- 在以下情况下，bntftp.exe 占用的内存量会增加到 7.5 GB：有两个 Provisioning Server 配置为使用 TFTP 服务选项时，NetScaler 平衡了服务器的负载时，以及您增大了显示器探测的频率以使运行速度快于默认时间 5 秒时。

[#LC2314]

- XenDesktop 设置向导在一个存储中创建 ESX 虚拟机元数据，而非通过为虚拟机创建的不同磁盘来分发元数据。

[#LC2549]

- 如果运行 Boot Device Manager 时分配了静态 IP 地址，则首次保存 .iso 映像文件并增加 IP 地址后，后续尝试保存的新映像将覆盖现有文件。

[#LC2619]

- 重新启动 Provisioning Server 时，Soap 服务器可能会意外关闭。

[#LC2750]

- 尝试对 Microsoft Windows 使用 MAK 激活会失败，并显示以下错误消息：

Confirmation ID not retrieved, check internet access (无法获取确认 ID，请检查 Internet 访问权限)。

如果 Microsoft Office 安装在虚拟磁盘上，并且 Office 产品的记录存在于 批量激活管理工具 (VAMT) 数据库中，则会出现此问题。激活过程中，Install-Vamt productKey 命令将尝试安装 Windows 和 Office 的 Windows 产品密钥，并返回相同的错误。应用此修复后，Office 将不包含在 MAK 激活中。

此外，Get-VamtConfirmationId 命令返回的结果保存在不正确的位置，因此，当 Microsoft Office 安装在虚拟磁盘上时，也会出现相同的错误。应用此修复后，Get-VamtConfirmationId 命令返回的结果将保存在正确的位置。

注意：此修复不支持 Microsoft Office MAK。Provisioning Services 不支持适用于 Office 的 MAK。在 PVS 映像上安装 Office 的唯一受支持的方式是同时对 Windows 和 Office 使用 密钥管理服务 (KMS)。

[#LC3120]

- 使用 BDM 分区时，如果列表中最上面的服务器无法访问，VMware 上运行的目标设备将不尝试登录列表中的所有服务器。

[#LC3805]

- 尝试在 Provisioning Server 上装载虚拟机磁盘失败，除非服务器对虚拟磁盘具有逻辑访问权限。

[#LC3835]

- 技术支持管理员通过 XenDesktop 设置向导从独立的 Provisioning Services 控制台创建新虚拟机 (VM) 时，尝试从 BDM 分区

启动目标设备失败，并导致登录服务器显示错误的 IP 地址。

[#LC3911]

- 当导出通过运行 PowerShell 命令“Mcli-Run ExportDisk -p DiskLocatorName="DISK\_NAME", StoreName="STORE\_NAME", SiteName="SITE\_NAME”导出虚拟磁盘时，可能会创建其中包含对应于每个虚拟磁盘版本的多个条目的清单文件。当多个站点中存在同名的虚拟磁盘时，会出现此问题。每个版本的重复条目数量对应于具有虚拟磁盘的站点的数目。

[#LC4225]

- 在 SCVMM 环境中，如果 VM 存储路径末尾存在尾随反斜杠 (\)，通过 XenDesktop 设置向导创建计算机将失败。

[#LC4418]

- 这是用于辅助执行 NIC 成组的增强功能，通过 HP Moonshot 系统中使用的最新 Mellanox NIC 和固件实现。

[#LC4646]

- 如果在 System Center Virtual Machine Manager (SCVMM) 中创建的模板具有位于两个不同网络上的 NIC (例如，网络 xxx 上的 NIC1 和网络 yyy 上的 NIC2) ，则 XenDesktop 设置向导的默认行为是将这两个 NIC 均更改为主机记录的网络 (网络 zzz) 。要使 NIC2 网络保持不变，请在安装此修复后设置以下注册表项：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ProvisioningServices\PlatformScvmm

名称：RequireMatchingNetworks

类型：REG\_DWORD

值：1

[#LC4650]

## 目标

- Windows Server 2008 R2 目标设备遇到致命异常，并出现蓝屏，上面显示错误代码 0x4E。

[#LC0350]

- 多个目标在遇到网络问题后尝试重新连接时，由于多次重新尝试向目标设备发送数据包，流进程 (StreamProcess.exe) 可能会意外关闭。

[#LC0488]

- 关闭系统过程中，预配的虚拟机 (VM) 可能随机无响应。

[#LC1573]

- 启用目标设备日志后，BNDevice.exe 无法启动。

[#LC2058]

- 如果服务器不可用，IO 重新连接请求将仅被发送到不可用的服务器，不发送到高可用性配置中的其他服务器。

[#LC2146]

- 使用 Provisioning Services 映像向导创建映像时，或者如果映像处于专有映像模式，写入虚拟磁盘会导致在目标上多次执行

重试操作。

[#LC2218]

- 在 Microsoft Hyper-V 中的目标设备上，当操作系统为意大利语时，不会从旧版网络适配器切换到合成型网络适配器。

[#LC2379]

- 构建个人虚拟磁盘 (PVD) 并安装 Provisioning Services 后，当您使用 XenDesktop 设置向导创建启用了 PVD 的池时，部分 VM 将启动，并且 PVD 软件将初始化写入缓存驱动器作为 PVD。不为 Provisioning Services 创建写入缓存。

[#LC2497]

- 重新启动后，VMware ESX 目标设备上的主机名设置为 MAC 地址。

[#LC2816]

- 在带有 ESX VMXNET3 NIC 的系统上安装 Provisioning Services 目标设备时需安装 Microsoft 修补程序 <https://support.microsoft.com/en-us/kb/2550978> 或替代修补程序。通过此修补程序，将不会明确要求安装 KB2550978，而会显示一条警告消息，通知管理员确保安装 KB2550978 或替代修补程序。

[#LC3016]

- 目标设备可能会向写入缓存磁盘发送每次失败的写入尝试对应的错误日志条目。因此，Provisioning Server 日志中将显示过量的错误消息。

[#LC3110]

- 服务登录帐户设置为“本地系统”（默认值）时，PVS Device Service (BNDDevice.exe) 可能无法成功启动。

[#LC3209]

- 与 Active Directory 密码更改相关的某些严重错误日志的日志记录级别可能未正确设置，因此，这些日志不会发送到服务器以便 Citrix Diagnostic Facility 进行跟踪。

[#LC3803]

- 在启用了 PVD 的虚拟磁盘上，自动虚拟磁盘更新功能不运行清单更新。

[#LC3997]

- 使用 VMXnet3 网络驱动程序的 ESX 目标设备会遇到致命问题，在使用 Jumbo 帧（每个帧的负载超过 1500 字节）时显示蓝屏。

[#LC4238]

- 预配的目标设备具有 96 小时的许可宽限期，在此之后，如果没有有效的可用许可证，目标设备将关闭。通过此增强功能，目标设备的许可宽限期延长至 30 天（720 小时）。

[#LC4645]

## 会话录制

## 代理

- 在 Session Recording Agent 属性中启用“Allow third party applications to record custom data on this VDA machine”（允许第三方应用程序在此 VDA 计算机上记录自定义数据）的情况下，在日语版本的 Windows 操作系统上运行的 Session Recording Agent Service 可能无法启动，并且无法记录客户端会话。

[#LC3861]

## 播放器

- Microsoft 画图会话的录制件无法在 Session Recording Player 中正确播放。

[#LC4389]

- 播放在多显示器用户设备上录制的会话时出现错误。

[#LC4391]

## StoreFront

- 此修复解决了管理控制台用户界面中术语“Classic”的日语翻译不一致的问题。

[#LC3607]

- 单击启动第二个或后续的应用程序时，可能会启动所启动的第一个应用程序的一个或多个实例。如果配置了多站点聚合，则在使用除 Citrix Receiver for Web 以外的 Receiver 版本时会出现此问题。第一个应用程序的另外一个实例可能会从每个聚合的站点启动。

[#LC4278]

- 在 default.ica 文件中为已发布的桌面所做的自定义设置可能不会被接受。例如，您可能无法查看某些桌面内部的连接栏，即使已设置“ConnectionBar = 1”也是如此。

[#LC4688]

- 在某些情况下，StoreFront 会生成包含重复资源的枚举响应。这可能会导致 Receiver for Web 报告故障，并且应用程序可能无法显示。在下列一种或多种情况下会出现此问题：

- 场由多站点配置中的多个 UserFarmMapping 引用。
- 用户属于已应用多个 UserFarmMapping 的 Active Directory 组。
- 其中包含场的 EquivalentFarmSets 没有聚合组，或者存在其中包含针对用户的多个分配的交付组。

[#LC4863]

## 通用打印服务器

## 客户端

- 可能无法在 VDA for Server OS 上的 Microsoft 打印管理控制台中管理远程打印服务器上的端口或打印机，并出现以下错误消息：“Failed to complete the operation. This operation is not supported.”（无法完成此操作。此操作不受支持。）此外，在导航到“端口”选项卡时，可能不会列出端口。

此外，当您右键单击任何打印机并选择“Open Printer Queue”（打开打印机队列）时，可能会出现以下错误消息：

“Windows can't find the printer. Make sure the network is working and you've entered the name of the printer and print server correctly.”（Windows 找不到打印机。请确保网络正常工作，并且您已正确输入打印机和打印服务器的名称。）

要解决此问题，请在 VDA 的注册表中删除注册表

项“HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\Print\Providers\Universal Printer”，然后重新启动打印后台处理程序服务。这些端口将在 Microsoft 打印管理控制台中正确枚举，并且您可以配置端口和打印机。

[#LC3740]

## 服务器

- 通过使用 Microsoft GDI Print API 进行的批量打印可能失败，无法打印到最后一页，并出现以下错误消息：

“Dispatch::CDriverTripSummary::PrintReport, Error Occured While Printing....Check  
Printer”（Dispatch::CDriverTripSummary::PrintReport，打印时出现错误....请检查打印机）

[#LC3920]

- 此修复程序支持适用于通用打印服务器 7.6.300 的 Citrix UPS Print Driver Certification Tool。有关详细信息，请参阅知识中心文章 [CTX142119](#)。

[#LC4265]

## VDA for Desktop OS

内容重定向	<a href="#">登录/身份验证</a>
HDX 3D Pro	<a href="#">打印</a>
HDX MediaStream Flash 重定向	<a href="#">无缝窗口</a>
HDX MediaStream Windows Media 重定向	<a href="#">服务器/站点管理</a>
安装、卸载、升级	<a href="#">会话/连接</a>

键盘	智能卡
	系统异常

## 内容重定向

- 在为 Mailto 链接启用内容重定向的情况下，其中含有逗号的 Mailto 链接无法启动，并出现以下错误消息：

“Could not perform this operation because the default mail client is not properly installed” (因为默认邮件客户端未正确安装，无法执行此操作。)

该问题不会在控制台或远程桌面会话中发生。

[#LC3701]

## HDX 3D Pro

- 在 HDX 3D Pro 双显示器配置中，在一个显示器上锁定 Windows 可能不会使第二个显示器屏幕显示空白。如果与一个双显示器客户端会话断开连接后，从一个显示器客户端重新连接，然后从该会话中断开连接，再从该双显示器客户端重新连接，则会发生此问题。

[#LC3934]

- 将鼠标放置在 Microsoft Notepad 应用程序窗口边缘时，鼠标指针可能无法呈现正确的形状。

要启用此项修复，必须设置以下注册表项：

- 在 32 位 Windows 上：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\HDX3D

名称：EnableUnknownCursorHandling

类型：REG\_DWORD

值：1

- 在 64 位 Windows 上：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\HDX3D

名称：EnableUnknownCursorHandling

类型：REG\_DWORD

值：1

[#LC4160]

- 尝试调整会话屏幕分辨率可能会间歇性失败，从而使 DesktopViewer 窗口灰显。

[#LC4261]

- 在启用 HDX 3D Pro 的情况下，用于呈现应用程序的 3D 图形中的自定义鼠标指针可能无法正确显示。

[#LC4713]

## HDX MediaStream Flash 重定向

- 如果启用了 HDX MediaStream Flash 重定向，在 Internet Explorer 中打开和关闭多个含 Flash 内容的选项卡会导致 Internet Explorer 意外退出。

[#LC0375]

- 在启用了 HDX MediaStream for Flash 的情况下，在 Internet Explorer 中打开和关闭多个选项卡会导致 Internet Explorer 意外关闭。

[#LC1141]

- 在启用 HDX MediaStream for Flash 重定向的情况下浏览 Web 站点时，如果 HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\AppInit\_DLLs 注册表值设置为“mfaphook.dll”或“mfaphook64.dll”而非“mfaphook.dll”或“mfaphook64.dll”的完整路径，则 Flash 重定向功能会失败。

[#LC4388]

#### HDX MediaStream Windows Media 重定向

- 在 Receiver 会话中，如果在播放 .MOD、ac3 和 mpeg 文件期间在 Windows Media Player 中向前搜寻，可能会导致播放视频但不播放音频。

[#LC2768]

- 如果您在 ICA 会话（或已发布的桌面会话）中使用 Windows Media Player 播放 .avi 文件，然后在不停止第一个 .avi 文件的情况下开始播放另一个 .avi 文件，则视频帧可能无法正确定向到用户设备。由此，mmvdhost.exe 进程的 CPU 使用率可高于正常使用率，并且视频可能无法在用户设备上正常显示。

[#LC4260]

#### 安装、卸载、升级

- 在安装以下一个或多个 Microsoft 安全更新后，登录正在运行 Windows 10 的 XenDesktop VDA 7.6.300 或 7.7 的尝试会失败。有关详细信息，请参阅知识中心文章 [CTX205398](#)。

	安全更新	发行日期
Windows 10 RTM [Build 10240]  (当前 Business Branch 和 LTSB)	<a href="#">KB3124266</a>	2016 年 1 月
	<a href="#">KB3135174</a>	2016 年 2 月
	<a href="#">KB3140745</a>	2016 年 3 月
	<a href="#">KB3147461</a>	2016 年 4 月
	<a href="#">KB3156387</a>	2016 年 5 月
Windows 10 版本 1511  [Build 10586.36]	<a href="#">KB3124263</a>	2016 年 1 月
	<a href="#">KB3124262</a>	2016 年 1 月

	<a href="#">KB3135173</a>	2016 年 2 月
	<a href="#">KB3140768</a>	2016 年 3 月
	<a href="#">KB3147458</a>	2016 年 4 月
	<a href="#">KB3156421</a>	2016 年 5 月
Windows 10 版本 1511  (2016 年 2 月更新)	其中包含 2016 年 2 月的所有更新的累积映像	2016 年 3 月

注意：如果您已安装上述任何 Microsoft 安全更新：

如果您已经在 Windows 10 RTM (Build 10240) VDA 或 Windows 10 版本 1511 (Build 10586.36) VDA 上安装任何上述 Microsoft 安全更新，并需要应用此更新，请执行以下操作：

1. 重新启动并使用安全模式登录到 Windows 10 VDA。
2. 卸载上述 Microsoft 安全更新，然后重新启动。
3. 安装此更新并重新启动。
4. 安装任何适用的 Microsoft 安全更新。

对于在 Windows 10 (RTM/版本 1511/版本 1511 (在 2016 年 2 月更新)) 上新部署的 7.6.300 VDA，请执行以下操作：

1. 准备 Windows 10 (RTM/版本 1511/版本 1511 (在 2016 年 2 月更新)) 映像。

警告：在下一步中安装 VDA 并重新启动会使计算机进入无法恢复的状态。无需在安装 VDA 后执行重新启动。

2. 安装 7.6.300 VDA 并选择不重新启动。
3. 安装此更新并重新启动。

[#LC4604]

## 键盘

- 如果您在 VDA 会话中运行 Citrix GoToMeeting 并被设置为演示者，则您的鼠标指针可能会开始闪烁。如果会话禁用了“旧图形模式”策略设置，则会发生此问题。

[#LC3033]

## 登录/身份验证

- 如果“Windows 远程桌面会话主机配置”策略设置“始终在连接时提示输入密码”已启用，则当用户使用 ICA 协议登录到 VDA 7.x 时，系统会提示用户重新输入凭据。

要启用此修复，请设置以下注册表项：

HKEY\_LOCAL\_MACHINE\Software\Citrix\Portica

名称：AutoLogon

类型：DWORD

数据：0x00000001 (值必须介于 0 到 2147483647 之间)

注意：如果多次尝试运行 MSP 文件，可标记 Citrix Display Drive 以进行删除。这将导致无法安装修补程序。此外，VDA 的显示分辨率可能不正常。要使其正常，请重新启动 VDA，然后再安装修补程序。

[#LC1180]

- 安装 Microsoft 修补程序 KB3124266（对于 Windows 10）或 KB3124263（对于 Windows 10 1511）后，尝试登录到 Windows 10 上运行的 XenDesktop VDA 7.6.300 或 7.7 可能会失败。有关详细信息，请参阅知识中心文章 [CTX205398](#)。

注意：如果您已安装 KB3124266 或 KB3124263，并希望应用此更新，请执行以下操作：

1. 重新启动并使用安全模式登录到 Windows 10 计算机，然后卸载 KB3124266 或 KB3124263
2. 重新启动 Windows 10 计算机，然后安装此更新。
3. 重新安装 KB3124266 或 KB3124263。

[#LC4540]

## 打印

- Citrix 打印后台处理程序服务可能会意外退出。

[#LC4180]

## 无缝窗口

- 无缝应用程序可能无响应，它在 Windows 任务栏中的图标将还原为通用 Citrix Receiver 图标。

[#LC3783]

- 关闭一个无缝已发布应用程序后，焦点将转到另一个已发布应用程序，而不是典型 [Windows Z 顺序](#) 中的窗口。

[#LC4009]

## 服务器/站点管理

- 在管理员尝试从 Hyper-V 控制台访问虚拟机时，如果某个会话已断开连接，但处于活动状态，则会显示黑屏。在使用 XPDM 驱动程序的部署环境中会发生此问题。

[#LC3536]

- VDA 可能不再接受连接。启动“旧图形模式”策略后，VDA 将再次开始接受连接。

[#LC3749]

- 当启动 VM 托管的应用程序时，可能会在应用程序完全启动之前显示 Windows 登录屏幕。此修复程序将提供 15 秒的宽限期，然后欢迎屏幕才会出现。它还支持以下注册表项，使您可以自定义宽限期的持续时间。

注意：在宽限期内，不会向用户显示信息以指出应用程序正在启动。如果配置过高的宽限期，可能使应用程序启动延迟，并导致用户无意中启动应用程序多次。

要更改宽限期的持续时间，请设置以下注册表项：

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI

名称：LogonUIHideTimeout

类型：DWORD

值：任何大于零值，以毫秒为单位（例如，20000 毫秒对应于 20 秒）

[#LC3828]

- 尝试使用 attrib 命令更改映射的客户端驱动器上的文件的文件属性可能会失败。

[#LC3958]

- “输出会话带宽性能监控”计数器可能会长时间内在记录时报告不一致的值。

[#LC4151]

- 如果您使用显式凭据（用户名/密码）登录到 7.6.300 VDA 版本，并且已启用用户帐户控制 (UAC)，则在尝试使用智能卡对正在会话中运行的应用程序进行身份验证时，可能会出现以下错误消息：

“An authentication error has occurred. No credentials are available in the security package.” (发生身份验证错误。安全包中没有可用的凭据。)

[#LC4486]

## 会话/连接

- 当端点安装有多个网络摄像机或视频捕捉设备时，只会将其中一个设备映射到客户端会话。此外，设备将映射为 Citrix HDX 网络摄像机，而不会留下关于所映射设备的任何明显迹象。

[#LC1919]

- 在已启用本地应用程序访问的会话中，无法激活屏幕保护程序。

[#LC3182]

- Citrix 策略“拖动时查看窗口内容”无法正常工作。

[#LC3552]

- 已断开的会话可能会在物理计算机上保持打开，即使已经过在“断开会话计时器时间间隔”中指定的时间后也是如此。

要启用此修复，请设置以下注册表项：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\Portica

名称：ForceDisableRemotePC

类型：DWORD

值：任何大于零的值

[#LC3650]

- 如果端点在几分钟里丢失网络连接，则重新连接尝试可能会失败，直至 VDA 重新启动。

[#LC3700]

- 当在 VDA 长时间处于空闲状态后登录到 VDA 时，在重新连接时可能不会自动将凭据传递给登录屏幕，并且登录屏幕上会提示输入密码。

[#LC3720]

- 即使相关已发布应用程序关闭了文件，WFICA32.exe 进程也仍会使该文件保持锁定状态。因此，在一段时间内无法编辑该文件。

[#LC3724]

- 某些第三方发布的应用程序可能无法在 XenApp 服务器上启动。由此，wfshell.exe 进程可能会意外关闭。发生此错误时，不会在用户设备上显示任何表明会话正在启动的信息，也不会显示错误消息。

[#LC3766]

- 移除多显示器会话中的 Thomson Reuters Eikon 工具栏后，会话不回收该工具栏占用的空间。

在其中的主显示器不位于阵列左上角的显示器配置中，您还必须安装修复程序 #LC1599（此修复程序在 Receiver for Windows 4.4 及更高版本中提供）。

[#LC3773]

- 当在会话主机上启用 App-V 配置设置“EnablePublishingRefreshUI”并且已启用“Session Lingering”时，如果尝试在 iOS 设备上关闭应用程序，可能会导致设备屏幕上显示黑色窗口。

[#LC3800]

- 启用 Citrix Windows XP 显示驱动程序模型 (XPDM) 显示驱动程序后，鼠标阴影设置将始终处于启用状态，即使在控制面板中将其禁用也是如此。

[#LC3806]

- 如果启用了 Excelhook，则在最小化后还原 Excel 工作簿时，可能导致 Excel 窗口丢失焦点。

[#LC3873]

- 对于使用 Citrix Receiver for Android 的会话，“限制会话剪贴板写入”和“限制客户端剪贴板写入”策略无法正常工作。由此，用户可在会话和用户设备之间复制并粘贴内容，而不管这两个策略的配置如何。

[#LC3894]

- 当您尝试重新连接到已断开的会话时，会出现 Windows 锁屏界面，其中包含一组键，但没有用于输入密码的选项。当单击“其他凭据”时，会显示第二个凭据图标，可用于输入密码并解锁会话。

[#LC4053]

- 如果在 ICA 会话中关闭电源或强制重新启动远程计算机，可能会在远程 PC 重启完成时禁用所有音频驱动程序。

[#LC4071]

- 如果在相关已发布应用程序正在运行时向用户设备文件夹添加文件，然后尝试从该应用程序中打开该文件，则该应用程序的“打开文件”对话框可能无法显示该文件，即使单击刷新按钮也是如此。

[#LC4073]

- 由于 picadm.sys 上的死锁，VDA 可能在出现“欢迎”屏幕后无响应。

[#LC4195]

- 启用通用 USB 重定向功能后，每当在会话中与通用重定向的 USB 设备断开物理连接并重新连接时，该设备都会被视为新设

备。因此，每次重新连接这种 USB 设备时，系统都会为其另外创建一个 GUID。

[#LC4259]

- 如果满足所有三个下列条件，则 Citrix Receiver for Chrome 和 VDA 之间的 TLS 连接会失败：

- 已在 VDA 上安装修复程序 #LC2179（修补程序 ICAWS760WX64032 或其替代项）
- 连接已配置为使用 SSL
- Citrix Gateway Protocol (CGP) 已禁用

[#LC4405]

- 在安装修补程序 ICAWS760WX64032 和启用 SSL 后，重新连接到 VDA 的尝试可能会间歇性失败。如果 Citrix ICA 服务因为 SSL 倾听器故障而意外退出或无响应，将出现该问题。

[#LC4438]

- 当在用户设备之间漫游会话时，在 VDA for Desktop OS 7.6.300 版本（已安装 RES Workspace Manager）上运行的会话可能不响应。

[#LC4570]

## 智能卡

- 在 Microsoft Internet Explorer 中，某些 Web 站点的智能卡登录用户界面可能间歇性不可用。

[#LC3988]

## 系统异常

- 在登录或更改显示分辨率时，Ctxgfx.exe 进程可能进入死锁状态，并导致会话挂起。

[#LC2410]

- 操作系统中的 picadm.sys 出现错误，并显示蓝屏和停止代码 0x20。

[#LC3473]

- 操作系统中的 picadm.sys 出现错误，并显示蓝屏和停止代码 0x00000050。

[#LC3921]

- 操作系统中的 ctxad.sys 出现错误，并显示蓝屏和错误检测代码 0xD1。

[#LC4007]

- 在将 VDA for Desktop OS 或 Server OS 升级到 7.6.300 版后，Citrix Print Manager Service (CpSvc.exe) 可能会在注销时意外退出。

[#LC4102]

- 操作系统中的 picadm.sys 出现错误，并显示蓝屏和停止代码 0x000000C1。

[#LC4334]

- 当您在 Windows Media Player 上重复播放 .avi 文件时，wfica32.exe 进程消耗的内存可能会持续增加，直到此进程意外退

出。

[#LC4335]

- 在从 Citrix Receiver 会话注销时，VDA 可能会在 picadd.sys 中遇到严重异常，并显示蓝屏。

[#LC4360]

- VDA 可能在 ctxdvcs.sys 中的错误检测代码 0x00000044 处遇到严重异常，并显示蓝屏。

[#LC4505]

- 如果已定义注册表项 HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ICA\Thinwire\DisableOssForProcesses，则在尝试重新启动 VDA 和启动已发布的桌面时可导致蓝屏。

[#LC4597]

## VDA for Server OS

内容重定向	服务器/站点管理
HDX MediaStream Windows Media 重定向	会话/连接
键盘	智能卡
打印	系统异常
无缝窗口	用户体验

### 内容重定向

- 在除运行 Windows Server 2008 R2 的 VDA 外的其他 VDA 上，从服务器到客户端的内容重定向会失败。因此，当您单击 VDA 会话中的 URL 时，链接将在运行于会话中的浏览器中打开，而不是在本地浏览器中打开。

[#LC2221]

- 在为 Mailto 链接启用内容重定向的情况下，其中含有逗号的 Mailto 链接无法启动，并出现以下错误消息：

“Could not perform this operation because the default mail client is not properly installed”（因为默认邮件客户端未正确安装，无法执行此操作。）

该问题不会在控制台或远程桌面会话中发生。

[#LC3701]

### HDX MediaStream Windows Media 重定向

- 在 Receiver 会话中，如果在播放 .MOD、ac3 和 mpeg 文件期间在 Windows Media Player 中向前搜寻，可能会导致播放视频但不播放音频。

[#LC2768]

- 如果您在 ICA 会话（或已发布的桌面会话）中使用 Windows Media Player 播放 .avi 文件，然后在不停止第一个 .avi 文件的情况下开始播放另一个 .avi 文件，则视频帧可能无法正确定向到用户设备。由此，mmvdhost.exe 进程的 CPU 使用率可高于正常使用率，并且视频可能无法在用户设备上正常显示。

[#LC4260]

## 键盘

- 如果您在 VDA 会话中运行 Citrix GoToMeeting 并被设置为演示者，则您的鼠标指针可能会开始闪烁。如果会话禁用了“旧图形模式”策略设置，则会发生此问题。

[#LC3033]

## 打印

- Citrix 打印后台处理程序服务可能会意外退出。

[#LC4180]

## 无缝窗口

- 无缝应用程序可能无响应，它在 Windows 任务栏中的图标将还原为通用 Citrix Receiver 图标。

[#LC3783]

- 关闭一个无缝已发布应用程序后，焦点将转到另一个已发布应用程序，而不是典型 Windows Z 顺序中的窗口。

[#LC4009]

## 服务器/站点管理

- 当启动 VM 托管的应用程序时，可能会在应用程序完全启动之前显示 Windows 登录屏幕。此修复程序将提供 15 秒的宽限期，然后欢迎屏幕才会出现。它还支持以下注册表项，使您可以自定义宽限期的持续时间。

注意：在宽限期内，不会向用户显示信息以指出应用程序正在启动。如果配置过高的宽限期，可能使应用程序启动延迟，并导致用户无意中启动应用程序多次。

要更改宽限期的持续时间，请设置以下注册表项：

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix\wfshell\TWI

名称：LogonUIHideTimeout

类型：DWORD

值：任何大于零值，以毫秒为单位（例如，20000 毫秒对应于 20 秒）

[#LC3828]

- 尝试使用 attrib 命令更改映射的客户端驱动器上的文件的文件属性可能会失败。

[#LC3958]

- 从单独用户设备建立与 VDA 的远程桌面 (RDP) 连接的多个并行尝试可能会导致 VDA 取消注册。

[#LC4014]

- “输出会话带宽性能监控”计数器可能会长时间在记录时报告不一致的值。

[#LC4151]

- 当 VDA for Server OS 未注册或 Citrix Desktop Service 被禁用时，即使是域管理员也无法通过远程桌面 (RDP) 连接登录到 VDA。然而该行为是为非管理员角色设计的，管理员应能够进行登录。

[#LC4290]

- 如果您使用显式凭据（用户名/密码）登录到 7.6.300 VDA 版本，并且已启用用户帐户控制 (UAC)，则在尝试使用智能卡对正在会话中运行的应用程序进行身份验证时，可能会出现以下错误消息：

“An authentication error has occurred. No credentials are available in the security package.” (发生身份验证错误。安全包中没有可用的凭据。)

[#LC4486]

- 无法在 Excel 电子表格中进行实时滚动（翻页和滚动的同步状态）。VDA 7.6.300 版本中引入了修复程序 #LC2965，用于解决此问题。但是，修复程序 #LC2965 无法在所有情况下完全解决此问题。修复程序 #LC4579 可确保更正此问题，即使在修复程序 #LC2965 不起作用的系统中也是如此。

根据 #LC2965 的说明：

无法在 Excel 电子表格中进行实时滚动（翻页和滚动的同步状态）。之所以发生此问题，是因为在用户每次登录 VDA 时，VDA 上的注册表位置 HKEY\_CURRENT\_USER\Control Panel\Desktop\UserPreferencesMask 中的注册表项和值被 wfshell.exe 进程重写。要阻止此问题，请在 VDA 上创建以下注册表项，并将值设置为 1：

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix

名称：EnableVisualEffect

类型：REG\_DWORD

值：1

[#LC4579]

- 安装修补程序 ICATS760WX64022（或其替代项）之后，注册表项 HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\Graphics\下的任何新自定义注册表配置在重新启动系统后可能无法保留。

[#LC4931]

## 会话/连接

- “源网络地址”在服务器的 Windows 安全日志中为远程用户设备显示不正确的 IP 地址（事件 ID 为 4624）。

[#LC1352]

- 在禁用“客户端音频重定向”或“Windows Media 重定向”策略的情况下，已发布的桌面会话的通知区域中的音量控制（扬声器）图标可能显示不正确的音频状态。

[#LC2538]

- 在 Citrix Receiver for Android 发布的桌面会话中，打开 Microsoft Outlook 日历邀请的尝试可能会失败，并出现以下错误消息：

“Cannot open item”（无法打开项目）

此问题发生于其他用户所创建的日历邀请；由相同用户创建的邀请不受影响。

[#LC2828]

- 在某些情况下，在登录或重新连接到已断开的会话时，客户端打印机重定向和 Citrix 组策略访问控制过滤器可能无法工作。

[#LC3083]

- 在已启用本地应用程序访问的会话中，无法激活屏幕保护程序。

[#LC3182]

- 即使相关已发布应用程序关闭了文件，WFICA32.exe 进程也仍会使该文件保持锁定状态。因此，在一段时间内无法编辑该文件。

[#LC3724]

- 某些第三方发布的应用程序可能无法在 XenApp 服务器上启动。由此，wfshell.exe 进程可能会意外关闭。发生此错误时，不会在用户设备上显示任何表明会话正在启动的信息，也不会显示错误消息。

[#LC3766]

- 移除多显示器会话中的 Thomson Reuters Eikon 工具栏后，会话不回收该工具栏占用的空间。

在其中的主显示器不位于阵列左上角的显示器配置中，您还必须安装修复程序 #LC1599（此修复程序在 Receiver for Windows 4.4 及更高版本中提供）。

[#LC3773]

- 当在会话主机上启用 App-V 配置设置“EnablePublishingRefreshUI”并且已启用“Session Lingering”时，如果尝试在 iOS 设备上关闭应用程序，可能会导致设备屏幕上显示黑色窗口。

[#LC3800]

- 在通过 RDP 会话连接到服务器时，在终端服务 (TermService) 中注册的服务主机 (svchost.exe) 进程可能会在 RPM.dll 上意外关闭。

[#LC3808]

- 如果启用了 Excelhook，则在最小化后还原 Excel 工作簿时，可能导致 Excel 窗口丢失焦点。

[#LC3873]

- 即使在已启用客户端音频重定向策略的情况下，音频 (.wav) 文件仍可能无法播放。在重复使用会话 ID 且已为上一个会话禁用客户端音频重定向策略的情况下，会出现此问题。

[#LC3882]

- 对于使用 Citrix Receiver for Android 的会话，“限制会话剪贴板写入”和“限制客户端剪贴板写入”策略无法正常工作。由此，用户可在会话和用户设备之间复制并粘贴内容，而不管这两个策略的配置如何。

[#LC3894]

- 当因为许可证错误而导致 Windows Server 2008 R2 VDA 的连接失败时，无法显示错误消息“由于没有可用的许可证，无法访问此会话。”。

[#LC4026]

- 如果在相关已发布应用程序正在运行时向用户设备文件夹添加文件，然后尝试从该应用程序中打开该文件，则该应用程序的“打开文件”对话框可能无法显示该文件，即使单击刷新按钮也是如此。

[#LC4073]

- 在注销新安装的 Feature Pack 3 VDA for Server OS (7.6.300) 后，Citrix Studio 可能会将 VDA 的状态显示为“正在初始化”而不是“已注册”。在此期间，将不会为该 VDA 代理任何新会话。

[#LC4188]

- 由于 picadmsys 上的死锁，VDA 可能在出现“欢迎”屏幕后无响应。

[#LC4195]

- 启用通用 USB 重定向功能后，每当在会话中与通用重定向的 USB 设备断开物理连接并重新连接时，该设备都会被视为新设备。因此，每次重新连接这种 USB 设备时，系统都会为其另外创建一个 GUID。

[#LC4259]

- COM 端口映射可能会间歇性地失败。

[#LC4267]

- 在启用“应用程序预启动”功能的情况下，可能会在用户设备上临时显示一个黑色窗口。当在不启动应用程序的情况下启动 Citrix Receiver 时，可能会出现此问题。

[#LC4280]

- Citrix 策略“拖动时查看窗口内容”无法在已发布的桌面上正常工作。当您登录到 VDA 时，窗口内容会正确显示。但是，在重新连接已断开的会话后，将不再显示窗口内容。

[#LC4301]

- 如果满足所有三个下列条件，则 Citrix Receiver for Chrome 和 VDA 之间的 TLS 连接会失败：

- 已在 VDA 上安装修复程序 #LC2179 (修补程序 ICATS760WX64032 或其替代项)
- 连接已配置为使用 SSL
- Citrix Gateway Protocol (CGP) 已禁用

[#LC4405]

- 在 VDA 7.6.300 会话中启动应用程序时，在应用程序启动之前，会显示含以下消息的进度条几分钟：“Please wait for Local Session Manager”（请等待 Local Session Manager）。在此期间，应用程序看上去无响应，即使它已正确启动也是如此。

[#LC4406]

- 用户会话中的某些应用程序可能默认使用不正确的输入法。可通过在各控制面板中清除“允许我为每个应用窗口设置不同的

输入法”复选框来更正此行为。但是，当您重新连接到会话时，设置会恢复为错误的默认设置。

要使设置不恢复，请设置以下注册表项：

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Citrix

名称：EnableLocalInputSetting

类型：DWORD

数据：1 (可以更改输入方法设置)

[#LC4416]

- 当通过 NetScaler Gateway 连接时，SmartAccess Control 过滤器可能无法正确应用。

[#LC4503]

- 已发布的应用程序路径中的非 ASCII 字符导致应用程序无法启动。

[#LC4595]

- 在启用“客户端自动重新连接”策略的情况下，重新连接到会话的尝试可间歇性地失败，并导致 VDA 重新注册。将出现以下警告消息：

“Event 1048, Citrix Desktop Service (Warning)

The Citrix Desktop Service is re-registering with the DDC: "NotificationManager:NotificationServiceThread: WCF failure or rejection by broker (*DDC NAME>*)" (事件 1048 , Citrix Desktop Service (警告) Citrix Desktop Service 正在重新注册，DDC：“NotificationManager:NotificationServiceThread: WCF 发生故障或被 Broker 拒绝 (“))

[#LC4767]

## 智能卡

- 在 Microsoft Internet Explorer 中，某些 Web 站点的智能卡登录用户界面可能间歇性不可用。

[#LC3988]

## 系统异常

- 操作系统中的 picadmsys 出现错误，并显示蓝屏和停止代码 0x20。

[#LC3473]

- 操作系统中的 picadmsys 出现错误，并显示蓝屏和停止代码 0x00000050。

[#LC3921]

- 在将 VDA for Desktop OS 或 Server OS 升级到 7.6.300 版后，Citrix Print Manager Service (CpSvc.exe) 可能会在注销时意外退出。

[#LC4102]

- 在终端服务 (TermService) 中注册的服务主机 (svchost.exe) 进程可能会意外退出。

[#LC4150]

- 操作系统中的 picadm.sys 出现错误，并显示蓝屏和停止代码 0x000000C1。  
[#LC4334]
- 当您在 Windows Media Player 上重复播放 .avi 文件时，wfica32.exe 进程消耗的内存可能会持续增加，直到此进程意外退出。  
[#LC4335]
- 在从 Citrix Receiver 会话注销时，VDA 可能会在 picadd.sys 中遇到严重异常，并显示蓝屏。  
[#LC4360]
- VDA 可能在 ctxdvc.sys 中的错误检测代码 0x00000044 处遇到严重异常，并显示蓝屏。  
[#LC4505]
- 如果已定义注册表项 HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ICA\Thinwire\DisableOssForProcesses，则在尝试重新启动 VDA 和启动已发布的桌面时可导致蓝屏。  
[#LC4597]

## 用户体验

- 当尝试在无缝的双显示器会话中移动 Microsoft Excel 窗口时，该窗口可能会在重绘新位置时发生延迟。  
[#LC4441]

# 虚拟桌面组件 - 其他

- 操作系统中的 picadm.sys 出现错误，并显示蓝屏和停止代码 0x20。  
[#LC3473]
- 操作系统中的 picadm.sys 出现错误，并显示蓝屏和停止代码 0x00000050。  
[#LC3921]
- 在将 VDA for Desktop OS 或 Server OS 升级到 7.6.300 版后，Citrix Print Manager Service (CpSvc.exe) 可能在注销时意外退出。  
[#LC4102]
- 在终端服务 (TermService) 中注册的服务主机 (svchost.exe) 进程可能会意外退出。  
[#LC4150]
- 操作系统中的 picadm.sys 出现错误，并显示蓝屏和停止代码 0x000000C1。  
[#LC4334]
- 当您在 Windows Media Player 上重复播放 .avi 文件时，wfica32.exe 进程消耗的内存可能会持续增加，直到此进程意外退出。

[#LC4335]

- 在从 Citrix Receiver 会话注销时，VDA 可能会在 picadd.sys 中遇到严重异常，并显示蓝屏。

[#LC4360]

- VDA 可能在 ctxdvcs.sys 中的错误检测代码 0x00000044 处遇到严重异常，并显示蓝屏。

[#LC4505]

- 如果已定义注册表项 HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ICA\Thinwire\DisableOssForProcesses，则在尝试重新启动 VDA 和启动已发布的桌面时可导致蓝屏。

[#LC4597]

# Long Term Service Release (LTSR)

Dec 16, 2016

发布日期：2016 年 1 月 11 日

## 安装和升级 LTSR 组件

要满足 XenApp 和 XenDesktop 7.6 长期服务版本 (LTSR) 的要求，必须升级属于 LTSR 的一部分以及 LTSR 版本部署的一部分的 XenApp 和 XenDesktop 7.6 的组件。例如：如果 Provisioning Services 属于您的部署的一部分，则必须将 Provisioning Services 组件升级到其 LTSR 版本。如果 Provisioning Services 不属于您的部署的一部分，则不需要安装或升级该组件。

根据 LTSR 条款，为使您的部署有资格享有各项优势，必须升级到 LTSR 版本。

此外，Citrix 还建议您使用特定版本的 Citrix Receiver 及其他组件。升级到这些组件的当前版本可确保进一步简化维护过程以及确保您的部署中最新修复的可用性，但这并非是 LTSR 合规性的必需条件。

有用链接：

- [下载 LTSR \(XenApp\)](#)
- [下载 LTSR \(XenDesktop\)](#)
- [XenApp 和 XenDesktop 服务选项](#)
- [LTSR 常见问题解答 \(FAQ\)](#)
- [产品生命周期日期](#)
- [Receiver for Windows 的 LTSR 计划](#)

LTSR 基础组件和必需版本

### 注意

下面是 LTSR 基础版本特定的信息。有关 CU1 或 CU2 的此类信息，请参阅各自的文档。

虽然 LTSR 合规性不要求在您的部署中安装以下组件，但您必须将部署中的每个组件都升级到下文指示的版本。

LTSR 基础组件	版本	注意
VDA for Desktop OS	7.6.300	适用于 Windows 10 的特殊规则。请参阅 <a href="#">兼容组件和平台</a> 。
VDA for Server OS	7.6.300	

Delivery Controller	7.6 Update 3	
Citrix Studio	7.6 Update 3	
Citrix Director	7.6.300	
组策略管理体验	7.6.300 (2.5)	
StoreFront	3.0.1	
Provisioning Services	7.6 Update 1	适用于 Windows 10 的特殊规则。请参阅 <a href="#">兼容组件和平台</a> 。
通用打印服务器	7.6.300	仅支持 Windows 2008 R2 SP1 Windows 2012 Windows 2012 R2
会话录制	7.6.100	仅限 Platinum Edition

## 兼容组件和平台

建议您在 7.6 LTSR 环境中使用以下组件。这些组件无权享有 LTSR 的优势（扩展的生命周期以及仅用于修复的累积更新）。Citrix 可能会要求您在 7.6 LTSR 环境中升级到这些组件的较新版本。

**Windows 10 注意事项：**可以通过当前版本路径获取对 Windows 10 的常规支持。Windows 10 无法享有 7.6 LTSR 的所有优势。对于包括 Windows 10 计算机的部署，Citrix 建议您使用 VDA for Desktop OS 7.9 和 Provisioning Services 7.9。

有关详细信息，请参阅 [Adding Windows 10 Compatibility to XenApp and XenDesktop 7.6 LTSR](#)（向 XenApp 和 XenDesktop 7.6 LTSR 添加 Windows 10 兼容性）和 [XenApp and XenDesktop Servicing Options \(LTSR\) FAQ](#)（XenApp 和 XenDesktop 服务选项 (LTSR) 常见问题解答）。

LTSR 兼容的组件和平台	版本
Profile Management	5.4
AppDNA	7.6.5
许可证服务器	11.12.1
HDX RealTime Optimization Pack	2.0
Windows 10	VDA：版本 7.9

## Citrix Receiver 的兼容版本

为简化维护过程以及确保实现最佳性能，Citrix 建议您在最新版本的 Citrix Receiver 可用时随时升级到相应版本。可以从 <https://www.citrix.com/downloads/citrix-receiver.html> 下载最新版本。为方便起见，请考虑订阅 [Citrix Receiver RSS 源](#) 以便在新版本的 Citrix Receiver 可用时接收通知。

请注意，Citrix Receiver 无法享有 XenApp 和 XenDesktop LTSR 的优势（扩展的生命周期和仅用于修复的累积更新）。Citrix 可能会要求您在 7.6 LTSR 环境中升级到 Citrix Receiver 的较新版本。如果使用的是 Citrix Receiver for Windows，Citrix 已公布特殊的 LTSR 计划。可以从 [Citrix Receiver 的生命周期里程碑](#) 页面获取有关该计划的详细信息。

特别需要指出的是，LTSR 支持以下版本的 Citrix Receiver 以及之后的所有版本：

LTSR 兼容的 Citrix Receiver	版本
<a href="#">Citrix Receiver for Windows</a>	4.4 或更高版本
<a href="#">Citrix Receiver for Linux</a>	13.2.1 或更高版本
<a href="#">Citrix Receiver for Mac</a>	12.1 或更高版本
<a href="#">Citrix Receiver for Chrome</a>	1.8 或更高版本
<a href="#">Citrix Receiver for HTML5</a>	1.8 或更高版本
<a href="#">Citrix Receiver for iOS</a>	6.1.1 或更高版本
<a href="#">Citrix Receiver for Android</a>	3.8 或更高版本

## 需要注意的例外

以下功能、组件和平台无法享有 LTSR 的生命周期里程碑和优势。需要特别指出的是，累积更新和扩展生命周期优势被排除在外。可以通过常规的最新版本获取扩展功能和组件的更新。

排除的功能
本地应用程序访问
Framehawk

## 排除的组件

Linux VDA

Personal vDisk

## 排除的 Windows 平台\*

Windows 2008 32 位 (面向通用打印服务器)

\* Citrix 保留根据第三方供应商的生命周期里程碑更新平台支持的权利。

## 升级到 XenApp 和 XenDesktop 7.6 LTSR

可以直接从 XenApp 和 XenDesktop 7.6 升级到 LTSR 以及从三个 7.6 Feature Pack 之一进行升级。

下载位置：

- [下载 LTSR \(XenApp\)](#)
- [下载 LTSR \(XenDesktop\)](#)

好消息：多个组件的 LTSR 版本已经发布了一段时间，主要作为 Feature Pack 3 的一部分提供。这意味着，如果您已将部署升级到 Feature Pack 3，多个组件已符合 LTSR。在这些情况下，您不需要进一步执行任何操作。请注意，本版本最初是在下文中列出的各种组件的相应章节中发布的，以确认您是否需要越过 Feature Pack 3 进行升级。

升级 Controller 之前的注意事项：升级到 Controller 的 LTSR 版本会修改您的站点数据存储的一个或多个 DbSchema。这些修改具有永久性和不可逆转性，即，不能自动还原这些修改。因此，升级 Controller 之前，请务必阅读并理解有关升级到 Controller 的 LTSR 版本的相关章节。

## Virtual Delivery Agent (VDA) for Desktop OS 7.6.300

LTSR 版本：VDA for Desktop OS 7.6.300

本版本最初是在 2015 年 9 月 30 日作为 Feature Pack 3 的一部分发布的 (VDAWorkstationSetup\_7.6.300.exe)

### 系统要求

### 已修复的问题

### 安装/升级

在要安装 VDA 的计算机上下载并运行 VDAWorkstationSetup\_7.6.300.exe。请使用图形界面或命令行。

有关详细信息，请参阅[使用独立的软件包安装 VDA](#)。

## Virtual Delivery Agent (VDA) for Server OS 7.6.300

LTSR 版本 : VDA for Server OS 7.6.300

本版本最初是在 2015 年 9 月 30 日作为 Feature Pack 3 的一部分发布的 (VDASetup\_7.6.300.exe)

### 系统要求

#### 已修复的问题

#### 安装/升级

在要安装 VDA 的计算机上下载并运行 VDASetup\_7.6.300.exe。请使用图形界面或命令行。

VDA for Windows Server OS 安装会自动部署 Microsoft Visual C++ 2013 Runtime (32 位和 64 位) 以及 2008 和 2010 Runtime (32 位和 64 位)。不再部署 Microsoft Visual C++ 2005。这些必备项将启动服务器重新启动，并且 VDA 安装将在重新启动后继续运行。

有关详细信息，请参阅[使用独立的软件包安装 VDA](#)。

## Delivery Controller 7.6.3 (Controller Hotfixes Update 3)

LTSR 版本 : Delivery Controller 7.6.3

本版本最初是在 2015 年 11 月 12 日作为 Delivery Controller 7.6.3 (Controller Hotfixes Update 3) 的一部分发布的

### 系统要求

#### 已修复的问题 (32 位)

#### 已修复的问题 (64 位)

#### 安装/升级

如果您的 Controller 的版本为 7.6.3 :

Controller 7.6.3 (Controller Hotfixes Update 3) 为 LTSR 版本。如果您之前已升级到版本 7.6.3，则 Controller 符合 LTSR，不需要进行升级，可以跳至 Citrix Studio 部分。重要：请务必安装版本 7.6.3 的所有组件；否则，您的 Controller 可能会处在不稳定状态。

如果您的 Controller 的版本为 7.6、7.6.1 或 7.6.2 :

要符合 LTSR，需要将您的 Controller 升级到 LTSR 版本。为此，请将 LTSR 版本下载到您的 Controller 并按照下面的升级说明进行操作。

警告：不支持从各个 Controller 组件降级（又称为回滚），并且降级可能会将您的系统保留在不稳定状态。Controller 组件不修补现有安装，每个组件都会使用新安装完全替换原始组件。因此，卸载某个组件会从 Controller 中删除整个组件。如果需要还原到早期版本的 Controller，则必须卸载每个组件，然后重新安装每个组件的早期版本。还原到早期版本的组件可能会导致丢失您在安装此升级时配置的设置。

重要：必须安装 LTSR 版本的所有组件；否则，您的 Controller 可能会保留在不稳定状态。

如果要从 7.6 Controller 的基础版本 (RTM) 进行升级，请安装 LTSR Controller 的所有组件。

如果要从 Delivery Controller 7.6.1 (Controller Hotfixes Update 1) 或 Delivery Controller 7.6.2 (Controller Hotfixes Update 2) 进行升级，请仅安装 LTSR 版本中的新组件（与已安装的早期版本相比）。不需要按照特定顺序安装各个组件。

- 要成功升级，服务器不得设置注册表修改限制。
- 有关安装 XenDesktop/XenApp 7.x Controller 更新的补充信息，请参阅 [CTX201988](#)。

#### 从 Delivery Controller 7.6.2 (Controller Hotfixes Update 2) 进行升级

警告。根据设计，Broker Service (BrokerSrv760WX64003.msi) 组件会修改您的站点数据存储的 Broker DbSchema。这些修改具有永久性和不可逆转性。如果您因任何原因决定稍后卸载 Broker Service 组件，这些修改不会自动还原。以防万一，Citrix 强烈建议您先备份站点数据存储，然后再安装 Broker Service 组件。这样将允许您将站点数据存储手动还原到备份的版本。即使这样，您在备份和还原站点数据存储期间对其所做的所有更改都将丢失。有关备份和还原数据存储的信息，请参阅 [CTX135207](#)。

仅当至少创建了一个站点时，才能成功更新 DbSchema。如果尚未创建站点，请先至少创建一个站点，然后再安装此更新。否则，安装将无法更新现有 DbSchema，并且您需要重新构建 XenDesktop。

注意：升级到本版本后，系统将显示一条针对 Citrix Studio 中的许可证服务器兼容性检查的提示，用于确保您的许可证服务器为所需版本。如果使用的是随 XenDesktop 7.6 发布的许可证服务器或更新版本中的许可证服务器，则不需要升级许可证服务器。单击“继续”以继续升级 DBschema。

1. 务必确认从 7.6.2 Controller 进行升级。否则，请参阅下文“从 Delivery Controller 7.6.1 或 7.6 进行升级”。
2. 确保至少存在一个站点。
3. 备份您的站点数据存储。
4. 将发行包复制到网络上的共享文件夹。
5. 保存要更新的 Delivery Controller 上的组件 msi 文件。
6. 运行 .msi 文件。
7. 重新启动 Delivery Controller（即使系统未提示也需要重新启动）。
8. 要升级到本版本安装的最新 DbSchema，请转至 Citrix Studio 的“控制板”，然后单击“升级”。

#### 从 Delivery Controller 7.6.1 或 7.6 进行升级

注意。本部分不适用于从 Controller 7.6.2 进行升级。

警告。根据设计，Broker Service (BrokerSrv760WX64003.msi) 和 Host Service (HostSrv760WX64003.msi) 组件会分别修改您的站点数据存储的 Broker 和主机 DbSchema。这些修改具有永久性和不可逆转性。如果您因任何原因决定稍后卸载 Broker Service 或 Host Service 组件，这些修改不会自动还原。以防万一，Citrix 强烈建议您先备份站点数据存储，然后再安装 Broker Service 和 Host Service 组件。这样将允许您将站点数据存储手动还原到备份的版本。即使这样，您在备份和还原站点数据存储期间对其所做的所有更改都将丢失。有关备份和还原您的数据存储的信息，请参阅 [CTX135207](#)。

仅当至少创建了一个站点时，才能成功更新 DbSchema。如果尚未创建站点，请先至少创建一个站点，然后再安装此更新。否则，安装将无法更新现有 DbSchema，并且您需要重新构建 XenDesktop。

注意。升级到本版本后，系统将显示一条针对 Citrix Studio 中的许可证服务器兼容性检查的提示，用于确保您的许可证服务器为所需版本。如果使用的是随 XenDesktop 7.6 发布的许可证服务器或更新版本中的许可证服务器，则不需要升级许可证服务器。单击“继续”以继续升级 DBschema。

1. 确保至少存在一个站点。
2. 备份您的站点数据存储。
3. 将发行包复制到网络上的共享文件夹。
4. 保存要更新的 Delivery Controller 上的组件 msi 文件。

5. 运行 .msi 文件。
6. 重新启动 Delivery Controller (即使系统未提示也需要重新启动)。
7. 要升级到本版本安装的最新 DbSchema , 请转至 Citrix Studio 的“控制板” , 然后单击“升级”。

卸载 Delivery Controller 组件以及还原到早期版本的组件和站点数据存储

1. 从“ARP”/“程序和功能”中卸载组件。
2. 按 [CTX135207](#) 中所述还原数据存储。
3. 安装所需的组件版本 (基础版本或更高版本)。
4. 重新启动 Controller (即使系统未提示也需要重新启动)。

## Citrix Studio 7.6 Update 3

LTSR 版本 : Citrix Studio 7.6 Update 3

本版本最初是在 2015 年 10 月 29 日作为修补程序 DStudio760WX64003 发布的 ; 修补程序 DStudio760WX86003

### 系统要求

#### 已修复的问题

- [64 位](#)
- [32 位](#)

#### 已知问题

如果升级过程中 Citrix Studio 处于打开状态 , 并且您在此修补程序的安装向导的“正在使用的文件”页面上选择设置“关闭应用程序并尝试重新启动” , 则可能会显示以下消息 :

“Setup was unable to automatically close all requested applications. Please ensure that the applications holding files in use are closed before continuing with the installation. (安装程序无法自动关闭所有请求的应用程序。请务必先关闭正在使用文件的应用程序 , 然后再继续安装。)

如果显示此消息 , 您可以安全地将其关闭并单击“确定”以继续安装。

#### 安装/升级

下载 Citrix Studio 的 LTSR 版本并按照 [CTX201572](#) 中提供的安装说明进行操作。

## Citrix Director 7.6.300

LTSR 版本 : Director 7.6.300

本版本最初是在 9 月 30 日作为 Feature Pack 3 的一部分发布的 (Director\_7.6.300.zip)

### 系统要求

请确保您已在 IIS 中选中所有必需的功能。有关完整列表 , 请参阅 [CTX142260](#)。安装 Citrix Group Policy Management 组件 (如果尚未安装)。

#### 已修复的问题

#### 安装/升级

将 Citrix Director 的 LTSR 版本下载到运行 Director 的服务器并按照 [Director](#) 上的说明进行操作。

## Group Policy Management 7.6.300 (2.5)

LTSR 版本 : Group Policy Management 7.6.300

本版本最初是在 9 月 30 日作为 Feature Pack 3 的一部分发布的 (CitrixGroupPolicyManagement\_7.6.300.zip)

系统要求 :

运行 Windows 7、Windows 8、Windows 8.1、Server 2008 R2、Server 2012 或 Server 2012 R2 的计算机

VDA 中新增和增强的 HDX 技术功能使用更新后的 Group Policy Management 软件包进行管理。注意 : 安装后, 此组件在“程序和功能”中显示为版本 2.5.0.0。

安装/升级

需要在安装了 Director 的系统中安装 Citrix Group Policy Management, 以使策略在“用户详细信息”视图中显示。在运行 Director 的服务器上下载并安装 Citrix Group Policy Management (Citrix Policy) 的 LTSR 版本。下一步, 请启动 Studio 或 GPMC, 此时将显示新策略和更新后的策略。

有关更新后的策略的详细信息, 请参阅[视觉显示策略设置](#), 了解增强的 Thinwire 兼容模式; 参阅[USB 设备策略设置](#), 了解签名设备和绘图平板电脑支持; 参阅[Flash 重定向和多媒体策略设置](#), 了解视频回退防护。

## StoreFront 3.0.1

LTSR 版本 : 3.0.1

本版本最初是在 2015 年 9 月 30 日作为 Feature Pack 3 的一部分发布的 (CitrixStoreFront-x64.exe)

系统要求

已修复的问题

已知问题

安装/升级

将 StoreFront 的 LTSR 版本下载到 StoreFront 服务器并按照[升级说明](#)进行操作。

## Provisioning Services 7.6 Update 1

LTSR 版本 : Provisioning Services 7.6 Update 1 (面向服务器和控制台的 Provisioning Services 7.6 累积更新 1) ;  
PVS760TargetDeviceWX64001.zip、PVS760TargetDeviceWX86001.zip

本版本最初是在 2015 年 9 月 15 日作为 PVS760ConsoleServerWX86001.zip 发布的; PVS760ConsoleServerWX64001.zip

Provisioning Services 7.6 Update 1 中包含在基础 7.6 版本中发现的 40 多个问题的修复。

系统要求

已修复的问题

- 控制台、服务器 ([64 位 | 32 位](#))
- 目标设备 ([64 位 | 32 位](#))

## 安装/升级

下载 Provisioning Services 的 LTSR 版本并按照[安装 Provisioning Services 控制台软件](#)（控制台）、[安装 Provisioning Services 服务器软件](#)（服务器）和[CTX135746](#)（目标设备）中的安装说明进行操作。

## Session Recording 7.6.100

LTSR 版本：7.6.100

本版本最初是在 2015 年 6 月 30 日作为 Feature Pack 2 的一部分发布的 (SessionRecording7.6.100.zip)

作为 Feature Pack 2 的一部分发布的 Session Recording 7.6.100 包括以下新增功能和增强功能。

- 可以在安装 Session Recording 数据库组件时指定数据库的连接凭据。
- 可以在安装 Session Recording 数据库和 Session Recording Server 组件时测试数据库的连接性，在安装 Session Recording Agent 组件时测试 Session Recording Server 的连接性。
- 安装 Session Recording 数据库无需具备 Microsoft Shared Management Objects。
- Citrix 体验改善计划 (CEIP) 集成到 Session Recording 中。有关详细信息，请参阅关于 Citrix 客户体验改善计划。升级过程中保留现有设置。

## 系统要求

### 安装/升级

下载 LTSR 版本，然后按照[升级说明](#)进行操作。

在 LTSR 部署中使用时 Session Recording 7.6.100 的已知问题：

- Microsoft 画图会话的录制件无法在 Session Recording Player 中正确播放。[#0604700]
- 播放在多显示器用户设备上录制的会话时出现错误。[#0605129]

## 通用打印服务器 7.6.300

LTSR 版本：7.6.300

本版本最初是在 2015 年 9 月 30 日作为 Feature Pack 3 的一部分发布的 (UpsServer\_7.6.300.zip)

注意：通用打印服务器由客户端和服务器组件组成。客户端组件作为 VDA 的一部分进行安装；因此，LTSR 版本中不包含任何客户端安装文件。在服务器端，LTSR 不支持在 32 位 Windows 操作系统中安装通用打印服务器；因此，仅包含 64 位服务器安装程序。

## 系统要求

### 已修复的问题

### 安装/升级

通用打印服务器包中包含更新版本的独立 UPS 服务器组件 (UpsServer\_x64.msi) 和必备的 vcredist\_x64.exe、vcredist\_x86.exe 和 cdf\_x64.msi 文件。

- 将 LTSR 版本下载到 Windows 2008 R2 SP1、Windows Server 2012 或 Windows Server 2012 R2 打印服务器。
- 安装必备的 vcredist\_x64.exe、vcredist\_x86.exe 和 cdf\_x64.msi 文件。

3. 安装通用打印服务器组件 UpsServer\_x64.msi。

4. 安装通用打印服务器组件后重新启动服务器。

通用打印客户端组件属于 VDA 安装的一部分。因此，不需要手动安装客户端组件，并且客户端组件不作为 LTSR 版本的独立组件包括在内。

有关详细信息，请参阅[预配打印机](#)。

## HDX Flash 重定向

HDX Flash 重定向功能可将大部分 Adobe Flash 内容（包括动画、视频和应用程序）处理工作转移到连接至 LAN 和 WAN 的用户 Windows 设备，从而降低服务器和网络的工作负载。这样将提供更高的可扩展性，同时确保获得高清晰度用户体验。

客户端组件作为桌面和服务器操作系统 VDA 的一部分进行安装。因此，升级到 VDA 的 LTSR 版本会将您的部署升级到最新版本的 HDX Flash 重定向。

不需要安装任何服务器端组件。但是，配置 Flash 重定向时，必须同时设置服务器端和客户端。有关配置 Flash 重定向的信息，请参阅[Flash 重定向](#)。有关 HDX Flash 最新更新的兼容性，请参阅 [CTX136588](#)。

# 本版本中不提供的功能

Oct 04, 2016

## 已弃用的功能

XenApp 和 XenDesktop 7.6 LTSR 基于 XenApp 和 XenDesktop 7.6 RTM。版本 7.6 RTM 中已弃用以下功能，并会在 LTSR 中继续弃用：

- **启动触控优化桌面** - 此设置已针对 Windows 10 计算机禁用。有关详细信息，请参阅 [移动体验策略设置](#)。
- **低于 128 位的安全 ICA 加密** - 在 7.x 之前的版本中，可以使用安全 ICA 加密客户端连接，以实现基本加密、40 位、56 位和 128 位加密。在 7.x 版本中，安全 ICA 加密仅适用于 128 位加密。
- **旧版打印** - 7.x 版本不支持以下打印功能：
  - 向后兼容 DOS 客户端和 16 位打印机，包括旧版客户端打印机名称。
  - 支持连接到 Windows 95 和 Windows NT 操作系统的打印机，包括增强型扩展打印机属性和 Win32FavorRetainedSetting。
  - 启用或禁用自动保留和自动恢复的打印机的功能。
  - DefaultPrnFlag。这是服务器上用于启用或禁用自动保留和自动恢复的打印机的一项注册表设置，存储在服务器上的用户配置文件中。
- **Secure Gateway** - 在 7.x 之前的版本中，Secure Gateway 是用于在服务器和用户设备之间提供安全连接的选项。NetScaler Gateway 是用于确保外部连接安全的替代选项。
- **重影用户** - 在 7.x 之前的版本中，管理员通过设置策略控制用户对用户重影操作。在 7.x 版本中，重影最终用户是 Director 组件的一项集成功能，该功能使用 Microsoft 远程协助来允许管理员重影和解决与已交付的无缝应用程序和虚拟桌面有关的问题。
- **电源和容量管理** - 在 7.x 之前的版本中，可以使用电源和容量管理功能来降低电耗并管理服务器容量。Microsoft Configuration Manager 工具替代了此功能。
- **Flash v1 重定向** - 不支持第二代 Flash 重定向的客户端（包括 3.0 之前的 Receiver for Windows 版本、11.100 之前的 Receiver for Linux 版本以及 Citrix Online Plug-in 12.1）将回退到服务器端呈现，以实现旧版 Flash 重定向功能。7.x 版本中包括的 VDA 支持第二代 Flash 重定向功能。
- **本地文本回显** - 此功能与早期的 Windows 应用程序技术结合使用，用于在高延迟连接中，在用户设备上加速显示输入文本。由于图形子系统和 HDX SuperCodec 的功能得以增强，因此 7.x 版本中不提供此功能。
- **Smart Auditor** - 在 7.x 之前的版本中，可以通过 Smart Auditor 录制用户会话的屏幕活动。7.x 版本中不提供此组件。在 7.6 Feature Pack 1 中，被 Session Recording 取代。
- **单点登录** - 此功能可以保证密码安全，但在 Windows 8 和 Windows Server 2012 环境中不受支持。在 Windows 2008 R2 和 Windows 7 环境中仍然支持此功能，但 7.x 版不提供此功能。可以在 Citrix 下载 Web 站点找到此功能：<http://citrix.com/downloads>。
- **Oracle 数据库支持** - 7.x 版需要使用 SQL Server 数据库。
- **运行状况监视与恢复 (HMR)** - 在 7.x 之前的版本中，HMR 可以在服务器场中的服务器上运行测试，以监视它们的状态并发现任何运行状况风险。在 7.x 版本中，Director 从 Director 控制台监视整个基础结构并提供警报，从而提供了一种从中央位置查看系统运行状况的方式。
- **自定义 ICA 文件** - 自定义 ICA 文件用于从用户设备（使用 ICA 文件）直接连接到特定计算机。在 7.x 版本中，此功能默认处于禁用状态。但在正常情况下，可以通过本地组将其启用。在 Controller 不可用时，还可以在高可用性模式中使用该功能。
- **Management Pack for System Center Operations Manager (SCOM) 2007** - 该管理包之前使用 SCOM 监视场的活动，但不支持 7.x 版本。
- **CNAME 功能** - 在 7.x 之前的版本中，CNAME 功能默认处于启用状态。如果部署依赖于 CNAME 记录进行 FQDN 重新路由并且使用 NETBIOS 名称，则可能会失败。在 7.x 版本中，Delivery Controller 自动更新是其替代功能，该功能可以动态更新 Controller 的列表，并且还可以在向站点添加 Controller 或从站点删除 Controller 时自动向 VDA 发送通知。Controller 自动

更新功能在 Citrix 策略中默认处于启用状态，但可以通过创建策略禁用该功能。

或者，也可以在注册表中重新启用 CNAME 功能，以继续使用现有部署并允许 FQDN 重新路由和使用 NETBIOS 名称。有关详细信息，请参阅 [CTX137960](#)。

- **快速部署向导** - 在 7.x 之前的 Studio 版本中，利用此选项可以对完整安装的 XenDesktop 部署进行快速部署。7.x 版本中提供简化的全新安装和配置工作流程，不需要再使用“快速部署”向导选项。
- **用于实现自动管理的 Remote PC Service 配置文件和 PowerShell 脚本** - Remote PC 现在已集成到 Studio 和 Controller 中。
- **Workflow Studio** - 在 7.x 之前的版本中，Workflow Studio 是用于 XenDesktop 的工作流组合的图形界面。7.x 版本不支持此功能。
- **颜色深度** - 在 7.6 之前的 Studio 版本中，此选项位于交付组“用户设置”页面，用于设置交付组的颜色深度。在 7.6 版本中，可以使用 New-BrokerDesktopGroup 或 Set-BrokerDesktopGroup PowerShell cmdlet 设置颜色深度。
- **在客户端连接期间启动非发布程序** - 在 7.x 之前的版本中，此 Citrix 策略设置指定是否在服务器上通过 ICA 或 RDP 启动初始应用程序或已发布的应用程序。在 7.x 版本中，此设置仅指定是否在服务器上通过 RDP 启动初始应用程序或已发布的应用程序。
- **桌面启动** - 在 7.x 之前的版本中，Citrix 策略设置指定非管理员用户是否可以连接到桌面会话。在 7.x 版本中，非管理员用户必须属于 VDA 计算机的直接访问用户组才能连接到此 VDA 上的会话。**桌面启用**设置使 VDA 直接访问用户组的非管理员用户可以使用 ICA 连接连接到 VDA。**桌面启动**设置不会影响 RDP 连接；无论是否启用了此设置，VDA 直接访问用户组的用户均可通过 RDP 连接来连接到 VDA

## Receiver 中未提供或具有不同默认值的功能

- **Citrix Receiver Enterprise Edition 和脱机插件** - Citrix Receiver Enterprise Edition 和脱机插件都已结束使用。这两个产品不会作为 LTSR 安装程序的一部分进行更新。我们欢迎客户改为部署最新版本的 Citrix Receiver for Windows。
- **COM 端口映射** - COM 端口映射可允许或阻止访问用户设备上的 COM 端口。在之前版本中，COM 端口映射默认处于启用状态。在 XenDesktop 和 XenApp 的 7.x 版本中，COM 端口映射默认处于禁用状态。有关详细信息，请参阅[使用注册表配置 COM 端口和 LPT 端口重定向设置](#)。
- **LPT 端口映射** - LPT 端口映射控制旧版应用程序对 LPT 端口的访问。在之前版本中，LPT 端口映射默认处于启用状态。在 7.x 版本中，LPT 端口映射默认处于禁用状态。
- **PCM 音频编解码器** - 在 7.x 版本中，只有 HTML5 客户端支持 PCM 音频编解码器。
- **支持 Microsoft ActiveSync**。
- **针对旧版本的代理支持** - 包括：
  - Microsoft Internet Security and Acceleration (ISA) 2006 (Windows Server 2003)。
  - Oracle iPlanet Proxy Server 4.0.14 (Windows Server 2003)。
  - Squid Proxy Server 3.1.14 (Ubuntu Linux Server 11.10)。

# 已知问题

Aug 15, 2018

## 累积更新 6 中的已知问题

尝试使用 metainstaller 从 StoreFront 2.5、2.6 或 3.0.1 版升级到任意适用于 XenApp 和 XenDesktop 7.6 LTSR 的累积更新随附的任何 StoreFront 版本都会失败。升级过程中 StoreFront 管理控制台处于打开状态或者 PowerShell 会话正在运行但不发出警告时会出现此问题。[LCM-4801]

## 累积更新 5 中的已知问题

尝试从 StoreFront 2.5 或 2.6 版升级到任意适用于 XenApp 和 XenDesktop 7.6 LTSR 的累积更新随附的任何 StoreFront 版本都会失败。升级过程中 StoreFront 管理控制台处于打开状态或者 PowerShell 会话正在运行但不发出警告时会出现此问题。此问题仅限于运行 Windows 2012 R2 Server 并且安装了 .NET 4.6 或 .NET 4.7 更新的系统。[#3283]

## 累积更新 4 中的已知问题

迄今为止在 CU4 中未发现任何新问题。

## 累积更新 3 中的已知问题

迄今为止在 CU3 中未发现任何新问题。

## 累积更新 2 中的已知问题

- 尝试使用 PowerShell SDK 手动更新 XenDesktop 5.6、7.1、7.5 或 XenApp 7.5 部属可能无法升级一个或多个 DBSchema。解决方法：不使用 PowerShell SDK，而是从 Citrix Studio 使用自动或手动站点升级方法，升级 Site DBschema。

[#LCM-903]

- 使用 Citrix Receiver for Linux 时，HDX Flash 重定向可能会回退到服务器端呈现，且 Web 站点被添加到动态黑名单。解决方法：使用模拟模式。

[#LCM-944]

- Citrix Studio 可能在启动时意外退出。如果您在以前更新了 Microsoft 文章 [KB3163251](#) 和 KB3135996v2 的单一 Windows 2008 R2 SP1 系统上安装了 Studio 和 StoreFront，则会出现该问题。以下错误消息在事件查看器中显示：

.NET Runtime version 2.0.50727.5485 - Fatal Execution Engine Error. (.NET Runtime 版本 2.0.50727.5485 - 致命执行引擎错误。)

解决方法：从命令行运行以下提示：

“C:\windows\microsoft.net\framework64\v2.0.50727\ngen update /force”

[#LCM-969]

- 尝试安装 VDA for Server OS 可能会失败，并生成一般性错误代码 1603。有关详细信息（包括解决方法），请参阅知识中心文章 [CTX213807](#)。

[#LCM-1013]

- 注意：此问题在 CU4 中已通过 #LC6934 解决。

某些 Web 站点（包括 Qumu）会自动加入黑名单，并回退到服务器端内容呈现。解决方法：保持受影响的站点在黑名单中，并在 VDA 上设置以下注册表项：

HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer

名称：SupportedUrlHeads

类型：REG\_MULTI\_SZ

数据：<每个值都位于单独的一行，以空值分隔：>

http://

https://

file://

[#LCM-1605]

- 注意：此问题在 CU3 中已通过 #LC6471 解决。

安装 StoreFront 3.0.1000 或 3.0.2000 后，管理控制台无法启动并显示以下错误消息：The Management console is unavailable because of a root certificate missing, go to verisign and download the certificate - Verisign class primary CA - G5.（由于缺少根证书，管理控制台不可用，请转至 Verisign 并下载证书 - Verisign 类主 CA - G5。）有关详细信息，请参阅知识中心文章 [CTX218815](#)。

[#LC6471]

- 注意：此问题在 CU3 中已通过 #LC6816 解决。

将 StoreFront 从版本 2.5 升级到版本 3.0.2000 失败，错误为 1603。有关详细信息，请参阅知识中心文章 [CTX220411](#)。

[#LC6816]

## 累积更新 1 中的已知问题

- 如果使用此组件版本的独立 msi（不建议）安装此组件，而不是通过 Metainstaller 安装，将出现一条指示在 Desktop

Studio 中进行许可证服务器兼容性检查的提示，以确保您的许可证服务器是所需版本。如果使用的是随 XenApp/Desktop 7.6 发布的许可证服务器或更新版本中的许可证服务器，则不需要升级许可证服务器。单击“继续”以继续升级 DBschema。

[#575064]

- 当升级以前使用 Active Directory 部署的许可证服务器 11.12.1 版本（包含在 XenApp/XenDesktop 7.6 RTM 版本中）实例时，Citrix Licensing 和 Citrix Licensing Support Service 均会被禁用。

为避免此问题，请首先使用 citrixlicensing.exe 从 CU1 介质安装许可证服务器 11.13.1 版本，然后再安装 CU1 的其余部分。

[#630116]

- 注意：此问题在 CU2 中已通过 #630814 解决。

在选择“使用现有许可证”时，可能无法继续进行 Citrix Studio 中的站点设置。解决方法：在许可证服务器上重新启动“Citrix Web Services for Licensing”服务来完成其配置。

[#630814]

- 如果使用组件的独立 msi（不建议）安装此版本组件，而不是通过 Metainstaller 安装，Citrix Scout 将为此组件显示两个条目。

[#636862]

- 注意：此问题在 CU3 中已通过 #LC6471 解决。

安装 StoreFront 3.0.1000 或 3.0.2000 后，管理控制台无法启动并显示以下错误消息：The Management console is unavailable because of a root certificate missing, go to verisign and download the certificate - Verisign class primary CA - G5.（由于缺少根证书，管理控制台不可用，请转至 Verisign 并下载证书 - Verisign 类主 CA - G5。）有关详细信息，请参阅知识中心文章 [CTX218815](#)。

[#LC6471]

- 注意：此问题在 CU3 中已通过 #LC6816 解决。

将 StoreFront 从版本 2.5 升级到版本 3.0.2000 失败，错误为 1603。有关详细信息，请参阅知识中心文章 [CTX220411](#)。

[#LC6816]

## LTSR 中的已知问题

- 尝试更新 XenApp 6.5 服务器使其成为 VDA for Server OS 可能会失败。以控制器和会话-主机模式安装的 XenApp 6.5 服务器上会发生该问题，因为 Citrix XML Service 与 IIS 服务器共享公用端口。

解决方法：卸载 XenApp 6.5 服务器，重新启动服务器，然后安装 LTSR 或其最新累积更新。有关详细信息，请参阅[将](#)

XenApp 6.5 工作进程升级至新的 VDA for Windows Server OS。

[#LCM-893]

- 注意：此问题在 LTSR CU2 VDA 中已通过 #LC5098 解决。

将 VDA 升级到 7.6 LTSR (7.6.300) 后，基于 DirectShow 的应用程序（例如 QUMU 和 QVOP）的客户端内容重定向不起作用，并且视频无法呈现。

[#LC5098-x]

- VDA Metainstaller 不再包含或更新以下 Citrix 客户端：

- Citrix Receiver for Windows Enterprise Edition
- 脱机插件

这两个客户端已到达[生命周期结束](#)。可以从 <https://www.citrix.com/downloads/citrix-receiver.html> 下载最新版本的 Citrix Receiver。

[#XA-1532]

- 在虚拟桌面中选择的通用打印服务器打印机不会在 Windows“控制面板”的设备和打印机窗口中显示。但是，当用户在使用应用程序时，可以使用这些打印机进行打印。此问题仅出现在 Windows Server 2012、Windows 10 和 Windows 8 平台上。有关详细信息，请参阅知识中心文章 [CTX213540](#)。[#335153]

# 系统要求

Dec 15, 2017  
在本文中：

[Session Recording](#)

[Delivery Controller](#)

[数据库](#)

[Studio](#)

[Director](#)

[Virtual Delivery Agent \(VDA\) for Windows Desktop OS](#)

[Virtual Delivery Agent \(VDA\) for Windows Server OS](#)

[主机/虚拟化资源](#)

[Active Directory 功能级别支持](#)

[HDX - 桌面组合重定向](#)

[HDX - Windows Media 交付](#)

[HDX - Flash 重定向](#)

[HDX 3D Pro](#)

[HDX - 视频会议对网络摄像机视频压缩的要求](#)

[HDX - 其他](#)

[通用打印服务器的要求](#)

[其他要求](#)

本文档中的系统要求适用于此发布版本的产品。本文档中未涉及的组件（例如 StoreFront、主机系统、Receiver 和插件以及 Provisioning Services）的系统要求在其相应文档中进行说明。

**重要：**请在开始安装之前，阅读[准备安装](#)。

除非另有说明，否则组件安装程序将自动部署必备软件（如果未在计算机上检测到），例如 .NET 和 C++ 软件包。Citrix 安装介质还包含部分必备软件。

安装介质包含多个第三方组件。使用 Citrix 软件之前，请检查是否存在第三方安全更新并进行安装。

磁盘空间值仅为估计值，且是除产品映像、操作系统和其他软件所需空间以外的额外空间。

如果在单个服务器上安装所有核心组件（包括 Controller、SQL Server Express、Studio、Director、StoreFront 和 Licensing），最低需要 3 GB RAM 才能评估产品；建议为用户运行环境时使用更多 RAM。性能会因为您的具体配置而有所不同，包括用户数量、应用程序、桌面以及其他因素。

**重要：**在 Windows Server 2012 R2 系统上安装 XenApp 后，使用 Kerberos Enable Tool (XASSonKerb.exe) 以确保 Citrix Kerberos 身份验证正确运行。此工具位于安装介质上的“Support”（支持）>“Tools”（工具）>“XASSonKerb”文件夹中；必须具有本地管理员权限才能使用此工具。要确保 Kerberos 正确运行，请从服务器上的命令提示窗口运行 xassonkerb.exe -install。如果稍后应用更改注册表位置 HKLM\System\CurrentControlSet\Control\LSA\OSConfig 的更新，请重新运行命令。要查看所有可用工具选项，请运行带有 –help 参数的命令。

## Session Recording

[Session Recording Administration 组件](#)

可以将 Session Recording Administration 组件（Session Recording 数据库、Session Recording Server、Session Recording 策略控制台）安装在单台服务器或不同的服务器上。

### Session Recording 数据库

支持的操作系统：

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- 带有 Service Pack 1 的 Microsoft Windows Server 2008 R2

要求：

- .NET Framework Version 3.5 Service Pack 1（仅限 Windows Server 2008 R2）或 .NET Framework 4.5.2 或 4.6。

### Session Recording Server

支持的操作系统：

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012；带 Service Pack 1 的 Microsoft Windows Server 2008 R2

要求：

启动 Session Recording 安装前，您必须安装某些必备程序。打开服务器管理器并添加 IIS 角色。从以下选项中进行选择：

- 应用程序开发：

- Server 2012 和 Server 2012 R2 上为 ASP.NET 4.5，Server 2008 R2 上为 ASP.NET（其他组件自动选中。单击“添加”接受所需角色）
- 安全性 > Windows 身份验证
- 管理工具 — IIS 6 管理兼容性
  - IIS 6 元数据库兼容性
  - IIS 6 WMI 兼容性
  - IIS 6 脚本工具
  - IIS 6 管理控制台
- .NET Framework Version 3.5 Service Pack 1（仅限 Windows Server 2008 R2）或 .NET Framework 4.5.2 或 4.6。
- 如果 Session Recording Server 使用 HTTPS 作为其通信协议，请添加有效证书。默认情况下，Session Recording 使用 HTTPS（Citrix 推荐）。
- Microsoft 消息队列 (MSMQ)，Active Directory 集成处于禁用状态，MSMQ HTTP 支持处于启用状态。

## Session Recording 策略控制台

支持的操作系统：

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- 带有 Service Pack 1 的 Microsoft Windows Server 2008 R2

要求：

- .NET Framework Version 3.5 Service Pack 1（仅限 Windows Server 2008 R2）或 .NET Framework 4.5.2 或 4.6。

## Session Recording Agent

在要录制会话的每台 XenApp 和 XenDesktop 服务器上安装 Session Recording Agent。

支持的操作系统：

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- 带有 Service Pack 1 的 Microsoft Windows Server 2008 R2

要求：

- Microsoft 消息队列 (MSMQ)，Active Directory 集成处于禁用状态，MSMQ HTTP 支持处于启用状态
- .NET Framework Version 3.5 Service Pack 1（仅限 Windows Server 2008 R2）或 .NET Framework 4.5.2 或 4.6。

## Session Recording Player

支持的操作系统：

- Microsoft Windows 8.1
- Microsoft Windows 8
- Microsoft Windows 7 Service Pack 1

要获得最佳结果，在以下工作站上安装 Session Recording Player：

- 屏幕分辨率为 1024 x 768
- 颜色深度至少为 32 位
- 内存：1GB RAM（最低要求）。更多 RAM 和 CPU/GPU 资源可提高播放图形密集型录制件时的性能，特别是当录制件中有大量动画时。

搜寻响应时间取决于录制件的大小和计算机的硬件规格。

要求：

- .NET Framework 3.5 Service Pack 1 或 .NET Framework 4.5.2 或 4.6。

## Session Recording Administration 组件

可以将 Session Recording Administration 组件（Session Recording 数据库、Session Recording Server、Session Recording 策略控制台）安装在单台服务器或不同的服务器上。

## Session Recording 数据库

支持的操作系统：

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- 带有 Service Pack 1 的 Microsoft Windows Server 2008 R2

要求：

- .NET Framework Version 3.5 Service Pack 1（仅限 Windows Server 2008 R2）或 .NET Framework 4.5.2 或 4.6。

## Session Recording Server

支持的操作系统：

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012；带有 Service Pack 1 的 Microsoft Windows Server 2008 R2

要求：

启动 Session Recording 安装前，您必须安装某些必备程序。打开服务器管理器并添加 IIS 角色。从以下选项中进行选择：

- 应用程序开发：
  - Server 2012 和 Server 2012 R2 上为 ASP.NET 4.5，Server 2008 R2 上为 ASP.NET（其他组件自动选中。单击“添加”接受所需角色）
- 安全性 > Windows 身份验证
- 管理工具 — IIS 6 管理兼容性
  - IIS 6 元数据库兼容性
  - IIS 6 WMI 兼容性
  - IIS 6 脚本工具
  - IIS 6 管理控制台
- .NET Framework Version 3.5 Service Pack 1（仅限 Windows Server 2008 R2）或 .NET Framework 4.5.2 或 4.6。
- 如果 Session Recording Server 使用 HTTPS 作为其通信协议，请添加有效证书。默认情况下，Session Recording 使用 HTTPS（Citrix 推荐）。
- Microsoft 消息队列 (MSMQ)，Active Directory 集成处于禁用状态，MSMQ HTTP 支持处于启用状态。

## Session Recording 策略控制台

支持的操作系统：

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- 带有 Service Pack 1 的 Microsoft Windows Server 2008 R2

要求：

- .NET Framework Version 3.5 Service Pack 1（仅限 Windows Server 2008 R2）或 .NET Framework 4.5.2 或 4.6。

## Session Recording Agent

在要录制会话的每台 XenApp 和 XenDesktop 服务器上安装 Session Recording Agent。

支持的操作系统：

- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- 带有 Service Pack 1 的 Microsoft Windows Server 2008 R2

要求：

- Microsoft 消息队列 (MSMQ)，Active Directory 集成处于禁用状态，MSMQ HTTP 支持处于启用状态
- .NET Framework Version 3.5 Service Pack 1（仅限 Windows Server 2008 R2）或 .NET Framework 4.5.2 或 4.6。

## Session Recording Player

支持的操作系统：

- Microsoft Windows 8.1
- Microsoft Windows 8
- Microsoft Windows 7 Service Pack 1

要获得最佳结果，在以下工作站上安装 Session Recording Player：

- 屏幕分辨率为 1024 x 768
- 颜色深度至少为 32 位
- 内存：1GB RAM（最低要求）。更多 RAM 和 CPU/GPU 资源可提高播放图形密集型录制件时的性能，特别是当录制件中有大量动画时。

搜寻响应时间取决于录制件的大小和计算机的硬件规格。

要求：

- .NET Framework 3.5 Service Pack 1 或 .NET Framework 4.5.2 或 4.6。

## Delivery Controller

支持的操作系统：

- Windows Server 2012 R2 Standard Edition 和 Datacenter Edition。
- Windows Server 2012 Standard Edition 和 Datacenter Edition
- Windows Server 2008 R2 SP1 Standard Edition、Enterprise Edition 和 Datacenter Edition

要求：

- 磁盘空间：100 MB。连接租用（默认情况下启用）包含在此要求内；具体大小取决于用户和应用程序的数量以及模式（RDS 或 VDI）。例如，100,000 个 RDS 用户和 100 个最近使用的应用程序需要大约 3 GB 的空间用于连接租用；具有更多应用程序的部署可能需要更大的空间。对于专用 VDI 桌面，40,000 个桌面至少需要 400-500 MB。建议在任何情况下都提供多个 GB 级额外空间。
- Microsoft .NET Framework 3.5.1（仅限 Windows Server 2008 R2）。
- Microsoft .NET Framework 4.5.2、4.6、4.6.1
- Windows PowerShell 2.0（随 Windows Server 2008 R2 提供）或 3.0（随 Windows Server 2012 R2 和 Windows Server 2012 提供）。
- Visual C++ 2005、2008 SP1 和 2010 可再发行组件包。

## 数据库

站点配置数据库（最初包括配置日志记录数据库和监视数据库）支持的 Microsoft SQL Server 版本：

- SQL Server 2017 Express Edition、Standard Edition 和 Enterprise Edition。
- SQL Server 2016 Express Edition、Standard Edition 和 Enterprise Edition。
- SQL Server 2014 到 SP2 Express Edition、Standard Edition 和 Enterprise Edition。
- SQL Server 2012 到 SP3 Express Edition、Standard Edition 和 Enterprise Edition。默认情况下，如果未检测到支持的现有 SQL Server 安装，安装 Controller 时将安装 CU4、SQL Server 2012 SP1 Express。截至 CU4，如果未检测到支持的现有 SQL Server 安装，安装 Controller 时将安装 SQL Server 2012 SP3 Express。
- SQL Server 2008 R2 SP2 和 SP3 Express Edition、Standard Edition、Enterprise Edition 以及 Datacenter Edition。

支持下列数据库功能（SQL Server Express 除外，此版本仅支持独立模式）：

- SQL Server 群集实例
- SQL Server 镜像
- SQL Server AlwaysOn 可用性组（包括 Basic 可用性组）

Controller 与 SQL Server 数据库之间的连接需要 Windows 身份验证。

有关受支持的最新数据库版本的信息，请参阅[CTX114501](#)。

## Studio

支持的操作系统：

- Windows 8.1 Professional Edition 和 Enterprise Edition
- Windows 8 Professional Edition 和 Enterprise Edition
- Windows 7 Professional Edition、Enterprise Edition 和 Ultimate Edition
- Windows Server 2012 R2 Standard Edition 和 Datacenter Edition
- Windows Server 2012 Standard Edition 和 Datacenter Edition
- Windows Server 2008 R2 SP1 Standard Edition、Enterprise Edition 和 Datacenter Edition

要求：

- 磁盘空间：75 MB
- Microsoft .NET Framework 4.6.1
- Microsoft .NET Framework 4.5.2、4.6
- Microsoft .NET Framework 3.5 SP1（仅限 Windows Server 2008 R2 和 Windows 7）
- Microsoft Management Console 3.0（随所有支持的操作系统提供）
- Windows PowerShell 2.0（随 Windows 7 和 Windows Server 2008 R2 提供）或 3.0（随 Windows 8.1、Windows 8、Windows Server 2012 R2 和 Windows Server 2012 提供）

## Director

支持的操作系统：

- Windows Server 2012 R2 Standard Edition 和 Datacenter Edition
- Windows Server 2012 Standard Edition 和 Datacenter Edition
- Windows Server 2008 R2 SP1 Standard Edition、Enterprise Edition 和 Datacenter Edition

要求：

- 磁盘空间：50 MB。
- Microsoft .NET Framework 4.5.2、4.6
- Microsoft .NET Framework 3.5 SP1（仅限 Windows Server 2008 R2）
- Microsoft Internet Information Services (IIS) 7.0 和 ASP.NET 2.0。确保 IIS 服务器角色安装了静态内容角色服务。如果尚未安装这些项，系统会提示您插入 Windows Server 安装介质并进行安装。
- 支持查看 Director 的浏览器：
  - Internet Explorer 11 和 10。  
Internet Explorer 不支持兼容模式。您必须使用建议的浏览器设置访问 Director。安装 Internet Explorer 时，接受默认设置以使用建议的安全性和兼容性设置。如果已经安装了浏览器并选择不使用建议的设置，请转到“工具 > Internet 选项 > 高级 > 重置”并按照说明进行操作。
  - Firefox ESR（扩展支持版本）。
  - Chrome。

## Virtual Delivery Agent (VDA) for Windows Desktop OS

支持的操作系统：

有关 Windows 10 兼容性的信息，请参阅我们的[博客](#)。

- Windows 8.1 Professional Edition 和 Enterprise Edition
- Windows 8 Professional Edition 和 Enterprise Edition
- Windows 7 SP1 Professional Edition、Enterprise Edition 和 Ultimate Edition

要使用 Server VDI 功能，可以在支持的服务器操作系统上使用命令行接口安装 VDA for Windows Desktop OS。有关指南，请参阅[Server VDI](#)。

- Windows Server 2012 R2 Standard Edition 和 Datacenter Edition
- Windows Server 2012 Standard Edition 和 Datacenter Edition
- Windows Server 2008 R2 SP1 Standard Edition、Enterprise Edition 和 Datacenter Edition

要求：

- Microsoft .NET Framework 4.5.2、4.6、4.6.1
- Microsoft .NET Framework 3.5.1（仅限 Windows 7）
- Microsoft Visual C++ 2005、2008 和 2010 Runtime（32 位或 64 位）。
- Microsoft Visual C++ 2008、2010 和 2013 Runtime（32 位或 64 位）。适用于 XenApp 和 XenDesktop VDA 独立安装。

Remote PC Access 使用此 VDA（您可将其安装在办公室物理 PC 上）。

多种多媒体加速功能（如 HDX MediaStream Windows Media 重定向）要求在安装 VDA 的计算机上安装 Microsoft 媒体基础。如果该计算机未安装媒体基础，将无法安装和使用多媒体加速功能。请勿在安装 Citrix 软件后从计算机上删除媒体基础；否则，用户将无法登录到此计算机。在大多数 Windows 8.1、Windows 8 和 Windows 7 版本上，已经安装了媒体基础支持，并且无法将其删除。但是，N 版本不包括某些与媒体相关的技术；您可以从 Microsoft 或第三方获取该软件。

在 VDA 安装期间，可以选择安装 HDX 3D Pro 版的 VDA for Windows Desktop OS。此版本特别适合与 DirectX 和 OpenGL 驱动的应用程序以及视频等富媒体结合使用。

## Virtual Delivery Agent (VDA) for Windows Server OS

支持的操作系统：

- Windows Server 2012 R2 Standard Edition 和 Datacenter Edition。
- Windows Server 2012 Standard Edition 和 Datacenter Edition
- Windows Server 2008 R2 SP1 Standard Edition、Enterprise Edition 和 Datacenter Edition

安装程序将自动部署以下必需的组件，这些组件也可以在 Citrix 安装介质上的 Support 文件夹中找到：

- Microsoft .NET Framework 4.5.2、4.6、4.6.1
- Microsoft .NET Framework 3.5.1（仅限 Windows Server 2008 R2）
- Microsoft Visual C++ 2005、2008 和 2010 Runtime（32 位或 64 位）。
- Microsoft Visual C++ 2008、2010 和 2013 Runtime（32 位或 64 位）。适用于 XenApp 和 XenDesktop VDA 独立安装。

如果尚未安装并启用远程桌面服务角色服务，安装程序会自动安装并启用。

多种多媒体加速功能（如 HDX MediaStream Windows Media 重定向）要求在安装 VDA 的计算机上安装 Microsoft 媒体基础。如果该计算机未安装媒体基础，将无法安装和使用多媒体加速功能。请勿在安装 Citrix 软件后从计算机上删除媒体基础；否则，用户将无法登录到此计算机。在大多数 Windows Server 2012 R2、Windows Server 2012 和 Windows Server 2008 R2 版本中，媒体基础功能通过服务器管理器进行安装（对于 Windows Server 2012 R2 和 Windows Server 2012：ServerMediaFoundation；对于 Windows Server 2008 R2：DesktopExperience）。但是，N 版本不包括某些与媒体相关的技术；您可以从 Microsoft 或第三方获取该软件。

## 主机/虚拟化资源

支持的平台

重要：支持以下 major.minor 版本，包括这些版本的更新。[CTX131239](#) 包含最新虚拟机管理程序版本信息，以及已知问题的链接。

XenServer。

- XenServer 7.2
- XenServer 7.1
- XenServer 7.0
- XenServer 6.5 SP1
- XenServer 6.5
- XenServer 6.2 SP1 加上修补程序（必须应用 SP1 才能应用将来的修补程序）
- XenServer 6.1

VMware vSphere (vCenter + ESXi)。不支持 vSphere vCenter“链接模式”操作。

- VMware vSphere 6.5
- VMware vSphere 6.0
- VMware vSphere 5.5
- VMware vSphere 5.1
- VMware vSphere 5.0
- VMware vCenter 5.5/6 设备

System Center Virtual Machine Manager - 包括可以注册到受支持的 System Center Virtual Machine Manager 版本的任意 Hyper-V 版本。

- System Center Virtual Machine Manager 2012 R2
- System Center Virtual Machine Manager 2012 SP1
- System Center Virtual Machine Manager 2012

Nutanix Acropolis 4.5 - 使用此平台时，多项 XenApp 和 XenDesktop 功能不可用；有关详细信息，请参阅 [CTX202032](#)。有关结合使用此产品与 Acropolis 的详细信息，请参阅 <https://portal.nutanix.com/#/page/docs>。

Amazon Web Services (AWS)

- 可以在支持的 Windows 服务器操作系统上置备应用程序和桌面。
- 不支持 Amazon Relational Database Service (RDS)。
- 请参阅 [Citrix XenDesktop on AWS](#) 了解更多信息。

Citrix CloudPlatform

- 支持的最低版本为含修补程序 4.2.1-4 的 4.2.1 版。

- 部署经过 XenServer 6.2（具有 Service Pack 1 和修补程序 XS62ESP1003）和 vSphere 5.1 虚拟机管理程序的测试。
- CloudPlatform 不支持 Hyper-V 虚拟机管理程序。
- CloudPlatform 4.3.0.1 支持 VMware vSphere 5.5。
- 有关其他支持信息和基于 Linux 的系统要求信息，请参阅 CloudPlatform 文档（包括您的 CloudPlatform 版本的发行说明）和 [XenApp and XenDesktop concepts and deployment on CloudPlatform](#)（XenApp 和 XenDesktop 概念和在 CloudPlatform 上的部署）。

Machine Creation Services 以及面向 VM 的运行时 Active Directory 帐户注入功能支持以下虚拟化资源和存储技术的组合。标有星号 (\*) 的组合为推荐组合。

虚拟化资源	本地磁盘	NFS	块存储	存储链接
XenServer	是	是*	是	否
VMware	是（不支持 vMotion 或动态放置）	是*	是	否
Hyper-V	是	否	是*（需要群集共享卷）	否

Remote PC Access 局域网唤醒功能需要 Microsoft System Center Configuration Manager。有关详细信息，请参阅 [Configuration Manager 和 Remote PC Access 局域网唤醒](#)。

## Active Directory 功能级别支持

支持以下 Active Directory 林和域功能级别：

- Windows 2000 本机（不支持域控制器）
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

## HDX - 桌面组合重定向

Windows 用户设备或瘦客户端必须支持或包含：

- DirectX 9
  - Pixel Shader 2.0（硬件支持）
  - 32 位/像素
  - 1.5 GHz 32 位或 64 位处理器
  - 1 GB RAM
  - 图形卡或集成图形处理器上具有 128 MB 视频内存
- HDX 将查询 Windows 设备，以验证设备是否具备所需的 GPU 功能，如果不具备所需功能则自动恢复为服务器端桌面组合。具有所需 GPU 功能、但不符合处理器速度或 RAM 规格要求的设备将列在从桌面组合重定向中排除的设备 GPO 组中。

最小可用带宽为 1.5 Mbps；建议带宽为 5 Mbps。这些值包含了端到端延迟。

## HDX - Windows Media 交付

以下客户端支持 Windows Media 客户端内容提取、Windows Media 重定向和实时 Windows Media 多媒体代码转换功能：Receiver for Windows、Receiver for iOS 和 Receiver for Linux。

要在 Windows 8 设备上使用 Windows Media 客户端内容提取，请将 Citrix Multimedia Redirector 设置为默认程序：在控制面板 > 程序 > 默认程序 > 设置默认程序中，选择 **Citrix Multimedia Redirector**，然后单击**将此程序设置为默认程序或选择此程序的默认值**。

执行 GPU 代码转换需使用具有 Compute Capability 1.1 或更高版本且支持 NVIDIA CUDA 的 GPU；请参阅 <http://developer.nvidia.com/cuda/cuda-gpus>。

## HDX - Flash 重定向

支持以下客户端和 Adobe Flash Player：

- Receiver for Windows（支持第二代 Flash 重定向功能）- 第二代 Flash 重定向功能要求安装适用于其他浏览器的 Adobe Flash Player（有时称为 NPAPI（Netscape 插件应用程序编程接口）Flash Player）
- Receiver for Linux（支持第二代 Flash 重定向功能）- 第二代 Flash 重定向功能需要安装适用于其他 Linux 的 Adobe Flash Player 或 Adobe Flash Player for Ubuntu。
- Citrix 联机插件 12.1（支持旧的 Flash 重定向功能）- 旧的 Flash 重定向功能要求安装 Adobe Flash Player for Windows Internet Explorer（有时称为 ActiveX 播放器）。

端点上的 Flash Player 主版本号必须大于或等于 VDA 上的 Flash Player 主版本号。如果端点上安装了早期版本的 Flash Player，或者端点上无法安装 Flash Player，则 Flash 内容将在 VDA 上呈现。

运行 VDA 的计算机需要：

- Adobe Flash Player for Windows Internet Explorer（ActiveX 播放器）
- Internet Explorer 11（非现代 UI 模式）。- Flash 重定向功能的工作原理是从 VDA 向端点上的 Flash Player 远程使用 ActiveX 协议。由于 Internet Explorer 是唯一可支持 ActiveX 协议的浏览器，因此该功能仅在已安装 Internet Explorer 的 VDA 中起作用。否则，会在 VDA 上呈现 Flash 内容。
- 在 Internet Explorer 中禁用保护模式（不要选中“工具”>“Internet 选项”>“安全”选项卡>“启用保护模式”复选框）。重新启动 Internet Explorer 以使更改生效。

## HDX 3D Pro

安装 VDA for Windows Desktop OS 时，可以选择安装 HDX 3D Pro 版本。

托管应用程序的物理机或虚拟机可以使用 GPU 直通或虚拟 GPU (vGPU) 功能：

- Citrix XenServer 中提供了 GPU 直通功能。GPU 直通也可随 VMware vSphere 和 VMware ESX 获得，此时它称为虚拟直接图形加速 (vDGA)。
- Citrix XenServer 中提供了 vGPU 功能；请访问 [www.citrix.com/go/vGPU](http://www.citrix.com/go/vGPU) (需要提供 Citrix 我的帐户凭据)。

Citrix 建议的主机计算机规格如下：至少 4 GB RAM，4 个时钟速度至少为 2.3 GHz 的虚拟 CPU。

图形处理器 (GPU)：

- 对于基于 CPU 的压缩（包括无损压缩），HDX 3D Pro 支持主机计算机上与要交付的应用程序兼容的任何显示适配器。
- 为通过 NVIDIA GRID API 实现优化的 GPU 帧缓冲访问，HDX 3D Pro 要求安装具有最新 NVIDIA 驱动程序的 NVIDIA Quadro 图形卡。NVIDIA GRID 将提供高帧速率，从而实现高度互动的用户体验。
- 对于使用 XenServer 的 vGPU，HDX 3D Pro 的要求包括 NVIDIA GRID K1 和 K2 卡。

用户设备：

- HDX 3D Pro 支持主机计算机上的 GPU 支持的所有显示器分辨率。但是，要在建议的最低用户设备和 GPU 规格条件下实现最佳性能，Citrix 提出了以下建议：对于 LAN 连接，建议为用户设备将显示器最大分辨率设置为 1920 x 1200 像素，对于 WAN 连接，建议将其设置为 1280 x 1024 像素。
- Citrix 建议的用户设备规格如下：至少 1 GB RAM，1 个时钟速度至少为 1.6 GHz 的 CPU。要使用适用于低带宽连接的默认的深度压缩编解码器，需要功能更强大的 CPU，除非解码在硬件上完成。要获得最佳性能，Citrix 建议用户设备至少配有一个 2 GB 的 RAM 以及一个时钟速度至少为 3 GHz 的双核 CPU。
- 对于多显示器访问，Citrix 建议在用户设备中配备四核 CPU。
- 用户设备无需配备专用 GPU 即可访问通过 HDX 3D Pro 交付的桌面或应用程序。
- 必须安装 Citrix Receiver。

## HDX - 视频会议对网络摄像机视频压缩的要求

支持的客户端：Citrix Receiver for Windows、Receiver for Mac 和 Receiver for Linux。

支持的视频会议应用程序：

- Citrix GoToMeeting HDFaces
- Adobe Connect
- Cisco WebEx
- IBM Sametime
- Microsoft Lync 2010 和 2013
- Microsoft Office Communicator
- Google+ Hangouts
- Windows 8.x、Windows Server 2012 和 Windows Server 2012 R2 上基于 Media Foundation 的视频应用程序
- Skype 6.7。要在 Windows 客户端上使用 Skype，请在客户端和服务器上编辑注册表：
  - 客户端注册表项 HKEY\_CURRENT\_USER\Software\Citrix\HdxRealTime  
名称：DefaultHeight，类型：REG\_DWORD，数据：240
  - 名称：DefaultWidth，类型：REG\_DWORD，数据：320
- 服务器注册表项 HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\Vd3d\Compatibility  
名称：skype.exe，类型：REG\_DWORD，数据：设置为 0

其他用户设备要求：

- 产生声音的相应硬件。
- 与 DirectShow 兼容的网络摄像机（使用网络摄像机默认设置）。支持硬件编码的网络摄像机可降低客户端的 CPU 使用率。
- 如有可能，应安装网络摄像机制造商提供的网络摄像机驱动程序。

## HDX - 其他

Receiver for Windows 和 Receiver for Linux 13 支持多流 ICA 的 UDP 音频。

Citrix Receiver for Windows 支持回声消除。

## 通用打印服务器的要求

- 通用打印服务器 - 通用打印服务器由客户端和服务器组件组成。UPClient 组件包含在 VDA 安装中。通用打印服务器组件（安装在共享打印机所在的每个打印服务器上，而您要在用户会话中为该打印机置备 Citrix 通用打印驱动程序）在以下操作系统中受支持：
  - Windows Server 2008 R2 SP1
  - Windows Server 2012 R2 和 2012。
- 以下是在打印服务器上安装通用打印服务器组件的必备条件：
  - Microsoft Visual Studio 2013 Runtime (32 位和 64 位)
  - Microsoft .NET Framework 4.5.2
  - CDF\_x64.msi
  - UpsServer\_x64.msi

打印操作期间进行用户身份验证需要将通用打印服务器连接到与远程桌面服务 VDA 相同的域。

## 其他

- Citrix 建议安装或升级到在安装介质中为此版本提供的组件软件版本。
  - StoreFront 需要 2 GB 内存。有关系统要求，请参阅 StoreFront 文档。StoreFront 2.6 是此版本所支持的最低版本。
  - 将 Provisioning Services 与此版本结合使用时，支持的最低 Provisioning Services 版本是 7.0。
  - Citrix 许可服务器需要 40 MB 磁盘空间。有关系统要求，请参阅许可文档。仅支持 Citrix License Server for Windows。支持的最低版本是 11.13.1。
- 如果您将 Citrix 策略信息存储在 Active Directory 而非站点配置数据库中，则需要 Microsoft 组策略管理控制台 (GPMC)。有关详细信息，请参阅 Microsoft 文档。
- 默认情况下，安装 VDA 时将安装 Receiver for Windows。有关其他平台的系统要求，请参阅 Receiver for Windows 文档。
- Receiver for Linux 和 Receiver for Mac 在产品安装介质中提供。有关系统要求，请参阅相应的文档。
- 将 Access Gateway 10.0 版之前的版本与此版本结合使用时，不支持 Windows 8.1 和 Windows 8 客户端。
- Desktop Lock - 支持的操作系统：
  - Windows 7 (包括 Embedded Edition)
  - Windows XP Embedded
  - Windows Vista

用户设备必须连接到局域网 (LAN)。

支持的 Receiver : Citrix Receiver for Windows Enterprise 3.4 软件包 (最低)。

- 客户端文件夹重定向 - 支持的操作系统：
  - 服务器 : Windows Server 2008 R2 SP1、Windows Server 2012 和 Windows Server 2012 R2
  - 客户端 (具有最新的 Citrix Receiver for Windows) : Windows 7、Windows 8 和 Windows 8.1
- 支持多个网络接口卡。
- 有关受支持的版本，请参阅[App-V](#)一文。
- 在 CU4 中，Microsoft Visual C++ 2008 SP1 (9.0.30729.4148) 的介质上提供的软件版本已更新到 Microsoft Visual C++ 2008 SP1 (9.0.30729.5677)。

# 技术概述

May 28, 2016

XenApp and XenDesktop are virtualization solutions that give IT control of virtual machines, applications, licensing, and security while providing anywhere access for any device.

XenApp and XenDesktop allow:

- End users to run applications and desktops independently of the device's operating system and interface.
- Administrators to manage the network and provide or restrict access from selected devices or from all devices.
- Administrators to manage an entire network from a single data center.

XenApp and XenDesktop share a unified architecture called FlexCast Management Architecture (FMA). FMA's key features are the ability to run multiple versions of XenApp or XenDesktop from a single Site and integrated provisioning.

## FMA key components

A typical XenApp or XenDesktop environment consists of a few key technology components, which interact when users connect to applications and desktops, and log data about Site activity.

### Citrix Receiver

A software client that is installed on the user device, supplies the connection to the virtual machine via TCP port 80 or 443, and communicates with StoreFront using the StoreFront Service API.

### StoreFront

The interface that authenticates users, manages applications and desktops, and hosts the application store. StoreFront communicates with the Delivery Controller using XML.

### Delivery Controller

The central management component of a XenApp or XenDesktop Site that consists of services that manage resources, applications, and desktops; and optimize and balance the loads of user connections.

### Virtual Delivery Agent (VDA)

An agent that is installed on machines running Windows Server or Windows desktop operating systems that allows these machines and the resources they host to be made available to users. The VDA-installed machines running Windows Server OS allow the machine to host multiple connections for multiple users and are connected to users on one of the following ports:

- TCP port 80 or port 443 if SSL is enabled
- TCP port 2598, if Citrix Gateway Protocol (CGP) is enabled, which enables session reliability
- TCP port 1494 if CGP is disabled or if the user is connecting with a legacy client

### Broker Service

A Delivery Controller service that tracks which users are logged in and where, what session resources the users have, and if users need to reconnect to existing applications. The Broker Service executes PowerShell and communicates with the Broker agent over TCP port 80. It does not have the option to use TCP port 443.

### Broker Agent

An agent that hosts multiple plugins and collects real-time data. The Broker agent is located on the VDA and is connected to the Controller by TCP port 80. It does not have the option to use TCP port 443.

### Monitor Service

A Delivery Controller component that collects historical data and puts it in the Site database by default. The Monitor Service communicates on TCP port 80 or 443.

## **ICA File/Stack**

Bundled user information that is required to connect to the VDA.

## **Site Database**

A Microsoft SQL database that stores data for the Delivery Controller, such as site policies, machine catalogs, and delivery groups.

## **NetScaler Gateway**

A data-access solution that provides secure access inside or outside the LAN's firewall with additional credentials.

## **Director**

A web-based tool that allows administrators access to real-time data from the Broker agent, historical data from the Site database, and HDX data from NetScaler for troubleshooting and support. Director communicates with the Controller on TCP port 80 or 443.

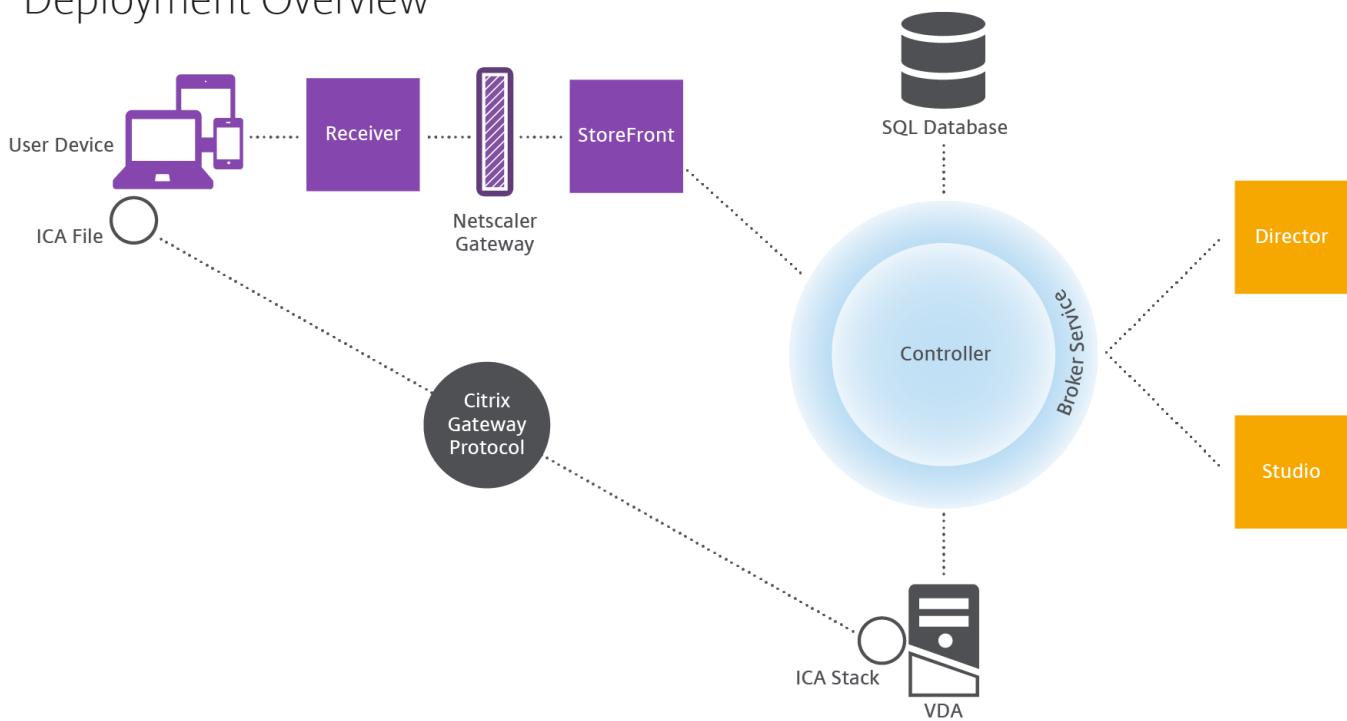
## **Studio**

A management console that allows administrators to configure and manage Sites, and gives access to real-time data from the Broker agent. Studio communicates with the Controller on TCP port 80.

## How typical deployments work

XenApp and XenDesktop Sites are made up of machines with dedicated roles that allow for scalability, high availability, and failover, and provide a solution that is secure by design. A XenApp or XenDesktop Site consists of VDA-installed Windows servers and desktop machines, and the Delivery Controller, which manages access.

## Deployment Overview



The VDA enables users to connect to desktops and applications. It is installed on server or desktop machines within the data center for most delivery methods, but it can also be installed on physical PCs for Remote PC Access.

The Controller is made up of independent Windows services that manage resources, applications, and desktops, and optimize and balance user connections. Each Site has one or more Controllers, and because sessions are dependent on latency, bandwidth, and network reliability, all Controllers ideally should be on the same LAN.

Users never directly access the Controller. The VDA serves as an intermediary between users and the Controller. When users log on to the Site using StoreFront, their credentials are passed through to the Broker Service, which obtains their profiles and available resources based on the policies set for them.

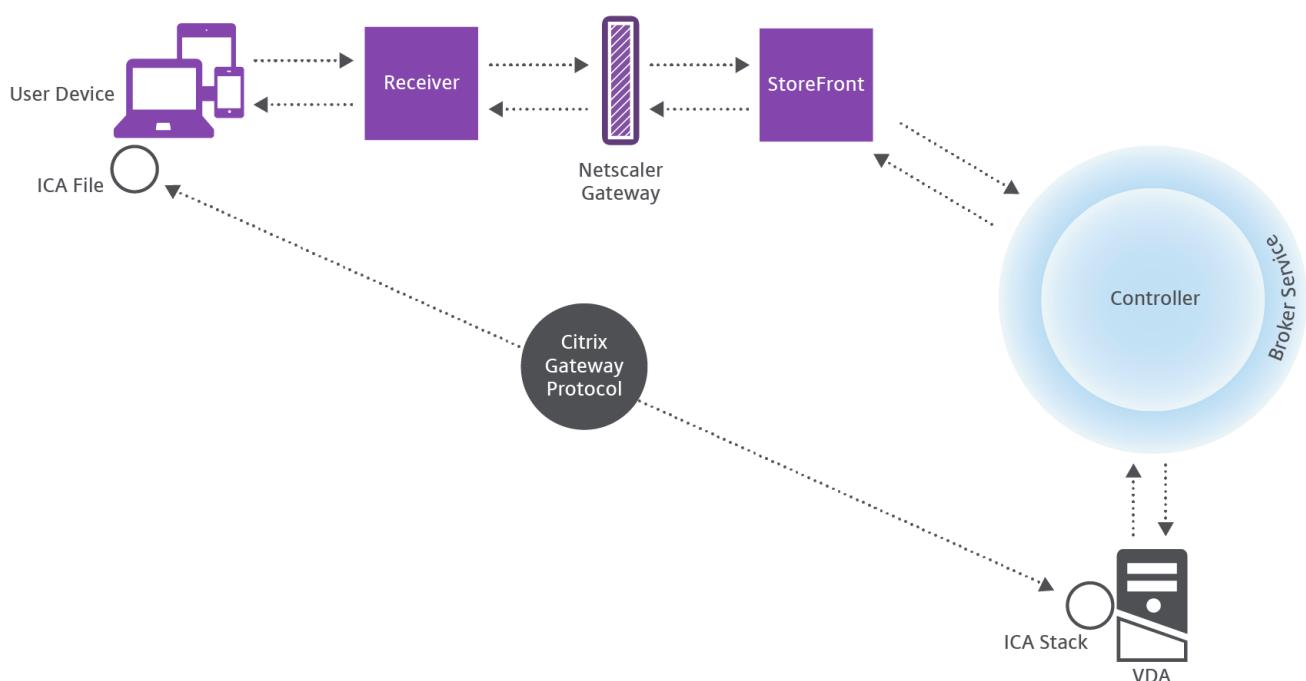
### How user connections are handled

To start a XenApp or XenDesktop session, the user connects either via Citrix Receiver, which is installed on the user's device, or via Receiver for Web (RFW).

Within Receiver, the user selects the physical or virtual desktop or virtual application that is needed.

The user's credentials move through this pathway to access the Controller, which determines what resources are needed by communicating with a Broker Service. It is recommended for administrators to put a SSL certificate on StoreFront to encrypt the credentials coming from Receiver.

## User connections



The Broker Service determines which desktops and applications the user is allowed to access.

Once the credentials are verified, the information about available apps or desktops is sent back to the user through the StoreFront-Receiver pathway. When the user selects applications or desktops from this list, that information goes back down the pathway to the Controller, which determines the proper VDA to host the specific applications or desktop.

The Controller sends a message to the VDA with the user's credentials and sends all the data about the user and the connection to the VDA. The VDA accepts the connection and sends the information back through the same pathways all the way to Receiver. Receiver bundles up all the information that has been generated in the session to create Independent Computing Architecture (ICA) file on the user's device if Receiver is installed locally or on RFW if accessed through the web. As long as the Site was properly set up, the credentials remain encrypted throughout this process.

The ICA file is copied to the user's device and establishes a direct connection between the device and the ICA stack running

on the VDA. This connection bypasses the management infrastructure: Receiver, StoreFront, and Controller.

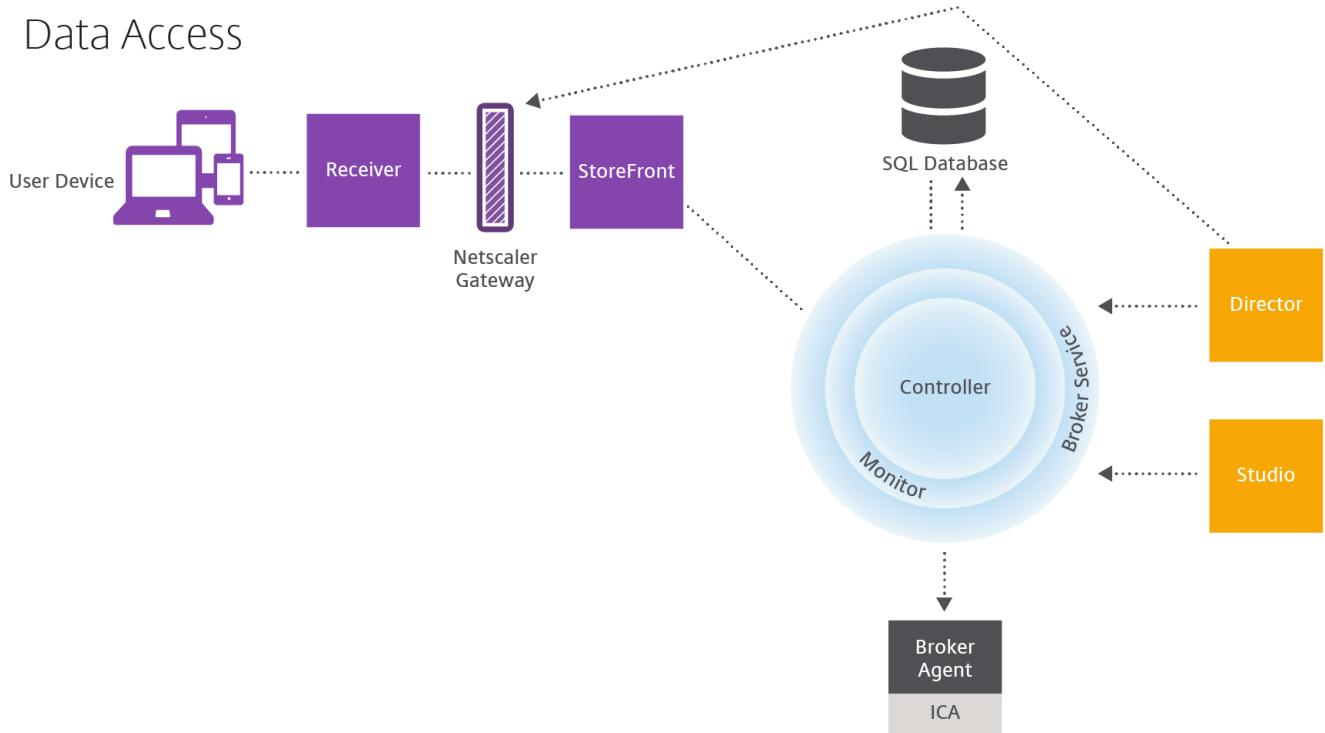
The connection between Receiver and the VDA uses the Citrix Gateway Protocol (CGP). If a connection is lost, the Session Reliability feature enables the user to reconnect to the VDA rather than having to relaunch through the management infrastructure. Session Reliability can be enabled or disabled in Studio.

Once the client connects to the VDA, the VDA notifies the Controller that the user is logged on, and the Controller sends this information to the Site database and starts logging data in the Monitoring database.

### How data access works

Every XenApp or XenDesktop session produces data that IT can access through Studio or Director. Studio allows administrators to access real-time data from the Broker Agent to better manage sites. Director has access to the same real-time data plus historical data stored in the Monitoring database as well as HDX data from NetScaler Gateway for help-desk support and troubleshooting purposes.

## Data Access



Within the Controller, the Broker Service reports session data for every session on the virtual machine providing real-time data. The Monitor Service also tracks the real-time data and stores it as historical data in the Monitoring database.

Studio can communicate only with the Broker Service; therefore, it has access only to real-time data. Director communicates with the Broker Service (through a plugin in the Broker Agent) to access the Site database.

Director can also access NetScaler Gateway to get information on the HDX data.

### Related content

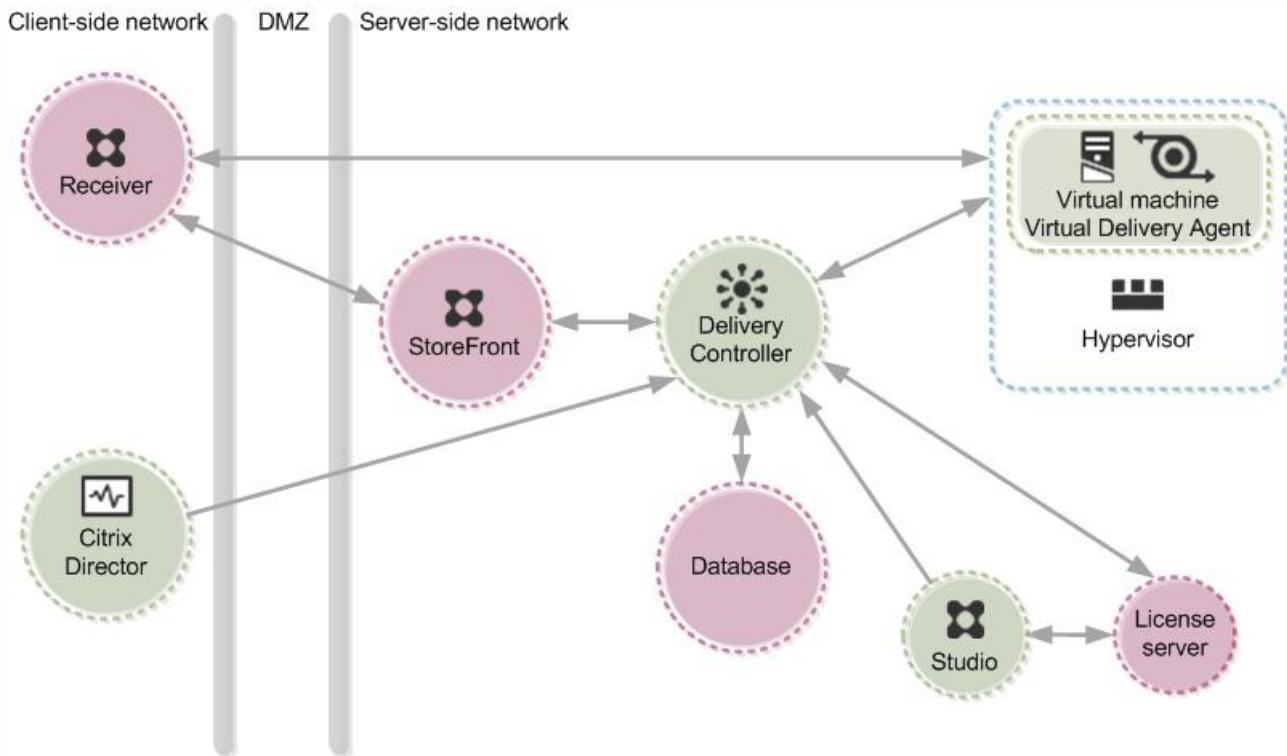
- [Concepts and components](#)
- [Active Directory](#)
- [Fault tolerance](#)

- Delivery methods

# 概念和组件

May 28, 2016

This illustration shows the key components in a typical XenApp or XenDesktop deployment, which is called a Site.



The components in this illustration are:

- **Delivery Controller** — The Delivery Controller is the central management component of any XenApp or XenDesktop Site. Each Site has one or more Delivery Controllers. It is installed on at least one server in the data center. (For Site reliability and availability, install the Controller on more than one server.) The Controller consists of services that communicate with the hypervisor to distribute applications and desktops, authenticate and manage user access, broker connections between users and their virtual desktops and applications, optimize use connections, and load-balance these connections.

Each service's data is stored in the Site database.

The Controller manages the state of the desktops, starting and stopping them based on demand and administrative configuration. In some editions, the Controller allows you to install Profile management to manage user personalization settings in virtualized or physical Windows environments.

- **Database** — At least one Microsoft SQL Server database is required for every XenApp or XenDesktop Site to store all configuration and session information. This database stores the data collected and managed by the services that make up the Controller. Install the database within your data center, and ensure it has a persistent connection to the Controller.
- **Virtual Delivery Agent (VDA)** — The VDA is installed on each physical or virtual machine in your Site that you want to make available to users. It enables the machine to register with the Controller, which in turn allows the machine and the resources it is hosting to be made available to users. VDAs establish and manage the connection between the machine and the user device, verify that a Citrix license is available for the user or session, and apply whatever policies have been configured for the session. The VDA communicates session information to the Broker Service in the Controller through

the broker agent included in the VDA.

XenApp and XenDesktop include VDAs for Windows server and desktop operating systems. VDAs for Windows server operating systems allow multiple users to connect to the server at one time. VDAs for Windows desktops allow only one user to connect to the desktop at a time.

- **StoreFront** — StoreFront authenticates users to Sites hosting resources and manages stores of desktops and applications that users access. It hosts your enterprise application store, which lets you give users self-service access to desktops and applications you make available to them. It also keeps track of users' application subscriptions, shortcut names, and other data to ensure they have a consistent experience across multiple devices.
- **Receiver** — Installed on user devices and other endpoints, such as virtual desktops, Citrix Receiver provides users with quick, secure, self-service access to documents, applications, and desktops from any of the user's devices, including smartphones, tablets, and PCs. Receiver provides on-demand access to Windows, Web, and Software as a Service (SaaS) applications. For devices that cannot install Receiver software, Receiver for HTML5 provides a connection through a HTML5-compatible web browser.
- **Studio** — Studio is the management console that enables you to configure and manage your deployment, eliminating the need for separate management consoles for managing delivery of applications and desktops. Studio provides various wizards to guide you through the process of setting up your environment, creating your workloads to host applications and desktops, and assigning applications and desktops to users. You can also use Studio to allocate and track Citrix licenses for your Site.

Studio gets the information it displays from the Broker Service in the Controller.

- **Director** — Director is a web-based tool that enables IT support and help desk teams to monitor an environment, troubleshoot issues before they become system-critical, and perform support tasks for end users. Director can be installed outside your trusted network. You can use one Director deployment to connect to and monitor multiple XenApp or XenDesktop Sites.

Director shows session and Site information from these sources:

- Real-time session data from the Broker Service in the Controller, which include data the Broker Service gets from the broker agent in the VDA.
- Historical Site data from Monitor Service in the Controller.
- Data about HDX traffic (also known as ICA traffic) captured by HDX Insight from the NetScaler, if your deployment includes a NetScaler and your XenApp or XenDesktop edition includes HDX Insights.

You can also view and interact with a user's sessions using Microsoft Remote Assistance.

- **License server** — License server manages your product licenses. It communicates with the Controller to manage licensing for each user's session and with Studio to allocate license files. You must create at least one license server to store and manage your license files.
- **Hypervisor** — The hypervisor hosts the virtual machines in your Site. These can be the virtual machines you use to host applications and desktops as well as virtual machines you use to host the XenApp and XenDesktop components. A hypervisor is installed on a host computer dedicated entirely to running the hypervisor and hosting virtual machines. Citrix XenServer hypervisor is included with XenApp and XenDesktop, but you can use other supported hypervisors, such as Microsoft Hyper-V or VMware vSphere.

Although most implementations of XenApp and XenDesktop require a hypervisor, you don't need one to provide remote PC access or when you are using Provisioning Services (included with some editions of XenApp and XenDesktop) instead of MCS to provision virtual machine.

These additional components, not shown in the illustration above, may also be included in typical XenApp or XenDesktop deployments:

- **Provisioning Services** — Provisioning Services is an optional component of XenApp and XenDesktop available with some editions. It provides an alternative to MCS for provisioning virtual machines. Whereas MCS creates copies of a master image, Provisioning Services streams the master image to user device. Provisioning Services doesn't require a hypervisor to do this, so you can use it to host physical machines. When Provisioning Services is included in a Site, it communicates with the Controller to provide users with resources.
- **NetScaler Gateway** — When users connect from outside the corporate firewall, this release can use Citrix NetScaler Gateway (formerly Access Gateway) technology to secure these connections with SSL. NetScaler Gateway or NetScaler VPX virtual appliance is an SSL VPN appliance that is deployed in the demilitarized zone (DMZ) to provide a single secure point of access through the corporate firewall.
- **Citrix CloudBridge** — In deployments where virtual desktops are delivered to users at remote locations such as branch offices, Citrix CloudBridge (formerly Citrix Branch Repeater or WANScaler) technology can be employed to optimize performance. Repeaters accelerate performance across wide-area networks, so with Repeaters in the network, users in the branch office experience LAN-like performance over the WAN. CloudBridge can prioritize different parts of the user experience so that, for example, the user experience does not degrade in the branch location when a large file or print job is sent over the network. HDX WAN Optimization with CloudBridge provides tokenized compression and data deduplication, dramatically reducing bandwidth requirements and improving performance. For more information, see the Citrix CloudBridge documentation.

With XenApp and XenDesktop, you set up the resources you want to provide to users with machine catalogs, but you designate which users have access to these resources with Delivery Groups.

## Machine catalogs

Machine catalogs are collections of virtual or physical machines that you manage as a single entity. These machines, and the application or virtual desktops on them, are the resources you want to provide to your users. All the machines in a machine catalog have the same operating system and the same VDA installed. They also have the same applications or virtual desktops available on them. Typically, you create a master image and use it to create identical virtual machines in the catalog.

When you create a machine catalog, you specify the type of machine and provisioning method for the machines in that catalog.

## Machine types

- Windows Server OS machines — Virtual or physical machines based on a Windows server operating system used for delivering XenApp published apps, also known as server-based hosted applications, and XenApp published desktops, also known as server-hosted desktops. These machines allow multiple users to connect to them at one time.
- Desktop OS machines — Virtual or physical machines based on a Windows desktop operating system used for delivering VDI desktops (desktops running Window desktop operating systems that can be fully personalized, depending on the options you choose), and VM-hosted apps (applications from desktop operating systems) and hosted physical desktops. Only one user at a time can connect each of these desktops.
- Remote PC Access — User devices that are included on a whitelist, enabling users to access resources on their office PCs remotely, from any device running Citrix Receiver. Remote PC Access enables you to manage access to office PCs through your XenDesktop deployment.

## Provisioning methods

- Machine Creation Services (MCS) — A collection of services that create virtual servers and desktops from a master image on demand, optimizing storage utilization and providing a virtual machine to users every time they log on. Machine Creation Services is fully integrated and administered in Citrix Studio.

- Provisioning Services — Enables computers to be provisioned and reprovisioned in real-time from a single shared-disk image. Provisioning Services manages target devices as a device collection. The desktop and applications are delivered from a Provisioning Services vDisk that is imaged from a master target device, which enables you to leverage the processing power of physical hardware or virtual machines. Provisioning Services is managed through its own console.
- Existing images — Applies to desktops and applications that you have already migrated to virtual machines in the data center. You must manage target devices on an individual basis or collectively using third-party electronic software distribution (ESD) tools.

## Delivery Groups

Delivery Groups are collections of users given to access a common group of resources. Delivery Groups contain machines from your machine catalogs and Active Directory users who have access to your Site. Often it makes sense to assign users to your Delivery Groups by their Active Directory group because both Active Directory groups and Delivery Groups are ways of grouping together users with similar requirements.

Each Delivery Group can contain machines from more than one machine catalog, and each machine catalog can contribute machines to more than one Delivery Group, but each individual machine can only belong to one Delivery Group at a time. You can set up a Delivery Group to deliver applications, desktops, or both.

You define which resources users in the Delivery Group can access. For example, if you want to deliver different applications to different users, one way to do this is to install all the applications you want to deliver on the master image for one machine catalog and create enough machines in that catalog to distribute among several Delivery Groups. Then you configure each Delivery Group to deliver a different subset of the applications installed on the machines.

If you are familiar with XenApp 6.5 and previous versions of XenApp, it may be helpful to think of XenApp 7.6 and XenDesktop 7.6 in terms of how they differ from those versions.

Although they are not exact equivalents, the following table helps map functional elements from XenApp 6.5 and previous versions to XenApp 7.6 and XenDesktop 7.6:

Instead of this in XenApp 6.5 and before:	Think of this in XenApp and XenDesktop 7.6:
Independent Management Architecture (IMA)	FlexCast Management Architecture (FMA)
Farm	Site
Worker Group	machine catalog Delivery Group
Worker	Virtual Delivery Agent (VDA) Server OS machine, Server OS VDA Desktop OS machine, Desktop OS VDA
Remote Desktop Services (RDS) or Terminal Services machine	Server OS machine, Server OS VDA

Zone and Data Collector Instead of this in XenApp 6.5 and before:	Delivery Controller Think of this in XenApp and XenDesktop 7.6:
Delivery Services Console	Citrix Studio and Citrix Director
Publishing applications	Delivering applications
Data store	Database
Load Evaluator	Load Management Policy
Administrator	Delegated Administrator Role Scope

XenApp 7.6 and XenDesktop 7.6 are based on FlexCast Management Architecture (FMA). FMA is a service-oriented architecture that allows interoperability and management modularity across Citrix technologies. FMA provides a platform for application delivery, mobility, services, flexible provisioning, and cloud management.

FMA replaces the Independent Management Architecture (IMA) used in XenApp 6.5 and previous versions.

These are the key elements of FMA in terms of how they relate to elements of XenApp 6.5 and previous versions:

### Delivery Sites

Farms were the top-level objects in XenApp 6.5 and previous versions. In XenApp 7.6 and XenDesktop 7.6, the Delivery Site is the highest level item. Sites offer applications and desktops to groups of users.

FMA requires that you must be in a domain to deploy a site. For example, to install the servers, your account must have local administrator privileges and be a domain user in the Active Directory.

### Machine catalogs and Delivery Groups

Machines hosting applications in XenApp 6.5 and previous versions belonged to Worker Groups for efficient management of the applications and server software. Administrators could manage all machines in a Worker Group as a single unit for their application management and load-balancing needs. Folders were used to organize applications and machines.

In XenApp 7.6 and XenDesktop 7.6, you use a combination of machine catalogs and Delivery Groups to manage machines, load balancing, and hosted applications or desktops.

### Virtual Delivery Agents

In XenApp 6.5 and previous versions, worker machines in Worker Groups ran applications for the user and communicated with data collectors. In XenApp 7.6 and XenDesktop 7.6, the VDA communicates with Delivery Controllers that manage the user connections.

### Delivery Controllers

In XenApp 6.5 and previous versions there was a zone master responsible for user connection requests and communication with hypervisors. In XenApp 7.6 and XenDesktop 7.6, Controllers in the Site distribute and handle connection requests.

XenApp 6.5 and previous versions, zones provided a way to aggregate servers and replicate data across WAN connections.

Although zones have no exact equivalent in XenApp 7.6 and XenDesktop 7.6, you can provide users with applications that

cross WANs and locations. You can design Delivery Sites for a specific geographical location or data center and then allow your users access to multiple Delivery Sites. App Orchestration with XenApp 7.6 and XenDesktop 7.6 provides capabilities for managing multiple Sites in multiple geographies.

### Citrix Studio and Citrix Director

Use the Studio console to configure your environments and provide users with access to applications and desktops. Studio replaces the Delivery Services Console in XenApp 6.5 and previous versions.

Administrators use Director to monitor the environment, shadow user devices, and troubleshoot IT issues. To shadow users, Microsoft Remote Assistance must be enabled; it is enabled by default when the VDA is installed.

### Delivering applications

XenApp 6.5 and previous versions used the Publish Application wizard to prepare applications and deliver them to users. In XenApp 7.6 and XenDesktop 7.6, you use Studio to create and add applications to make them available to users who are included in a Delivery Group. Using Studio, you first configure a Site, create and specify machine catalogs, and then create Delivery Groups within those machine catalogs. The Delivery Groups determine which users have access to the applications you deliver.

### Database

XenApp 7.6 and XenDesktop 7.6 do not use the IMA data store for configuration information. They use a Microsoft SQL Server database to store configuration and session information.

### Load Management Policy

In XenApp 6.5 and previous versions, load evaluators use predefined measurements to determine the load on a machine. User connections can be matched to the machines with less load.

In XenApp 7.6 and XenDesktop 7.6, use load management policies for balancing loads across machines.

### Delegated Administrators

In XenApp 6.5 and previous versions, you created custom administrators and assigned them permissions based on folders and objects. In XenApp 7.6 and XenDesktop 7.6, custom administrators are based on role and scope pairs. A role represents a job function and has defined permissions associated with it to allow delegation. A scope represents a collection of objects. Built-in administrator roles have specific permission sets, such as help desk, applications, hosting, and catalog. For example, help desk administrators can work only with individual users on specified sites, while full administrators can monitor the entire deployment and resolve systemwide IT issues.

The transition to FMA also means some features available in XenApp 6.5 and previous versions may be implemented differently or may require you to substitute other features, components, or tools to achieve the same goals.

Instead of this in XenApp 6.5 and before:	Use this in XenApp and XenDesktop 7.6:
Session prelaunch and session linger configured with policy settings	Session prelaunch and session linger configured by editing Delivery Group settings.  As in XenApp 6.5, these features help users connect to applications quickly, by starting sessions before they are requested (session prelaunch) and keeping sessions active after a user closes all applications (session linger). In XenApp and XenDesktop 7.6, you enable these features for specified users by configuring these settings for existing Delivery groups. See <a href="#">Configure session prelaunch and session linger</a> .
Support for unauthenticated (anonymous) users provided by granting rights to anonymous user when setting	Support for unauthenticated (anonymous) users provided by configuring this option when setting user properties of a Delivery Group. See <a href="#">Users</a> .

<b>the properties of published applications. Instead of this in XenApp 6.5 and before:</b>	<b>Use this in XenApp and XenDesktop 7.6:</b>
Local host cache permits a worker servers to function even when a connection to the data store is not available	Connection leasing enables users to connect and reconnect to their most recently used applications and desktops, even when the Site database is not available. The connection leasing feature supplements the SQL Server high availability best practices. See <a href="#">Connection leasing</a> .
Application streaming	App-V delivers streamed applications, managed using Studio.
Web Interface	Citrix recommends you transition to StoreFront.
SmartAuditor	Use configuration logging to log all session activities from an administrative perspective or use a third-party, Citrix-ready tool to record sessions.

# Active Directory

May 28, 2016

Active Directory is required for authentication and authorization. The Kerberos infrastructure in Active Directory is used to guarantee the authenticity and confidentiality of communications with the Delivery Controllers. For information about Kerberos, see the Microsoft documentation.

The [System requirements](#) document lists the supported functional levels for the forest and domain. To use Policy Modeling, the domain controller must be running on Windows Server 2003 to Windows Server 2012 R2; this does not affect the domain functional level.

This product supports:

- Deployments in which the user accounts and computer accounts exist in domains in a single Active Directory forest. User and computer accounts can exist in arbitrary domains within a single forest. All domain functional levels and forest functional levels are supported in this type of deployment.
- Deployments in which user accounts exist in an Active Directory forest that is different from the Active Directory forest containing the computer accounts of the controllers and virtual desktops. In this type of deployment, the domains containing the Controller and virtual desktop computer accounts must trust the domains containing user accounts. Forest trusts or external trusts can be used. All domain functional levels and forest functional levels are supported in this type of deployment.
- Deployments in which the computer accounts for Controllers exist in an Active Directory forest that is different from one or more additional Active Directory forests that contain the computer accounts of the virtual desktops. In this type of deployment a bi-directional trust must exist between the domains containing the Controller computer accounts and all domains containing the virtual desktop computer accounts. In this type of deployment, all domains containing Controller or virtual desktop computer accounts must be at "Windows 2000 native" functional level or higher. All forest functional levels are supported.
- Writable domain controllers. Read-only domain controllers are not supported.

Optionally, Virtual Delivery Agents (VDAs) can use information published in Active Directory to determine which Controllers they can register with (discovery). This method is supported primarily for backward compatibility, and is available only if the VDAs are in the same Active Directory forest as the Controllers. For information about this discovery method see [Active Directory OU-based Controller discovery](#) and [CTX118976](#).

Note: This information applies to minimum version XenDesktop 7.1 and XenApp 7.5. It does not apply to earlier versions of XenDesktop or XenApp.

In an Active Directory environment with multiple forests, if one-way or two-way trusts are in place you can use DNS forwarders for name lookup and registration. To allow the appropriate Active Directory users to create computer accounts, use the Delegation of Control wizard. Refer to Microsoft documentation for more information about this wizard.

No reverse DNS zones are necessary in the DNS infrastructure if appropriate DNS forwarders are in place between forests.

The SupportMultipleForest key is necessary if the VDA and Controller are in separate forests, regardless of whether the Active Directory and NetBios names are different. The SupportMultipleForest key is only necessary on the VDA. Use the following information to add the registry key:

Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor

at your own risk. Be sure to back up the registry before you edit it.

- HKEY\_LOCAL\_MACHINE\Software\Citrix\VirtualDesktopAgent\SupportMultipleForest
  - Name: SupportMultipleForest
  - Type: REG\_DWORD
  - Data: 0x00000001 (1)

You might need reverse DNS configuration if your DNS namespace is different than that of Active Directory.

If external trusts are in place during setup, the ListOfIDs registry key is required. The ListOfIDs registry key is also necessary if the Active Directory FQDN is different than the DNS FQDN or if the domain containing the Domain Controller has a different Netbios name than the Active Directory FQDN. To add the registry key, use the following information:

- For a 32-bit or 64-bit VDA, locate the registry key  
HKEY\_LOCAL\_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfIDs
  - Name: ListOfIDs
  - Type: REG\_SZ
  - Data: Security Identifier (SID) of the Controllers

When external trusts are in place, make the following changes on the VDA:

1. Locate the file <ProgramFiles>\Citrix\Virtual Desktop Agent\brokeragentconfig.exe.config.
2. Make a backup copy of the file.
3. Open the file in a text editing program such as Notepad.
4. Locate the text allowNtlm="false" and change the text to allowNtlm="true".
5. Save the file.

After adding the ListOfIDs registry key and editing the brokeragent.exe.config file, restart the Citrix Desktop Service to apply the changes.

The following table lists the supported trust types:

Trust type	Transitivity	Direction	Supported in this release
Parent and child	Transitive	Two-way	Yes
Tree-root	Transitive	Two-way	Yes
External	Nontransitive	One-way or two-way	Yes
Forest	Transitive	One-way or two-way	Yes
Shortcut	Transitive	One-way or two-way	Yes
Realm	Transitive or nontransitive	One-way or two-way	No

For more information about complex Active Directory environments, see [CTX134971](#).

# 容错

May 28, 2016

This document outlines ways in which you can increase the level of fault tolerance in your deployment to make sure that business-critical applications and desktops are always available.

All information is stored in the Site configuration database; Delivery Controllers communicate only with the database and not with each other. A Controller can be unplugged or turned off without affecting other Controllers in the Site. This means, however, that the Site configuration database forms a single point of failure. If the database server fails, existing connections to virtual desktops will continue to function until a user either logs off or disconnects from a virtual desktop; new connections cannot be established if the database server is unavailable.

Citrix recommends that you back up the database regularly so that you can restore from the backup if the database server fails. In addition, there are several high availability solutions to consider for ensuring automatic failover:

- SQL Mirroring — This is the recommended solution. Mirroring the database makes sure that, should you lose the active database server, the automatic failover process happens in a matter of seconds, so that users are generally unaffected. This method, however, is more expensive than other solutions because full SQL Server licenses are required on each database server; you cannot use SQL Server Express edition for a mirrored environment.
- Using the hypervisor's high availability features — With this method, you deploy the database as a virtual machine and use your hypervisor's high availability features. This solution is less expensive than mirroring as it uses your existing hypervisor software and you can also use SQL Express. However, the automatic failover process is slower, as it can take time for a new machine to start for the database, which may interrupt the service to users.
- SQL Clustering — The Microsoft SQL clustering technology can be used to automatically allow one server to take over the tasks and responsibilities of another server that has failed. However, setting up this solution is more complicated, and the automatic failover process is typically slower than with alternatives such as SQL Mirroring.
- AlwaysOn Availability Groups is an enterprise-level high-availability and disaster recovery solution introduced in SQL Server 2012 to enable you to maximize availability for one or more user databases. AlwaysOn Availability Groups requires that the SQL Server instances reside on Windows Server Failover Clustering (WSFC) nodes. For more information, see [AlwaysOn Availability Groups \(SQL Server\)](#).

Note: Installing a Controller on a node in an SQL clustering or SQL mirroring installation is not supported.

The configuration process involves tasks an administrator completes using SQL Server management tools before creating the Site. The remaining tasks occur when the administrator runs the Site creation wizard.

A mirror environment requires at least two SQL Server machines (in the following example, SQL Server A and SQL Server B). SQL Server Express edition cannot be used as either a principal or mirror.

Using Microsoft SQL Server management tools, configure the SQL Server databases:

1. Install the SQL Server software on SQL Server A and SQL Server B.
2. On SQL Server A, create the database intended to be used as the principal (for example, myDatabaseMirror).
  - Make sure that the database uses the full recovery model and not the simple model. (The simple model is configured by default, but prevents the transaction log from being backed up.)
  - Use the following collation setting when creating the database: Latin1\_General\_100\_CI\_AS\_KS (where Latin1\_General varies depending on the country; for example Japanese\_100\_CI\_AS\_KS). If this collation setting is not

specified during database creation, subsequent creation of the service schemas within the database will fail, and an error similar to "<service>: schema requires a case-insensitive database" appears (where <service> is the name of the service whose schema is being created).

- Enable a Read-Committed snapshot as described in [CTX137161](#). It is important to enable this before the database is mirrored to avoid errors.
3. On SQL Server A, back up the database to a file and copy it to SQL Server B.
  4. On SQL Server B, restore the backup file to that server (SQL Server B).
  5. On SQL Server A, start mirroring.

The next step depends on whether the Citrix administrator (that is, the person running the Site creation wizard) also has full database privileges:

- If the Citrix administrator has database privileges (the same person is the database administrator and the Citrix administrator), Studio does everything for you:
  1. The Citrix administrator uses Studio to create a Site, specifying the address of the previously-created SQL Server A database and its name (myDatabaseMirrorForXD).
  2. The database scripts are automatically applied and the principal and mirror databases are set.
- If the Citrix administrator does not have database privileges, the Citrix administrator must get help from a database administrator:
  1. The Citrix administrator uses Studio to create a Site, specifying the address of the previously-created SQL Server and its name (myDatabaseMirrorForXD).
  2. In the Site creation wizard, selecting Generate Script generates a mirror script and a primary script. The Citrix administrator gives those scripts to the database administrator, who applies the scripts (the mirror script should be applied first). The database administrator must tell the Citrix administrator when that task is completed.
  3. Back in Studio, the Citrix administrator can now complete the Create Site wizard. The principal and mirror databases are set.

To verify mirroring after creating the Site, run the PowerShell cmdlet `get-configdbconnection` to make sure that the Failover Partner has been set in the connection string to the mirror.

If you later add, move, or remove a Delivery Controller in a mirrored database environment, see [Add, remove, or move Controllers, or move a VDA](#) for considerations.

If all Delivery Controllers in a Site fail, you can configure the Virtual Delivery Agents to operate in high availability mode so that users can continue to access and use their desktops and applications. In high availability mode, the VDA accepts direct ICA connections from users, rather than connections brokered by the Controller.

This feature is for use only on the rare occasion when communication with all Controllers fails; it is not an alternative to other high availability solutions. For more information, see [CTX127564](#).

The connection leasing feature supplements the SQL Server high availability best practices by enabling users to connect and reconnect to their most recently used applications and desktops, even when the Site database is not available. For details, see [Connection leasing](#).

# 交付方法

May 28, 2016

It's challenging to meet the needs of every user with one virtualization deployment. XenApp and XenDesktop allow administrators to customize the user experience with a variety of methods sometimes referred to as FlexCast models.

This collection of delivery methods — each with its own advantages and disadvantages — provide the best user experience in any use-case scenario.

Touch-screen devices, such as tablets and smartphones, are now standard in mobility. These devices can cause problems when running Windows-based applications that typically utilize full-size screens and rely on right-click inputs for full functionality.

XenApp with Citrix Receiver offers a secure solution that allows mobile-device users access to all the functionality in their Windows-based apps without the cost of rewriting those apps for native mobile platforms.

The XenApp published apps delivery method utilizes HDX Mobile technology that solves the problems associated with mobilizing Windows applications. This method allows Windows applications to be refactored for a touch experience while maintaining features such as multitouch gestures, native menu controls, camera, and GPS functions. Many touch features are available natively in XenApp and XenDesktop and do not require any application source code changes to activate.

These features include:

- Automatic display of the keyboard when an editable field has the focus
- Larger picker control to replace Windows combo box control
- Multitouch gestures, such as pinch and zoom
- Inertia-sensed scrolling
- Touchpad or direct-cursor navigation

Upgrading physical machines is a daunting task many businesses face every three to five years, especially if the business needs to maintain the most up-to-date operating systems and applications. Growing businesses also face daunting overhead costs of adding new machines to their network.

The VDI Personal vDisk delivery method provides fully personalized desktop operating systems to single users on any machine or thin client using server resources. Administrators can create virtual machines whose resources — such as processing, memory, and storage — are stored in the network's data center.

This can extend the life of older machines, keep software up to date, and minimize downtime during upgrades.

Network security is an ever-growing problem, especially when working with contractors, partners, and other third-party contingent workers who need access to a company's apps and data. The workers may also need loaner laptops or other devices, which cause additional cost concerns.

Data, applications, and desktops are stored behind the firewall of the secure network with XenDesktop and XenApp, so the only thing the end user transmits is user-device inputs and outputs, such as keystrokes, mouse clicks, audio, and screen

updates. By maintaining these resources in a data center, XenDesktop and XenApp offer a more secure remote access solution than using the typical SSL VPN.

With a VDI with Personal vDisk deployment, administrators can utilize thin clients or users' personal devices by creating a virtual machine on a network server and providing a single-user desktop operating system. This allows IT to maintain security with third-party workers without the need of purchasing expensive equipment.

When switching to a new operating system, IT can face the challenge of delivering legacy and incompatible applications.

With virtual-machine-hosted apps, users can run older applications through Citrix Receiver on the upgraded virtual machine without any compatibility issues. This allows IT additional time to resolve and test application compatibility issues, ease users into the transition, and make help desk calls more efficient.

Additional benefit for using XenDesktop during migration include:

- Reducing complexity for desktops
- Improving IT's control
- Enhancing end-user flexibility in terms of device usage and workspace location

Many design firms and manufacturing companies rely heavily on professional 3-D graphics applications. These companies face financial strain from the costs of powerful hardware to support this type of software and also logistic problems that come with the sharing of large design files via FTP, email, and similar ad hoc methods.

XenDesktop's hosted physical desktop delivery method provides a single desktop image to workstations and blade servers without the need of hypervisors to run graphic-intensive 3-D applications on a native operating system.

All files are saved in a central data center within the network, so sharing large design files to other users in the network is faster and more secure because the files are not being transferred from one workstation to another.

Businesses that need large-scale call centers face the difficult challenge of maintaining adequate staffing for peak periods while not overprovisioning machines during less busy hours.

The Pooled VDI delivery method provides multiple users access to a standardized desktop dynamically at a minimal cost when provisioning a large number of users. The pooled machines are allocated on a per-session, first-come, first-served basis.

There is less day-to-day management of these virtual machines because any change made during the session is discarded when the user logs off. This also increases security.

The XenApp hosted desktops delivery method is another viable option for transforming call centers. This method hosts multiple user desktops on a single server-based operating system.

This is a more cost-efficient method than Pooled VDI, but with XenApp hosted desktops, users are restricted from installing applications, changing system settings, and restarting the server.

# 新部署

Jan 25, 2017

To build a XenApp or XenDesktop deployment:

1. Set up the virtualization environment to host and manage the components of your XenApp or XenDesktop environment. See [System requirements](#) for supported versions of the virtualization platforms, management tools, and cloud deployment solutions listed here.

You can use these virtualization platforms to host and manage machines in your XenApp or XenDesktop environment:

- XenServer. See [XenServer](#) for information on setting up and using XenServer.
- VMware vSphere. See [Prepare the virtualization environment: VMware](#) for guidance on setting up and using VMware vSphere with XenApp or XenDesktop.
- Hyper-V with Microsoft System Center Virtualization Machine Manager (VMM). See [Prepare the virtualization environment: Microsoft System Center Virtual Machine Manager](#) for guidance on setting up and using Hyper-V with VMM with XenApp or XenDesktop.

You can use Microsoft System Center Configuration Manager with Citrix Connector 7.5 for System Center Configuration Manager 2012 to manage physical and virtual machines in your XenApp or XenDesktop environment or use it to enable the Wake on LAN feature of Remote PC Access. See [Prepare for using Microsoft System Center Configuration Manager](#).

You can use these cloud deployment solutions to host product components and provision virtual machines. These solutions pool computing resources to build public, private, and hybrid Infrastructure as a Service (IaaS) clouds.

- Amazon Web Services, see [Deploy XenApp and XenDesktop 7.5 and 7.6 with Amazon VPC](#).
  - Citrix CloudPlatform, see [XenApp and XenDesktop concepts and deployment on CloudPlatform](#).
2. Set up the non-Citrix infrastructure components required to build your XenApp or XenDesktop Site. These include at least one domain controller running Active Directory Domain Services.
  3. Install the Citrix components that make up your XenApp or XenDesktop Site. You can install components using a wizard-based graphical interface or a command-line interface, which enables scripted installation. Both methods install most prerequisites automatically.
    1. Before beginning any installation, review the [System requirements](#). Also, read and complete the [Prepare to install](#) checklist.
    2. Install the core components: Delivery Controller, Citrix Studio, Citrix Director, Citrix License Server, and Citrix StoreFront. See [Install using the graphical interface](#) or [Install using the command line](#) for information on installing these components.
    3. From Studio, create a Site. See [Create a Site](#).
    4. Install a Virtual Delivery Agent (VDA), either on the master image you will use to create virtual machines or directly on each machine. See [Install using the graphical interface](#) or [Install using the command line](#) for information on installing the VDA. You may also want to see [Install or remove Virtual Delivery Agents using scripts](#).  
For Remote PC Access deployments, install a VDA for Desktop OS on each office PC. Citrix recommends using the VDA installer's command line interface and your existing Electronic Software Distribution (ESD) methods.
  5. Optionally, install the Universal Print Server on the print servers in your environment. See [Install using the graphical](#)

[interface](#) or [Install using the command line](#) for information on installing the Universal Print Server.

4. Optionally, integrate additional Citrix components into your XenApp or XenDesktop deployment. For example:
  - Provisioning Services is an optional component of XenApp and XenDesktop that provisions machines by streaming a master image to target devices. See [Provisioning Services](#).
  - Citrix NetScaler Gateway is a secure application access solution that provides administrators granular application-level policy and action controls to secure access to applications and data. See [Citrix NetScaler Gateway](#).
  - Citrix CloudBridge is a set of appliances that optimize WAN performance. See [Citrix CloudBridge](#).
5. Set up the resources you will deliver to users. How you do this depends on the delivery method you are using, but this is the basic sequence for most delivery methods:
  1. Using your hypervisor's management tool, create a master image that defines the desktops or applications you want to provide. See [Prepare a master image](#).
  2. Create a machine catalog containing physical and virtual machines from that master image. See [Create a machine catalog](#).
    - If you are using Machine Creation Services to provision machines, you can add machines to the machine catalog from within Studio.
    - If you are using Provisioning Services to provision machines, you add machines to the machine catalog from the Provisioning Services console.
  3. From Studio, create a Delivery Group to specify which users can access these machines and the applications installed on them. See [Delivery groups](#).

# 安装和升级分析

Mar 22, 2017

When you use the full-product installer to deploy or upgrade XenApp or XenDesktop components, anonymous information about the installation process is gathered and stored on the machine where you are installing/upgrading the component. This data is used to help Citrix improve its customers' installation experiences. For more information, see <http://more.citrix.com/XD-INSTALLER>.

The information is stored locally under %ProgramData%\Citrix\CTQs.

Automatic upload of this data is enabled by default in both the graphical and command line interfaces of the full-product installer.

- You can change the default value in a registry setting. If you change the registry setting before installing/upgrading, that value will be used when you use the full-product installer.
- You can override the default setting if you install/upgrade with the command line interface by specifying an option with the command.

Registry setting that controls automatic upload of install/upgrade analytics (default = 1):

Location: HKLM:\Software\Citrix\MetaInstall

Name: SendExperienceMetrics

Value: 0 = disabled, 1 = enabled

Using PowerShell, the following cmdlet disables automatic upload of install/upgrade analytics:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\MetaInstall -Name SendExperienceMetrics -PropertyType DWORD -  
Value 0
```

To disable automatic uploads with the XenDesktopServerSetup.exe or XenDesktopVDASetup.exe command, include the /disableexperiencemetrics option.

To enable automatic uploads with the XenDesktopServerSetup.exe or XenDesktopVDASetup.exe command, include the /sendexperiencemetrics option.

# 准备安装

Jul 07, 2016

The following tables list tasks to complete and things to consider or be aware of before installing the core components (Delivery Controller, Citrix Studio, Citrix Director, Citrix License Server, StoreFront) and Virtual Delivery Agents (VDAs).

• Description
<p>First:</p> <ul style="list-style-type: none"><li>• If you are unfamiliar with the product, review the <a href="#">Technical overview</a> and related content.</li><li>• Check<ul style="list-style-type: none"><li>— <i>Known issues</i> for installation issues you might encounter.</li></ul></li><li>• If you are installing components in a cloud environment, see:<ul style="list-style-type: none"><li>• <a href="#">Deploy XenApp and XenDesktop 7.5 and 7.6 with Amazon VPC</a> for Amazon Web Services;</li><li>• <a href="#">XenApp and XenDesktop concepts and deployment on CloudPlatform</a> for Citrix CloudPlatform.</li></ul></li><li>• If you are using XenServer for your virtualization environment, see the XenServer documentation for guidance.</li><li>• If you are using <a href="#">VMware</a> or <a href="#">Microsoft System Center Virtual Machine Manager</a> for your virtualization environment, see the linked documents.</li></ul>
<p>Decide where you will install the components and then prepare the machines and operating systems.</p> <ul style="list-style-type: none"><li>• Review <a href="#">System requirements</a> for supported operating systems and versions for the Controller, Studio, Director, Virtualization resources, and VDAs. The Citrix StoreFront and the Citrix License Server requirements documents specify their supported platforms.<ul style="list-style-type: none"><li>• You can install the core components on the same server or on different servers. For example, to manage a smaller deployment remotely, you can install Studio on a different machine than the server where you installed the Controller. To accommodate future expansion, consider installing components on separate servers; for example, install the License Server and Director on different servers.</li><li>• You can install both the Delivery Controller and the Virtual Delivery Agent for Windows Server OS on the same server. Launch the installer and select the Delivery Controller (plus any other core components you want on that machine); then launch the installer again and select the Virtual Delivery Agent for Windows Server OS.</li><li>• Do not install Studio on a server running XenApp 6.5 Feature Pack 2 for Windows Server 2008 R2 or any earlier version of XenApp.</li></ul></li><li>• Be sure that each operating system has the latest updates.</li><li>• Be sure that all machines have synchronized system clocks. Synchronization is required by the Kerberos infrastructure that secures communication between the machines.</li><li>• Components are installed in C:\Program Files\Citrix by default. You can specify a different location during installation, but it must have execute permissions for network service.</li><li>• Most component prerequisites are installed automatically; however, the<ul style="list-style-type: none"><li>— <i>System requirements</i> document notes exceptions.</li></ul></li></ul>
<p>Decide where to install the SQL Server software for the Site Configuration Database.</p> <ul style="list-style-type: none"><li>• By default, SQL Server 2012 Express is installed automatically on the server when you install the Controller, if another instance is not detected.</li></ul> <p>The default installation uses the default Windows service accounts and permissions. Refer to Microsoft documentation for details of these defaults, including the addition of Windows service accounts to the sysadmin role. The Controller uses the Network Service account in this configuration. The Controller does not require any additional SQL Server roles or permissions.</p> <p>If required, you can select <b>Hide instance</b> for the database instance. When configuring the address of the database in Studio, enter the instance's static port number, rather than its name. Refer to Microsoft documentation for details about hiding an instance of SQL Server Database Engine.</p> <ul style="list-style-type: none"><li>• Alternatively, you can separately install a supported SQL Server version on that server or on a different server. In such cases, the SQL Server software does not need to be installed before you install the core components, but it must be installed before you create the Site.</li><li>• Review the database considerations in the<ul style="list-style-type: none"><li>— <i>Plan</i> documents, and set up any supported redundancy infrastructure.</li></ul></li></ul>

<ul style="list-style-type: none"> <li>•</li> </ul>	<p><b>Description</b></p> <p>Important: Windows authentication is required between the Controller and the database.</p>
	<p>Decide how you want ports opened.</p> <p>By default, the following ports are opened automatically if the Windows Firewall Service is running, even if the firewall is not enabled. You can disable this default action and open the ports manually if you use a third-party firewall or no firewall, or if you just prefer to do it yourself.</p> <ul style="list-style-type: none"> <li>• Controller: TCP 80, 443</li> <li>• Director: TCP 80, 443</li> <li>• License Server: TCP 7279, 8082, 8083, 27000</li> <li>• StoreFront: TCP 80, 443</li> </ul> <p>Tip: For complete port information, see <a href="#">CTX101810</a>. For additional installation options, see <a href="#">Install using the command line</a>.</p>
	<p>Configure your Active Directory domain.</p> <ul style="list-style-type: none"> <li>• In addition to being a domain user, you must be a local administrator on the machines where you are installing core components.</li> <li>• Do not attempt to install any components on a domain controller.</li> <li>• The <i>System requirements</i> document lists the supported functional levels. See the Microsoft documentation for instructions.</li> </ul> <p>When you install the License Server, that user account is automatically made a full administrator on the license server.</p>
	<p>Before you install Director, decide if you will use the shadowing feature of Director, which uses Windows Remote Assistance.</p>
	<p><b>Good to know:</b></p> <ul style="list-style-type: none"> <li>• If a component does not install successfully, the process stops with an error message. Components that installed successfully are retained; you do not need to reinstall them.</li> <li>• Studio starts automatically after it is installed. You can disable this action during installation.</li> <li>• When you create objects before, during, and after installation, it is best practice to specify unique names for each object (for example networks, groups, catalogs, resources).</li> <li>• After installing components in Amazon Web Services (AWS), you will need to know the region, availability zone, VPC name, subnet addresses, domain name, security group names, and credentials when you use Studio to create a Site.</li> </ul>

	<p><b>Description</b></p>
	<p>If you will be installing a VDA for Windows Desktop OS, decide if you want to install the HDX 3D Pro version.</p> <p>The HDX3D Pro feature delivers desktops and applications that perform best with a GPU for hardware acceleration. For more information, see the HDX 3D Pro documentation.</p>
	<p>Decide how you will use the VDA.</p> <p>The default setting assumes that you will use a master image containing an installed VDA with Machine Creation Services or Provisioning Services to create other virtual machines. You can override this default if you want to install the VDA on an existing machine.</p>
	<p>Decide if you want to install Citrix Receiver for Windows (CitrixReceiver.exe).</p> <p>You can disable this default action.</p>

 <b>Description</b>	<p>Decide how you want ports opened.</p> <p>By default, the following ports are opened automatically if the Windows Firewall Service is running, even if the firewall is not enabled. You can disable this default action and open the ports manually if you use a third-party firewall or no firewall, or if you just prefer to do it yourself.</p> <ul style="list-style-type: none"> <li>• Controller: TCP 80, 1494, 2598, 8008 <ul style="list-style-type: none"> <li>• For communication between user devices and virtual desktops, configure inbound TCP on ports 1494 and 2598 as port exceptions. For security, Citrix recommends that you do not use these registered ports for anything other than the ICA protocol and the Common Gateway Protocol.</li> <li>• For communication between Controllers and virtual desktops, configure inbound port 80 as a port exception.</li> </ul> </li> <li>• Windows Remote Assistance: TCP 3389 Windows opens this port automatically if the feature is enabled, even if you choose to open the ports manually.</li> <li>• Real-Time Audio Transport: UDP 16500-16509</li> </ul> <p><b>Tip:</b> For complete port information, see <a href="#">CTX101810</a>.</p>
	<p>Decide how you will specify the locations of installed Controllers.</p> <ul style="list-style-type: none"> <li>• Manually, by entering the Fully Qualified Domain Name (FQDN) of the Controller. Although you can specify a Controller that is not currently in the domain, a VDA can connect only to a Controller in the domain. Also, you can test the connection only for Controllers in the domain.</li> <li>• Using Active Directory, if the Controller is in the domain.</li> <li>• Allowing Machine Creation Services to specify the Controller.</li> <li>• Later, by rerunning the installer, using Citrix policies, setting registry values, or using Active Directory OUs.</li> </ul> <p>Citrix Group Policy settings that specify Controller locations will override settings provided during installation.</p> <p>After you initially specify the Controller location, you can use the auto-update feature to update VDAs when additional Controllers are installed.</p>
	<p>Decide if you want to use the following features:</p> <ul style="list-style-type: none"> <li>• Optimize performance: When this feature is enabled, the optimization tool is used for VDAs running in a VM on a hypervisor. VM optimization includes disabling offline files, disabling background defragmentation, and reducing event log size. For more information, see <a href="#">CTX125874</a>. Do not enable this option if you will be using Remote PC Access. Default = enabled.</li> <li>• Windows Remote Assistance: When this feature is enabled, Windows Remote Assistance is used with the user shadowing feature of Director, and Windows automatically opens TCP port 3389 in the firewall, even if you choose to open firewall ports manually. Default = enabled.</li> <li>• Real-Time Audio Transport for audio: When this feature is enabled, UDP is used for audio packets, which can improve audio performance. Default = enabled.</li> <li>• Personal vDisk: (Available only when installing a VDA for Windows Desktop OS on a VM.) When this feature is enabled, Personal vDisks can be used with a master image. For more information, see <a href="#">Personal vDisks</a>. Default = disabled.</li> </ul>
	<p>Good to know:</p> <ul style="list-style-type: none"> <li>• The Print Spooler Service is enabled by default on the Windows server. If you disable this service, you cannot successfully install a VDA for Windows Server OS. Therefore, ensure that this service is enabled before installing a VDA.</li> </ul>

 <b>Description</b> <ul style="list-style-type: none"> <li>The installer automatically detects your operating system and allows you to install only the VDA type supported on that system: VDA for Windows Server OS or VDA for Windows Desktop OS.</li> <li>Profile management is installed during VDA installation.</li> <li>When you install the VDA, a new local user group called Direct Access Users is automatically created. On a VDA for Windows Desktop OS, this group applies only to RDP connections; on a VDA for Windows Server OS, this group applies to ICA and RDP connections.</li> <li>When you install a VDA for Windows Server OS, Remote Desktop Services role services are automatically installed and enabled (if they are not already installed and enabled).</li> <li>For Remote PC Access configurations, install the VDA for Windows Desktop OS on each physical office PC that users will access remotely.</li> <li>As an alternative to using the full-product ISO to install VDAs, you can use a standalone VDA installation package. For details, see <a href="#">Install VDAs using the standalone package</a>.</li> </ul>
--

The latest Virtual Delivery Agents (VDAs) are not supported on Windows XP or Windows Vista systems. Additionally, some of the features in this release (and other recent releases) cannot be used on those operating systems. To use the full functionality in this release, Citrix recommends you replace Windows XP or Windows Vista systems with Windows 7, Windows 8 or Windows 10, then install a Virtual Delivery Agent from this release.

To accommodate cases when you must continue to accommodate machines running Windows XP or Windows Vista, you can install an earlier Virtual Desktop Agent version (5.6 FP1 with certain hotfixes). See [CTX140941](#) for details.

Keep in mind that:

- You cannot install core components (Controller, Studio, Director, StoreFront, Citrix License Server) on a Windows XP or Windows Vista system.
- Remote PC Access is not supported on Windows Vista systems.
- Citrix support for Windows XP ended April 8, 2014 when Microsoft ended its extended support.
- Continuing to use older VDAs can affect feature availability and VDA registration with the Controller; see [Mixed environment considerations](#).

# 准备虚拟化环境：VMware

Aug 31, 2016

Follow this guidance if you use VMware to provide virtual machines.

1. Install vCenter Server and the appropriate management tools. (No support is provided for vSphere vCenter Linked Mode operation.)
2. Create a VMware user account with the following permissions, at the DataCenter level, at a minimum. This account has permissions to create new VMs and is used to communicate with vCenter.

SDK	User Interface
Datastore.AllocateSpace	Datastore > Allocate space
Datastore.Browse	Datastore > Browse datastore
Datastore.FileManagement	Datastore > Low level file operations
Network.Assign	Network > Assign network
Resource.AssignVMToPool	Resource > Assign virtual machine to resource pool
System.Anonymous, System.Read, and System.View	Added automatically.
Task.Create	Tasks > Create task
VirtualMachine.Config.AddRemoveDevice	Virtual machine > Configuration > Add or remove device
VirtualMachine.Config.AddExistingDisk	Virtual machine > Configuration > Add existing disk
VirtualMachine.Config.AddNewDisk	Virtual machine > Configuration > Add new disk
VirtualMachine.Config.AdvancedConfig	Virtual machine > Configuration > Advanced
VirtualMachine.Config.CPUCount	Virtual machine > Configuration > Change CPU Count
VirtualMachine.Config.Memory	Virtual machine > Configuration > Memory

<b>VirtualMachine.Config.RemoveDisk</b>	User interface > Configuration > Remove disk
<b>VirtualMachine.Config.Resource</b>	Virtual machine > Configuration > Change resource
<b>VirtualMachine.Config.Settings</b>	Virtual machine > Configuration > Settings
<b>VirtualMachine.Interact.PowerOff</b>	Virtual machine > Interaction > Power Off
<b>VirtualMachine.Interact.PowerOn</b>	Virtual machine > Interaction > Power On
<b>VirtualMachine.Interact.Reset</b>	Virtual machine > Interaction > Reset
<b>VirtualMachine.Interact.Suspend</b>	Virtual machine > Interaction > Suspend
<b>VirtualMachine.Inventory.Create</b>	Virtual machine > Inventory > Create new
<b>VirtualMachine.Inventory.CreateFromExisting</b>	Virtual machine > Inventory > Create from existing
<b>VirtualMachine.Inventory.Delete</b>	Virtual machine > Inventory > Remove
<b>VirtualMachine.Inventory.Register</b>	Virtual machine > Inventory > Register
<b>VirtualMachine.Provisioning.Clone</b>	Virtual machine > Provisioning > Clone virtual machine
<b>VirtualMachine.Provisioning.DiskRandomAccess</b>	Virtual machine > Provisioning > Allow disk access
<b>VirtualMachine.Provisioning.GetVmFiles</b>	Virtual machine > Provisioning > Allow virtual machine download
<b>VirtualMachine.Provisioning.PutVmFiles</b>	Virtual machine > Provisioning > Allow virtual machine files upload
<b>VirtualMachine.Provisioning.DeployTemplate</b>	Virtual machine > Provisioning > Deploy template
<b>VirtualMachine.Provisioning.MarkAsVM</b>	Virtual machine > Provisioning > Mark as virtual machine
<b>VirtualMachine.State.CreateSnapshot</b>	vSphere 5.0, Update 2 and vSphere 5.1, Update 1: Virtual machine > State > Create snapshot  vSphere 5.5: Virtual machine > Snapshot management > Create snapshot

<b>SDK</b> VirtualMachine.State.RemoveSnapshot	<b>User Interface</b> vSphere 5.0, Update 2 and vSphere 5.1, Update 1: Virtual machine > State > Remove snapshot  vSphere 5.5: Virtual machine > Snapshot management > Remove snapshot
VirtualMachine.State.RevertToSnapshot	vSphere 5.0, Update 2 and vSphere 5.1, Update 1: Virtual machine > State > Revert to snapshot  vSphere 5.5: Virtual machine > Snapshot management > Revert to snapshot

3. If you want the VMs you create to be tagged, add the following permissions for the user account:

<b>SDK</b>	<b>User Interface</b>
Global.ManageCustomFields	Global > Manage custom attributes
Global.SetCustomField	Global > Set custom attribute

To ensure that you use a clean base image for creating new VMs, tag VMs created with Machine Creation Services to exclude them from the list of VMs available to use as base images.

To protect vSphere communications, Citrix recommends that you use HTTPS rather than HTTP. HTTPS requires digital certificates. Citrix recommends you use a digital certificate issued from a certificate authority in accordance with your organization's security policy.

If you are unable to use a digital certificate issued from a certificate authority, and your organization's security policy permits it, you can use the VMware-installed self-signed certificate. Add the VMware vCenter certificate to each Controller. Follow this procedure:

1. Add the fully qualified domain name (FQDN) of the computer running vCenter Server to the hosts file on that server, located at %SystemRoot%/WINDOWS/system32/Drivers/etc/. This step is required only if the FQDN of the computer running vCenter Server is not already present in the domain name system.
2. Obtain the vCenter certificate using any of the following methods:
  - From the vCenter server:
    1. Copy the file rui.crt from the vCenter server to a location accessible on your Delivery Controllers.
    2. On the Controller, navigate to the location of the exported certificate and open the rui.crt file.
  - Download the certificate using a web browser. If you are using Internet Explorer, depending on your user account, you may need to right-click on Internet Explorer and choose Run as Administrator to download or install the certificate.
    1. Open your web browser and make a secure web connection to the vCenter server, for example <https://server1.domain1.com>
    2. Accept the security warnings.
    3. Click on the address bar where it shows the certificate error.

4. View the certificate and click on the Details tab.
  5. Select Copy to file and export in .CER format, providing a name when prompted to do so.
  6. Save the exported certificate.
  7. Navigate to the location of the exported certificate and open the .CER file.
- Import directly from Internet Explorer running as an administrator:
    1. Open your web browser and make a secure web connection to the vCenter server; for example <https://server1.domain1.com>.
    2. Accept the security warnings.
    3. Click on the address bar where it shows the certificate error.
    4. View the certificate.
  - Import the certificate into the certificate store on each of your Controllers:
    1. Click Install certificate, select Local Machine, and then click Next.
    2. Select Place all certificates in the following store, and then click Browse.
    3. If you are using Windows Server 2008 R2:
      1. Select the Show physical stores check box.
      2. Expand Trusted People.
      3. Select Local Computer.
      4. Click Next, then click Finish.
    - If you are using Windows Server 2012 or Windows Server 2012 R2:
      1. Select Trusted People, then click OK.
      2. Click Next, then click Finish.

**Important:** If you change the name of the vSphere server after installation, you must generate a new self-signed certificate on that server before importing the new certificate.

Use a master VM to provide user desktops and applications.

1. Install a VDA on the master VM, selecting the option to optimize the desktop, which improves performance.
2. Take a snapshot of the master VM to use as a back-up. For more information, see [Prepare a master image](#).

If you are using Studio to create VMs, rather than selecting an existing machine catalog, specify the following information when setting up your hosting infrastructure to create virtual desktops.

1. Select the VMware vSphere host type.
2. Enter the address of the access point for the vCenter SDK (<https://vmware.example.com/sdk>).
3. Enter the credentials for the VMware user account you set up earlier that has permissions to create new VMs. Specify the username in the form domain/username.

# 准备虚拟化环境：Microsoft System Center Virtual Machine Manager

May 28, 2016

Follow this guidance if you use Hyper-V with Microsoft System Center Virtual Machine Manager (VMM) to provide virtual machines.

This release supports:

- VMM 2012 — Provides improved management capabilities, letting you manage the entire virtualized datacenter as well as virtual machines. This release now orchestrates cluster host patching as well as integrating with Windows Server Update Services, allowing you to define baselines of patches that each host needs.
- VMM 2012 SP1 — Provides performance improvements for Machine Creation Services (MCS) when using SMB 3.0 on file servers with clustered shared volumes and Storage Area Networks (SANs). These file shares provide low cost caching and reduced IO on the SAN storage improving the performance.
- VMM 2012 R2 — Enables at-scale management of major Windows Server 2012 R2 capabilities, including running VM snapshots, dynamic VHDX resize, and Storage Spaces.

This release supports only Generation 1 virtual machines with VMM 2012 R2. Generation 2 virtual machines are not supported for Machine Creation Services (MCS) and Provisioning Services deployments. When creating VMs with MCS or Provisioning Services, Generation 2 VMs do not appear in the selection list for a master VM; they have Secure Boot enabled by default, which prevents the VDA from functioning properly.

- Upgrade from VMM 2012 to VMM 2012 SP1 or VMM 2012 R2

For VMM and Hyper-V Hosts requirements, see <http://technet.microsoft.com/en-us/library/gg610649.aspx>. For VMM Console requirements, see <http://technet.microsoft.com/en-us/library/gg610640.aspx>.

A mixed Hyper-V cluster is not supported. An example of a mixed cluster is one in which half the cluster is running Hyper-V 2008 and the other is running Hyper-V 2012.

- Upgrade from VMM 2008 R2 to VMM 2012 SP1

If you are upgrading from XenDesktop 5.6 on VMM 2008 R2, follow this sequence to avoid XenDesktop downtime.

1. Upgrade VMM to 2012 (now running XenDesktop 5.6 and VMM 2012)
2. Upgrade XenDesktop to the latest version (now running the latest XenDesktop and VMM 2012)
3. Upgrade VMM from 2012 to 2012 SP1 (now running the latest XenDesktop and VMM 2012 SP1)

- Upgrade from VMM 2012 SP1 to VMM 2012 R2

If you are starting from XenDesktop or XenApp 7.x on VMM 2012 SP1, follow this sequence to avoid XenDesktop downtime.

1. Upgrade XenDesktop or XenApp to the latest version (now running the latest XenDesktop or XenApp, and VMM 2012 SP1)

2. Upgrade VMM 2012 SP1 to 2012 R2 (now running the latest XenDesktop or XenApp, and VMM 2012 R2)

1. Install and configure a hypervisor.

1. Install Microsoft Hyper-V server and VMM on your servers. All Delivery Controllers must be in the same forest as the

VMM servers.

2. Install the System Center Virtual Machine Manager console on all Controllers.

3. Verify the following account information:

- The account you use to specify hosts in Studio is a VMM administrator or VMM delegated administrator for the relevant Hyper-V machines. If this account only has the delegated administrator role in VMM, the storage data is not listed in Studio during the host creation process.
- The user account used for Studio integration must also be a member of the administrators local security group on each Hyper-V server to support VM life cycle management (such as VM creation, update, and deletion).

Note: Installing Controller on a server running Hyper-V is not supported.

2. Create a master VM.

1. Install a Virtual Delivery Agent on the master VM, and select the option to optimize the desktop. This improves performance.

2. Take a snapshot of the master VM to use as a backup.

For more information, see [Prepare a master image](#).

3. Create virtual desktops. If you are using MCS to create VMs, when creating a Site or a connection,

1. Select the Microsoft virtualization host type.

2. Enter the address as the fully qualified domain name of the host server.

3. Enter the credentials for the administrator account you set up earlier that has permissions to create new VMs.

4. In the Host Details dialog box, select the cluster or standalone host to use when creating new VMs.

Important: Browse for and select a cluster or standalone host even if you are using a single Hyper-V host deployment.

For Machine Catalogs created with MCS on SMB 3 file shares for VM storage, make sure that credentials meet the following requirements so that calls from the Controller's Hypervisor Communications Library (HCL) connect successfully to SMB storage:

- VMM user credentials must include full read write access to the SMB storage.
- Storage virtual disk operations during VM life cycle events are performed through the Hyper-V server using the VMM user credentials.

When you use SMB as storage, enable the Authentication Credential Security Support Provider (CredSSP) from the Controller to individual Hyper-V machines when using VMM 2012 SP1 with Hyper-V on Windows Server 2012. For more information, see [CTX137465](#).

Using a standard PowerShell V3 remote session, the HCL uses CredSSP to open a connection to the Hyper-V machine. This feature passes Kerberos-encrypted user credentials to the Hyper-V machine, and the PowerShell commands in the session on the remote Hyper-V machine run with the credentials provided (in this case, those of the VMM user), so that communication commands to storage work correctly.

The following tasks use PowerShell scripts that originate in the HCL and are then sent to the Hyper-V machine to act on the SMB 3.0 storage.

- **Consolidate Master Image** - A master image creates a new MCS provisioning scheme (machine catalog). It clones and flattens the master VM ready for creating new VMs from the new disk created (and removes dependency on the original master VM).

ConvertVirtualHardDisk on the root\virtualization\v2 namespace

Example:

```
$ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
$result = $ims.ConvertVirtualHardDisk($diskName, $vhdstext)
$result
```

- **Create difference disk** - Creates a difference disk from the master image generated by consolidating the master image. The difference disk is then attached to a new VM.

CreateVirtualHardDisk on the root\virtualization\v2 namespace

Example:

```
$ims = Get-WmiObject -class $class -namespace "root\virtualization\v2";
$result = $ims.CreateVirtualHardDisk($vhdstext);
$result
```

- **Upload identity disks** - The HCL cannot directly upload the identity disk to SMB storage. Therefore, the Hyper-V machine must upload and copy the identity disk to the storage. Because the Hyper-V machine cannot read the disk from the Controller, the HCL must first copy the identity disk through the Hyper-V machine as follows.

1. The HCL uploads the Identity to the Hyper-V machine through the administrator share.
2. The Hyper-V machine copies the disk to the SMB storage through a PowerShell script running in the PowerShell remote session. A folder is created on the Hyper-V machine and the permissions on that folder are locked for the VMM user only (through the remote PowerShell connection).
3. The HCL deletes the file from the administrator share.
4. When the HCL completes the identity disk upload to the Hyper-V machine, the remote PowerShell session copies the identity disks to SMB storage and then deletes it from the Hyper-V machine.

The identity disk folder is recreated if it is deleted so that it is available for reuse.

- **Download identity disks** - As with uploads, the identity disks pass through the Hyper-V machine to the HCL. The following process creates a folder that only has VMM user permissions on the Hyper-V server if it does not exist.
  1. The HyperV machine copies the disk from the SMB storage to local Hyper-V storage through a PowerShell script running in the PowerShell V3 remote session.
  2. HCL reads the disk from the Hyper-V machine's administrator share into memory.
  3. HCL deletes the file from the administrator share.

- **Personal vDisk creation** - If the administrator creates the VM in a Personal vDisk machine catalog, you must create an empty disk (PvD).

The call to create an empty disk does not require direct access to the storage. If you have PvD disks that reside on different storage than the main or operating system disk, then use remote PowerShell to create the PvD in a directory folder that has the same name of the VM from which it was created. For CSV or LocalStorage, do not use remote PowerShell. Creating the directory before creating an empty disk avoids VMM command failure.

From the Hyper-V machine, perform a mkdir on the storage.

# 准备使用 Microsoft System Center Configuration Manager

May 28, 2016

Sites that use System Center Configuration Manager (Configuration Manager) 2012 to manage access to applications and desktops on physical devices can extend that use to XenApp or XenDesktop through these integration options.

- **Citrix Connector 7.5 for Configuration Manager 2012** – Citrix Connector provides a bridge between Configuration Manager and XenApp or XenDesktop. The Connector enables you to unify day-to-day operations across the physical environments you manage with Configuration Manager and the virtual environments you manage with XenApp or XenDesktop. For information about the Connector, see [Citrix Connector 7.5 for System Center Configuration Manager 2012](#).
- **Configuration Manager Wake Proxy feature** – Whether or not your environment includes Citrix Connector, the Remote PC Access Wake on LAN feature requires Configuration Manager. For more information, see [Configuration Manager and Remote PC Access Wake on LAN](#).
- **XenApp and XenDesktop properties** – XenApp and XenDesktop properties enable you to identify Citrix virtual desktops for management through Configuration Manager. These properties are automatically used by the Citrix Connector but can also be manually configured, as described in the following section.

Properties are available to Microsoft System Center Configuration Manager 2012 and 2012 R2 to manage virtual desktops.

Boolean properties displayed in Configuration Manager 2012 may appear as 1 or 0, not true or false.

The properties are available for the `Citrix_virtualDesktopInfo` class in the `Root\Citrix\DesktopInformation` namespace. Property names come from the Windows Management Instrumentation (WMI) provider.

Property	Description
AssignmentType	Sets the value of <code>IsAssigned</code> . Valid values are: <ul style="list-style-type: none"><li>• ClientIP</li><li>• ClientName</li><li>• None</li><li>• User – Sets <code>IsAssigned</code> to True</li></ul>
BrokerSiteName	Site; returns the same value as <code>HostIdentifier</code> .
DesktopCatalogName	Machine Catalog associated with the desktop.
DesktopGroupName	Delivery Group associated with the desktop.
HostIdentifier	Site; returns the same value as <code>BrokerSiteName</code> .

IsAssigned	True to assign the desktop to a user, set to False for a random desktop.
IsMasterImage	Allows decisions about the environment. For example, you may want to install applications on the Master Image and not on the provisioned machines, especially if those machines are in a clean state on boot machines. Valid values are: <ul style="list-style-type: none"> <li>True on a VM that is used as a master image (this value is set during installation based on a selection).</li> <li>Cleared on a VM that is provisioned from that image.</li> </ul>
IsVirtualMachine	True for a virtual machine, false for a physical machine.
OSChangesPersist	False if the desktop operating system image is reset to a clean state every time it is restarted; otherwise, true.
PersistentDataLocation	The location where Configuration Manager stores persistent data. This is not accessible to users.
PersonalvDiskDriveLetter	For a desktop with a Personal vDisk, the drive letter you assign to the Personal vDisk.
BrokerSiteName, DesktopCatalogName, DesktopGroupName, HostIdentifier	Determined when the desktop registers with the Controller; they are null for a desktop that has not fully registered.

To collect the properties, run a hardware inventory in Configuration Manager. To view the properties, use the Configuration Manager Resource Explorer. In these instances, the names may include spaces or vary slightly from the property names. For example, **BrokerSiteName** may appear as Broker Site Name. For information about the following tasks, see [Citrix WMI Properties and System Center Configuration Manager 2012](#):

- Configure Configuration Manager to collect Citrix WMI properties from the Citrix VDA
- Create query-based device collections using Citrix WMI properties
- Create global conditions based on Citrix WMI properties
- Use global conditions to define application deployment type requirements

You can also use Microsoft properties in the Microsoft class CCM/DesktopMachine in the Root\ccm\_vdi namespace. For more information, see the Microsoft documentation.

For information about planning for and delivering Remote PC Access, see [Remote PC Access](#) and [Provide users with](#)

## [Remote PC Access](#).

To configure the Remote PC Access Wake on LAN feature, complete the following before installing a VDA on the office PCs and using Studio to create or update the Remote PC Access deployment:

- Configure Configuration Manager 2012 within the organization, and then deploy the Configuration Manager client to all Remote PC Access machines, allowing time for the scheduled SCCM inventory cycle to run (or forcing one manually, if required). The access credentials you specify in Studio to configure the connection to Configuration Manager must include collections in the scope and the Remote Tools Operator role.
- For Intel Active Management Technology (AMT) support:
  - The minimum supported version on the PC must be AMT 3.2.1.
  - Provision the PC for AMT use with certificates and associated provisioning processes.
- For Configuration Manager Wake Proxy and/or magic packet support:
  - Configure Wake on LAN in each PC's BIOS settings.
  - For Configuration Manager Wake Proxy support, enable the option in Configuration Manager. For each subnet in the organization that contains PCs that will use the Remote PC Access Wake on LAN feature, ensure that three or more machines can serve as sentinel machines.
  - For magic packet support, configure network routers and firewalls to allow magic packets to be sent, using either a subnet-directed broadcast or unicast.

After you install the VDA on office PCs, enable or disable power management when you create the Remote PC Access deployment in Studio.

- If you enable power management, specify connection details: the Configuration Manager address and access credentials, plus a name.
- If you do not enable power management, you can add a power management (Configuration Manager) connection later and then edit a Remote PC Access machine catalog to enable power management and specify the new power management connection.

You can edit a power management connection to configure the use of the Configuration Manager Wake Proxy and magic packets, as well as change the packet transmission method.

# 使用图形界面进行安装

May 28, 2016

Before beginning any installation, review and complete the tasks in [Prepare to install](#).

Launch the installer graphical interface:

1. Download the product package and unzip it. Optionally, burn a DVD of the ISO file.
2. Log on to the server where you are installing the components, using a local administrator account.
3. Insert the DVD in the drive or mount the ISO file. If the installer does not launch automatically, double-click the AutoSelect application or the mounted drive.
4. Select the component you want to install:
  - If you're just getting started, select Delivery Controller. From there, you can install the Delivery Controller and optionally, Studio, Director, License Server, and StoreFront on the same server.
  - If you've already installed some components and want to extend your deployment, click the component you want to install from the right column. This column offers core components and the Universal Print Server, which you can install on your print server.
  - To install a Virtual Delivery Agent (VDA), click the available VDA entry - the installer knows which one is right for the operating system where you're running the installer.

Later, if you want to customize a VDA that you've already installed:

1. From the Windows feature for removing or changing programs, select Citrix Virtual Delivery Agent <version-number>, then right-click and select Change.
2. Select Customize Virtual Delivery Agent Settings. When the installer launches, you can change the Controller addresses, TCP/IP port to register with the Controller (default = 80), or whether to automatically open Windows Firewall port exceptions.

You can also use the graphical interface to upgrade components; see [Upgrade a deployment](#).

As an alternative to using the full-product ISO to install VDAs, you can use a standalone VDA installation package. For details, see [Install VDAs using the standalone package](#).

# 使用命令行安装

Jan 24, 2018

Use the command line interface to:

- Install one or more core components: Delivery Controller, Citrix Studio, Citrix Director, License Server, and StoreFront.
- Install a Virtual Delivery Agent (VDA) on a master image or on a virtual or physical machine.  
You can also customize scripts provided on the media, then use them to install and remove VDAs in Active Directory.
- Customize a previously-installed VDA.
- Install a Universal Print Server, which provisions network session printers. The Controller already has the Universal Print Server functionality; you need only install the Universal Print Server on the print servers in your environment.

You can also:

- Remove components from this version that you previously installed, using the /remove or /removeall options. For details, see [Remove components](#).
- Upgrade components; for details, see [Upgrade a deployment](#).

To see command execution progress and return values, you must be the original administrator or use 'Run as administrator.' For more information, see the Microsoft command documentation.

Important: Before beginning an installation, read and complete the tasks in [Prepare to install](#).

From the \x64\XenDesktop Setup directory on the media, run the XenDesktopServerSetup.exe command. The following table describes command options.

Note: To install XenApp, include the /xenapp option on the command line. To install XenDesktop, do not include the /xenapp option.

Option	Description
/help or /h	Displays command help.
/quiet or /passive	No user interface appears during the installation. The only evidence of the installation process is in Windows Task Manager. If this option is omitted, the graphical interface launches.
/logpath path	Log file location. The specified folder must already exist; the installer does not create it. Default = "%TEMP%\Citrix\XenDesktop Installer"
/noreboot	Prevents a restart after installation. (For most core components, a restart is not enabled by default.)
/remove	Removes the core components specified with the /components option.
/removeall	Removes all installed core components.
/xenapp	Installs XenApp. If this option is omitted, XenDesktop is installed.
/configure_firewall	Opens all ports in the Windows firewall needed by components being installed, if the Windows Firewall Service is running, even if the firewall is not enabled. If you are using a third-party firewall or no firewall, you must manually open the ports.
/components component [component]...	(Required.) Comma-separated list of components to install or remove. Valid values are: <ul style="list-style-type: none"><li>• CONTROLLER - Controller</li><li>• DESKTOPSTUDIO - Studio</li><li>• DESKTOPDIRECTOR - Director</li><li>• LICENSESERVER - Citrix Licensing</li><li>• STOREFRONT - StoreFront</li></ul> If this option is omitted, all components are installed (or removed, if the /remove option is also specified).
/installdir directory	Existing empty directory where components will be installed. Default = c:\Program Files\Citrix.
/tempdir directory	Directory that holds temporary files during installation. Default = c:\Windows\Temp.
/nosql	Prevents installation of Microsoft SQL Server Express on the server where you are installing the Controller. If this option is omitted, SQL Server Express will be installed.

Option	Description
For example, the following command installs a XenDesktop Controller, Studio, Citrix Licensing, and SQL Server Express on the server. Ports required for component communications will be opened automatically.	
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /components controller,desktopstudio,licenseserver /configure_firewall	
The following command installs a XenApp Controller, Studio, and SQL Server Express on the server. Ports required for component communication will be opened automatically.	
\x64\XenDesktop Setup\XenDesktopServerSetup.exe /xenapp /components controller,desktopstudio /configure_firewall	
When installing a VDA for use with Remote PC Access, specify only options that are valid on physical machines (not VMs or master images) and for VDAs for Windows Desktop OS.	
From the XenDesktop Setup directory on the product media, run the XenDesktopVdaSetup.exe command. The following table describes command options. Unless otherwise noted, options apply to physical and virtual machines, and to VDAs for Windows Desktop OS and VDAs for Windows Server OS.	
Option	Description
/h or /help	Displays command help.
/quiet or /passive	No user interface appears during the installation. The only evidence of the installation and configuration process is in Windows Task Manager. If this option is omitted, the graphical interface launches.
/logpath path	Log file location. The specified folder must already exist; the installer does not create it. Default = "%TEMP%\CitrixXenDesktop Installer"
/noreboot	Prevents a restart after installation. The VDA will not be fully available for use until after a restart.
/remove	Removes the components specified with the /components option.
/removeall	Removes all installed VDA components.
/reconfig	Customizes previously-configured VDA settings when used with the /portnumber, /controllers, or /enable_hdx_ports options. If you specify this option without also specifying the /quiet option, the graphical interface for customizing the VDA launches.
/portnumber port	(Valid only if the /reconfig option is specified.) Port number to enable for communications between the VDA and the Controller. The previously-configured port is disabled, unless it is port 80.
/components component[,component]	Comma-separated list of components to install or remove. Valid values are: <ul style="list-style-type: none"> <li>• VDA - installs the VDA</li> <li>• PLUGINS - installs the Citrix Receiver for Windows (CitrixReceiver.exe)</li> </ul> <p>If this option is omitted, all components are installed.</p>
/installdir directory	Existing empty directory where components will be installed. Default = c:\Program Files\Citrix.
/tempdir directory	Directory to hold temporary files during installation. (This option is not available in the graphical interface.) Default = c:\Windows\Temp.
/site_guid guid	Globally Unique Identifier of the site Active Directory Organizational Unit (OU). This associates a virtual desktop with a Site when you are using Active Directory for discovery (auto-update is the recommended and default discovery method). The site GUID is a site property displayed in Studio. Do not specify both the /site_guid and /controllers options.
/controllers "controller [controller] [...]"	Space-separated Fully Qualified Domain Names (FQDNs) of Controllers with which the VDA can communicate, enclosed in quotation marks. Do not specify both the /site_guid and /controllers options.
/xa_server_location url	URL of the server for Windows server applications.
/enable_remote_assistance	Enables Windows Remote Assistance for use with Director. If you specify this option, Windows opens TCP port 3389 in the firewall, even if you omit the /enable_hdx_ports option.

<code>/enable_hdx_ports</code>	Opens ports in the Windows firewall required by the Controller and features you specified (Windows Remote Assistance, real-time transport, and optimize), if the Windows Firewall Service is detected, even if the firewall is not enabled. If you are using a different firewall or no firewall, you must configure the firewall manually.
<code>/optimize</code>	Enables optimization for VDAs running in a VM on a hypervisor. VM optimization includes disabling offline files, disabling background defragmentation, and reducing event log size. Do not specify this option for Remote PC Access. For more information about the optimization tool, see <a href="#">CTX125874</a> .
<code>/baseimage</code>	(Valid only when installing a VDA for Windows Desktop OS on a VM.) Enables the use of Personal vDisks with a master image. For more information, see <a href="#">Personal vDisks</a> .
<code>/enable_hdx_3d_pro</code>	Installs the VDA for HDX 3D Pro. For more information, see the HDX 3D Pro documentation.
<code>/enable_real_time_transport</code>	Enables or disables use of UDP for audio packets (Real-Time Audio Transport for audio). Enabling this feature can improve audio performance. Include the <code>/enable_hdx_ports</code> option if you want the UDP ports opened automatically if the Windows Firewall Service is detected.
<code>/masterimage</code>	(Valid only when installing a VDA on a VM.) Sets up the VDA as a master image.
<code>/virtualmachine</code>	(Valid only when installing a VDA on a VM.) Overrides detection by the installer of a physical machine, where BIOS information passed to VMs makes them appear as physical machines.
<code>/nodesktopexperience</code>	(Valid only when installing a VDA for Windows Server OS.) Prevents enabling of the Enhanced Desktop Experience feature. This feature is also controlled with the Enhanced Desktop Experience Citrix policy setting.
<code>/nocitrixwddm</code>	(Valid only on Windows 7 machines that do not include a WDDM driver.) Disables installation of the Citrix WDDM driver.
<code>/servervdi</code>	Installs a VDA for Windows Desktop OS on a supported Windows Server. Omit this option when installing a VDA for Windows Server OS on a Windows Server. Before using this option, see <a href="#">Server VDI</a> . <b>Note:</b> Add the <code>/masterimage</code> option if you are installing the VDA on an image, and will use MCS to create server VMs from that image.
<code>/installwithsecurebootenabled</code>	Allows VDA installation when Secure Boot is enabled. If this option is omitted, a warning displays that Secure Boot must be disabled to successfully install a VDA.
<code>/exclude "Personal vDisk","Machine Identity Service"</code>	(Valid only when upgrading from an earlier 7.x VDA version on a physical machine.) Excludes Personal vDisk and Machine Identity Service from the upgrade. For advanced use of this option, see <a href="#">CTX140972</a> .

For example, the following command installs a VDA for Windows Desktop OS and Citrix Receiver to the default location on a VM. This VDA will be used as a master image. The VDA will register initially with the Controller on the server named 'Contr-Main' in the domain 'mydomain,' and will use Personal vDisks, the optimization feature, and Windows Remote Assistance.

```
XenDesktop SetupXenDesktopVdaSetup.exe /quiet /components  
vda.plugins /controllers "Contr-Main.mydomain.local" /enable_hdx_ports /optimize  
/masterimage /baseimage /enable_remote_assistance
```

The following command installs a VDA for Windows Desktop OS and Citrix Receiver to the default location on an office PC that will be used with Remote PC Access. The machine will not be restarted after the VDA is installed; however, a restart is required before the VDA can be used. The VDA will register initially with the Controller on the server named 'Contr-East' in the domain 'mydomain,' and will use UDP for audio packets. HDX ports will be opened if the Windows Firewall service is detected.

```
XenDesktop SetupXenDesktopVdaSetup.exe /quiet /components vda.plugins /controllers "Contr-East.mydomain.local" /enable_hdx_ports /enable_real_time_transport /noreboot
```

As an alternative to using the full-product ISO to install VDAs, you can use a standalone VDA installation package. For details, see [Install VDAs using the standalone package](#).

By default, when a machine restart is needed during an installation, the installer resumes automatically after the restart completes. To override the default, specify `/noresume` with the installation command. This can be helpful if you must re-mount the media or want to capture information during an automated installation.

After you install a VDA, you can customize several settings. From the `\x64\XenDesktop Setup` directory on the product media, run the `XenDesktopVdaSetup.exe` command, using one or more of the following options, which are described above.

- `/reconfigure` - this option is required when customizing a VDA
- `/h` or `/help`
- `/quiet`

- /noreboot
- /controllers
- /portnumber port
- /enable\_hdx\_ports

Run one of the following commands on each print server:

- On a supported 32-bit operating system: From the \x86\Universal Print Server\ directory on the Citrix installation media, run UpsServer\_x86.msi.
- On a supported 64-bit operating system: From the \x64\Universal Print Server\ directory on the Citrix installation media, run UpsServer\_x64.msi.

In XenApp and XenDesktop 7.6 FP3, the UPS package contains updated versions of the standalone UPS client and server components. For installation instructions, see [Provision printers](#).

In XenApp and XenDesktop 7.6 FP3, if you install the Universal Print Server using the command line, we recommend that you add the command option, ENABLE\_CEIP set to 1, to opt in to the [Citrix Customer Experience Improvement Program](#) (CEIP).

For example:



```
msiexec /i UpsServer.msi ENABLE_CEIP=1
```

When you opt in, anonymous statistics and usage information is sent to Citrix to help improve the quality and performance of our products.

To deploy UpsServer\_x86.msi on Windows 2008 32-bit platform, the Minimum Version for Windows Installer for the cdf\_x86.msi and UpsServer\_x86.msi needs to be adjusted first, either by using VB scripts or by using a tool such as Orca. To do this:

1. Copy the 7.6 FP3 32-bit versions of the CDF and UPS msi's (cdf\_x86.msi and UpsServer\_x86.msi) to a temp folder.
2. Install the WiSumInf.vbs script or Orca tool, both available in the [Windows SDK Components for Windows Installer Developers](#) package. For more information on the script, see the MSDN article [Manage Summary Information](#).
3. You can modify the Minimum Version for the Windows Installer using one of the two methods below:
  - Using WiSumInf.vbs script:
    1. Copy WiSumInf.vbs to the same temp folder with the two Citrix msi's.
    2. Run the script for each package with these parameters:
      - WiSumInf.vbs cdf\_x86.msi Pages=405
      - WiSumInf.vbs UpsServer\_x86.msi Pages=405
  - Using Orca, open each of the cdf\_x86.msi and UpsServer\_x86.msi packages, go to the View menu > Summary Information, and change the value of the "Schema" textbox to 405.

# 创建站点

May 28, 2016

A Site is the name you give to a product deployment. It comprises the Delivery Controllers and the other core components, VDAs, virtual resource connections (if used), plus the machine catalogs and Delivery Groups you create and manage. A Site does not necessarily correspond to a geographical location, although it can. You create the Site after you install the components and before creating machine catalogs and Delivery Groups.

The following table describes the tasks to complete and things to consider or be aware of before starting the Site creation wizard in Studio.

✔	Description																				
	<p>Decide which type of Site you will create:</p> <ul style="list-style-type: none"><li>Application and desktop delivery Site - When you choose to create an application and desktop delivery Site, you can further choose to create a full deployment Site (recommended) or a empty Site. (Empty Sites are only partially configured, and are usually created by advanced users.)</li><li>Remote PC Access Site - Allows designated users to remotely access their office PCs through a secure connection. If you will use the Remote PC Access Wake on LAN feature, complete the tasks described in <a href="#">Configuration Manager and Remote PC Access Wake on LAN</a>.</li></ul> <p>If you create an application and desktop delivery deployment now, you can add a Remote PC Access deployment later. Conversely, if you create a Remote PC Access deployment now, you can add a full deployment later.</p>																				
	<p>Site creation includes creating the Site Configuration database. Make sure the SQL Server software is installed before you create a Site.</p> <p>To create the database, you must be a local administrator and a domain user. You must also either have SQL Server permissions, or you can generate scripts to give to your database administrator to run.</p> <ul style="list-style-type: none"><li>Permissions – you need the following permissions when setting up the database; the permissions can be explicitly configured or acquired by Active Directory group membership:</li></ul> <table border="1"><thead><tr><th data-bbox="234 1462 472 1531">Operation</th><th data-bbox="472 1462 1128 1531">Purpose</th><th data-bbox="1128 1462 1266 1531">Server role</th><th data-bbox="1266 1462 1488 1531">Database role</th></tr></thead><tbody><tr><td data-bbox="234 1531 472 1686">Database creation</td><td data-bbox="472 1531 1128 1686">Create a suitable empty database</td><td data-bbox="1128 1531 1266 1686">dbcreator</td><td data-bbox="1266 1531 1488 1686"></td></tr><tr><td data-bbox="234 1686 472 1814">Schema creation</td><td data-bbox="472 1686 1128 1814">Create all service-specific schemas and add the first Controller to the Site</td><td data-bbox="1128 1686 1266 1814">securityadmin *</td><td data-bbox="1266 1686 1488 1814">db_owner</td></tr><tr><td data-bbox="234 1814 472 1920">Add Controller</td><td data-bbox="472 1814 1128 1920">Add a Controller (other than the first) to the Site</td><td data-bbox="1128 1814 1266 1920">securityadmin *</td><td data-bbox="1266 1814 1488 1920">db_owner</td></tr><tr><td data-bbox="234 1920 472 2014">Add Controller (mirror server)</td><td data-bbox="472 1920 1128 2014">Add a Controller login to the database server currently in the mirror role of a mirrored database</td><td data-bbox="1128 1920 1266 2014">securityadmin *</td><td data-bbox="1266 1920 1488 2014"></td></tr></tbody></table>	Operation	Purpose	Server role	Database role	Database creation	Create a suitable empty database	dbcreator		Schema creation	Create all service-specific schemas and add the first Controller to the Site	securityadmin *	db_owner	Add Controller	Add a Controller (other than the first) to the Site	securityadmin *	db_owner	Add Controller (mirror server)	Add a Controller login to the database server currently in the mirror role of a mirrored database	securityadmin *	
Operation	Purpose	Server role	Database role																		
Database creation	Create a suitable empty database	dbcreator																			
Schema creation	Create all service-specific schemas and add the first Controller to the Site	securityadmin *	db_owner																		
Add Controller	Add a Controller (other than the first) to the Site	securityadmin *	db_owner																		
Add Controller (mirror server)	Add a Controller login to the database server currently in the mirror role of a mirrored database	securityadmin *																			

	Description	Purpose	Server role	Database role
	Schema update	Apply schema updates or hotfixes		db_owner role
<p>* While technically more restrictive, in practice, the securityadmin server role should be treated as equivalent to the sysadmin server role.</p> <p>When using Studio to perform these operations, the user account must be a member of the sysadmin server role.</p>				
<p>If your Studio user credentials do not include these permissions, you are prompted for SQL Server user credentials.</p> <ul style="list-style-type: none"> <li>Scripts - If your database server is locked down and you do not have the required SQL Server permissions, the Site creation wizard can generate two database scripts: one that sets up the database and the other to use in a mirroring environment. After you request script generation, you give the generated scripts to your database administrator (or someone with required SQL Server permissions) to run on the database server, and the mirrored database, if needed. After the script is executed and the database is successfully created, you can finish creating the Site.</li> </ul>				
<p>Consider if you will use the 30-day free trial license that allows you to add license files later, or if you will use existing licenses. You can add or download license files from within the Site creation wizard.</p>				
<p>Configure your virtualization resource (host) environment.</p> <p>If you use XenServer:</p> <ul style="list-style-type: none"> <li>See the XenServer documentation.</li> <li>You must provide the credentials for a VM Power Admin or higher-level user.</li> <li>Citrix recommends using HTTPS to secure communications with XenServer. To use HTTPS, you must replace the default SSL certificate that was installed on XenServer with a certificate from a trusted authority; see <a href="#">CTX128656</a>.</li> <li>You can configure high availability if it is enabled on the XenServer. Citrix recommends that you select all servers in the pool to allow communication with XenServer if the pool master fails. It can be selected from "Edit High Availability" of added host.</li> <li>You can also select a GPU type and group, or passthrough, if the XenServer supports vGPU. The display indicates if the selection has dedicated GPU resources.</li> </ul> <p>If you use VMware, see that product's documentation and <a href="#">Prepare the virtualization environment: VMware</a>.</p> <p>If you are using Hyper-V, see that product's documentation and <a href="#">Prepare the virtualization environment: Microsoft System Center Virtual Machine Manager</a>.</p> <p>Decide if you will use Machine Creation Services (MCS) or other tools to create VMs on the virtualization resources.</p> <p>Decide if you will use shared or local storage. Shared storage is available through the network. If you use shared storage, you can enable the use of IntelliCache to reduce load on the storage device. For information, see <a href="#">Use IntelliCache for XenServer connections</a>.</p>				

	<p><b>Description</b></p> <p>Decide if you will use Personal vDisks and whether they will use shared or local storage. Personal vDisks can use the same or different storage as the VMs. (LTSR: Not supported)</p> <p>If you installed product components in a cloud environment, you will need the API key and secret key values when configuring the first connection. You can export the key file containing those values from AWS or CloudPlatform, and then import them into the Site creation wizard.</p> <p>When you create a Site for a cloud deployment, you will also need the region, availability zone, VPC name, subnet addresses, domain name, security group names, and credentials you configured in AWS.</p>
	<p>Decide if you will use App-V publishing, and configure those resources, if needed.</p>
	<p>Good to know:</p> <ul style="list-style-type: none"> <li>● When you create a Remote PC Access Site: <ul style="list-style-type: none"> <li>● A machine catalog named Remote PC Access Machines, and a Delivery Group named Remote PC Access Desktops are automatically created.</li> <li>● You must specify users or user groups; there is no default action that automatically adds all users.</li> <li>● You can enable the Wake on LAN feature (power management) and specify the Microsoft System Center Configuration Manager (ConfigMgr) address and credentials, plus a connection name.</li> </ul> </li> <li>● The user who creates a Site becomes a Full Administrator; for more information, see <a href="#">Delegated Administration</a>.</li> <li>● When an empty database is created, it has default attributes except: <ul style="list-style-type: none"> <li>● The collation sequence is set to Latin1_General_100_CI_AS_KS (where Latin1_General varies, depending on the country, for example Japanese_100_CI_AS_KS). If this collation setting is not specified during database creation, subsequent creation of the service schemas within the database will fail, and an error similar to "&lt;service&gt;: schema requires a case-insensitive database" appears. (When a database is created manually, any collation sequence can be used, provided it is case-sensitive, accent-sensitive, and kanatype-sensitive; the collation sequence name typically ends with _CI_AS_KS.)</li> <li>● The recovery mode is set to Simple. For use as a mirrored database, change the recovery mode to Full.</li> </ul> </li> <li>● When you create the Site Configuration Database, it also stores configuration changes recorded by the Configuration Logging Service, plus trend and performance data that is used by the Monitoring Service and displayed by Citrix Director. If you use those features and store more than seven days of data, Citrix recommends that you specify different locations for the Configuration Logging Database and the Monitoring Database (known as the secondary databases) after you create a Site.</li> <li>● When naming the Monitoring Database, or a Site Configuration Database that includes the Monitoring Database, using a name that includes spaces causes errors when the database is accessed. For more information, see to <a href="#">CTX200325</a>.</li> <li>● At the end of the Site creation wizard, you are asked if you want to participate in the Citrix Customer Experience Improvement Program. When you join this program, anonymous statistics and usage information is sent to Citrix; see <a href="#">About the Citrix Customer Experience Improvement Program</a> for more information.</li> </ul>

Start Studio, if it is not already open. After you choose to create a Site from the center pane, specify the following:

- The type of Site and the Site name.
- Database information. If you chose during Controller installation to have the default SQL Server Express database

installed, some information is already provided. If you use a database server that is installed on a different server, enter the database server and name:

<b>Database type</b>	<b>What to enter</b>	<b>With this database configuration</b>
Standalone or mirror	servername	The default instance is used and SQL Server uses the default port.
	servername\INSTANCENAME	A named instance is used and SQL Server uses the default port.
	servername,port-number	The default instance is used and SQL Server uses a custom port. (The comma is required.)
Other	cluster-name	A clustered database.
	availability-group-listener	An AlwaysOn database.

After you click Next and are alerted that the services could not connect to a database, indicate that you want Studio to create it. If you do not have permission to edit the database, use Generate database script. The scripts must be run before you can finish creating the Site.

- License Server address in the form name:[port], where name is a Fully Qualified Domain Name (FQDN), NetBIOS, or IP address; FQDN is the recommended format. If you omit the port number, the default is 27000. You cannot proceed until a successful connection is made to the license server.
- (Remote PC Access Sites only.) Power management information, including ConfigMgr connection information.
- Connection information to your virtualization resource and storage information. If you are not using a resource, or if you will use Studio to manage user desktops hosted on dedicated blade PCs, select the connection type None.
- App-V management and App-V publishing server information.
- (Remote PC Access Sites only.) User and machine accounts information.
  - User information. Click Add Users. Select users and user groups, and then click Add users.
  - Machine accounts information. Click Add machine accounts. Select machine accounts, and then click Add machine accounts. Click Add OUs. Select the domain and Organizational Units, and indicate if items in subfolders should be included. Click Add OUs.

You can view an HTML report of the site test results. To run the tests:

1. From Studio, click the Studio (<site-name>) entry at the top of the left pane.
2. In the center pane, click Test site.

# 使用脚本安装或删除 Virtual Delivery Agent

May 28, 2016

The installation media contains sample scripts that install, upgrade, or remove Virtual Delivery Agents (VDAs) for groups of machines in Active Directory. You can also apply the scripts to individual machines, and use them to maintain master images used by Machine Creation Services and Provisioning Services.

Required access:

- The scripts need Everyone Read access to the network share where the VDA installation command is located. The installation command is XenDesktopVdaSetup.exe from the full product ISO, or VDAWorkstationSetup.exe or VDAServerSetup.exe from the standalone installer.
- Logging details are stored on each local machine. If you also want to log results centrally for review and analysis, the scripts need Everyone Read and Write access to the appropriate network share.

To check the results of running a script, examine the central log share. Captured logs include the script log, the installer log, and the MSI installation logs. Each installation or removal attempt is recorded in a time-stamped folder. The folder title indicates if the operation was successful with the prefix PASS or FAIL. You can use standard directory search tools to quickly find a failed installation or removal in the central log share, rather than searching locally on the target machines.

Important: Before beginning any installation, read and complete the tasks in [Prepare to install](#).

1. Obtain the sample script InstallVDA.bat from \Support\AdDeploy\ on the installation media. Citrix recommends that you make a backup of the original script before customizing it.
2. Edit the script:
  - Specify the version of the VDA to install: SET DESIREDVERSION. For example, version 7 can be specified as 7.0; the full value can be found on the installation media in the ProductVersion.txt file (such as 7.0.0.3018); however, a complete match is not required.
  - Specify the network share location from which the installer will be invoked. Point to the root of the layout (the highest point of the tree): the appropriate version of the installer (32-bit or 64-bit) will be called automatically when the script runs. For example: SET DEPLOYSHARE=\\fileserver1\\share1.
  - Optionally, specify a network share location for storing centralized logs. For example: SET LOGSHARE=\\fileserver1\\log1.
  - Specify VDA configuration options as described in [Install using the command line](#). The /quiet and /noreboot options are included by default in the script and are required: SET COMMANDLINEOPTIONS=/QUIET /NOREBOOT.
3. Using Group Policy Startup Scripts, assign the script to the OU in Active Directory where your machines are located. This OU should contain only machines on which you want to install the VDA. When the machines in the OU are restarted, the script runs on all of them, installing a VDA on each machine that has a supported operating system.
  
1. Obtain the sample script UninstallVDA.bat from \Support\AdDeploy\ on the installation media. Citrix recommends that you make a backup of the original script before customizing it.
2. Edit the script.
  - Specify the version of the VDA to remove: SET CHECK\_VDA\_VERSION. For example, version 7 can be specified as 7.0; the full value can be found on the installation media in the ProductVersion.txt file (such as 7.0.0.3018); however, a complete match is not required.
  - Optionally, specify a network share location for storing centralized logs.

3. Using Group Policy Startup Scripts, assign the script to the OU in Active Directory where your machines are located. This OU should contain only machines from which you want to remove the VDA. When the machines in the OU are restarted, the script runs on all of them, removing a VDA from each machine.

The script generates internal log files that describe script execution progress. The script copies a Kickoff\_VDA\_Startup\_Script log to the central log share within seconds of starting the deployment to the machine, so that you can verify that the overall process is working. If this log is not copied to the central log share as expected, you can troubleshoot further by inspecting the local machine: the script places two debugging log files in the %temp% folder on each machine, for early troubleshooting:

- Kickoff\_VDA\_Startup\_Script\_<DateTimeStamp>.log
- VDA\_Install\_ProcessLog\_<DateTimeStamp>.log

Review the content of these logs to ensure that the script is:

- Running as expected.
- Properly detecting the target operating system.
- Correctly configured to point to the ROOT of the DEPLOYSHARE share (contains the file named AutoSelect.exe).
- Capable of authenticating to both the DEPLOYSHARE and LOG shares.

# 使用独立的软件包安装 VDA

Sep 16, 2016

As an alternative to using the full-product XenApp or XenDesktop ISO to install Virtual Delivery Agents (VDAs), you can use a standalone VDA installation package. The smaller package more easily accommodates deployments using Electronic Software Delivery (ESD) packages that are staged or copied locally, have physical machines, or have remote offices.

The standalone VDA package is intended primarily for deployments that use command-line (silent) installation - it supports the same command line parameters as the XenDesktopVdaSetup.exe command, which is used by the full-product installer. The package also offers a graphical interface that is very similar to the VDA installer on the full-product ISO.

There are two self-extracting standalone VDA packages: one for installation on supported server OS machines, and another for supported workstation (desktop) OS machines.

The supported operating systems for VDAs, plus other requirements before installation, are listed in [System requirements](#). See [Prepare to install](#) for details about the information you provide and choices you make during VDA installation.

The VDA package automatically deploys prerequisites, if the machine does not already have them; this includes Visual C++ 2008, 2010 and 2013 Runtimes (32-bit and 64-bit) and .NET Framework 4.5.1.

When installing on a supported server OS machine, the Remote Desktop Services (RDS) role services are installed and enabled before installing the VDA. Alternatively, you can install the prerequisites yourself before installing the VDA.

Exception: Verify that Windows Server 2008 R2 and Windows 7 machines have at least .NET 3.5.1 installed before you start the VDA installation.

## About restarts

- A restart is required at the end of the VDA installation.
- To minimize the number of additional restarts needed during the installation sequence, ensure that .NET Framework 4.5.1 or 4.5.2 is installed before beginning the VDA installation. Also, for Windows Server OS machines, install and enable the RDS role services before installing the VDA. (Other prerequisites do not typically require machine restarts, so you can let the installer take care of those for you.)
- If you do not install prerequisites before beginning the VDA installation, and you specify the /noreboot option for a command line installation, you must manage the restarts. For example, when using automatic prerequisite deployment, the installer will suspend after installing RDS, waiting for a restart; be sure to run the command again after the restart, to continue with the VDA installation.

If you use the graphical interface or the command line interface option that runs the package, the files in the package are extracted to the Temp folder. More disk space is required on the machine when extracting to the Temp folder than when using the full-product ISO. Files extracted to the Temp folder are not automatically deleted, but you can manually delete them (from C:\Windows\Temp\Ctx-\*, where \* is a random Globally Unique Identifier) after the installation completes.

Alternatively, use a third party utility that can extract cabinet archives from EXE files (such as 7-Zip) to extract the files to a directory of your choice, and then run the XenDesktopVdaSetup.exe command. You can use the /extract command with an absolute path. For more information, see [How to use](#) in the section below.

If your deployment uses Microsoft System Center Configuration Manager, a VDA installation might appear to fail with exit

code 3, even though the VDA installed successfully. To avoid the misleading message, you can wrap your installation in a CMD script or change the success codes in your Configuration Manager package. For more information, see the forum discussion [here](#).

## Citrix Display Only Driver

The Citrix Display Only Driver (DOD) is the only installed and supported display driver on the XenDesktop Standard VDA on Windows 10.

The Citrix DOD has no GPU assist, even if a GPU or vGPU is present. All rendering is performed by the MS Basic Renderer in the software using the CPU. The Citrix DOD does not support Desktop Composition Redirection (DCR). The Citrix DOD is not installed or supported on XenApp.

**Important:** You must either have elevated administrative privileges before starting the installation, or use "Run as administrator."

1. Use the following table to determine which VDA installer package to use:

Where are you installing the VDA?	Install this package
On a supported server OS machine	VDASetup.exe
On a supported workstation (desktop) OS machine	VDAWorkstationSetup.exe

For single user, single server OS deployments (for example, delivering Windows Server 2012 to one user for web development), use the VDAWorkstationSetup.exe package. For more information, see [Server VDI](#).

2. Install the VDA using the graphical interface or the command line interface.

**Remember:** You must either have elevated administrative privileges before starting the installation, or use **Run as administrator**.

### Using the graphical interface:

1. Disable User Account Control (UAC), then right-click the downloaded package and choose **Run as administrator**. The installer launches and proceeds through the installation wizard. The restart at the end of the wizard is required before the VDA can be used in a site. (The wizard is the same as the one used in the full-product ISO to install a VDA; you will not encounter anything different.)

### Using the command line interface:

1. Extract the files from the package and then run XenDesktopVdaSetup.exe.

To extract the files before installing, use /extract with the absolute path, for example:

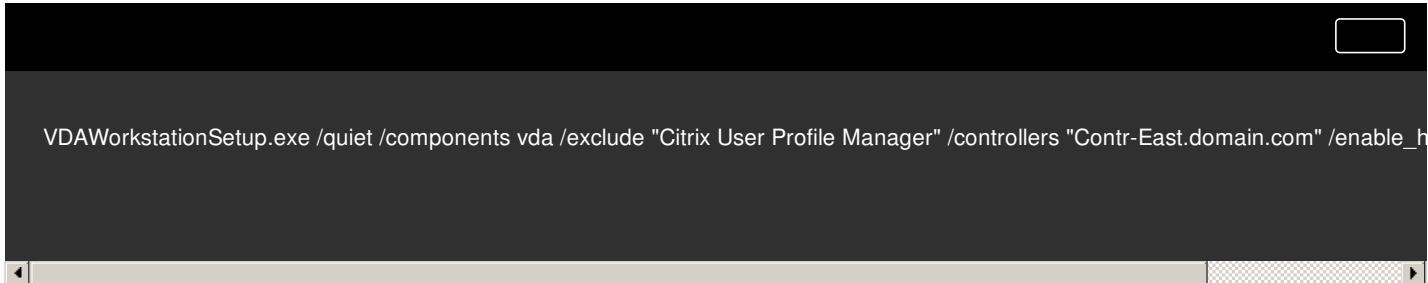
```
.\VDAWorkstationSetup.exe /extract %temp%\CitrixVDAInstallMedia
```

Then, in a separate command, run XenDesktopVdaSetup.exe from the directory containing the extracted content.

See [Install using the command line](#) and [CTX140972](#) for parameter information.

2. Run the appropriate VDA installer package as if it was the XenDesktopVdaSetup.exe command in everything except its name. See [Install using the command line](#) and [CTX140972](#) for parameter information.

For example, the most common installation command used for Remote PC Access installs a VDA on a physical office PC, without installing Citrix Receiver or Citrix Profile Manager. The machine will not automatically be restarted after the VDA is installed; however, a restart is required before the VDA can be used. The VDA will register initially with the Controller on the server named 'Contr-East'. Ports will be opened if the Windows Firewall Service is detected.



## 注意

Excluding Citrix Profile management from the installation (Using the /exclude "Citrix User Profile Manager" option) will affect monitoring and troubleshooting of VDAs with Citrix Director. On the User details and EndPoint pages, the Personalization panel and the Logon Duration panel will fail. On the Dashboard and Trends pages, the Average Logon Duration panel will display data only for machines that have Profile management installed.

Even if you are using a third party user profile management solution, it is recommended that you install and run the Citrix Profile management Service to avoid loss of monitoring and troubleshooting in Citrix Director (enabling the Citrix Profile management Service is not required).

# 计算机目录

May 28, 2016

Collections of physical or virtual machines are managed as a single entity called a session machine catalog. Many deployments create a master image or template on their host, and then use that in the machine catalog as a guide for Citrix tools (such as Machine Creation Services or Provisioning Services) to create VMs from the image/template. A catalog can also contain physical machines.

After you create a machine catalog, tests run automatically to ensure that it is configured correctly. When the tests complete, you can view a test report. You can also run the tests later on demand from Citrix Studio site-name in the Studio navigation pane.

After the tests complete, create a [Delivery group](#).

# 创建计算机目录

May 28, 2016

If you will use Citrix tools (Machine Creation Services or Provisioning Services) to create VMs for your deployment, prepare a master image or template on your host hypervisor. Then, create the machine catalog.

Make sure the host has sufficient processors, memory, and storage to accommodate the number of machines you will create.

The master image contains the operating system, non-virtualized applications, VDA, and other software. VMs are created in a machine catalog, based on a master image you created earlier and specify when you create the catalog.

Good to know:

- Master image is also known as clone image, golden image, or base image.
- Cloud deployments use templates rather than master images. See the template guidance
  - in Amazon Web Services, see [Deploy XenApp and XenDesktop 7.5 and 7.6 with Amazon VPC](#)
  - in Citrix CloudPlatform, see [XenApp and XenDesktop concepts and deployment on CloudPlatform](#).

When using Provisioning Services, you can use a master image or a physical computer as the master target device.

- Remote PC Access machine catalogs do not use master images.
- Microsoft KMS activation considerations when using Machine Creation Services:
  - If your deployment includes 7.x VDAs with a XenServer 6.1 or 6.2, vSphere, or Microsoft System Center Virtual Machine Manager host, you do not need to manually re-arm Microsoft Windows or Microsoft Office.
  - If your deployment includes a 5.x VDA with a XenServer 6.0.2 host, see [CTX128580](#).

Important: If you are using Provisioning Services or Machine Creation Services, do not run Sysprep on master images.

1. Using your hypervisor's management tool, create a new master image and then install the operating system, plus all service packs and updates.

The number of vCPUs and amount of memory are not critical at this point because you can change those values when you create the machine catalog. However, be sure to configure the amount of hard disk space required for desktops and applications, because that value cannot be changed later or in the catalog.

2. Make sure that the hard disk is attached at device location 0. Most standard master image templates configure this location by default, but some custom templates may not.
3. Install and configure the following software on the master image:
  - Integration tools for your hypervisor (such as XenServer Tools, Hyper-V Integration Services, or VMware tools). If you omit this step, your applications and desktops might not function correctly.
  - A VDA for Windows Server OS or VDA for Windows Desktop OS (Citrix recommends installing the latest version to allow access to the newest features. During installation, enable the optimization option, which improves performance by reconfiguring certain Windows features).
  - Third-party tools as needed, such as anti-virus software or electronic software distribution agents. Configure services such as Windows Update with settings that are appropriate for users and the machine type.
  - Third-party applications that you are not virtualizing. Citrix recommends virtualizing applications because it significantly reduces costs by eliminating the need to update the master image after adding or reconfiguring an application. In addition, fewer installed applications reduce the size of the master image hard disks, which saves storage costs.

- App-V clients with the recommended settings, if you plan to publish App-V applications.
  - When using Machine Creation Services, and you will localize Microsoft Windows, install the locales and language packs. During provisioning, when a snapshot is created, the provisioned VMs use the installed locales and language packs.
4. When using Provisioning Services, create a VHD file for the vDisk from your master target device before you join the master target device to a domain.
  5. Join the master image to the domain where desktops and applications will be members, and make sure that the master image is available on the host where the machines will be created.
  6. Citrix recommends that you create and name a snapshot of your master image so that it can be identified later. If you specify a master image rather than a snapshot when creating a machine catalog, Studio creates a snapshot, but you cannot name it.

**Prepare a master image for GPU-capable machines on XenServer** - When using XenServer for your hosting infrastructure, GPU-capable machines require a dedicated master image. Those VMs require video card drivers that support GPUs and must be configured to allow the VM to operate with software that uses the GPU for operations.

1. In XenCenter, create a VM with standard VGA, networks, and vCPU.
2. Update the VM configuration to enable GPU use (either Passthrough or vGPU).
3. Install a supported operating system and enable RDP.
4. Install XenServer Tools and NVIDIA drivers.
5. Turn off the Virtual Network Computing (VNC) Admin Console to optimize performance, and then restart the VM.
6. You are prompted to use RDP. Using RDP, install the VDA and then restart the VM.
7. Optionally, create a snapshot for the VM as a baseline template for other GPU master images.
8. Using RDP, install customer-specific applications that are configured in XenCenter and use GPU capabilities.

Before you start the machine catalog creation wizard, review the following procedure to learn about the choices you will make and information you will supply. When you start the wizard, some of the items may not appear or they may have different titles, based on your environment and the selections you make.

From Studio:

- If you have created a Site but haven't yet created a machine catalog, Studio will guide you to the correct starting place to create a machine catalog.
- If you have already created a machine catalog and want to create another, select Machine Catalogs in the Studio navigation pane, and then select Create Machine Catalog in the Actions pane.

The wizard walks you through the items described below.

- Operating system

Each catalog contains machines of only one type:

- Windows Server OS – A Windows Server OS catalog provides desktops and applications that can be shared by multiple users.
- Windows Desktop OS – A Windows Desktop OS catalog provides desktops and applications that are assigned to individual users.
- Remote PC Access – A Remote PC Access catalog provides users with remote access to their physical office desktop machines. Remote PC Access does not require a VPN to provide security.

Amazon Web Services (AWS) supports only Server OS machine catalogs (and Server VDI, see [Server VDI](#)), not Desktop OS or Remote PC Access catalogs.

- Machine management

Indicate whether machines in the catalog will be power managed through Studio:

- Machines are power managed through Studio or provisioned through a cloud environment (for example, VMs or blade PCs). This option is available only if you have a hypervisor or cloud environment connection already configured. You probably configured a connection when you created the Site. If not, you can create a new connection later and then edit the machine catalog.
- Machines are not power managed through Studio (for example, physical machines).

Indicate which tool you will use to deploy machines:

- Machine Creation Services (MCS) – Uses a master image or template to create and manage virtual machines.
  - MCS is not available for physical machines.
  - Machine catalogs in cloud environments use MCS.
- Provisioning Services – Manages target devices as a device collection. A Provisioning Services vDisk imaged from a master target device delivers desktops and applications.
- Other – A tool that manages machines already in the data center. Citrix recommends you use Microsoft System Center Configuration Manager or another third-party application to ensure that the machines in the catalog are consistent.
- Desktop experience

For machine catalogs containing Desktop OS machines that will be used to deliver desktops:

- Specify whether users will connect to a new (random) desktop each time they log on, or if they will connect to the same (static) desktop each time.
- If users connect to the same desktop, specify what will happen to any changes they make on the desktop. You can save changes to a separate Personal vDisk or the user's local VM disk, or you can discard changes. (If you choose to save changes to the separate Personal vDisk, you specify the drive letter and size later in the wizard.)

- Master image or machine template

Select the master image (non-cloud) or machine template (cloud) you created earlier. Remember: If you are using Provisioning Services or Machine Creation Services, do not run Sysprep on master images.

- Security

(Cloud environments) Select one or more security groups for the VMs; these are shown only if the availability zone supports security groups. Choose whether machines will use shared hardware or account-dedicated hardware.

- Virtual machines or Device collection or VMs and users

Specify how many virtual machines to create. You can choose how many virtual CPUs and the amount of memory (in MB) each machine will have. Each VM will have a 32 GB hard disk; this value is set in the master image, it cannot be changed in the catalog.

If you indicated previously that user changes to desktops should be saved on a separate Personal vDisk, specify its size in gigabytes and the drive letter.

If you plan to use multiple Network Interface Cards (NICs), associate a virtual network with each card. For example, you can assign one card to access a specific secure network, and another card to access a more commonly-used network. You can also add or remove NICs from this wizard.

- Machine accounts

(Remote PC Access catalogs) Specify the Active Directory machine accounts or Organizational Units (OUs) to add that correspond to users or user groups.

You can choose a previously-configured power management connection or elect not to use power management. If you want to use power management but a suitable connection hasn't been configured yet, you can create that connection

later and then edit the machine catalog to update the power management settings.

- Computer accounts

Each machine in the catalog must have a corresponding Active Directory computer account. Indicate whether to create new accounts or use existing accounts, and the location for those accounts.

If you use existing accounts, make sure you have enough unused computer accounts for the machines that will be created.

You can browse Active Directory to locate the existing accounts, or you can import a .csv file that lists the account names. The imported file content must use the format:

```
[ADComputerAccount]  
ADcomputeraccountname.domain  
...
```

For catalogs containing physical machines or existing machines, select or import existing accounts and assign each machine to both an Active Directory computer account and to a user account.

For machines created with Provisioning Services, computer accounts for target devices are managed differently; see the Provisioning Services documentation.

Also specify the account naming scheme for the machines that are created – hash marks (#) in the scheme represent sequential numbers or letters that will be included with additional name text you provide.

- Name and description

On the final page of the creation wizard, you specify the name and description of the machine catalog. This information appears in Studio.

# 管理计算机目录

May 28, 2016

For random machine catalogs, you can maintain users' desktops by applying global changes (such as Windows updates, anti-virus software updates, operating system upgrades, or configuration changes) to the master image. Then modify the machine catalog to use the updated master image so users receive the updated desktop the next time they log on. You can make significant changes for large numbers of users in one operation.

For static and Remote PC Access machine catalogs, you must manage updates to users' desktops outside of Studio, either on an individual basis or collectively using third-party software distribution tools. For machines created through Provisioning Services, updates to users' desktops are propagated through the vDisk.

Citrix recommends that you save copies or snapshots of master images before you make updates. The database keeps a historical record of the master images used with each machine catalog. Do not delete, move, or rename master images. You can revert a machine catalog to use the previous version of the master image if users encounter problems with updates you deployed to their desktops, thereby minimizing user downtime.

Before you start:

- Make sure the virtualization host has sufficient processors, memory, and storage to accommodate the additional machines.
- Make sure that you have enough unused Active Directory computer accounts. If using existing accounts, keep in mind that the number of machines you can add is limited by the number of accounts available.
- If you will use Studio to create Active Directory computer accounts for the additional machines, you must also have appropriate domain administrator permission.

1. Select Machine Catalogs in the Studio navigation pane.

2. Select a machine catalog and then select Add machines in the Actions pane.

3. Select the number of virtual machines to add.

4. If you indicate that new Active Directory accounts should be created (this step is required if there are insufficient existing accounts for the number of VMs you are adding):

- Select the domain and location where the accounts will be created.
- Specify an account naming scheme, using hash marks to indicate where sequential numbers or letters will appear (a name cannot begin with a number). For example, a naming scheme of PC-Sales-## (with 0-9 selected) results in computer accounts named PC-Sales-01, PC-Sales-02, PC-Sales-03, etc.

If you indicate that existing Active Directory accounts should be used:

- Either browse to the accounts or click Import and specify a .csv file containing account names. Make sure that there are enough accounts for all the machines you're adding.
- Studio manages these accounts, so either allow Studio to reset the passwords for all the accounts or specify the account password (which must be the same for all accounts).

The machines are created as a background process, and can be lengthy when creating a large number of machines. Machine creation continues even if you close Studio.

1. Select Machine Catalogs in the Studio navigation pane.

2. Select a catalog and then select Edit Machine Catalog in the Actions pane.
  3. (Remote PC Access catalogs only) On the Power Management page, you can change a Remote PC Access catalog's power management settings and select a power management connection. On the Organizational Units page, add or remove OUs.
- On the Description page, change the machine catalog description.

1. Select Machine Catalogs in the Studio navigation pane.
2. Select a catalog and then select Rename Machine Catalog in the Actions pane.
3. Enter the new name.

Before deleting a machine catalog, ensure that:

- All users are logged off and that no disconnected sessions are running.
- Maintenance mode is turned on for all machines in the catalog, and then all machines are shut down.
- The catalog is not associated with a Delivery Group.

1. Select Machine Catalogs in the Studio navigation pane.
2. Select a catalog and then select Delete Machine Catalog in the Actions pane.
3. Indicate whether the machines in the catalog should be deleted. If you choose to delete the machines, indicate whether the associated computer accounts should be left as-is, disabled, or deleted in Active Directory.

After you delete a machine from a catalog, users no longer can access it. Before deleting a machine, ensure that:

- User data is backed up or no longer required.
- All users are logged off. Turning on maintenance mode will stop users from connecting to a machine.
- Desktops are not powered on or suspended.

1. Select Machine Catalogs in the Studio navigation pane.
2. Select a catalog and then select View Machines in the Actions pane.
3. Select one or more machines and then click Turn On Maintenance Mode in the Actions pane.
4. Select Delete in the Actions pane.
5. Choose whether to delete the machines being removed. If you choose to delete the machines, select what to do with the associated Active Directory computer accounts:

In machine catalog	In Active Directory
Leave	Do not change
Remove	Do not remove
Remove	Disable
Remove	Delete

To manage Active Directory accounts in a machine catalog, you can:

- Free unused machine accounts by removing Active Directory computer accounts from Desktop OS and Server OS machine catalogs. Those accounts can then be used for other machines.
- Add accounts so that when more machines are added to the catalog, the computer accounts are already in place
  1. Select Machine Catalogs in the Studio navigation pane.
  2. Select a machine catalog and then select Manage AD accounts in the Actions pane.
  3. Choose whether to add or delete computer accounts.
    - If you add accounts, you are prompted to specify what to do with the account passwords: either reset them all or enter a password that applies to all accounts. You might reset passwords if you do not know the current account passwords; you must have permission to perform a password reset. If you enter a password, the password will be changed on the accounts as they are imported.
    - If you delete an account, you are prompted to choose whether the account in Active Directory should be kept, disabled, or deleted.

Update a master image to apply changes to all the desktops and applications in a machine catalog that were created with that master image. Managing common aspects through a single master image lets you deploy system-wide changes such as Windows updates or configuration changes to a large number of machines quickly.

After preparing and testing a new/updated master image on the host (see [Prepare a master image](#)), modify the machine catalog to use it.

Note the following:

- Citrix recommends that you save copies or snapshots of master images before you make updates. The database keeps a historical record of the master images used with each machine catalog. You can revert a machine catalog to use the previous version of the master image if users encounter problems with updates you deployed to their desktops, thereby minimizing user downtime. Do not delete, move, or rename master images; otherwise, you will not be able to revert a machine catalog to use them.

Although Studio can create a snapshot, Citrix recommends that you create a snapshot using the hypervisor management console, and then select that snapshot in Studio. This enables you to provide a meaningful name and description rather than an automatically generated name.

- For GPU master images, you can change the master image only through the XenServer XenCenter console.
- For machine catalogs that use Provisioning Services, you must publish a new vDisk to apply changes to the catalog. For details, see the Provisioning Services documentation.
- After updating the master image, you must restart the machines through Studio for the changes to take effect and be available to your users. This may occur automatically; for example, when a user logs off a desktop, or it may occur as part of a configured restart schedule. Alternatively, you can restart a machine from Studio.

1. Select Machine Catalogs in the Studio navigation pane.
2. Select a machine catalog and then select Update Machines in the Actions pane.
3. On the Master Image page, select the host and the new/updated master image.
4. On the Rollout Strategy page, specify when the new or updated master image is applied to users' machines: on the next shutdown or immediately.
  - If you choose to update the image on the next shutdown, you can notify users of the update.
  - If you choose to update the image immediately, you can specify whether to restart all machines at the same time or at specified intervals. You can send a notification message to users 1, 5, or 15 minutes before they are logged off and the machine restarted.

1. Select Machine Catalogs in the Studio navigation pane.
2. Select the machine catalog and then select Rollback machine update in the Actions pane.
3. Specify how to apply the reverted master image to user desktops, as described above.

The rollback strategy is applied only to desktops that need to be reverted. For desktops that have not been updated with the new/updated master image that prompted the rollback (for example, desktops with users who have not logged off), users do not receive messages and are not forced to log off.

Upgrade the machine catalog after you upgrade the VDAs on the machines to a newer version. Citrix recommends upgrading all VDAs to the latest version so they can all access the newest features.

Note: If you have Windows XP or Windows Vista machines, they must use an earlier VDA version, and will not be able to use the latest product features. If you cannot upgrade those machines to a currently supported Windows operating system, Citrix recommends you keep them in a separate machine catalog. For more information, see [VDAs on machines running Windows XP or Windows Vista](#) and [Mixed VDA support](#).

Before you upgrade a machine catalog:

- If you're using Provisioning Services, upgrade the VDA version in the Provisioning Services console.
- Start the upgraded machines so that they register with the Controller. This lets Studio determine that the machines in the machine catalog need upgrading.

1. Select Machine Catalogs in the Studio navigation pane.
2. Select the machine catalog. The Details tab in the lower pane displays version information.
3. Select Upgrade Catalog.
  - If Studio detects that the catalog needs upgrading, it displays a message. Follow the prompts.
  - If one or more machines cannot be upgraded, a message explains why. Citrix recommends you resolve machine issues before upgrading the machine catalog to ensure that all machines function properly.

Before you revert a machine catalog upgrade, if you used Provisioning Services to create the machine catalog, change the VDA version in the Provisioning Services console.

1. Select Machine Catalogs in the Studio navigation pane.
2. Select the machine catalog. The Details tab in the lower pane displays version information.
3. Select Undo and then follow the prompts.

# 交付组

May 28, 2016

A Delivery group is a collection of machines selected from one or more machine catalogs. The Delivery group specifies which users can use those machines, and the applications available to those users.

Begin by creating the Delivery group. Later, you can change the initial settings and configure additional ones.

To create a Delivery Group:

1. Select Delivery Groups in the Studio navigation pane.
2. Select Create Delivery Group in the Actions pane. The wizard walks you through the items described below.

Select a machine catalog and specify the number of machines you want to use from the catalog.

- At least one machine must remain unused in the selected machine catalog.
- A machine catalog can be specified in more than one Delivery group; however, a machine can be used in only one Delivery group.
- A Delivery group can use more than one machine catalog; however, those catalogs must contain the same machine types (Server OS, Desktop OS, or Remote PC Access). In other words, you cannot mix machine types in a Delivery group or in a machine catalog.
- Similarly, you cannot create a Delivery group containing Desktop OS machines from a machine catalog configured for static desktops and machines from a machine catalog configured for random desktops.
- Each machine in a Remote PC Access machine catalog is automatically associated with a Delivery group.

The type indicates what the Delivery group offers: only desktops, only applications, or both desktops and applications. Delivery groups with static Desktop OS machines cannot offer both desktops and applications.

Specify the users and user groups who can use the applications and/or desktops in the Delivery group.

There are two types of users: authenticated and unauthenticated (unauthenticated is also called anonymous). You can configure one or both types.

- **Authenticated** - The users and group members you specify by name must present credentials (such as smart card or user name and password) to StoreFront or Citrix Receiver to access applications and desktops.
- **Unauthenticated (anonymous)** - For Delivery Groups containing Server OS machines, you can select a check box that will allow users to access applications and desktops without presenting credentials to StoreFront or Citrix Receiver. For example, when users access applications through kiosks, the application might require credentials, but the Citrix access portal and tools do not. An Anonymous Users Group is created when you install the VDA.
  - To grant access to unauthenticated users, each machine in the Delivery Group must have a VDA for Windows Server OS (minimum version 7.6) installed. When unauthenticated users are enabled, you must have an unauthenticated StoreFront store.
  - Unauthenticated user accounts are created on demand when a session is launched, and named AnonXYZ, in which XYZ is a unique three-digit value.

- Unauthenticated user sessions have a default idle timeout of 10 minutes, and are logged off automatically when the client disconnects. Reconnection, roaming between clients, and Workspace Control are not supported.

The following table describes your choices.

Enable access for	Add/assign users and user groups?	Enable the "Give access to unauthenticated users" check box?
Only authenticated users	Yes	No
Only unauthenticated users	No	Yes
Both authenticated and unauthenticated users	Yes	Yes

For Desktop groups containing Desktop OS machines, you can import user data (a list of users) after you create the Delivery group. See [Import or export user lists](#).

A list displays the applications that were discovered on a machine created from the master image, a template in the machine catalog, or on the App-V management server. Choose one or more applications to add to the Delivery group.

You can also add (create) applications manually. You'll need to provide the path to the executable, working directory, optional command line arguments, and display names for administrators and users.

You can change an application's properties; see [Change application properties](#) for details.

You cannot create applications for Remote PC Access Delivery groups.

By default, applications you add are placed in a folder named Applications. Folders can make it easier to manage large numbers of applications. You can specify a different folder when you add the application; however, it's easier to manage folders later. See [Manage application folders](#) for details.

If you publish two applications with the same name to the same users, change the Application name (for user) property in Studio; otherwise, users will see duplicate names in Receiver.

Select or add StoreFront URLs that will be used by the Citrix Receiver that is installed on each machine in the Delivery group. You can also specify the StoreFront server address later by selecting Configuration > StoreFront in the navigation pane. When adding the StoreFront Server add '/Discovery' to the end of the URL.

# 设置

May 28, 2016

The following documents describe how to configure and manage most of the settings you can specify and update for Delivery Groups:

- [Applications](#)
- [Machines](#)
- [Remote PC Access](#)
- [Session](#)
- [Users](#)

The information below describes settings that are not covered in those documents.

Before changing an application only or desktop and applications Delivery group to a desktop only Delivery group, delete all applications from the Delivery group.

1. Select Delivery Groups in the Studio navigation pane.
  2. Select a Delivery group, and then select Edit Delivery Group in the Actions pane.
  3. On the Delivery Type page, select the delivery type you want to change the Delivery group to.
- 
1. Select Delivery Groups in the Studio navigation pane.
  2. Select a Delivery group, and then select Edit Delivery Group in the Actions pane.
  3. On the Basic Settings page, you can change the following:

Setting	Description
Description	The text that StoreFront uses and that users see.
Enabled check box	Whether or not the Delivery Group is enabled.
Desktops per user	(Desktop OS machines only) The maximum number of shared desktops that a user can have active at the same time. In assign-on-first-use deployments, this value specifies how many desktops users can assign to themselves.
Time zone	
Enable Secure ICA	Secures communications to and from machines in the Delivery Group using SecureICA, which encrypts the ICA protocol (default level is 128-bit; the level can be changed using the SDK). Citrix recommends using additional encryption methods such as SSL/TLS encryption when traversing public networks. Also, SecureICA does not check data integrity.

Upgrade a Delivery Group after you upgrade the VDAs on its machines.

Note: If you must continue using earlier VDA versions, newer product features may not be available. For more information, see [Upgrade a deployment](#).

Before you start the Delivery Group upgrade:

- If you use Provisioning Services, upgrade the VDA version in the Provisioning Services console.
- Start the machines containing the new VDA so that they can register with the Controller. This process tells Studio what needs upgrading in the Delivery Group.

1. Select Delivery Groups in the Studio navigation pane.

2. Select the Delivery group and then select Upgrade Delivery Group in the Actions pane.

Before starting the upgrade process, Studio tells you which, if any, machines cannot be upgraded and why. You can then cancel the upgrade, resolve the machine issues, and then start the Delivery Group upgrade again.

After the Delivery Group upgrade completes, you can revert the machines to their previous states by selecting the Delivery Group and then selecting Undo in the Actions pane.

# 计算机

May 23, 2017

Unless otherwise noted, the following procedures are supported for all Delivery Group types: Server OS, Desktop OS, and Remote PC Access.

## Shut down and restart machines

Note: This procedure is not supported for Remote PC Access machines.

1. Select Delivery Groups in the Studio navigation pane.
2. Select the Delivery Group and then select View Machines in the Actions pane.
3. Select the machine and select one of the following in the Actions pane (some options may not be available, depending on the machine state):
  - Force shut down — Forcibly powers off the machine and refreshes the list of machines.
  - Restart — Requests the operating system to shut down and then start the machine again. If the operating system cannot comply, the machine remains in its current state.
  - Suspend — Pauses the machine without shutting it down, and refreshes the list of machines.
  - Shut down — Requests the operating system to shut down.

If the machine does not shut down within 10 minutes, it is powered off. If Windows attempts to install updates during the shutdown, there is a risk that the machine will be powered off before the updates finish.

Note: Citrix recommends that you prevent Desktop OS machine users from selecting Shut Down within a session. See the Microsoft policy documentation for details.

## Power manage machines

Note: You can power manage only virtual Desktop OS machines, not physical ones (including Remote PC Access machines). Desktop OS machines with GPU capabilities cannot be suspended, so power off operations fail. For Server OS machines, see [Create a restart schedule](#)

Machines can be in one of the following states:

Delivery Group	State
Random	Randomly allocated and in use
	Unallocated and unconnected
Static (assigned)	Permanently allocated and in use
	Permanently allocated and unconnected (but ready)
	Unallocated and unconnected

During normal use, static Delivery Groups typically contain both permanently allocated and unallocated machines. Initially, all machines are unallocated (except for those manually allocated when the Delivery Group was created). As users connect, machines become permanently allocated. You can fully power manage the unallocated machines in those Delivery Groups, but only partially manage the permanently allocated machines.

- **Pools and buffers** - For random Delivery Groups and unallocated machines in static Delivery Groups, a pool is a set of unallocated (or temporarily allocated) machines that are kept in a powered-on state, ready for users to connect; a user

gets a machine immediately after log on. The pool size (the number of machines kept powered-on) is configurable by time of day. (For static Delivery Groups, use the SDK to configure the pool.)

A buffer is an additional standby set of unallocated machines that are turned on when the number of machines in the pool falls below a threshold that is a percentage of the Delivery Group size. For large Delivery Groups, a significant number of machines might be turned on when the threshold is exceeded, so plan Delivery Group sizes carefully or use the SDK to adjust the default buffer size.

- **Power state timers** - You can use power state timers to suspend machines after users have disconnected for a specified amount of time. For example, machines will suspend automatically outside of office hours if users have been disconnected for at least ten minutes. Random machines or machines with Personal vDisks automatically shut down when users log off, unless you configure the ShutdownDesktopsAfterUse Delivery Group property in the SDK. You can configure timers for weekdays and weekends, and for peak and nonpeak intervals.
- **Partial power management of permanently allocated machines** - For permanently allocated machines, you can set power state timers, but not pools or buffers. The machines are turned on at the start of each peak period, and turned off at the start of each off-peak period; you do not have the fine control that you have with unallocated machines over the number of machines that become available to compensate for machines that are consumed.

To power manage virtual Desktop OS machines:

1. Select Delivery Groups in the Studio navigation pane.
2. Select a Delivery Group, and then select Edit Delivery Group in the Actions pane.
3. On the Power Management page, select Weekdays in the Power manage machines dropdown. (By default, weekdays are Monday to Friday.)
4. For random Delivery Groups, in Machines to be powered on, select Edit and then specify the pool size during weekdays. Then, select the number of machines to power on.
5. In Peak hours, set the peak and off-peak hours for each day.
6. Set the power state timers for peak and non-peak hours during weekdays:
  - In During peak hours > When disconnected, specify the delay (in minutes) before suspending any disconnected machine in the Delivery Group, and select Suspend.
  - In During off-peak hours > When disconnected, specify the delay before turning off any logged-off machine in the Delivery Group, and select Shutdown. This timer is not available for Delivery Groups with random machines.
7. Select Weekend in the Power manage machines dropdown, and then configure the peak hours and power state timers for weekends.

Use the [SDK](#) to:

- Shut down, rather than suspend, machines in response to power state timers, or if you want the timers to be based on logoffs, rather than disconnections.
- Change the default weekday and weekend definitions.

Create a restart schedule

Note: You can use a restart schedule for Server OS machines only. For Desktop OS machines, see [Power manage machines](#).

To configure a restart schedule:

1. Select Delivery Groups in the Studio navigation pane.
2. Select a Delivery Group, and then select Edit Delivery Group in the Actions pane,
3. On the Restart Schedule page:
  - In the Restart machines drop-down, choose how often to restart the machines.
  - In the Restart first group at fields, specify the hour and minute (in 24-hour format) when the first server will begin the restart process.

- In the Restart additional groups every drop-down, Indicate whether all servers should be restarted at once, or how much time should be allowed to restart every server in the Delivery Group.  
For example, assume a Delivery Group has five servers, a Restart first group at time of 13:00 (1:00 pm), and a Restart additional groups every selection of 1 hour. That duration (60 minutes) is divided by the number of machines (five), which yields a restart interval of 12 minutes. So, the restart times are 1:00 pm, 1:12 pm, 1:24 pm, 1:36 pm, and 1:48 pm. This gives all five machines the chance to complete their restart at the end of the specified interval (1 hour).
- Indicate whether you want to send a message to users at a specified interval before they are logged off. The notification will be sent relative to each server's calculated restart time, as described in the example.

You cannot perform an automated power-on or shutdown in Studio.

#### Prevent users from connecting to a machine (maintenance mode)

When you need to temporarily stop new connections to machines, you can turn on maintenance mode for one or all the machines in a Delivery Group. You might do this before applying patches or using management tools.

- When a Server OS machine is in maintenance mode, users can connect to existing sessions, but cannot start new sessions.
- When a Desktop OS machine (or a PC using Remote PC Access) is in maintenance mode, users cannot connect or reconnect. Current connections remain connected until they disconnect or log off.

1. Select Delivery Groups in the Studio navigation pane.
2. Select a Delivery Group.
3. To turn on maintenance mode for all machines in the Delivery Group, select Turn On Maintenance Mode in the Actions pane.  
To turn on maintenance mode for one machine:
  1. Select View Machines in the Actions pane.
  2. Select a machine, and then select Turn On Maintenance Mode in the Actions pane.
4. To turn maintenance mode off for one or all machines in a Delivery Group, follow the previous instructions, but select Turn Off Maintenance Mode in the Actions pane.

Windows Remote Desktop Connection (RDC) settings also affect whether a Server OS machine is in maintenance mode. Maintenance mode is on when any of the following occur:

- Server maintenance mode is set to on, as described above.
- RDC is set to Don't allow connections to this computer.
- RDC is not set to Don't allow connections to this computer, and the Remote Host Configuration User Logon Mode setting is one of the following:
  - Allow reconnections, but prevent new logons
  - Allow reconnections, but prevent new logons until the server is restarted.

#### Reallocate machines (change users)

Note: You can reallocate only Desktop OS machines, not Server OS machines or machines created through Provisioning Services.

1. Select Delivery Groups in the Studio navigation pane.
2. Select a Delivery Group.
3. To reallocate more than one machine:
  1. Select Edit Delivery Group in the Actions pane.
  2. On the Machine Allocation (User Assignment) page, select machines and specify the new users.
4. To reallocate one machine:

1. Select View Machines in the Actions pane.
2. Select a machine, and then select Change User in the Actions pane.
3. Add or remove the user.

## Change the maximum number of machines per user

1. Select Delivery Groups in the Studio navigation pane.
2. Select a Delivery Group, and then select Edit Delivery Group in the Actions pane.
3. On the User Settings page, set the desktops per user value.

## Identify machines using tags

You can use tags to refine a machine search or to limit machine access. You can add any number of tags of any length.

1. Select Delivery Groups in the Studio navigation pane.
2. Select a Delivery Group, and then select View Machines in the Actions pane.
3. Select a machine.
4. To add tags, select Add Tag in the Actions menu and then enter one or more tags, separated by semicolons (;).  
To change or remove tags, select Edit Tags in the Actions menu and then make the necessary changes.

## Load manage

Note: You can load manage Server OS machines only.

Load Management measures the server load and determines which server to select under the current environment conditions. This selection is based on:

- **Server maintenance mode status** – a Server OS machine is considered for load balancing only when maintenance mode is off. (See [Prevent users from connecting to a machine \(maintenance mode\)](#) for details.)
- **Server load index** – determines how likely a server delivering Server OS machines is to receive connections. The index is a combination of load evaluators: the number of sessions and the settings for performance metrics such as CPU, disk, and memory use. You specify the load evaluators in load management policy settings.
  - You can monitor the load index in Director, Studio search, and the SDK.
  - In Studio, the Server Load Index column is hidden by default. To display it, select a machine, right-select a column heading and then choose Select Column. In the Machine category, select Load Index.
  - In the SDK, use the Get-BrokerMachine cmdlet.
- A server load index of 10000 indicates that the server is fully loaded. If no other servers are available, users might receive a message that the desktop or application is currently unavailable when they launch a session.
- **Concurrent logon tolerance policy setting** - the maximum number of concurrent requests to log on to the server. (This setting is equivalent to load throttling in XenApp versions earlier than 7.5.)

If all servers are at or higher than the concurrent logon tolerance setting, the next logon request is assigned to the server with the lowest pending logons. If more than one server meets this criteria, the server with the lowest load index is selected.

For more information, see the

— [Policy settings reference](#)

## Remove a machine

Removing a machine deletes it from a Delivery Group but does not delete it from the machine catalog that the Delivery Group uses. Therefore, the machines are available for assignment to other Delivery Groups.

Machines must be shut down before they can be removed. To temporarily stop users from connecting to a machine while you are removing it, put the machine into maintenance mode before shutting it down.

Keep in mind that machines may contain personal data, so use caution before allocating the machine to another user. You may want to reimagine the machine.

1. Select Delivery Groups in the Studio navigation pane.
2. Select a Delivery Group and then select View Machines in the Actions pane.
3. Make sure that the machine is shut down.
4. Select Remove from Delivery Group in the Actions pane.

## Restrict access to machines

Any changes you make to restrict access to machines in a Delivery Group supersede previous settings, regardless of the method you use. You can:

- Restrict access for administrators using Delegated Administration scopes. You can create and assign a scope that permits administrators to access all applications, and another scope that provides access to only certain applications. See the Delegated Administration documentation for details.
- Restrict access for users through SmartAccess policy expressions that filter user connections made through NetScaler Gateway.
  1. Select Delivery Groups in the Studio navigation pane.
  2. Select the Delivery Group and then select Edit Delivery Group in the Actions pane.
  3. On the Access policy page, select Connections through NetScaler Gateway.
  4. To choose a subset of those connections, select Connections meeting any of the following filters. Then define the NetScaler Gateway site, and add, edit, or remove the SmartAccess policy expressions for the allowed user access scenarios. For details, see the NetScaler Gateway documentation.
- Restrict access for users through exclusion filters on access policies that you set in the SDK. Access policies are applied to Delivery Groups to refine connections. For example, you can restrict machine access to a subset of users, and you can specify allowed user devices. Exclusion filters further refine access policies. For example, for security you can deny access to a subset of users or devices.

By default, exclusion filters are disabled.

For example, for a teaching lab on a subnet in the corporate network, to prevent access from that lab to a particular Delivery Group, regardless of who is using the machines in the lab, use the following command: Set-BrokerAccessPolicy -Name VPDesktops\_Direct -ExcludedClientIPFilterEnabled \$True -

You can use the asterisk (\*) wildcard to match all tags that start with the same policy expression. For example, if you add the tag VPDesktops\_Direct to one machine and VPDesktops\_Test to another, setting the tag in the Set-BrokerAccessPolicy script to VPDesktops\_\* applies the filter to both machines.

## Update a machine

1. Select Delivery Groups in the Studio navigation pane.
2. Select the Delivery Group, select View Machines in the Action pane.
3. Select a machine and then select Update machines in the Actions pane.
  - To choose a different master image, select Master image. Then select a snapshot. Expanding a selected snapshot displays associated master images.
  - To apply changes and notify machine users, select Rollout notification to end-users. Then specify:
    - When to update the master image: now or on the next restart.
    - The restart distribution time: all machines at the same time or at time variations.

- If and when users will be notified of the restart, plus the message they will receive.

# 应用程序

May 28, 2016

## Add applications

To add an application to a Delivery Group:

1. Select Delivery Groups in the Studio navigation pane.
2. Select the Delivery Group.
3. Select Add Applications in the Actions pane.

A list displays the applications that were discovered on a machine created from the master image, a template in the machine catalog, or on the App-V management server. Choose one or more applications to add to the Delivery Group.

You can also add (create) applications manually. You'll need to provide the path to the executable, working directory, optional command line arguments, and display names for administrators and users.

You can change an application's properties; see below.

By default, applications you add are placed in a folder named Applications. For more information about application folders, see below.

## Duplicate, disable, rename, edit tags, or delete an application

To duplicate, disable, rename, edit tags, or delete an application:

1. Select Delivery Groups in the Studio navigation pane.
2. Select the Applications tab in the middle pane and then select the application.
3. Select the appropriate task in the Actions pane.

Good to know:

- When you duplicate an application, it is automatically renamed and placed adjacent to the original.
- Deleting an application removes it from the Delivery Group but not from the master image.
- To move an application to a different application folder, see below.

## Change application properties

To change the properties of an application:

1. Select Delivery Groups in the Studio navigation pane.
2. Select the Applications tab in the middle pane and then select the application.
3. Select Properties in the Actions pane.

You can view and change the following:

Property to view or change	Select this page
Application name	Identification
Category in Receiver	Delivery
Command line arguments	Location
Description	Identification

Property to view or change	Select this page
File type association	File Type Association
Icon	Delivery
Keywords for StoreFront	Identification
Path to executable	Location
Shortcut on user's desktop	Delivery
Visibility	Limit Visibility
Working directory	Location

Application changes might not take effect for current application users until they log off their sessions.

### Manage application folders

By default, applications you add are placed in a folder named

— *Applications*

. You can:



- Create additional folders and then move applications into those new folders.
  - Folders can be nested up to five levels.
  - Folders do not have to contain applications; empty folders are allowed.
  - Folders are listed alphabetically unless you move them or specify a different location when you create them.
  - You can have more than one folder with the same name, as long as each has a different parent folder. Similarly, you can have more than one application with the same name, as long as each is in a different folder.

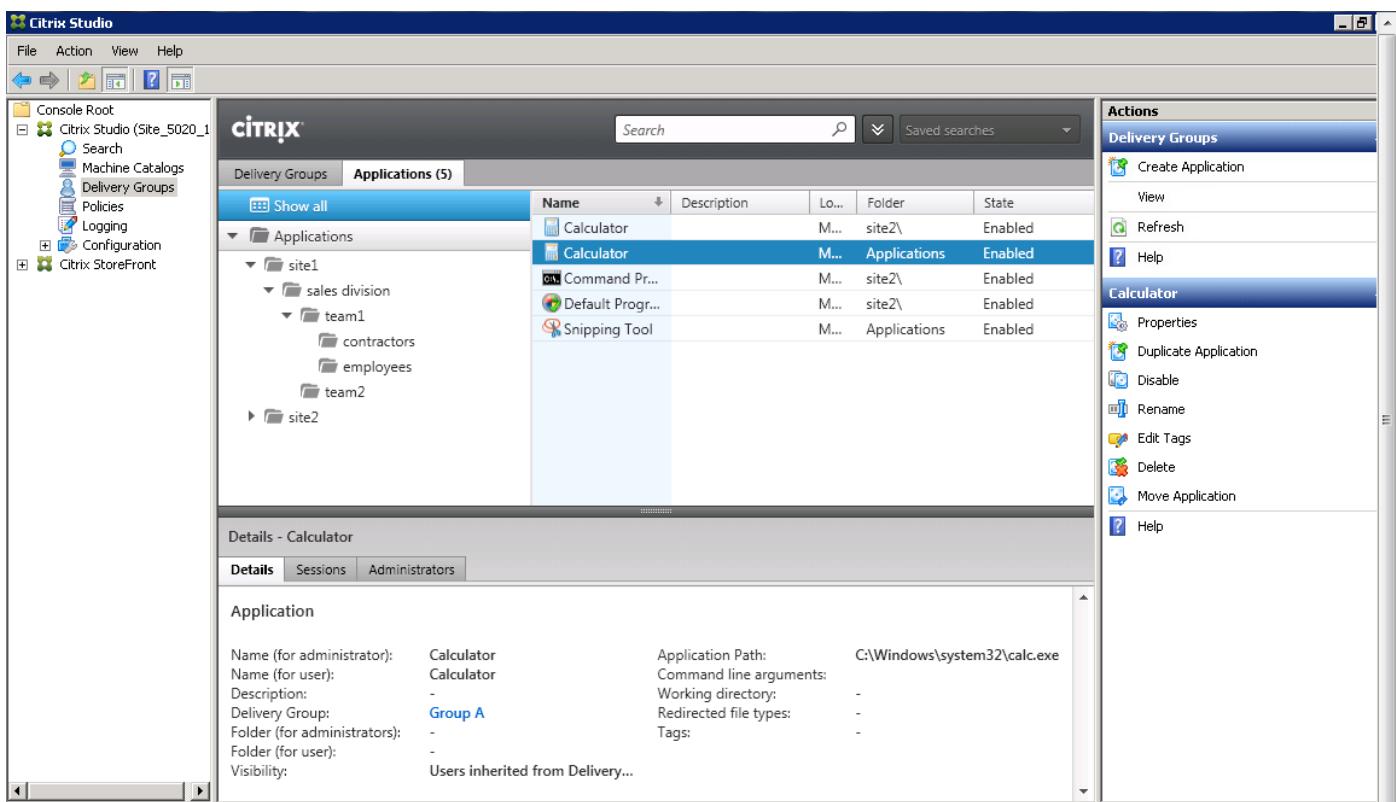
- Move a folder to the same or a different level. Moving is easiest using drag-and-drop.
- Rename or delete a folder you created. You cannot rename or delete the Applications folder, but you can move all the applications it contains to other folders you create.

You can also create folders for applications when you create a Delivery Group.

You must have View Applications permission to see the applications in folders, and you must have Edit Application Properties permission for all applications in the folder to remove, rename, or delete a folder that contains applications. For details, see [Delegated Administration](#).

**Tip:** The following instructions use the Actions pane in Studio. Alternatively, you can use right-click menus or drag and drop. If you create or move a folder in a location you did not intend, you can drag and drop it to the correct location. Select Delivery Groups in the Studio navigation pane, and then select the Applications tab in the middle pane.

- To view all folders (excluding nested folders), click Show all.



- To create a folder:
  1. To place the new folder at the highest level (not nested under another folder), select the top Applications folder. To place the new folder under an existing folder other than Applications, select that folder.
  2. Select Create Folder in the Actions pane. Enter a 1-64 character name for the folder. Spaces are permitted.
- To move a folder:
  1. Select the folder and then select Move Folder in the Actions pane. (You can move only one folder at a time unless the folder contains nested folders.)
  2. To move the folder to the highest level (not nested under another folder), select the top Applications folder. To move a new folder under an existing folder other than Applications, select that folder.
- To rename a folder, select the folder, and then select Rename Folder in the Actions pane. Enter a 1-64 character new name.
- To delete a folder, select the folder, and then select Delete Folder in the Actions pane. When you delete a folder that contains applications and other folders, those objects are also deleted. Deleting an application removes the application assignment from the Delivery Group; it does not remove it from the machine.
- To move applications into a folder, select one or more applications, and then select Move Application in the Actions pane. Select the folder.

To add or move applications to folders from within the Create Delivery Group wizard, select one or more applications on the Applications page, and then select Change.

- To move the application to an existing folder, select that folder.
- To move the application to a new folder:
  - To create a folder at the highest level (not nested under another folder), select the top Applications folder and then select New folder. Specify a 1-64 character folder name. Spaces are allowed.
  - To create a new nested folder under an existing folder (other than Applications), select an existing folder and then select New folder. Specify a 1-64 character folder name. Spaces are allowed.

# 用户

May 28, 2016

## Add users, remove users, and enable/disable access to unauthenticated (anonymous) users

There are two types of users: authenticated and unauthenticated (unauthenticated is also called anonymous). You can configure one or both types.

- **Authenticated** - The users and group members you specify by name must present credentials (such as smart card or user name and password) to StoreFront or Citrix Receiver to access applications and desktops.
- **Unauthenticated (anonymous)** - For Delivery Groups containing Server OS machines, you can select a check box that will allow users to access applications and desktops without presenting credentials to StoreFront or Citrix Receiver. For example, when users access applications through kiosks, the application might require credentials, but the Citrix access portal and tools do not. An Anonymous Users Group is created when you install the VDA.
  - To grant access to unauthenticated users, each machine in the Delivery Group must have a VDA for Windows Server OS (minimum version 7.6) installed. When unauthenticated users are enabled, you must have an unauthenticated StoreFront store.
  - Unauthenticated user accounts are created on demand when a session is launched, and named AnonXYZ, in which XYZ is a unique three-digit value.
  - Unauthenticated user sessions have a default idle timeout of 10 minutes, and are logged off automatically when the client disconnects. Reconnection, roaming between clients, and Workspace Control are not supported.

1. Select Delivery Groups in the Studio navigation pane.
2. Select a Delivery Group, and then select Edit Delivery Group in the Actions pane.
3. The following table describes your choices.

Enable access for	Add/assign users and user groups?	Enable the "Give access to unauthenticated users" check box?
Only authenticated users	Yes	No
Only unauthenticated users	No	Yes
Both authenticated and unauthenticated users	Yes	Yes

For Desktop Groups containing Desktop OS machines, you can import user data (a list of users) after you create the Delivery Group. See [Import or export user lists](#) below.

### Import or export user lists

For Delivery Groups containing physical Desktop OS machines, you can import user information from a .csv file after you create the Delivery Group. You can also export user information to a .csv file. The .csv file can contain data from a previous product version.

The first line in the .csv file must contain comma-separated column headings (in any order), which can include: ADComputerAccount, AssignedUser, VirtualMachine, and HostId. Subsequent lines in the file contain comma-separated data. The ADComputerAccount entries can be common names, IP addresses, distinguished names, or domain and computer name pairs.

To import or export user information:

1. Select Delivery Groups in the Studio navigation pane.
2. Select a Delivery Group, and then select Edit Delivery Group in the Actions pane.
3. On the Machine Allocation page, select the Import list or Export list button, and then browse to the file location.

# 会话

May 28, 2016

## Log off or disconnect a session, or send a message to users

1. Select Delivery Groups in the Studio navigation pane.
2. Select a Delivery Group and then select View Machines in the Actions pane.
3. To log a user off a session, select the session or desktop and select Log off in the Actions pane. The session closes and the machine becomes available to other users, unless it is allocated to a specific user.

To disconnect a session, select the session or desktop, and select Disconnect in the Actions pane. Applications continue to run and the machine remains allocated to that user. The user can reconnect to the same machine.

To send a message to users, select the session, machine, or user, and then select Send message in the Actions pane. Enter the message.

You can configure power state timers for Desktop OS machines to automatically handle unused sessions. See [Power manage machines](#) for details.

## Configure session prelaunch and session linger

Note: These features are supported on Server OS machines only.

This brief video shows you how to configure session prelaunch and session linger:

The session prelaunch and session linger features help specified users access applications quickly, by starting sessions before they are requested (session prelaunch) and keeping application sessions active after a user closes all applications (session linger).

By default, session prelaunch and session linger are not used: a session starts (launches) when a user starts an application, and remains active until the last open application in the session closes.

### Considerations:

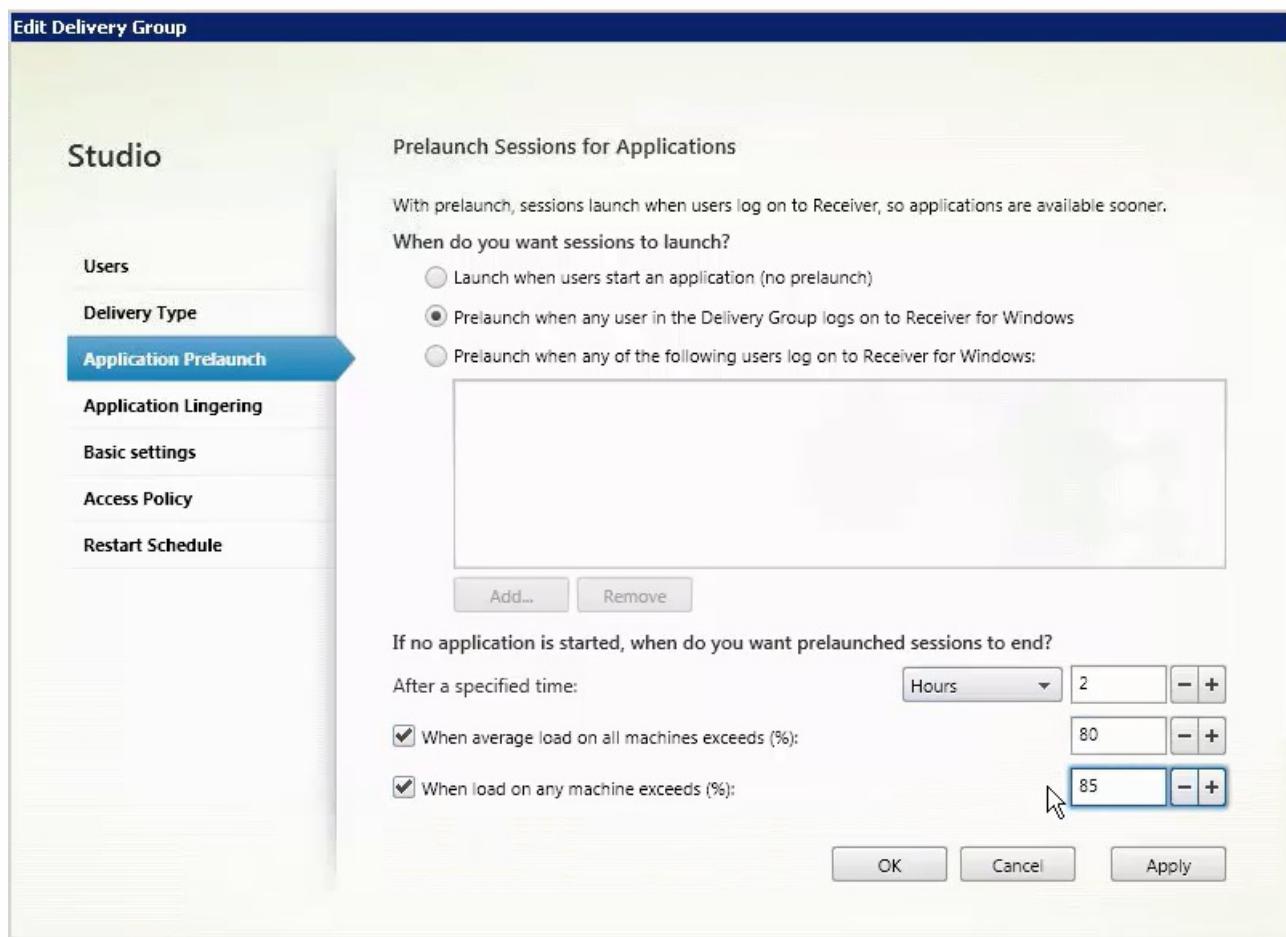
- The Delivery Group must support applications, and the machines must be running a VDA for Server OS, minimum version 7.6.
- Session prelaunch is supported only when using Citrix Receiver for Windows. Session linger is supported when using Citrix Receiver for Windows and Receiver for Web. Additional Receiver configuration is required. For instructions, search for "session prelaunch" in the eDocs content for your Receiver for Windows version.
- Note: Receiver for HTML5 is not supported.
- When using session prelaunch:
  - Regardless of the admin-side settings, if an end user's machine is put into "suspend" or "hibernate" mode, prelaunch will not work.
  - Pre-launch will work as long as the end user locks their machine/session, but if the end user logs off from Citrix Receiver, the session is ended and pre-launch no longer applies.
- Pre-launched and lingering sessions consume a license, but only when connected. Unused pre-launched and lingering sessions disconnect after 15 minutes by default. This value can be configured in PowerShell (New/Set-BrokerSessionPreLaunch cmdlet).
- Careful planning and monitoring of your users' activity patterns are essential to tailoring these features to complement each other. Optimal configuration balances the benefits of earlier application availability for users against the cost of

keeping licenses in use and resources allocated.

- You can also configure session prelaunch for a scheduled time of day in Receiver.

To enable session prelaunch:

1. Select Delivery Groups in the Studio navigation pane.
2. Select a Delivery Group, and then click Edit Delivery Group in the Actions pane.
3. On the Application Prelaunch page, enable session prelaunch by choosing when sessions should launch:
  - When a user starts an application. This is the default setting; session prelaunch is disabled.
  - When any user in the Delivery Group logs on to Receiver for Windows.
  - When anyone in a list of users and user groups logs on to Receiver for Windows. Be sure to also specify users or user groups if you choose this option.



4. A prelaunched session is replaced with a regular session when the user starts an application. If the user does not start an application (the prelaunched session is unused), the following settings affect how long that session remains active. For details about these settings, see

— *How long unused prelaunched and lingering sessions remain active*

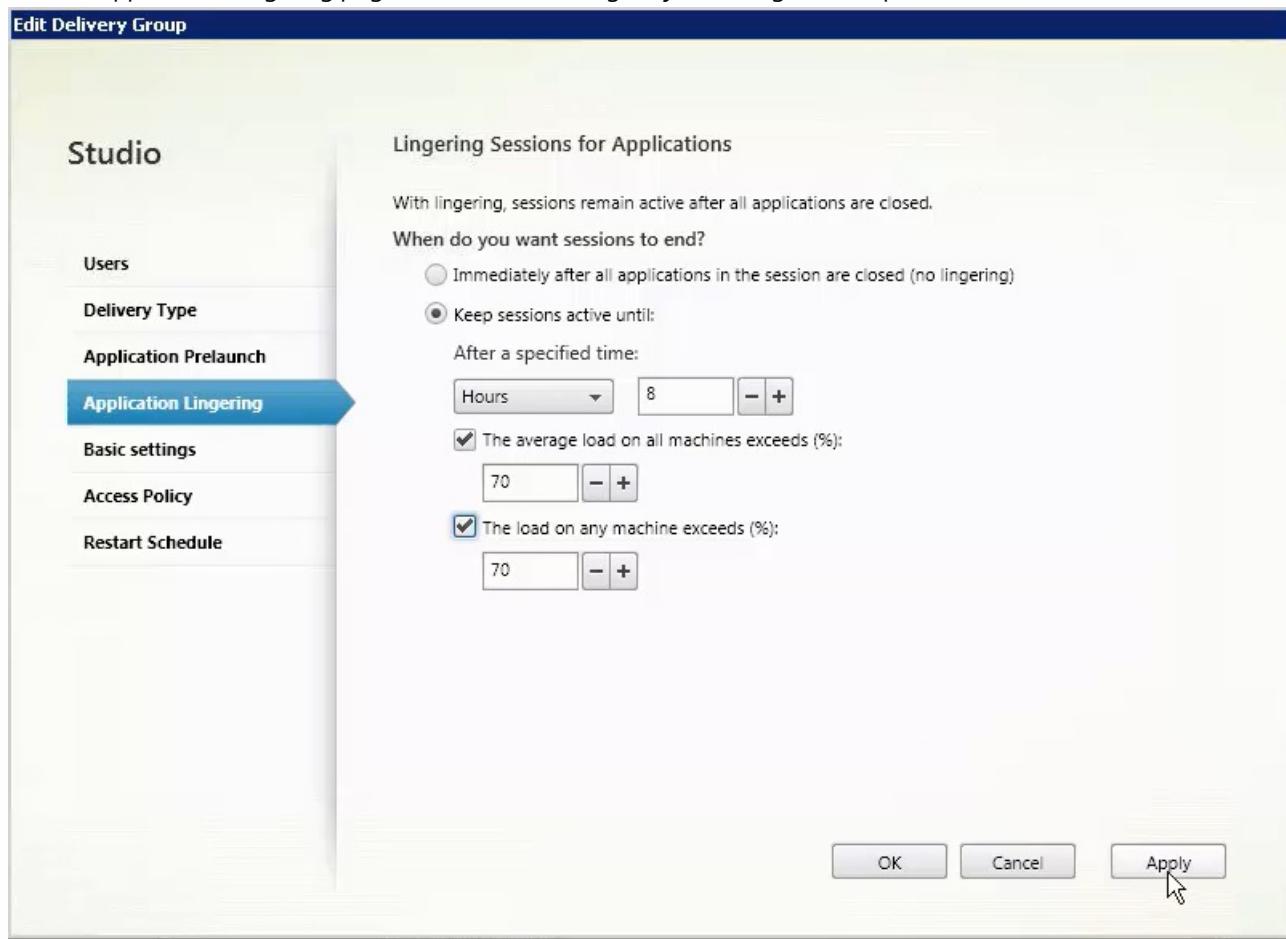
below.

- When a specified time interval elapses. You can change the time interval (1-99 days, 1-2376 hours, or 1-142,560 minutes).
- When the average load on all machines in the Delivery Group exceeds a specified percentage (1-99%).
- When the load on any machine in the Delivery Group exceeds a specified percentage (1-99%).

Recap: A prelaunched session remains active until one of the following events occurs: a user starts an application, the specified time elapses, or a specified load threshold is exceeded.

To enable session linger:

1. Select Delivery Groups in the Studio navigation pane.
2. Select a Delivery Group, and then click Edit Delivery Group in the Actions pane.
3. On the Application Lingering page, enable session linger by selecting the Keep sessions active until radio button.



4. Several settings affect how long a lingering session remains active if the user does not start another application. For details about these settings, see  
— *How long prelaunched and lingering sessions remain active* below.
  - When a specified time interval elapses. You can change the time interval (1-99 days, 1-2376 hours, or 1-142,560 minutes).
  - When the average load on all machines in the Delivery Group exceeds a specified percentage (1-99%).
  - When the load on any machine in the Delivery Group exceeds a specified percentage (1-99%).Recap: A lingering session remains active until one of the following events occurs: a user starts an application, the specified time elapses, or a specified load threshold is exceeded.

**How long unused prelaunched and lingering sessions remain active** - There are several ways to specify how long an unused session remains active if the user does not start an application: a configured timeout and server load thresholds. You can configure all of them; the event that occurs first will cause the unused session to end.

- Timeout - A configured timeout specifies the number of minutes, hours, or days an unused prelaunched or lingering session remains active. If you configure too short a timeout, prelaunched sessions will end before they provide the user benefit of quicker application access. If you configure too long a timeout, incoming user connections might be denied because the server doesn't have enough resources.

You cannot disable this timeout from Studio, but you can in the SDK (New/Set-BrokerSessionPreLaunch cmdlet). If you

disable the timeout, it will not appear in the Studio display for that Delivery Group or in the Edit Delivery Group wizard.

- **Thresholds** - Automatically ending prelaunched and lingering sessions based on server load ensures that sessions remain open as long as possible, assuming server resources are available. Unused prelaunched and lingering sessions will not cause denied connections because they will be ended automatically when resources are needed for new user sessions. You can configure two thresholds: the average percentage load of all servers in the Delivery Group, and the maximum percentage load of a single server in the Delivery Group. When a threshold is exceeded, the sessions that have been in the prelaunch or lingering state for the longest time are ended, sessions are ended one-by-one at minute intervals until the load falls below the threshold. (While the threshold is exceeded, no new prelaunch sessions are started.)

Servers with VDAs that have not registered with the Controller, and servers in maintenance mode are considered fully loaded. An unplanned outage will cause prelaunch and lingering sessions to be ended automatically to free capacity.

# XenApp 发布的应用程序和桌面

May 28, 2016

Use Server OS machines to deliver XenApp published apps and XenApp published desktops.

This table describe the situations, users, and considerations for using these delivery methods.

<b>Use Case</b>	<p><b>You want</b></p> <p>Inexpensive server-based delivery to minimize the cost of delivering applications to a large number of users, while providing a secure, high-definition user experience.</p> <p><b>Your users</b></p> <p>Perform well-defined tasks and do not require personalization or offline access to applications. Users may include task workers such as call center operators and retail workers, or users that share workstations.</p> <p><b>Application types</b></p> <p>Any application.</p>
<b>Benefits and considerations</b>	<p><b>Benefits</b></p> <p>Manageable and scalable solution within your datacenter.</p> <p>Most cost effective application delivery solution.</p> <p>Hosted applications are managed centrally and users cannot modify the application, providing a user experience that is consistent, safe, and reliable.</p> <p><b>Considerations</b></p> <p>Users must be online to access their applications.</p>
<b>User experience</b>	<p>User requests one or more applications from StoreFront, their Start menu, or a URL you provide to them.</p> <p>Applications are delivered virtually and display seamlessly in high definition on user devices.</p> <p>Depending on profile settings, user changes are saved when the user's application session ends. Otherwise, the changes are deleted.</p>
<b>Process, host, and deliver applications</b>	<p><b>Process</b></p> <p>Application processing takes place on hosting machines, rather than on the user devices.</p> <p>The hosting machine can be a physical or a virtual machine.</p> <p><b>Host</b></p>

	<p>Applications and desktops reside on a Server OS machine.</p> <p>Machines become available through machine catalogs.</p> <p><b>Delivery</b></p> <p>Machines within machine catalogs are organized into Delivery groups that deliver the same set of applications to groups of users.</p> <p>Server OS machines support:</p> <ul style="list-style-type: none"> <li>• Desktop and applications Delivery groups that host both desktops and applications.</li> <li>• Application Delivery groups that host only applications.</li> </ul>
<b>Session management and assignment</b>	<p><b>Sessions</b></p> <p>Server OS machines run multiple sessions from a single machine to deliver multiple applications and desktops to multiple, simultaneously connected users. Each user requires a single session from which they can run all their hosted applications.</p> <p>For example, a user logs on and requests an application. One session on that machine becomes unavailable to other users. A second user logs on and requests an application which that machine hosts. A second session on the same machine is now unavailable. If both users request additional applications, no additional sessions are required because a user can run multiple application using the same session. If two more users log on and request desktops, and two sessions are available on that same machine, that single machine is now using four sessions to host four different users.</p> <p><b>Random machine assignments</b></p> <p>Within the Delivery group to which a user is assigned, a machine on the least loaded server is selected. A machine with session availability is randomly assigned to deliver applications to a user when that user logs on.</p>

To deliver XenApp published apps:

1. Install the applications you want to deliver on a master image running a supported Windows server OS.
2. Create a machine catalog for this master image or update an existing catalog with the master image.
3. Create an application Delivery group to deliver the application to users.
4. From the list of application installed, select the application you want to deliver.

To deliver XenApp published desktops:

1. Install apps on a master image running a supported Windows server OS.
2. Create a machine catalog for this master image or update an existing catalog with the master image.
3. Create a desktop Delivery group to deliver the desktops to users.

# VM 托管应用程序

May 28, 2016

Use Desktop OS machines to deliver VM hosted app.

This table describe the situations, users, and considerations for using this delivery method.

<b>Use Case</b>	<p><b>You want</b></p> <p>A client-based application delivery solution that is secure, provides centralized management, and supports a large number of users per host server (or hypervisor), while providing users with applications that display seamlessly in high-definition.</p> <p><b>Your users</b></p> <p>Are internal, external contractors, third-party collaborators, and other provisional team members.</p> <p>Your users do not require off line access to hosted applications.</p> <p><b>Application types</b></p> <p>Applications that might not work well with other applications or might interact with the operation system, such as Microsoft .NET framework. These types of applications are ideal for hosting on virtual machines.</p> <p>Applications running on older operating systems such as Windows XP or Windows Vista, and older architectures, such as 32-bit or 16-bit. By isolating each application on its own virtual machine, if one machine fails, it does not impact other users.</p>
<b>Benefits and considerations</b>	<p><b>Benefits</b></p> <p>Applications and desktops on the master image are securely managed, hosted, and run on machines within your datacenter, providing a more cost effective application delivery solution.</p> <ul style="list-style-type: none"><li>On log on, users can be randomly assigned to a machine within a Delivery Group that is configured to host the same application.</li><li>You can also statically assign a single machine to deliver an application to a single user each time that user logs on. Statically assigned machines allow users to install and manage their own applications on the virtual machine.</li></ul> <p><b>Considerations</b></p> <p>Running multiple sessions is not supported on Desktop OS machines. Therefore, each user consumes a single machine within a Delivery group when they log on, and users must be online to access their applications.</p> <p>This method may increase the amount of server resources for processing applications and increase the amount of storage for users' Personal vDisks.</p>
<b>User</b>	The same seamless application experience as hosting shared applications on Server OS machines.

<b>experience</b>	
<b>Process, host, and deliver applications</b>	<p><b>Process</b> The same as Server OS machines except they are virtual Desktop OS machines.</p> <p><b>Host</b> The same as Server OS machines except they are virtual Desktop OS machines.</p> <p><b>Delivery</b> The same as Server OS machines except Desktop OS machines can exist only in a desktop Delivery group.</p>
<b>Session management and assignment</b>	<p><b>Sessions</b> Desktop OS machines run a single desktop session from a single machine. When accessing applications only, a single user can use multiple applications (and is not limited to a single application) because the operating system sees each application as a new session.</p> <p><b>Random and static machine assignments</b> Within a Delivery group to which a user is assigned, when users log on they can access:</p> <ul style="list-style-type: none"> <li>• Statically assigned machine so that each time the user logs on to the same machine.</li> <li>• Randomly assigned machine that is selected based on session availability.</li> </ul>

To deliver VM hosted apps:

1. Install the applications you want to deliver on a master image running a supported Windows desktop OS.

2. Create a machine catalog for this master image or update an existing catalog with the master image.

When defining the desktop experience for the machine catalog, decide whether you want users to connect to a new VM each time they log in or connect to the same machine each time they log in.

3. Create an application Delivery group to deliver the application to users.

4. From the list of application installed, select the application you want to deliver.

# VDI 桌面

Jan 12, 2017

Use Desktop OS machines to deliver VDI desktops.

VDI desktops are hosted on virtual machines and provide each user with a desktop operating system.

VDI desktops require more resources than XenApp published desktops, but do not require that applications installed on them support server-based operating systems. In addition, depending on the type of VDI desktop you choose, these desktops can be assigned to individual users and allow these users a high degree of personalization.

When you create a machine catalog for VDI desktops, you create one of these types of desktops:

- Random non-persistent desktops, also known as Pooled VDI desktops. Each time users log in to use one of these desktops, they connect to a dynamically selected desktop in a pool of desktops based on a single master image. All changes to the desktop are lost when the machine reboots.
- Static non-persistent desktop. The first time a user logs on to use one off these desktops, the user is assigned a desktop from a pool of desktops based on a single master image. After the first use, each time a user logs in to use one of these desktops, the user connects to the same desktop that user was assigned on first use. All changes to the desktop are lost when the machine reboots.
- Static persistent, also known as VDI with Personal vDisk. Unlike other types of VDI desktops, these desktops can be fully personalized by users. The first time a user logs on to use one off these desktops, the user is assigned a desktop from a pool of desktops based on a single master image. After the first use, each time a user logs in to use one of these desktops, the user connects to the same desktop that user was assigned on first use. Changes to the desktop are retained when the machine reboots because they are stored in a Personal vDisk.

To deliver VDI desktops:

1. Create a master image running a supported Windows desktop OS.
2. Create a machine catalog for this master image or update an existing catalog with the master image.

When defining the desktop experience for the machine catalog, decide whether you want users to connect to a new VM each time they log in or connect to the same machine each time they log in and specify how changes to the desktop are retained.

3. Create a desktop Delivery group to deliver the desktops to users.

# Remote PC Access

Aug 10, 2016

Remote PC Access allows an end user to log on remotely from virtually anywhere to the physical Windows PC in the office. The Virtual Delivery Agent (VDA) is installed on the office PC; it registers with the Delivery Controller and manages the HDX connection between the PC and the end user client devices. Remote PC Access supports a self-service model; after you set up the whitelist of machines that users are permitted to access, those users can join their office PCs to a Site themselves, without administrator intervention. The Citrix Receiver running on their client device enables access to the applications and data on the office PC from the Remote PC Access desktop session.

A user can have multiple desktops, including more than one physical PC or a combination of physical PCs and virtual desktops.

Note: Sleep mode & Hibernation mode for Remote PC is not supported. Remote PC Access is valid only for XenDesktop licenses; sessions consume licenses in the same way as other XenDesktop sessions.

Active Directory considerations:

- Before configuring the remote PC deployment site, set up your Organizational Units (OUs) and security groups and then create user accounts. Use these accounts to specify users for the Delivery Groups you will use to provide Remote PC Access.
- If you modify Active Directory after a machine has been added to a machine catalog, Remote PC Access does not reevaluate that assignment. You can manually reassign a machine to a different catalog, if needed.
- If you move or delete OUs, those used for Remote PC Access can become out of date. VDAs might no longer be associated with the most appropriate (or any) machine catalog or Delivery Group.

Machine catalog and Delivery Group considerations:

- A machine can be assigned to only one machine catalog and one Delivery Group at a time.
- You can put machines in one or more Remote PC Access machine catalogs.
- When choosing Machine Accounts for a machine catalog, select the lowest applicable OU to avoid potential conflicts with machines in another catalog. For example, in the case of Bank/officers/tellers, select tellers.
- You can allocate all machines from one remote PC machine catalog through one or more Delivery Groups. For example, if one group of users requires certain policy settings and another group requires different settings, assigning the users to different Delivery Groups enables you to filter the HDX policies according to each Delivery Group.
- If your IT infrastructure assigns responsibility for servicing users based on geographic location, department, or some other category, you can group machines and users accordingly to allow for delegated administration. Ensure that each administrator has permissions for both the relevant machine catalogs and the corresponding Delivery Groups.
- For users with office PCs running Windows XP, create a separate machine catalog and Delivery Group for those systems. When choosing machine accounts for that catalog in Studio, select the checkbox indicating that some machines are running Windows XP.

Deployment considerations:

- You can create a Remote PC Access deployment and then add traditional Virtual Desktop Infrastructure (VDI) desktops or applications later. You can also add Remote PC Access desktops to an existing VDI deployment.
- Consider whether to enable the Windows Remote Assistance feature when you install the VDA on the office PC. This option allows help desk teams using Director to view and interact with a user sessions using Windows Remote Assistance.
- Consider how you will deploy the VDA to each office PC. Citrix recommends using electronic software distribution such as Active Directory scripts and Microsoft System Center Configuration Manager. The installation media contains sample

Active Directory scripts.

- Secure Boot functionality is currently unsupported. Disable Secure Boot if intending to deploy the workstation VDA.
- Each office PC must be domain-joined with a wired network connection.
- Windows 7 Aero is supported on the office PC, but not required.
- Connect the keyboard and mouse directly to the PC or laptop, not to the monitor or other components that can be turned off. (If you must connect input devices to components such as monitors, they should not be turned off.)
- If you are using smart cards, see [Smart cards](#).
- Remote PC Access can be used on most laptop computers. To improve accessibility and deliver the best connection experience, configure the laptop power saving options to those of a desktop PC. For example:
  - Disable the Hibernate feature.
  - Disable the Sleep feature.
  - Set the close lid action to Do Nothing.
  - Set the press the power button action to Shut Down.
  - Disable video card energy saving features.
  - Disable network interface card energy saving features.
  - Disable battery saving technologies.

The following are not supported for Remote PC Access devices:

- Docking and undocking the laptop.
- KVM switches or other components that can disconnect a session.
- Hybrid PCs (including All-in-One and NVIDIA Optimus laptops and PCs) and Surface Pro/Books.
- Install Citrix Receiver on each client device that remotely accesses the office PC.
- Multiple users with remote access to the same office PC see the same icon in Receiver. When any user remotely logs on to the PC, that resource appears as unavailable to other users.
- By default, a remote user's session is automatically disconnected when a local user initiates a session on that machine (by pressing CTRL+ALT+DEL). To prevent this automatic action, add the following registry entry on the office PC, and then restart the machine.

Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

HKLM\SOFTWARE\Citrix\PortICA\RemotePC "SasNotification"=dword:00000001

To further customize the behavior of this feature under HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\PortICA\RemotePC

- RpcMode (dword)
- RpcTimeout (dword)

RpcMode:

1 - Means that the remote user will always win if he does not respond to the Messaging UI in the specified timeout period.

2 - Means that the Local user will always win. If this setting is not specified, the Remote user will always win by default.

RpcTimeout:

The number of seconds given to the user before we automatically decide which type of mode to enforce. If this setting is not specified, the default value is :30 seconds. The minimum value here should be :30 seconds. The User needs to restart the machine for these changes to take place.

When user wants to forcibly get the console access: The local user can hit Ctr+Alt+Del twice in a gap of :10 seconds to get local control over a remote session and force a disconnect event.

After the registry change and machine restart, if a local user presses CTRL+ALT+DEL to log on to that PC while it is in use by a remote user, the remote user receives a prompt asking whether or not to allow or deny the local user's connection. Allowing the connection will disconnect the remote user's session.

The following XenDesktop features are not supported for Remote PC Access deployments:

- Creating master images and virtual machines
- Delivering hosted applications
- Personal vDisks
- Client folder redirection

## Wake on LAN

Remote PC Access supports Wake on LAN, which gives users the ability to turn on physical PCs remotely. This feature enables users to keep their office PCs turned off when not in use, saving energy costs. It also enables remote access when a machine has been turned off inadvertently, such as during weather events.

With XenDesktop 7.6 Feature Pack 3, Citrix released an experimental Wake on LAN SDK. This enables you or a third-party Wake on LAN solution to create a connector without the requirement of System Center 2012 R2. For more information, see Knowledge Center article [CTX202272](#).

The Remote PC Access Wake on LAN feature is supported on both of the following:

- PCs that support Intel Active Management Technology (AMT)
- PCs that have the Wake on LAN option enabled in the BIOS

You must configure Microsoft System Center Configuration Manager (ConfigMgr) 2012 to use the Wake on LAN feature. ConfigMgr provides access to invoke AMT power commands for the PC, plus Wake-up proxy and magic-packet support. Then, when you use Studio to create a Remote PC Access deployment (or when you add another power management connection to be used for Remote PC Access), you enable power management and specify ConfigMgr access information.

Additionally:

- Using AMT power operations is preferred for security and reliability; however, support is also provided for two non-AMT methods: ConfigMgr Wake-up proxy and raw magic packets.
- On AMT-capable machines only, the Wake on LAN feature also supports the Force-Shutdown and Force-Restart actions in Studio and Director. Additionally, a Restart action is available in StoreFront and Receiver.

For more information, see [Configuration Manager and Remote PC Access Wake on LAN](#) and [Provide users with Remote PC Access](#).

# 向用户提供 Remote PC Access

May 28, 2016

Using Remote PC Access, desktop users can securely access resources on the office PC while experiencing the benefits of Citrix HDX technology.

Note: Remote PC Access is valid only for XenDesktop licenses.

1. To use the Remote PC Access power management feature (also known as Remote PC Access Wake on LAN), complete the configuration tasks on the PCs and on Microsoft System Center Configuration Manager (ConfigMgr) before creating the Remote PC Access deployment in Studio. See [Configuration Manager and Remote PC Access Wake on LAN](#) for details.

2. When creating the initial Remote PC Access deployment, you can enable or disable power management for the machines in the default Remote PC Access Machine Catalog. If you enable power management, specify ConfigMgr connection information. Then specify users and machine accounts. See [Create a Site](#) for more information. Creating a Remote PC deployment does not prevent VDI use of the Site in the future.

Creating a Remote PC Access deployment creates a default machine catalog named

— *Remote PC Access Machines*

and a default delivery group named

— *Remote PC Access Desktops*

.

3. When creating another machine catalog for use with Remote PC Access:

- Operating System: Select Remote PC Access, and choose a power management connection. You can also choose not to use power management. If there are no configured power management connections, you can add one after you finish the machine catalog creation wizard (connection type = Microsoft Configuration Manager Wake on LAN), and then edit the machine catalog, specifying that new connection.
- Machine Accounts: You can select from the machine accounts or Organizational Units (OUs) displayed, or add machine accounts and OUs.

4. Install the VDA on the office PC used for local and remote access. Typically, you deploy the VDA automatically using your package management software; however, for proof-of-concept or small deployments, you can install the VDA manually on each office PC.

After the VDA is installed, the next domain user that logs on to a console session (locally or through RDP) on the office PC is automatically assigned to the Remote PC desktop. If additional domain users log on to a console session, they are also added to the desktop user list, subject to any restrictions you have configured.

Note: To use RDP connections outside of your XenApp or XenDesktop environment, you must add users or groups to the Direct Access Users group.

5. Instruct users to download and install Citrix Receiver onto each client device they will use to access the office PC remotely. Citrix Receiver is available from <http://www.citrix.com> or the application distribution systems for supported mobile devices.

You can edit a power management connection to configure advanced settings. You can enable:

- Wake-up proxy delivered by ConfigMgr.
- Wake on LAN (magic) packets. If you enable Wake on LAN packets, you can select a Wake on LAN transmission method: subnet-directed broadcasts or Unicast.

The PC uses AMT power commands (if they are supported), plus any of the enabled advanced settings. If the PC does not use AMT power commands, it uses the advanced settings.

## Troubleshooting

The Delivery Controller writes the following diagnostic information about Remote PC Access to the Windows Application Event log. Informational messages are not throttled. Error messages are throttled by discarding duplicate messages.

- 3300 (informational) - Machine added to catalog
- 3301 (informational) - Machine added to delivery group
- 3302 (informational) - Machine assigned to user
- 3303 (error) - Exception

When power management for Remote PC Access is enabled, subnet-directed broadcasts might fail to start machines that are located on a different subnet from the Controller. If you need power management across subnets using subnet-directed broadcasts, and AMT support is not available, try the Wake-up proxy or Unicast method (ensure those settings are enabled in the advanced properties for the power management connection).

# 管理 Remote PC Access 交付组

May 28, 2016

If a machine in a Remote PC Access machine catalog is not assigned to a user, Studio temporarily assigns the machine to a Delivery Group associated with that machine catalog. This temporary assignment provides information, so that the machine can be assigned later to a user. The Delivery Group to machine catalog association has a priority value.

Priority determines to which Delivery Group that machine is assigned when it registers with the system or when a user needs a machine assignment. The lower the value, the higher the priority. If a Remote PC Access machine catalog has multiple Delivery Group assignments, the software selects the match with the highest priority. You can set this priority value using the PowerShell SDK.

## Add or remove a Remote PC Access machine catalog association

When first created, Remote PC Access machine catalogs are associated with a Delivery Group. This means that machine accounts or Organizational Units added to the machine catalog later can be added to the Delivery Group. This association can be switched off or on.

1. Select Delivery Groups in the Studio navigation pane.
2. Select a Remote PC Access Delivery Group.
3. In the Details section, select the Catalogs tab and then select a Remote PC Access machine catalog.
4. To add or restore an association, select Add Desktops. To remove an association, select Remove Association.

# App-V

May 28, 2016

Microsoft Application Virtualization (App-V) lets you deploy, update, and support applications as services. Users access applications without installing them on their own devices. App-V and Microsoft User State Virtualization (USV) provide access to applications and data, regardless of location and connection to the Internet.

The following table lists supported versions. (The App-V 4.6 2 client is no longer supported.)

App-V	XenDesktop and XenApp versions	
	Delivery Controller	VDA
5.0	XenDesktop 7 through current XenApp 7.5 through current	7.0 through current
5.0 SP1	XenDesktop 7 through current XenApp 7.5 through current	7.0 through current
5.0 SP2	XenDesktop 7 through current XenApp 7.5 through current	7.1 through current
5.0 SP3 and 5.1	XenDesktop 7.6 XenApp 7.6	7.6.300

The supported App-V client does not support offline access to applications. App-V integration support includes using SMB shares for applications; the HTTP protocol is not supported.

Applications are available seamlessly without any pre-configuration or changes to operating system settings. App-V contains the following components:

- Management server — Provides a centralized console to manage App-V infrastructure and deliver virtual applications to both the App-V Desktop Client as well as a Remote Desktop Services Client. The App-V management server authenticates, requests, and provides the security, metering, monitoring, and data gathering required by the administrator. The server uses Active Directory and supporting tools to manage users and applications.
- Publishing server — Provides App-V clients with applications for specific users, and hosts the virtual application package for streaming. It fetches the packages from the management server.
- Client — Retrieves virtual applications, publishes the applications on the client, and automatically sets up and manages virtual environments at runtime on Windows devices. The App-V client is installed on the VDA and stores user-specific virtual application settings, such as registry and file changes in each user's profile.

You can launch App-V applications from Server OS and Desktop OS Delivery Groups:

- Through Citrix Receiver
- From the Start menu
- Through the App-V client and Citrix Receiver
- Simultaneously by multiple users on multiple devices
- Through Citrix StoreFront

Modified App-V application properties are implemented when the application is started. For example, for applications with a modified display name or customized icon, the modification appears when users start the application.

There is no change in App-V applications performance when a desktop and application Delivery Group is changed to an application-only Delivery Group.

Only an App-V server-based deployment in which an administrator uses an App-V management server and publishing server to manage App-V applications is supported.

## Configure App-V

To deliver App-V applications:

1. Deploy App-V, as described in the instructions in <http://technet.microsoft.com/en-us/virtualization/hh710199>.
2. Publish the App-V applications on the App-V management server. Configure settings such as permissions and File Type Association. These settings already exist if you already deployed App-V.
3. Optionally, change App-V publishing server settings; see below.
4. Install the App-V client on VDAs.
5. During Site creation in Studio, specify the App-V publishing and management server URLs with port numbers. These servers are automatically used by the Delivery Groups.
6. Install the App-V client in the master image for machine catalogs. Configured the client with settings such as ShareContentStoreMode and EnablePackageScripts. (You do not need to configure the App-V Publishing Server in the master image because it is configured during application launch.)
7. During Delivery Group creation, select the App-V applications.

The applications are now available.

You can specify or change App-V server information after you create a Site. Select Configuration > App-V Publishing in the Studio navigation pane and then selecting entries in the Actions pane. You can add App-V publishing by specifying URLs with port numbers for the App-V management and publishing servers. You can also edit or remove those addresses. If you refresh the App-V applications, the display indicates if there is a problem connecting to a server and removes entries for applications that are no longer available.

## App-V publishing server settings

To change publishing server settings, Citrix recommends using the SDK cmdlets on the Controller.

- To view publishing server settings, enter Get-CtxAppvServerSetting -AppVPublishingServer <pubServer>.
- To ensure that App-V applications launch properly, enter Set-CtxAppvServerSetting –UserRefreshOnLogon 0.

The following cmdlet changes the settings of the App-V publishing server on the Controller. Not all parameters are mandatory.

```
Set-CtxAppvServerSetting –AppVPublishingServer  
<pubServer> -UserRefreshOnLogon <bool> -UserRefreshEnabled <bool>  
-UserRefreshInterval <int> -UserRefreshIntervalUnit <Day/Hour>  
-GlobalRefreshOnLogon <bool> -GlobalRefreshEnabled<bool>  
-GlobalRefreshInterval <int> -GlobalRefreshIntervalUnit <Day/Hour>
```

Note: If you previously used GPO policy settings for managing publishing server settings, the GPO settings override any App-V integration settings, including the previous cmdlet settings. This may result in App-V application launch failure. Citrix recommends that you remove all GPO policy settings and configure the same settings using the SDK.

## Troubleshoot

- If the Test connection operation returns an error when you specify App-V management server and publishing server addresses in Studio, check the following:
  1. The App-V server is powered on: either send a Ping command or check the IIS Manager (each App-V server should be in a Started and Running state).
  2. PowerShell remoting is enabled on the App-V server. If it is not, follow the procedure in <http://technet.microsoft.com/en-us/magazine/ff700227.aspx>.
  3. The App-V server is added to Active Directory.  
If the Studio machine and the App-V server are in different Active Directory domains that do not have a trust relationship, from the PowerShell console on the Studio machine, run winrm s winrm/Config/client '@(TrustedHosts=<App-V server FQDN>)'. If TrustedHosts is managed by GPO, the following error message will display: "The config setting TrustedHosts cannot be changed because use is controlled by policies. The policy would need to be set to "Not Configured" in order to change the config setting". If this message displays, add an entry for the App-V server name to the TrustedHosts policy in GPO (Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Client).
  4. The Studio administrator is also an App-V server administrator.
  5. File sharing is enabled on the App-V server: enter \\<App-V server FQDN> in Windows Explorer or with the Run command.
  6. The App-V server has the same file sharing permissions as the App-V administrator: on the App-V server, add an entry for \\<App-V Server FQDN> in Stored User Names and Passwords, specifying the credentials of the user who has administrator privileges on the App-V server. For guidance, see <http://support.microsoft.com/kb/306541>.
- If Application discovery fails, check the following:
  1. Studio administrator is an App-V management server administrator.
  2. The App-V management server is running. Check this by opening the IIS Manager; the server should be in a Started and Running state.
  3. PowerShell remoting is enabled on the App-V servers. If either is not enabled, follow the procedure in <http://technet.microsoft.com/en-us/magazine/ff700227.aspx>.
  4. Packages have appropriate security permissions for the Studio administrator to access.
- If App-V applications do not launch, check the following:
  1. The publishing server is running. Check this by opening the IIS Manager; the server should be in a Started and Running state.
  2. App-V packages have appropriate security permissions so that users can access.
  3. On the VDA:
    - Make sure that Temp is pointing to the correct location, and that there is enough space available in the Temp directory.
    - Make sure that the App-V client is installed, and no earlier than version 5.0.
    - Make sure you have Administrator permissions and run Get-AppvClientConfiguration. Make sure that EnablePackageScripts is set to 1. If it is not set to 1, run Set-AppvClientConfiguration -EnablePackageScripts \$true. Citrix recommends that you perform this step when you create a master image so that all VDAs created from the master image have the correct configuration.
    - From the Registry editor (regedit), go to HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Citrix\AppV. Make sure that the AppVServers key has the following value format: AppVManagementServer+metadata;PublishingServer (for example: http://xmas-demo-appv.blrstrm.com+0+0+0+1+1+1+0+1;http://xmas-demo-appv.blrstrm.com:8082).
    - Make sure that CtxAppVCOMAdmin has administrator privileges. During VDA installation CtxAppVCOMAdmin is usually created and added to the Local Administrators Group on the VDA machine. However, depending on the Active Directory policy, this user might lose the administrative association.

Run compmgmt.msc and browse to Local Users and Groups Users. If CtxAppVCOMAdmin is not an administrator, edit the group policy or contact your administrator, so that this user account retains its administrative association.

4. On the master image where the App-V client is installed, the PowerShell ExecutionPolicy should be set to RemoteSigned because the AppV client module provided by Microsoft is not signed, and this ExecutionPolicy allows PowerShell to run unsigned local scripts and cmdlets. Use one of the following methods to set the ExecutionPolicy:
  - Logged in as administrator, enter the following PowerShell cmdlet: Set-ExecutionPolicy RemoteSigned.
  - From Group Policy settings, go to Computer Configuration > Policies > Administrative Templates > Windows Components > Windows PowerShell> Turn on Script Execution.
5. Check the publishing servers:
  - Run Get-AppvPublishingServer \* to display the list of publishing servers.
  - Check whether UserRefreshOnLogon is set to False. If not, the first App-V application launch typically fails.
  - With Administrator privileges, run Set-AppvPublishingServer and set UserRefreshOnLogon to False.If these steps do not resolve the issues, enable and examine the logs.

## Enable logs

To enable Studio logs:

1. Create the folder C:\CtxAppvLogs.
2. Go to C:\ProgramFiles\Citrix\StudioAppVIntegration\SnapIn\Citrix.Appv.Admin.V1 and open CtxAppvCommon.dll.config in a text editor such as Notepad, as an administrator. Uncomment the following line:  
`<add key ="LogFileName" value="C:\CtxAppvLogs\log.txt"/>`

To enable VDA logs:

1. Create the folder C:\CtxAppvLogs.
2. Go to C:\ProgramFiles\Citrix\ Virtual Desktop Agent, and open CtxAppvCommon.dll.config in a text editor such as Notepad, as an administrator. Uncomment the following line:  
`<add key ="LogFileName" value="C:\CtxAppvLogs\log.txt"/>`
3. Uncomment the following line and set the value field to 1, as shown in the following example:  
`<add key ="EnableLauncherLogs" value="1"/>`

All configuration-related logs are located at C:\CtxAppvLogs. The application launch logs are located at:

- XenDesktop 7.1 and later, and XenApp 7.5 and later — %LOCALAPPDATA%\Citrix\CtxAppvLogs.
  - XenDesktop 7.0 — %LocalAppData%\temp\CtxAppVLogs
- LOCALAPPDATA resolves to the local folder for the logged in user. Make sure to check in the local folder of the launching user (for whom application launch failed).

4. As administrator, restart the Broker service or restart the VDA machine to start logging.

# 本地应用程序访问和 URL 重定向

Sep 09, 2015

Local App Access seamlessly integrates locally installed Windows applications into a hosted desktop environment without changing from one computer to another. With Local App Access, you can:

- Access applications installed locally on a physical laptop, PC, or other device directly from the virtual desktop.
- Provide a flexible application delivery solution. If users have local applications that you cannot virtualize or that IT does not maintain, those applications still behave as though they are installed on a virtual desktop.
- Eliminate double-hop latency when applications are hosted separately from the virtual desktop, by putting a shortcut to the published application on the user's Windows device.
- Use applications such as:
  - Video conferencing software such as GoToMeeting.
  - Specialty or niche applications that are not yet virtualized.
  - Applications and peripherals that would otherwise transfer large amounts of data from a user device to a server and back to the user device, such as DVD burners and TV tuners.

In XenApp and XenDesktop, hosted desktop sessions use URL redirection to launch Local App Access applications. URL redirection makes the application available under more than one URL address. It launches a local browser (based on the browser's URL blacklist) by selecting embedded links within a browser in a desktop session. If you navigate to a URL that is not present in the blacklist, the URL is opened in the desktop session again.

URL redirection works only for desktop sessions, not application sessions. The only redirection feature you can use for application sessions is host-to-client content redirection, which is a type of server FTA. This FTA redirects certain protocols to the client, such as http, https, rtsp, or mms. For example, if you only open embedded links with http, the links directly open with the client application. There is no URL blacklist or whitelist support.

When Local App Access is enabled, URLs that are displayed to users as links from locally-running applications, from user-hosted applications, or as shortcuts on the desktop are redirected in one of the following ways:

- From the user's computer to the hosted desktop
- From the XenApp or XenDesktop server to the user's computer
- Rendered in the environment in which they are launched (not redirected)

To specify the redirection path of content from specific Web sites, configure the URL whitelist and URL blacklist on the Virtual Delivery Agent. Those lists contain multi-string registry keys that specify the URL redirection policy settings; for more information, see the Local App Access policy settings.

URLs can be rendered on the VDA with the following exceptions:

- Geo/Locale information — Web sites that require locale information, such as msn.com or news.google.com (opens a country specific page based on the Geo). For example, if the VDA is provisioned from a data center in the UK and the client is connecting from India, the user expects to see in.msn.com but instead sees uk.msn.com.
- Multimedia content — Web sites containing rich media content, when rendered on the client device, give the end users a native experience and also save bandwidth even in high latency networks. Although there is Flash redirection feature, this complements by redirecting sites with other media types such as Silverlight. This is in a very secure environment. That is, the URLs that are approved by the administrator are run on the client while the rest of the URLs are redirected to the VDA.

In addition to URL redirection, you can use File Type Association (FTA) redirection. FTA launches local applications when a file is encountered in the session. If the local app is launched, it must have access to the file to open it. Therefore, you can

only open files that reside on network shares or on client drives (using client drive mapping) using local applications. For example, when opening a PDF file, if a PDF reader is a local app, then the file opens using that PDF reader. Because the local app can access the file directly, there is no network transfer of the file through ICA to open the file.

## Requirements, considerations, and limitations

Local App Access is supported on the valid operating systems for VDAs for Windows Server OS and VDAs for Windows Desktop OS, and requires Citrix Receiver for Windows version 4.1 (minimum). The following browsers are supported:

- Internet Explorer 8, 9, 10, and 11
- Firefox 3.5 through 21.0
- Chrome 10

Review the following considerations and limitations when using Local App Access and URL redirection.

- Local App Access is designed for full-screen, virtual desktops spanning all monitors:
  - The user experience can be confusing if Local App Access is used with a virtual desktop that runs in windowed mode or does not cover all monitors.
  - For multiple monitors, when one monitor is maximized it becomes the default desktop for all applications launched in that session, even if subsequent applications typically launch on another monitor.
  - The feature supports one VDA; there is no integration with multiple concurrent VDAs.
- Some applications can behave unexpectedly, affecting users:
  - Users might be confused with drive letters, such as local C: rather than virtual desktop C: drive.
  - Available printers in the virtual desktop are not available to local applications.
  - Applications that require elevated permissions cannot be launched as client-hosted applications.
  - There is no special handling for single-instance applications (such as Windows Media Player).
  - Local applications appear with the Windows theme of the local machine.
  - Full-screen applications are not supported. This includes applications that open to full screen, such as PowerPoint slide shows or photo viewers that cover the entire desktop.
  - Local App Access copies the properties of the local application (such as the shortcuts on the client's desktop and Start menu) on the VDA; however, it does not copy other properties such as shortcut keys and read-only attributes.
  - Applications that customize how overlapping window order is handled can have unpredictable results. For example, some windows might be hidden.
  - Shortcuts are not supported, including My Computer, Recycle Bin, Control Panel, Network Drive shortcuts, and folder shortcuts.
  - The following file types and files are not supported: custom file types, files with no associated programs, zip files, and hidden files.
  - Taskbar grouping is not supported for mixed 32-bit and 64-bit client-hosted or VDA applications, such as grouping 32-bit local applications with 64-bit VDA applications.
  - Applications cannot be launched using COM. For example, if you click an embedded Office document from within an Office application, the process launch cannot be detected, and the local application integration fails.
- URL redirection supports only explicit URLs (that is, those appearing in the browser's address bar or found using the in-browser navigation, depending on the browser).
- URL redirection works only with desktop sessions, not with application sessions.
- The local desktop folder in a VDA session does not allow users to create new files.
- Multiple instances of a locally-running application behave according to the taskbar settings established for the virtual desktop. However, shortcuts to locally-running applications are not grouped with running instances of those applications. They are also not grouped with running instances of hosted applications or pinned shortcuts to hosted applications. Users can close only windows of locally-running applications from the Taskbar. Although users can pin local application windows to the desktop Taskbar and Start menu, the applications might not launch consistently when using

these shortcuts.

## Interaction with Windows

The Local App Access interaction with Windows includes the following behaviors.

- Windows 8 and Windows Server 2012 short cut behavior
  - Windows Store applications installed on the client are not enumerated as part of Local App Access shortcuts.
  - Image and video files are usually opened by default using Windows store applications. However, Local App Access enumerates the Windows store applications and opens shortcuts with desktop applications.
- Local Programs
  - For Windows 7, the folder is available in the Start menu.
  - For Windows 8, Local Programs is available only when the user chooses All Apps as a category from the Start screen. Not all subfolders are displayed in Local Programs.
- Windows 8 graphics features for applications
  - Desktop applications are restricted to the desktop area and are covered by the Start screen and Windows 8 style applications.
  - Local App Access applications do not behave like desktop applications in multi-monitor mode. In multi-monitor mode, the Start screen and the desktop display on different monitors.
- Windows 8 and Local App Access URL Redirection
  - Because Windows 8 Internet Explorer has no add-ons enabled, use desktop Internet Explorer to enable URL redirection.
  - In Windows Server 2012, Internet Explorer disables add-ons by default. To implement URL Redirection, disable Internet Explorer enhanced configuration. Then reset the Internet Explorer options and restart to ensure that add-ons are enabled for standard users.

# 配置本地应用程序访问和 URL 重定向

Jan 24, 2017

To use Local App Access and URL redirection with Citrix Receiver:

- Install Receiver on the local client machine. You can enable both features during Receiver installation or you can enable Local App Access template using the Group Policy editor.
- Set the Allow local app access policy setting to Enabled. You can also configure URL whitelist and blacklist policy settings for URL redirection. For more information, see [Local App Access policy settings](#).

Enable local app access and URL redirection during Receiver installation

To enable Local App Access and URL redirection for all local applications:

1. Set the Allow local app access policy setting to Enabled. When this setting is enabled, the VDA allows the client to decide whether administrator-published applications and Local App Access shortcuts are enabled in the session. (When this setting is disabled, both administrator-published applications and Local App Access shortcuts do not work for the VDA.) This policy setting applies to the entire machine, as well as the URL redirection policy.
2. Enable Local App Access and URL redirection when you install Citrix Receiver for all users on a machine. This action also registers the browser add-ons required for URL redirection.

From the command prompt, run the appropriate command to install the Receiver with the following option:

CitrixReceiver.exe /ALLOW\_CLIENTHOSTEDAPPSURL=1

CitrixReceiverWeb.exe /ALLOW\_CLIENTHOSTEDAPPSURL=1

Enable the local app access template using the Group Policy editor

1. Run gpedit.msc.
2. Select Computer Configuration. Right-click Administrative Templates and select Add/Remote Templates > Add.
3. Add the icaclient.adm template located in the Receiver Configuration folder (usually in c:\Program Files (x86)\Citrix\Online Plugin\Configuration). (After the icaclient.adm template is added to Computer Configuration, it is also available in User Configuration.)
4. Expand Administrative Templates > Classic Administrative Templates (ADM) > Citrix Components > Citrix Receiver > User Experience.
5. Select Local App Access settings.
6. Select Enabled and then select Allow URL Redirection. For URL redirection, register browser add-ons using the command line, as described below.

Provide access to only published applications

To provide access to only published applications:

1. On the server where the Delivery Controller is installed, run regedit.exe.
  1. Navigate to HKLM\Software\Wow6432Node\Citrix\DesktopStudio.
  2. Add the REG\_DWORD entry ClientHostedAppsEnabled with a value of 1. (A 0 value disables Local App Access.)
2. Restart the Delivery Controller server and then restart Studio.
3. Publish Local App Access applications.
  1. Select Delivery Groups in the Studio navigation pane and then select the Applications tab.
  2. Select Create Local Access Application in the Actions pane.
  3. Select the desktop Delivery Group.
  4. Enter the full executable path of the application on the user's local machine.
  5. Indicate if the shortcut to the local application on the virtual desktop will be visible on the Start menu, the desktop, or

both.

6. Accept the default values on the Name page and then review the settings.
4. Enable Local App Access and URL redirection when you install Citrix Receiver for all users on a machine. This action also registers the browser add-ons required for URL redirection.  
From the command prompt, run the command to install the Receiver with the following option:  
`CitrixReceiver.exe /ALLOW_CLIENTHOSTEDAPPSURL=1`  
`CitrixReceiverWeb.exe /ALLOW_CLIENTHOSTEDAPPSURL=1`
5. Set the Allow local app access policy setting to Enabled. When this setting is enabled, the VDA allows the client to decide whether administrator-published applications and Local App Access shortcuts are enabled in the session. (When this setting is disabled, both administrator-published applications and Local App Access shortcuts do not work for the VDA.)

## Register browser add-ons

Note: The browser add-ons required for URL redirection are registered automatically when you install Receiver from the command line with the /ALLOW\_CLIENTHOSTEDAPPSURL=1 option.

You can use the following commands to register and unregister one or all add-ons:

- To register add-ons on a client device: <client-installation-folder>\redirector.exe /reg<browser>
- To unregister add-ons on a client device: <client-installation-folder>\redirector.exe /unreg<browser>
- To register add-ons on a VDA: <VDAinstallation-folder>\VDARedirector.exe /reg<browser>
- To unregister add-ons on a VDA: <VDAinstallation-folder>\VDARedirector.exe /unreg<browser>

where <browser> is IE, FF, Chrome, or All.

For example, the following command registers Internet Explorer add-ons on a device running Receiver.

`C:\Program Files\Citrix\ICA Client\redirector.exe/regIE`

The following command registers all add-ons on a Windows Server OS VDA.

`C:\Program Files (x86)\Citrix\System32\VDARedirector.exe /regAll`

## URL interception across browsers

Description	Configuration
By default, Internet Explorer redirects the URL entered. If the URL is not in the blacklist but is redirected to another URL by the browser or website, the final URL is not redirected, even if it is on the blacklist.	For URL redirection to work correctly, enable the add-on when prompted by the browser. If the add-ons using Internet options or the add-ons in the prompt are disabled, URL redirection does not work correctly.
The Firefox add-ons always redirect the URLs.	When an add-on is installed, Firefox prompts to allow/prevent installing the add-on on a new tab page. You must allow the add-on for the feature to work.
The Chrome add-on always redirects the final URL that is navigated and not the entered URLs.	The extensions have been installed externally. If you disable the extension, the URL redirection feature does not work in Chrome. If the URL redirection is required in Incognito mode, allow the extension to run in that mode in the browser Settings.

## Configure local application behavior on logoff and disconnect

1. On the hosted desktop, run regedit.msc.
  1. Navigate to HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\Client Hosted Apps\Policies\Session State.  
For a 64-bit system, navigate to HKEY\_LOCAL\_MACHINE\SOFTWARE\wow6432node\Citrix\Client Hosted Apps\Policies\Session State.
2. Add the REG\_DWORD entry Terminate with one of the values:
  - 1 - Local applications continue to run when a user logs off or disconnects from the virtual desktop. Upon reconnection, local applications are reintegrated if they are available in the local environment.
  - 3 - Local applications close when a user logs off or disconnects from the virtual desktop.

# 服务器 VDI

Oct 24, 2016

Use the Server VDI (Virtual Desktop Infrastructure) feature to deliver a desktop from a server operating system for a single user.

- Enterprise administrators can deliver server operating systems as VDI desktops, which can be valuable for users such as engineers and designers.
- Service Providers can offer desktops from the cloud; those desktops comply with the Microsoft Services Provider License Agreement (SPLA).

You can use the Enhanced Desktop Experience Citrix policy setting to make the server operating system look like a Windows 7 operating system.

The following features cannot be used with Server VDI:

- Personal vDisks
- HDX 3D Pro
- Hosted applications
- Local App Access
- Direct (non-brokered) desktop connections
- Remote PC Access

For Server VDI to work with TWAIN devices such as scanners, the Windows Server Desktop Experience feature must be installed. In Windows Server 2012, this is an optional feature which you install from Administrative Tools > Server Manager > Features > Add features > Desktop Experience.

Server VDI is supported on the same server operating systems as the VDA for Windows Server OS.

1. Prepare the Windows server for installation: ensure that Remote Desktop Services role services are not installed and that users are restricted to a single session:
  - Use Windows Server Manager to ensure that the Remote Desktop Services role services are not installed. If they were previously installed, remove them.
  - Ensure that the 'Restrict each user to a single session' property is enabled.
    - On Windows Server 2008 R2, access this property through Administrative Tools > Remote Desktop Services > Remote Desktop Session Host Configuration. In the Edit settings > General section, the Restrict each user to a single session setting should indicate Yes.
    - On Windows Server 2012, edit the registry to set the Terminal Server setting. In registry key HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer to set DWORD fSingleSessionPerUser to 1.
2. For Windows Server 2008 R2, install Microsoft .NET Framework 3.5 SP1 on the server before installing the VDA.
3. Use the command line interface to install a VDA on a supported server or server master image, specifying the /quiet and /servervdi options. (By default, the installer blocks the Windows Desktop OS VDA on a server operating system; using the command line overrides this behavior.)  
`XenDesktopVdaSetup.exe /quiet /servervdi`

You can specify the Delivery Controller or Controllers while installing the VDA using the **/controllers** option.

Use the **/enable\_hdx\_ports** option to open ports in the firewall, unless the firewall is to be configured manually.

Add the **/masterimage** option if you are installing the VDA on an image, and will use MCS to create server VMs from that image.

Do not include options for features that are not supported with Server VDI, such as **/baseimage**, **/enable\_hdx\_3d\_pro**, or **/xa\_server\_location**.

4. Create a Machine Catalog for Server VDI.
  1. On the Operating System page, select Windows Desktop OS.
  2. On the Summary page, specify a machine catalog name and description for administrators that clearly identifies it as Server VDI; this will be the only indicator in Studio that the catalog supports Server VDI.
- When using Search in Studio, the Server VDI catalog you created is displayed on the Desktop OS Machines tab, even though the VDA was installed on a server.
5. Create a Delivery Group and assign the Server VDI catalog you created in the previous step.

If you did not specify the Delivery Controllers while installing the VDA, specify them afterward using Citrix policy setting, Active Directory, or by editing the VDA machine's registry values.

# 删除组件

May 28, 2016

To remove components, Citrix recommends using the Windows feature for removing or changing programs. Alternatively, you can remove components using the command line, or a script on the installation media.

When you remove components, prerequisites are not removed, and firewall settings are not changed. When you remove a Controller, the SQL Server software and the databases are not removed.

Before removing a Controller, remove it from the Site. Before removing Studio or Director, Citrix recommends closing them.

If you upgraded a Controller from an earlier deployment that included Web Interface, you must remove the Web Interface component separately; you cannot use the installer to remove Web Interface.

To remove components using the Windows feature for removing or changing programs

From the Windows feature for removing or changing programs:

- To remove a Controller, Studio, Director, License Server, or StoreFront, select Citrix XenApp <version> or Citrix XenDesktop <version>, then right-click and select Uninstall. The installer launches, and you can select the components to be removed.  
Alternatively, you can remove StoreFront by right-clicking Citrix StoreFront and selecting Uninstall.
- To remove a VDA, select Citrix Virtual Delivery Agent <version>, then right-click and select Uninstall. The installer launches and you can select the components to be removed.
- To remove the Universal Print Server, select Citrix Universal Print Server, then right-click and select Uninstall.

To remove core components using the command line

From the \x64\XenDesktop Setup directory on the installation media, run the XenDesktopServerSetup.exe command.

- To remove one or more components, use the /remove and /components options.
- To remove all components, use the /removeall option.

For command and parameter details, see [Install using the command line](#).

For example, the following command removes Studio.

\x64\XenDesktop Setup\XenDesktopServerSetup.exe /remove /components studio

To remove a VDA using the command line

From the \x64\XenDesktop Setup directory on the installation media, run the XenDesktopVdaSetup.exe command.

- To remove one or more components, use the /remove and /components options.
- To remove all components, use the /removeall option.

For command and parameter details, see [Install using the command line](#).

For example, the following command removes the VDA and Receiver.

\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /removeall

To remove VDAs using a script in Active Directory; see [Install or remove Virtual Delivery Agents using scripts](#).

# 升级和迁移

May 28, 2016

## Upgrade

Upgrading changes deployments to the newest component versions without having to set up new machines or Sites; this is known as an in-place upgrade. You can upgrade:

- From XenDesktop version 5.6 (or a later version) to the latest version of 7.6 LTSR
- From XenApp version 7.5 to the latest version of 7.6 LTSR

You can also upgrade a XenApp 6.5 worker server to a XenApp 7.6 VDA for Windows Server OS. This is a supplementary activity to migrating XenApp 6.5.

To upgrade a XenDesktop 5.6 (or later) farm or a XenApp 7.5 Site:

1. Run the installer on the machines where the core components and VDAs are installed. The software determines if an upgrade is available and installs the newer version.
2. Use the newly upgraded Studio to upgrade the database and the Site.

For more information, see [Upgrade a deployment](#).

For information about installing Controller hotfixes, see Knowledge Center article [CTX201988](#).

To upgrade a XenApp 6.5 worker server to the latest version of the 7.6 LTSR VDA:

1. Run the product installer on the XenApp 6.5 worker server. The software removes the server from the XenApp 6.5 farm, removes the XenApp 6.5 software, and installs the latest version of the 7.6 LTSR VDA for Windows Server OS.
2. After upgrading the server, add it to machine catalogs and Delivery Groups in the 7.6 Site.

For more information, see [Upgrade a XenApp 6.5 worker to a new VDA for Windows Server OS](#).

## Migrate

Migrating moves data from an earlier deployment to the newest version. You can migrate a XenApp 6.5 or a XenDesktop 4 deployment. Migrating includes installing the latest 7.6 LTSR components and creating a new Site, exporting data from the older farm, and then importing the data to the new Site.

To migrate from XenApp 6.5:

1. Install core components and create a new Site based on the latest 7.6 LTSR.
2. From the XenApp 6.5 Controller, use PowerShell cmdlets to export policy and/or farm data to XML files. You can edit the XML file content to tailor the information you will import.
3. From the new 7.6 Site, use PowerShell cmdlets and the XML files to import policy and/or application data to the new Site.
4. Complete post-migration tasks on the new Site.

For more information, see [Migrate XenApp 6.x](#).

To migrate from XenDesktop 4:

1. Install core components and create a new XenDesktop Site.
2. From the XenDesktop 4 farm, use the export command tool to export farm data to an XML file. You can edit the XML file content to tailor the information you will import.
3. From the 7.6 Site, use the import command tool and the XML file to import the farm data to the new Site.

4. Complete post-migration tasks on the new Site.

For more information, see [Migrate XenDesktop 4](#).

# 安装和升级分析

Mar 22, 2017

When you use the full-product installer to deploy or upgrade XenApp or XenDesktop components, anonymous information about the installation process is gathered and stored on the machine where you are installing/upgrading the component. This data is used to help Citrix improve its customers' installation experiences. For more information, see <http://more.citrix.com/XD-INSTALLER>.

The information is stored locally under %ProgramData%\Citrix\CTQs.

Automatic upload of this data is enabled by default in both the graphical and command line interfaces of the full-product installer.

- You can change the default value in a registry setting. If you change the registry setting before installing/upgrading, that value will be used when you use the full-product installer.
- You can override the default setting if you install/upgrade with the command line interface by specifying an option with the command.

Registry setting that controls automatic upload of install/upgrade analytics (default = 1):

Location: HKLM:\Software\Citrix\MetaInstall

Name: SendExperienceMetrics

Value: 0 = disabled, 1 = enabled

Using PowerShell, the following cmdlet disables automatic upload of install/upgrade analytics:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\MetaInstall -Name SendExperienceMetrics -PropertyType DWORD -  
Value 0
```

To disable automatic uploads with the XenDesktopServerSetup.exe or XenDesktopVDASetup.exe command, include the /disableexperiencemetrics option.

To enable automatic uploads with the XenDesktopServerSetup.exe or XenDesktopVDASetup.exe command, include the /sendexperiencemetrics option.

# 升级部署

May 09, 2017

You can upgrade certain deployments to newer versions without having to first set up new machines or Sites; this is called an in-place upgrade. You can upgrade:

- From XenDesktop version 5.6 (or a later version) to the latest version of 7.6 LTSR
- From XenApp version 7.5 to the latest version of 7.6 LTSR

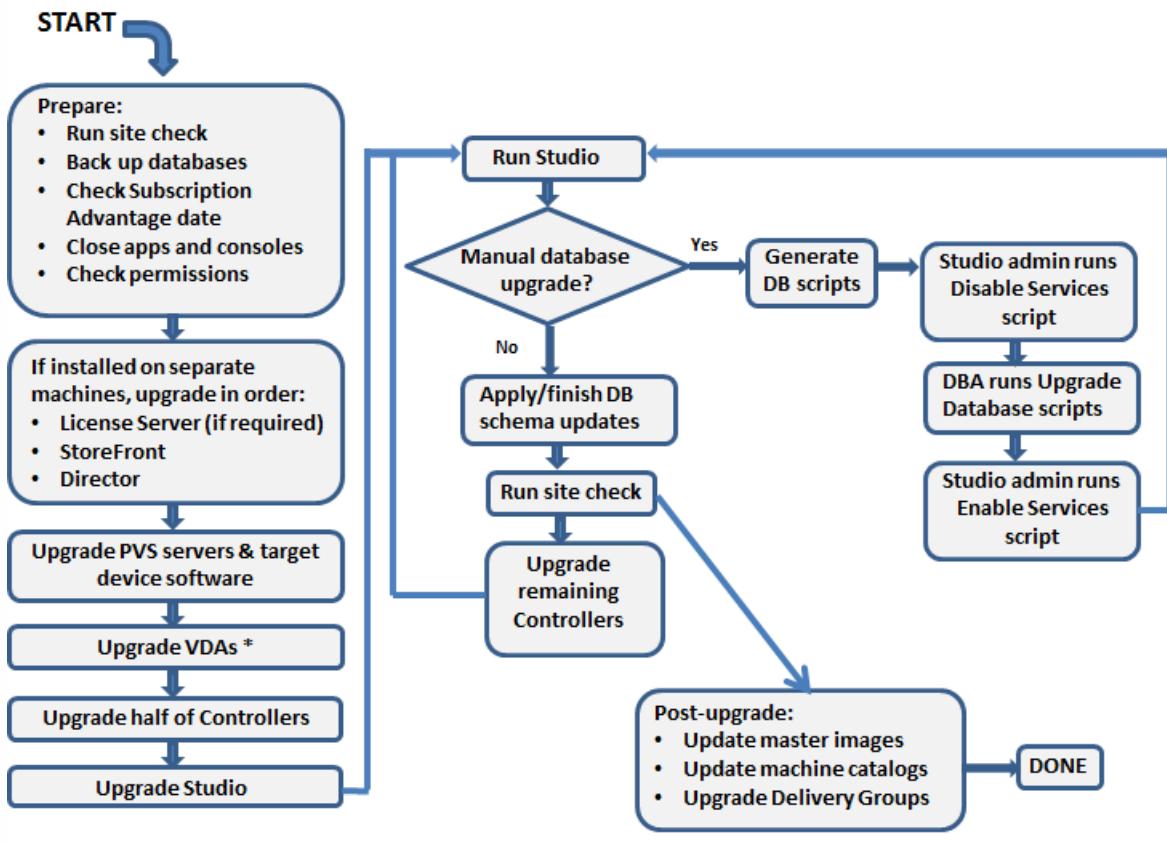
You can also use the latest XenApp 7.6 LTSR installer to upgrade a XenApp 6.5 worker server to the latest XenApp 7.6 LTSR VDA for Windows Server OS. This is a supplementary activity to migrating XenApp 6.5; see [Upgrade a XenApp 6.5 worker to a new VDA for Windows Server OS](#).

To start an upgrade, you run the installer from the new version to upgrade previously installed core components (Delivery Controller, Citrix Studio, Citrix Director, Citrix License Server) and VDAs. The installer determines which components require upgrading and then starts the upgrade at your command. After upgrading the components, you use the newly upgraded Studio to upgrade the Site database and the Site.

Be sure to review all the information in this article before beginning the upgrade.

## Upgrade sequence

The following diagram summarizes the upgrade sequence. Details are provided in *Upgrade procedure* below. For example, if you have more than one core component installed on a server, running the installer on that machine will upgrade all components that have new versions. You might want to upgrade the VDA used in a master image, and then update the image. Then, update the catalog that uses that image and the Delivery Group that uses that catalog. Details also cover how to upgrade the Site databases and the Site automatically or manually.



## Which product component versions can be upgraded

Using the product installer and Studio, you can upgrade:

- Citrix License Server, Studio, and StoreFront
- Delivery Controllers 5.6 or later
- VDA 5.6 or later
  - Unlike earlier VDA releases, you must use the product installer to upgrade VDAs; you cannot use MSIs.
  - If the installer detects Receiver for Windows (Receiver.exe) on the machine, it is upgraded to the Receiver version included on the product installation media.
- Director 1 or later
- Database: This Studio action upgrades the schema and migrates data for the Site database (plus the Configuration Logging and Monitoring databases, if you're upgrading from an earlier 7.x version)

Using the guidance in the feature/product documentation, upgrade the following if needed:

- Provisioning Services (for XenApp 7.x and XenDesktop 7.x, Citrix recommends using the latest released version; the minimum supported version is Provisioning Services 7.0).
  - Upgrade the Provisioning Services server using the server rolling upgrade, and the clients using vDisk versioning.
  - Provisioning Services 7.x does not support creating new desktops with XenDesktop 5 versions. So, although existing desktops will continue to work, you cannot use Provisioning Services 7.x to create new desktops until you upgrade XenDesktop. Therefore, if you plan a mixed environment of XenDesktop 5.6 and 7.x Sites, do not upgrade Provisioning Services to version 7.

- Microsoft System Center Virtual Machine Manager SCVMM. The current product supports SCVMM 2012 and SCVMM 2012 SP1; XenDesktop 5.x supports earlier versions. Use the following upgrade sequence to avoid downtime:
  1. If you have Controllers running versions earlier than XenDesktop 5.6 FP1, upgrade them to XenDesktop 5.6 FP1 (see the XenDesktop documentation for that version).
  2. Upgrade the SCVMM server to SCVMM 2012; see the Microsoft documentation for instructions.
  3. Upgrade XenDesktop components to the current version.
  4. Optionally, upgrade the SCVMM server to SCVMM 2012 SP1.
- StoreFront.

## Limitations

The following limitations apply to upgrades:

### Selective component install

If you install or upgrade any components to the new version but choose not to upgrade other components (on different machines) that require upgrade, Studio will remind you. For example, let's say an upgrade includes new versions of the Controller and Studio. You upgrade the Controller but you do not run the installer on the machine where Studio is installed. Studio will not let you continue to manage the Site until you upgrade Studio.

You do not have to upgrade VDAs, but Citrix recommends upgrading all VDAs to enable you to use all available features. If you do not plan to upgrade all VDAs to the latest version, review Mixed VDA support.

### XenApp version earlier than 7.5

You cannot upgrade from a XenApp version earlier than 7.5. You can migrate from XenApp 6.x; see [Migrate XenApp 6.x](#).

Although you cannot upgrade a XenApp 6.5 farm, you can replace the XenApp 6.5 software on a Windows Server 2008 R2 machine with a current VDA for Server OS. See [Upgrade a XenApp 6.5 worker to a new VDA](#).

### XenDesktop version earlier than 5.6

You cannot upgrade from a XenDesktop version earlier than 5.6.

### XenDesktop Express Edition

You cannot upgrade XenDesktop Express edition. Obtain and install a license for a currently supported edition, and then upgrade it.

### Early Release or Technology Preview versions

You cannot upgrade from a XenApp or XenDesktop Early Release or Technology Preview version.

### Windows XP/Vista

If you have VDAs installed on Windows XP or Windows Vista machines, see [VDAs on machines running Windows XP or Windows Vista](#).

### Product selection

When you upgrade from an earlier 7.x version, you do not choose or specify the product (XenApp or XenDesktop) that was set during the initial installation.

## Mixed environments/sites

If you must continue to run earlier version Sites and current version Sites, see [Mixed environment considerations](#).

# Preparation

Before beginning an upgrade:

### Decide which interface to use

Use the installer's graphical or command-line interface to upgrade core components and VDAs. You cannot import or migrate data from an earlier version.

### Check your Site's health

Ensure the Site is in a stable and functional state before starting an upgrade. If a Site has issues, upgrading will not fix them, and can leave the Site in a complex state that is difficult to recover from. To test the Site, select the **Site** entry in the Studio navigation pane. In the Site configuration portion of the middle pane, click **Test site**.

### Back up the Site, monitoring, and Configuration Logging databases

Follow the instructions in [CTX135207](#). If any issues are discovered after the upgrade, you can restore the backup.

Optionally, back up templates and upgrade hypervisors, if needed.

Complete any other preparation tasks dictated by your business continuity plan.

In a high availability environment, ensure that the Site, monitoring, and Configuration Logging databases are running on the primary database server before starting an upgrade.

### Ensure your Citrix licensing is up to date

Before upgrading the Citrix License Server, be sure your Subscription Advantage date is valid for the new product version. If you are upgrading from an earlier 7.x product version, the date must be at least 2016.0420.

### Close applications and consoles

Before starting an upgrade, close all programs that might potentially cause file locks, including administration consoles and PowerShell sessions. (Restarting the machine ensures that any file locks are cleared, and that there are no Windows updates pending.)

**Important:** Before starting an upgrade, stop and disable any third-party monitoring agent services.

### Ensure you have proper permissions

In addition to being a domain user, you must be a local administrator on the machines where you are upgrading product components.

The Site database and the Site can be upgraded automatically or manually. For an automatic database upgrade, the

Studio user's permissions must include the ability to update the SQL Server database schema (for example, the db\_securityadmin or db\_owner database role). If the Studio user does not have those permissions, initiating a manual database upgrade will generate scripts. The Studio user runs some of the scripts from Studio; the database administrator runs other scripts using a tool such as SQL Server Management Studio.

## Use StoreFront

If your deployment includes Web Interface, Citrix recommends using StoreFront.

# Mixed environment considerations

When your environment contains Sites/farms with different product versions (a mixed environment), Citrix recommends using StoreFront to aggregate applications and desktops from different product versions (for example, if you have a XenDesktop 7.1 Site and a XenDesktop 7.5 Site). For details, see the StoreFront documentation.

- In a mixed environment, continue using the Studio and Director versions for each release, but ensure that different versions are installed on separate machines.
- If you plan to run XenDesktop 5.6 and 7.x Sites simultaneously and use Provisioning Services for both, either deploy a new Provisioning Services for use with the 7.x Site, or upgrade the current Provisioning Services and be unable to provision new workloads in the XenDesktop 5.6 Site.

Within each Site, Citrix recommends upgrading all components. Although you can use earlier versions of some components, all the features in the latest version might not be available. For example, although you can use current VDAs in deployments containing earlier Controller versions, new features in the current release may not be available. VDA registration issues can also occur when using non-current versions.

- Sites with Controllers at version 5.x and VDAs at version 7.x should remain in that state only temporarily. Ideally, you should complete the upgrade of all components as soon as possible.
- Do not upgrade a standalone Studio version until you are ready to use the new version.

# VDAs on machines running Windows XP or Windows Vista

You cannot upgrade VDAs installed on machines running Windows XP or Windows Vista to a 7.x version. You must use VDA 5.6 FP1 with certain hotfixes; see [CTX140941](#) for instructions. Although earlier-version VDAs will run in a 7.x Site, they cannot use many of its features, including:

- Features noted in Studio that require a newer VDA version.
- Configuring App-V applications from Studio.
- Configuring Receiver StoreFront addresses from Studio.
- Automatic support for Microsoft Windows KMS licensing when using Machine Creation Services. See [CTX128580](#).
- Information in Director:
  - Logon times and logon end events impacting the logon duration times in the Dashboard, Trends, and User Detail views.
  - Logon duration breakdown details for HDX connection and authentication time, plus duration details for profile load,

GPO load, logon script, and interactive session establishment.

- Several categories of machine and connection failure rates.
- Activity Manager in the Help Desk and User Details views.

Citrix recommends reimaging Windows XP and Windows Vista machines to a supported operating system version and then installing the latest VDA.

## VDAs on machines running Windows 8.x and Windows 7

To upgrade VDAs installed on machines running Windows 8.x or Windows 7 to Windows 10, Citrix recommends reimaging Windows 7 and Windows 8.x machines to Windows 10 and then installing the supported VDA for Windows 10, using the standalone VDA installation package delivered with XenApp and XenDesktop 7.6 FP3. If reimaging is not an option, uninstall the VDA prior to upgrading the operating system, otherwise the VDA will be in an unsupported state.

## Mixed VDA support

When you upgrade the product to a later version, Citrix recommends you upgrade all the core components and VDAs so you can access all the new and enhanced features in your edition.

In some environments, you may not be able to upgrade all VDAs to the most current version. In this scenario, when you create a machine catalog, you can specify the VDA version installed on the machines. By default, this setting specifies the latest recommended VDA version. Consider changing this setting only if the machine catalog contains machines with earlier VDA versions. Mixing VDA versions in a machine catalog is not recommended.

If a machine catalog is created with the default recommended VDA version setting, and any of the machines in the catalog has an earlier VDA version installed, those machines will not be able to register with the Controller and will not work.

For example, you create a machine catalog with the default VDA setting: "7.6 (recommended, to access the latest features)." You add three machines to that catalog: two with VDA 7.6 and one with VDA 7.1. The VDA 7.1 machine will not register with the Controller. If you cannot upgrade that VDA, consider creating a separate machine catalog configured with a VDA setting of "version 7.0 or later" and adding that machine. Although that machine will not be able to take advantage of new 7.6 features, it will be able to register with the Controller.

## Upgrade procedure

To run the product installer graphical interface, log on to the machine and then insert the media or mount the ISO drive for the new release. Double-click **AutoSelect**. To use the command-line interface, see *Install using the command line*.

**Step 1.** If more than one core component is installed on the same server (for example, the Controller, Studio, and License Server) and several of those components have new versions available, they will all be upgraded when you run the installer on that server.

If any core components are installed on machines other than the Controller, run the installer on each of those machines.

The recommended order is: License Server, StoreFront, and then Director.

**Step 2.** If you use Provisioning Services, upgrade the PVS servers and target devices, using the guidance in the Provisioning Services documentation.

**Step 3.** Run the product installer on machines containing VDAs. (See Step 12 if you use master images and Machine Creation Services.)

When upgrading VDAs from an earlier 7.x version that are installed on physical machines (including Remote PC Access), use the command-line interface with the option /exclude "Personal vDisk","Machine Identity Service". For example:

```
C:\x64\XenDesktop Setup\XenDesktopVdaSetup.exe /exclude "Personal vDisk","Machine Identity Service"
```

**Step 4.** Run the product installer on half of the Controllers. (This also upgrades any other core components installed on those servers.) For example, if your Site has four Controllers, run the installer on two of them.

- Leaving half of the Controllers active allows users to access the Site. VDAs can register with the remaining Controllers. There may be times when the Site has reduced capacity because fewer Controllers are available. The upgrade causes only a brief interruption in establishing new client connections during the final database upgrade steps. The upgraded Controllers cannot process requests until the entire Site is upgraded.
- If your Site has only one Controller, the Site is inoperable during the upgrade.

**Step 5.** If Studio is installed on a different machine than one you've already upgraded, run the installer on the machine where Studio is installed.

**Step 6.** From the newly upgraded Studio, upgrade the Site database. For details, see *Upgrade the databases and the Site* below.

**Step 7.** From the newly upgraded Studio, select **Citrix Studio site-name** in the navigation pane. Select the **Common Tasks** tab. Select **Upgrade remaining Delivery Controllers**.

**Step 8.** After completing the upgrade and confirming completion, close and then reopen Studio.

**Step 9.** In the Site Configuration section of the Common Tasks page, select **Perform registration**. Registering the Controllers makes them available to the Site.

**Step 10.** After you select **Finish** when the upgrade completes, you are offered the opportunity to enroll in the Citrix telemetry programs, which collect information about your deployment. That information is used to improve product quality, reliability, and performance.

**Step 11.** After upgrading components, the database, and the Site, test the newly-upgraded Site. From Studio, select **Citrix Studio site-name** in the navigation pane. Select the **Common Tasks** tab and then select **Test Site**. These tests were run automatically after you upgraded the database, but you can run them again at any time.

**Step 12.** If you use Machine Creation Services and want to use upgraded VDAs: After you upgrade and test the deployment, update the VDA used in the master images (if you haven't done that already). Update master images that use those VDAs. Then update machine catalogs that use those master images, and upgrade Delivery Groups that use those catalogs.

## Upgrade the database and Site

After upgrading the core components and VDAs, use the newly upgraded Studio to initiate an automatic or manual database and Site upgrade.

- For an automatic database upgrade, the Studio user's permissions must include the ability to update the SQL Server database schema (for example, the db\_securityadmin or db\_owner database role).
- If the Studio user does not have those permissions, initiating a manual database upgrade will generate scripts. The Studio user runs some of the scripts from Studio. The database administrator runs other scripts using a tool such as SQL Server Management Studio. If the SQL scripts are run manually, they should be run using either the SQLCMD utility or the SQL Management Studio in SQLCMD mode. Inaccurate errors may result otherwise.

**Important:** Citrix strongly recommends you back up the databases before upgrading, as described in [CTX135207](#).

During a database upgrade, product services are disabled. During that time, Controllers cannot broker new connections for the Site, so plan carefully.

After the database upgrade completes and product services are enabled, Studio tests the environment and configuration, and then generates an HTML report. If problems are identified, you can restore the database backup. After resolving issues, you can upgrade the database again.

### **Upgrade the databases and Site automatically**

Launch the newly upgraded Studio. After you choose to start the Site upgrade automatically and confirm that you are ready, the database and Site upgrade proceeds.

### **Upgrade the databases and Site manually**

This process includes generating and running scripts.

**Step 1.** Launch the newly created Studio. After you choose to manually upgrade the Site, the wizard prompts to confirm that you have backed up the databases. Then, the wizard generates and displays the scripts and a checklist of upgrade steps.

**Step 2.** Run the following scripts in the order shown.

- **DisableServices.ps1:** PowerShell script to be run by the Studio user on a Controller to disable product services.
- **UpgradeSiteDatabase.sql:** SQL script to be run by the database administrator on the server containing the Site database.
- **UpgradeMonitorDatabase.sql:** SQL script to be run by the database administrator on the server containing the Monitor database.
- **UpgradeLoggingDatabase.sql:** SQL script to be run by the database administrator on the server containing the Configuration logging database. Run this script only if this database changes (for example, after applying a hotfix).
- **EnableServices.ps1:** PowerShell script to be run by the Studio user on a Controller to enable product services.

**Step 3.** After completing all the checklist tasks shown in the wizard, click **Finish upgrade**.

# 将 XenApp 6.5 工作进程升级至新的 VDA for Windows Server OS

May 28, 2016

When you run the LTSR installer on a XenApp 6.5 worker server, it:

- Removes the server from the XenApp 6.5 farm (this task automatically invokes the XenApp 6.5 installer's command-line interface)
- Removes the XenApp 6.5 software
- Installs a new (XenApp 7.6 or later supported release) VDA for Windows Server OS

When you use the installer's graphical interface, you are guided through the same wizard that you used when installing VDAs for Windows Server OS in your new XenApp Site. Similarly, the command-line interface uses the same commands and parameters you use to install other VDAs.

You are probably already familiar with using the installer from installing your XenApp 7.6 core components and other VDAs. To review preparatory information, see [VDA installation preparation](#). Then, launch the installer ([Install using the graphical interface](#)) or issue the command ([Install a VDA using the command line](#)) on the XenApp 6.5 worker server.

Good to know:

- This upgrade is valid on XenApp 6.5 servers that are configured in session-host only mode (also called session-only or worker servers).
- Uninstalling XenApp 6.5 requires several server restarts. When using the command-line interface, you can use the /NOREBOOT option to inhibit that automatic action; however, you must restart the server for the uninstallation and subsequent installation to proceed.
- If an error occurs during the XenApp uninstallation process, check the uninstall error log referenced in the error message. Uninstall log files reside in the folder "%TEMP%\Citrix\XenDesktop Installation\XenApp 6.5 Uninstall Log Files\."
- After you upgrade the XenApp 6.5 worker servers, from Studio in the new XenApp Site, create Machine Catalogs (or edit existing catalogs) for the upgraded workers.
- If you migrated policy and application settings from a XenApp 6.5 controller server (see [Migrate XenApp 6.x](#)), assign the Delivery Groups containing the migrated published applications to the machine catalog that hosted those applications in XenApp 6.5.

## Troubleshooting

Symptoms: Removal of the XenApp 6.5 software fails. The uninstall log contains the message: "Error 25703. An error occurred while plugging XML into Internet Information Server. Setup cannot copy files to your IIS Scripts directory. Please make sure that your IIS installation is correct."

- Cause: The issue occurs on systems where (1) during the initial XenApp 6.5 installation, you indicated that the Citrix XML Service (CtxHttp.exe) should not share a port with IIS, and (2) .NET Framework 3.5.1 is installed.
- Resolution:
  1. Remove the Web Server (IIS) role using the Windows Remove Server Roles wizard. (You can reinstall the Web Server (IIS) role later.)
  2. Restart the server.
  3. Using Add/Remove Programs, uninstall the following:
    1. Citrix XenApp 6.5
    2. Microsoft Visual C++ 2005 Redistributable (x64), version 8.0.56336

4. Restart the server.
5. Run the XenApp 7.6 installer to install the VDA for Windows Server OS.

# 迁移 XenApp 6.x

May 28, 2016

Important: Review this entire article before beginning a migration.

The XenApp 6.x Migration Tool (the migration tool) is a collection of PowerShell scripts containing cmdlets that migrate XenApp 6.x (6.0 or 6.5) policy and farm data. On the XenApp 6.x controller server, you run export cmdlets that gather that data into XML files. Then, from the XenApp 7.6 Controller, you run import cmdlets that create objects using the data gathered during the export.

A video overview of the migration tool is available [here](#).

The following sequence summarizes the migration process; details are provided later.

1. On a XenApp 6.0 or 6.5 controller:
  1. Import the PowerShell export modules.
  2. Run the export cmdlets to export policy and/or farm data to XML files.
2. Copy the XML files (and icons folder if you chose not to embed them in the XML files during the export) to the XenApp 7.6 Controller.
3. On the XenApp 7.6 Controller:
  1. Import the PowerShell import modules.
  2. Run the import cmdlets to import policy and/or farm data (applications), using the XML files as input.
4. Complete post-migration steps.

Before you run an actual migration, you can export your XenApp 6.x settings and then perform a preview import on the XenApp 7.6 site. The preview identifies possible failure points so you can resolve issues before running the actual import. For example, a preview might detect that an application with the same name already exists in the new XenApp 7.6 site. You can also use the log files generated from the preview as a migration guide.

Unless otherwise noted, the term 6.x refers to XenApp 6.0 or 6.5.

## New in this release

This December 2014 release (version 20141125) contains the following updates:

- If you encounter issues using the migration tool on a XenApp 6.x farm, report them to the support forum <http://discussions.citrix.com/forum/1411-xenapp-7x/>, so that Citrix can investigate them for potential improvements to the tool.
- New packaging - the XAMigration.zip file now contains two separate, independent packages: ReadIMA.zip and ImportFMA.zip. To export from a XenApp 6.x server, you need only ReadIMA.zip. To import to a XenApp 7.6 server, you

need only ImportFMA.zip.

- The Export-XAFarm cmdlet supports a new parameter (EmbedIconData) that eliminates the need to copy icon data to separate files.
- The Import-XAFarm cmdlet supports three new parameters:
  - MatchServer - import applications from servers whose names match an expression
  - NotMatchServer - import applications from servers whose names do not match an expression
  - IncludeDisabledApps - import disabled applications
- Prelaunched applications are not imported.
- The Export-Policy cmdlet works on XenDesktop 7.x.

## Migration Tool package

The migration tool is available under the XenApp 7.6 Citrix [download site](#). The XAMigration.zip file contains two separate, independent packages:

- ReadIMA.zip - contains the files used to export data from your XenApp 6.x farm, plus shared modules.

Module or file	Description
ExportPolicy.psm1	PowerShell script module for exporting XenApp 6.x policies to an XML file.
ExportXAFarm.psm1	PowerShell script module for exporting XenApp 6.x farm settings to an XML file.
ExportPolicy.psd1	PowerShell manifest file for script module ExportPolicy.psm1.
ExportXAFarm.psd1	PowerShell manifest file for script module ExportXAFarm.psm1.
LogUtilities.psm1	Shared PowerShell script module that contains logging functions.
XmlUtilities.psd1	PowerShell manifest file for script module XmlUtilities.psm1.
XmlUtilities.psm1	Shared PowerShell script module that contains XML functions.

- ImportFMA.zip - contains the files used to import data to your XenApp 7.6 farm, plus shared modules.

Module or file	Description
ImportPolicy.psm1	PowerShell script module for importing policies to XenApp 7.6.
ImportXAFarm.psm1	PowerShell script module for importing applications to XenApp 7.6
ImportPolicy.psd1	PowerShell manifest file for script module ImportPolicy.psm1.
ImportXAFarm.psd1	PowerShell manifest file for script module ImportXAFarm.psm1.
PolicyData.xsd	XML schema for policy data.
XAFarmData.xsd	XML schema for XenApp farm data.
LogUtilities.psm1	Shared PowerShell script module that contains logging functions.
XmlUtilities.psd1	PowerShell manifest file for script module XmlUtilities.psm1.

## Module profile

## Description

Shared PowerShell script module that contains XML functions.

## Limitations

- Not all policies settings are imported; see [Policy settings not imported](#). Settings that are not supported are ignored and noted in the log file.
- While all application details are collected in the output XML file during the export operation, only server-installed applications are imported into the XenApp 7.6 site. Published desktops, content, and most streamed applications are not supported (see the Import-XAFarm cmdlet parameters in [Step-by-step: import data](#) for exceptions).
- Application servers are not imported.
- Many application properties are not imported because of differences between the XenApp 6.x Independent Management Architecture (IMA) and the XenApp 7.6 FlexCast Management Architecture (FMA) technologies; see [Application property mapping](#).
- A Delivery Group is created during the import. See [Advanced use](#) for details about using parameters to filter what is imported.
- Only Citrix policy settings created with the AppCenter management console are imported; Citrix policy settings created with Windows Group Policy Objects (GPOs) are not imported.
- The migration scripts are intended for migrations from XenApp 6.x to XenApp 7.6 only.
- Nested folders greater than five levels deep are not supported by Studio and will not be imported. If your application folder structure includes folders more than five levels deep, consider reducing the number of nested folder levels before importing.

## Security considerations

The XML files created by the export scripts can contain sensitive information about your environment and organization, such as user names, server names, and other XenApp farm, application, and policy configuration data. Store and handle these files in secure environments.

Carefully review the XML files before using them as input when importing policies and applications, to ensure they contain no unauthorized modifications.

Policy object assignments (previously known as policy filters) control how policies are applied. After importing the policies, carefully review the object assignments for each policy to ensure that there are no security vulnerabilities resulting from the import. Different sets of users, IP addresses, or client names may be applied to the policy after the import. The allow/deny settings may have different meanings after the import.

## Logging and error handling

The scripts provide extensive logging that tracks all cmdlet executions, informative messages, cmdlet execution results, warnings, and errors.

- Most Citrix PowerShell cmdlet use is logged. All PowerShell cmdlets in the import scripts that create new site objects are logged.
- Script execution progress is logged, including the objects being processed.
- Major actions that affect the state of the flow are logged, including flows directed from the command line.
- All messages printed to the console are logged, including warnings and errors.
- Each line is time-stamped to the millisecond.

Citrix recommends specifying a log file when you run each of the export and import cmdlets.

If you do not specify a log file name, the log file is stored in the current user's home folder (specified in the PowerShell \$HOME variable) if that folder exists; otherwise, it is placed in the script's current execution folder. The default log name is "XFarmYYYYMMDDHHmmSS-xxxxxx" where the last six digits constitute a random number.

By default, all progress information is displayed. To suppress the display, specify the NoDetails parameter in the export and import cmdlet.

Generally, a script stops execution when an error is encountered, and you can run the cmdlet again after clearing the error conditions.

Conditions that are not considered errors are logged; many are reported as warnings, and script execution continues. For example, unsupported application types are reported as warnings and are not imported. Applications that already exist in the XenApp 7.6 site are not imported. Policy settings that are deprecated in XenApp 7.6 are not imported.

The migration scripts use many PowerShell cmdlets, and all possible errors might not be logged. For additional logging coverage, use the PowerShell logging features. For example, PowerShell transcripts log everything that is printed to the screen. For more information, see the help for the Start-Transcript and Stop-Transcript cmdlets.

## Requirements, preparation, and best practices

**Important:** Remember to review this entire article before beginning a migration.

You should understand basic PowerShell concepts about execution policy, modules, cmdlets, and scripts. Although extensive scripting expertise is not required, you should understand the cmdlets you execute. Use the Get-Help cmdlet to review each migration cmdlet's help before executing it. For example:

```
Get-Help -full Import-XAFarm
```

Specify a log file on the command line and always review the log file after running a cmdlet. If a script fails, check and fix the error identified in the log file and then run the cmdlet again.

### Good to know:

- To facilitate application delivery while two deployments are running (the XenApp 6.x farm and the new XenApp 7.6 site), you can aggregate both deployments in StoreFront or Web Interface. See the eDocs documentation for your StoreFront or Web Interface release (Manage > Create a store).
- Application icon data is handled in one of two ways:
  - If you specify the EmbedIconData parameter in the Export-XAFarm cmdlet, exported application icon data is embedded in the output XML file.
  - If you do not specify the EmbedIconData parameter in the Export-XAFarm cmdlet, exported application icon data is stored under a folder named by appending the string "-icons" to the base name of the output XML file. For example, if the XmlOutputFile parameter is "FarmData.xml" then the folder "FarmData-icons" is created to store the application icons.

The icon data files in this folder are .txt files that are named using the browser name of the published application (although the files are .txt files, the stored data is encoded binary icon data, which can be read by the import script to re-create the application icon). During the import operation, if the icon folder is not found in the same location as the import XML file, generic icons are used for each imported application.

- The names of the script modules, manifest files, shared module, and cmdlets are similar. Use tab completion with care to avoid errors. For example, Export-XAFarm is a cmdlet. ExportXAfarm.psd1 and ExportXAfarm.psm1 are files that cannot be executed.
- In the step-by-step sections below, most <string> parameter values show surrounding quotation marks. These are optional for single-word strings.

### **For exporting from the XenApp 6.x server:**

- The export must be run on a XenApp 6.x server configured with the controller and session-host (commonly known as controller) server mode.
- To run the export cmdlets, you must be a XenApp administrator with permission to read objects. You must also have sufficient Windows permission to run PowerShell scripts; the step-by-step procedures below contain instructions.
- Ensure the XenApp 6.x farm is in a healthy state before beginning an export. Back up the farm database. Verify the farm's integrity using the Citrix IMA Helper utility ([CTX133983](#)): from the IMA Datastore tab, run a Master Check (and then use the DSCheck option to resolve invalid entries). Repairing issues before the migration helps prevent export failures. For example, if a server was removed improperly from the farm, its data might remain in the database; that could cause cmdlets in the export script to fail (for example, Get-XAServer -ZoneName). If the cmdlets fail, the script fails.
- You can run the export cmdlets on a live farm that has active user connections; the export scripts read only the static farm configuration and policy data.

### **For importing to the XenApp 7.6 server:**

- You can import data to XenApp 7.6 deployments (and later supported versions). You must install a XenApp 7.6 Controller and Studio, and create a site before importing the data you exported from the XenApp 6.x farm. Although VDAs are not required to import settings, they allow application file types to be made available.
- To run the import cmdlets, you must be a XenApp administrator with permission to read and create objects. A Full Administrator has these permissions. You must also have sufficient Windows permission to run PowerShell scripts; the step-by-step procedures below contain instructions.
- No other user connections should be active during an import. The import scripts create many new objects, and disruptions may occur if other users are changing the configuration at the same time.

Remember that you can export data and then use the -Preview parameter with the import cmdlets to see what would happen during an actual import, but without actually importing anything. The logs will indicate exactly what would happen during an actual import; if errors occur, you can resolve them before starting an actual import.

### **Step-by-step: export data**

A video of an export walk-through is available [here](#).

Complete the following steps to export data from a XenApp 6.x controller to XML files.

1. Download the XAMigration.zip migration tool package from the Citrix download site. For convenience, place it on a network file share that can be accessed by both the XenApp 6.x farm and the XenApp 7.6 site. Unzip XAMigration.zip on the network file share. There should be two zip files: ReadIMA.zip and ImportFMA.zip.
2. Log on to the XenApp 6.x controller as a XenApp administrator with at least read-only permission and Windows permission to run PowerShell scripts.
3. Copy ReadIMA.zip from the network file share to the XenApp 6.x controller. Unzip and extract ReadIMA.zip on the controller to a folder (for example: C:\XAMigration).
4. Open a PowerShell console and set the current directory to the script location. For example:  
`cd C:\XAMigration`
5. Check the script execution policy by running `Get-ExecutionPolicy`.
6. Set the script execution policy to at least RemoteSigned to allow the scripts to be executed. For example:  
`Set-ExecutionPolicy RemoteSigned`
7. Import the module definition files ExportPolicy.psd1 and ExportXAFarm.psd1:  
`Import-Module .\ExportPolicy.psd1`  
`Import-Module .\ExportXAFarm.psd1`

**Good to know:**

- If you intend to export only policy data, you can import only the ExportPolicy.psd1 module definition file. Similarly, if you intend to export only farm data, import only ExportXAFarm.psd1.
- Importing the module definition files also adds the required PowerShell snap-ins.
- Do not import the .psm1 script files.

8. To export policy data, run the Export-Policy cmdlet.

Parameter	Description
-XmlOutputFile "<string>.xml"	XML output file name; this file will hold the exported data. Must have an .xml extension. The file must not exist, but if a path is specified, the parent path must exist.  Default: None; this parameter is required.
-LogFile "<string>"	Log file name. An extension is optional. The file is created if it does not exist. If the file exists and the NoClobber parameter is also specified, an error is generated; otherwise, the file's content is overwritten.  Default: See <a href="#">Logging and error handling</a>
-NoLog	Do not generate log output. This overrides the LogFile parameter if it is also specified.  Default: False; log output is generated
-NoClobber	Do not overwrite an existing log file specified in the LogFile parameter. If the log file does not exist, this parameter has no effect.  Default: False; an existing log file is overwritten
-NoDetails	Do not send detailed reports about script execution to the console.  Default: False; detailed reports are sent to the console
-SuppressLogo	Do not print the message "XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#" to the console. This message, which identifies the script version, can be helpful during troubleshooting; therefore, Citrix recommends omitting this parameter.  Default: False; the message is printed to the console

Example: The following cmdlet exports policy information to the XML file named MyPolicies.xml. The operation is logged to the file named MyPolicies.log.

```
Export-Policy -XmlOutputFile ".\MyPolicies.XML"
-LogFile ".\MyPolicies.Log"
```

9. To export farm data, run the Export-XAFarm cmdlet, specifying a log file and an XML file.

Parameter	Description

<b>Parameter</b> -XmlOutputFile "<string>.xml"	<b>Description</b> XML output file name; this file will hold the exported data. Must have an .xml extension. The file must not exist, but if a path is specified, the parent path must exist.  Default: None; this parameter is required.
-LogFile " <string>"	Log file name. An extension is optional. The file is created if it does not exist. If the file exists and the NoClobber parameter is also specified, an error is generated; otherwise, the file's content is overwritten.  Default: See <a href="#">Logging and error handling</a>
-NoLog	Do not generate log output. This overrides the LogFile parameter if it is also specified.  Default: False; log output is generated
-NoClobber	Do not overwrite an existing log file specified in the LogFile parameter. If the log file does not exist, this parameter has no effect.  Default: False; an existing log file is overwritten
-NoDetails	Do not send detailed reports about script execution to the console.  Default: False; detailed reports are sent to the console
-SuppressLogo	Do not print the message "XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#" to the console. This message, which identifies the script version, can be helpful during troubleshooting; therefore, Citrix recommends omitting this parameter.  Default: False; the message is printed to the console
-IgnoreAdmins	Do not export administrator information. See <a href="#">Advanced use</a> for how-to-use information.  Default: False; administrator information is exported
-IgnoreApps	Do not export application information. See <a href="#">Advanced use</a> for how-to-use information.  Default: False; application information is exported
-IgnoreServers	Do not export server information.  Default: False; server information is exported
-IgnoreZones	Do not export zone information.  Default: False; zone information is exported.

<b>Parameter</b>	<b>Description</b>
-IgnoreOthers <integer>	<p>Do not export information such as configuration logging, load evaluators, load balancing policies, printer drivers, and worker groups.</p> <p>Default: False; other information is exported</p> <p>Note: The purpose of the -IgnoreOthers switch is to allow you to proceed with an export when an error exists that would not affect the actual data being used for the exporting or importing process.</p>
-AppLimit <integer>	<p>Number of applications to be exported. See <a href="#">Advanced use</a> for how-to-use information.</p> <p>Default: All applications are exported</p>
-EmbedIconData	<p>Embed application icon data in the same XML file as the other objects.</p> <p>Default: Icons are stored separately. See <a href="#">Requirements, preparation, and best practices</a> for details</p>
-SkipApps <integer>	<p>Number of applications to skip. See <a href="#">Advanced use</a> for how-to-use information.</p> <p>Default: No applications are skipped</p>

Example: The following cmdlet exports farm information to the XML file named MyFarm.xml. The operation is logged to the file MyFarm.log. A folder named "MyFarm-icons" is created to store the application icon data files; this folder is at the same location as MyFarm.XML.

```
Export-XAFarm -XmlOutputFile ".\MyFarm.XML"
-LogFile ".\MyFarm.Log"
```

After the export scripts complete, the XML files specified on the command lines contain the policy and XenApp farm data. The application icon files contain icon data files, and the log file indicate what occurred during the export.

### Step-by-step: import data

A video of an import walk-through is available [here](#).

Remember that you can run a preview import (by issuing the Import-Policy or Import-XAFarm cmdlet with the Preview parameter) and review the log files before performing an actual import.

Complete the following steps to import data to a XenApp 7.6 site, using the XML files generating from the export.

1. Log on to the XenApp 7.6 controller as an administrator with read-write permission and Windows permission to run PowerShell scripts.
  2. If you have not unzipped the migration tool package XAMigration on the network file share, do so now. Copy ImportFMA.zip from the network file share to the XenApp 7.6 Controller. Unzip and extract ImportFMA.zip on the Controller to a folder (for example: C:\XAMigration).
  3. Copy the XML files (the output files generated during the export) from the XenApp 6.x controller to the same location on the XenApp 7.6 Controller where you extracted the ImportFMA.zip files.
- If you chose not to embed the application icon data in the XML output file when you ran the Export-XAFarm cmdlet, be

sure to copy the icon data folder and files to the same location on the XenApp 7.6 controller as the output XML file containing the application data and the extracted ImportFMA.zip files.

4. Open a PowerShell console and set the current directory to the script location.  
cd C:\XAMigration
5. Check the script execution policy by running Get-ExecutionPolicy.
6. Set the script execution policy to at least RemoteSigned to allow the scripts to be executed. For example:  
Set-ExecutionPolicy RemoteSigned
7. Import the PowerShell module definition files ImportPolicy.psd1 and ImportXAfarm.psd1:  
Import-Module .\ImportPolicy.psd1  
  
Import-Module .\ImportXAfarm.psd1

**Good to know:**

- If you intend to import only policy data, you can import only the ImportPolicy.psd1 module definition file. Similarly, if you intend to import only farm data, import only ImportXAfarm.psd1.
- Importing the module definition files also adds the required PowerShell snap-ins.
- Do not import the .psm1 script files.

8. To import policy data, run the Import-Policy cmdlet, specifying the XML file containing the exported policy data.

Parameter	Description
-XmlInputFile "<string>.xml"	XML input file name; this file contains data collected from running the Export-Policy cmdlet. Must have an .xml extension.  Default: None; this parameter is required.
-XsdFile "<string>"	XSD file name. The import scripts use this file to validate the syntax of the XML input file. See <a href="#">Advanced use</a> for how-to-use information.  Default: PolicyData.XSD
-LogFile "<string>"	Log file name. If you copied the export log files to this server, consider using a different log file name with the import cmdlet.  Default: See <a href="#">Logging and error handling</a>
-NoLog	Do not generate log output. This overrides the LogFile parameter, if it is also specified.  Default: False; log output is generated
-NoClobber	Do not overwrite an existing log file specified in the LogFile parameter. If the log file does not exist, this parameter has no effect.  Default: False; an existing log file is overwritten
-NoDetails	Do not send detailed reports about script execution to the console.

Parameter	Description
-SuppressLogo	<p>Do not print the message "XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#" to the console. This message, which identifies the script version, can be helpful during troubleshooting; therefore, Citrix recommends omitting this parameter.</p> <p>Default: False; the message is printed to the console</p>
-Preview	<p>Perform a preview import: read data from the XML input file, but do not import objects to the site. The log file and console indicate what occurred during the preview import. A preview shows administrators what would happen during a real import.</p> <p>Default: False; a real import occurs</p>

Example: The following cmdlet imports policy data from the XML file named MyPolicies.xml. The operation is logged to the file named MyPolicies.log.

```
Import-Policy -XmlInputFile ".\MyPolicies.XML"
-LogFile ".\MyPolicies.Log"
```

9. To import applications, run the Import-XAFarm cmdlet, specifying a log file and the XML file containing the exported farm data.

Parameter	Description
-XmlInputFile "<string>.xml"	<p>XML input file name; this file contains data collected from running the Export-XAFarm cmdlet. Must have an .xml extension.</p> <p>Default: None; this parameter is required.</p>
-XsdFile "<string>"	<p>XSD file name. The import scripts use this file to validate the syntax of the XML input file. See <a href="#">Advanced use</a> for how-to-use information.</p> <p>Default: XAFarmData.XSD</p>
-LogFile "<string>"	<p>Log file name. If you copied the export log files to this server, consider using a different log file name with the import cmdlet.</p> <p>Default: See <a href="#">Logging and error handling</a></p>
-NoLog	<p>Do not generate log output. This overrides the LogFile parameter, if it is also specified.</p> <p>Default: False; log output is generated</p>
-NoClobber	<p>Do not overwrite an existing log file specified in the LogFile parameter. If the log file does not exist, this parameter has no effect.</p> <p>Default: False; an existing log file is overwritten</p>

<b>Parameter</b> -NoDetails	<b>Description</b> Do not send detailed reports about script execution to the console.  Default: False; detailed reports are sent to the console
-SuppressLogo	Do not print the message "XenApp 6.x to XenApp/XenDesktop 7.6 Migration Tool Version #yyyyMMdd-hhmm#" to the console. This message, which identifies the script version, can be helpful during troubleshooting; therefore, Citrix recommends omitting this parameter.  Default: False; the message is printed to the console
-Preview	Perform a preview import: read data from the XML input file, but do not import objects to the site. The log file and console indicate what occurred during the preview import. A preview shows administrators what would happen during a real import.  Default: False; a real import occurs
-DeliveryGroupName "<string>"	Delivery Group name for all imported applications. See <a href="#">Advanced use</a> for how-to-use information.  Default: "<xenapp-farm-name> - Delivery Group"
-MatchFolder "<string>"	Import only those applications in folders with names that match the string. See <a href="#">Advanced use</a> for how-to-use information.  Default: No matching occurs
-NotMatchFolder "<string>"	Import only those applications in folders with names that do not match the string. See <a href="#">Advanced use</a> for how-to-use information.  Default: No matching occurs
-MatchServer "<string>"	Import only those applications from servers whose names match the string. See <a href="#">Advanced use</a> for how-to-use information.
-NotMatchServer "<string>"	Import only those applications from servers whose names do not match the string. See <a href="#">Advanced use</a> for how-to-use information.  Default: No matching occurs
-MatchWorkerGroup "<string>"	Import only those applications published to worker groups with names that match the string. See <a href="#">Advanced use</a> for how-to-use information.  Default: No matching occurs

<b>Parameter</b>	<b>Description</b>
NotMatchWorkerGroup "<string>"	Import only those applications published to worker groups with names that do not match the string. See <a href="#">Advanced use</a> for how-to-use information.  Default: No matching occurs
-MatchAccount " <string>"	Import only those applications published to user accounts with names that match the string. See <a href="#">Advanced use</a> for how-to-use information.  Default: No matching occurs
-NotMatchAccount " <string>"	Import only those applications published to user accounts with names that do not match the string. See <a href="#">Advanced use</a> for how-to-use information.  Default: No matching occurs
-IncludeStreamedApps	Import applications of type "StreamedToClientOrServerInstalled". (No other streamed applications are imported.)  Default: Streamed applications are not imported
-IncludeDisabledApps	Import applications that have been marked as disabled.  Default: Disabled applications are not imported

Example: The following cmdlet imports applications from the XML file named MyFarm.xml. The operation is logged to the file named MyFarm.log.

```
Import-XAFarm -XmlInputFile ".\MyFarm.XML"
-LogFile ".\MyFarm.Log"
```

## 10. After the import completes successfully, complete the post-migration tasks.

### Post-migration tasks

After successfully importing XenApp 6.x policies and farm settings into a XenApp 7.6 site, use the following guidance to ensure that the data has been imported correctly.

- **Policies and policy settings**

Importing policies is essentially a copy operation, with the exception of deprecated settings and policies, which are not imported. The post-migration check essentially involves comparing the two sides.

1. The log file lists all the policies and settings imported and ignored. First, review the log file and identify which settings and policies were not imported.
2. Compare the XenApp 6.x policies with the policies imported to XenApp 7.6. The values of the settings should remain the same (except for deprecated policy settings, as noted in the next step).
  - If you have a small number of policies, you can perform a side-by-side visual comparison of the policies displayed in the XenApp 6.x AppCenter and the policies displayed in the XenApp 7.6 Studio.
  - If you have a large number of policies, a visual comparison might not be feasible. In such cases, use the policy export cmdlet (Export-Policy) to export the XenApp 7.6 policies to a different XML file, and then use a text diff

tool (such as windiff) to compare that file's data to the data in the XML file used during the policy export from XenApp 6.x.

3. Use the information in the [Policy settings not imported](#) section to determine what might have changed during the import. If a XenApp 6.x policy contains only deprecated settings, as a whole policy, it is not imported. For example, if a XenApp 6.x policy contains only HMR test settings, that policy is completely ignored because there is no equivalent setting supported in XenApp 7.6.

Some XenApp 6.x policy settings are no longer supported, but the equivalent functionality is implemented in XenApp 7.6. For example, in XenApp 7.6, you can configure a restart schedule for Server OS machines by editing a Delivery Group; this functionality was previously implemented through policy settings.

4. Review and confirm how filters will apply to your XenApp 7.6 site versus their use in XenApp 6.x; significant differences between the XenApp 6.x farm and the XenApp 7.6 site could change the effect of filters.

- **Filters**

Carefully examine the filters for each policy. Changes may be required to ensure they still work in XenApp 7.6 as originally intended in XenApp 6.x.

Filter	Considerations
Access Control	Access Control Should contain the same values as the original XenApp 6.x filters and should work without requiring changes.
Citrix CloudBridge	A simple Boolean; should work without requiring changes.
Client IP Address	Lists client IP address ranges; each range is either allowed or denied. The import script preserves the values, but they may require changes if different clients connect to the XenApp 7.6 VDA machines.
Client Name	Similar to the Client IP Address filter, the import script preserves the values, but they may require changes if different clients connect to the XenApp 7.6 VDA machines.
Organizational Unit	Values might be preserved, depending on whether or not the OUs can be resolved at the time they are imported. Review this filter closely, particularly if the XenApp 6.x and XenApp 7.6 machines reside in different domains. If you do not configure the filter values correctly, the policy may be applied to an incorrect set of OUs.  The OUs are represented by names only, so there is a small chance that an OU name will be resolved to an OU containing different members from the OUs in the XenApp 6.x domain. Even if some of the values of the OU filter are preserved, you should carefully review the values.
User or Group	Values might be preserved, depending on whether or not the accounts can be resolved at the time they are imported.  Similar to OUs, the accounts are resolved using names only, so if the XenApp 7.6 site has a domain with the same domain and user names, but are actually two different domains and users, the resolved accounts could be different from the XenApp 6.x domain users. If you do not properly

Filter	review and modify the filter values, incorrect policy applications can occur. <b>Considerations</b>
Worker Group	<p>Worker groups are not supported in XenApp 7.6. Consider using the Delivery Group, Delivery Group Type, and Tag filters, which are supported in XenApp 7.6 (not in XenApp 6.x).</p> <ul style="list-style-type: none"> <li>• Delivery Group: Allows policies to be applied based on Delivery Groups. Each filter entry specifies a Delivery Group and can be allowed or denied.</li> <li>• Delivery Group Type: Allows policies to be applied based on the Delivery Group types. Each filter specifies a Delivery Group type that can be allowed or denied.</li> <li>• Tag: Specifies policy application based on tags created for the VDA machines. Each tag can be allowed or denied.</li> </ul>

To recap, filters that involve domain user changes require the most attention if the XenApp 6.x farm and the XenApp 7.6 site are in different domains. Because the import script uses only strings of domain and user names to resolve users in the new domain, some of the accounts might be resolved and others might not. While there is only a small chance that different domains and users have the same name, you should carefully review these filters to ensure they contain correct values.

#### • Applications

The application importing scripts do not just import applications; they also create objects such as Delivery Groups. If the application import involves multiple iterations, the original application folder hierarchies can change significantly.

1. First, read the migration log files that contain details about which applications were imported, which applications were ignored, and the cmdlets that were used to create the applications.
2. For each application:
  - Visually check to ensure the basic properties were preserved during the import. Use the information in the [Application property mapping](#) section to determine which properties were imported without change, not imported, or initialized using the XenApp 6.x application data.
  - Check the user list. The import script automatically imports the explicit list of users into the application's limit visibility list in XenApp 7.6. Check to ensure that the list remains the same.
3. Application servers are not imported. This means that none of the imported applications can be accessed yet. The Delivery Groups that contain these applications must be assigned machine catalogs that contain the machines that have the published applications' executable images. For each application:
  - Ensure that the executable name and the working directory point to an executable that exists in the machines assigned to the Delivery Group (through the machine catalogs).
  - Check a command line parameter (which may be anything, such as file name, environment variable, or executable name). Verify that the parameter is valid for all the machines in the machine catalogs assigned to the Delivery Group.

#### • Log files

The log files are the most important reference resources for an import and export. This is why existing log files are not overwritten by default, and default log file names are unique.

As noted in the “Logging and error handling” section, if you chose to use additional logging coverage with the PowerShell Start-Transcript and Stop-Transcript cmdlets (which record everything typed and printed to the console), that output, together with the log file, provides a complete reference of import and export activity.

Using the time stamps in the log files, you can diagnose certain problems. For example, if an export or import ran for a very long time, you could determine if a faulty database connection or resolving user accounts took most of the time.

The commands recorded in the log files also tell you how some objects are read or created. For example, to create a Delivery Group, several commands are executed to not only create the Delivery Group object itself, but also other objects such as access policy rules that allow application objects to be assigned to the Delivery Group.

The log file can also be used to diagnose a failed export or import. Typically, the last lines of the log file indicate what caused the failure; the failure error message is also saved in the log file. Together with the XML file, the log file can be used to determine which object was involved in the failure.

After reviewing and testing the migration, you can:

1. Upgrade your XenApp 6.5 worker servers to current Virtual Delivery Agents (VDAs) by running the 7.6 installer on the server, which removes the XenApp 6.5 software and then automatically installs a current VDA. See [Upgrade a XenApp 6.5 worker to a new VDA for Windows Server OS](#) for instructions.

For XenApp 6.0 worker servers, you must manually uninstall the XenApp 6.0 software from the server. You can then use the 7.6 installer to install the current VDA. You cannot use the 7.6 installer to automatically remove the XenApp 6.0 software.

2. From Studio in the new XenApp site, create machine catalogs (or edit existing catalogs) for the upgraded workers.
3. Add the upgraded machines from the machine catalog to the Delivery Groups that contain the applications installed on those VDAs for Windows Server OS.

## Advanced use

By default, the Export-Policy cmdlet exports all policy data to an XML file. Similarly, Export-XAFarm exports all farm data to an XML file. You can use command line parameters to more finely control what is exported and imported.

- **Export applications partially** - If you have a large number of applications and want to control how many are exported to the XML file, use the following parameters:
  - AppLimit - Specifies the number of applications to export.
  - SkipApps - Specifies the number of applications to skip before exporting subsequent applications.

You can use both of these parameters to export large quantities of applications in manageable chunks. For example, the first time you run Export-XAFarm, you want to export only the first 200 applications, so you specify that value in the AppLimit parameter.

```
Export-XAFarm -XmlOutputFile "Apps1-200.xml"  
-AppLimit "200"
```

The next time you run Export-XAFarm, you want to export the next 100 applications, so you use the SkipApps parameter to disregard the applications you've already exported (the first 200), and the AppLimit parameter to export the next 100 applications.

```
Export-XAFarm -XmlOutputFile "Apps201-300.xml"  
-AppLimit "100" -SkipApps "200"
```

- **Do not export certain objects** - Some objects can be ignored and thus do not need to be exported, particularly those objects that are not imported; see [Policy settings not imported](#) and [Application property mapping](#). Use the following parameters to prevent exporting unneeded objects:

- IgnoreAdmins - Do not export administrator objects
- IgnoreServers - Do not export server objects
- IgnoreZones - Do not export zone objects
- IgnoreOthers - Do not export configuration logging, load evaluator, load balancing policy, printer driver, and worker group objects
- IgnoreApps - Do not export applications; this allows you to export other data to an XML output file and then run the export again to export applications to a different XML output file.

You can also use these parameters to work around issues that could cause the export to fail. For example, if you have a bad server in a zone, the zone export might fail; if you include the IgnoreZones parameter, the export continues with other objects.

- **Delivery Group names** - If you do not want to put all of your applications into one Delivery Group (for example, because they are accessed by different sets of users and published to different sets of servers), you can run Import-XAFarm multiple times, specifying different applications and a different Delivery Group each time. Although you can use PowerShell cmdlets to move applications from one Delivery Group to another after the migration, importing selectively to unique Delivery Groups can reduce or eliminate the effort of moving the applications later.

1. Use the DeliveryGroupName parameter with the Import-XAFarm cmdlet. The script creates the specified Delivery Group if it doesn't exist.
2. Use the following parameters with regular expressions to filter the applications to be imported into the Delivery Group, based on folder, worker group, user account, and/or server names. Enclosing the regular expression in single or double quotation marks is recommended. For information about regular expressions, see [http://msdn.microsoft.com/en-us/library/hs600312\(v=vs.110\).aspx](http://msdn.microsoft.com/en-us/library/hs600312(v=vs.110).aspx).

- MatchWorkerGroup and NotMatchWorkerGroup - For example, for applications published to worker groups, the following cmdlet imports applications in the worker group named "Productivity Apps" to a XenApp 7.6 Delivery Group of the same name:

```
Import-XAFarm –XmlInputFile XAFarm.xml –LogFile XAFarmImport.log  
–MatchWorkerGroup 'Productivity Apps' –DeliveryGroupName 'Productivity Apps'
```

- MatchFolder and NotMatchFolder - For example, for applications organized in application folders, the following cmdlet imports applications in the folder named "Productivity Apps" to a XenApp 7.6 Delivery Group of the same name.

```
Import-XAFarm –XmlInputFile XAFarm.xml –LogFile XAFarmImport.log  
–MatchFolder 'Productivity Apps' –DeliveryGroupName 'Productivity Apps'
```

For example, the following cmdlet imports applications in any folder whose name contains "MS Office Apps" to the default Delivery Group.

```
Import-XAFarm -XmlInputFile .\TheFarmApps.XML -MatchFolder ".*/MS Office Apps/*"
```

- MatchAccount and NotMatchAccount - For example, for applications published to Active Directory users or user groups, the following cmdlet imports applications published to the user group named "Finance Group" to a XenApp 7.6 Delivery Group named "Finance."

```
Import-XAFarm –XmlInputFile XAFarm.xml –LogFile XAFarmImport.log  
–MatchAccount 'DOMAIN\\Finance Group' –DeliveryGroupName 'Finance'
```

- MatchServer and NotMatchServer - For example, for applications organized on servers, the following cmdlet imports applications associated with the server not named "Current" to a XenApp Delivery Group named "Legacy."

```
Import-XAFarm -XmlInputFile XAFarm.xml -LogFile XAFarmImport.log  
-NotMatchServer 'Current' -DeliveryGroupName 'Legacy'
```

- **Customization** - PowerShell programmers can create their own tools. For example, you can use the export script as an inventory tool to keep track of changes in a XenApp 6.x farm. You can also modify the XSD files or (create your own XSD files) to store additional data or data in different formats in the XML files. You can specify a nondefault XSD file with each of the import cmdlets.

Note: Although you can modify script files to meet specific or advanced migration requirements, support is limited to the scripts in their unmodified state. Citrix Technical Support will recommend reverting to the unmodified scripts to determine expected behavior and provide support, if necessary.

## Troubleshooting

- If you are using PowerShell version 2.0 and you added the Citrix Group Policy PowerShell Provider snap-in or the Citrix Common Commands snap-in using the Add-PSSnapIn cmdlet, you might see the error message "Object reference not set to an instance of an object" when you run the export or import cmdlets. This error does not affect script execution and can be safely ignored.
- Avoid adding or removing the Citrix Group Policy PowerShell Provider snap-in in the same console session where the export and import script modules are used, because those script modules automatically add the snap-in. If you add or remove the snap-in separately, you might see one of the following errors:
  - "A drive with the name 'LocalGpo' already exists." This error appears when the snap-in is added twice; the snap-in attempts to mount the drive LocalGpo when it's loaded, and then reports the error.
  - "A parameter cannot be found that matches parameter name 'Controller'." This error appears when the snap-in has not been added but the script attempts to mount the drive. The script is not aware that the snap-in was removed. Close the console and launch a new session. In the new session, import the script modules; do not add or remove the snap-in separately.
- When importing the modules, if you right-click a .psd1 file and select Open or Open with PowerShell, the PowerShell console window will rapidly open and close until you stop the process. To avoid this error, enter the complete PowerShell script module name directly in the PowerShell console window (for example, Import-Module .\ExportPolicy.psd1).
- If you receive a permission error when running an export or import, ensure you are a XenApp administrator with permission to read objects (for export) or read and create objects (for import). You must also have sufficient Windows permission to run PowerShell scripts.
- If an export fails, check that the XenApp 6.x farm is in a healthy state by running the DSMAINT and DSCHECK utilities on the XenApp 6.x controller server.
- If you run a preview import and then later run the import cmdlets again for an actual migration, but discover that nothing was imported, verify that you removed the Preview parameter from the import cmdlets.

## Policy settings not imported

The following computer and user policy settings are not imported because they are no longer supported. Please note, unfiltered policies are never imported. The features and components that support these settings have either been replaced by new technologies/components or the settings do not apply because of architectural and platform changes.

### **Computer policy settings not imported**

- Connection access control
- CPU management server level
- DNS address resolution
- Farm name
- Full icon caching
- Health monitoring, Health monitoring tests
- License server host name, License server port
- Limit user sessions, Limits on administrator sessions
- Load evaluator name
- Logging of logon limit events
- Maximum percent of servers with logon control
- Memory optimization, Memory optimization application exclusion list, Memory optimization interval, Memory optimization schedule: day of month, Memory optimization schedule: day of week, Memory optimization schedule: time
- Offline app client trust, Offline app event logging, Offline app license period, Offline app users
- Prompt for password
- Reboot custom warning, Reboot custom warning text, Reboot logon disable time, Reboot schedule frequency, Reboot

schedule randomization interval, Reboot schedule start date, Reboot schedule time, Reboot warning interval, Reboot warning start time, Reboot warning to users, Scheduled reboots

- Shadowing \*
- Trust XML requests (configured in StoreFront)
- Virtual IP adapter address filtering, Virtual IP compatibility programs list, Virtual IP enhanced compatibility, Virtual IP filter adapter addresses programs list
- Workload name
- XenApp product edition, XenApp product model
- XML service port

\* Replaced with Windows Remote Assistance

#### **User policy settings not imported**

- Auto connect client COM ports, Auto connect client LPT ports
- Client COM port redirection, Client LPT port redirection
- Client printer names
- Concurrent logon limit
- Input from shadow connections \*
- Linger disconnect timer interval, Linger terminate timer interval
- Log shadow attempts \*
- Notify user of pending shadow connections \*
- Pre-launch disconnect timer interval, Pre-launch terminate timer interval
- Session importance
- Single Sign-On, Single Sign-On central store
- Users who can shadow other users, Users who cannot shadow other users \*

\* Replaced with Windows Remote Assistance

#### Application types not imported

The following application types are not imported.

- Server desktops
- Content
- Streamed applications (App-V is the new method used for streaming applications)

#### Application property mapping

The farm data import script imports only applications. The following application properties are imported without change.

IMA Property	FMA Property
AddToClientDesktop	ShortcutAddedToDesktop
AddToClientStartMenu	ShortcutAddedToStartMenu
ClientFolder	ClientFolder
CommandLineExecutable	CommandLineExecutable
CpuPriorityLevel	CpuPriorityLevel

Description <b>IMA Property</b>	Description <b>FMA Property</b>
DisplayName	PublishedName
Enabled	Enabled
StartMenuFolder	StartMenuFolder
WaitOnPrinterCreation	WaitForPrinterCreation
WorkingDirectory	WorkingDirectory
FolderPath	AdminFolderName

Note: IMA and FMA have different restrictions on folder name length. In IMA, the folder name limit is 256 characters; the FMA limit is 64 characters. When importing, applications with a folder path containing a folder name of more than 64 characters are skipped. The limit applies only to the folder name in the folder path; the entire folder path can be longer than the limits noted. To avoid applications from being skipped during the import, Citrix recommends checking the application folder name length and shortening it, if needed, before exporting.

The following application properties are initialized or uninitialized by default, or set to values provided in the XenApp 6.x data:

<b>FMA Property</b>	<b>Value</b>
Name	Initialized to the full path name, which contains the IMA properties FolderPath and DisplayName, but stripped of the leading string "Applications\"
ApplicationType	HostedOnDesktop
CommandLineArguments	Initialized using the XenApp 6.x command line arguments
IconFromClient	Uninitialized; defaults to false
IconUid	Initialized to an icon object created using XenApp 6.x icon data
SecureCmdLineArgumentsEnabled	Uninitialized; defaults to true
UserFilterEnabled	Uninitialized; defaults to false
UUID	Read-only, assigned by the Controller
Visible	Uninitialized; defaults to true

The following application properties are partially migrated:

<b>IMA Property</b>	<b>Comments</b>
FileTypes	Only the file types that exist on the new XenApp site are migrated. File types that do not exist on the new site are ignored. File types are imported only after the file types on the new site are updated.
IconData	New icon objects are created if the icon data has been provided for the exported applications.

<b>IMA Accounts Property</b>	<b>Comments</b>
IMA accounts of an application are split between the user list for the Delivery Group and the application. Explicit users are used to initialize the user list for the application. In addition, the "Domain Users" account for the domain of the user accounts is added to the user list for the Delivery Group.	

The following XenApp 6.x properties are not imported:

<b>IMA Property</b>	<b>Comments</b>
ApplicationType	Ignored.
HideWhenDisabled	Ignored.
AccessSessionConditions	Replaced by Delivery Group access policies.
AccessSessionConditionsEnabled	Replaced by Delivery Group access policies.
ConnectionsThroughAccessGatewayAllowed	Replaced by Delivery Group access policies.
OtherConnectionsAllowed	Replaced by Delivery Group access policies.
AlternateProfiles	FMA does not support streamed applications.
OfflineAccessAllowed	FMA does not support streamed applications.
ProfileLocation	FMA does not support streamed applications.
ProfileProgramArguments	FMA does not support streamed applications.
ProfileProgramName	FMA does not support streamed applications.
RunAsLeastPrivilegedUser	FMA does not support streamed applications.
AnonymousConnectionsAllowed	FMA uses a different technology to support unauthenticated (anonymous) connections.
ApplicationId, SequenceNumber	IMA-unique data.
AudioType	FMA does not support advanced client connection options.
EncryptionLevel	SecureICA is enabled/disabled in Delivery Groups.
EncryptionRequired	SecureICA is enabled/disabled in Delivery Groups.
SslConnectionEnabled	FMA uses a different SSL implementation.
ContentAddress	FMA does not support published content.
ColorDepth	FMA does not support advanced window appearances.
MaximizedOnStartup	FMA does not support advanced window appearances.
TitleBarHidden	FMA does not support advanced window appearances.

<b>IMA Property</b>	<b>Comments</b>
WindowsType	FMA does not support advanced window appearances.
InstanceLimit	FMA does not support application limits.
MultipleInstancesPerUserAllowed	FMA does not support application limits.
LoadBalancingApplicationCheckEnabled	FMA uses a different technology to support load balancing.
PreLaunch	FMA uses a different technology to support session prelaunch.
CachingOption	FMA uses a different technology to support session prelaunch.
ServerNames	FMA uses a different technology.
WorkerGroupNames	FMA does not support worker groups.

# 迁移 XenDesktop 4

May 28, 2016

You can transfer data and settings from a XenDesktop 4 farm to a XenDesktop 7.x Site using the Migration Tool, which is available in the Support > Tools > MigrationTool folder on the XenDesktop installation media. The tool includes:

- The export tool, XdExport, which exports XenDesktop 4 farm data to an XML file (default name: XdSettings.xml). The XML file schema resides in the file XdFarmxsd.
- The import tool, XdImport, which imports the data by running the PowerShell script Import-XdSettings.ps1.

To successfully use the Migration Tool, both deployments must have the same hypervisor version (for example, XenServer 6.2), and Active Directory environment.

You cannot use this tool to migrate XenApp, and you cannot migrate XenDesktop 4 to XenApp.

Tip: You can upgrade XenDesktop 5 (or later XenDesktop versions) to the current XenDesktop version; see [Upgrade a deployment](#).

## Limitations

Not all data and settings are exported. The following configuration items are not migrated because they are exported but not imported:

- Administrators
- Delegated administration settings
- Desktop group folders
- Licensing configuration
- Registry keys

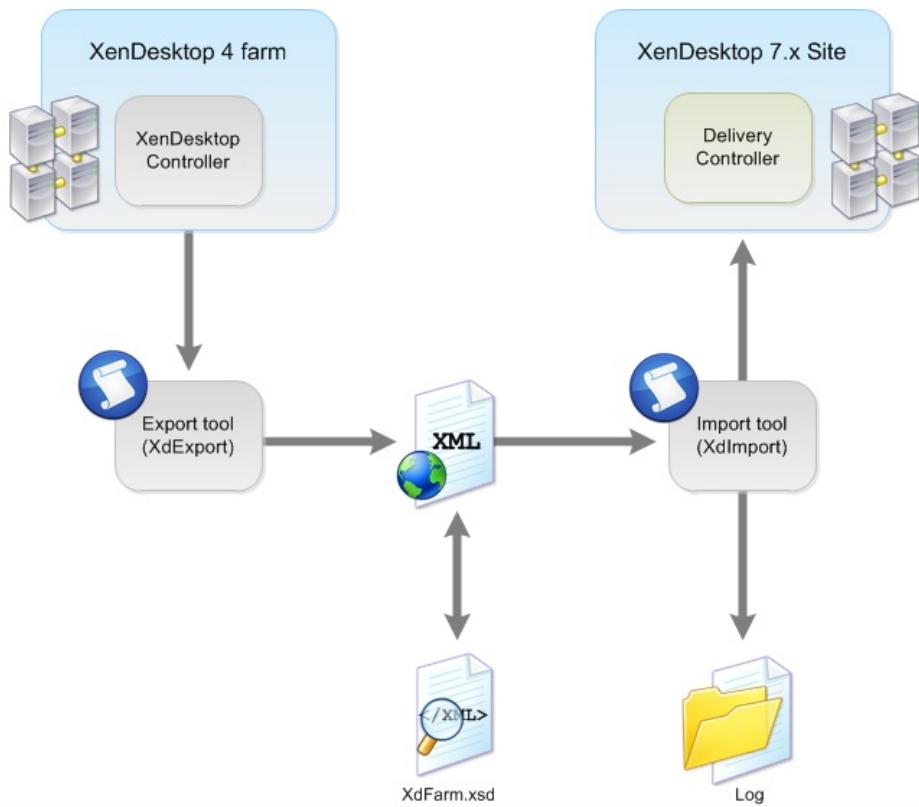
These use cases are not directly supported in migration:

- Merging settings of policies or desktop group or hosting settings.
- Merging private desktops into random Delivery Groups.
- Adjusting existing component settings through the migration tools.

For more information, see [What is and is not migrated](#).

## Migration steps

The following figure summarizes the migration process.



The migration process follows this sequence:

1. In the Studio console on the XenDesktop 4 Controller, turn on maintenance mode for all machines to be exported.
2. Export data and settings from your XenDesktop 4 farm to an XML file using XdExport; see [Export from a XenDesktop 4 farm](#).
3. Edit the XML file so that it contains only the data and settings you want to import into your new XenDesktop Site; see [Edit the Migration Tool XML file](#).
4. Import the data and settings from the XML file to your new XenDesktop Site using XdImport; see [Import XenDesktop 4 data](#).
5. To make additional changes, repeat steps 3 and 4. After making changes, you might want to import additional desktops into existing Delivery Groups. To do so, use the Mergedesktops parameter when you import.
6. Complete the post-migration tasks; see [Post-migration tasks](#).

### Before migrating

Complete the following before beginning a migration:

- Make sure you understand which data can be exported and imported, and how this applies to your own deployment. See [What is and is not migrated](#).
- Citrix strongly recommends that you manually back up the Site database so that you can restore it if any issues are discovered.
- Install the XenDesktop 7.x components and create a Site, including the database.
- To migrate from XenDesktop 4, all VDAs must be at a XenDesktop 5.x level so that they are compatible with both XenDesktop 4 and XenDesktop 7.x controllers. After the Controller infrastructure is fully running XenDesktop 7.x, Windows 7 VDAs can be upgraded to XenDesktop 7.x. For details, see [Migration examples](#).

# 从 XenDesktop 4 场中导出

May 28, 2016

The export tool, XdExport, extracts data from a single XenDesktop 4 farm and produces an XML file from representations of the data values.

The schema of the XML file resides in the file XdFarm.xsd, which is included in the migration tool download XdExport.zip and XdImport.zip.

Run XdExport on a XenDesktop 4 Controller in the farm from which you want to export data. This machine must have the XenDesktop 4 PowerShell SDK installed. You must have the following permissions to export the data:

- The user identity of at least read-only Citrix administrator of the farm.
- Permission to read the registry.

Although not recommended, you can run the tool while the XenDesktop Controller is in active use (for example, users are logged in to VDAs).

Citrix strongly recommends:

- The XenDesktop 4 Controller on which you run the tool be up-to-date with public hotfixes.
- Not making configuration changes to the Site while the export is running (for example, removing Desktop Groups).

1. Download XdExport.zip and extract the files to the XenDesktop 4 Controller.
2. At a command line prompt, run XdExport.exe with the following optional parameters:

Parameter	Description
-Verbose	Generates messages providing detailed progress information.
-FilePath <path>	Indicates the location of the XML file to which the farm data is exported. Default = .\XdSettings.xml
-Overwrite	Overwrites any file existing in the location specified in -FilePath. If you do not supply this parameter and an output file already exists, the tool fails with the message "Error: File already exists. Specify -Overwrite to allow the file to be overwritten."
-? or -help	Displays text describing the parameters and exits without exporting any data.

3. If the tool runs successfully, the message Done appears. The XdSettings.xml file resides in the location specified in the FilePath parameter. If the tool fails, an error message appears.

# 编辑迁移工具 XML 文件

May 28, 2016

Before importing data to a XenDesktop 7.x Site, check and edit the contents of the XML file generated by the export tool (XdExport), particularly if you migrate in multiple stages and import some users, Delivery Groups, and policies before importing others.

Use any text editor to view or change the file contents; you can use a specialized XML editor such as Microsoft XML Notepad.

Some elements within the XML content must be present for the XML file to be accepted by the import tool (XdImport).

The required XML schema is defined in the XdFarmxsd file that is supplied as part of the Migration Tool download. When working with this file:

- A minOccurs attribute with a value of 1 or more indicates that particular elements must be present if the parent element is present.
- If the XML file supplied to the Import tool is not valid, the tool halts and an error message appears that should enable you to locate where the problem lies in the XML file.

## Import a subset of desktops or Delivery Groups

To import only a subset of Delivery Groups and desktops, edit the contents of the DesktopGroups element. The DesktopGroups element can hold many DesktopGroup elements, and within each DesktopGroup element there is a Desktops element that can contain many Desktop elements.

Do not delete the DesktopGroups element, although you can delete all the DesktopGroup elements and leave it empty. Similarly, within each DesktopGroup element, the Desktops element must be present but can be empty of Desktop elements.

Delete Desktop or DesktopGroup elements to avoid importing particular single machines or entire Delivery Groups. For example, the XML file contains:

```
<DesktopGroups>
  <DesktopGroup name="Group1">
    ...
    <Desktops>
      <Desktop sameName="DOMAIN\MACHINE1$">
        ...
        </Desktop>
      </Desktops>
    ...
    </DesktopGroup>
  <DesktopGroup name="Group2">
    ...
    <Desktops>
      <Desktop samName="DOMAIN\MACHINE2$">
        ...
        </Desktop>
      <Desktop samName="DOMAIN\MACHINE3$">
        ...
    </Desktops>
  </DesktopGroups>
```

```
</Desktop>  
</Desktops>  
...  
</DesktopGroup>  
</DesktopGroups>
```

In this example, the edits prevent Group1 group from being imported. Only Machine3 from the Group2 group will be imported:

```
<DesktopGroups>  
<DesktopGroup name="Group2">  
...  
<Desktops>  
<Desktop samName="DOMAIN\MACHINE3$">  
...  
</Desktop>  
</Desktops>  
...  
</DesktopGroup>  
</DesktopGroups>
```

#### Manage Delivery Groups with duplicate names

In XenDesktop 4, Desktop Groups can be organized in folders, Desktop Groups with the same name can appear in different folders, and the internal desktop group name is the name that appears to users. In this release, Delivery Groups cannot be placed in folders, and each Delivery Group must have a unique internal name, and the name that appears to users can be different from the internal name. To accommodate these differences, you might have to rename Desktop Groups.

For example, in your XenDesktop 4 farm, you could have two different Desktop Groups that appear with the name "My Desktop" to two different users, and you could use Desktop Groups folders to achieve this. If these Delivery Groups are to remain separate in the XenDesktop 7.x Site, you must edit the Desktop Group names in the XML file to make them unique.

If a Delivery Group in the XenDesktop 7.x Site has the same name as a Desktop Group to be imported, and the Delivery Groups are to remain separate in the XenDesktop 7.x Site, you must edit the XenDesktop 4 Desktop Group name in the XML file to keep the name unique in the Site. If the Desktop Group to be imported is really the same as the XenDesktop 7.x Delivery Group, and the machines in the XML file are to be merged into the existing Desktop Group, you do not need to rename the Desktop Group; instead, specify the -MergeDesktops parameter to the Import tool. For example, if the XML file contains:

```
<DesktopGroups>  
<DesktopGroup name="My Desktop">  
...  
<Folder>\Sales</Folder>  
</DesktopGroup>  
<DesktopGroup name="My Desktop">  
...  
<Folder>\Finance</Folder>  
</DesktopGroup>  
</DesktopGroups>
```

Remove the duplicate names as follows:

```
<DesktopGroups>  
<DesktopGroup name="Sales Desktops">  
...
```

```
<Folder>\Sales</Folder>
</DesktopGroup>
<DesktopGroup name="Finance Desktops">
...
<Folder>\Finance</Folder>
</DesktopGroup>
</DesktopGroups>
```

## Manage policy imports

You can delete policies from the XML file, and you can specify unique names to avoid policy name duplication. There is no support for merging policies.

- When you import policy data, either all policies are imported successfully or, if there is any failure, no policy data is imported.
- Importing large numbers of policies with many settings can take several hours.
- If you import policies in batches, their original prioritization may be affected. When you import policies, the relative priorities of the imported policies are maintained, but they are given higher priority than policies already in the Site. For example, if you have four policies to import with priority numbers 1 to 4, and you decide to import them in two batches, you should import policies with priorities 3 and 4 first, because the second batch of policies automatically gets higher priority.

To import only a subset of policies into the XenDesktop 7.x Site, edit the contents of the Policies element. The Policies element can hold many Policy elements. You must not delete the Policies element, although you can delete all the Policy elements and leave it empty. Delete entire Policy elements to avoid importing particular XenDesktop 4 farm policies. For example, if the XML file contains:

```
<Policies>
<Policy name="Sales Policy">
...
</Policy>
...
</Policies>
```

To avoid importing any XenDesktop 4 policies, and avoid clashes with policies already configured in the XenDesktop 7.x Site, edit the file to remove the individual Policy elements as follows:

```
<Policies>
</Policies>
```

Alternatively, edit the file so that the policy is imported with a different name as follows:

```
<Policies>
<Policy name="XD4 Sales Policy">
...
</Policy>
...
</Policies>
```

# 导入 XenDesktop 4 数据

May 28, 2016

The import tool, XdImport, reads settings from XenDesktop 4 that are contained in the XML file produced by the export tool, XdExport, and applies those settings to an existing XenDesktop 7.x Site. The Import tool uses the PowerShell script Import-XdSettings.ps1.

To apply only a subset of the exported data, edit the XML file before running the Import tool. For example, you might want to remove desktop groups and policies that are not needed in your XenDesktop 7.x deployment. The import tool runs successfully if you leave entire elements empty. For example, you can delete all the desktop groups without causing any issues. The tool always validates the XML file before attempting to import any data.

Run XdImport on any machine on which all the XenDesktop 7.x SDKs are installed. You must be a Full XenDesktop administrator identity to run the tool.

Before you import, make sure that you have set up a XenDesktop 7.x Site, including its database. Citrix recommends that you complete the import to XenDesktop 7.x before any user testing or general Site configuration occurs. Merge configurations only when the Site is not in use.

1. Create a XenDesktop 7.x Site.
2. Download XdImport.zip and extract the files to the machine where you will run the tool.
3. In a PowerShell session, run Import-XdSettings.ps1 with the following parameters:

Parameter	Description
-HypervisorConnectionCredentials	(Required.) A PowerShell hash table that maps Hypervisor addresses to PSCredential instances as required for the creation of Hypervisor connections. Default = @{}  Enter credentials for the Hypervisor to which the XenDesktop 4 farm connects.  For a single Hypervisor, create the argument as follows:  <pre>\$credential = Get-Credential \$mappings = @{"http://&lt;HypervisorIP&gt;"     =\$credential} .\\Import-XdSettings.ps1 -FilePath .\\XdSettings.xml -HypervisorConnectionCredentials \$mappings</pre> The address specified in the hash table must exactly match the address in the XML file.  For example, with both a XenServer and a VMware hypervisor, create the following argument:  <pre>\$Xencredential = Get-Credential \$VMWcredential = Get-Credential \$mappings = @{"http://&lt;XenHypervisorIP&gt;"     = \$Xencredential;"http://&lt;VmWHypervisorIP&gt;/SDK"</pre>

<b>Parameter</b>	<p><b>Description</b>  <code>\$VMWcredential</code>  <code>.\Import-XdSettings.ps1</code></p> <p>-FilePath. \XdSettings.xml  -HypervisorConnectionCredentials \$mappings</p>
-FilePath <path>	(The value for <path> is required. ) The location of the XML file from which the farm data is to be imported.
-AdminAddress	The name of a Controller in the XenDesktop 7.x Site. Default = localhost
-MergeDesktops	<p>Adds desktops defined in the XML file to Delivery Groups in the XenDesktop 7.x Site that have the same name as the groups described in the XML file. The associated machines and users are also added.</p> <p>If this parameter is not supplied, no content is added to existing Delivery Groups in the XenDesktop 7.x Site.</p>
-SkipMachinePolicy	The script does not create a machine policy that contains site-level settings. If you do not supply this parameter and the machine policy for the Site exists, the script fails.
-WhatIf	Completes a trial run to determine what would be changed in or added to the XenDesktop 7.x Site. Including this parameter sends the information to the log file, but does not change the Site.
-LogFilePath <path>	Indicates the full path of the log file. The log file contains text describing all writes performed against the XenDesktop 7.x Site. Default = .\Import-XdSettings.log
-? or -help	Displays information about parameters and exits without importing any data.

If the XML file contains policy data, either all policies are imported successfully or if there is any failure, no policy data is imported. Importing large numbers of policies with many settings can take several hours.

When the script completes, the message Done appears. After successfully importing the data from the XML file, you can either run further export and import iterations, or if you have imported all the relevant data, complete the post-migration tasks.

# 迁移后需执行的任务

May 28, 2016

After successfully importing data from a XenDesktop 4 farm to a XenDesktop 7.x Site, complete the following tasks before using the new Site for production work:

- Upgrade the Virtual Delivery Agents (VDAs). Although it is not required, Citrix recommends that you upgrade VDAs before upgrading Controllers, Studio, or Director.
  - For Windows Vista and Windows XP, upgrade to XenDesktop 5.6 Feature Pack 1 Virtual Desktop Agent.
  - For Windows 7, upgrade to the XenDesktop 7.x Virtual Delivery Agent.
- Create administrators you need for the XenDesktop 7.x Site.
- Update user devices — Citrix recommends that you update user devices with the latest version of Citrix Receiver to benefit from hotfixes and to receive support for the latest features.
- Modify the imported desktops to use registry-based Controller discovery, and point them to the XenDesktop 7.x Controllers using one of the following methods:
  - Manually edit the registry to remove the unnecessary Organizational Unit (OU) GUID registry entry, and add a ListOfDDCs registry entry.
  - Set up a machine policy to distribute the list of Controllers to the desktops, using the Active Directory policy GPMC.msc. You cannot use Studio to configure this setting.

Registry-based Controller discovery is the default for XenDesktop 7.x, but Active Directory-based discovery is still available.

- Optionally, implement the following registry key settings described in the best practices for XenDesktop registry-based registration in [CTX133384](#):
  - HeartbeatPeriodMS
  - PrepareSessionConnectionTimeoutSec
  - MaxWorkers
  - DisableActiveSessionReconnect
  - ControllersGroupGuid

If you do not perform this action, the default XenDesktop 7.x settings for these keys are used.

- Turn off maintenance mode for the imported machines if they were in maintenance mode in XenDesktop 4 before the XML file was generated.
- Check the XenDesktop 7.x settings to make sure that they are correct, particularly if you had changed the PortICAConfig XML file on XenDesktop 4.
- Review all migrated components to make sure that the migration was successful.

# 迁移示例

May 28, 2016

## Example 1: Single large-scale XenDesktop 4 farm to a XenDesktop 7 Site

In this example, a XenDesktop 4 farm is in use. The XenDesktop 4 farm has 50 desktop groups, where each group contains an average 100 desktops. The XenDesktop 4 desktops are provided through Provisioning Services (PVS), and the machines are running on VMware ESX hypervisors. The VDA installed on all the VMs is the XenDesktop version 4.

### Migration steps

1. Upgrade all XenDesktop 4 VDAs to XenDesktop 5.6 Feature Pack 1 VDA software. This allows the VDAs to register with both the XenDesktop 4 controller and the XenDesktop 7 Delivery Controller.
  - For Windows 7 VDAs, see [Upgrading the Virtual Desktop Agent on a VM or Blade Computer](#).
  - For Windows XP and Windows Vista VDAs, see [Virtual Desktop Agents on Windows XP or Windows Vista](#).
2. Make sure that all users log off the XenDesktop 4 farm.
3. Make sure that all these machines are in maintenance mode.
4. Run the export tool (XdExport) on the XenDesktop 4 farm.
5. Install XenDesktop 7 components.
  1. Use Studio to create a full production mode Site.
  2. If Provisioning Services is part of the deployment, upgrade the Provisioning Services server and agents.
  3. Upgrade the License Server and associated licenses.
6. Unzip the Import Tool (XdImport) to a local directory on the XenDesktop 7 Controller.
7. Copy the XML file (XdSettings.xml) generated in Step 4 by the export tool to the local directory.
8. From the PowerShell console of the Studio root node on the XenDesktop 7 Site, start a PowerShell session.
9. Run the import tool (XdImport), passing the credentials of the associated hypervisors and the path of the XML file.
10. Manually recreate administrator settings from the Administrator node in the Studio navigation pane; see [Delegated Administration](#) for details.
11. Modify the imported desktops to use registry-based Controller discovery; and point them to the new XenDesktop 7 Controller.
12. For VDAs running on Windows 7, Citrix recommends you upgrade those VDAs to use the XenDesktop 7 VDA for Windows Desktop OS, which provides access to all new features.  
After upgrading the VDAs to XenDesktop 7 for machines in a catalog or Delivery Group, upgrade the catalog (see [Manage machine catalogs](#)) and Delivery Groups (see [Manage settings in Delivery Groups](#)).
13. Turn off maintenance mode for the Delivery Groups.
14. Configure StoreFront to provide the desktops formerly provided through Web Interface. See the StoreFront documentation.

## Example 2: XenDesktop 4 farm export with a partial import to XenDesktop 7.1 Site

In this example, the migration occurs in a number of steps, each step migrating a subset of the remaining desktops. A XenDesktop 4 farm is in use, and a XenDesktop 7.1 Site has already been created and is in use. The XenDesktop 4 farm has 50 desktop groups, and each group contains an average 100 desktops. The XenDesktop 4 desktops are provided through Provisioning Services, and the machines are running on Citrix XenServer hypervisors. The VDA installed on all the VMs is the XenDesktop version 4.

### Migration steps

1. Run the export tool on the XenDesktop 4 farm.
  1. Unzip the Export Tool (XdExport) on one of the Desktop Delivery Controllers in the farm.
  2. As a Citrix Administrator, run the export tool with no parameters.
2. Copy and edit the resulting XML file so that it contains only the groups and desktops that you want to migrate.
3. In the XenDesktop 4 farm, make sure that all users on desktops to be migrated have logged off and turn on maintenance mode for all desktops that are to be migrated.
4. Unzip the Import Tool (XdlImport) to a local directory on the XenDesktop 7.1 Delivery Controller.
5. Copy the edited XML to the local directory.
6. From the PowerShell console of the Studio root node on the XenDesktop 7.1 Site, start a PowerShell session.
7. Run the Import Tool (XdlImport), passing the credentials of the associated hypervisors and the path of the XML file.
8. Manually recreate Administrator settings from the Administrator node in the Studio navigation pane; see [Delegated Administration](#) for details.
9. Modify the imported desktops to use registry-based Controller discovery; and point them to the new XenDesktop 7.1 Controller.
10. Upgrade all VDAs to the appropriate VDA software:
  - For Windows 7 VDAs:
    - Upgrade to XenDesktop 7 Virtual Delivery Agents as described in [Upgrading the Virtual Desktop Agent on a VM or Blade Computer](#)
    - After upgrading all VDA software to XenDesktop 7 for machines in a catalog or Delivery Group, upgrade the catalog (see [Manage machine catalogs](#)) and Delivery Groups (see [Manage settings in Delivery Groups](#)).
  - For Windows XP and Windows Vista VDAs, upgrade to XenDesktop 5.6 FP1; see [Virtual Desktop Agents on Windows XP or Windows Vista](#).
11. Turn off maintenance mode for the Delivery Groups.
12. Configure StoreFront to provide the desktops formerly provided through Web Interface. See the StoreFront documentation.

# 迁移和不迁移的内容

May 28, 2016

## What is migrated

Although not all inclusive, the following table describes what happens to the most significant data during migration to this release. Unless noted, the data type is imported.

Data type	Notes
Desktop Groups	<p>Desktop Groups become Delivery Groups in this release. Desktop Group icons are not exported.</p> <p>SecureIcaRequired is set to True if the DefaultEncryptionLevel in XenDesktop 4 is not Basic.</p> <p>If a Desktop Group in the XenDesktop 4 farm has the same name as a Delivery Group in the XenDesktop 7.x Site, you can add desktops belonging to the XenDesktop 4 group to a Delivery group of the same name in the target Site.</p> <p>To do this, specify the MergeDesktops parameter when you run the import tool. The settings of the XenDesktop 7.x Delivery Group are not overwritten with the settings of the XenDesktop 4 group. If this parameter is not specified and there is a group with the same name as one defined in the XML file, the tool displays an error and stops before any data is imported.</p>
Desktops	You cannot add private desktops to a random Delivery Group. Random desktops cannot be added to a static Delivery Group.
Machines	<p>Machines are imported into four machine catalogs. The following machine catalogs are automatically created in the XenDesktop 7.x Site by the import tool:</p> <ul style="list-style-type: none"><li>• Imported existing random (for pooled VMs)</li><li>• Imported existing static (for assigned VMs)</li><li>• Imported physical random (for pooled PCs or blades)</li><li>• Imported physical static (for private PCs or blades).</li></ul> <p>Any subsequent import of machines uses the same four machine catalogs.</p>
Pool management pools	<p>Includes multi-pool pools, and idle pool settings including schedule.</p> <ul style="list-style-type: none"><li>• PeakBuffersizePercent is set to 10% by default.</li><li>• OffPeakBufferSizePercent is set to 10% by default.</li><li>• Any unselected days in the Business days setting on XenDesktop 4 are imported as part of the Weekend power time scheme in this release.</li><li>• HostingXD4 action times are rounded up to the nearest minute.</li><li>• Start times are rounded down to the nearest hour.</li><li>• End times are rounded up to the nearest hour.</li></ul>
Farm settings	The following farm settings are imported as a Machine policy: <ul style="list-style-type: none"><li>• IcaKeepAlive</li></ul>

<b>Data type</b>	<p><b>Notes</b></p> <ul style="list-style-type: none"> <li>• AutoClientReconnect</li> <li>• SessionReliability</li> </ul> <p>The setting to enable Flash player is not imported.</p>
Policies	<p>Some policy data is imported. Filters, settings, and printers are imported as User policies. For further details of user policy export and import, see the other table in this document.</p> <ul style="list-style-type: none"> <li>• New access policy rules are created from XenDesktop 4 group settings.</li> <li>• When policies are imported, their relative priority order is preserved. However, they are always added with a higher priority than any existing policies on the XenDesktop 7.x Site.</li> <li>• Policy merging is not supported.</li> </ul> <p>There is no option to import policies into Active Directory. They are always stored in the Site.</p>
User assignments	
Hypervisor settings	<p>This parameter is required with the XdImport tool.</p> <p>Hypervisor addresses are exported, but not the credentials required to access those hypervisors. To create hypervisor connections in the XenDesktop 7.x Site, extract the addresses from the XML file and create a PowerShell hash table that maps them to the relevant credential instances. Then specify this hash table in the import tool HypervisorConnectionCredentials parameter. For further details, see <a href="#">Import XenDesktop 4 data</a></p> <p>Merging or updating hypervisor settings for existing Desktop Groups and hypervisor connections is not supported.</p>
Administrators	(Not imported.) No administrator data is imported, including data about delegated administrators. You create new administrators for your XenDesktop 7.x Site.
Licensing configuration	(Not imported.) Includes information such as the License Server name and edition. License files are not exported.
Desktop Group folders	(Not imported.) This release does not support Desktop Group folders. If there are duplicate Desktop Group names (because different folders in the XenDesktop 4 farm contained groups with the same names) and you do not edit names in the XML file, the Import Tool halts.
Registry keys	(Not imported.) For information on implementing registry keys, see <a href="#">Post-migration tasks</a> .

## User policy data

The following table describes how User policy data is exported and imported.

<b>XenDesktop 4 category and setting</b>	<b>XML file</b>	<b>XenDesktop 7.x category and setting</b>
Bandwidth\Visual Effects\Session Limits  OEM Virtual Channels	ClientOEMVCBandwidth	Not imported
Client Devices\Resources\Other  Turn off OEM virtual channels	DisableOEMVirtualChannels	Not imported
User Workspace\Time Zones  Do not use client's local time	DoNotUseClientLocalTime	Not imported
Security\Encryption  SecureICA encryption	ClientSecurityRequirement	Not imported
Bandwidth\SpeedScreen  Image acceleration using lossy compression	LossyCompression settings	ICA\Visual Display\Still Images  Lossy compression level  Lossy compression threshold value  Heavyweight compression  ICA\Visual Display\Moving Images  Progressive compression level  Progressive compression threshold value
Bandwidth\Visual Effects  Turn off desktop wallpaper	TurnOffWallpaper	ICA\Desktop UI  Desktop wallpaper
Bandwidth\Visual Effects  Menu animation	TurnOffMenuWindowAnimation	ICA\Desktop UI  Menu animation

<b>XenDesktop 4 category and setting</b> Turn OFF window contents while dragging	<b>XML file</b> DoNotShowWindowContentsWhileDragging	<b>XenDesktop 7.x category and setting</b> View window contents while dragging
Bandwidth\Visual Effects\Session Limits  Audio	ClientAudioBandwidth__AllowedBandWidth	ICA\Bandwidth  Audio redirection bandwidth limit
Bandwidth\Visual Effects\Session Limits  Clipboard	ClientClipboardBandwidth__AllowedBandWidth	ICA\Bandwidth  Clipboard redirection bandwidth limit
Bandwidth\Visual Effects\Session Limits  COM Ports	ClientComBandwidth__AllowedBandWidth	COM port redirection is deprecated in XenDesktop 7.x
Bandwidth\Visual Effects\Session Limits  Drives	ClientDriveBandwidth__AllowedBandWidth	ICA\Bandwidth  File redirection bandwidth limit
Bandwidth\Visual Effects\Session Limits  LPT Ports	ClientLptBandwidth__AllowedBandWidth	LPT port redirection is deprecated in XenDesktop 7.x
Bandwidth\Visual Effects\Session Limits  Overall Session	OverallBandwidth__AllowedBandWidth	ICA\Bandwidth  Overall session bandwidth limit
Bandwidth\Visual Effects\Session Limits  Printer	LimitPrinterBandWidth__AllowedBandWidth	ICA\Bandwidth  Printer redirection bandwidth limit
Client Devices\Resources\Audio  Microphones	ClientAudioMicrophone__TurnOn	ICA\Audio  Client microphone redirection

XenDesktop 4 category and setting	Client AudioQuality__Quality XML file	ICA\Audio XenDesktop 7.x category and setting Audio quality
Client Devices\Resources\Audio Turn off speakers	DisableClientAudioMapping	ICA\Audio Client audio redirection
Client Devices\Resources\Drives Connection	ConnectClientDriveAtLogon__TurnOn	ICA\File Redirection Auto connect drives
Client Devices\Resources\Drives Turn off Floppy disk drives	DisableClientDriveMapping__DisableFloppyDrive	ICA\File Redirection Client floppy drives
Client Devices\Resources\Drives Turn off Hard drives	DisableClientDriveMapping__DisableHardDrive	ICA\File Redirection Client fixed drives
Client Devices\Resources\Drives Turn off CD-ROM drives	DisableClientDriveMapping__DisableCdrom	ICA\File Redirection Client optical drives
Client Devices\Resources\Drives Turn off Remote drives	DisableClientDriveMapping__DisableRemote	ICA\File Redirection Client network drives
Client Devices\Resources\Drives Turn off USB disk drives	DisableClientDriveMapping__DisableUSB	ICA\File Redirection Client removable drives
Client Devices\Resources\Drives\Optimize Asynchronous writes	CDMAsyncWrites	ICA\File Redirection User asynchronous writes
Client Devices\Resources\Other Turn off clipboard mapping	DisableClientClipboardMapping	ICA Client clipboard redirection
Client Devices\Resources\Ports Turn off COM ports	DisableClientCOMPortMapping	COM port redirection is deprecated in XenDesktop 7.x
Client Devices\Resources\Ports	DisableClientLPTPortMapping	LPT port redirection is

XenDesktop 4 category and setting	XML file	deprecated in XenDesktop 7.x category and setting
Client Devices\Resources\USB USB	RemoteUSBDevices__DisableRemoteUSBDevices	ICA\USB Devices Client USB device redirection
Printing\Client Printers Auto-creation	ConnectClientPrinterAtLogon__Flag	ICA\Printing\Client Printers Auto-create client printers
Printing\Client Printers Legacy client printers	LegacyClientPrinters__TurnOn	ICA\Printing\Client Printers Client printer names
Printing\Client Printers Printer properties retention	ModifiedPrinterProperties__WriteMethod	ICA\Printing\Client Printers Printer properties retention
Printing\Client Printers Print job routing	ClientPrintingForNetworkPrinter__TurnOn	ICA\Printing\Client Printers Direct connections to print servers
Printing\Client Printers Turn off client printer mapping	DisableClientPrinterMapping	ICA\Printing Client printer redirection
Printing\Drivers Native printer driver auto-install	PrintDriverAutoInstall__TurnOn	ICA\Printing\Drivers Automatic installation of inbox printer drivers
Printing\Drivers Universal driver	ClientPrintDriverToUse	ICA\Printing\Drivers Universal print driver use
Printing\Session printers Session printers	NetworkPrinters	ICA\Printing Session printers
Printing\Session printers Choose client's default printer	DefaultToMainClientPrinter__NetworkDefault DefaultToMainClientPrinter__TurnOn	ICA\Printing Default printer

## What is not migrated

Not all XenDesktop 4 components are supported in this release. The following items are not migrated:

- **Virtual Delivery Agent** - Before a XenDesktop 7.x Delivery Controller can manage virtual desktops from XenDesktop 4, you must upgrade the VDAs to a minimum release of XenDesktop 5.x. For information about upgrading VDAs, see [Post-migration tasks](#).
- **Controllers** - You must deploy new Controller servers. You cannot upgrade a XenDesktop 4 Controller to a XenDesktop 7.x Site. XenDesktop 7.x Sites cannot join a XenDesktop 4 farm, and XenDesktop 4 Controllers cannot join a XenDesktop 7.x Site. In addition, each version has different server requirements; XenDesktop 4 requires Windows Server 2003 and XenDesktop 7.x requires later Windows Server versions.
- **Web Interface** - Citrix recommends using StoreFront with XenDesktop 7.x. See the StoreFront documentation for installation and setup details. When the XenDesktop installer detects Web Interface, it installs StoreFront, but does not remove Web Interface.
- **Active Directory Organizational Unit (OU) configuration** - Sharing an Organizational Unit (OU) between two farms or two Sites, or a farm and a Site is not supported. If you plan to configure the new Site to use Active Directory-based Controller discovery rather than the default registry-based Controller discovery, you must create a new OU to support it.
- **PortICAConfig XML file** - If you have changed the default settings for this file you may need to configure these settings for the new Site through Group Policy Objects.
- **Configuration logging settings provided through XenDesktop 4 Service Pack 1**.
- **Provisioning Services-related data**.
- **Applications**.
- **List of Controllers**.
- **NetScaler Gateway**.
- **Event log throttling settings**.

# 安全性

May 28, 2016

PDF

## Getting Started with Citrix XenApp and XenDesktop Security

XenApp and XenDesktop offer a secure-by-design solution that allows you to tailor your environment to your security needs.

One security concern IT faces with mobile workers is lost or stolen data. By hosting applications and desktops, XenApp and XenDesktop securely separate sensitive data and intellectual property from end-point devices by keeping all data in a data center. When policies are enabled to allow data transfer, all data is encrypted.

The XenDesktop and XenApp data centers also make incident response easier with a centralized monitoring and management service. Director allows IT to monitor and analyze data that is being accessed around the network, and Studio allows IT to patch and remedy most vulnerabilities in the data center instead of fixing the problems locally on each end-user device.

XenApp and XenDesktop also simplify audits and regulatory compliance because investigators can use a centralized audit trail to determine who accessed what applications and data. Director gathers historical data regarding updates to the system and user data usage by accessing Configuration Logging and OData API.

Delegated Administration allows you to set up administrator roles to control access to XenDesktop and XenApp at a granular level. This allows flexibility in your organization to give certain administrators full access to tasks, operations, and scopes while other administrators have limited access.

XenApp and XenDesktop give administrators granular control over users by applying policies at different levels of the network — from the local level to the Organizational Unit level. This control of policies determines if a user, device, or groups of users and devices can connect, print, copy/paste, or map local drives, which could minimize security concerns with third-party contingency workers. Administrators can also use the Desktop Lock feature so end users can only use the virtual desktop while preventing any access to the local operating system of the end-user device.

Administrators can increase security on XenApp or XenDesktop by configuring the Site to use the Secure Sockets Layer (SSL) security protocol of the Controller or between end users and Virtual Delivery Agents (VDA). Transport Layer Security (TLS) security protocol can also be enabled on a Site to provide server authentication, data stream encryption, and message integrity checks for a TCP/IP connection.

XenApp and XenDesktop also support multifactor authentication for Windows or a specific application. Multifactor authentication could also be used to manage all resources delivered by XenApp and XenDesktop. These methods include:

- Tokens
- Smart cards
- RADIUS
- Kerberos
- Biometrics

XenDesktop can be integrated with many third-party security solutions, ranging from identity management through to antivirus software. A list of supported products can be found at <http://www.citrix.com/ready>.

Select releases of XenApp and XenDesktop are certified for Common Criteria standard. For a list of those standards, go to

<http://www.commoncriteriaportal.org/cc/>.

## Related content

- Security best practices and considerations
- Delegated Administration
- Smart cards
- SSL
- Desktop Lock

# 安全最佳实践和注意事项

Jan 31, 2017

This document describes:

- General security best practices when using this release, and any security-related differences between this release and a conventional computer environment
- Manage user accounts
- Manage user privileges
- Manage logon rights
- Configure user rights
- Configure service settings
- Deployment scenarios and their security implications
- Remote PC Access security considerations

Your organization may need to meet specific security standards to satisfy regulatory requirements. This document does not cover this subject, because such security standards change over time. For up-to-date information on security standards and Citrix products, consult <http://www.citrix.com/security/>.

## Security best practices

Keep all machines in your environment up to date with security patches. One advantage is that you can use thin clients as terminals, which simplifies this task.

Protect all machines in your environment with antivirus software.

Protect all machines in your environment with perimeter firewalls, including at enclave boundaries as appropriate.

If you are migrating a conventional environment to this release, you may need to reposition an existing perimeter firewall or add new perimeter firewalls. For example, suppose there is a perimeter firewall between a conventional client and database server in the data center. When this release is used, that perimeter firewall must instead be placed so that the virtual desktop and user device are on one side, and the database servers and Delivery Controllers in the data center are on the other side. You should therefore consider creating an enclave within your data center to contain the database servers and Controllers. You should also consider having protection between the user device and the virtual desktop.

All machines in your environment should be protected by a personal firewall. When you install core components and Virtual Delivery Agents (VDAs), you can choose to have the ports required for component and feature communication opened automatically if the Windows Firewall Service is detected (even if the firewall is not enabled). You can also choose to configure those firewall ports manually. If you use a different firewall, you must configure the firewall manually.

Note: TCP ports 1494 and 2598 are used for ICA and CGP and are therefore likely to be open at firewalls so that users outside the data center can access them. Citrix recommends that you do not use these ports for anything else, to avoid the possibility of inadvertently leaving administrative interfaces open to attack. Ports 1494 and 2598 are officially registered with the Internet Assigned Number Authority (see <http://www.iana.org/>).

All network communications should be appropriately secured and encrypted to match your security policy. You can secure all communication between Microsoft Windows computers using IPSec; refer to your operating system documentation for details about how to do this. In addition, communication between user devices and desktops is secured through Citrix SecureICA, which is configured by default to 128-bit encryption. You can configure SecureICA when you are creating or updating an assignment; see [Change basic settings](#).

# Manage user accounts

If the option to install App-V publishing components is selected when installing a VDA, or if this feature is added later, the local administrative account CtxAppVCOMAdmin is added to the VDA. If you use the App-V publishing feature, do not modify this account. If you do not need to use the App-V publishing feature, do not select it at installation time. If you later decide not to use the App-V publishing feature, you can disable or delete this account.

This account is created with an initial password that is a strong password, compatible with all Group Policy settings for password policy. You cannot change the password for this account.

## Manage user privileges

Grant users only the capabilities they require. Microsoft Windows privileges continue to be applied to desktops in the usual way: configure privileges through User Rights Assignment and group memberships through Group Policy. One advantage of this release is that it is possible to grant a user administrative rights to a desktop without also granting physical control over the computer on which the desktop is stored.

When planning for desktop privileges, note:

- By default, when non-privileged users connect to a desktop, they see the time zone of the system running the desktop instead of the time zone of their own user device. For information on how to allow users to see their local time when using desktops, see [Change basic settings](#).
- A user who is an administrator on a desktop has full control over that desktop. If a desktop is a pooled desktop rather than a dedicated desktop, the user must be trusted in respect of all other users of that desktop, including future users. All users of the desktop need to be aware of the potential permanent risk to their data security posed by this situation. This consideration does not apply to dedicated desktops, which have only a single user; that user should not be an administrator on any other desktop.
- A user who is an administrator on a desktop can generally install software on that desktop, including potentially malicious software. The user can also potentially monitor or control traffic on any network connected to the desktop.

Some applications require desktop privileges, even though they are intended for users rather than for administrators. These users may not be as aware of security risks.

Treat these applications as highly-sensitive applications, even if their data is not sensitive. Consider these approaches to reduce security risk:

- Enforce two-factor authentication and disable any single sign-on mechanism for the application
- Enforce contextual access policies
- Publish the application to a dedicated desktop. If the application must be published to a shared hosted desktop, do not publish any other applications to that shared hosted desktop
- Ensure the desktop privileges are only applied to that desktop, and not to other computers
- Enable Session Recording for the application. Also enable other security logging capabilities in the application, and within Windows itself.
- Configure XenApp and XenDesktop to limit features used with the application (for example, clipboard, printer, client drive, and USB redirection)
- Enable any security features of the application. Limit it to match strictly the users' requirements - no more
- Configure security features of Windows to match strictly the users' requirements. This will be a simpler configuration if only that single application is published to the desktop; for example, a restrictive AppLocker configuration can be used. Control access to the file system.

- Plan to reconfigure, upgrade, or replace the application so that desktop privileges are not required in future

These approaches will not remove all security risk from applications that require desktop privileges.

## Manage logon rights

Logon rights are required for both user accounts and computer accounts. As with Microsoft Windows privileges, logon rights continue to be applied to desktops in the usual way: configure logon rights through User Rights Assignment and group memberships through Group Policy.

The Windows logon rights are: log on locally, log on through Remote Desktop Services, log on over the network (access this computer from the network), log on as a batch job, and log on as a service.

For computer accounts, grant computers only the logon rights they require. The logon right "Access this computer from the network" is required:

- At VDAs, for the computer accounts of Delivery Controllers
- At Delivery Controllers, for the computer accounts of VDAs. See [Active Directory OU-based Controller discovery](#).
- At StoreFront servers, for the computer accounts of other servers in the same StoreFront server group

For user accounts, grant users only the logon rights they require.

According to Microsoft, by default the group Remote Desktop Users is granted the logon right "Allow log on through Remote Desktop Services" (except on domain controllers).

Your organization's security policy may state explicitly that this group should be removed from that logon right. Consider the following approach:

- The Virtual Delivery Agent (VDA) for Server OS uses Microsoft Remote Desktop Services. You can configure the Remote Desktop Users group as a restricted group, and control membership of the group via Active Directory group policies. Refer to Microsoft documentation for more information.
- For other components of XenApp and XenDesktop, including the VDA for Desktop OS, the group Remote Desktop Users is not required. So, for those components, the group Remote Desktop Users does not require the logon right "Allow log on through Remote Desktop Services"; you can remove it. Additionally:
  - If you administer those computers via Remote Desktop Services, ensure that all such administrators are already members of the Administrators group.
  - If you do not administer those computers via Remote Desktop Services, consider disabling Remote Desktop Services itself on those computers.

Although it is possible to add users and groups to the login right "Deny logon through Remote Desktop Services", the use of deny logon rights is not generally recommended. Refer to Microsoft documentation for more information.

## Configure user rights

Delivery Controller installation creates the following Windows services:

- Citrix AD Identity Service (NT SERVICE\CitrixADIdentityService): Manages Microsoft Active Directory computer accounts for VMs.

- Citrix Analytics (NT SERVICE\CitrixAnalytics): Collects site configuration usage information for use by Citrix, if this collection been approved by the site administrator. It then submits this information to Citrix, to help improve the product.
- Citrix App Library (NT SERVICE\CitrixAppLibrary): Supports management and provisioning of AppDisks, AppDNA integration, and management of App-V.
- Citrix Broker Service (NT SERVICE\CitrixBrokerService): Selects the virtual desktops or applications that are available to users.
- Citrix Configuration Logging Service (NT SERVICE\CitrixConfigurationLogging): Records all configuration changes and other state changes made by administrators to the site.
- Citrix Configuration Service (NT SERVICE\CitrixConfigurationService): Site-wide repository for shared configuration.
- Citrix Delegated Administration Service (NT SERVICE\CitrixDelegatedAdmin): Manages the permissions granted to administrators.
- Citrix Environment Test Service (NT SERVICE\CitrixEnvTest): Manages self-tests of the other Delivery Controller services.
- Citrix Host Service (NT SERVICE\CitrixHostService): Stores information about the hypervisor infrastructures used in a XenApp or XenDesktop deployment, and also offers functionality used by the console to enumerate resources in a hypervisor pool.
- Citrix Machine Creation Service (NT SERVICE\CitrixMachineCreationService): Orchestrates the creation of desktop VMs.
- Citrix Monitor Service (NT SERVICE\CitrixMonitor): Collects metrics for XenApp or XenDesktop, stores historical information, and provides a query interface for troubleshooting and reporting tools.
- Citrix Storefront Service (NT SERVICE\ CitrixStorefront): Supports management of StoreFront. (It is not part of the StoreFront component itself.)
- Citrix Storefront Privileged Administration Service (NT SERVICE\CitrixPrivilegedService): Supports privileged management operations of StoreFront. (It is not part of the StoreFront component itself.)

Delivery Controller installation also creates the following Windows services. These are also created when installed with other Citrix components:

- Citrix Diagnostic Facility COM Server (NT SERVICE\CdfSvc): Supports the collection of diagnostic information for use by Citrix Support.
- Citrix Telemetry Service (NT SERVICE\CitrixTelemetryService): Collects diagnostic information for analysis by Citrix, such that the analysis results and recommendations can be viewed by administrators to help diagnose issues with the site.

Except for the Citrix Storefront Privileged Administration Service, these services are granted the logon right Log on as a service and the privileges Adjust memory quotas for a process, Generate security audits, and Replace a process level token. You do not need to change these user rights. These privileges are not used by the Delivery Controller and are automatically disabled.

## Configure service settings

Except for the Citrix Storefront Privileged Administration service and the Citrix Telemetry Service, the Delivery Controller Windows services listed above in the "Configure user rights" section are configured to log on as the NETWORK SERVICE identity. Do not alter these service settings.

The Citrix Storefront Privileged Administration service is configured to log on Local System (NT AUTHORITY\SYSTEM). This is required for Delivery Controller StoreFront operations that are not normally available to services (including creating Microsoft IIS sites). Do not alter its service settings.

The Citrix Telemetry Service is configured to log on as its own service-specific identity.

You can disable the Citrix Telemetry Service. Apart from this service, and services that are already disabled, do not disable any other of these Delivery Controller Windows services.

## Deployment scenario security implications

Your user environment can consist either of user devices that are unmanaged by your organization and completely under the control of the user, or of user devices that are managed and administered by your organization. The security considerations for these two environments are generally different.

- **Managed user devices** - Managed user devices are under administrative control; they are either under your own control, or the control of another organization that you trust. You may configure and supply user devices directly to users; alternatively, you may provide terminals on which a single desktop runs in full-screen-only mode. You should follow the general security best practices described above for all managed user devices. This release has the advantage that minimal software is required on a user device.

A managed user device can be set up to be used in full-screen-only mode or in window mode:

- If a user device is configured to be used in full-screen-only mode, users log on to it with the usual Log On To Windows screen. The same user credentials are then used to log on automatically to this release.
- If a user device is configured so that users see their desktop in a window, users first log on to the user device, then log on to this release through a Web site supplied with the release.
- **Unmanaged user devices** - User devices that are not managed and administered by a trusted organization cannot be assumed to be under administrative control. For example, you might permit users to obtain and configure their own devices, but users might not follow the general security best practices described above. This release has the advantage that it is possible to deliver desktops securely to unmanaged user devices. These devices should still have basic antivirus protection that will defeat keylogger and similar input attacks.
- **Data storage considerations** - When using this release, you can prevent users from storing data on user devices that are under their physical control. However, you must still consider the implications of users storing data on desktops. It is not good practice for users to store data on desktops; data should be held on file servers, database servers, or other repositories where it can be appropriately protected.

Your desktop environment may consist of various types of desktops, such as pooled and dedicated desktops:

- Users should never store data on desktops that are shared amongst users, such as pooled desktops.
- If users store data on dedicated desktops, that data should be removed if the desktop is later made available to other users.
- **Mixed-version environments** Mixed-version environments are inevitable during some upgrades. Follow best-practice and minimize the time that Citrix components of different versions co-exist.

In mixed-version environments security policy, for example, may not be uniformly enforced.

**Note:** This is typical of other software products; the use of an earlier version of Active Directory only partially enforces Group Policy with later versions of Windows.

The following scenario describes a security issue that can occur in a specific mixed-version Citrix environment. When Citrix Receiver 1.7 is used to connect to a virtual desktop running the Virtual Delivery Agent in XenApp and XenDesktop 7.6 Feature Pack 2, the policy "Allow file transfer between desktop and client" is enabled in the Site but cannot be disabled by a Delivery Controller running XenApp and XenDesktop 7.1. It does not recognize the policy, which was released only in

the later version of the product. This policy allows users to upload and download files to their virtual desktop – the security issue. To work around this, upgrade the Delivery Controller, or a standalone instance of Studio, to Version 7.6 Feature Pack 2 and then use GP to disable the policy. Alternatively, use local policy on all affected virtual desktops.

## Remote PC Access

Remote PC Access implements the following security features:

- Smart card use is supported.
- When a remote session connects, the office PC's monitor appears as blank.
- Remote PC Access redirects all keyboard and mouse input to the remote session, except CTRL+ALT+DEL and USB-enabled smart cards and biometric devices.
- SmoothRoaming is supported for a single user only.
- When a user has a remote session connected to an office PC, only that user can resume local access of the office PC. To resume local access, the user presses Ctrl-Alt-Del on the local PC and then logs on with the same credentials used by the remote session. The user can also resume local access by inserting a smart card or leveraging biometrics, if your system has appropriate third-party Credential Provider integration.

This default behavior can be overridden by enabling Fast User Switching via Group Policy Objects (GPOs) or by editing the registry.

- By default, Remote PC Access supports automatic assignment of multiple users to a VDA. In XenDesktop 5.6 Feature Pack 1, administrators could override this behavior using the `RemotePCAccess.ps1` PowerShell script. This release uses a registry entry to allow or prohibit multiple automatic remote PC assignments; this setting applies to the entire Site. Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

To restrict automatic assignments to a single user:

1. Set the following registry entry on each Controller in the Site:

HKEY\_LOCAL\_MACHINE\Software\Citrix\DesktopServer

Name: AllowMultipleRemotePCAssignments

Type: REG\_DWORD

Data: 0 = Disable multiple user assignment, 1 = (Default) Enable multiple user assignment.

2. If there are any existing user assignments, remove them using SDK commands for the VDA to subsequently be eligible for a single automatic assignment.
  1. Remove all assigned users from the VDA: `$machine.AssociatedUserNames | % { Remove-BrokerUser-Name $_ - Machine $machine }`
  2. Remove the VDA from the Delivery Group: `$machine | Remove-BrokerMachine -DesktopGroup $desktopGroup`
  3. Restart the physical office PC.

# 委派管理

May 28, 2016

The Delegated Administration model offers the flexibility to match how your organization wants to delegate administration activities, using role and object-based control. Delegated Administration accommodates deployments of all sizes, and allows you to configure more permission granularity as your deployment grows in complexity. Delegated Administration uses three concepts: administrators, roles, and scopes.

- **Administrators** — An administrator represents an individual person or a group of people identified by their Active Directory account. Each administrator is associated with one or more role and scope pairs.
- **Roles** — A role represents a job function, and has defined permissions associated with it. For example, the Delivery Group Administrator role has permissions such as 'Create Delivery Group' and 'Remove Desktop from Delivery Group.' An administrator can have multiple roles for a Site, so a person could be a Delivery Group Administrator and a Machine Catalog Administrator. Roles can be built-in or custom.

The built-in roles are:

Role	Permissions
Full Administrator	Can perform all tasks and operations. A Full Administrator is always combined with the All scope.
Read Only Administrator	Can see all objects in specified scopes as well as global information, but cannot change anything. For example, a Read Only Administrator with Scope=London can see all global objects (such as Configuration Logging) and any London-scoped objects (for example, London Delivery Groups). However, that administrator cannot see objects in the New York scope (assuming that the London and New York scopes do not overlap).
Help Desk Administrator	Can view Delivery Groups, and manage the sessions and machines associated with those groups. Can see the Machine Catalog and host information for the Delivery Groups being monitored, and can also perform session management and machine power management operations for the machines in those Delivery Groups.
Machine Catalog Administrator	Can create and manage Machine Catalogs and provision the machines into them. Can build Machine Catalogs from the virtualization infrastructure, Provisioning Services, and physical machines. This role can manage base images and install software, but cannot assign applications or desktops to users.
Delivery Group Administrator	Can deliver applications, desktops, and machines; can also manage the associated sessions. Can also manage application and desktop configurations such as policies and power management settings.
Host Administrator	Can manage host connections and their associated resource settings. Cannot deliver machines, applications, or desktops to users.

In certain product editions, you can create custom roles to match the requirements of your organization, and delegate permissions with more detail. You can use custom roles to allocate permissions at the granularity of an action or task in a console.

- **Scopes** — A scope represents a collection of objects. Scopes are used to group objects in a way that is relevant to your

organization (for example, the set of Delivery Groups used by the Sales team). Objects can be in more than one scope; you can think of objects being labeled with one or more scopes. There is one built-in scope: 'All,' which contains all objects. The Full Administrator role is always paired with the All scope.

### Example

Company XYZ decided to manage applications and desktops based on their department (Accounts, Sales, and Warehouse) and their desktop operating system (Windows 7 or Windows 8). The administrator created five scopes, then labeled each Delivery Group with two scopes: one for the department where they are used and one for the operating system they use.

The following administrators were created:

Administrator	Roles	Scopes
domain/fred	Full Administrator	All (the Full Administrator role always has the All scope)
domain/rob	Read Only Administrator	All
domain/heidi	Read Only Administrator Help Desk Administrator	All Sales
domain/warehouseadmin	Help Desk Administrator	Warehouse
domain/peter	Delivery Group Administrator Machine Catalog Administrator	Win7

- Fred is a Full Administrator and can view, edit, and delete all objects in the system.
- Rob can view all objects in the Site but cannot edit or delete them.
- Heidi can view all objects and can perform help desk tasks on Delivery Groups in the Sales scope. This allows her to manage the sessions and machines associated with those groups; she cannot make changes to the Delivery Group, such as adding or removing machines.
- Anyone who is a member of the warehouseadmin Active Directory security group can view and perform help desk tasks on machines in the Warehouse scope.
- Peter is a Windows 7 specialist and can manage all Windows 7 Machine Catalogs and can deliver Windows 7 applications, desktops, and machines, regardless of which department scope they are in. The administrator considered making Peter a Full Administrator for the Win7 scope; however, she decided against this, because a Full Administrator also has full rights over all objects that are not scoped, such as 'Site' and 'Administrator.'

### How to use Delegated Administration

Generally, the number of administrators and the granularity of their permissions depends on the size and complexity of the deployment.

- In small or proof-of-concept deployments, one or a few administrators do everything; there is no delegation. In this case, create each administrator with the built-in Full Administrator role, which has the All scope.
- In larger deployments with more machines, applications, and desktops, more delegation is needed. Several administrators

might have more specific functional responsibilities (roles). For example, two are Full Administrators, and others are Help Desk Administrators. Additionally, an administrator might manage only certain groups of objects (scopes), such as machine catalogs. In this case, create new scopes, plus administrators with one of the built-in roles and the appropriate scopes.

- Even larger deployments might require more (or more specific) scopes, plus different administrators with unconventional roles. In this case, edit or create additional scopes, create custom roles, and create each administrator with a built-in or custom role, plus existing and new scopes.

For flexibility and ease of configuration, you can create new scopes when you create an administrator. You can also specify scopes when creating or editing Machine Catalogs or connections.

## Create and manage administrators

When you create a Site as a local administrator, your user account automatically becomes a Full Administrator with full permissions over all objects. After a Site is created, local administrators have no special privileges.

The Full Administrator role always has the All scope; you cannot change this.

By default, an administrator is enabled. Disabling an administrator might be necessary if you are creating the new administrator now, but that person will not begin administration duties until later. For existing enabled administrators, you might want to disable several of them while you are reorganizing your object/scopes, then re-enable them when you are ready to go live with the updated configuration. You cannot disable a Full Administrator if it will result in there being no enabled Full Administrator. The enable/disable check box is available when you create, copy, or edit an administrator.

When you delete a role/scope pair while copying, editing, or deleting an administrator, it deletes only the relationship between the role and the scope for that administrator; it does not delete either the role or the scope, nor does it affect any other administrator who is configured with that role/scope pair.

To manage administrators, click Configuration > Administrators in the Studio navigation pane, and then click the Administrators tab in the upper middle pane.

- To create an administrator, click Create new Administrator in the Actions pane. Type or browse to the user account name, select or create a scope, and select a role. The new administrator is enabled by default; you can change this.
- To copy an administrator, select the administrator in the middle pane and then click Copy Administrator in the Actions pane. Type or browse to the user account name. You can select and then edit or delete any of the role/scope pairs, and add new ones. The new administrator is enabled by default; you can change this.
- To edit an administrator, select the administrator in the middle pane and then click Edit Administrator in the Actions pane. You can edit or delete any of the role/scope pairs, and add new ones.
- To delete an administrator, select the administrator in the middle pane and then click Delete Administrator in the Actions pane. You cannot delete a Full Administrator if it will result in there being no enabled Full Administrator.

## Create and manage roles

Role names can contain up to 64 Unicode characters; they cannot contain the following characters: \ (backslash), / (forward slash), ; (semicolon), : (colon), # (pound sign), , (comma), \* (asterisk), ? (question mark), = (equal sign), < (left arrow), > (right arrow), | (pipe), [ ] (left or right bracket), ( ) (left or right parenthesis), " (quotation marks), and ' (apostrophe). Descriptions can contain up to 256 Unicode characters.

You cannot edit or delete a built-in role. You cannot delete a custom role if any administrator is using it.

Note: Only certain product editions support custom roles. Editions that do not support custom roles do not have related entries in the Actions pane.

To manage roles, click Configuration > Administrators in the Studio navigation pane, and then click the Roles tab in the upper middle pane.

- To view role details, select the role in the middle pane. The lower portion of the middle pane lists the object types and associated permissions for the role. Click the Administrators tab in the lower pane to display a list of administrators who currently have this role.
- To create a custom role, click Create new Role in the Actions pane. Enter a name and description. Select the object types and permissions.
- To copy a role, select the role in the middle pane and then click Copy Role in the Actions pane. Change the name, description, object types, and permissions, as needed.
- To edit a custom role, select the role in the middle pane and then click Edit Role in the Actions pane. Change the name, description, object types, and permissions, as needed.
- To delete a custom role, select the role in the middle pane and then click Delete Role in the Actions pane. When prompted, confirm the deletion.

## Create and manage scopes

When you create a Site, the only available scope is the 'All' scope, which cannot be deleted.

You can create scopes using the procedure below. You can also create scopes when you create an administrator; each administrator must be associated with at least one role and scope pair. When you are creating or editing desktops, machine catalogs, applications, or hosts, you can add them to an existing scope; if you do not add them to a scope, they remain part of the 'All' scope.

Site creation cannot be scoped, nor can Delegated Administration objects (scopes and roles). However, objects you cannot scope are included in the 'All' scope. (Full Administrators always have the All scope.) Machines, power actions, desktops, and sessions are not directly scoped; administrators can be allocated permissions over these objects through the associated machine catalogs or Delivery Groups.

Scope names can contain up to 64 Unicode characters; they cannot include the following characters: \ (backslash), / (forward slash), ; (semicolon), : (colon), # (pound sign), , (comma), \* (asterisk), ? (question mark), = (equal sign), < (left arrow), > (right arrow), | (pipe), [ ] (left or right bracket), ( ) (left or right parenthesis), " (quotation marks), and ' (apostrophe).

Descriptions can contain up to 256 Unicode characters.

When you copy or edit a scope, keep in mind that removing objects from the scope can make those objects inaccessible to the administrator. If the edited scope is paired with one or more roles, ensure that the scope updates you make do not make any role/scope pair unusable.

To manage scopes, click Configuration > Administrators in the Studio navigation pane, and then click the Scopes tab in the upper middle pane.

- To create a scope, click Create new Scope in the Actions pane. Enter a name and description. To include all objects of a particular type (for example, Delivery Groups), select the object type. To include specific objects, expand the type and then select individual objects (for example, Delivery Groups used by the Sales team).
- To copy a scope, select the scope in the middle pane and then click Copy Scope in the Actions pane. Enter a name and description. Change the object types and objects, as needed.
- To edit a scope, select the scope in the middle pane and then click Edit Scope in the Actions pane. Change the name, description, object types, and objects, as needed.
- To delete a scope, select the scope in the middle pane and then click Delete Scope in the Actions pane. When prompted, confirm the deletion.

## Create reports

You can create two types of Delegated Administration reports:

- An HTML report that lists the role/scope pairs associated with an administrator, plus the individual permissions for each type of object (for example, Delivery Groups and Machine Catalogs). You generate this report from Studio.

To create this report, click Configuration > Administrators in the navigation pane. Select an administrator in the middle pane and then click Create Report in the Actions pane.

You can also request this report when creating, copying, or editing an administrator.

- An HTML or CSV report that maps all built-in and custom roles to permissions. You generate this report by running a PowerShell script named OutputPermissionMapping.ps1.

To run this script, you must be a Full Administrator, a Read Only Administrator, or a custom administrator with permission to read roles. The script is located in: Program

Files\Citrix\DelegatedAdmin\SnapIn\Citrix.DelegatedAdmin.Admin.V1\Scripts\.

Syntax:

OutputPermissionMapping.ps1 [-Help] [-Csv] [-Path <string>] [-AdminAddress <string>] [-Show] [<CommonParameters>]

Parameter	Description
-Help	Displays script help.
-Csv	Specifies CSV output. Default = HTML
-Path <string>	Where to write the output. Default = stdout
-AdminAddress <string>	IP address or host name of the Delivery Controller to connect to. Default = localhost
-Show	(Valid only when the -Path parameter is also specified) When you write the output to a file, -Show causes the output to be opened in an appropriate program, such as a web browser.
<CommonParameters>	Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer, and OutVariable. For details, see the Microsoft documentation.

The following example writes an HTML table to a file named Roles.html and opens the table in a web browser.

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\  
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"  
-Path Roles.html -Show
```

The following example writes a CSV table to a file named Roles.csv. The table is not displayed.

```
& "$env:ProgramFiles\Citrix\DelegatedAdmin\SnapIn\  
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1"  
-CSV -Path Roles.csv
```

From a Windows command prompt, the preceding example command is:

```
powershell -command "& '%ProgramFiles%\Citrix\DelegatedAdmin\SnapIn\  
Citrix.DelegatedAdmin.Admin.V1\Scripts\OutputPermissionMapping.ps1'  
-CSV -Path Roles.csv"
```

# 智能卡

Aug 29, 2016

Smart cards and equivalent technologies are supported within the guidelines described in this article. To use smart cards with XenApp or XenDesktop:

- Understand your organization's security policy concerning the use of smart cards. These policies might, for example, state how smart cards are issued and how users should safeguard them. Some aspects of these policies might need to be reassessed in a XenApp or XenDesktop environment.
- Determine which user device types, operating systems, and published applications are to be used with smart cards.
- Familiarize yourself with smart card technology and your selected smart card vendor hardware and software.
- Know how to deploy digital certificates in a distributed environment.

## Types of smart cards

Enterprise and consumer smart cards have the same dimensions, electrical connectors, and fit the same smart card readers.

Smart cards for enterprise use contain digital certificates. These smart cards support Windows logon, and can also be used with applications for digital signing and encryption of documents and e-mail. XenApp and XenDesktop support these uses.

Smart cards for consumer use do not contain digital certificates; they contain a shared secret. These smart cards can support payments (such as a chip-and-signature or chip-and-PIN credit card). They do not support Windows logon or typical Windows applications. Specialized Windows applications and a suitable software infrastructure (including, for example, a connection to a payment card network) are needed for use with these smart cards. Contact your Citrix representative for information on supporting these specialized applications on XenApp or XenDesktop.

For enterprise smart cards, there are compatible equivalents that can be used in a similar way.

- A smart card-equivalent USB token connects directly to a USB port. These USB tokens are usually the size of a USB flash drive, but can be as small as a SIM card used in a mobile phone. They appear as the combination of a smart card plus a USB smart card reader.
- A virtual smart card using a Windows Trusted Platform Module (TPM) appears as a smart card. These virtual smart cards are supported for Windows 8 and Windows 10, using Citrix Receiver minimum 4.3.
  - Versions of XenApp and XenDesktop earlier than 7.6 FP3 do not support virtual smart cards.
  - For more information on virtual smart cards, see [Virtual Smart Card Overview](#).

**Note:** The term "virtual smart card" is also used to describe a digital certificate simply stored on the user computer. These digital certificates are not strictly equivalent to smart cards.

XenApp and XenDesktop smart card support is based on the Microsoft Personal Computer/Smart Card (PC/SC) standard specifications. A minimum requirement is that smart cards and smart card devices must be supported by the underlying Windows operating system and must be approved by the Microsoft Windows Hardware Quality Labs (WHQL) to be used on computers running qualifying Windows operating systems. See the Microsoft documentation for additional information about hardware PC/SC compliance. Other types of user devices may comply with the PS/SC standard. For more information, refer to the Citrix Ready program at <http://www.citrix.com/ready/>.

Usually, a separate device driver is needed for each vendor's smart card or equivalent. However, if smart cards conform to a

standard such as the NIST Personal Identity Verification (PIV) standard, it may be possible to use a single device driver for a range of smart cards. The device driver must be installed on both the user device and the Virtual Delivery Agent (VDA). The device driver is often supplied as part of a smart card middleware package available from a Citrix partner; the smart card middleware package will offer advanced features. The device driver may also be described as a Cryptographic Service Provider (CSP), Key Storage Provider (KSP), or minidriver.

The following smart card and middleware combinations for Windows systems have been tested by Citrix as representative examples of their type. However, other smart cards and middleware can also be used. For more information about Citrix-compatible smart cards and middleware, see <http://www.citrix.com/ready>.

<b>Middleware</b>	<b>Matching cards</b>
ActivClient 7.0 (DoD mode enabled)	DoD CAC card
ActivClient 7.0 in PIV mode	NIST PIV card
Microsoft mini driver	NIST PIV card
Gemalto Mini Driver for .NET card	Gemalto .NET v2+
Microsoft native driver	Virtual Smart Cards (TPM)

For information about smart card usage with other types of devices, see the Citrix Receiver documentation for that device.

#### Remote PC Access

Smart cards are supported only for remote access to physical office PCs running Windows 10, Windows 8 or Windows 7; smart cards are not supported for office PCs running Windows XP.

The following smart cards were tested with Remote PC Access:

<b>Middleware</b>	<b>Matching cards</b>
Gemalto .NET minidriver	Gemalto .NET v2+
ActivIdentity ActivClient 6.2	NIST PIV
ActivIdentity ActivClient 6.2	CAC
Microsoft minidriver	NIST PIV
Microsoft native driver	Virtual smart cards

# Types of smart card readers

A smart card reader may be built in to the user device, or be separately attached to the user device (usually via USB or Bluetooth). Contact card readers that comply with the USB Chip/Smart Card Interface Devices (CCID) specification are supported. They contain a slot or swipe into which the user inserts the smart card. The Deutsche Kreditwirtschaft (DK) standard defines four classes of contact card readers.

- Class 1 smart card readers are the most common, and usually just contain a slot. Class 1 smart card readers are supported, usually with a standard CCID device driver supplied with the operating system.
- Class 2 smart card readers also contain a secure keypad that cannot be accessed by the user device. Class 2 smart card readers may be built into a keyboard with an integrated secure keypad. For class 2 smart card readers, contact your Citrix representative; a reader-specific device driver may be required to enable the secure keypad capability.
- Class 3 smart card readers also contain a secure display. Class 3 smart card readers are not supported.
- Class 4 smart card readers also contain a secure transaction module. Class 4 smart card readers are not supported.

**Note:** The smart card reader class is unrelated to the USB device class.

Smart card readers must be installed with a corresponding device driver on the user device.

## User experience

Smart card support is integrated into XenApp and XenDesktop, using a specific ICA/HDX smart card virtual channel that is enabled by default.

**Important:** Do not use generic USB redirection for smart card readers. This is disabled by default for smart card readers, and is not supported if enabled.

Multiple smart cards and multiple readers can be used on the same user device, but if pass-through authentication is in use, only one smart card must be inserted when the user starts a virtual desktop or application. When a smart card is used within an application (for example, for digital signing or encryption functions), there might be additional prompts to insert a smart card or enter a PIN. This can occur if more than one smart card has been inserted at the same time.

- If users are prompted to insert a smart card when the smart card is already in the reader, they should select Cancel.
- If users are prompted for the PIN, they should enter the PIN again.

If you are using hosted applications running on Windows Server 2008 or 2008 R2 and with smart cards requiring the Microsoft Base Smart Card Cryptographic Service Provider, you might find that if a user runs a smart card transaction, all other users who use a smart card in the logon process are blocked. For further details and a hotfix for this issue, see <http://support.microsoft.com/kb/949538>.

You can reset PINs using a card management system or vendor utility.

## Before deploying smart cards

- Obtain a device driver for the smart card reader and install it on the user device. Many smart card readers can use the CCID device driver supplied by Microsoft.
- Obtain a device driver and cryptographic service provider (CSP) software from your smart card vendor, and install them on both user devices and virtual desktops. The driver and CSP software must be compatible with XenApp and XenDesktop; check the vendor documentation for compatibility. For virtual desktops using smart cards that support and use the minidriver model, smart card minidrivers should download automatically, but you can obtain them from <http://catalog.update.microsoft.com> or from your vendor. Additionally, if PKCS#11 middleware is required, obtain it from the card vendor.
- **Important:** Citrix recommends that you install and test the drivers and CSP software on a physical computer before installing Citrix software.
- Add the Citrix Receiver for Web URL to the Trusted Sites list for users who work with smart cards in Internet Explorer with Windows 10. In Windows 10, Internet Explorer does not run in protected mode by default for trusted sites.
- Ensure that your public key infrastructure (PKI) is configured appropriately. This includes ensuring that certificate-to-account mapping is correctly configured for Active Directory environment and that user certificate validation can be performed successfully.
- Ensure your deployment meets the system requirements of the other Citrix components used with smart cards, including Citrix Receiver and StoreFront.
- Ensure access to the following servers in your Site:
  - The Active Directory domain controller for the user account that is associated with a logon certificate on the smart card
  - Delivery Controller
  - Citrix StoreFront
  - Citrix NetScaler Gateway/Citrix Access Gateway 10.x
  - VDA
  - (Optional for Remote PC Access): Microsoft Exchange Server

## Enable smart card use

**Step 1.** Issue smart cards to users according to your card issuance policy.

**Step 2.** (Optional) Set up the smart cards to enable users for Remote PC Access.

**Step 3.** Install and configure the Delivery Controller and StoreFront (if not already installed) for smart card remoting.

**Step 4.** Enable StoreFront for smart card use. For details, see Configure smart card authentication in the StoreFront documentation.

**Step 5.** Enable NetScaler Gateway/Access Gateway for smart card use. For details, see Configuring Authentication and Authorization and Configuring Smart Card Access with the Web Interface in the NetScaler documentation.

**Step 6.** Enable VDAs for smart card use.

- Ensure the VDA has the required applications and updates.
- Install the middleware.
- Set up smart card remoting, enabling the communication of smart card data between Citrix Receiver on a user device and a virtual desktop session.

**Step 7.** Enable user devices (including domain-joined or non-domain-joined machines) for smart card use. See Configure

smart card authentication in the StoreFront documentation for details.

- Import the certificate authority root certificate and the issuing certificate authority certificate into the device's keystore.
- Install your vendor's smart card middleware.
- Install and configure Citrix Receiver for Windows, being sure to import icaclient.adm using the Group Policy Management Console and enable smart card authentication.

**Step 8.** Test the deployment. Ensure that the deployment is configured correctly by launching a virtual desktop with a test user's smart card. Test all possible access mechanisms (for example, accessing the desktop through Internet Explorer and Citrix Receiver).

# 智能卡部署

May 28, 2016

The following types of smart card deployments are supported by this product version and by mixed environments containing this version. Other configurations might work but are not supported.

Type	StoreFront connectivity
Local domain-joined computers	Directly connected
Remote access from domain-joined computers	Connected through NetScaler Gateway
Non-domain-joined computers	Directly connected
Remote access from non-domain-joined computers	Connected through NetScaler Gateway
Non-domain-joined computers and thin clients accessing the Desktop Appliance site	Connected through Desktop Appliance sites
Domain-joined computers and thin clients accessing StoreFront through the XenApp Services URL	Connected through XenApp Services URLs

The deployment types are defined by the characteristics of the user device to which the smart card reader is connected:

- Whether the device is domain-joined or non-domain-joined.
- How the device is connected to StoreFront.
- What software is used to view virtual desktops and applications.

In addition, smart card-enabled applications such as Microsoft Word, and Microsoft Excel can be used in these deployments. Those applications allow users to digitally sign or encrypt documents.

## Bimodal authentication

Where possible in each of these deployments, Receiver supports bimodal authentication by offering the user a choice between using a smart card and entering their user name and password. This is useful if the smart card cannot be used (for example, the user has left it at home or the logon certificate has expired).

Because users of non-domain-joined devices log on to Receiver for Windows directly, you can enable users to fall back to explicit authentication. If you configure bimodal authentication, users are initially prompted to log on using their smart cards and PINs but have the option to select explicit authentication if they experience any issues with their smart cards.

If you deploy NetScaler Gateway, users log on to their devices and are prompted by Receiver for Windows to authenticate to NetScaler Gateway. This applies to both domain-joined and non-domain-joined devices. Users can log on to NetScaler Gateway using either their smart cards and PINs, or with explicit credentials. This enables you to provide users with bimodal authentication for NetScaler Gateway logons. Configure pass-through authentication from NetScaler Gateway to StoreFront and delegate credential validation to NetScaler Gateway for smart card users so that users are silently authenticated to StoreFront.

## Multiple Active Directory forest considerations

In a Citrix environment, smart cards are supported within a single forest. Smart card logons across forests require a direct two-way forest trust to all user accounts. More complex multi-forest deployments involving smart cards (that is, where trusts are only one-way or of different types) are not supported.

You can use smart cards in a Citrix environment that includes remote desktops. This feature can be installed locally (on the user device that the smart card is connected to) or remotely (on the remote desktop that the user device connects to).

### Smart card removal policy

The smart card removal policy set on the product determines what happens if you remove the smart card from the reader during a session. The smart card removal policy is configured through and handled by the Windows operating system.

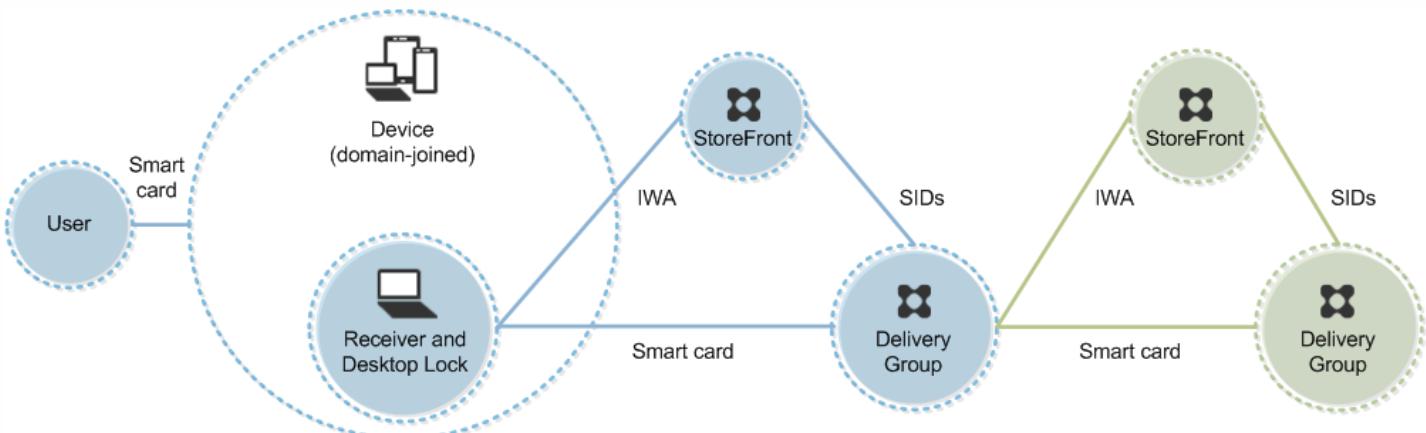
Policy setting	Desktop behavior
No action	No action.
Lock workstation	The desktop session is disconnected and the virtual desktop is locked.
Force logoff	The user is forced to log off. If the network connection is lost and this setting is enabled, the session may be logged off and the user may lose data.
Disconnect if a remote Terminal Services session	The session is disconnected and the virtual desktop is locked.

### Certificate revocation checking

If certificate revocation checking is enabled and a user inserts a smart card with an invalid certificate into a card reader, the user cannot authenticate or access the desktop or application related to the certificate. For example, if the invalid certificate is used for email decryption, the email remains encrypted. If other certificates on the card, such as ones used for authentication, are still valid, those functions remain active.

### Deployment example: domain-joined computers

This deployment involves domain-joined user devices that run the Desktop Viewer and connect directly to StoreFront.



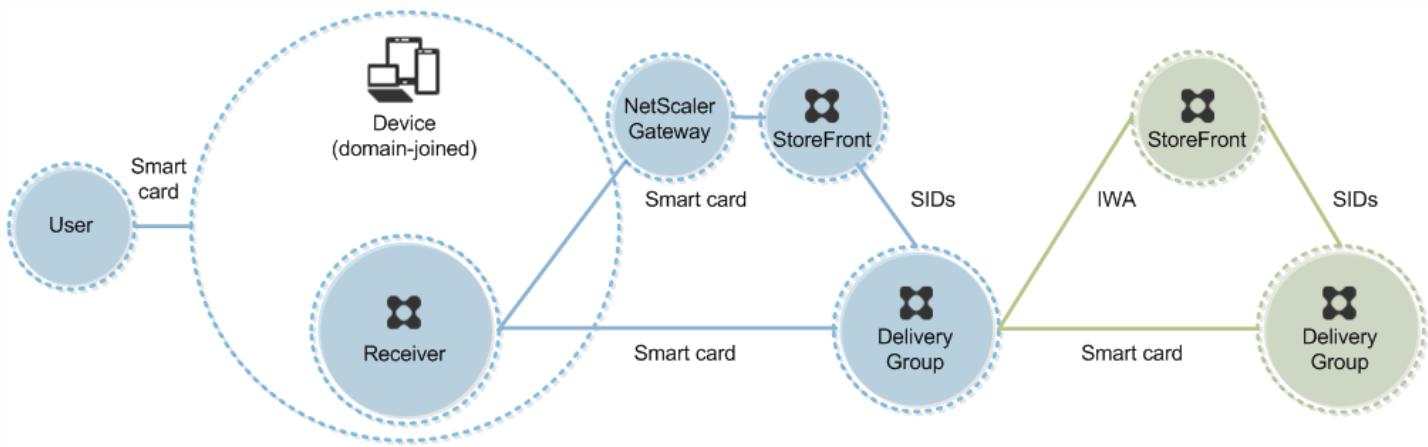
A user logs on to a device using a smart card and PIN. Receiver authenticates the user to a Storefront server using

Integrated Windows Authentication (IWA). StoreFront passes the user security identifiers (SIDs) to XenApp or XenDesktop. When the user starts a virtual desktop or application, the user is not prompted for a PIN again because the single sign-on feature is configured on Receiver.

This deployment can be extended to a double-hop with the addition of a second StoreFront server and a server hosting applications. A Receiver from the virtual desktop authenticates to the second StoreFront server. Any authentication method can be used for this second connection. The configuration shown for the first hop can be reused in the second hop or used in the second hop only.

#### Deployment example: remote access from domain-joined computers

This deployment involves domain-joined user devices that run the Desktop Viewer and connect to StoreFront through NetScaler Gateway/Access Gateway.



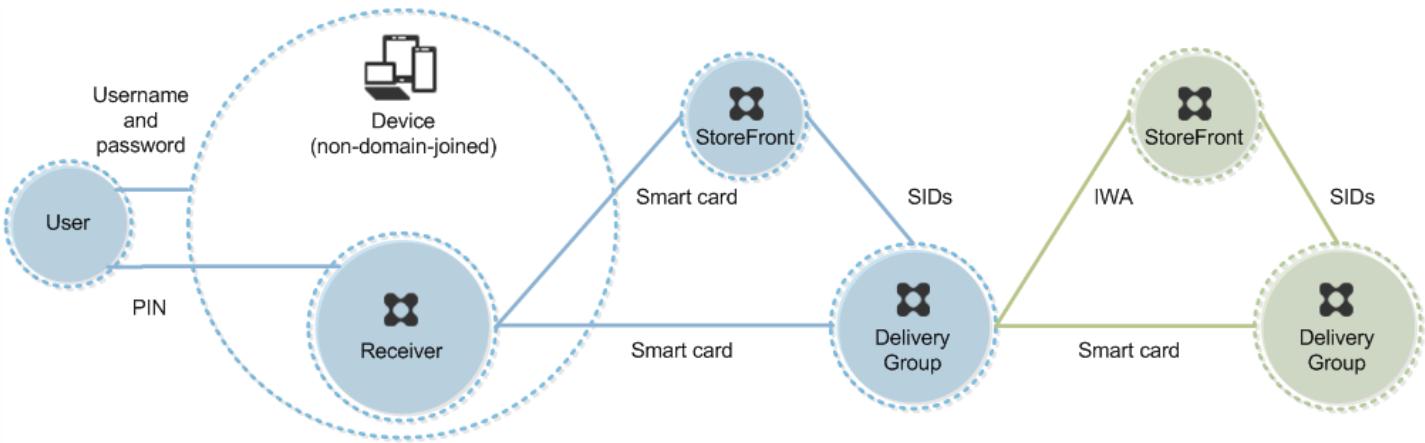
A user logs on to a device using a smart card and PIN, and then logs on again to NetScaler Gateway/Access Gateway. This second logon can be with either the smart card and PIN or a user name and password because Receiver allows bimodal authentication in this deployment.

The user is automatically logged on to StoreFront, which passes the user security identifiers (SIDs) to XenApp or XenDesktop. When the user starts a virtual desktop or application, the user is not prompted again for a PIN because the single sign-on feature is configured on Receiver.

This deployment can be extended to a double-hop with the addition of a second StoreFront server and a server hosting applications. A Receiver from the virtual desktop authenticates to the second StoreFront server. Any authentication method can be used for this second connection. The configuration shown for the first hop can be reused in the second hop or used in the second hop only.

#### Deployment example: non-domain-joined computers

This deployment involves non-domain-joined user devices that run the Desktop Viewer and connect directly to StoreFront.



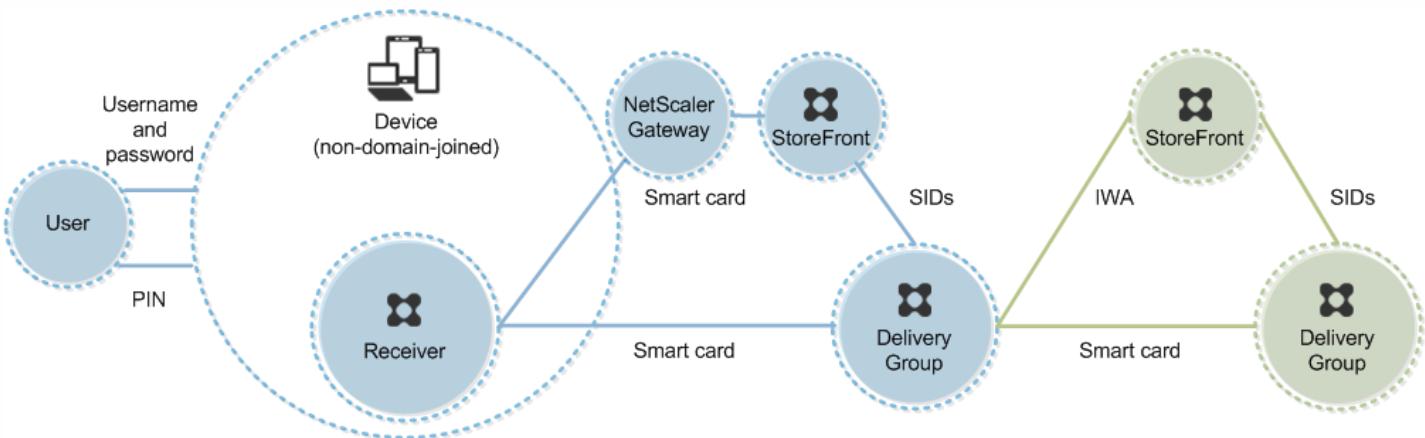
A user logs on to a device. Typically, the user enters a user name and password but, since the device is not joined to a domain, credentials for this logon are optional. Because bimodal authentication is possible in this deployment, Receiver prompts the user either for a smart card and PIN or a user name and password. Receiver then authenticates to Storefront.

StoreFront passes the user security identifiers (IDs) to XenApp or XenDesktop. When the user starts a virtual desktop or application, the user is prompted for a PIN again because the single sign-on feature is not available in this deployment.

This deployment can be extended to a double-hop with the addition of a second StoreFront server and a server hosting applications. A Receiver from the virtual desktop authenticates to the second StoreFront server. Any authentication method can be used for this second connection. The configuration shown for the first hop can be reused in the second hop or used in the second hop only.

#### Deployment example: remote access from non-domain-joined computers

This deployment involves non-domain-joined user devices that run the Desktop Viewer and connect directly to StoreFront.



A user logs on to a device. Typically, the user enters a user name and password but, since the device is not joined to a domain, credentials for this logon are optional. Because bimodal authentication is possible in this deployment, Receiver prompts the user either for a smart card and PIN or a user name and password. Receiver then authenticates to Storefront.

StoreFront passes the user security identifiers (IDs) to XenApp or XenDesktop. When the user starts a virtual desktop or application, the user is prompted for a PIN again because the single sign-on feature is not available in this deployment.

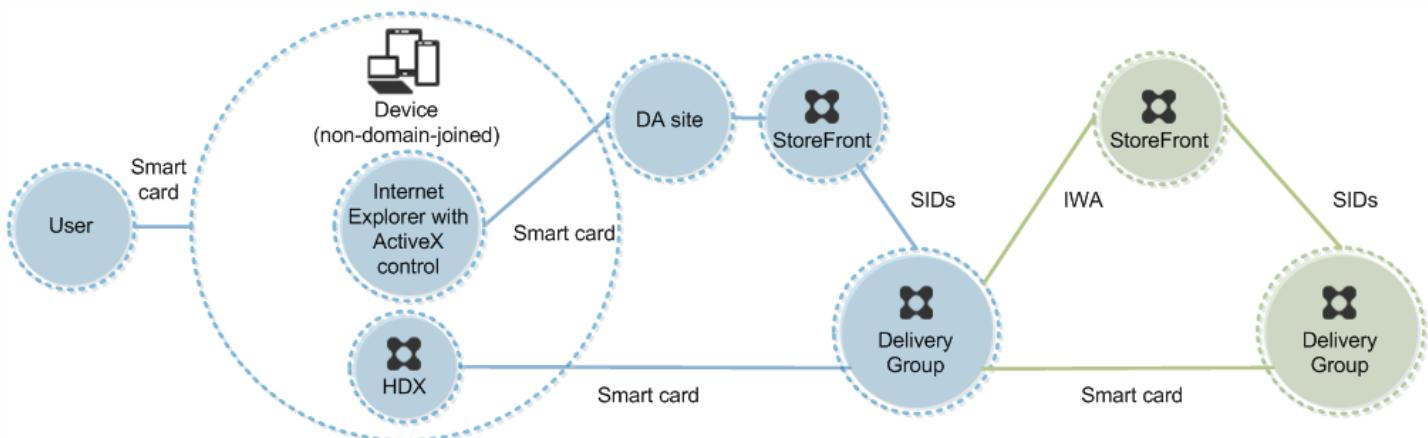
This deployment can be extended to a double-hop with the addition of a second StoreFront server and a server hosting

applications. A Receiver from the virtual desktop authenticates to the second StoreFront server. Any authentication method can be used for this second connection. The configuration shown for the first hop can be reused in the second hop or used in the second hop only.

**Deployment example: non-domain-joined computers and thin clients accessing the Desktop Appliance site**

This deployment involves non-domain-joined user devices that may run the Desktop Lock and connect to StoreFront through Desktop Appliance sites.

The Desktop Lock is a separate component that is released with XenApp, XenDesktop, and VDI-in-a-Box. It is an alternative to the Desktop Viewer and is designed mainly for repurposed Windows computers and Windows thin clients. The Desktop Lock replaces the Windows shell and Task Manager in these user devices, preventing users from accessing the underlying devices. With the Desktop Lock, users can access Windows Server Machine desktops and Windows Desktop Machine desktops. Installation of Desktop Lock is optional.



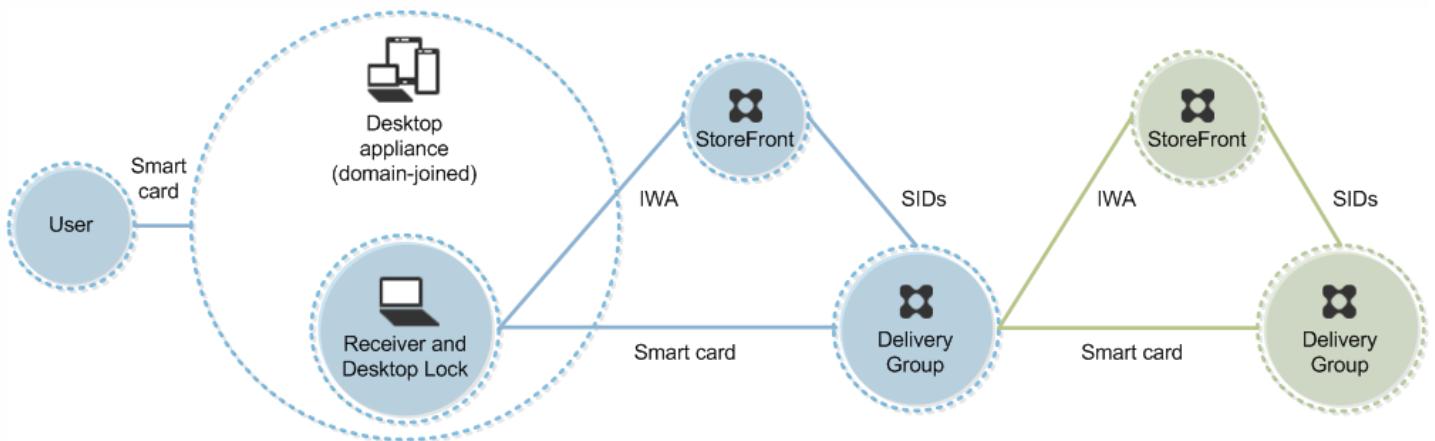
A user logs on to a device with a smart card. If Desktop Lock is running on the device, the device is configured to launch a Desktop Appliance site through Internet Explorer running in Kiosk Mode. An ActiveX control on the site prompts the user for a PIN, and sends it to StoreFront. StoreFront passes the user security identifiers (IDs) to XenApp or XenDesktop. The first available desktop in the alphabetical list in an assigned Desktop Group starts.

This deployment can be extended to a double-hop with the addition of a second StoreFront server and a server hosting applications. A Receiver from the virtual desktop authenticates to the second StoreFront server. Any authentication method can be used for this second connection. The configuration shown for the first hop can be reused in the second hop or used in the second hop only.

**Deployment example: domain-joined computers and thin clients accessing StoreFront through the XenApp Services URL**

This deployment involves domain-joined user devices that run the Desktop Lock and connect to StoreFront through XenApp Services URLs.

The Desktop Lock is a separate component that is released with XenApp, XenDesktop, and VDI-in-a-Box. It is an alternative to the Desktop Viewer and is designed mainly for repurposed Windows computers and Windows thin clients. The Desktop Lock replaces the Windows shell and Task Manager in these user devices, preventing users from accessing the underlying devices. With the Desktop Lock, users can access Windows Server Machine desktops and Windows Desktop Machine desktops. Installation of Desktop Lock is optional.



A user logs on to a device using a smart card and PIN. If Desktop Lock is running on the device, it authenticates the user to a Storefront server using Integrated Windows Authentication (IWA). StoreFront passes the user security identifiers (SIDs) to XenApp or XenDesktop. When the user starts a virtual desktop, the user is not prompted for a PIN again because the single sign-on feature is configured on Receiver.

This deployment can be extended to a double-hop with the addition of a second StoreFront server and a server hosting applications. A Receiver from the virtual desktop authenticates to the second StoreFront server. Any authentication method can be used for this second connection. The configuration shown for the first hop can be reused in the second hop or used in the second hop only.

# 使用智能卡进行直通身份验证和单点登录

Aug 30, 2017

## Pass-through authentication

Pass-through authentication with smart cards to virtual desktops is supported on user devices running Windows 10, and Windows 8 and Windows 7 SP1 Enterprise and Professional Editions.

Pass-through authentication with smart cards to hosted applications is supported on servers running Windows Server 2008 and Windows Server 2012.

To use pass-through authentication with smart cards hosted applications, ensure you enable the use of Kerberos when you configure Pass-through with smartcard as the authentication method for the site.

Note: The availability of pass-through authentication with smart cards depends on many factors including, but not limited to:

- Your organization's security policies regarding pass-through authentication.
- Middleware type and configuration.
- Smart card reader types.
- Middleware PIN caching policy.

Pass-through authentication with smart cards is configured on Citrix StoreFront. See the StoreFront documentation for details.

## Single sign-on

Single sign-on is a Citrix feature that implements pass-through authentication with virtual desktop and application launches. You can use this feature in domain-joined, direct-to-StoreFront and domain-joined, NetScaler-to-StoreFront smart card deployments to reduce the number of times that users enter their PIN. To use single sign-on in these deployment types, edit the following parameters in the default.ica file, which is located on the StoreFront server:

- Domain-joined, direct-to-StoreFront smart card deployments — Set DisableCtrlAltDel to Off
- Domain-joined, NetScaler-to-StoreFront smart card deployments — Set UseLocalUserAndPassword to On

For more instructions on setting these parameters, see the StoreFront or NetScaler Gateway documentation.

The availability of single sign-on functionality depends on many factors including, but not limited to:

- Your organization's security policies regarding single sign-on.
- Middleware type and configuration.
- Smart card reader types.
- Middleware PIN caching policy.

Note: When the user logs on to the Virtual Delivery Agent (VDA) on a machine with an attached smart card reader, a Windows tile may appear representing the previous successful mode of authentication, such as smart card or password. As a result, when single sign-on is enabled, the single sign-on tile may appear. To log on, the user must select Switch Users to select another tile because the single sign-on tile will not work.

# SSL

May 28, 2016

Configuring a XenApp or XenDesktop Site to use the Secure Sockets Layer (SSL) security protocol includes the following procedures:

- Obtain, install, and register a server certificate on all Delivery Controllers, and configure a port with the SSL certificate.  
For details, see [Install SSL server certificates on Controllers](#).  
 Optionally, you can change the ports the Controller uses to listen for HTTP and HTTPS traffic.
- Enable SSL connections between users and Virtual Delivery Agents (VDAs) by completing the following tasks:
  - Configure SSL on the machines where the VDAs are installed. (For convenience, further references to machines where VDAs are installed are simply called "VDAs.") You can use a PowerShell script supplied by Citrix, or configure it manually.  
For general information, see [About SSL settings on VDAs](#). For details, see [Configure SSL on a VDA using the PowerShell script](#) and [Manually configure SSL on a VDA](#).
  - Configure SSL in the Delivery Groups containing the VDAs by running a set of PowerShell cmdlets in Studio. For details, see [Configure SSL on Delivery Groups](#).

Requirements and considerations:

- Enabling SSL connections between users and VDAs is valid only for XenApp 7.6 and XenDesktop 7.6 Sites, plus later supported releases.
- Configure SSL in the Delivery Groups and on the VDAs after you install components, create a Site, create Machine Catalogs, and create Delivery Groups.
- To configure SSL in the Delivery Groups, you must have permission to change Controller access rules; a Full Administrator has this permission.
- To configure SSL on the VDAs, you must be a Windows administrator on the machine where the VDA is installed.
- If you intend to configure SSL on VDAs that have been upgraded from earlier versions, uninstall any SSL relay software on those machines before upgrading them.
- The PowerShell script configures SSL on static VDAs; it does not configure SSL on pooled VDAs that are provisioned by Machine Creation Services or Provisioning Services, where the machine image resets on each restart.

For tasks that include working in the Windows registry:

Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

For information about enabling SSL to the Site database, see [CTX137556](#).

## Install SSL server certificates on Controllers

For HTTPS, the XML Service supports SSL features through the use of server certificates, not client certificates. To obtain, install, and register a certificate on a Controller, and to configure a port with the SSL certificate:

- If the Controller has IIS installed, follow the guidance in <https://technet.microsoft.com/en-us/library/cc771438%28v=ws.10%29.aspx>.
- If the Controller does not have IIS installed, one method of configuring the certificate is:
  1. Obtain an SSL server certificate and install it on the Controller using the guidance in <http://blogs.technet.com/b/pki/archive/2009/08/05/how-to-create-a-web-server-ssl-certificate-manually.aspx>. For information on the certreq tool, see [http://technet.microsoft.com/en-us/library/cc736326\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc736326(WS.10).aspx).  
If you intend to use the PowerShell script to configure SSL on VDAs, and unless you intend on specifying the SSL certificate's thumbprint, make sure the certificate is located in the Local Computer > Personal > Certificates area of

the certificate store. If more than one certificate resides in that location, the first one found will be used.

2. Configure a port with the certificate; see <http://msdn.microsoft.com/en-us/library/ms733791%28v=vs.110%29.aspx>.

## Change HTTP or HTTPS ports

By default, the XML Service on the Controller listens on port 80 for HTTP traffic and port 443 for HTTPS traffic. Although you can use non-default ports, be aware of the security risks of exposing a Controller to untrusted networks. Deploying a standalone StoreFront server is preferable to changing the defaults.

To change the default HTTP or HTTPS ports used by the Controller, run the following command from Studio:

```
BrokerService.exe -WIPORT <http-port> -WISSLPORT <https-port>
```

where <http-port> is the port number for HTTP traffic and <https-port> is the port number for HTTPS traffic.

Note: After changing a port, Studio might display a message about license compatibility and upgrading. To resolve the issue, re-register service instances using the following PowerShell cmdlet sequence:

```
Get-ConfigRegisteredServiceInstance -ServiceType Broker -Binding  
XML_HTTPS | Unregister-ConfigRegisteredServiceInstance  
Get-BrokerServiceInstance | where Binding -eq "XML_HTTPS" |  
Register-ConfigServiceInstance
```

## Enforce HTTPS traffic only

If you want the XML Service to ignore HTTP traffic, set the following registry value in HKLM\Software\Citrix\DesktopServer\ on the Controller and then restart the Broker Service.

To ignore HTTP traffic, set XmlServicesEnableNonSsl to 0.

There is a corresponding registry value to ignore HTTPS traffic: XmlServicesEnableSsl. Ensure that this is not set to 0.

### About SSL settings on VDAs

When you configure SSL on VDAs, it changes permissions on the installed SSL certificate, giving the ICA Service read access to the certificate's private key, and informing the ICA Service of the following:

- **Which certificate in the certificate store to use for SSL.**
- **Which TCP port number to use for SSL connections.**

The Windows Firewall (if it is enabled) must be configured to allow incoming connection on this TCP port. This configuration is done for you when you use the PowerShell script.

- **Which versions of the SSL protocol to allow.**

The supported SSL protocol versions follow a hierarchy (lowest to highest): SSL 3.0, TLS 1.0, TLS 1.1, and TLS 1.2. You specify the minimum allowed version; all protocol connections using that version or a higher version are allowed.

For example, if you specify TLS 1.1 as the minimum version, then TLS 1.1 and TLS 1.2 protocol connections are allowed. If you specify SSL 3.0 as the minimum version, then connections for all the supported versions are allowed. If you specify TLS 1.2 as the minimum version, only TLS 1.2 connections are allowed.

- **Which SSL ciphers to allow.**

A cipher suite is a list of common SSL ciphers. When a client connects and sends a list of supported SSL ciphers, the VDA matches one of the client's ciphers with one of the ciphers in its configured cipher suite and accepts the connection. If

the client sends a cipher that is not in the VDA's cipher suite, the VDA rejects the connection.

Three cipher suites are supported: GOV(erment), COM(mercial), and ALL. The ciphers in those cipher suites depend on the Windows FIPS mode; see <http://support.microsoft.com/kb/811833> for information about Windows FIPS mode. The following table lists the ciphers in each supported cipher suite.

SSL cipher suite	GOV	COM	ALL	GOV	COM	ALL
<b>FIPS Mode</b>	Off	Off	Off	On	On	On
<b>RSA_KEYX</b>	X	X	X	X	X	X
<b>RSA_SIGN</b>	X	X	X	X	X	X
<b>3DES</b>	X		X	X		X
<b>RC4</b>		X	X			
<b>MD5</b>	X	X	X			
<b>SHA</b>	X	X	X	X	X	X
<b>SHA_256</b>	X	X	X	X	X	X
<b>SHA_384</b>	X	X	X	X	X	X
<b>SHA_512</b>	X	X	X	X	X	X
<b>AES</b>	X	X	X	X	X	X

A Delivery Group cannot have a mixture of some VDAs with SSL configured and some VDAs without SSL configured. When you configure SSL for a Delivery Group, you should have already configured SSL for all of the VDAs in that Delivery Group.

### Configure SSL on a VDA using the PowerShell script

The Enable-VdaSSL.ps1 script enables or disables the SSL listener on a VDA. This script is available in the Support >Tools > SslSupport folder on the installation media.

When you enable SSL, the script disables all existing Windows Firewall rules for the specified TCP port before adding a new rule that allows the ICA Service to accept incoming connections only on the SSL TCP port. It also disables the Windows Firewall rules for:

- Citrix ICA (default: 1494)
- Citrix CGP (default: 2598)
- Citrix WebSocket (default: 8008)

The result is that users can connect only over SSL; they cannot use raw ICA, CGP, or WebSocket to connect.

The script contains the following syntax descriptions, plus additional examples; you can use a tool such as Notepad++ to review this information.

You must specify either the –Enable or –Disable parameter; all other parameters are optional.

## Syntax

```
Enable-VdaSSL {-Enable | -Disable} [-SSLPort <port>] [-SSLMinVersion "<min-ssl-version>"] [-SSLCipherSuite "<suite>"] [-CertificateThumbPrint "<thumbprint>"]
```

Parameter	Description
-Enable	Installs and enables the SSL listener on the VDA. Either this parameter or the –Disable parameter is required.
-Disable	Disables the SSL listener on the VDA. Either this parameter or the –Enable parameter is required. If you specify this parameter, no other parameters are valid.
-SSLPort <port>	SSL port. Default: 443
-SSLMinVersion "<min-ssl-version>"	Minimum SSL protocol version, enclosed in quotation marks. Valid values: "SSL_3.0", "TLS_1.0", "TLS_1.1", and "TLS_1.2". Default: "TLS_1.0"
-SSLCipherSuite "<suite>"	SSL cipher suite, enclosed in quotation marks. Valid values: "GOV", "COM", and "ALL". Default: "ALL"
-CertificateThumbPrint "<thumbprint>"	Thumbprint of the SSL certificate in the certificate store, enclosed in quotation marks. This parameter is generally used when the certificate store has multiple certificates; the script uses the thumbprint to select the certificate you want to use. Default: the first available certificate found in the Local Computer > Personal > Certificates area of the certificate store.

## Examples

The following script installs and enables the SSL listener, using default values for all optional parameters.

```
Enable-VdaSSL –Enable
```

The following script installs and enables the SSL listener, and specifies SSL port 400, the GOV cipher suite, and a minimum TLS 1.2 SSL protocol value.

```
Enable-VdaSSL – Enable –SSLPort 400 ‘SSLMinVersion “TLS_1.2”
```

```
–SSLCipherSuite “GOV”
```

The following script disables the SSL listener on the VDA.

```
Enable-VdaSSL –Disable
```

## Manually configure SSL on a VDA

When configuring SSL on a VDA manually, you grant generic read access to the SSL certificate's private key for the appropriate service on each VDA: NT SERVICE\PorticaService for a VDA for Windows Desktop OS, or NT SERVICE\TermService for a VDA for Windows Server OS. On the machine where the VDA is installed:

1. Launch the Microsoft Management Console (MMC): Start > Run > mmc.exe.
2. Add the Certificates snap-in to the MMC:
  1. Select File > Add/Remove Snap-in.
  2. Select Certificates and then click Add.
  3. When prompted with "This snap-in will always manage certificates for:" choose "Computer account" and then click Next.
  4. When prompted with "Select the computer you want this snap-in to manage" choose "Local computer" and then click Finish.

3. Under Certificates (Local Computer) > Personal > Certificates, right-click the certificate and then select All Tasks > Manage Private Keys.
4. The Access Control List Editor displays “Permissions for (FriendlyName) private keys” where (FriendlyName) is the name of your SSL certificate. Add one of the following services and give it Read access:
  - For a VDA for Windows Desktop OS, "PORTICASERVICE"
  - For a VDA for Windows Server OS, "TERMSERVICE"
5. Double-click the installed SSL certificate. In the certificate dialog, select the Details tab and then scroll to the bottom. Click Thumbprint.
6. Run regedit and go to HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\icawd.
  1. Edit the SSL Thumbprint key and copy the value of the SSL certificate's thumbprint into this binary value. You can safely ignore unknown items in the Edit Binary Value dialog box (such as '0000' and special characters).
  2. Edit the SSLEnabled key and change the DWORD value to 1. (To disable SSL later, change the DWORD value to 0.)
  3. If you want to change the default settings (optional), use the following in the same registry path:
    - SSLPort DWORD – SSL port number. Default: 443.
    - SSLMinVersion DWORD – 1 = SSL 3.0, 2 = TLS 1.0, 3 = TLS 1.1, 4 = TLS 1.2. Default: 2 (TLS 1.0).
    - SSLCipherSuite DWORD – 1 = GOV, 2 = COM, 3 = ALL. Default: 3 (ALL).
7. Ensure the SSL TCP port is open in the Windows Firewall if it is not the default 443. (When you create the inbound rule in Windows Firewall, make sure its properties have the "Allow the connection" and "Enabled" entries selected.)
8. Ensure that no other applications or services (such as IIS) are using the SSL TCP port.
9. For VDAs for Windows Server OS, restart the machine for the changes to take effect. (You do not need to restart machines containing VDAs for Windows Desktop OS.)

## Configure SSL on Delivery Groups

Complete this procedure for each Delivery Group that contains VDAs you have configured for SSL connections.

1. From Studio, open the PowerShell console.
2. Run asnp Citrix.\* to load the Citrix product cmdlets.
3. Run Get-BrokerAccessPolicyRule –DesktopGroupName '<delivery-group-name>' | Set-BrokerAccessPolicyRule –HdxSslEnabled \$true.  
where <delivery-group-name> is the name of the Delivery Group containing VDAs.
4. Run Set-BrokerSite –DnsResolutionEnabled \$true.

## Troubleshooting

If a connection error occurs, check the VDA's system event log.

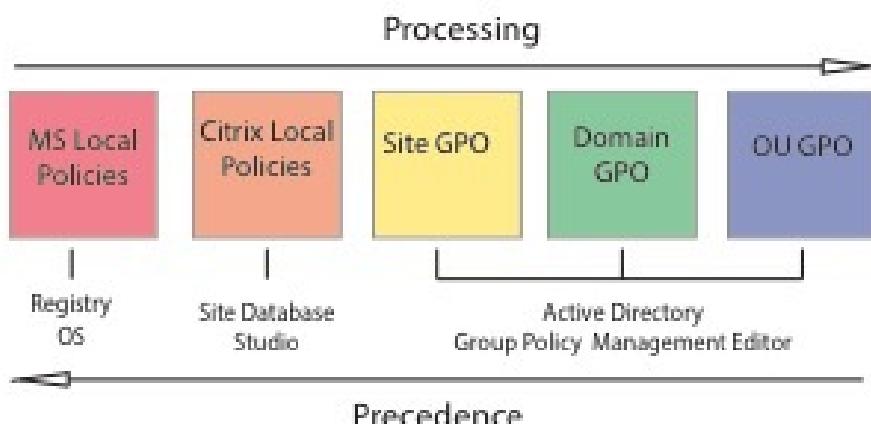
When using Receiver for Windows, if you receive a connection error (such as 1030) that indicates an SSL error, disable Desktop Viewer and then try connecting again; although the connection will still fail, an explanation of the underlying SSL issue might be provided (for example, you specified an incorrect template when requesting a certificate from the certificate authority).

# 策略

May 28, 2016

Policies are a collection of settings that define how sessions, bandwidth, and security are managed for a group of users, devices, or connection types.

You can apply policy settings to physical and virtual machines or to users. You can apply settings to individual users at the local level or in security groups in Active Directory. The configurations define specific criteria and rules, and if you do not specifically assign the policies, the settings are applied to all connections.



You can apply policies on different levels of the network. Policy settings placed at the Organizational Unit GPO level take the highest precedence on the network. Policies at the Domain GPO level override policies on the Site Group Policy Object level, which override any conflicting policies on both the Microsoft and Citrix Local Policies levels.

All Citrix Local Policies are created and managed in the Citrix Studio console and stored in the Site Database; whereas, Group Policies are created and managed with the Microsoft Group Policy Management Console (GPMC) and stored in Active Directory. Microsoft Local Policies are created in the Windows Operating System and are stored in the registry.

Studio uses a Modeling Wizard to help administrators compare configuration settings within templates and policies to help eliminate conflicting and redundant settings. Administrators can set GPOs using the GPMC to configure settings and apply them to a target set of users at different levels of the network.

These GPOs are saved in Active Directory, and access to the management of these settings is generally restricted for most of IT for security.

Settings are merged according to priority and their condition. Any disabled setting overrides a lower-ranked enabled setting. Unconfigured policy settings are ignored and do not override lower-ranked settings.

Local policies can also have conflicts with group policies in the Active Directory, which could override each other depending on the situation.

All policies are processed in the following order:

1. The end user logs on to a machine using domain credentials.
2. Credentials are sent to the domain controller.
3. Active Directory applies all policies (end user, endpoint, organizational unit, and domain).
4. The end user logs on to Receiver and accesses an application or desktop.

5. Citrix and Microsoft policies are processed for the end user and machine hosting the resource.
6. Active Directory determines precedence for policy settings and applies them to the registries of the endpoint device and to the machine hosting the resource.
7. The end user logs off from the resource. Citrix policies for the end user and endpoint device are no longer active.
8. The end user logs off the user device, which releases the GPO user policies.
9. The end user turns off the device, which releases the GPO machine policies.

When creating policies for groups of users, devices, and machines, some members may have different requirements and would need exceptions to some policy settings. Exceptions are made by way of filters in Studio and the GPMC that determine who or what the policy affects.

## Related content

- [Work with policies](#)
- [Policy templates](#)
- [Create policies](#)
- [Compare, prioritize, model, and troubleshoot policies](#)
- [Default policy settings](#)
- [Policy settings reference](#)

# 使用策略

May 28, 2016

Configure Citrix policies to control user access and session environments. Citrix policies are the most efficient method of controlling connection, security, and bandwidth settings. You can create policies for specific groups of users, devices, or connection types. Each policy can contain multiple settings.

## Tools for working with Citrix policies

You can use the following tools to work with Citrix policies.

- **Studio** - If you are a Citrix administrator without permission to manage group policy, use Studio to create policies for your site. Policies created using Studio are stored in the site database and updates are pushed to the virtual desktop either when that virtual desktop registers with the broker or when a user connects to that virtual desktop.
- **Local Group Policy Editor** (Microsoft Management Console snap-in) - If your network environment uses Active Directory and you have permission to manage group policy, you can use the Local Group Policy Editor to create policies for your Site. The settings you configure affect the Group Policy Objects (GPOs) you specify in the Group Policy Management Console.

Important: You must use the Local Group Policy Editor to configure some policy settings, including those related to registering VDAs with a Controller and those related to Microsoft App-V servers.

## Policy processing order and precedence

Group policy settings are processed in the following order:

1. Local GPO
2. XenApp or XenDesktop Site GPO (stored in the Site database)
3. Site-level GPOs
4. Domain-level GPOs
5. Organizational Units

However, if a conflict occurs, policy settings that are processed last can overwrite those that are processed earlier. This means that policy settings take precedence in the following order:

1. Organizational Units
2. Domain-level GPOs
3. Site-level GPOs
4. XenApp or XenDesktop Site GPO (stored in the Site database)
5. Local GPO

For example, a Citrix administrator uses Studio to create a policy (Policy A) that enables client file redirection for the company's sales employees. Meanwhile, another administrator uses the Group Policy Editor to create a policy (Policy B) that disables client file redirection for sales employees. When the sales employees log on to the virtual desktops, Policy B is applied and Policy A is ignored because Policy B was processed at the domain level and Policy A was processed at the XenApp or XenDesktop Site GPO level.

However, when a user launches an ICA or Remote Desktop Protocol (RDP) session, Citrix session settings override the same settings configured in an Active Directory policy or using Remote Desktop Session Host Configuration. This includes settings that are related to typical RDP client connection settings such as Desktop wallpaper, Menu animation, and View window contents while dragging.

When using multiple policies, you can prioritize policies that contain conflicting settings; see [Compare, prioritize, model, and troubleshoot policies](#) for details.

## Workflow for Citrix policies

The process for configuring policies is as follows:

1. Create the policy.
2. Configure policy settings.
3. Assign the policy to machine and user objects.
4. Prioritize the policy.
5. Verify the effective policy by running the Citrix Group Policy Modeling wizard.

## Navigate Citrix policies and settings

In the Local Group Policy Editor, policies and settings appear in two categories: Computer Configuration and User Configuration. Each category has a Citrix Policies node. See the Microsoft documentation for details about navigating and using this snap-in.

In Studio, policy settings are sorted into categories based on the functionality or feature they affect. For example, the Profile management section contains policy settings for Profile management.

- Computer settings (policy settings applying to machines) define the behavior of virtual desktops and are applied when a virtual desktop starts. These settings apply even when there are no active user sessions on the virtual desktop. User settings define the user experience when connecting using ICA. User policies are applied when a user connects or reconnects using ICA. User policies are not applied if a user connects using RDP or logs on directly to the console.

To access policies, settings, or templates, select Policies in the Studio navigation pane.

- The **Policies** tab lists all policies. When you select a policy, tabs to the right display: Overview (name, priority, enabled/disabled status, and description), Settings (list of configured settings), and Assigned to (user and machine objects to which the policy is currently assigned). For more information, see [Create policies](#).
- The **Templates** tab lists Citrix-provided and custom templates you created. When you select a template, tabs to the right display: Description (why you might want to use the template) and Settings (list of configured settings). For more information, see [Policy templates](#).
- The **Comparison** tab enables you to compare the settings in a policy or template with those in other policies or templates. For example, you might want to verify setting values to ensure compliance with best practices. For more information, see [Compare, prioritize, model, and troubleshoot policies](#).
- From the **Modelling** tab, you can simulate connection scenarios with Citrix policies. For more information, see [Compare, prioritize, model, and troubleshoot policies](#).

To search for a setting in a policy or template:

1. Select the policy or template.
2. Select Edit policy or Edit Template in the Actions pane.
3. On the Settings page, begin to type the name of the setting.

You can refine your search by selecting a specific product version, selecting a category (for example, Bandwidth), or by selecting the View selected only check box or selecting to search only the settings that have been added to the selected policy. For an unfiltered search, select All Settings.

- To search for a setting within a policy :
  1. Select the policy.
  2. Select the Settings tab, begin to type the name of the setting.

You can refine your search by selecting a specific product version or by selecting a category. For an unfiltered search, select

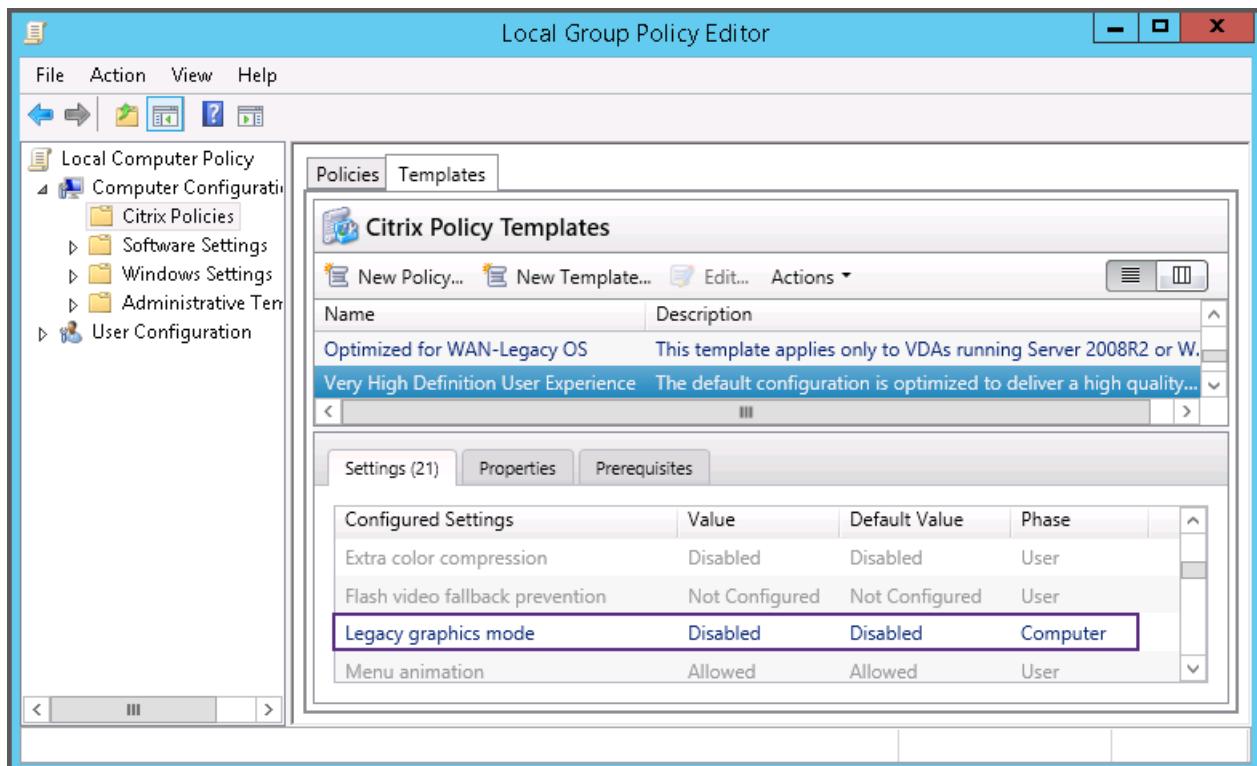
All Settings.

A policy, once created, is completely independent of the template used. You can use the Description field on a new policy to keep track of the source template used.

In Studio, policies and templates are displayed in a single list regardless of whether they contain user, computer or both types of settings and can be applied using both user and computer filters.

In Group Policy Editor, Computer and User settings must be applied separately, even if created from a template that contains both types of settings. In this example choosing to use Very High Definition User Experience in Computer Configuration:

- Legacy Graphics mode is a Computer setting that will be used in a policy created from this template.
- The User settings, grayed out, will not be used in a policy created from this template.



# 策略模板

May 28, 2016

Templates are a source for creating policies from a predefined starting point. Built-in Citrix templates, optimized for specific environments or network conditions, can be used as:

- A source for creating your own policies and templates to share between sites.
- A reference for easier comparison of results between deployments as you will be able to quote the results, for example, "...when using Citrix template x or y...".
- A method for communicating policies with Citrix Support or trusted third parties by importing or exporting templates.

Policy templates can be imported or exported. For additional templates and updates to the built-in templates, see [CTX202000](#).

For considerations when using templates to create policies, see [CTX202330](#).

## Built-in Citrix templates

The Group Policy Management package includes the following policy templates that replace and enhance the previously available built-in Citrix templates:

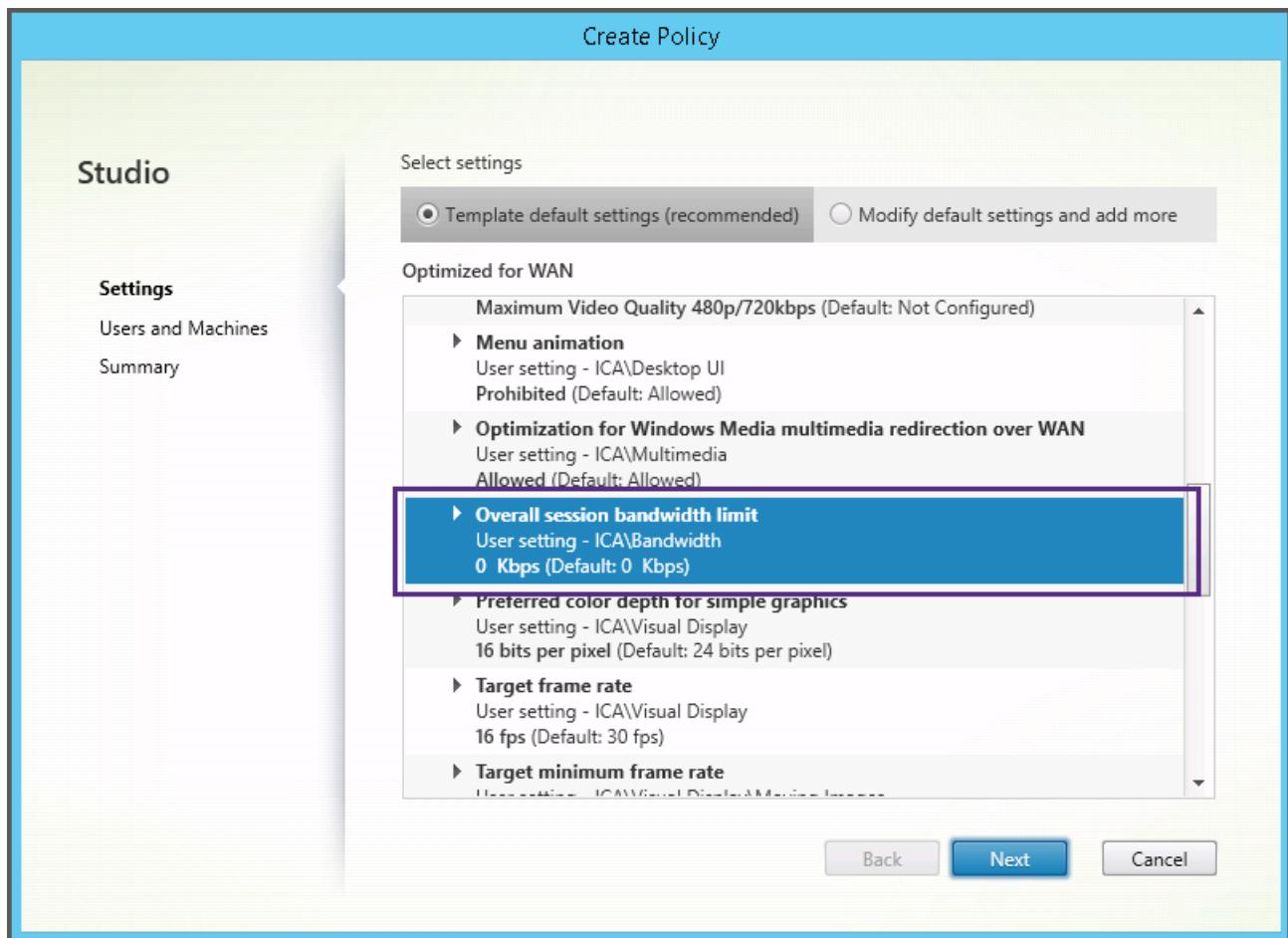
- **Very High Definition User Experience.** This template enforces default settings which maximize the user experience. Use this template in scenarios where multiple policies are processed in order of precedence.
- **High Server Scalability.** Apply this template to economize on server resources. This template balances user experience and server scalability. It offers a good user experience while increasing the number of users you can host on a single server. This template does not use video codec for compression of graphics and prevents server side multimedia rendering.
- **High Server Scalability-Legacy OS.** This High Server Scalability template applies only to VDAs running Server 2008 R2 or Windows 7 and earlier. This template relies on the Legacy graphics mode which is more efficient for those operating systems.
- **Optimized for CloudBridge.** Apply this template for users working from branch offices with CloudBridge deployed for optimizing delivery of XenDesktop. These locations typically have highly utilized links and/or high latencies. This template optimizes bandwidth efficiency for use in such conditions.

Settings:

- Desktop Composition Redirection
  - Menu Animation
  - View window contents while dragging
- **Optimized for WAN.** This template is intended for task workers in branch offices using a shared WAN connection or remote locations with low bandwidth connections accessing applications with graphically simple user interfaces with little multimedia content. This template trades off video playback experience and some server scalability for optimized bandwidth efficiency.
  - **Optimized for WAN-Legacy OS.** This Optimized for WAN template applies only to VDAs running Server 2008 R2 or Windows 7 and earlier. This template relies on the Legacy graphics mode which is more efficient for those operating systems.
  - **Security and Control.** Use this template in environments with low tolerance to risk, to minimize the features enabled by default in XenApp and XenDesktop. This template includes settings which will disable access to printing, clipboard,

peripheral devices, drive mapping, port redirection, and Flash acceleration on user devices. Applying this template may use more bandwidth and reduce user density per server.

While we recommend using the built-in Citrix templates with their default settings, you will find settings that do not have a specific recommended value. For example, Overall session bandwidth limit, included in the Optimized for WAN templates. In this case, the template takes the approach of exposing the setting so the administrator will understand this setting is likely to apply to the scenario.



If you are working with a deployment (policy management and VDAs) prior to XenApp and XenDesktop 7.6 FP3, and require High Server Scalability and Optimized for WAN templates, please use the Legacy OS versions of these templates when these apply.

## 注意

Built-in templates are created and updated by Citrix. You cannot modify or delete these templates.

Create and manage templates using Studio

To create a new template based on a template:

1. Select **Policies** in the Studio navigation pane.
2. Select the **Templates** tab and then select the template from which you will create the new template.
3. Select **Create Template** in the Actions pane.

4. Select and configure the policy settings to include in the template. Remove any existing settings that should not be included. Enter a name for the template.

After you click **Finish**, the new template appears on the **Templates** tab.

To create a new template based on a policy:

1. Select **Policies** in the Studio navigation pane.
2. Select the **Policies** tab and then select the policy from which you will create the new template.
3. Select **Save as Template** in the Actions pane.
4. Select and configure any new policy settings to include in the template. Remove any existing settings that should not be included. Enter a name and description for the template, and then click **Finish**.

To import a template:

1. Select **Policies** in the Studio navigation pane.
2. Select the **Templates** tab and then select **Import Template**.
3. Select the template file to import and then click **Open**. If you import a template with the same name as an existing template, you can choose to overwrite the existing template or save the template with a different name that is generated automatically.

To export a template:

1. Select **Policies** in the Studio navigation pane.
2. Select the **Templates** tab and then select **Export Template**.
3. Select the location where you want to save the template and then click **Save**.

A .gpt file is created in the specified location.

Create and manage templates using the Group Policy Editor

From the Group Policy Editor, expand Computer Configuration or User Configuration. Expand the Policies node and then select Citrix Policies. Choose the appropriate action below.

Task	Instruction
Create a new template from an existing policy	On the Policies tab, select the policy and then select Actions > Save as Template.
Create a new policy from an existing template	On the Templates tab, select the template and then click New Policy.
Create a new template from an existing template	On the Templates tab, select the template and then click New Template.
Import a template	On the Templates tab, select Actions > Import.
Export a template	On the Templates tab, select Actions > Export.
View template settings	On the Templates tab, select the template and then click the Settings tab.

<b>Task</b>	View a summary of template properties On the Templates tab, select the template and then click the Properties tab.
View template prerequisites	On the Templates tab, select the template and then click the Prerequisites tab.

## Templates and Delegated Administration

Policy templates are stored on the machine where the policy management package was installed. This machine is either the Delivery Controller machine or the Group Policy Objects management machine - not the XenApp and XenDesktop Site's database. This means that the policy template files are controlled by Windows administrative permissions rather than Site's Delegated Administration roles and scopes.

As a result, an administrator with read-only permission in the Site can, for example, create new templates. However, because templates are local files, no changes are actually made to your environment.

Custom templates are only visible to the user account that creates them and stored in the user's Windows profile. To expose a custom template further, create a policy from it or export it to a shared location.

# 创建策略

May 28, 2016

Before creating a policy, decide which group of users or devices it should affect. You may want to create a policy based on user job function, connection type, user device, or geographic location. Alternatively, you can use the same criteria that you use for Windows Active Directory group policies.

If you already created a policy that applies to a group, consider editing that policy and configuring the appropriate settings, instead of creating another policy. Avoid creating a new policy solely to enable a specific setting or to exclude the policy from applying to certain users.

When you create a new policy, you can base it on settings in a policy template and customize settings as needed, or you can create it without using a template and add all the settings you need.

## Policy settings

Policy settings can be enabled, disabled, or not configured. By default, policy settings are not configured, which means they are not added to a policy. Settings are applied only when they are added to a policy.

Some policy settings can be in one of the following states:

- Allowed or Prohibited allows or prevents the action controlled by the setting. In some cases, users are allowed or prevented from managing the setting's action in a session. For example, if the Menu animation setting is set to Allowed, users can control menu animations in their client environment.
- Enabled or Disabled turns the setting on or off. If you disable a setting, it is not enabled in lower-ranked policies.

In addition, some settings control the effectiveness of dependent settings. For example, Client drive redirection controls whether or not users are allowed to access the drives on their devices. To allow users to access their network drives, both this setting and the Client network drives setting must be added to the policy. If the Client drive redirection setting is disabled, users cannot access their network drives, even if the Client network drives setting is enabled.

In general, policy setting changes that impact machines go into effect either when the virtual desktop restarts or when a user logs on. Policy setting changes that impact users go into effect the next time users log on. If you are using Active Directory, policy settings are updated when Active Directory re-evaluates policies at 90-minute intervals and applied either when the virtual desktop restarts or when a user logs on.

For some policy settings, you can enter or select a value when you add the setting to a policy. You can limit configuration of the setting by selecting Use default value; this disables configuration of the setting and allows only the setting's default value to be used when the policy is applied, regardless of the value that was entered before selecting Use default value.

As best practice:

- Assign policies to groups rather than individual users. If you assign policies to groups, assignments are updated automatically when you add or remove users from the group.
- Do not enable conflicting or overlapping settings in Remote Desktop Session Host Configuration. In some cases, Remote Desktop Session Host Configuration provides similar functionality to Citrix policy settings. When possible, keep all settings consistent (enabled or disabled) for ease of troubleshooting.
- Disable unused policies. Policies with no settings added create unnecessary processing.

## Policy assignments

When creating a policy, you assign it to certain user and machine objects; that policy is applied to connections according to specific criteria or rules. In general, you can add as many assignments as you want to a policy, based on a combination of criteria. If you specify no assignments, the policy is applied to all connections.

The following table lists the available assignments:

<b>Assignment Name</b>	<b>Applies a policy based on</b>
Access Control	Access control conditions through which a client is connecting. <ul style="list-style-type: none"> <li>• Connection type - Whether to apply the policy to connections made with or without NetScaler Gateway.</li> <li>• NetScaler Gateway farm name - Name of the NetScaler Gateway virtual server.</li> <li>• Access condition - Name of the end point analysis policy or session policy to use.</li> </ul>
Citrix CloudBridge	Whether or not a user session is launched through Citrix CloudBridge.  Note: You can add only one Citrix CloudBridge assignment to a policy.
Client IP Address	IP address of the user device used to connect to the session. <ul style="list-style-type: none"> <li>• IPv4 examples: 12.0.0.0, 12.0.0.* , 12.0.0.1-12.0.0.70, 12.0.0.1/24</li> <li>• IPv6 examples: 2001:0db8:3c4d:0015:0:0:abcd:ef12, 2001:0db8:3c4d:0015::/54</li> </ul>
Client Name	Name of the user device. <ul style="list-style-type: none"> <li>• Exact match: ClientABCName</li> <li>• Using wildcard: Client*Name</li> </ul>
Delivery Group	Delivery Group membership.
Delivery Group type	Type of desktop or application: private desktop, shared desktop, private application, or shared application.
Organizational Unit (OU)	Organizational unit.
Tag	Tags.
User or Group	User or group name.

When a user logs on, all policies that match the assignments for the connection are identified. Those policies are sorted into priority order and multiple instances of any setting are compared. Each setting is applied according to the priority ranking of the policy. Any policy setting that is disabled takes precedence over a lower-ranked setting that is enabled. Policy settings that are not configured are ignored.

Important: When configuring both Active Directory and Citrix policies using the Group Policy Management Console,

assignments and settings may not be applied as expected. For more information, see [CTX127461](#)

A policy named "Unfiltered" is provided by default.

- If you use Studio to manage Citrix policies, settings you add to the Unfiltered policy are applied to all servers, desktops, and connections in a Site.
- If you use the Local Group Policy Editor to manage Citrix policies, settings you add to the Unfiltered policy are applied to all Sites and connections that are within the scope of the Group Policy Objects (GPOs) that contain the policy. For example, the Sales OU contains a GPO called Sales-US that includes all members of the US sales team. The Sales-US GPO is configured with an Unfiltered policy that includes several user policy settings. When the US Sales manager logs on to the Site, the settings in the Unfiltered policy are automatically applied to the session because the user is a member of the Sales-US GPO.

An assignment's mode determines if the policy is applied only to connections that match all the assignment criteria. If the mode is set to Allow (the default), the policy is applied only to connections that match the assignment criteria. If the mode is set to Deny, the policy is applied if the connection does not match the assignment criteria. The following examples illustrate how assignment modes affect Citrix policies when multiple assignments are present.

- **Example: Assignments of like type with differing modes** - In policies with two assignments of the same type, one set to Allow and one set to Deny, the assignment set to Deny takes precedence, provided the connection satisfies both assignments. For example:

Policy 1 includes the following assignments:

- Assignment A specifies the Sales group; the mode is set to Allow
- Assignment B specifies the Sales manager's account; the mode is set to Deny

Because the mode for Assignment B is set to Deny, the policy is not applied when the Sales manager logs on to the Site, even though the user is a member of the Sales group.

- **Example: Assignments of differing type with like modes** - In policies with two or more assignments of differing types, set to Allow, the connection must satisfy at least one assignment of each type in order for the policy to be applied. For example:

Policy 2 includes the following assignments:

- Assignment C is a User assignment that specifies the Sales group; the mode is set to Allow
- Assignment D is a Client IP Address assignment that specifies 10.8.169.\* (the corporate network); the mode is set to Allow

When the Sales manager logs on to the Site from the office, the policy is applied because the connection satisfies both assignments.

Policy 3 includes the following assignments:

- Assignment E is a User assignment that specifies the Sales group; the mode is set to Allow
- Assignment F is an Access Control assignment that specifies NetScaler Gateway connection conditions; the mode is set to Allow

When the Sales manager logs on to the Site from the office, the policy is not applied because the connection does not satisfy Assignment F.

Create a new policy based on a template, using Studio

1. Select Policies in the Studio navigation pane.
2. Select the Templates tab and select a template.
3. Select Create Policy from Template in the Actions pane.
4. By default, the new policy uses all the default settings in the template (the Use template default settings radio button is selected). If you want to change settings, select the Modify defaults and add more settings radio button, and then add

or remove settings.

5. Specify how to apply the policy by selecting one of the following:
  - Assign to selected user and machine objects and then select the user and machine objects to which the policy will apply.
  - Assign to all objects in a site to apply the policy to all user and machine objects in the Site.
6. Enter a name for the policy (or accept the default); consider naming the policy according to who or what it affects, for example Accounting Department or Remote Users. Optionally, add a description.  
The policy is enabled by default; you can disable it. Enabling the policy allows it to be applied immediately to users logging on. Disabling prevents the policy from being applied. If you need to prioritize the policy or add settings later, consider disabling the policy until you are ready to apply it.

### Create a new policy using Studio

1. Select Policies in the Studio navigation pane.
2. Select the Policies tab.
3. Select Create Policy in the Actions pane.
4. Add and configure policy settings.
5. Specify how to apply the policy by choosing one of the following:
  - Assign to selected user and machine objects and then select the user and machine objects to which the policy will apply.
  - Assign to all objects in a site to apply the policy to all user and machine objects in the Site.
6. Enter a name for the policy (or accept the default); consider naming the policy according to who or what it affects, for example Accounting Department or Remote Users. Optionally, add a description.  
The policy is enabled by default; you can disable it. Enabling the policy allows it to be applied immediately to users logging on. Disabling prevents the policy from being applied. If you need to prioritize the policy or add settings later, consider disabling the policy until you are ready to apply it.

### Create and manage policies using the Group Policy Editor

From the Group Policy Editor, expand Computer Configuration or User Configuration. Expand the Policies node and then select Citrix Policies. Choose the appropriate action below.

Task	Instruction
Create a new policy	On the Policies tab, click New.
Edit an existing policy	On the Policies tab, select the policy and then click Edit.
Change the priority of an existing policy	On the Policies tab, select the policy and then click either Higher or Lower.
View summary information about a policy	On the Policies tab, select the policy and then click the Summary tab.
View and amend policy settings	On the Policies tab, select the policy and then click the Settings tab.
View and amend policy filters	On the Policies tab, select the policy and then click the Filters tab.
Enable or disable a policy	On the Policies tab, select the policy and then select either Actions > Enable or Actions > Disable.

Create a new policy from an existing  
**Task**  
template

On the Templates tab, select the template and then click New Policy.  
**Instruction**

# 对策略进行比较、设定优先级、建模和故障排除

Sep 16, 2016

You can use multiple policies to customize your environment to meet users' needs based on their job functions, geographic locations, or connection types. For example, for security you may need to place restrictions on user groups who regularly work with sensitive data. You can create a policy that prevents users from saving sensitive files on their local client drives. However, if some people in the user group do need access to their local drives, you can create another policy for only those users. You then rank or prioritize the two policies to control which one takes precedence.

When using multiple policies, you must determine how to prioritize them, how to create exceptions, and how to view the effective policy when policies conflict.

In general, policies override similar settings configured for the entire Site, for specific Delivery Controllers, or on the user device. The exception to this principle is security. The highest encryption setting in your environment, including the operating system and the most restrictive shadowing setting, always overrides other settings and policies.

Citrix policies interact with policies you set in your operating system. In a Citrix environment, Citrix settings override the same settings configured in an Active Directory policy or using Remote Desktop Session Host Configuration. This includes settings that are related to typical Remote Desktop Protocol (RDP) client connection settings such as Desktop wallpaper, Menu animation, and View window contents while dragging. For some policy settings, such as Secure ICA, the settings in policies must match the settings in the operating system. If a higher priority encryption level is set elsewhere, the Secure ICA policy settings that you specify in the policy or when you are delivering application and desktops can be overridden.

For example, the encryption settings that you specify when creating Delivery Groups should be at the same level as the encryption settings you specified throughout your environment.

Note: In the second hop of double-hop scenarios, when a Desktop OS VDA connects to Server OS VDA, Citrix policies act on the Desktop OS VDA as if it were the user device. For example, if policies are set to cache images on the user device, the images cached for the second hop in a double-hop scenario are cached on the Desktop OS VDA machine.

## Compare policies and templates

You can compare settings in a policy or template with those in other policies or templates. For example, you might need to verify setting values to ensure compliance with best practices. You might also want to compare settings in a policy or template with the default settings provided by Citrix.

1. Select Policies in the Studio navigation pane.
2. Click the Comparison tab and then click Select.
3. Choose the policies or templates to compare. To include default values in the comparison, select the Compare to default settings check box.
4. After you click Compare, the configured settings are displayed in columns.
5. To see all settings, select Show All Settings. To return to the default view, select Show Common Settings.

## Prioritize policies

Prioritizing policies allows you to define the precedence of policies when they contain conflicting settings. When a user logs on, all policies that match the assignments for the connection are identified. Those policies are sorted into priority order and multiple instances of any setting are compared. Each setting is applied according to the priority ranking of the policy.

You prioritize policies by giving them different priority numbers in Studio. By default, new policies are given the lowest priority. If policy settings conflict, a policy with a higher priority (a priority number of 1 is the highest) overrides a policy with a

lower priority. Settings are merged according to priority and the setting's condition; for example, whether the setting is disabled or enabled. Any disabled setting overrides a lower-ranked setting that is enabled. Policy settings that are not configured are ignored and do not override the settings of lower-ranked settings.

1. Select Policies in the Studio navigation pane. Make sure the Policies tab is selected.
2. Select a policy.
3. Select Lower Priority or Higher Priority in the Actions pane.

## Exceptions

When you create policies for groups of users, user devices, or machines, you may find that some members of the group require exceptions to some policy settings. You can create exceptions by:

- Creating a policy only for those group members who need the exceptions and then ranking the policy higher than the policy for the entire group
- Using the Deny mode for an assignment added to the policy

An assignment with the mode set to Deny applies a policy only to connections that do not match the assignment criteria.

For example, a policy contains the following assignments:

- Assignment A is a client IP address assignment that specifies the range 208.77.88.\*; the mode is set to Allow
- Assignment B is a user assignment that specifies a particular user account; the mode is set to Deny

The policy is applied to all users who log on to the Site with IP addresses in the range specified in Assignment A. However, the policy is not applied to the user logging on to the Site with the user account specified in Assignment B, even though the user's computer is assigned an IP address in the range specified in Assignment A.

## Determine which policies apply to a connection

Sometimes a connection does not respond as expected because multiple policies apply. If a higher priority policy applies to a connection, it can override the settings you configure in the original policy. You can determine how final policy settings are merged for a connection by calculating the Resultant Set of Policy.

You can calculate the Resultant Set of Policy in the following ways:

- Use the Citrix Group Policy Modeling Wizard to simulate a connection scenario and discern how Citrix policies might be applied. You can specify conditions for a connection scenario such as domain controller, users, Citrix policy assignment evidence values, and simulated environment settings such as slow network connection. The report that the wizard produces lists the Citrix policies that would likely take effect in the scenario. If you are logged on to the Controller as a domain user, the wizard calculates the Resultant Set of Policy using both site policy settings and Active Directory Group Policy Objects (GPOs).
- Use Group Policy Results to produce a report describing the Citrix policies in effect for a given user and controller. The Group Policy Results tool helps you evaluate the current state of GPOs in your environment and generates a report that describes how these objects, including Citrix policies, are currently being applied to a particular user and controller.

You can launch the Citrix Group Policy Modeling Wizard from the Actions pane in Studio. You can launch either tool from the Group Policy Management Console in Windows.

If you run the Citrix Group Policy Modeling Wizard or Group Policy Results tool from the Group Policy Management Console, site policy settings created using Studio are not included in the Resultant Set of Policy.

To ensure you obtain the most comprehensive Resultant Set of Policy, Citrix recommends launching the Citrix Group Policy Modeling wizard from Studio, unless you create policies using only the Group Policy Management Console.

## Use the Citrix Group Policy Modeling Wizard

Open the Citrix Group Policy Modeling Wizard using one of the following:

- Select Policies in the Studio navigation pane, select the Modeling tab, and then select Launch Modeling Wizard in the Actions pane.
- Launch the Group Policy Management Console (gpmc.msc), right-click Citrix Group Policy Modeling in the tree pane, and then select Citrix Group Policy Modeling Wizard.

Follow the wizard instructions to select the domain controller, users, computers, environment settings, and Citrix assignment criteria to use in the simulation. After you click Finish, the wizard produces a report of the modeling results. In Studio, the report appears in the middle pane under the Modeling tab.

To view the report, select View Modeling Report.

### Troubleshoot policies

Users, IP addresses, and other assigned objects can have multiple policies that apply simultaneously. This can result in conflicts where a policy may not behave as expected. When you run the Citrix Group Policy Modeling Wizard or the Group Policy Results tool, you might discover that no policies are applied to user connections. When this happens, users connecting to their applications and desktops under conditions that match the policy evaluation criteria are not affected by any policy settings. This occurs when:

- No policies have assignments that match the policy evaluation criteria.
- Policies that match the assignment do not have any settings configured.
- Policies that match the assignment are disabled.

If you want to apply policy settings to the connections that meet the specified criteria, make sure:

- The policies you want to apply to those connections are enabled.
- The policies you want to apply have the appropriate settings configured.

# 默认策略设置

Aug 08, 2016

The following tables list policy settings, their default, and the Virtual Delivery Agent (VDA) versions to which they apply.

## ICA

Name	Default setting	VDA
Client clipboard redirection	Allowed	All VDA versions
Desktop launches	Prohibited	VDA for Server OS 7 through current
ICA listener connection timeout	120000 milliseconds	VDA 5, 5.5, 5.6 Feature Pack 1, VDA for Desktop OS 7 through current
ICA listener port number	1494	All VDA versions
Launching of non-published programs during client connection	Prohibited	VDA for Server OS 7 through current
Client clipboard write allowed formats	No formats are specified	VDA 7.6 through current
Restrict client clipboard write	Prohibited	VDA 7.6 through current
Restrict session clipboard write	Prohibited	VDA 7.6 through current
Session clipboard write allowed formats	No formats are specified	VDA 7.6 through current

## ICA/Adobe Flash Delivery/Flash Redirection

Name	Default setting	VDA
Flash video fallback prevention	Not configured	VDA 7.6 FP3 through current
Flash video fallback prevention error *.swf		VDA 7.6 FP3 through current

## ICA/Audio

Name	Default setting	VDA
Audio Plug N Play	Allowed	VDA for Server OS 7 through current
Audio quality	High - high definition audio	All VDA versions
Client audio redirection	Allowed	All VDA versions

<b>Name</b>	<b>Default setting</b>	All VDA versions VDA
-------------	------------------------	-------------------------

## ICA/Auto Client Reconnect

<b>Name</b>	<b>Default setting</b>	<b>VDA</b>
Auto client reconnect	Allowed	VDA
Auto client reconnect authentication	Do not require authentication	VDA
Auto client reconnect logging	Do not log auto-reconnect events	VDA

## ICA/Bandwidth

<b>Name</b>	<b>Default setting</b>	<b>VDA</b>
Audio redirection bandwidth limit	0 Kbps	VDA
Audio redirection bandwidth limit percent	0	VDA
Client USB device redirection bandwidth limit	0 Kbps	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current
Client USB device redirection bandwidth limit percent	0	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current
Clipboard redirection bandwidth limit	0 Kbps	All VDA versions
Clipboard redirection bandwidth limit percent	0	All VDA versions
COM port redirection bandwidth limit	0 Kbps	All VDA versions; for VDA 7.x, configure this setting using the registry.
COM port redirection bandwidth limit percent	0	All VDA versions; for VDA 7.x, configure this setting using the registry.
File redirection bandwidth limit	0 Kbps	All VDA versions
File redirection bandwidth limit percent	0	All VDA versions
HDX MediaStream Multimedia Acceleration bandwidth limit	0 Kbps	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current
HDX MediaStream Multimedia Acceleration bandwidth limit percent	0	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current
LPT port redirection bandwidth limit	0 Kbps	All VDA versions; for VDA 7.x, configure this setting using the registry.

LPT port redirection bandwidth limit percent	0 <b>Default setting</b>	All VDA versions; for VDA 7.x, configure this setting using the registry.
Overall session bandwidth limit	0 Kbps	All VDA versions
Printer redirection bandwidth limit	0 Kbps	All VDA versions
Printer redirection bandwidth limit percent	0	All VDA versions
TWAIN device redirection bandwidth limit	0 Kbps	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current
TWAIN device redirection bandwidth limit percent	0	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current

## ICA/Client Sensors

Name	Default setting	VDA
Allow applications to use the physical location of the client device	Prohibited	VDA 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current

## ICA/Desktop UI

Name	Default setting	VDA
Desktop Composition Redirection	Disabled (7.6 FP3 through current) Enabled (5.6 through 7.6 FP2)	VDA 5.6, VDA for Desktop OS 7 through current, VDA
Desktop Composition Redirection graphics quality	Medium	VDA 5.6, VDA for Desktop OS 7 through current, VDA
Desktop wallpaper	Allowed	All VDA versions
Menu animation	Allowed	All VDA versions
View window contents while dragging	Allowed	All VDA versions

## ICA/End User Monitoring

Name	Default setting	VDA
ICA round trip calculation	Enabled	All VDA versions
ICA round trip calculation interval	15 seconds	All VDA versions

<b>Name</b>	ICA round trip calculations for idle connections	<b>Default setting</b>	Disabled	All VDA versions
-------------	--	------------------------	----------	------------------

## ICA/Enhanced Desktop Experience

<b>Name</b>	<b>Default setting</b>	<b>VDA</b>
Enhanced Desktop Experience	Allowed	VDA for Server OS 7 through current

## ICA/File Redirection

<b>Name</b>	<b>Default setting</b>	<b>VDA</b>
Auto connect client drives	Allowed	All VDA versions
Client drive redirection	Allowed	All VDA versions
Client fixed drives	Allowed	All VDA versions
Client floppy drives	Allowed	All VDA versions
Client network drives	Allowed	All VDA versions
Client optical drives	Allowed	All VDA versions
Client removable drives	Allowed	All VDA versions
Host to client redirection	Disabled	VDA for Server OS 7 through current
Preserve client drive letters	Disabled	VDA 5, 5.5, 5.6 Feature Pack 1, VDA for Desktop OS 7 through current
Read-only client drive access	Disabled	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current
Special folder redirection	Allowed	Web Interface deployments only; VDA for Server OS 7 through current
Use asynchronous writes	Disabled	All VDA versions

## ICA/Graphics

<b>Name</b>	<b>Default setting</b>	<b>VDA</b>
Display memory limit	65536 Kb	VDA 5, 5.5, 5.6 Feature Pack 1, VDA for Desktop OS 7 through current

Name	Default setting	VDA
Display mode degrade preference	Degrade color depth first	All VDA versions
Dynamic windows preview	Enabled	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current
Image caching	Enabled	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current
Legacy graphics mode	Disabled	VDA for Server OS 7 and VDA for Desktop OS 7 through current
Maximum allowed color depth	32 bits per pixel	All VDA versions
Notify user when display mode is degraded	Disabled	VDA for Server OS 7 through current
Queuing and tossing	Enabled	All VDA versions

#### ICA/Graphics/Caching

Name	Default setting	VDA
Persistent cache threshold	3000000 bps	VDA for Server OS 7 through current

#### ICA/Keep Alive

Name	Default setting	VDA
ICA keep alive timeout	60 seconds	All VDA versions
ICA keep alives	Do not send ICA keep alive messages	All VDA versions

#### ICA/Local App Access

Name	Default setting	VDA
Allow local app access	Prohibited	VDA for Server OS 7 and VDA for Desktop OS 7 through current
URL redirection black list	No sites are specified	VDA for Server OS 7 and VDA for Desktop OS 7 through current
URL redirection white list	No sites are specified	VDA for Server OS 7 and VDA for Desktop OS 7 through current

#### ICA/Mobile Experience

Name	Default setting	VDA
Automatic keyboard display	Prohibited	VDA 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current

<b>Name</b> Launch touch-optimized desktop	<b>Default Allowed setting</b>	<b>VDA</b> VDA 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current
This setting is disabled and not available for Windows 10 machines.		
Remote the combo box	Prohibited	VDA 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current

## ICA/Multimedia

<b>Name</b>	<b>Default setting</b>	<b>VDA</b>
Limit video quality	Not configured	VDA for Server OS 7 and VDA for Desktop OS 7 through current
Multimedia conferencing	Allowed	All VDA versions
Optimization for Windows Media multimedia redirection over WAN	Allowed	VDA for Server OS 7 and VDA for Desktop OS 7 through current
Use GPU for optimizing Windows Media multimedia redirection over WAN	Prohibited	VDA for Server OS 7 and VDA for Desktop OS 7 through current
Video load management policy setting	Not configured	VDA 7.6 FP3 through current
Windows Media client-side content fetching	Allowed	VDA for Server OS 7 and VDA for Desktop OS 7 through current
Windows Media Redirection	Allowed	All VDA versions
Windows Media Redirection buffer size	5 seconds	VDA 5, 5.5, and 5.6, Feature Pack 1 through current
Windows Media Redirection buffer size use	Disabled	VDA 5, 5.5, and 5.6, Feature Pack 1 through current

## ICA/Multi-Stream Connections

Name	Default setting	VDA
Audio over UDP	Allowed	VDA for Server OS 7 through current
Audio UDP port range	16500, 16509	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current
Multi-Port policy	Primary port (2598) has High Priority	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current
Multi-Stream computer setting	Disabled	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current
Multi-Stream user setting	Disabled	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current

## ICA/Port Redirection

Name	Default setting	VDA
Auto connect client COM ports	Disabled	All VDA versions; for VDA 7.x, configure this setting using the registry.
Auto connect client LPT ports	Disabled	All VDA versions; for VDA 7.x, configure this setting using the registry.
Client COM port redirection	Prohibited	All VDA versions; for VDA 7.x, configure this setting using the registry.
Client LPT port redirection	Prohibited	All VDA versions; for VDA 7.x, configure this setting using the registry.

## ICA/Printing

Name	Default setting	VDA
Client printer redirection	Allowed	All VDA versions
Default printer	Set default printer to the client's main printer	All VDA versions
Printer assignments	User's current printer is used as the default printer for the session	All VDA versions
Printer auto-creation event log preference	Log errors and warnings	All VDA versions

Session printers	No printers are specified <b>Default setting</b>	All VDA versions
Wait for printers to be created (desktop)	Disabled	All VDA versions

## ICA/Printing/Client Printers

Name	Default setting	VDA
Auto-create client printers	Auto-create all client printers	All VDA versions
Auto-create generic universal printer	Disabled	All VDA versions
Client printer names	Standard printer names	All VDA versions
Direct connections to print servers	Enabled	All VDA versions
Printer driver mapping and compatibility	No rules are specified	All VDA versions
Printer properties retention	Held in profile only if not saved on client	All VDA versions
Retained and restored client printers	Allowed	VDA 5, 5.5 and 5.6 Feature Pack 1

## ICA/Printing/Drivers

Name	Default setting	VDA
Automatic installation of in-box printer drivers	Enabled	All VDA versions
Universal driver preference	EMF; XPS; PCL5c; PCL4; PS	All VDA versions
Universal print driver usage	Use universal printing only if requested driver is unavailable	All VDA versions

## ICA/Printing/Universal Print Server

Name	Default setting	VDA
Universal Print Server enable	Disabled	All VDA versions
Universal Print Server print data stream (CGP) port	7229	All VDA versions
Universal Print Server print stream input bandwidth limit (kbps)	0	All VDA versions
Universal Print Server web service (HTTP/SOAP) port	8080	All VDA versions

## ICA/Printing/Universal Printing

Name	Default setting	VDA
Universal printing EMF processing mode	Spool directly to printer	All VDA versions
Universal printing image compression limit	Best quality (lossless compression)	All VDA versions
Universal printing optimization defaults	Image Compression <ul style="list-style-type: none"> <li>• Desired image quality = Standard quality</li> <li>• Enable heavyweight compression = False</li> </ul> Image and Font Caching <ul style="list-style-type: none"> <li>• Allow caching of embedded images = True</li> <li>• Allow caching of embedded fonts = True</li> </ul> Allow non-administrators to modify these settings = False	All VDA versions
Universal printing preview preference	Do not use print preview for auto-created or generic universal printers	All VDA versions
Universal printing print quality limit	No limit	All VDA versions

## ICA/Security

Name	Default setting	VDA
SecureICA minimum encryption level	Basic	VDA for Server OS 7 through current VDA for Server OS

## ICA/Server Limits

Name	Default setting	VDA
Server idle timer interval	0 milliseconds	VDA for Server OS 7 through current VDA for Server OS

## ICA/Session Limits

Name	Default setting	VDA
Disconnected session timer	Disabled	VDA 5, 5.5, 5.6 Feature Pack 1, VDA for Desktop OS 7 through current
Disconnected session timer	1440 minutes	VDA 5, 5.5, 5.6 Feature Pack 1, VDA for Desktop OS 7 through

<b>Name</b>	<b>Default setting</b>	<b>VDA</b>
Session connection timer	Disabled	VDA 5, 5.5, 5.6 Feature Pack 1, VDA for Desktop OS 7 through current
Session connection timer interval	1440 minutes	VDA 5, 5.5, 5.6 Feature Pack 1, VDA for Desktop OS 7 through current
Session idle timer	Enabled	VDA 5, 5.5, 5.6 Feature Pack 1, VDA for Desktop OS 7 through current
Session idle timer interval	1440 minutes	VDA 5, 5.5, 5.6 Feature Pack 1, VDA for Desktop OS 7 through current

## ICA/Session Reliability

<b>Name</b>	<b>Default setting</b>	<b>VDA</b>
Session reliability connections	Allowed	All VDA versions
Session reliability port number	2598	All VDA versions
Session reliability timeout	180 seconds	All VDA versions

## ICA/Time Zone Control

<b>Name</b>	<b>Default setting</b>	<b>VDA</b>
Estimate local time for legacy clients	Enabled	VDA for Server OS 7 through current
Use local time of client	Use server time zone	All VDA versions

## ICA/TWAIN Devices

<b>Name</b>	<b>Default setting</b>	<b>VDA</b>
Client TWAIN device redirection	Allowed	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current
TWAIN compression level	Medium	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current

## ICA/USB Devices

<b>Name</b>	<b>Default setting</b>	<b>VDA</b>
Client USB device optimization rules	No rules are specified	VDA 7.6 FP3 through current

Client USB device redirection	Prohibited	All VDA versions
Client USB device redirection rules	No rules are specified	All VDA versions
Client USB Plug and Play device redirection	Allowed	VDA for Server OS 7 and VDA for Desktop OS 7 through current

## ICA/Visual Display

Name	Default setting	VDA
Preferred color depth for simple graphics	24 bits per pixel	VDA 7.6 FP3 through current
Target frame rate	30 fps	All VDA versions
Visual quality	Medium	VDA for Server OS 7 and VDA for Desktop OS 7 through current
Use video codec for compression	Use video codec when available	VDA 7.6 FP3 through current

## ICA/Visual Display/Moving Images

Name	Default setting	VDA
Minimum image quality	Normal	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current
Moving image compression	Enabled	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current
Progressive compression level	None	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current
Progressive compression threshold value	2147483647 Kbps	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current
Target minimum frame rate	10 fps	VDA 5.5, 5.6 Feature Pack 1, VDA for Server OS 7 and VDA for Desktop OS 7 through current

## ICA/Visual Display/Still Images

<b>Name</b>	<b>Default setting</b>	<b>VDA</b>
Extra color compression	Disabled	All VDA versions
Extra color compression threshold	8192 Kbps	All VDA versions
Heavyweight compression	Disabled	All VDA versions
Lossy compression level	Medium	All VDA versions
Lossy compression threshold value	2147483647 Kbps	All VDA versions

## ICA/WebSockets

<b>Name</b>	<b>Default setting</b>	<b>VDA</b>
WebSockets connections	Prohibited	VDA for Server OS 7 and VDA for Desktop OS 7 through current
WebSockets port number	8008	VDA for Server OS 7 and VDA for Desktop OS 7 through current
WebSockets trusted origin server list	The wildcard, *, is used to trust all Receiver for Web URLs	VDA for Server OS 7 and VDA for Desktop OS 7 through current

## Load Management

<b>Name</b>	<b>Default setting</b>	<b>VDA</b>
Concurrent logon tolerance	2	VDA for Server OS 7 through current
CPU usage	Disabled	VDA for Server OS 7 through current
CPU usage excluded process priority	Below Normal or Low	VDA for Server OS 7 through current
Disk usage	Disabled	VDA for Server OS 7 through current
Maximum number of sessions	250	VDA for Server OS 7 through current
Memory usage	Disabled	VDA for Server OS 7 through current
Memory usage base load	Zero load: 768MB	VDA for Server OS 7 through current

## Profile Management/Advanced settings

<b>Name</b>	<b>Default setting</b>	<b>VDA</b>
Disable automatic configuration	Disabled	All VDA versions

<b>Name</b> Log off user if a problem is encountered	Disabled	All VDA versions
Number of retries when accessing locked files	5	All VDA versions
Process Internet cookie files on logoff	Disabled	All VDA versions

## Profile Management/Basic settings

<b>Name</b>	<b>Default setting</b>	<b>VDA</b>
Active write back	Disabled	All VDA versions
Enable Profile management	Disabled	All VDA versions
Excluded groups	Disabled. Members of all user groups are processed.	All VDA versions
Offline profile support	Disabled	All VDA versions
Path to user store	Windows	All VDA versions
Process logons of local administrators	Disabled	All VDA versions
Processed groups	Disabled. Members of all user groups are processed.	All VDA versions

## Profile Management/Cross-Platform Settings

<b>Name</b>	<b>Default setting</b>	<b>VDA</b>
Cross-platform settings user groups	Disabled. All user groups specified in Processed groups are processed	All VDA versions
Enable cross-platform settings	Disabled	All VDA versions
Path to cross-platform definitions	Disabled. No path is specified.	All VDA versions
Path to cross-platform settings store	Disabled. Windows\PM_CM is used.	All VDA versions
Source for creating cross-platform settings	Disabled	All VDA versions

## Profile Management/File System/Exclusions

<b>Name</b>	<b>Default setting</b>	<b>VDA</b>
Exclusion list - directories	Disabled. All folders in the user profile are synchronized.	All VDA versions
Exclusion list - files	Disabled. All files in the user profile are synchronized.	All VDA versions

## Profile Management/File System/Synchronization

Name	Default setting	VDA
Directories to synchronize	Disabled. Only non-excluded folders are synchronized.	All VDA versions
Files to synchronize	Disabled. Only non-excluded files are synchronized.	All VDA versions
Folders to mirror	Disabled. No folders are mirrored.	All VDA versions

## Profile Management/Folder Redirection

Name	Default setting	VDA
Grant administrator access	Disabled	All VDA versions
Include domain name	Disabled	All VDA versions

## Profile Management/Folder Redirection/AppData(Roaming)

Name	Default setting	VDA
AppData(Roaming) path	Disabled. No location is specified.	All VDA versions
Redirection settings for AppData(Roaming)	Contents are redirected to the UNC path specified in the AppData(Roaming) path policy settings	All VDA versions

## Profile Management/Folder Redirection/Contacts

Name	Default setting	VDA
Contacts path	Disabled. No location is specified.	All VDA versions
Redirection settings for Contacts	Contents are redirected to the UNC path specified in the Contacts path policy settings	All VDA versions

## Profile Management/Folder Redirection/Desktop

Name	Default setting	VDA
Desktop path	Disabled. No location is specified.	All VDA versions
Redirection settings for Desktop	Contents are redirected to the UNC path specified in the Desktop path policy settings	All VDA versions

## Profile Management/Folder Redirection/Documents

<b>Name</b>	<b>Default setting</b>	<b>VDA</b>
Documents path	Disabled. No location is specified.	All VDA versions
Redirection settings for Documents	Contents are redirected to the UNC path specified in the Documents path policy settings	All VDA versions

#### Profile Management/Folder Redirection/Downloads

<b>Name</b>	<b>Default setting</b>	<b>VDA</b>
Downloads path	Disabled. No location is specified.	All VDA versions
Redirection settings for Downloads	Contents are redirected to the UNC path specified in the Downloads path policy settings	All VDA versions

#### Profile Management/Folder Redirection/Favorites

<b>Name</b>	<b>Default setting</b>	<b>VDA</b>
Favorites path	Disabled. No location is specified.	All VDA versions
Redirection settings for Favorites	Contents are redirected to the UNC path specified in the Favorites path policy settings	All VDA versions

#### Profile Management/Folder Redirection/Links

<b>Name</b>	<b>Default setting</b>	<b>VDA</b>
Links path	Disabled. No location is specified.	All VDA versions
Redirection settings for Links	Contents are redirected to the UNC path specified in the Links path policy settings	All VDA versions

#### Profile Management/Folder Redirection/Music

<b>Name</b>	<b>Default setting</b>	<b>VDA</b>
Music path	Disabled. No location is specified.	All VDA versions
Redirection settings for Music	Contents are redirected to the UNC path specified in the Music path policy settings	All VDA versions

## Profile Management/Folder Redirection/Pictures

Name	Default setting	VDA
Pictures path	Disabled. No location is specified.	All VDA versions
Redirection settings for Pictures	Contents are redirected to the UNC path specified in the Pictures path policy settings	All VDA versions

## Profile Management/Folder Redirection/Saved Games

Name	Default setting	VDA
Saved Games path	Disabled. No location is specified.	All VDA versions
Redirection settings for Saved Games	Contents are redirected to the UNC path specified in the Saved Games path policy settings	All VDA versions

## Profile Management/Folder Redirection/Searches

Name	Default setting	VDA
Searches path	Disabled. No location is specified.	All VDA versions
Redirection settings for Searches	Contents are redirected to the UNC path specified in the Searches path policy settings	All VDA versions

## Profile Management/Folder Redirection/Start Menu

Name	Default setting	VDA
Start Menu path	Disabled. No location is specified.	All VDA versions
Redirection settings for Start Menu	Contents are redirected to the UNC path specified in the Start Menu path policy settings	All VDA versions

## Profile Management/Folder Redirection/Video

Name	Default setting	VDA
Video path	Disabled. No location is specified.	All VDA versions
Redirection settings for Video	Contents are redirected to the UNC path specified in the Video path policy settings	All VDA versions

Name	Default setting	VDA
Profile Management/Log settings		
Active Directory actions	Disabled	All VDA versions
Common information	Disabled	All VDA versions
Common warnings	Disabled	All VDA versions
Enable logging	Disabled	All VDA versions
File system actions	Disabled	All VDA versions
File system notifications	Disabled	All VDA versions
Logoff	Disabled	All VDA versions
Logon	Disabled	All VDA versions
Maximum size of the log file	1048576	All VDA versions
Path to log file	Disabled. Log files are saved in the default location; %SystemRoot%\System32\Logfiles\UserProfileManager.	All VDA versions
Personalized user information	Disabled	All VDA versions
Policy values at logon and logoff	Disabled	All VDA versions
Registry actions	Disabled	All VDA versions
Registry differences at logoff	Disabled	All VDA versions

## Profile Management/Profile handling

Name	Default setting	VDA

<b>Name</b>	<b>Default setting</b>	All VDA versions
Delete locally cached profiles on logoff	Disabled	All VDA versions
Local profile conflict handling	Use local profile	All VDA versions
Migration of existing profiles	Local and roaming	All VDA versions
Path to the template profile	Disabled. New user profiles are created from the default user profile on the device where a user first logs on.	All VDA versions
Template profile overrides local profile	Disabled	All VDA versions
Template profile overrides roaming profile	Disabled	All VDA versions
Template profile used as a Citrix mandatory profile for all logons	Disabled	All VDA versions

#### Profile Management/Registry

<b>Name</b>	<b>Default setting</b>	<b>VDA</b>
Exclusion list	Disabled. All registry keys in the HKCU hive are processed when a user logs off.	All VDA versions
Inclusion list	Disabled. All registry keys in the HKCU hive are processed when a user logs off.	All VDA versions

#### Profile Management/Streamed user profiles

<b>Name</b>	<b>Default setting</b>	<b>VDA</b>
Always cache	Disabled	All VDA versions
Always cache size	0 Mb	All VDA versions
Profile streaming	Disabled	All VDA versions
Streamed user profile groups	Disabled. All user profiles within an OU are processed normally.	All VDA versions
Timeout for pending area lock files (days)	1 day	All VDA versions

## Receiver

Name	Default setting	VDA
StoreFront accounts list	No stores are specified	VDA for Server OS 7 and VDA for Desktop OS 7 through current

## Virtual Delivery Agent

Name	Default setting	VDA
Controller registration IPv6 netmask	No netmask is specified	VDA for Server OS 7 and VDA for Desktop OS 7 through current
Controller registration port	80	All VDA versions
Controller SIDs	No SIDs are specified	All VDA versions
Controllers	No controllers are specified	All VDA versions
Enable auto update of controllers	Enabled	VDA for Server OS 7 and VDA for Desktop OS 7 through current
Only use IPv6 controller registration	Disabled	VDA for Server OS 7 and VDA for Desktop OS 7 through current
Site GUID	No GUID is specified	All VDA versions

## Virtual IP

Name	Default setting	VDA
Virtual IP loopback support	Disabled	VDA 7.6
Virtual IP virtual loopback programs list	None	VDA 7.6

## HDX 3D Pro

Name	Default setting	VDA
Enable lossless	Enabled	VDA 5.5 and 5.6 Feature Pack 1
HDX 3D Pro quality settings		VDA 5.5 and 5.6 Feature Pack 1

# 策略设置参考

May 28, 2016

Policies contain settings that are applied when the policy is enforced. Descriptions in this section also indicate if additional settings are required to enable a feature or are similar to a setting.

## Quick reference

The following tables list the settings you can configure within a policy. Find the task you want to complete in the left column, then locate its corresponding setting in the right column.

## Audio

For this task	Use this policy setting
Control whether to allow the use of multiple audio devices	Audio Plug N Play
Control whether to allow audio input from microphones on the user device	Client microphone redirection
Control audio quality on the user device	Audio quality
Control audio mapping to speakers on the user device	Client audio redirection

## Bandwidth for user devices

To limit bandwidth used for	Use this policy setting
Client audio mapping	<ul style="list-style-type: none"><li>● Audio redirection bandwidth limit or</li><li>● Audio redirection bandwidth limit percent</li></ul>
Cut-and-paste using local clipboard	<ul style="list-style-type: none"><li>● Clipboard redirection bandwidth limit or</li><li>● Clipboard redirection bandwidth limit percent</li></ul>
Access in a session to local client drives	<ul style="list-style-type: none"><li>● File redirection bandwidth limit or</li><li>● File redirection bandwidth limit percent</li></ul>
HDX MediaStream Multimedia Acceleration	<ul style="list-style-type: none"><li>● HDX MediaStream Multimedia Acceleration bandwidth limit or</li><li>● HDX MediaStream Multimedia Acceleration bandwidth limit percent</li></ul>

<b>To limit bandwidth used for Client session</b>	<b>Use this policy setting</b> Overall session bandwidth limit
Printing	<ul style="list-style-type: none"> <li>• Printer redirection bandwidth limit or</li> <li>• Printer redirection bandwidth limit percent</li> </ul>
TWAIN devices (such as a camera or scanner)	<ul style="list-style-type: none"> <li>• TWAIN device redirection bandwidth limit or</li> <li>• TWAIN device redirection bandwidth limit percent</li> </ul>
USB devices	<ul style="list-style-type: none"> <li>• Client USB device redirection bandwidth limit or</li> <li>• Client USB device redirection bandwidth limit percent</li> </ul>

## Redirection of client drives and user devices

<b>For this task</b>	<b>Use this policy setting</b>
Control whether or not drives on the user device are connected when users log on to the server	Auto connect client drives
Control cut-and-paste data transfer between the server and the local clipboard	Client clipboard redirection
Control how drives map from the user device	Client drive redirection
Control whether users' local hard drives are available in a session	<ul style="list-style-type: none"> <li>• Client fixed drives and</li> <li>• Client drive redirection</li> </ul>
Control whether users' local floppy drives are available in a session	<ul style="list-style-type: none"> <li>• Client floppy drives and</li> <li>• Client drive redirection</li> </ul>
Control whether users' network drives are available in a session	<ul style="list-style-type: none"> <li>• Client network drives and</li> <li>• Client drive redirection</li> </ul>
Control whether users' local CD, DVD, or Blu-ray drives are available in a session	<ul style="list-style-type: none"> <li>• Client optical drives and</li> <li>• Client drive redirection</li> </ul>
Control whether users' local removable drives are available in a session	<ul style="list-style-type: none"> <li>• Client removable drives and</li> <li>• Client drive redirection</li> </ul>
Control whether users' TWAIN devices, such as scanners and	<ul style="list-style-type: none"> <li>• Client TWAIN device redirection</li> </ul>

<b>For this task</b> cameras, are available in a session and control compression of image data transfers	<b>Use this policy setting</b> TWAIN compression redirection
Control whether USB devices are available in a session	<ul style="list-style-type: none"> <li>Client USB device redirection and</li> <li>Client USB device redirection rules</li> </ul>
Improve the speed of writing and copying files to a client disk over a WAN	Use asynchronous writes

## Content redirection

<b>For this task</b>	<b>Use this policy setting</b>
Control whether to use content redirection from the server to the user device	Host to client redirection

## Desktop UI

<b>For this task</b>	<b>Use this policy setting</b>
Control whether or not Desktop wallpaper is used in users' sessions	Desktop wallpaper
View window contents while a window is dragged	View window contents while dragging

## Graphics and multimedia

<b>For this task</b>	<b>Use this policy setting</b>
Control the maximum number of frames per second sent to user devices from virtual desktops	Target frame rate
Control the visual quality of images displayed on the user device	Visual quality
Control whether Flash content is rendered in sessions	Flash default behavior
Control whether websites can display Flash content when accessed in sessions	<ul style="list-style-type: none"> <li>Flash server-side content fetching URL list</li> <li>Flash URL compatibility list</li> </ul>

<b>For this task</b>	<ul style="list-style-type: none"> <li>● <b>Use this policy setting</b></li> <li>● Flash video fallback prevention policy setting</li> <li>● Flash video fallback prevention error *.swf</li> </ul>
----------------------	---

## Prioritize Multi-Stream network traffic

<b>For this task</b>	<b>Use this policy setting</b>
Specify ports for ICA traffic across multiple connections and establish network priorities	Multi-Port policy
Enable support for multi-stream connections between servers and user devices	Multi-Stream (computer and user settings)

## Print

<b>For this task</b>	<b>Use this policy setting</b>
Control creation of client printers on the user device	<ul style="list-style-type: none"> <li>● Auto-create client printers and</li> <li>● Client printer redirection</li> </ul>
Control the location where printer properties are stored	Printer properties retention
Control whether print requests are processed by the client or the server	Direct connections to print servers
Control whether users can access printers connected to their user devices	Client printer redirection
Control installation of native Windows drivers when automatically creating client and network printers	Automatic installation of in-box printer drivers
Control when to use the Universal Printer Driver	Universal print driver usage
Choose a printer based on a roaming user's session information	Default printer

Note: Policies cannot be used to enable a screen saver in a desktop or application session. For users who require screen savers, the screen saver can be implemented on the user device.

# ICA 策略设置

May 28, 2016

The ICA section contains policy settings related to ICA listener connections and mapping to the clipboard.

## Client clipboard redirection

This setting allows or prevents the clipboard on the user device being mapped to the clipboard on the server.

By default, clipboard redirection is allowed.

To prevent cut-and-paste data transfer between a session and the local clipboard, select Prohibit. Users can still cut and paste data between applications running in sessions.

After allowing this setting, configure the maximum allowed bandwidth the clipboard can consume in a client connection using the Clipboard redirection bandwidth limit or the Clipboard redirection bandwidth limit percent settings.

## Client clipboard write allowed formats

When the Restrict client clipboard write setting is Enabled, host clipboard data cannot be shared with the client endpoint but you can use this setting to allow specific data formats to be shared with the client endpoint clipboard. To use this setting, enable it and add the specific formats to be allowed.

The following clipboard formats are system defined:

- CF\_TEXT
- CF\_BITMAP
- CF\_METAFILEPICT
- CF\_SYLK
- CF\_DIF
- CF\_TIFF
- CF\_OEMTEXT
- CF\_DIB
- CF\_PALETTE
- CF\_PENDATA
- CF\_RIFF
- CF\_WAVE
- CF\_UNICODETEXT
- CF\_ENHMETAFILE
- CF\_HDROP
- CF\_LOCALE
- CF\_DIBV5
- CF\_OWNERDISPLAY
- CF\_DSPTEXT
- CF\_DSPBITMAP
- CF\_DSPMETAFILEPICT
- CF\_DISPENHMETAFILE

The following custom formats are predefined in XenApp and XenDesktop:

- CFX\_RICHTEXT

- CFX\_OfficeDrawingShape
- CFX\_BIFF8

Additional custom formats can be added. The custom format name must match the formats to be registered with the system. Format names are case-sensitive.

This setting does not apply if either Client clipboard redirection or Restrict client clipboard write is set to Prohibited.

#### Desktop launches

This setting allows or prevents non-administrative users in a VDA's Direct Access Users group connecting to a session on that VDA using an ICA connections.

By default, non-administrative users cannot connect to these sessions.

This setting has no effect on non-administrative users in a VDA's Direct Access Users group who are using a RDP connection; these users can connect to the VDA whether this setting is enabled or disabled. This setting has no effect on non-administrative users not in a VDA's Direct Access Users group; these users cannot connect to the VDA whether this setting is enabled or disabled.

#### ICA listener connection timeout

**Note:** This setting applies only to these Virtual Delivery Agents: 5.0, 5.5, and 5.6 Feature Pack 1.

This setting specifies the maximum wait time for a connection using the ICA protocol to be completed.

By default, the maximum wait time is 120000 milliseconds, or two minutes.

#### ICA listener port number

This setting specifies the TCP/IP port number used by the ICA protocol on the server.

By default, the port number is set to 1494.

Valid port numbers must be in the range of 0-65535 and must not conflict with other well-known port numbers. If you change the port number, restart the server for the new value to take effect. If you change the port number on the server, you must also change it on every Receiver or plug-in that connects to the server.

#### Launching of non-published programs during client connection

This setting specifies whether to allow launching initial applications through RDP on the server.

By default, launching initial applications through RDP on the server is not allowed.

#### Restrict client clipboard write

If this setting is Allowed, host clipboard data cannot be shared with the client endpoint. You can allow specific formats by enabling the Client clipboard write allowed formats setting.

By default, this is set to Prohibited.

#### Restrict session clipboard write

When this setting is Allowed, client clipboard data cannot be shared within the user session. You can allow specific formats by enabling the Session clipboard write allowed formats setting.

By default, this is set to Prohibited.

## Session clipboard write allowed formats

When the Restrict session clipboard write setting is Allowed, client clipboard data cannot be shared with session applications, but you can use this setting to allow specific data formats to be shared with the session clipboard.

The following clipboard formats are system defined:

- CF\_TEXT
- CF\_BITMAP
- CF\_METAFILEPICT
- CF\_SYLK
- CF\_DIF
- CF\_TIFF
- CF\_OEMTEXT
- CF\_DIB
- CF\_PALETTE
- CF\_PENDATA
- CF\_RIFF
- CF\_WAVE
- CF\_UNICODETEXT
- CF\_ENHMETAFILE
- CF\_HDROP
- CF\_LOCALE
- CF\_DIBV5
- CF\_OWNERDISPLAY
- CF\_DSPTEXT
- CF\_DSPBITMAP
- CF\_DSPMETAFILEPICT
- CF\_DISPENHMETAFILE

The following custom formats are predefined in XenApp and XenDesktop:

- CFX\_RICHTEXT
- CFX\_OfficeDrawingShape
- CFX\_BIFF8

Additional custom formats can be added. The custom format name must match the formats to be registered with the system. Format names are case-sensitive.

This setting does not apply if either the Client clipboard redirection setting or Restrict session clipboard write setting is set to Prohibited.

# 客户端自动重新连接策略设置

May 28, 2016

The Auto Client Reconnect section contains policy settings for controlling the automatic reconnection of sessions.

## Auto client reconnect

This setting allows or prevents automatic reconnection by the same client after a connection has been interrupted.

By default, automatic reconnection is allowed.

Allowing automatic reconnection allows users to resume working where they were interrupted when a connection was broken. Automatic reconnection detects broken connections and then reconnects the users to their sessions.

However, automatic reconnection can result in a new session being launched (instead of reconnecting to an existing session) if the Receiver's cookie, which contains the key to the session ID and credentials, is not used. The cookie is not used if it has expired, for example, because of a delay in reconnection, or if credentials must be reentered. Auto client reconnect is not triggered if users intentionally disconnect.

For application sessions, when automatic reconnection is allowed, Receiver attempts to reconnect to the session until there is a successful reconnection or the user cancels the reconnection attempts.

For desktop sessions, when automatic reconnection is allowed, Receiver attempts to reconnect to the session for a specified period of time, unless there is a successful reconnection or the user cancels the reconnection attempts. By default, this period of time is five minutes. To change this period of time, edit this registry on the user device:

`HKLM\Software\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds; DWORD;<seconds>`

where <seconds> is the number of seconds after which no more attempts are made to reconnect the session.

## Auto client reconnect authentication

This setting requires authentication for automatic client reconnections.

By default, authentication is not required.

When a user initially logs on, their credentials are encrypted, stored in memory, and a cookie is created containing the encryption key that is sent to Receiver. When this setting is configured, cookies are not used. Instead, a dialog box is displayed to users requesting credentials when Receiver attempts to reconnect automatically.

## Auto client reconnect logging

This setting enables or disables the recording of auto client reconnections in the event log.

By default, logging is disabled.

When logging is enabled, the server's System log captures information about successful and failed automatic reconnection events. A site does not provide a combined log of reconnection events for all servers.

# 音频策略设置

Jan 10, 2017

The Audio section contains policy settings that permit user devices to send and receive audio in sessions without reducing performance.

## Audio over UDP real-time transport

This setting allows or prevents the transmission and receipt of audio between the VDA and user device over RTP using the User Datagram Protocol (UDP). When this setting is disabled, audio is sent and received over TCP.

By default, audio over UDP is allowed.

## Audio Plug N Play

This setting allows or prevents the use of multiple audio devices to record and play sound.

By default, the use of multiple audio devices is allowed.

This setting applies only to Windows Server OS machines.

## Audio quality

This setting specifies the quality level of sound received in user sessions.

By default, sound quality is set to High - high definition audio.

To control sound quality, choose one of the following options:

- Select Low - for low speed connections for low-bandwidth connections. Sounds sent to the user device are compressed up to 16 Kbps. This compression results in a significant decrease in the quality of the sound but allows reasonable performance for a low-bandwidth connection.
- Select Medium - optimized for speech to deliver Voice over IP (VoIP) applications, to deliver media applications in challenging network connections with lines less than 512 Kbps, or significant congestion and packet loss. This codec offers very fast encode time, making it ideal for use with softphones and Unified Communications applications when you require server-side media processing.

Audio sent to the user device is compressed up to 64 Kbps; this compression results in a moderate decrease in the quality of the audio played on the user device, while providing low latency and consuming low bandwidth. If VoIP quality is unsatisfactory, ensure that the Audio over UDP Real-time Transport policy setting is set to Allowed.

Currently, Real-time Transport (RTP) over UDP is only supported when this audio quality is selected. Use this audio quality even for delivering media applications for the challenging network connections like very low (less than 512Kbps) lines and when there is congestion and packet loss in the network.

- Select High - high definition audio for connections where bandwidth is plentiful and sound quality is important. Clients can play sound at its native rate. Sounds are compressed at a high quality level maintaining up to CD quality, and using up to 112 Kbps of bandwidth. Transmitting this amount of data can result in increased CPU utilization and network congestion.

Bandwidth is consumed only while audio is recording or playing. If both occur at the same time, the bandwidth consumption is doubled.

To specify the maximum amount of bandwidth, configure the Audio redirection bandwidth limit or the Audio redirection bandwidth limit percent settings.

### Client audio redirection

This setting specifies whether applications hosted on the server can play sounds through a sound device installed on the user device. This setting also specifies whether users can record audio input.

By default, audio redirection is allowed.

After allowing this setting, you can limit the bandwidth consumed by playing or recording audio. Limiting the amount of bandwidth consumed by audio can improve application performance but may also degrade audio quality. Bandwidth is consumed only while audio is recording or playing. If both occur at the same time, the bandwidth consumption doubles. To specify the maximum amount of bandwidth, configure the Audio redirection bandwidth limit or the Audio redirection bandwidth limit percent settings.

On Windows Server OS machines, ensure that the Audio Plug N Play setting is Enabled to support multiple audio devices.

**Important:** Prohibiting Client audio redirection disables all HDX audio functionality.

### Client microphone redirection

This setting enables or disables client microphone redirection. When enabled, users can use microphones to record audio input in a session.

By default, microphone redirection is allowed.

For security, users are alerted when servers that are not trusted by their devices try to access microphones. Users can choose to accept or not accept access. Users can disable the alert on Citrix Receiver.

On Windows Server OS machines, ensure that the Audio Plug N Play setting is Enabled to support multiple audio devices.

If the Client audio redirection setting is disabled on the user device, this rule has no effect.

# 带宽策略设置

May 28, 2016

The Bandwidth section contains policy settings to avoid performance problems related to client session bandwidth use.

Important: Using these policy settings with the Multi-Stream policy settings may produce unexpected results. If you use Multi-Stream settings in a policy, ensure these bandwidth limit policy settings are not included.

## Audio redirection bandwidth limit

This setting specifies the maximum allowed bandwidth, in kilobits per second, for playing or recording audio in a user session.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the Audio redirection bandwidth limit percent setting, the most restrictive setting (with the lower value) is applied.

## Audio redirection bandwidth limit percent

This setting specifies the maximum allowed bandwidth limit for playing or recording audio as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the Audio redirection bandwidth limit setting, the most restrictive setting (with the lower value) is applied.

If you configure this setting, you must also configure the Overall session bandwidth limit setting, which specifies the total amount of bandwidth available for client sessions.

## Client USB device redirection bandwidth limit

This setting specifies the maximum allowed bandwidth, in kilobits per second, for the redirection of USB devices to and from the client.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the Client USB device redirection bandwidth limit percent setting, the most restrictive setting (with the lower value) is applied.

## Client USB device redirection bandwidth limit percent

This setting specifies the maximum allowed bandwidth for the redirection of USB devices to and from the client as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the Client USB device redirection bandwidth limit setting, the most restrictive setting (with the lower value) is applied.

If you configure this setting, you must also configure the Overall session bandwidth limit setting, which specifies the total amount of bandwidth available for client sessions.

## Clipboard redirection bandwidth limit

This setting specifies the maximum allowed bandwidth, in kilobits per second, for data transfer between a session and the local clipboard.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the Clipboard redirection bandwidth limit percent setting, the most restrictive setting (with the lower value) is applied.

#### Clipboard redirection bandwidth limit

This setting specifies the maximum allowed bandwidth for data transfer between a session and the local clipboard as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the Clipboard redirection bandwidth limit setting, the most restrictive setting (with the lower value) is applied.

If you configure this setting, you must also configure the Overall session bandwidth limit setting, which specifies the total amount of bandwidth available for client sessions.

#### COM port redirection bandwidth limit

Note: For the Virtual Delivery Agent 7.x, configure this setting using the registry; see [Configure COM Port and LPT Port Redirection settings using the registry](#).

This setting specifies the maximum allowed bandwidth in kilobits per second for accessing a COM port in a client connection. If you enter a value for this setting and a value for the COM port redirection bandwidth limit percent setting, the most restrictive setting (with the lower value) is applied.

#### COM port redirection bandwidth limit percent

Note: For the Virtual Delivery Agent 7.x, configure this setting using the registry; see [Configure COM Port and LPT Port Redirection settings using the registry](#).

This setting specifies the maximum allowed bandwidth for accessing COM ports in a client connection as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified

If you enter a value for this setting and a value for the COM port redirection bandwidth limit setting, the most restrictive setting (with the lower value) is applied.

If you configure this setting, you must also configure the Overall session bandwidth limit setting, which specifies the total amount of bandwidth available for client sessions

#### File redirection bandwidth limit

This setting specifies the maximum allowed bandwidth, in kilobits per second, for accessing a client drive in a user session.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the File redirection bandwidth limit percent setting, the most restrictive setting (with the lower value) takes effect.

#### File redirection bandwidth limit percent

This setting specifies the maximum allowed bandwidth limit for accessing client drives as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the File redirection bandwidth limit setting, the most restrictive setting (with the lower value) is applied.

If you configure this setting, you must also configure the Overall session bandwidth limit setting, which specifies the total amount of bandwidth available for client sessions.

#### HDX MediaStream Multimedia Acceleration bandwidth limit

This setting specifies the maximum allowed bandwidth limit, in kilobits per second, for delivering streaming audio and video using HDX MediaStream Multimedia Acceleration.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the HDX MediaStream Multimedia Acceleration bandwidth limit percent setting, the most restrictive setting (with the lower value) takes effect.

#### HDX MediaStream Multimedia Acceleration bandwidth limit percent

This setting specifies the maximum allowed bandwidth for delivering streaming audio and video using HDX MediaStream Multimedia Acceleration as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the HDX MediaStream Multimedia Acceleration bandwidth limit setting, the most restrictive setting (with the lower value) takes effect.

If you configure this setting, you must also configure the Overall session bandwidth limit setting, which specifies the total amount of bandwidth available for client sessions.

#### LPT port redirection bandwidth limit

Note: For the Virtual Delivery Agent 7.x, configure this setting using the registry; see [Configure COM Port and LPT Port Redirection settings using the registry](#).

This setting specifies the maximum allowed bandwidth, in kilobits per second, for print jobs using an LPT port in a single user session.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the LPT port redirection bandwidth limit percent setting, the most restrictive setting (with the lower value) is applied.

#### LPT port redirection bandwidth limit percent

Note: For the Virtual Delivery Agent 7.x, configure this setting using the registry; see [Configure COM Port and LPT Port Redirection settings using the registry](#).

This setting specifies the bandwidth limit for print jobs using an LPT port in a single client session as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the LPT port redirection bandwidth limit setting, the most restrictive setting (with the lower value) is applied.

If you configure this setting, you must also configure the Overall session bandwidth limit setting, which specifies the total amount of bandwidth available for client sessions.

#### Overall session bandwidth limit

This setting specifies the total amount of bandwidth available, in kilobits per second, for user sessions.

The maximum enforceable bandwidth cap is 10 Mbps (10,000 Kbps). By default, no maximum (zero) is specified.

Limiting the amount of bandwidth consumed by a client connection can improve performance when other applications outside the client connection are competing for limited bandwidth.

#### Printer redirection bandwidth limit

This setting specifies the maximum allowed bandwidth, in kilobits per second, for accessing client printers in a user session.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the Printer redirection bandwidth limit percent setting, the most restrictive setting (with the lower value) is applied.

#### Printer redirection bandwidth limit percent

This setting specifies the maximum allowed bandwidth for accessing client printers as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the Printer redirection bandwidth limit setting, the most restrictive setting (with the lower value) is applied.

If you configure this setting, you must also configure the Overall session bandwidth limit setting, which specifies the total amount of bandwidth available for client sessions.

#### TWAIN device redirection bandwidth limit

This setting specifies the maximum allowed bandwidth, in kilobits per second, for controlling TWAIN imaging devices from published applications.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the TWAIN device redirection bandwidth limit percent setting, the most restrictive setting (with the lower value) is applied.

#### TWAIN device redirection bandwidth limit percent

This setting specifies the maximum allowed bandwidth for controlling TWAIN imaging devices from published applications as a percentage of the total session bandwidth.

By default, no maximum (zero) is specified.

If you enter a value for this setting and a value for the TWAIN device redirection bandwidth limit setting, the most

restrictive setting (with the lower value) is applied.

If you configure this setting, you must also configure the Overall session bandwidth limit setting, which specifies the total amount of bandwidth available for client sessions.

# 客户端传感器策略设置

May 28, 2016

The Client Sensors section contains policy settings for controlling how mobile device sensor information is handled in a user session.

## Allow applications to use the physical location of the client device

This setting determines whether applications running in a session on a mobile device are allowed to use the physical location of the user device.

By default, the use of location information is prohibited

When this setting is prohibited, attempts by an application to retrieve location information return a "permission denied" value.

When this setting is allowed, a user can prohibit use of location information by denying a Receiver request to access the location. Android and iOS devices prompt at the first request for location information in each session.

When developing hosted applications that use the Allow applications to use the physical location of the client device setting, consider the following:

- A location-enabled application should not rely on location information being available because:
  - A user might not allow access to location information.
  - The location might not be available or might change while the application is running.
  - A user might connect to the application session from a different device that does not support location information.
- A location-enabled application must:
  - Have the location feature off by default.
  - Provide a user option to allow or disallow the feature while the application is running.
  - Provide a user option to clear location data that is cached by the application. (Receiver does not cache location data.)
- A location-enabled application must manage the granularity of the location information so that the data acquired is appropriate to the purpose of the application and conforms to regulations in all relevant jurisdictions.
- A secure connection (for example, using SSL/TLS or a VPN) should be enforced when using location services. Citrix Receiver should connect to trusted servers.
- Consider obtaining legal advice regarding the use of location services.

# 桌面 UI 策略设置

Aug 08, 2016

The Desktop UI section contains policy settings that control visual effects such as desktop wallpaper, menu animations, and drag-and-drop images, to manage the bandwidth used in client connections. You can improve application performance on a WAN by limiting bandwidth usage.

## Desktop Composition Redirection

This setting specifies whether to use the processing capabilities of the graphics processing unit (GPU) or integrated graphics processor (IGP) on the user device for local DirectX graphics rendering to provide users with a more fluid Windows desktop experience. When enabled, Desktop Composition Redirection delivers a highly responsive Windows experience while maintaining high scalability on the server.

By default, Desktop Composition Redirection is disabled.

To turn off Desktop Composition Redirection and reduce the bandwidth required in user sessions, select Disabled when adding this setting to a policy.

## Desktop Composition Redirection graphics quality

This setting specifies the quality of graphics used for Desktop Composition Redirection.

By default, this is set to high.

Choose from High, Medium, Low, or Lossless quality.

## Desktop wallpaper

This setting allows or prevents wallpaper showing in user sessions.

By default, user sessions can show wallpaper.

To turn off desktop wallpaper and reduce the bandwidth required in user sessions, select Prohibited when adding this setting to a policy.

## Menu animation

This setting allows or prevents menu animation in user sessions.

By default, menu animation is allowed.

Menu animation is a Microsoft personal preference setting for ease of access. When enabled, it causes a menu to appear after a short delay, either by scrolling or fading in. An arrow icon appears at the bottom of the menu. The menu appears when you point to that arrow.

Menu animation is enabled on a desktop if this policy setting is set to Allowed and the menu animation Microsoft personal preference setting is enabled.

Note: Changes to the menu animation Microsoft personal preference setting are changes to the desktop. This means that if the desktop is set to discard changes when the session ends, a user who has enabled menu animations in a session may not have menu animation available in subsequent sessions on the desktop. For users who require menu animation, enable

the Microsoft setting in the master image for the desktop or ensure that the desktop retains user changes.  
View window contents while dragging

This setting allows or prevents the display of window contents when dragging a window across the screen.

By default, viewing window contents is allowed.

When set to Allowed, the entire window appears to move when you drag it. When set to Prohibited, only the window outline appears to move until you drop it.

# 最终用户监控策略设置

May 28, 2016

The End User Monitoring section contains policy settings for measuring session traffic.

## ICA round trip calculation

This setting determines whether ICA round trip calculations are performed for active connections.

By default, calculations for active connections are enabled.

By default, each ICA round trip measurement initiation is delayed until some traffic occurs that indicates user interaction. This delay can be indefinite in length and is designed to prevent the ICA round trip measurement being the sole reason for ICA traffic.

## ICA round trip calculation interval

This setting specifies the frequency, in seconds, at which ICA round trip calculations are performed.

By default, ICA round trip is calculated every 15 seconds.

## ICA round trip calculations for idle connections

This setting determines whether ICA round trip calculations are performed for idle connections.

By default, calculations are not performed for idle connections.

By default, each ICA round trip measurement initiation is delayed until some traffic occurs that indicates user interaction. This delay can be indefinite in length and is designed to prevent the ICA round trip measurement being the sole reason for ICA traffic.

# Enhanced Desktop Experience 策略设置

May 28, 2016

The Enhanced Desktop Experience policy setting sessions running on server operating systems to look like local Windows 7 desktops, providing users with an enhanced desktop experience.

By default, this setting is allowed.

If a user profile with Windows Classic theme already exists on the virtual desktop, enabling this policy does not provide an enhanced desktop experience for that user. If a user with a Windows 7 theme user profile logs on to a virtual desktop running Windows Server 2012 for which this policy is either not configured or disabled, that user sees an error message indicating failure to apply the theme.

In both cases, resetting the user profile resolves the issue.

If the policy changes from enabled to disabled on a virtual desktop with active user sessions, the look and feel of those sessions is inconsistent with both the Windows 7 and Windows Classic desktop experience. To avoid this, ensure you restart the virtual desktop after changing this policy setting. You must also delete any roaming profiles on the virtual desktop. Citrix also recommends deleting any other user profiles on the virtual desktop to avoid inconsistencies between profiles.

If you are using roaming user profiles in your environment, ensure the Enhanced Desktop Experience feature is enabled or disabled for all virtual desktops that share a profile.

Citrix does not recommend sharing roaming profiles between virtual desktops running server operating systems and client operating systems. Profiles for client and server operating systems differ and sharing roaming profiles across both types can lead to inconsistencies in profile properties when a user moves between the two.

# 文件重定向策略设置

Oct 04, 2016

The File Redirection section contains policy settings relating to client drive mapping and client drive optimization.

## Auto connect client drives

This setting allows or prevents automatic connection of client drives when users log on.

By default, automatic connection is allowed.

When adding this setting to a policy, make sure to enable the settings for the drive types you want automatically connected. For example, to allow automatic connection of users' CD-ROM drives, configure this setting and the Client optical drives setting.

The following policy settings are related:

- Client drive redirection
- Client floppy drives
- Client optical drives
- Client fixed drives
- Client network drives
- Client removable drives

## Client drive redirection

This setting enables or disables file redirection to and from drives on the user device.

By default, file redirection is enabled.

When enabled, users can save files to all their client drives. When disabled, all file redirection is prevented, regardless of the state of the individual file redirection settings such as Client floppy drives and Client network drives.

The following policy settings are related:

- Client floppy drives
- Client optical drives
- Client fixed drives
- Client network drives
- Client removable drives

## Client fixed drives

This setting allows or prevents users from accessing or saving files to fixed drives on the user device.

By default, accessing client fixed drives is allowed.

When adding this setting to a policy, make sure the Client drive redirection setting is present and set to Allowed. If these settings are disabled, client fixed drives are not mapped and users cannot access these drives manually, regardless of the state of the Client fixed drives setting.

To ensure fixed drives are automatically connected when users log on, configure the Auto connect client drives setting.

## Client floppy drives

This setting allows or prevents users from accessing or saving files to floppy drives on the user device.

By default, accessing client floppy drives is allowed.

When adding this setting to a policy, make sure the Client drive redirection setting is present and set to Allowed. If these settings are disabled, client floppy drives are not mapped and users cannot access these drives manually, regardless of the state of the Client floppy drives setting.

To ensure floppy drives are automatically connected when users log on, configure the Auto connect client drives setting.

## Client network drives

This setting allows or prevents users from accessing and saving files to network (remote) drives through the user device.

By default, accessing client network drives is allowed.

When adding this setting to a policy, make sure the Client drive redirection setting is present and set to Allowed. If these settings are disabled, client network drives are not mapped and users cannot access these drives manually, regardless of the state of the Client network drives setting.

To ensure network drives are automatically connected when users log on, configure the Auto connect client drives setting.

## Client optical drives

This setting allows or prevents users from accessing or saving files to CD-ROM, DVD-ROM, and BD-ROM drives on the user device.

By default, accessing client optical drives is allowed.

When adding this setting to a policy, make sure the Client drive redirection setting is present and set to Allowed. If these settings are disabled, client optical drives are not mapped and users cannot access these drives manually, regardless of the state of the Client optical drives setting.

To ensure optical drives are automatically connected when users log on, configure the Auto connect client drives setting.

## Client removable drives

This setting allows or prevents users from accessing or saving files to USB drives on the user device.

By default, accessing client removable drives is allowed.

When adding this setting to a policy, make sure the Client drive redirection setting is present and set to Allowed. If these settings are disabled, client removable drives are not mapped and users cannot access these drives manually, regardless of the state of the Client removable drives setting.

To ensure removable drives are automatically connected when users log on, configure the Auto connect client drives setting.

## Host to client redirection

This setting enables or disables file type associations for URLs and some media content to be opened on the user device. When disabled, content opens on the server.

By default, file type association is disabled.

These URL types are opened locally when you enable this setting:

- Hypertext Transfer Protocol (HTTP)
- Secure Hypertext Transfer Protocol (HTTPS)
- Real Player and QuickTime (RTSP)
- Real Player and QuickTime (RTSPU)
- Legacy Real Player (PNM)
- Microsoft Media Server (MMS)

For more information, see the article on [Host to client redirection](#).

#### Preserve client drive letters

This setting enables or disables mapping of client drives to the same drive letter in the session.

By default, client drive letters are not preserved.

When adding this setting to a policy, make sure the Client drive redirection setting is present and set to Allowed.

#### Read-only client drive access

This setting allows or prevents users and applications from creating or modifying files or folders on mapped client drives.

By default, files and folders on mapped client drives can be modified.

If set to Enabled, files and folders are accessible with read-only permissions.

When adding this setting to a policy, make sure the Client drive redirection setting is present and set to Allowed.

#### Special folder redirection

This setting allows or prevents Citrix Receiver and Web Interface users to see their local Documents and Desktop special folders from a session.

By default, special folder redirection is allowed.

This setting prevents any objects filtered through a policy from having special folder redirection, regardless of settings that exist elsewhere. When this setting is prohibited, any related settings specified for StoreFront, Web Interface, or Citrix Receiver are ignored.

To define which users can have special folder redirection, select Allowed and include this setting in a policy filtered on the users you want to have this feature. This setting overrides all other special folder redirection settings.

Because special folder redirection must interact with the user device, policy settings that prevent users from accessing or saving files to their local hard drives also prevent special folder redirection from working.

When adding this setting to a policy, make sure the Client fixed drives setting is present and set to Allowed.

#### Use asynchronous writes

This setting enables or disables asynchronous disk writes.

By default, asynchronous writes are disabled.

Asynchronous disk writes can improve the speed of file transfers and writing to client disks over WANs, which are typically characterized by relatively high bandwidth and high latency. However, if there is a connection or disk fault, the client file or files being written may end in an undefined state. If this happens, a pop-up window informs the user of the files affected. The user can then take remedial action such as restarting an interrupted file transfer on reconnection or when the disk fault is corrected.

Citrix recommends enabling asynchronous disk writes only for users who need remote connectivity with good file access speed and who can easily recover files or data lost in the event of connection or disk failure.

When adding this setting to a policy, make sure that the Client drive redirection setting is present and set to Allowed. If this setting is disabled, asynchronous writes will not occur.

# Flash 重定向策略设置

May 28, 2016

The Flash Redirection section contains policy settings for handling Flash content in user sessions.

## Flash acceleration

This setting enables or disables Flash content rendering on user devices instead of the server. By default, client-side Flash content rendering is enabled.

Note: This setting is used for legacy Flash redirection with the Citrix online plug-in 12.1.

When enabled, this setting reduces network and server load by rendering Flash content on the user device. Additionally, the Flash URL compatibility list setting forces Flash content from specific websites to be rendered on the server.

On the user device, the Enable HDX MediaStream for Flash on the user device setting must be enabled as well.

When this setting is disabled, Flash content from all websites, regardless of URL, is rendered on the server. To allow only certain websites to render Flash content on the user device, configure the Flash URL compatibility list setting.

## Flash background color list

This setting enables you to set key colors for given URLs.

By default, no key colors are specified.

Key colors appear behind client-rendered Flash and help provide visible region detection. The key color specified should be rare; otherwise, visible region detection might not work properly.

Valid entries consist of a URL (with optional wildcards at the beginning or end) followed by a 24-bit RGB color hexadecimal code. For example: `http://citrix.com 000003`.

Ensure that the URL specified is the URL for the Flash content, which might be different from the URL of the website.

### 警告

Using Registry Editor incorrectly can cause serious problems that can require you to reinstall the operating system. Citrix cannot guarantee that problems resulting from incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Make sure you back up the registry before you edit it.

On VDA machines running Windows 8 or Windows 2012, this setting might fail to set key colors for the URL. If this occurs, edit the registry on the VDA machine.

For 32-bit machines, use this registry setting:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer]  
"ForceHDXFlashEnabled"=dword:00000001
```

For 64-bit machines, use this registry setting:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer]
```

"ForceHDXFlashEnabled"=dword:00000001

## Flash backwards compatibility

This setting enables or disables the use of original, legacy Flash redirection features with older versions of Citrix Receiver (formerly the Citrix online plug-in).

By default, this setting is enabled.

On the user device, the Enable HDX MediaStream for Flash on the user device setting must also be enabled.

Second generation Flash redirection features are enabled for use with Citrix Receiver 3.0. Legacy redirection features are supported for use with the Citrix online plug-in 12.1. To ensure second generation Flash redirection features are used, both the server and the user device must have second generation Flash redirection enabled. If legacy redirection is enabled on either the server or the user device, legacy redirection features are used.

## Flash default behavior

This setting establishes the default behavior for second generation Flash acceleration.

By default, Flash acceleration is enabled.

To configure this setting, choose one of the following options:

- Enable Flash acceleration. Flash Redirection is used.
- Block Flash Player. Flash Redirection and server-side rendering are not used. The user cannot view any Flash content.
- Disable Flash acceleration. Flash Redirection is not used. The user can view server-side rendered Flash content if a version of Adobe Flash Player for Windows Internet Explorer compatible with the content is installed on the server.

This setting can be overridden for individual Web pages and Flash instances based on the configuration of the Flash URL compatibility list setting. Additionally, the user device must have the Enable HDX MediaStream for Flash on the user device setting enabled.

## Flash event logging

This setting enables Flash events to be recorded in the Windows application event log.

By default, logging is allowed.

On computers running Windows 7 or Windows Vista, a Flash redirection-specific log appears in the Applications and Services Log node.

## Flash intelligent fallback

This setting enables or disables automatic attempts to employ server-side rendering for Flash Player instances where client-side rendering is either unnecessary or provides a poor user experience.

By default, this setting is enabled.

## Flash latency threshold

This setting specifies a threshold between 0-30 milliseconds to determine where Adobe Flash content is rendered.

By default, the threshold is 30 milliseconds.

During startup, HDX MediaStream for Flash measures the current latency between the server and user device. If the latency is under the threshold, HDX MediaStream for Flash is used to render Flash content on the user device. If the latency is above the threshold, the network server renders the content if an Adobe Flash player is available there.

When enabling this setting, make sure the Flash backwards compatibility setting is also present and set to Enabled.

Note: Applies only when using HDX MediaStream Flash redirection in Legacy mode.

#### Flash video fallback prevention

This setting specifies if and how "small" flash content is rendered and displayed to users.

By default, this setting is not configured.

To configure this setting, choose one of the following options:

- **Only small content.** Only intelligent fallback content will be rendered on the server; other Flash content will be replaced with an error \*.swf.
- **Only small content with a supported client.** Only intelligent fallback content will be rendered on the server if the client is currently using Flash Redirection; other content will be replaced with an error \*.swf.
- **No server side content.** All content on the server will be replaced with an error \*.swf.

To use this policy setting you should specify an error \*.swf file. This error \*.swf will replace any content that you do not want to be rendered on the VDA.

#### Flash video fallback prevention error \*.swf

This setting specifies the URL of the error message which is displayed to users to replace Flash instances when the server load management policies are in use. For example:

`http://domainName.tld/sample/path/error.swf`

#### Flash server-side content fetching URL list

This setting specifies websites whose Flash content can be downloaded to the server and then transferred to the user device for rendering.

By default, no sites are specified.

This setting is used when the user device does not have direct access to the Internet; the server provides that connection. Additionally, the user device must have the Enable server-side content fetching setting enabled.

Second generation Flash redirection includes a fallback to server-side content fetching for Flash .swf files. If the user device is unable to fetch Flash content from a Web site, and the Web site is specified in the Flash server-side content fetching URL list, server-side content fetching occurs automatically.

When adding URLs to the list:

- Add the URL of the Flash application instead of the top-level HTML page that initiates the Flash Player.
- Use an asterisk (\*) at the beginning or end of the URL as a wildcard.
- Use a trailing wildcard to allow all child URLs (`http://www.citrix.com/*`).
- The prefixes `http://` and `https://` are used when present, but are not required for valid list entries.

#### Flash URL compatibility list

This setting specifies the rules which determine whether Flash content on certain websites is rendered on the user device, rendered on the server, or blocked from rendering.

By default, no rules are specified.

When adding URLs to the list:

- Prioritize the list with the most important URLs, actions, and rendering locations at the top.
- Use an asterisk (\*) at the beginning or end of the URL as a wildcard.
- Use a trailing wildcard to refer to all child URLs ([http://www.citrix.com/\\*](http://www.citrix.com/*)).
- The prefixes http:// and https:// are used when present, but are not required for valid list entries.
- Add to this list websites whose Flash content does not render correctly on the user device and select either the Render on Server or Block options.

# 图形策略设置

May 28, 2016

The Graphics section contains policy settings for controlling how images are handled in user sessions.

## Display memory limit

This setting specifies the maximum video buffer size in kilobytes for the session.

By default, the display memory limit is 65536 kilobytes.

For connections requiring more color depth and higher resolution, increase the limit. Calculate the maximum memory required using the equation:

Memory depth in bytes = (color-depth-in-bits-per-pixel) / 8 \* (vertical-resolution-in-pixels) \* (horizontal-resolution-in-pixels).

For example, with a color depth of 32, vertical resolution of 600, and a horizontal resolution of 800, the maximum memory required is  $(32 / 8) * (600) * (800) = 1920000$  bytes, which yields a display memory limit of 1920 KB.

Color depths other than 32-bit are available only if the Legacy graphics mode policy setting is enabled.

HDX allocates only the amount of display memory needed for each session. So, if only some users require more than the default, there is no negative impact on scalability by increasing the display memory limit.

## Display mode degrade preference

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting specifies whether color depth or resolution degrades first when the session display memory limit is reached.

By default, color depth is degraded first.

When the session memory limit is reached, you can reduce the quality of displayed images by choosing whether color depth or resolution is degraded first. When color depth is degraded first, displayed images use fewer colors. When resolution is degraded first, displayed images use fewer pixels per inch.

To notify users when either color depth or resolution are degraded, configure the Notify user when display mode is degraded setting.

## Dynamic windows preview

This setting enables or disables the display of seamless windows in Flip, Flip 3D, Taskbar Preview, and Peek window preview modes.

Windows Aero preview option	Description
Taskbar Preview	When the user hovers over a window's taskbar icon, an image of that window appears above the taskbar.
Windows Peek	When the user hovers over a taskbar preview image, a full-sized image of the window appears on the screen.

Flip Windows Aero preview option	Description
Flip 3D	When the user presses ALT+TAB, small preview icons are shown for each open window.

By default, this setting is enabled.

### Image caching

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting enables or disables the caching and retrieving of sections of images in sessions. Caching images in sections and retrieving these sections when needed makes scrolling smoother, reduces the amount of data transmitted over the network, and reduces the processing required on the user device.

By default, the image caching setting is enabled.

Note: The image caching setting controls how images are cached and retrieved; it does not control whether images are cached. Images are cached if the Legacy graphics mode setting is enabled.

### Legacy graphics mode

This setting disables the rich graphics experience, providing fallback to the legacy graphics experience to improve scalability over a WAN or mobile connection.

By default, this setting is disabled and users are provided with the rich graphics experience.

### Maximum allowed color depth

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting specifies the maximum color depth allowed for a session.

By default, the maximum allowed color depth is 32 bits per pixel.

This setting applies only to ThinWire drivers and connections. It does not apply to VDAs that have a non-ThinWire driver as the primary display driver, such as VDAs that use a Windows Display Driver Model (WDDM) driver as the primary display driver. For Desktop OS VDAs using a WDDM driver as the primary display driver, such as Windows 8, this setting has no effect. For Windows Server OS VDAs using a WDDM driver, such as Windows Server 2012 R2, this setting might prevent users from connecting to the VDA.

Setting a high color depth requires more memory. To degrade color depth when the memory limit is reached, configure the Display mode degrade preference setting. When color depth is degraded, displayed images use fewer colors.

### Notify user when display mode is degraded

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting displays a brief explanation to the user when the color depth or resolution is degraded.

By default, notifying users is disabled.

### Queuing and tossing

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting discards queued images that are replaced by another image.

By default, queuing and tossing is enabled.

This improves response when graphics are sent to the user device. Configuring this setting can cause animations to become choppy because of dropped frames.

# 缓存策略设置

May 28, 2016

The Caching section contains policy settings that enable caching image data on user devices when client connections are limited in bandwidth.

## Persistent cache threshold

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting caches bitmaps on the hard drive of the user device. This enables re-use of large, frequently-used images from previous sessions.

By default, the threshold is 3000000 bits per second.

The threshold value represents the point below which the Persistent Cache feature will take effect. For example, using the default value, bitmaps are cached on the hard drive of the user device when bandwidth falls below 3000000 bps.

# 保持活动状态策略设置

May 28, 2016

The Keep Alive section contains policy settings for managing ICA keep-alive messages.

## ICA keep alive timeout

This setting specifies the number of seconds between successive ICA keep-alive messages.

By default, the interval between keep-alive messages is 60 seconds.

Specify an interval between 1-3600 seconds in which to send ICA keep-alive messages. Do not configure this setting if your network monitoring software is responsible for closing inactive connections.

## ICA keep alives

This setting enables or disables sending ICA keep-alive messages periodically.

By default, keep-alive messages are not sent.

Enabling this setting prevents broken connections from being disconnected. If the server detects no activity, this setting prevents Remote Desktop Services (RDS) from disconnecting the session. The server sends keep-alive messages every few seconds to detect if the session is active. If the session is no longer active, the server marks the session as disconnected.

ICA keep-alive does not work if you are using session reliability. Configure ICA keep-alive only for connections that are not using Session Reliability.

Related policy settings: Session reliability connections.

# 移动体验策略设置

May 28, 2016

The Mobile Experience section contains policy settings for handling the Citrix Mobility Pack.

## Automatic keyboard display

This setting enables or disables the automatic display of the keyboard on mobile device screens.

By default, the automatic display of the keyboard is disabled.

## Launch touch-optimized desktop

This setting is disabled and not available for Windows 10 machines.

This setting determines the overall Receiver interface behavior by allowing or prohibiting a touch-friendly interface that is optimized for tablet devices.

By default, a touch-friendly interface is used.

To use only the Windows interface, set this policy setting to Prohibited.

## Remote the combo box

This setting determines the types of combo boxes you can display in sessions on mobile devices. To display the device-native combo box control, set this policy setting to Allowed. When this setting is allowed, a user can change a Receiver for iOS session setting to use the Windows combo box.

By default, the Remote the combo box feature is prohibited.

# 多媒体策略设置

Apr 13, 2017

The Multimedia section contains policy settings for managing streaming audio and video in user sessions.

## Limit video quality

This setting specifies the maximum video quality level allowed for an HDX connection. When configured, maximum video quality is limited to the specified value, ensuring that multimedia Quality of Service (QoS) is maintained within an environment.

By default, this setting is not configured.

To limit the maximum video quality level allowed, choose one of the following options:

- 1080p/8.5mbps
- 720p/4.0mbps
- 480p/720kbps
- 380p/400kbps
- 240p/200kbps

Note: Playing multiple videos simultaneously on the same server consumes large amounts of resources and may impact server scalability.

## Multimedia conferencing

This setting allows or prevents support for video conferencing applications.

By default, video conferencing support is allowed.

When adding this setting to a policy, make sure the Windows Media Redirection setting is present and set to Allowed.

When using multimedia conferencing, make sure the following conditions are met:

- Manufacturer-supplied drivers for the web cam used for multimedia conferencing must be installed.
- The web cam must be connected to the user device before initiating a video conferencing session. The server uses only one installed web cam at any given time. If multiple web cams are installed on the user device, the server attempts to use each web cam in succession until a video conferencing session is created successfully.

## Optimization for Windows Media multimedia redirection over WAN

This setting enables real-time multimedia transcoding, allowing audio and video media streaming to mobile devices, and enhancing the user experience by improving how Windows Media content is delivered over a WAN.

By default, the delivery of Windows Media content over the WAN is optimized.

When adding this setting to a policy, make sure the Windows Media Redirection setting is present and set to Allowed.

When this setting is enabled, real-time multimedia transcoding is deployed automatically as needed to enable media streaming, providing a seamless user experience even in extreme network conditions.

## Use GPU for optimizing Windows Media multimedia redirection over WAN

This setting enables real-time multimedia transcoding to be done in the Graphics Processing Unit (GPU) on the Virtual

Delivery Agent (VDA), to improve server scalability. GPU transcoding is available only if the VDA has a supported GPU for hardware acceleration. Otherwise, transcoding falls back to the CPU.

Note: GPU transcoding is supported only on NVIDIA GPUs.

By default, using the GPU on the VDA to optimize the delivery of Windows Media content over the WAN is prohibited.

When adding this setting to a policy, make sure the Windows Media Redirection and Optimization for Windows Media multimedia redirection over WAN settings are present and set to Allowed.

## Windows media fallback prevention

Administrators can use the Windows media fallback prevention policy setting to specify the methods that will be attempted to deliver streamed content to users.

By default, this setting is not configured. When the setting is set to Not Configured, the behavior is the same as **Play all content**.

To configure this setting, choose one of the following options:

- **Play all content**. Attempt client-side content fetching, then Windows Media Redirection. If unsuccessful, play content on the server.
- **Play all content only on client**. Attempt client-side fetching, then Windows Media Redirection. If unsuccessful, the content does not play.
- **Play only client-accessible content on client**. Attempt only client-side fetching. If unsuccessful, the content does not play.

When the content does not play, the error message "Company has blocked video because of lack of resources" displays in the player window (for a default duration of 5 seconds).

The duration of this error message can be customized with the following registry key on the VDA. If the registry entry does not exist, the duration defaults to 5 seconds.

## Windows Media client-side content fetching

This setting enables a user device to stream multimedia files directly from the source provider on the Internet or Intranet, rather than through the host server.

By default, the streaming of multimedia files to the user device direct from the source provider is allowed.

Allowing this setting improves network utilization and server scalability by moving any processing on the media from the host server to the user device. It also removes the requirement that an advanced multimedia framework such as Microsoft DirectShow or Media Foundation be installed on the user device; the user device requires only the ability to play a file from a URL.

When adding this setting to a policy, make sure the Windows Media Redirection setting is present and set to Allowed. If this setting is disabled, the streaming of multimedia files to the user device direct from the source provider is also disabled.

## Windows Media Redirection

This setting controls and optimizes the way servers deliver streaming audio and video to users.

By default, the delivery of streaming audio and video to users is allowed.

Allowing this setting increases the quality of audio and video rendered from the server to a level that compares with audio and video played locally on a user device. The server streams multimedia to the client in the original, compressed form and allows the user device to decompress and render the media.

Windows Media redirection optimizes multimedia files that are encoded with codecs that adhere to Microsoft DirectShow, DirectX Media Objects (DMO), and Media Foundation standards. To play back a given multimedia file, a codec compatible with the encoding format of the multimedia file must be present on the user device.

By default, audio is disabled on Citrix Receiver. To allow users to run multimedia applications in ICA sessions, turn on audio or give users permission to turn on audio in their Receiver interface.

Select Prohibited only if playing media using Windows Media redirection appears worse than when rendered using basic ICA compression and regular audio. This is rare but can happen under low bandwidth conditions, for example, with media with a very low frequency of key frames.

#### Windows Media Redirection buffer size

This setting specifies a buffer size from 1 to 10 seconds for multimedia acceleration.

By default, the buffer size is 5 seconds.

#### Windows Media Redirection buffer size use

This setting enables or disables using the buffer size specified in the Windows Media Redirection buffer size setting.

By default, the buffer size specified is not used.

If this setting is disabled or if the Windows Media Redirection buffer size setting is not configured, the server uses the default buffer size value (5 seconds).

# 多流连接策略设置

May 28, 2016

The Multi-Stream Connections section contains policy settings for managing Quality of Service (QoS) prioritization for multiple ICA connections in a session.

## Audio over UDP

This setting allows or prevents audio over UDP on the server.

By default, audio over UDP is allowed on the server.

When enabled, this setting opens a UDP port on the server to support all connections configured to use Audio over UDP Realtime Transport.

## Audio UDP port range

This setting specifies the range of port numbers (in the form lowest port number,highest port number) used by the Virtual Delivery Agent (VDA) to exchange audio packet data with the user device. The VDA attempts to use each UDP port pair to exchange data with the user device, starting with the lowest and incrementing by two for each subsequent attempt. Each port handles both inbound and outbound traffic.

By default, this is set to 16500,16509.

## Multi-Port policy

This setting specifies the TCP ports to be used for ICA traffic and establishes the network priority for each port.

By default, the primary port (2598) has a High priority.

When you configure ports, you can assign the following priorities:

- Very High - for real-time activities, such as webcam conferences
- High - for interactive elements, such as screen, keyboard, and mouse
- Medium - for bulk processes, such as client drive mapping
- Low - for background activities, such as printing

Each port must have a unique priority. For example, you cannot assign a Very High priority to both CGP port 1 and CGP port 3.

To remove a port from prioritization, set the port number to 0. You cannot remove the primary port and you cannot modify its priority level.

When configuring this setting, restart the server. This setting takes effect only when the Multi-Stream computer setting policy setting is enabled.

## Multi-Stream computer setting

This setting enables or disables Multi-Stream on the server.

By default, Multi-Stream is disabled.

If you use Citrix Cloudbridge with Multi-Stream support in your environment, you do not need to configure this setting.

Configure this policy setting when using third-party routers or legacy Branch Repeaters to achieve the desired Quality of Service (QoS).

When configuring this setting, reboot the server to ensure changes take effect.

**Important:** Using this policy setting in conjunction with bandwidth limit policy settings such as Overall session bandwidth limit may produce unexpected results. When including this setting in a policy, ensure that bandwidth limit settings are not included.

#### Multi-Stream user setting

This setting enables or disables Multi-Stream on the user device.

By default, Multi-Stream is disabled for all users.

This setting takes effect only on hosts where the Multi-Stream computer setting policy setting is enabled.

**Important:** Using this policy setting with bandwidth limit policy settings such as Overall session bandwidth limit may produce unexpected results. When including this setting in a policy, ensure that bandwidth limit settings are not included.

# 端口重定向策略设置

May 28, 2016

The Port Redirection section contains policy settings for client LPT and COM port mapping.

Note: For the Virtual Delivery Agent 7.x, configure these settings using the registry; see [Configure COM Port and LPT Port Redirection settings using the registry](#).

## Auto connect client COM ports

This setting enables or disables automatic connection of COM ports on user devices when users log on to a site.

By default, client COM ports are not automatically connected.

## Auto connect client LPT ports

This setting enables or disables automatic connection of LPT ports on user devices when users log on to a site.

By default, client LPT ports are not connected automatically.

## Client COM port redirection

This setting allows or prevents access to COM ports on the user device.

By default, COM port redirection is prohibited.

The following policy settings are related:

- COM port redirection bandwidth limit
- COM port redirection bandwidth limit percent

## Client LPT port redirection

This setting allows or prevents access to LPT ports on the user device.

By default, LPT port redirection is prohibited.

LPT ports are used only by legacy applications that send print jobs to the LPT ports and not to the print objects on the user device. Most applications today can send print jobs to printer objects. This policy setting is necessary only for servers that host legacy applications that print to LPT ports.

The following policy settings are related:

- LPT port redirection bandwidth limit
- LPT port redirection bandwidth limit percent

# 打印策略设置

May 28, 2016

The Printing section contains policy settings for managing client printing.

## Client printer redirection

This setting controls whether client printers are mapped to a server when a user logs on to a session.

By default, client printer mapping is allowed. If this setting is disabled, the PDF printer for the session is not auto-created.

Related policy settings: auto-create client printers

## Default printer

This setting specifies how the default printer on the user device is established in a session.

By default, the user's current printer is used as the default printer for the session.

To use the current Remote Desktop Services or Windows user profile setting for the default printer, select Do not adjust the user's default printer. If you choose this option, the default printer is not saved in the profile and it does not change according to other session or client properties. The default printer in a session will be the first printer auto-created in the session, which is either:

- The first printer added locally to the Windows server in Control Panel > Devices and Printers.
- The first auto-created printer, if there are no printers added locally to the server.

You can use this option to present users with the nearest printer through profile settings (known as proximity printing).

## Printer assignments

This setting provides an alternative to the Default printer and Session printers settings. Use the individual Default printer and Session printers settings to configure behaviors for a site, large group, or organizational unit. Use the Printer assignments setting to assign a large group of printers to multiple users.

This setting specifies how the default printer on the listed user devices is established in a session.

By default, the user's current printer is used as the default printer for the session.

It also specifies the network printers to be auto-created in a session for each user device. By default, no printers are specified.

- When setting the default printer value:

To use the current default printer for the user device, select Do not adjust.

To use the current Remote Desktop Services or Windows user profile setting for the default printer, select Do no adjust. If you choose this option, the default printer is not saved in the profile and it does not change according to other session or client properties. The default printer in a session will be the first printer auto-created in the session, which is either:

- The first printer added locally to the Windows server in Control Panel > Devices and Printers.
  - The first auto-created printer, if there are no printers added locally to the server.
- When setting the session printers value: to add printers, type the UNC path of the printer you want to auto-create.

After adding the printer, you can apply customized settings for the current session at every logon.

#### Printer auto-creation event log preference

This setting specifies the events that are logged during the printer auto-creation process. You can choose to log no errors or warnings, only errors, or errors and warnings.

By default, errors and warnings are logged.

An example of a warning is an event in which a printer's native driver could not be installed and the Universal print driver is installed instead. To use the Universal print driver in this scenario, configure the Universal print driver usage setting to Use universal printing only or Use universal printing only if requested driver is unavailable.

#### Session printers

This setting specifies the network printers to be auto-created in a session.

By default, no printers are specified.

To add printers, type the UNC path of the printer you want to auto-create. After adding the printer, you can apply customized settings for the current session at every logon.

#### Wait for printers to be created (server desktop)

This setting allows or prevents a delay in connecting to a session so that server desktop printers can be auto-created.

By default, a connection delay does not occur.

# 客户端打印机策略设置

May 28, 2016

The Client Printers section contains policy settings for client printers, including settings to auto-create client printers, retain printer properties, and connect to print servers.

## Auto-create client printers

This setting specifies the client printers that are auto-created. This setting overrides default client printer auto-creation settings.

By default, all client printers are auto-created.

This setting takes effect only if the Client printer redirection setting is present and set to Allowed.

When adding this setting to a policy, select an option:

- Auto-create all client printers automatically creates all printers on a user device.
- Auto-create the client's default printer only automatically creates only the printer selected as the default printer on the user device.
- Auto-create local (non-network) client printers only automatically creates only printers directly connected to the user device through an LPT, COM, USB, TCP/IP, or other local port.
- Do not auto-create client printers turns off autocreation for all client printers when users log on. This causes the Remote Desktop Services (RDS) settings for autocreating client printers to override this setting in lower priority policies.

## Auto-create generic universal printer

This setting enables or disables autocreation of the generic Citrix Universal Printer object for sessions where a user device compatible with Universal Printing is in use.

By default, the generic Universal Printer object is not autocreated.

The following policy settings are related:

- Universal print driver usage
- Universal driver preference

## Client printer names

This setting selects the naming convention for auto-created client printers.

By default, standard printer names are used.

Select Standard printer names to use printer names such as "HPLaserJet 4 from clientname in session 3."

Select Legacy printer names to use old-style client printer names and preserve backward compatibility for users or groups using MetaFrame Presentation Server 3.0 or earlier. An example of a legacy printer name is "Client/clientname#/HPLaserJet 4." This option is less secure.

Note: This option is provided only for backwards compatibility with legacy versions of XenApp and XenDesktop.

## Direct connections to print servers

This setting enables or disables direct connections from the virtual desktop or server hosting applications to a print server for client printers hosted on an accessible network share.

By default, direct connections are enabled.

Enable direct connections if the network print server is not across a WAN from the virtual desktop or server hosting applications. Direct communication results in faster printing if the network print server and the virtual desktop or server hosting applications are on the same LAN.

Disable direct connections if the network is across a WAN or has substantial latency or limited bandwidth. Print jobs are routed through the user device where they are redirected to the network print server. Data sent to the user device is compressed, so less bandwidth is consumed as the data travels across the WAN.

If two network printers have the same name, the printer on the same network as the user device is used.

### Printer driver mapping and compatibility

This setting specifies the driver substitution rules for auto-created client printers.

By default, no rules are specified.

When you define driver substitution rules, you can allow or prevent printers to be created with the specified driver. Additionally, you can allow created printers to use only universal print drivers. Driver substitution overrides or maps printer driver names the user device provides, substituting an equivalent driver on the server. This gives server applications access to client printers that have the same drivers as the server, but different driver names.

You can add a driver mapping, edit an existing mapping, override custom settings for a mapping, remove a mapping, or change the order of driver entries in the list. When adding a mapping, enter the client printer driver name and then select the server driver you want to substitute.

### Printer properties retention

This setting specifies whether or not to store printer properties and where to store them.

By default, the system determines if printer properties are stored on the user device, if available, or in the user profile.

When adding this setting to a policy, select an option:

- Saved on the client device only is for user devices that have a mandatory or roaming profile that is not saved. Choose this option only if all the servers in your farm are running XenApp 5 and above and your users are using Citrix online plug-in versions 9 through 12.x, or Citrix Receiver 3.x.
- Retained in user profile only is for user devices constrained by bandwidth (this option reduces network traffic) and logon speed or for users with legacy plug-ins. This option stores printer properties in the user profile on the server and prevents any properties exchange with the user device. Use this option with MetaFrame Presentation Server 3.0 or earlier and MetaFrame Presentation Server Client 8.x or earlier. Note that this is applicable only if a Remote Desktop Services (RDS) roaming profile is used.
- Held in profile only if not saved on client allows the system to determine where printer properties are stored. Printer properties are stored either on the user device, if available, or in the user profile. Although this option is the most flexible, it can also slow logon time and use extra bandwidth for system-checking.
- Do not retain printer properties prevents storing printer properties.

### Retained and restored client printers

This setting enables or disables the retention and re-creation of printers on the user device. By default, client printers are auto-retained and auto-restored.

Retained printers are user-created printers that are created again, or remembered, at the start of the next session. When XenApp recreates a retained printer, it considers all policy settings except the Auto-create client printers setting.

Restored printers are printers fully customized by an administrator, with a saved state that is permanently attached to a client port.

# 驱动程序策略设置

May 28, 2016

The Drivers section contains policy settings related to printer drivers.

## Automatic installation of in-box printer drivers

This setting enables or disables the automatic installation of printer drivers from the Windows in-box driver set or from driver packages staged on the host using pnputil.exe /a.

By default, these drivers are installed as needed.

## Universal driver preference

This setting specifies the order in which universal printer drivers are used, beginning with the first entry in the list.

By default, the preference order is:

- EMF
- XPS
- PCL5c
- PCL4
- PS

You can add, edit, or remove drivers, and change the order of drivers in the list.

## Universal print driver usage

This setting specifies when to use universal printing.

By default, universal printing is used only if the requested driver is unavailable.

Universal printing employs generic printer drivers instead of standard model-specific drivers, potentially simplifying the burden of driver management on host computers. The availability of universal print drivers depends on the capabilities of the user device, host, and print server software. In certain configurations, universal printing might not be available.

When adding this setting to a policy, select an option:

- Use only printer model specific drivers specifies that the client printer uses only the standard model-specific drivers that are auto-created at logon. If the requested driver is unavailable, the client printer cannot be auto-created.
- Use universal printing only specifies that no standard model-specific drivers are used. Only universal print drivers are used to create printers.
- Use universal printing only if requested driver is unavailable uses standard model-specific drivers for printer creation if they are available. If the driver is not available on the server, the client printer is created automatically with the appropriate universal driver.
- Use printer model specific drivers only if universal printing is unavailable uses the universal print driver if it is available. If the driver is not available on the server, the client printer is created automatically with the appropriate model-specific printer driver.

# 通用打印服务器策略设置

May 28, 2016

The Universal Print Server section contains policy settings for handling the Universal Print Server.

## Universal Print Server enable

This setting enables or disables the Universal Print Server feature on the virtual desktop or the server hosting applications. Apply this policy setting to Organizational Units (OUs) containing the virtual desktop or server hosting applications.

By default, the Universal Print Server is disabled.

When adding this setting to a policy, select one of the following options:

- **Enabled with fallback to Windows native remote printing.** Network printer connections are serviced by the Universal Print Server, if possible. If the Universal Print Server is not available, the Windows Print Provider is used. The Windows Print Provider continues to handle all printers previously created with the Windows Print Provider.
- **Enabled with no fallback to Windows native remote printing.** Network printer connections are serviced by the Universal Print Server exclusively. If the Universal Print Server is unavailable, the network printer connection fails. This setting effectively disables network printing through the Windows Print Provider. Printers previously created with the Windows Print Provider are not created while a policy containing this setting is active.
- **Disabled.** The Universal Print Server feature is disabled. No attempt is made to connect with the Universal Print Server when connecting to a network printer with a UNC name. Connections to remote printers continue to use the Windows native remote printing facility.

## Universal Print Server print data stream (CGP) port

This setting specifies the TCP port number used by the Universal Print Server print data stream Common Gateway Protocol (CGP) listener. Apply this policy setting only to OUs containing the print server.

By default, the port number is set to 7229.

Valid port numbers must be in the range of 1 to 65535.

## Universal Print Server print stream input bandwidth limit (kbps)

This setting specifies the upper boundary (in kilobits per second) for the transfer rate of print data delivered from each print job to the Universal Print Server using CGP. Apply this policy setting to OUs containing the virtual desktop or server hosting applications.

By default, the value is 0, which specifies no upper boundary.

## Universal Print Server web service (HTTP/SOAP) port

This setting specifies the TCP port number used by the Universal Print Server's web service (HTTP/SOAP) listener. The Universal Print Server is an optional component that enables the use of Citrix universal print drivers for network printing scenarios. When the Universal Print Server is used, printing commands are sent from XenApp and XenDesktop hosts to the Universal Print Server via SOAP over HTTP. This setting modifies the default TCP port on which the Universal Print Server listens for incoming HTTP/SOAP requests.

You must configure both host and print server HTTP port identically. If you do not configure the ports identically, the host software will not connect to the Universal Print Server. This setting changes the VDA on XenApp and XenDesktop. In

addition, you must change the default port on the Universal Print Server.

By default, the port number is set to 8080.

Valid port numbers must be in the range of 0 to 65535.

# 通用打印策略设置

May 28, 2016

The Universal Printing section contains policy settings for managing universal printing.

## Universal printing EMF processing mode

This setting controls the method of processing the EMF spool file on the Windows user device.

By default, EMF records are spooled directly to the printer.

When adding this setting to a policy, select an option:

- Reprocess EMFs for printer forces the EMF spool file to be reprocessed and sent through the GDI subsystem on the user device. You can use this setting for drivers that require EMF reprocessing but that might not be selected automatically in a session.
- Spool directly to printer, when used with the Citrix Universal print driver, ensures the EMF records are spooled and delivered to the user device for processing. Typically, these EMF spool files are injected directly to the client's spool queue. For printers and drivers that are compatible with the EMF format, this is the fastest printing method.

## Universal printing image compression limit

This setting specifies the maximum quality and the minimum compression level available for images printed with the Citrix Universal print driver.

By default, the image compression limit is set to Best quality (lossless compression).

If No Compression is selected, compression is disabled for EMF printing only.

When adding this setting to a policy, select an option:

- No compression
- Best quality (lossless compression)
- High quality
- Standard quality
- Reduced quality (maximum compression)

When adding this setting to a policy that includes the Universal printing optimization defaults setting, be aware of the following:

- If the compression level in the Universal printing image compression limit setting is lower than the level defined in the Universal printing optimization defaults setting, images are compressed at the level defined in the Universal printing image compression limits setting.
- If compression is disabled, the Desired image quality and Enable heavyweight compression options of the Universal printing optimization defaults setting have no effect in the policy.

## Universal printing optimization defaults

This setting specifies the default values for printing optimization when the universal print driver is created for a session.

- Desired image quality specifies the default image compression limit applied to universal printing. By default, Standard Quality is enabled, meaning that users can only print images using standard or reduced quality compression.
- Enable heavyweight compression enables or disables reducing bandwidth beyond the compression level set by Desired image quality, without losing image quality. By default, heavyweight compression is disabled.

- Image and Font Caching settings specify whether or not to cache images and fonts that appear multiple times in the print stream, ensuring each unique image or font is sent to the printer only once. By default, embedded images and fonts are cached. Note that these settings apply only if the user device supports this behavior.
- Allow non-administrators to modify these settings specifies whether or not users can change the default print optimization settings within a session. By default, users are not allowed to change the default print optimization settings.

Note: All of these options are supported for EMF printing. For XPS printing, only the Desired image quality option is supported.

When adding this setting to a policy that includes the Universal printing image compression limit setting, be aware of the following:

- If the compression level in the Universal printing image compression limit setting is lower than the level defined in the Universal printing optimization defaults setting, images are compressed at the level defined in the Universal printing image compression limits setting.
- If compression is disabled, the Desired image quality and Enable heavyweight compression options of the Universal printing optimization defaults setting have no effect in the policy.

#### Universal printing preview preference

This setting specifies whether or not to use the print preview function for auto-created or generic universal printers.

By default, print preview is not used for auto-created or generic universal printers.

When adding this setting to a policy, select an option:

- Do not use print preview for auto-created or generic universal printers
- Use print preview for auto-created printers only
- Use print preview for generic universal printers only
- Use print preview for both auto-created and generic universal printers

#### Universal printing print quality limit

This setting specifies the maximum dots per inch (dpi) available for generating printed output in a session.

By default, No Limit is enabled, meaning users can select the maximum print quality allowed by the printer to which they connect.

If this setting is configured, it limits the maximum print quality available to users in terms of output resolution. Both the print quality itself and the print quality capabilities of the printer to which the user connects are restricted to the configured setting. For example, if configured to Medium Resolution (600 DPI), users are restricted to printing output with a maximum quality of 600 DPI and the Print Quality setting on the Advanced tab of the Universal Printer dialog box shows resolution settings only up to and including Medium Quality (600 DPI).

When adding this setting to a policy, select an option:

- Draft (150 DPI)
- Low Resolution (300 DPI)
- Medium Resolution (600 DPI)
- High Resolution (1200 DPI)
- No Limit

# 安全策略设置

Nov 27, 2017

The Security section contains the policy setting for configuring session encryption and encryption of logon data.

## SecureICA minimum encryption level

This setting specifies the minimum level at which to encrypt session data sent between the server and a user device.

**Important:**

For the Virtual Delivery Agent 7.x, this policy setting can be used only to enable the encryption of the logon data with RC5 128-bit encryption. Other settings are provided only for backwards compatibility with legacy versions of XenApp and XenDesktop.

For the VDA 7.x, encryption of session data is set using the basic settings of the VDA's Delivery group. If Enable Secure ICA is selected for the Delivery group, session data is encrypted with RC5 (128 bit) encryption. If Enable Secure ICA is not selected for the Delivery group, session data is encrypted with Basic encryption.

When adding this setting to a policy, select an option:

- Basic encrypts the client connection using a non-RC5 algorithm. It protects the data stream from being read directly, but it can be decrypted. By default, the server uses Basic encryption for client-server traffic.
- RC5 (128 bit) logon only encrypts the logon data with RC5 128-bit encryption and the client connection using Basic encryption.
- RC5 (40 bit) encrypts the client connection with RC5 40-bit encryption.
- RC5 (56 bit) encrypts the client connection with RC5 56-bit encryption.
- RC5 (128 bit) encrypts the client connection with RC5 128-bit encryption.

The settings you specify for client-server encryption can interact with any other encryption settings in your environment and your Windows operating system. If a higher priority encryption level is set on either a server or user device, settings you specify for published resources can be overridden.

You can raise encryption levels to further secure communications and message integrity for certain users. If a policy requires a higher encryption level, Receivers using a lower encryption level are denied connection.

SecureICA does not perform authentication or check data integrity. To provide end-to-end encryption for your site, use SecureICA with SSL/TLS encryption.

SecureICA does not use FIPS-compliant algorithms. If this is an issue, configure the server and Receivers to avoid using SecureICA.

SecureICA uses the RC5 block cipher as described in RFC 2040 for confidentiality. The block size is 64 bits (a multiple of 32-bit word units). The key length is 128 bits. The number of rounds is 12.

# 服务器限制策略设置

May 28, 2016

The Server Limits section contains the policy setting for controlling idle connections.

## Server idle timer interval

This setting determines, in milliseconds, how long an uninterrupted user session is maintained if there is no input from the user.

By default, idle connections are not disconnected (server idle timer interval = 0).

### 注意

When this policy setting is used, an "Idle timer expired" dialog box might appear to users when the session has been idle for the specified time. This is a Microsoft dialog box that is not controlled by Citrix policy settings. For more information, see Knowledge Center article [CTX118618](#).

# 会话限制策略设置

May 28, 2016

The Session Limits section contains policy settings that control how long sessions remain connected before they are forced to log off.

## Disconnected session timer

This setting enables or disables a timer that specifies how long a disconnected, locked desktop can remain locked before the session is logged off.

By default, disconnected sessions are not logged off.

## Disconnected session timer interval

This setting specifies how many minutes a disconnected, locked desktop can remain locked before the session is logged off.

By default, the time period is 1440 minutes (24 hours).

## Session connection timer

This setting enables or disables a timer that specifies the maximum duration of an uninterrupted connection between a user device and a desktop.

By default, this timer is disabled.

## Session connection timer interval

This setting specifies the maximum number of minutes for an uninterrupted connection between a user device and a desktop.

By default, the maximum duration is 1440 minutes (24 hours).

## Session idle timer

This setting enables or disables a timer that specifies how long an uninterrupted user device connection to a desktop will be maintained if there is no input from the user.

By default, this timer is enabled.

## Session idle timer interval

This setting specifies how many minutes an uninterrupted user device connection to a desktop will be maintained if there is no input from the user.

By default, idle connections are maintained for 1440 minutes (24 hours).

# 会话可靠性策略设置

May 28, 2016

The Session Reliability section contains policy settings for managing session reliability connections.

## Session reliability connections

This setting allows or prevents sessions to remain open during a loss of network connectivity.

By default, session reliability is allowed.

Session reliability keeps sessions active and on the user's screen when network connectivity is interrupted. Users continue to see the application they are using until network connectivity resumes.

With session reliability, the session remains active on the server. To indicate that connectivity is lost, the user's display freezes and the cursor changes to a spinning hourglass until connectivity is restored. The user continues to access the display during the interruption and can resume interacting with the application when the network connection is restored. Session reliability reconnects users without reauthentication prompts. If you do not want users to be able to reconnect to interrupted sessions without having to reauthenticate, configure the Auto client reconnect authentication setting to require authentication. Users are then prompted to reauthenticate when reconnecting to interrupted sessions.

If you use both session reliability and auto client reconnect, the two features work in sequence. Session reliability closes (or disconnects) the user session after the amount of time specified in the Session reliability timeout setting. After that, the auto client reconnect settings take effect, attempting to reconnect the user to the disconnected session.

## Session reliability port number

This setting specifies the TCP port number for incoming session reliability connections.

By default, the port number is set to 2598.

## Session reliability timeout

This setting specifies the length of time, in seconds, the session reliability proxy waits for a user to reconnect before allowing the session to be disconnected.

By default, this is set to 180 seconds, or three minutes.

Although you can extend the amount of time a session is kept open, this feature is designed to be convenient to the user and it does not prompt the user for reauthentication. As you extend the amount of time a session is kept open, chances increase that a user may get distracted and walk away from the user device, potentially leaving the session accessible to unauthorized users.

# 时区控制策略设置

May 28, 2016

The Time Zone Control section contains policy settings related to using local time in sessions.

## Estimate local time for legacy clients

This setting enables or disables estimating the local time zone of user devices that send inaccurate time zone information to the server.

By default, the server estimates the local time zone when necessary.

This setting is intended for use with legacy receivers or ICA clients that do not send detailed time zone information to the server. When used with receivers that send detailed time zone information to the server, such as supported versions of Receiver for Windows, this setting has no effect.

## Use local time of client

This setting determines the time zone setting of the user session. This can be either the time zone of the user session or the time zone of the user device.

By default, the time zone of the user session is used.

For this setting to take effect, enable the Allow time zone redirection setting in the Group Policy Editor (User Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Device and Resource Redirection).

# TWAIN 设备策略设置

May 28, 2016

The TWAIN devices section contains policy settings related to mapping client TWAIN devices, such as digital cameras or scanners, and optimizing image transfers from server to client.

## 注意

TWAIN 2.0 is not currently supported.

### Client TWAIN device redirection

This setting allows or prevents users from accessing TWAIN devices on the user device from image processing applications hosted on servers. By default, TWAIN device redirection is allowed.

The following policy settings are related:

- TWAIN compression level
- TWAIN device redirection bandwidth limit
- TWAIN device redirection bandwidth limit percent

### TWAIN compression level

This setting specifies the level of compression of image transfers from client to server. Use Low for best image quality, Medium for good image quality, or High for low image quality. By default, medium compression is applied.

# USB 设备策略设置

May 28, 2016

The USB devices section contains policy settings for managing file redirection for USB devices.

## Client USB device optimization rules

As of XenApp and XenDesktop 7.6 FP3 and LTSR, the Client USB device optimization rules can be applied to devices to disable optimization, or to change the optimization mode.

When a user plugs in a USB input device, the host checks if the device is allowed by the USB policy settings. If the device is allowed, the host then checks the **Client USB device optimization rules** for the device. If no rule is specified, then the device is handled as Interactive mode (02). Capture mode (04) is the recommended mode for signature devices. See descriptions below for available modes.

### Good to know

- For the use of Wacom signature pads and tablets, we recommend that you disable the screen saver. Steps on how to do this are at the end of this section.
- Support for the optimization of Wacom STU signature pads and tablets series of products has been preconfigured in the installation of XenApp and XenDesktop policies for XenApp and XenDesktop 7.6 FP3 and LTSR.
- Signature devices work across XenApp and XenDesktop and do not require a driver to be used as a signature device. Wacom has additional software that can be installed to customize the device further. See <http://www.wacom.com/>.
- Drawing tablets. Certain drawing input devices may present as an HID device on PCI/ACPI buses and are not supported. These devices should be attached on a USB host controller on the client to be redirected inside a XenDesktop session.

Policy rules take the format of tag=value expressions separated by whitespace. The following tags are supported:

Tag Name	Description
Mode	The optimization mode is supported for input devices for class=03. Supported modes are:  No optimization - value 01.  Interactive mode - value 02. Recommended for devices such as pen tablets and 3D Pro mice.  Capture mode - value 04. Preferred for devices such as signature pads.
VID	Vendor ID from the device descriptor
PID	Product ID from the device descriptor
REL	Release ID from the device descriptor

Class	Class from either the device descriptor or an interface descriptor
SubClass	Subclass from either the device descriptor or an interface descriptor
Prot	Protocol from either the device descriptor or an interface descriptor

## Examples

Mode=00000004 VID=1230 PID=1230 class=03 #Input device operating in capture mode

Mode=00000002 VID=1230 PID=1230 class=03 #Input device operating in interactive mode (default)

Mode=00000001 VID=1230 PID=1230 class=03 #Input device operating without any optimization

Mode=00000100 VID=1230 PID=1230 # Device setup optimization disabled (default)

Mode=00000200 VID=1230 PID=1230 # Device setup optimization enabled

### Disabling the optimization mode using a registry setting

The optimization mode can be disabled system-wide by a registry flag:

HKLM\System\CurrentControlSet\Services\Icausb\Parameters

**DisableInputOptimization** DWORD - set value to **1**

A system restart is required for this registry change to take effect.

### Disabling the screen saver for Wacom signature pad devices

For the use of Wacom signature pads and tablets, we recommend that you disable the screen saver as follows:

1. Install the **Wacom-STU-Driver** after redirecting the device.
2. Install **Wacom-STU-Display MSI** to gain access to the signature pad control panel.
3. Go to **Control Panel > Wacom STU Display > STU430 or STU530**, and select the tab for your model.
4. Click **Change**, then select **Yes** when the UAC security window pops up.
5. Select **Disable slideshow**, then **Apply**.

Once the setting is set for one signature pad model, it is applied to all models.

### Client USB device redirection

This setting allows or prevents redirection of USB devices to and from the user device.

By default, USB devices are not redirected.

### Client USB device redirection rules

This setting specifies redirection rules for USB devices.

By default, no rules are specified.

When a user plugs in a USB device, the host device checks it against each policy rule in turn until a match is found. The first

match for any device is considered definitive. If the first match is an Allow rule, the device is remoted to the virtual desktop. If the first match is a Deny rule, the device is available only to the local desktop. If no match is found, default rules are used.

Policy rules take the format {Allow:|Deny:} followed by a set of tag= value expressions separated by whitespace. The following tags are supported:

Tag Name	Description
VID	Vendor ID from the device descriptor
PID	Product ID from the device descriptor
REL	Release ID from the device descriptor
Class	Class from either the device descriptor or an interface descriptor
SubClass	Subclass from either the device descriptor or an interface descriptor
Prot	Protocol from either the device descriptor or an interface descriptor

When creating new policy rules, remember:

- Rules are case-insensitive.
- Rules may have an optional comment at the end, introduced by #.
- Blank and pure comment lines are ignored.
- Tags must use the matching operator = (for example, VID=1230\_).
- Each rule must start on a new line or form part of a semicolon-separated list.
- Refer to the USB class codes available from the USB Implementers Forum, Inc. web site.

Examples of administrator-defined USB policy rules:

- Allow: VID=1230 PID=0007 # ANOther Industries, ANOther Flash Drive
- Deny: Class=08 subclass=05 # Mass Storage
- To create a rule that denies all USB devices, use "DENY:" with no other tags.

### Client USB plug and play device redirection

This setting allows or prevents plug-and-play devices such as cameras or point-of-sale (POS) devices to be used in a client session.

By default, plug-and-play device redirection is allowed. When set to Allowed, all plug-and-play devices for a specific user or group are redirected. When set to Prohibited, no devices are redirected.

# 视频显示策略设置

May 28, 2016

The Visual Display section contains policy settings for controlling the quality of images sent from virtual desktops to the user device.

## Preferred color depth for simple graphics

Allows lowering of the color depth at which simple graphics are set to **16 bits per pixel**, potentially improving responsiveness over low bandwidth connections, at the cost of a slight degradation of image quality. This option is supported only when a video codec is not used to compress graphics.

By default, this is set to 24 bits per pixel.

## Target frame rate

This setting specifies the maximum number of frames per second sent from the virtual desktop to the user device.

By default, the maximum is 30 frames per second.

Setting a high number of frames per second (for example, 30) improves the user experience, but requires more bandwidth. Decreasing the number of frames per second (for example, 10) maximizes server scalability at the expense of user experience. For user devices with slower CPUs, specify a lower value to improve the user experience.

## Use video codec for compression

Allows use of a video codec to compress graphics when video decoding is available on the endpoint. When video decoding is not available on the endpoint, or when you specify **Do not use video codec** a combination of still image compression and bitmap caching is used.

By default, this is set to Use video codec when available.

## Visual quality

This setting specifies the desired visual quality for images displayed on the user device.

By default, this is set to Medium.

To specify the quality of images, choose one of the following options:

- **Low**
- **Medium** - Offers the best performance and bandwidth efficiency in most use cases
- **High** - Recommended if you require visually lossless image quality
- **Build to lossless** - Sends lossy images to the user device during periods of high network activity and lossless images after network activity reduces; this setting improves performance over bandwidth-constrained network connections
- **Always lossless** - In cases where preserving image data is vital (for example, when displaying X-ray images where no loss of quality is acceptable), select Always lossless to ensure lossy data is never sent to the user device.

If the **Legacy graphics mode** setting is enabled, the **Visual quality** setting has no effect in the policy.

# 移动图像策略设置

May 28, 2016

The Moving Images section contains settings that enable you to remove or alter compression for dynamic images.

## Minimum image quality

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting specifies the minimum acceptable image quality for Adaptive Display. The less compression used, the higher the quality of images displayed. Choose from Ultra High, Very High, High, Normal, or Low compression.

By default, this is set to Normal.

## Moving image compression

This setting specifies whether or not Adaptive Display is enabled. Adaptive Display automatically adjusts the image quality of videos and transitional slides in slide shows based on available bandwidth. With Adaptive Display enabled, users should see smooth-running presentations with no reduction in quality.

By default, Adaptive Display is enabled.

For VDA versions 7.0 through 7.6, this setting applies only when Legacy graphics mode is enabled. For VDA versions 7.6 FP1, FP2, FP3, and LTSR, this setting applies when Legacy graphics mode is enabled, or when the legacy graphics mode is disabled and a video codec is not used to compress graphics.

When legacy graphics mode is enabled, the session must be restarted before policy changes take effect. Adaptive Display is mutually exclusive with Progressive Display; enabling Adaptive Display disables Progressive Display and vice versa. However, both Progressive Display and Adaptive Display can be disabled at the same time. Progressive Display, as a legacy feature, is not recommended for XenApp or XenDesktop. Setting Progressive threshold Level will disable Adaptive Display.

## Progressive compression level

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting provides a less detailed but faster initial display of images.

By default, no progressive compression is applied.

The more detailed image, defined by the normal lossy compression setting, appears when it becomes available. Use Very High or Ultra High compression for improved viewing of bandwidth-intensive graphics such as photographs.

For progressive compression to be effective, its compression level must be higher than the Lossy compression level setting.

Note: The increased level of compression associated with progressive compression also enhances the interactivity of dynamic images over client connections. The quality of a dynamic image, such as a rotating three-dimensional model, is temporarily decreased until the image stops moving, at which time the normal lossy compression setting is applied.

The following policy settings are related:

- Progressive compression threshold value
- Progressive heavyweight compression

## Progressive compression threshold value

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting represents the maximum bandwidth in kilobits per second for a connection to which progressive compression is applied. This is applied only to client connections under this bandwidth.

By default, the threshold value is 2147483647 kilobits per second.

The following policy settings are related:

- Progressive compression threshold value
- Progressive heavyweight compression

#### Target minimum frame rate

This setting specifies the minimum frame rate per second the system attempts to maintain, for dynamic images, under low bandwidth conditions.

By default, this is set to 10fps.

For VDA versions 7.0 through 7.6, this setting applies only when Legacy graphics mode is enabled. For VDA versions 7.6 FP1, FP2, FP3, and LTSR, this setting applies when the Legacy graphics mode is disabled or enabled.

# 静态图像策略设置

May 28, 2016

The Still Images section contains settings that enable you to remove or alter compression for static images.

## Extra color compression

This setting enables or disables the use of extra color compression on images delivered over client connections that are limited in bandwidth, improving responsiveness by reducing the quality of displayed images.

By default, extra color compression is disabled.

When enabled, extra color compression is applied only when the client connection bandwidth is below the Extra color compression threshold value. When the client connection bandwidth is above the threshold value or Disabled is selected, extra color compression is not applied.

## Extra color compression threshold

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting represents the maximum bandwidth in kilobits per second for a connection below which extra color compression is applied. If the client connection bandwidth drops below the set value, extra color compression, if enabled, is applied.

By default, the threshold value is 8192 kilobits per second.

## Heavyweight compression

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting enables or disables reducing bandwidth beyond progressive compression without losing image quality by using a more advanced, but more CPU-intensive, graphical algorithm.

By default, heavyweight compression is disabled.

If enabled, heavyweight compression applies to all lossy compression settings. It is supported on Citrix Receiver but has no effect on other plug-ins.

The following policy settings are related:

- Progressive compression level
- Progressive compression threshold value

## Lossy compression level

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting controls the degree of lossy compression used on images delivered over client connections that are limited in bandwidth. In such cases, displaying images without compression can be slow.

By default, medium compression is selected.

For improved responsiveness with bandwidth-intensive images, use high compression. Where preserving image data is vital;

for example, when displaying X-ray images where no loss of quality is acceptable, you may not want to use lossy compression.

Related policy setting: Lossy compression threshold value

### Lossy compression threshold value

Note: For the Virtual Delivery Agent 7.x, this policy setting applies only when the Legacy graphics mode policy setting is enabled.

This setting represents the maximum bandwidth in kilobits per second for a connection to which lossy compression is applied.

By default, the threshold value is 2147483647 kilobits per second.

Adding the Lossy compression level setting to a policy and including no specified threshold can improve the display speed of high-detail bitmaps, such as photographs, over a LAN.

Related policy setting: Lossy compression level

# WebSocket 策略设置

May 28, 2016

The WebSockets section contains policy settings for accessing virtual desktops and hosted applications with Receiver for HTML5. The WebSockets feature increases security and reduces overhead by conducting two-way communication between browser-based applications and servers without opening multiple HTTP connections.

## WebSockets connections

This setting allows or prohibits WebSockets connections.

By default, WebSocket connections are prohibited.

## WebSockets port number

This setting identifies the port for incoming WebSocket connections.

By default, the value is 8008.

## WebSockets trusted origin server list

This setting provides a comma-separated list of trusted origin servers, usually Receiver for Web, expressed as URLs. Only WebSockets connections originating from one of these addresses is accepted by the server.

By default, the wildcard \* is used to trust all Receiver for Web URLs.

If you choose to type an address in the list, use this syntax:

<protocol>://<Fully qualified domain name of host>:[port]

The protocol should be HTTP or HTTPS. If the port is not specified, port 80 is used for HTTP and port 443 is used for HTTPS.

The wildcard \* can be used within the URL, except as part of an IP address (10.105.\*.\*).

# 负载管理策略设置

May 28, 2016

The Load Management section contains policy settings for enabling and configuring load management between servers delivering Windows Server OS machines.

## Concurrent logon tolerance

This setting specifies the maximum number of concurrent logons a server can accept.

By default, this is set to 2.

## CPU usage

This setting specifies the level of CPU usage, as a percentage, at which the server reports a full load. When enabled, the default value at which the server reports a full load is 90%.

By default, this setting is disabled and CPU usage is excluded from load calculations.

## CPU usage excluded process priority

This setting specifies the priority level at which a process' CPU usage is excluded from the CPU Usage load index.

By default, this is set to Below Normal or Low.

## Disk usage

This setting specifies the disk queue length at which the server reports a 75% full load. When enabled, the default value for disk queue length is 8.

By default, this setting is disabled and disk usage is excluded from load calculations.

## Maximum number of sessions

This setting specifies the maximum number of sessions a server can host. When enabled, the default setting for maximum number of sessions a server can host is 250.

By default, this setting is enabled.

## Memory usage

This setting specifies the level of memory usage, as a percentage, at which the server reports a full load. When enabled, the default value at which the server reports a full load is 90%.

By default, this setting is disabled and memory usage is excluded from load calculations.

## Memory usage base load

This setting specifies an approximation of the base operating system's memory usage and defines, in MB, the memory usage below which a server is considered to have zero load.

By default, this is set to 768 MB.

# Profile Management 策略设置

May 28, 2016

The Profile Management section contains policy settings for enabling profile management and specifying which groups to include in and exclude from profile management processing.

Other information (such as the names of the equivalent .ini file settings and which version of profile management is required for a policy setting) is available in [Profile Management Policies](#).

# 高级策略设置

May 28, 2016

The Advanced settings section contains policy settings relating to the advanced configuration of Profile management.

## Disable automatic configuration

This setting enables profile management to examine your environment, for example, to check for the presence of Personal vDisks and configure Group Policy accordingly. Only Profile management policies in the Not Configured state are adjusted, so any customizations made previously are preserved. This feature speeds up deployment and simplifies optimization. No configuration of the feature is necessary, but you can disable automatic configuration when upgrading (to retain settings from earlier versions) or when troubleshooting. Automatic configuration does not work in XenApp or other environments.

By default, automatic configuration is allowed.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, automatic configuration is turned on so Profile management settings might change if your environment changes.

## Log off user if a problem is encountered

This setting enables Profile management to log a user off if a problem is encountered; for example, if the user store is unavailable. When enabled, an error message is displayed to the user before they are logged off. When disabled, users are given a temporary profile.

By default, this setting is disabled and users are given a temporary profile if a problem is encountered.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, a temporary profile is provided.

## Number of retries when accessing locked files

This setting specifies the number of attempts Profile management makes to access locked files.

By default, this is set to five retries.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, the default value is used.

## Process Internet cookie files on logoff

This setting enables Profile management to process index.dat on logoff to remove Internet cookies left in the file system after sustained browsing that can lead to profile bloat. Enabling this setting increases logoff times, so only enable it if you experience this issue.

By default, this setting is disabled and Profile management does not process index.dat on logoff.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, no processing of Index.dat takes place.



# 基本策略设置

May 28, 2016

The Basic settings section contains policy settings relating to the basic configuration of Profile management.

## Active write back

This setting enables modified files and folders (but not registry settings) to be synchronized to the user store during a session, before logoff.

By default, synchronization to the user store during a session is disabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, it is enabled.

## Enable Profile management

This setting enables Profile management to process logons and logoffs.

By default, this setting is disabled to facilitate deployment.

Important: Citrix recommends enabling Profile management only after carrying out all other setup tasks and testing how Citrix user profiles perform in your environment.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, Profile management does not process Windows user profiles in any way.

## Excluded groups

This setting specifies which computer local groups and domain groups (local, global, and universal) are excluded from Profile management processing.

When enabled, Profile management does not process members of the specified user groups.

By default, this setting is disabled and members of all user groups are processed.

Specify domain groups in the form <DOMAIN NAME>\<GROUP NAME>.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, members of all user groups are processed.

## Offline profile support

This setting enables offline profile support, allowing profiles to synchronize with the user store at the earliest opportunity after a network disconnection.

By default, support for offline profiles is disabled.

This setting is applicable to laptop or mobile users who roam. When a network disconnection occurs, profiles remain intact on the laptop or device even after restarting or hibernating. As mobile users work, their profiles are updated locally and are

synchronized with the user store when the network connection is re-established.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, support for offline profiles is disabled.

## Path to user store

This setting specifies the path to the directory (user store) in which user settings, such as registry settings and synchronized files, are saved.

By default, the Windows directory on the home drive is used.

If this setting is disabled, user settings are saved in the Windows subdirectory of the home directory.

The path can be:

- **A relative path.** This must be relative to the home directory, typically configured as the #homeDirectory# attribute for a user in Active Directory.
- **An absolute UNC path.** This typically specifies a server share or a DFS namespace.
- **Disabled or unconfigured.** In this case, a value of #homeDirectory#\Windows is assumed.

Use the following types of variables when configuring this policy setting:

- System environment variables enclosed in percent signs (for example, %ProfVer%). Note that system environment variables generally require additional setup.
- Attributes of the Active Directory user object enclosed in hashes (for example, #sAMAccountName#).
- Profile management variables. For more information, see the Profile management documentation.

You can also use the %username% and %userdomain% user environment variables and create custom attributes to fully define organizational variables such as location or users. Attributes are case-sensitive.

Examples:

- \\server\share\#sAMAccountName# stores the user settings to the UNC path \\server\share\JohnSmith (if #sAMAccountName# resolves to JohnSmith for the current user)
- \\server\profiles\$\%USERNAME%.%USERDOMAIN%\!CTX\_PROFILEVER!!CTX\_OSBITNESS! might expand to \\server\profiles\$\JohnSmith.DOMAINCONTROLLER1\v2x64

Important: Whichever attributes or variables you use, check that this setting expands to the folder one level higher than the folder containing NTUSER.DAT. For example, if this file is contained in

\\server\profiles\$\JohnSmith.Finance\v2x64\UPM\_Profile, set the path to the user store as

\\server\profiles\$\JohnSmith.Finance\v2x64, not the \UPM\_Profile subfolder.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, the Windows directory on the home drive is used.

## Process logons of local administrators

This setting specifies whether or not logons of members of the BUILTIN\Administrators group are processed. This allows domain users with local administrator rights, typically users with assigned virtual desktops, to bypass processing, log on, and troubleshoot a desktop experiencing problems with Profile management.

If this setting is disabled or not configured on server operating systems, Profile management assumes that logons by domain users, but not local administrators, must be processed. On desktop operating systems, local administrator logons

are processed.

By default this setting is disabled, and local administrator logons are not processed.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, local administrator logons are not processed.

### Processed groups

This setting specifies which computer local groups and domain groups (local, global, and universal) are included in Profile management processing.

When enabled, Profile management processes only members of the specified user groups.

By default, this setting is disabled and members of all user groups are processed.

Specify domain groups in the form <DOMAIN NAME>\<GROUP NAME>.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, members of all user groups are processed.

# 跨平台策略设置

May 28, 2016

The Cross-Platform section contains policy settings relating to configuring the Profile management cross-platform settings feature.

## Cross-platform settings user groups

This setting specifies the Windows user groups whose profiles are processed when the cross-platform settings feature is enabled.

By default, this setting is disabled and all user groups specified in the Processed Group policy setting are processed.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, all user groups are processed.

## Enable cross-platform settings

This setting enables or disables the cross-platforms settings feature, that allows you to migrate users' profiles and roam them when a user connects to the same application running on multiple operating systems.

By default the cross-platform settings feature is disabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, no cross-platform settings are applied.

## Path to cross-platform definitions

This setting specifies the network location, as a UNC path, of the definition files copied from the download package.

Note: Users must have read access, and administrators write access, to this location and it must be either a Server Message Block (SMB) or Common Internet File System (CIFS) file share.

By default, no path is specified.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, no cross-platform settings are applied.

## Path to cross-platform settings store

This setting specifies the path to the cross-settings store, the folder in which users' cross-platform settings are saved. This path can be either a UNC path or a path relative to the home directory.

Note: Users must have write access to the cross-settings store.

By default, this setting is disabled and the path Windows\PM\_CP is used.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, the default value is used.

## Source for creating cross-platform settings

This setting specifies a platform as the base platform if this setting is enabled for that platform's OU. Data from the base platform's profiles is migrated to the cross-platform settings store.

Each platform's own set of profiles are stored in a separate OU. This means you must decide which platform's profile data to use to seed the cross-platform settings store. This is referred to as the base platform.

When enabled, Profile management migrates the data from the single-platform profile to the store if the cross-platform settings store contains a definition file with no data, or if the cached data in a single-platform profile is newer than the definition's data in the store.

**Important:** If this setting is enabled in multiple OUs, or multiple user or machine objects, the platform that the first user logs on to becomes the base profile.

By default, this setting is disabled and Profile management does not migrate the data from the single-platform profile to the store.

# 文件系统策略设置

May 28, 2016

The File System section contains policy settings for configuring which files and directories in a users profile are synchronized between the system where the profile is installed and the user store.

# 排除策略设置

May 28, 2016

The Exclusions section contains policy settings for configuring which files and directories in a users profile are excluded from the synchronization process.

## Exclusion list - directories

This setting specifies a list of folders in the user profile that are ignored during synchronization.

Specify folder names as paths relative to the user profile (%USERPROFILE%).

By default, this setting is disabled and all folders in the user profile are synchronized.

Example: Desktop ignores the Desktop folder in the user profile

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, all folders in the user profile are synchronized.

## Exclusion list - files

This setting specifies a list of files in the user profile that are ignored during synchronization.

By default, this setting is disabled and all files in the user profile are synchronized.

Specify file names as paths relative to the user profile (%USERPROFILE%). Note that wildcards are allowed and are applied recursively.

Example: Desktop\Desktop.ini ignores the file Desktop.ini in the Desktop folder

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, all files in the user profile are synchronized.

# 同步策略设置

May 28, 2016

The Synchronization section contains policy settings for specifying which files and folders in a user's profile are synchronized between the system on which the profile is installed and the user store.

## Directories to synchronize

This setting specifies any files you want Profile management to include in the synchronization process that are located in excluded folders. By default, Profile management synchronizes everything in the user profile. It is not necessary to include subfolders of the user profile by adding them to this list. For more information, see [Include and exclude items](#).

Paths on this list must be relative to the user profile.

Example: Desktop\exclude\include ensures that the subfolder called include is synchronized even if the folder called Desktop\exclude is not.

By default, this setting is disabled and no folders are specified.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, only non-excluded folders in the user profile are synchronized.

## Files to synchronize

This setting specifies any files you want Profile management to include in the synchronization process that are located in excluded folders. By default, Profile management synchronizes everything in the user profile. It is not necessary to include files in the user profile by adding them to this list. For more information, see [Include and exclude items](#).

Paths on this list must be relative to the user profile. Relative paths are interpreted as being relative to the user profile. Wildcards can be used but are allowed only for file names. Wildcards cannot be nested and are applied recursively.

Examples:

- AppData\Local\Microsoft\Office\Access.qat specifies a file below a folder that is excluded in the default configuration
- AppData\Local\MyApp\\*.cfg specifies all files with the extension .cfg in the profile folder AppData\Local\MyApp and its subfolders

By default, this setting is disabled and no files are specified.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, only non-excluded files in the user profile are synchronized.

## Folders to mirror

This setting specifies which folders relative to a user's profile root folder to mirror. Configuring this policy setting can help solve issues involving any transactional folder (also known as a referential folder), that is a folder containing interdependent files, where one file references others.

Mirroring folders allows Profile management to process a transactional folder and its contents as a single entity, avoiding profile bloat. Be aware that, in these situations the "last write wins" so files in mirrored folders that have been modified in more than one session will be overwritten by the last update, resulting in loss of profile changes.

For example, you can mirror the Internet Explorer cookies folder so that Index.dat is synchronized with the cookies that it indexes.

If a user has two Internet Explorer sessions, each on a different server, and they visit different sites in each session, cookies from each site are added to the appropriate server. When the user logs off from the first session (or in the middle of a session, if the active write back feature is configured), the cookies from the second session should replace those from the first session. However, instead they are merged, and the references to the cookies in Index.dat become out of date. Further browsing in new sessions results in repeated merging and a bloated cookie folder.

Mirroring the cookie folder solves the issue by overwriting the cookies with those from the last session each time the user logs off so Index.dat stays up to date.

By default, this setting is disabled and no folders are mirrored.

If this setting is not configured here, the value from the .ini file is used.

If this policy is not configured here or in the .ini file, no folders are mirrored.

# 文件夹重定向策略设置

May 28, 2016

The Folder Redirection section contains policy settings that specify whether to redirect folders that commonly appear in profiles to a shared network location.

## Grant administrator access

This setting enables an administrator to access the contents of a user's redirected folders.

By default, this setting is disabled and users are granted exclusive access to the contents of their redirected folders.

## Include domain name

This setting enables the inclusion of the %userdomain% environment variable as part of the UNC path specified for redirected folders.

By default, this setting is disabled and the %userdomain% environment variable is not included as part of the UNC path specified for redirected folders.

# “AppData (漫游)”策略设置

May 28, 2016

The AppData(Roaming) section contains policy settings for specifying whether to redirect the contents the AppData(Roaming) folder to a shared network location.

## AppData(Roaming) path

This setting specifies the network location to which the contents of the AppData(Roaming) folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile management does not redirect the specified folder.

## Redirection settings for AppData(Roaming)

This setting specifies how to redirect the contents of the AppData(Roaming) folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile management does not redirect the specified folder.

# “联系人”策略设置

May 28, 2016

The Contacts section contains policy settings for specifying whether to redirect the contents of the Contacts folder to a shared network location.

## Contacts path

This setting specifies the network location to which the contents of the Contacts folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile management does not redirect the specified folder.

## Redirection settings for Contacts

This setting specifies how to redirect the contents of the Contacts folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile management does not redirect the specified folder.

# 桌面策略设置

May 28, 2016

The Desktop section contains policy settings for specifying whether to redirect the contents of the Desktop folder to a shared network location.

## Desktop path

This setting specifies the network location to which the contents of the Desktop folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile management does not redirect the specified folder.

## Redirection settings for Desktop

This setting specifies how to redirect the contents of the Desktop folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile management does not redirect the specified folder.

# “文档”策略设置

May 28, 2016

The Documents section contains policy settings for specifying whether to redirect the contents of the Documents folder to a shared network location.

## Documents path

This setting specifies the network location to which files in the Documents folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile management does not redirect the specified folder.

The Documents path setting must be enabled not only to redirect files to the Documents folder, but also to redirect files to the Music, Pictures, and Videos folders.

## Redirection settings for Documents

This setting specifies how to redirect the contents of the Documents folder.

By default, contents are redirected to a UNC path.

To control how to redirect the contents of the Documents folder, choose one of the following options:

- Redirect to the following UNC path. Redirects content to the UNC path specified in the Documents path policy setting.
- Redirect to the users home directory. Redirects content to the users home directory, typically configured as the #homeDirectory# attribute for a user in Active Directory.

If this setting is not configured here, Profile management does not redirect the specified folder.

# “下载”策略设置

May 28, 2016

The Downloads section contains policy settings that specify whether to redirect the contents the Downloads folder to a shared network location.

## Downloads path

This setting specifies the network location to which files in the Downloads folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile management does not redirect the specified folder.

## Redirection settings for Downloads

This setting specifies how to redirect the contents of the Downloads folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile management does not redirect the specified folder.

# “收藏夹”策略设置

May 28, 2016

The Favorites section contains policy settings that specify whether to redirect the contents of the Favorites folder to a shared network location.

## Favorites path

This setting specifies the network location to which the contents of the Favorites folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile management does not redirect the specified folder.

## Redirection settings for Favorites

This setting specifies how to redirect the contents of the Favorites folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile management does not redirect the specified folder.

# “链接”策略设置

May 28, 2016

The Links section contains policy settings that specify whether to redirect the contents of the Links folder to a shared network location.

## Links path

This setting specifies the network location to which the contents of the Links folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile management does not redirect the specified folder.

## Redirection settings for Links

This setting specifies how to redirect the contents of the Links folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile management does not redirect the specified folder.

# “音乐”策略设置

May 28, 2016

The Music section contains policy settings that specify whether to redirect the contents of the Music folder to a shared network location.

## Music path

This setting specifies the network location to which the contents of the Music folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile management does not redirect the specified folder.

## Redirection settings for Music

This setting specifies how to redirect the contents of the Music folder.

By default, contents are redirected to a UNC path.

To control how to redirect the contents of the Music folder, choose one of the following options:

- Redirect to the following UNC path. Redirects content to the UNC path specified in the Music path policy setting.
- Redirect relative to Documents folder. Redirects content to a folder relative to the Documents folder.

To redirect content to a folder relative to the Documents folder, the Documents path setting must be enabled.

If this setting is not configured here, Profile management does not redirect the specified folder.

# “图片”策略设置

May 28, 2016

The Pictures section contains policy settings that specify whether to redirect the contents of the Pictures folder to a shared network location.

## Pictures path

This setting specifies the network location to which the contents of the Pictures folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile management does not redirect the specified folder.

## Redirection settings for Pictures

This setting specifies how to redirect the contents of the Pictures folder.

By default, contents are redirected to a UNC path.

To control how to redirect the contents of the Pictures folder, choose one of the following options:

- Redirect to the following UNC path. Redirects content to the UNC path specified in the Pictures path policy setting.
- Redirect relative to Documents folder. Redirects content to a folder relative to the Documents folder.

To redirect content to a folder relative to the Documents folder, the Documents path setting must be enabled.

If this setting is not configured here, Profile management does not redirect the specified folder.

# “保存的游戏”策略设置

May 28, 2016

The Saved Games section contains policy settings that specify whether to redirect the contents of the Saved Games folder to a shared network location.

## Redirection settings for Saved Games

This setting specifies how to redirect the contents of the Saved Games folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile management does not redirect the specified folder.

### Saved Games path

This setting specifies the network location to which the contents of the Saved Games folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile management does not redirect the specified folder.

# “搜索”策略设置

May 28, 2016

The Searches section contains policy settings that specify whether to redirect the contents of the Searches folder to a shared network location.

## Redirection settings for Searches

This setting specifies how to redirect the contents of the Searches folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile management does not redirect the specified folder.

## Searches path

This setting specifies the network location to which the contents of the Searches folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile management does not redirect the specified folder.

# “开始菜单”策略设置

May 28, 2016

The Start Menu section contains policy settings that specify whether to redirect the contents the Start Menu folder to a shared network location.

## Redirection settings for Start Menu

This setting specifies how to redirect the contents of the Start Menu folder.

By default, contents are redirected to a UNC path.

If this setting is not configured here, Profile management does not redirect the specified folder.

## Start Menu path

This setting specifies the network location to which the contents of the Start Menu folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile management does not redirect the specified folder.

# “视频”策略设置

May 28, 2016

The Video section contains policy settings that specify whether to redirect the contents of the Video folder to a shared network location.

## Redirection settings for Video

This setting specifies how to redirect the contents of the Video folder.

By default, contents are redirected to a UNC path.

To control how to redirect the contents of the Video folder, choose one of the following options:

- Redirect to the following UNC path. Redirects content to the UNC path specified in the Video path policy setting.
- Redirect relative to Documents folder. Redirects content to a folder relative to the Documents folder.

To redirect content to a folder relative to the Documents folder, the Documents path setting must be enabled.

If this setting is not configured here, Profile management does not redirect the specified folder.

## Video path

This setting specifies the network location to which the contents of the Video folder are redirected.

By default, this setting is disabled and no location is specified.

If this setting is not configured here, Profile management does not redirect the specified folder.

# “日志”策略设置

May 28, 2016

The Log section contains policy settings that configure Profile management logging.

## Active Directory actions

This setting enables or disables verbose logging of actions performed in Active Directory.

By default, this setting is disabled.

When enabling this setting, make sure the Enable logging setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

## Common information

This setting enables or disables verbose logging of common information.

By default, this setting is disabled.

When enabling this setting, make sure the Enable logging setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

## Common warnings

This setting enables or disables verbose logging of common warnings.

By default, this setting is disabled.

When enabling this setting, make sure the Enable logging setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

## Enable logging

This setting enables or disables Profile management logging in debug (verbose logging) mode. In debug mode, extensive status information is logged in the log files located in "%SystemRoot%\System32\Logfiles\UserProfileManager".

By default, this setting is disabled and only errors are logged.

Citrix recommends enabling this setting only if you are troubleshooting Profile management.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, only errors are logged.

## File system actions

This setting enables or disables verbose logging of actions performed in the file system.

By default, this setting is disabled.

When enabling this setting, make sure the Enable logging setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

## File system notifications

This setting enables or disables verbose logging of file systems notifications.

By default, this setting is disabled.

When enabling this setting, make sure the Enable logging setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

## Logoff

This setting enables or disables verbose logging of user logoffs.

By default, this setting is disabled.

When enabling this setting, make sure the Enable logging setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

## Logon

This setting enables or disables verbose logging of user logons.

By default, this setting is disabled.

When enabling this setting, make sure the Enable logging setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

## Maximum size of the log file

This setting specifies the maximum permitted size for the Profile management log file, in bytes.

By default, this is set to 1048576 bytes (1MB).

Citrix recommends increasing the size of this file to 5 MB or more, if you have sufficient disk space. If the log file grows beyond the maximum size, an existing backup of the file (.bak) is deleted, the log file is renamed to .bak, and a new log file is

created.

The log file is created in %SystemRoot%\System32\Logfiles\UserProfileManager.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, the default value is used.

#### Path to log file

This setting specifies an alternative path to save the Profile management log file.

By default, this setting is disabled and log files are saved in the default location:

%SystemRoot%\System32\Logfiles\UserProfileManager.

The path can point to a local drive or a remote network-based drive (UNC path). Remote paths can be useful in large distributed environments but they may create significant network traffic, which may be inappropriate for log files. For provisioned, virtual machines with a persistent hard drive, set a local path to that drive. This ensures log files are preserved when the machine restarts. For virtual machines without a persistent hard drive, setting a UNC path allows you to retain the log files, but the system account for the machines must have write access to the UNC share. Use a local path for any laptops managed by the offline profiles feature.

If a UNC path is used for log files, Citrix recommends that an appropriate access control list is applied to the log file folder to ensure that only authorized user or computer accounts can access the stored files.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, the default location %SystemRoot%\System32\Logfiles\UserProfileManager is used.

#### Personalized user information

This setting enables or disables verbose logging of personalized user information.

By default, this setting is disabled.

When enabling this setting, make sure the Enable logging setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

#### Policy values at logon and logoff

This setting enables or disables verbose logging of policy values when a user logs on and off.

By default, this setting is disabled.

When enabling this setting, make sure the Enable logging setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

#### Registry actions

This setting enables or disables verbose logging of actions performed in the registry.

By default, this setting is disabled.

When enabling this setting, make sure the Enable logging setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

### Registry differences at logoff

This setting enables or disables verbose logging of any differences in the registry when a user logs off.

By default, this setting is disabled.

When enabling this setting, make sure the Enable logging setting is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, errors and general information are logged.

# “配置文件处理”策略设置

May 28, 2016

The Profile handling section contains policy settings that specify how Profile management handles user profiles.

## Delay before deleting cached profiles

This setting specifies an optional extension to the delay, in minutes, before Profile management deletes locally cached profiles at logoff.

A value of 0 deletes the profiles immediately at the end of the logoff process. Profile management checks for logoffs every minute, so a value of 60 ensures that profiles are deleted between one and two minutes after users log off (depending on when the last check occurred). Extending the delay is useful if you know that a process keeps files or the user registry hive open during logoff. With large profiles, this can also speed up logoff.

By default, this is set to 0 and Profile management deletes locally cached profiles immediately.

When enabling this setting, ensure the Delete locally cached profiles on logoff is also enabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, profiles are deleted immediately.

## Delete locally cached profiles on logoff

This setting specifies whether locally cached profiles are deleted after a user logs off.

When this setting is enabled, a user's local profile cache is deleted after they have logged off. Citrix recommends enabling this setting for terminal servers.

By default, this setting is disabled and a user's local profile cache is retained after they log off.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, cached profiles are not deleted.

## Local profile conflict handling

This setting configures how Profile management behaves if a user profile exists both in the user store and as a local Windows user profile (not a Citrix user profile).

By default, Profile management uses the local Windows profile, but does not change it in any way.

To control how Profile management behaves, choose one of the following options:

- Use local profile. Profile management uses the local profile, but does not change it in any way.
- Delete local profile. Profile management deletes the local Windows user profile, and then imports the Citrix user profile from the user store.
- Rename local profile. Profile management renames the local Windows user profile (for backup purposes) and then imports the Citrix user profile from the user store.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, existing local profiles are used.

## Migration of existing profiles

This setting specifies the types of profile migrated to the user store during logon if a user has no current profile in the user store.

Profile management can migrate existing profiles "on the fly" during logon if a user has no profile in the user store. After this, the user store profile is used by Profile management in both the current session and any other session configured with the path to the same user store.

By default, both local and roaming profiles are migrated to the user store during logon.

To specifies the types of profile migrated to the user store during logon, choose one of the following options:

- Local and roaming profiles
- Local
- Roaming
- None (Disabled)

If you select None, the system uses the existing Windows mechanism to create new profiles, as if in a environment where Profile management is not installed.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, existing local and roaming profiles are migrated.

## Path to the template profile

This setting specifies the path to the profile you want Profile management to use as a template to create new user profiles.

The specified path must be the full path to the folder containing the NTUSER.DAT registry file and any other folders and files required for the template profile.

Note: Do not include NTUSER.DAT in the path. For example, with the file \\myservername\myprofiles\template\ntuser.dat, set the location as \\myservername\myprofiles\template.

Use absolute paths, which can be either UNC paths or paths on the local machine. Use the latter, for example, to specify a template profile permanently on a Citrix Provisioning Services image. Relative paths are not supported.

Note: This setting does not support expansion of Active Directory attributes, system environment variables, or the %USERNAME% and %USERDOMAIN% variables.

By default, this setting is disabled and new user profiles are created from the default user profile on the device where a user first logs on.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, no template is used.

## Template profile overrides local profile

This setting enables the template profile to override the local profile when creating new user profiles.

If a user has no Citrix user profile, but a local Windows user profile exists, by default the local profile is used (and migrated to the user store, if this is not disabled). Enabling this policy setting allows the template profile to override the local profile used

when creating new user profiles.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, no template is used.

#### Template profile overrides roaming profile

This setting enables the template profile to override a roaming profile when creating new user profiles.

If a user has no Citrix user profile, but a roaming Windows user profile exists, by default the roaming profile is used (and migrated to the user store, if this is not disabled). Enabling this policy setting allows the template profile to override the roaming profile used when creating new user profiles.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, no template is used.

#### Template profile used as a Citrix mandatory profile for all logons

This setting enables Profile management to use the template profile as the default profile for creating all new user profiles.

By default, this setting is disabled and new user profiles are created from the default user profile on the device where a user first logs on.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, no template is used.

# “注册表”策略设置

May 28, 2016

The Registry section contains policy settings that specify which registry keys are included or excluded from Profile management processing.

## Exclusion list

This setting specifies the list of registry keys in the HKCU hive excluded from Profile management processing when a user logs off.

When enabled, keys specified in this list are excluded from processing when a user logs off.

By default, this setting is disabled, and all registry keys in the HKCU hive are processed when a user logs off.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, no registry keys are excluded from processing.

## Inclusion list

This setting specifies the list of registry keys in the HKCU hive included in Profile management processing when a user logs off.

When enabled, only keys specified in this list are processed when a user logs off.

By default, this setting is disabled, and all registry keys in the HKCU hive are processed when a user logs off.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, all of HKCU is processed .

# “流用户配置文件”策略设置

May 28, 2016

The Streamed user profiles section contains policy settings that specify how Profile management processes streamed user profiles.

## Always cache

This setting specifies whether or not Profile management caches streamed files as soon as possible after a user logs on. Caching files after a user logs on saves network bandwidth, enhancing the user experience.

Use this setting with the Profile streaming setting.

By default, this setting is disabled and streamed files are not cached as soon as possible after a user logs on.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, it is disabled.

## Always cache size

This setting specifies a lower limit, in megabytes, on the size of files that are streamed. Profile management caches any files this size or larger as soon as possible after a user logs on.

By default, this is set to 0 (zero) and the cache entire profile feature is used. When the cache entire profile feature is enabled, Profile management fetches all profile contents in the user store, after a user logs on, as a background task.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, it is disabled.

## Profile streaming

This setting enables and disables the Citrix streamed user profiles feature. When enabled, files and folders contained in a profile are fetched from the user store to the local computer only when they are accessed by users after they have logged on. Registry entries and files in the pending area are fetched immediately.

By default, profile streaming is disabled.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, it is disabled.

## Streamed user profile groups

This setting specifies which user profiles within an OU are streamed, based on Windows user groups.

When enabled, only user profiles within the specified user groups are streamed. All other user profiles are processed normally.

By default, this setting is disabled and all user profiles within an OU are processed normally.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, all user profiles are processed.

#### Timeout for pending area lock files

This setting specifies the number of days after which users' files are written back to the user store from the pending area, in the event that the user store remains locked when a server becomes unresponsive. This prevents bloat in the pending area and ensures the user store always contains the most up-to-date files.

By default, this is set to 1 (one) day.

If this setting is not configured here, the value from the .ini file is used.

If this setting is not configured here or in the .ini file, the default value is used.

# Receiver 策略设置

May 28, 2016

The Receiver section contains policy settings that specify a list of StoreFront addresses to push to Receiver for Windows running on the virtual desktop.

## StoreFront accounts list

This setting specifies a list of StoreFront stores administrators can choose to push to Receiver for Windows running on the virtual desktop. When creating a Delivery Group, administrators can select which stores to push to Receiver for Windows running on virtual desktops within that group.

By default, no stores are specified.

For each store, specify the following information as a semicolon-delimited entry:

- Store name. The name displayed to users of the store.
- Store URL. The URL for the store.
- Store enabled state. Whether or not the store is available to users. This is either On or Off.
- Store description. The description displayed to users of the store.

For example: Sales Store;https://sales.mycompany.com/Citrix/Store/discovery;On;Store for Sales staff

# Virtual Delivery Agent 策略设置

May 28, 2016

The Virtual Delivery Agent (VDA) section contains policy settings that control communication between the VDA and controllers for a site.

Important: The VDA requires information provided by these settings to register with a Delivery Controller, if you are not using the auto-update feature. Because this information is required for registration, you must configure the following settings using the Group Policy Editor, unless you provide this information during the VDA installation:

- Controller registration IPv6 netmask
- Controller registration port
- Controller SIDs
- Controllers
- Only use IPv6 controller registration
- Site GUID

## Controller registration IPv6 netmask

This policy setting allows administrators to restrict the VDA to only a preferred subnet (rather than a global IP, if one is registered). This setting specifies the IPv6 address and network where the VDA will register. The VDA will register only on the first address that matches the specified netmask. This setting is valid only if the Only use IPv6 controller registration policy setting is enabled.

By default this setting is blank.

## Controller registration port

Use this setting only if the Enable auto update of controllers setting is disabled.

This setting specifies the TCP/IP port number the VDA uses to register with a Controller when using registry-based registration.

By default, the port number is set to 80.

## Controller SIDs

Use this setting only if the Enable auto update of controllers setting is disabled.

This setting specifies a space-separated list of controller Security Identifiers (SIDs) the VDA uses to register with a Controller when using registry-based registration. This is an optional setting which may be used with the Controllers setting to restrict the list of Controllers used for registration.

By default, this setting is blank.

## Controllers

Use this setting only if the Enable auto update of controllers setting is disabled.

This setting specifies a space-separated list of controller Fully Qualified Domain Names (FQDNs) the VDA uses to register with a Controller when using registry-based registration. This is an optional setting that may be used with the Controller SIDs setting.

By default, this setting is blank.

#### Enable auto update of controllers

This setting enables the VDA to register with a Controller automatically after installation.

After the VDA registers, the Controller with which it registered sends a list of the current controller FQDNs and SIDs to the VDA. The VDA writes this list to persistent storage. Each Controller also checks the Site database every 90 minutes for Controller information; if a Controller has been added or removed since the last check, or if a policy change has occurred, the Controller sends updated lists to its registered VDAs. The VDA will accept connections from all the Controllers in the most recent list it received.

By default, this setting is enabled.

#### Only use IPv6 controller registration

This setting controls which form of address the VDA uses to register with the Controller:

- When enabled, the VDA registers with the Controller using the machine's IPv6 address. When the VDA communicates with the Controller, it uses the following address order: global IP address, Unique Local Address (ULA), link-local address (if no other IPv6 addresses are available).
- When disabled, the VDA registers and communicates with the Controller using the machine's IPv4 address.

By default, this setting is disabled.

#### Site GUID

Use this setting only if the Enable auto update of controllers setting is disabled.

This setting specifies the Globally Unique Identifier (GUID) of the site the VDA uses to register with a Controller when using Active Directory-based registration.

By default, this setting is blank.

# HDX 3D Pro 策略设置

May 28, 2016

The HDX 3D Pro section contains policy settings for enabling and configuring the image quality configuration tool for users. The tool enables users to optimize use of available bandwidth by adjusting in real time the balance between image quality and responsiveness.

## Enable lossless

This setting specifies whether or not users can enable and disable lossless compression using the image quality configuration tool. By default, users are not given the option to enable lossless compression.

When a user enables lossless compression, the image quality is automatically set to the maximum value available in the image configuration tool. By default, either GPU or CPU-based compression can be used, according to the capabilities of the user device and the host computer.

## HDX 3D Pro quality settings

This setting specifies the minimum and maximum values that define the range of image quality adjustment available to users in the image quality configuration tool.

Specify image quality values of between 0 and 100, inclusive. The maximum value must be greater than or equal to the minimum value.

# 虚拟 IP 策略设置

May 28, 2016

The Virtual IP section contains policy settings that control whether sessions have their own virtual loopback address.

## Virtual IP loopback support

When this setting is enabled, each session has its own virtual loopback address. When disabled, sessions do not have individual loopback addresses.

By default, this setting is disabled.

## Virtual IP virtual loopback programs list

This setting specifies the application executables that can use virtual loopback addresses. When adding programs to the list, specify only the executable name; you do not need to specify the entire path.

By default, no executables are specified.

# 使用注册表配置 COM 端口和 LPT 端口重定向设置

May 28, 2016

Policy settings for COM Port and LPT Port Redirection are located under  
HKLM\Software\Citrix\GroupPolicy\Defaults\Deprecated on the VDA image or machine.

To enable COM port and LPT port redirection, add new registry keys of type REG\_DWORD, as follows:

Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Registry key	Description	Permitted values
AllowComPortRedirection	Allow or prohibit COM port redirection	1 (Allow) or 0 (Prohibit)
LimitComBw	Bandwidth limit for COM port redirection channel	Numeric value
LimitComBWPercent	Bandwidth limit for COM port redirection channel as a percentage of total session bandwidth	Numeric value between 0 and 100
AutoConnectClientComPorts	Automatically connect COM ports from the user device	1 (Allow) or 0 (Prohibit)
AllowLptPortRedirection	Allow or prohibit LPT port redirection	1 (Allow) or 0 (Prohibit)
LimitLptBw	Bandwidth limit for LPT port redirection channel	Numeric value
LimitLptBwPercent	Bandwidth limit for LPT port redirection channel as a percentage of total session bandwidth	Numeric value between 0 and 100
AutoConnectClientLptPorts	Automatically connect LPT ports from the user device	1 (Allow) or 0 (Prohibit)

After configuring these settings, modify your machine catalogs to use the new master image or updated physical machine. Desktops are updated with the new settings the next time users log off.

# Connector for Configuration Manager 2012 策略设置

May 28, 2016

The Connector for Configuration Manager 2012 section contains policy settings for configuring the Citrix Connector 7.5 agent.

Important: Warning, logoff, and reboot message policies apply only to deployments to Server OS machine catalogs that are managed manually or by Provisioning Services. For those machine catalogs, the Connector service alerts users when there are pending application installs or software updates.

For catalogs managed by MCS, use Studio to notify users. For manually managed Desktop OS catalogs, use Configuration Manager to notify users. For Desktop OS catalogs managed by Provisioning Services, use Provisioning Services to notify users.

## Advance warning frequency interval

This setting defines the interval between appearances of the advance warning message to users.

Intervals are set using the format ddd.hh:mm:ss, where:

- ddd is days, an optional parameter, with a range of 0 to 999.
- hh is hours with a range of 0 to 23.
- mm is minutes with a range of 0 to 59.
- ss is seconds with a range of 0 to 59.

By default, the interval setting is 1 hour (01:00:00).

## Advance warning message box body text

This setting contains the editable text of the message to users notifying them of upcoming software updates or maintenance that requires them to log off.

By default, the message is: {TIMESTAMP} Please save your work. The server will go offline for maintenance in {TIMELEFT}

## Advance warning message box title

This setting contains the editable text of the title bar of the advance warning message to users.

By default, the title is: Upcoming Maintenance

## Advance warning time period

This setting defines how far before maintenance the advance warning message first appears.

The time is set using the format ddd.hh:mm:ss, where:

- ddd is days, an optional parameter, with a range of 0 to 999.
- hh is hours with a range of 0 to 23.
- mm is minutes with a range of 0 to 59.
- ss is seconds with a range of 0 to 59.

By default, the setting is 16 hours (16:00:00), indicating that the first advance warning message appears approximately 16 hours before maintenance.

## Final force logoff message box body text

This setting contains the editable text of the message alerting users that a forced logoff has begun.

By default, the message is: The server is currently going offline for maintenance

## Final force logoff message box title

This setting contains the editable text of the title bar of the final force logoff message.

By default, the title is: Notification From IT Staff

## Force logoff grace period

This setting defines the period of time between notifying users to log off and the implementation of the forced logoff to process the pending maintenance.

The time is set using the format ddd.hh:mm:ss, where:

- ddd is days, an optional parameter, with a range of 0 to 999.
- hh is hours with a range of 0 to 23.
- mm is minutes with a range of 0 to 59.
- ss is seconds with a range of 0 to 59.

By default, the force logoff grace period setting is 5 minutes (00:05:00).

## Force logoff message box body text

This setting contains the editable text of the message telling users to save their work and log off prior to the start of a forced logoff.

By default, the message contains the following: {TIMESTAMP} Please save your work and log off. The server will go offline for maintenance in {TIMELEFT}

## Force logoff message box title

This setting contains the editable text of the title bar of the force logoff message.

By default, the title is: Notification From IT Staff

## Image-managed mode

The Connector agent automatically detects if it is running on a machine clone managed by Provisioning Services or MCS. The agent blocks Configuration Manager updates on image-managed clones and automatically installs the updates on the master image of the catalog.

After a master image is updated, use Studio to orchestrate the reboot of MCS catalog clones. The Connector Agent automatically orchestrates the reboot of PVS catalog clones during Configuration Manager maintenance windows. To override this behavior so that software is installed on catalog clones by Configuration Manager, change Image-managed mode to Disabled.

## Reboot message box body text

This setting contains the editable text of the message notifying users when the server is about to be restarted.

By default, the message is: The server is currently going offline for maintenance

Regular time interval at which the agent task is to run

This setting determines how frequently the Citrix Connector agent task runs.

The time is set using the format ddd.hh:mm:ss, where:

- ddd is days, an optional parameter, with a range of 0 to 999.
- hh is hours with a range of 0 to 23.
- mm is minutes with a range of 0 to 59.
- ss is seconds with a range of 0 to 59.

By default, the regular time interval setting is 5 minutes (00:05:00).

# 打印

May 28, 2016

Managing printers in your environment is a multistage process:

1. Become familiar with printing concepts, if you are not already.
2. Plan your printing architecture. This includes analyzing your business needs, your existing printing infrastructure, how your users and applications interact with printing today, and which printing management model best applies to your environment.
3. Configure your printing environment by selecting a printer provisioning method and then creating policies to deploy your printing design. Update policies when new employees or servers are added.
4. Test a pilot printing configuration before deploying it to users.
5. Maintain your Citrix printing environment by managing printer drivers and optimizing printing performance.
6. Troubleshoot issues that may arise.

## Printing concepts

Before you begin planning your deployment, make sure that you understand these core concepts for printing:

- The types of printer provisioning available
- How print jobs are routed
- The basics of printer driver management

Printing concepts build on Windows printing concepts. To configure and successfully manage printing in your environment, you must understand how Windows network and client printing works and how this translates into printing behavior in this environment.

## Print process

In this environment, all printing is initiated (by the user) on machines hosting applications. Print jobs are redirected through the network print server or user device to the printing device.

There is no persistent workspace for users of virtual desktops and applications. When a session ends the user's workspace is deleted, thus all settings need to be rebuilt at the beginning of each session. As a result, each time a user starts a new session, the system must rebuild the user's workspace.

When a user prints:

- Determines what printers to provide to the user. This is known as printer provisioning.
- Restores the user's printing preferences.
- Determines which printer is the default for the session.

You can customize how to perform these tasks by configuring options for printer provisioning, print job routing, printer property retention, and driver management. Be sure to evaluate how the various option settings might change the performance of printing in your environment and the user experience.

## Printer provisioning

The process that makes printers available in a session is known as provisioning. Printer provisioning is typically handled dynamically. That is, the printers that appear in a session are not predetermined and stored. Instead, the printers are assembled, based on policies, as the session is built during log on and reconnection. As a result, the printers can change

according to policy, user location, and network changes, provided they are reflected in policies. Thus, users who roam to a different location might see changes to their workspace.

The system also monitors client-side printers and dynamically adjusts in-session auto-created printers based on additions, deletions, and changes to the client-side printers. This dynamic printer discovery benefits mobile users as they connect from various devices.

The most common methods of printer provisioning are:

- **Universal Print Server** - The Citrix [Universal Print Server](#) provides universal printing support for network printers. The Universal Print Server uses the Universal print driver. This solution enables you to use a single driver on a Server OS machine to allow network printing from any device.

Citrix recommends the Citrix Universal Print Server for remote print server scenarios. The Universal Print Server transfers the print job over the network in an optimized and compressed format, thus minimizing network use and improving the user experience.

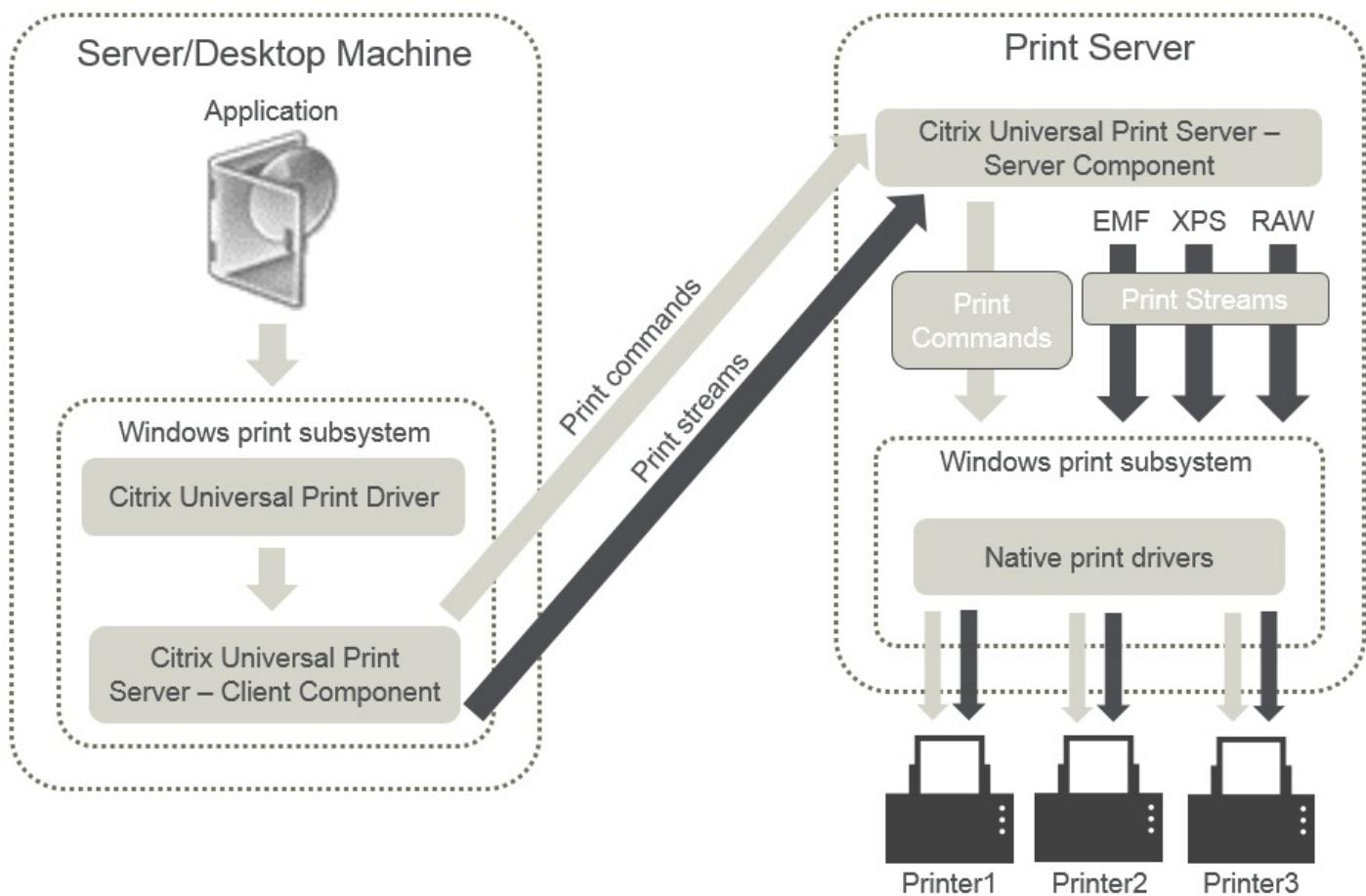
The Universal Print Server feature comprises:

- A client component, UPClient - Enable the UPClient on each Server OS machine that provisions session network printers and uses the Universal print driver.
- A server component, UPServer - Install UPServer on each print server that provisions session network printers and uses the Universal print driver for the session printers (whether or not the session printers are centrally provisioned).

For Universal Print Server requirements and setup details, refer to the system requirements and installation documents.

Note: The Universal Print Server is also supported for VDI-in-a-Box 5.3. For information about installing Universal Print Server with VDI-in-a-Box, refer to the VDI-in-a-Box documentation.

The following illustration shows the typical workflow for a network based printer in an environment that uses Universal Print Server.



When you enable the Citrix Universal Print Server, all connected network printers leverage it automatically through auto-discovery.

- **Autocreation** - *Autocreation* refers to printers automatically created at the beginning of each session. Both remote network printers and locally attached client printers can be auto-created. Consider auto-creating only the default client printer for environments with a large number of printers per user. Auto-creating a smaller number of printers uses less overhead (memory and CPU) on Server OS machines. Minimizing auto-created printers can also reduce user logon times. Auto-created printers are based on:

- The printers installed on the user device.
- Any policies that apply to the session.

Autocreation policy settings enable you to limit the number or type of printers that are auto-created. By default, the printers are available in sessions when configuring all printers on the user device automatically, including locally attached and network printers.

After the user ends the session, the printers for that session are deleted.

Client and network printer autocreation has associated maintenance. For example, adding a printer requires that you:

- Update the Session printers policy setting.
- Add the driver to all Server OS machines using the Printer driver mapping and compatibility policy setting.

## Print job routing

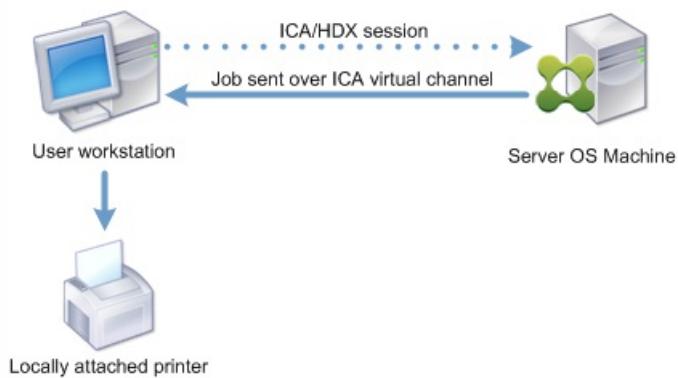
The term printing pathway encompasses both the path by which print jobs are routed and the location where print jobs are

spooled. Both aspects of this concept are important. Routing affects network traffic. Spooling affects utilization of local resources on the device that processes the job.

In this environment, print jobs can take two paths to a printing device: through the client or through a network print server. Those paths are referred to as the client printing pathway and the network printing pathway. Which path is chosen by default depends on the kind of printer used.

### Locally attached printers

The system routes jobs to locally attached printers from the Server OS machine, through the client, and then to the print device. The ICA protocol optimizes and compresses the print job traffic. When a printing device is attached locally to the user device, print jobs are routed over the ICA virtual channel.



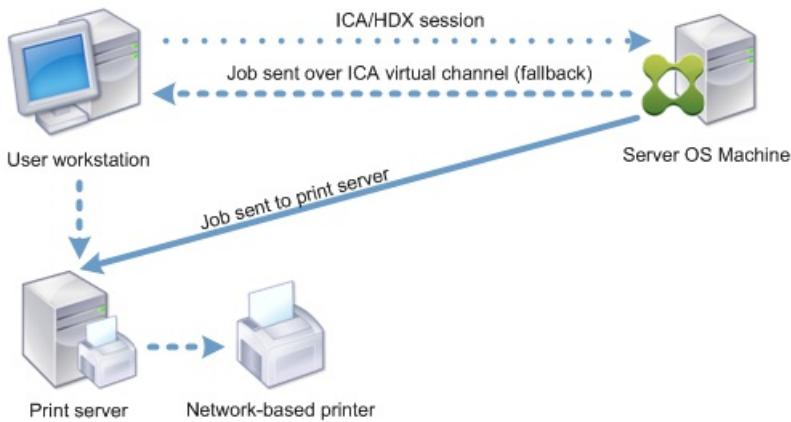
### Network-based printers

By default, all print jobs destined for network printers route from the Server OS machine, across the network, and directly to the print server. However, print jobs are automatically routed over the ICA connection in the following situations:

- If the virtual desktop or application cannot contact the print server.
- If the native printer driver is not available on the Server OS machine.

If the Universal Print Server is not enabled, configuring the client printing pathway for network printing is useful for low bandwidth connections, such as wide area networks, that can benefit from the optimization and traffic compression that results from sending jobs over the ICA connection.

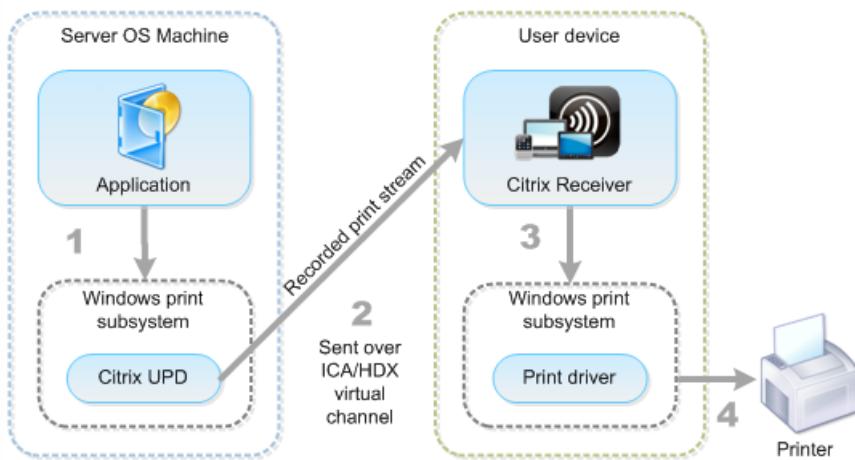
The client printing pathway also lets you limit traffic or restrict bandwidth allocated for print jobs. If routing jobs through the user device is not possible, such as for thin clients without printing capabilities, Quality of Service should be configured to prioritize ICA/HDX traffic and ensure a good in-session user experience.



## Print driver management

To simplify printing in this environment, Citrix recommends using Citrix Universal print driver. The Universal print driver is a device-independent driver that supports any print device and thus simplifies administration by reducing the number of drivers required.

The following illustration shows the Universal print driver components and a typical workflow for a printer locally attached to a device.

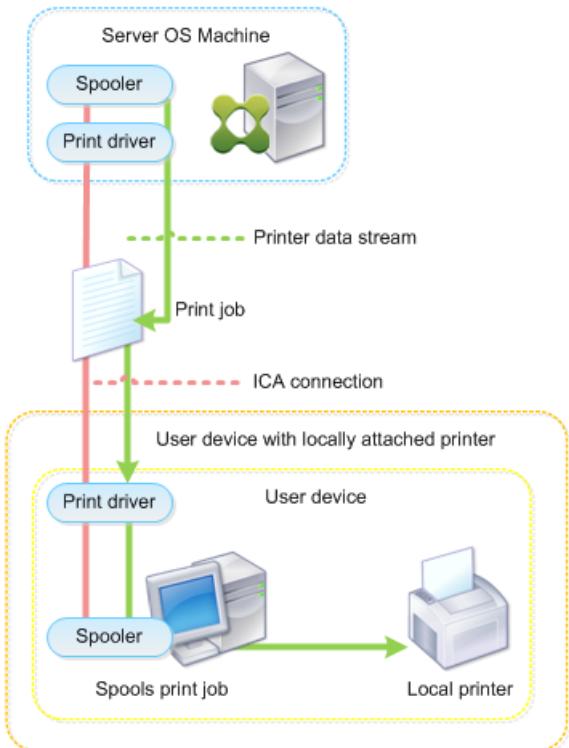


When planning your driver management strategy, determine if you will support the Universal print driver, device-specific drivers, or both. If you support standard drivers, you need to determine:

- The types of drivers to support.
- Whether to install printer drivers automatically when they are missing from Server OS machines.
- Whether to create driver compatibility lists.

During printer autocreation, if the system detects a new local printer connected to a user device, it checks the Server OS machine for the required printer driver. By default, if a Windows-native driver is not available, the system uses the Universal print driver.

The printer driver on the Server OS machine and the driver on the user device must match for printing to succeed. The illustration that follows shows how a printer driver is used in two places for client printing.



## Related content

- Printing configuration example
- Best practices, security considerations, and default operations
- Print policies and preferences
- Provision printers
- Maintain the printing environment
- Universal Print Server Requirements

# 打印配置示例

May 28, 2016

Choosing the most appropriate printing configuration options for your needs and environment can simplify administration. Although the default print configuration enables users to print in most environments, the defaults might not provide the expected user experience or the optimum network usage and management overhead for your environment.

Your printing configuration depends upon:

- Your business needs and your existing printing infrastructure.

Design your printing configuration around the needs of your organization. Your existing printing implementation (whether users can add printers, which users have access to what printers, and so on) might be a useful guide when defining your printing configuration.

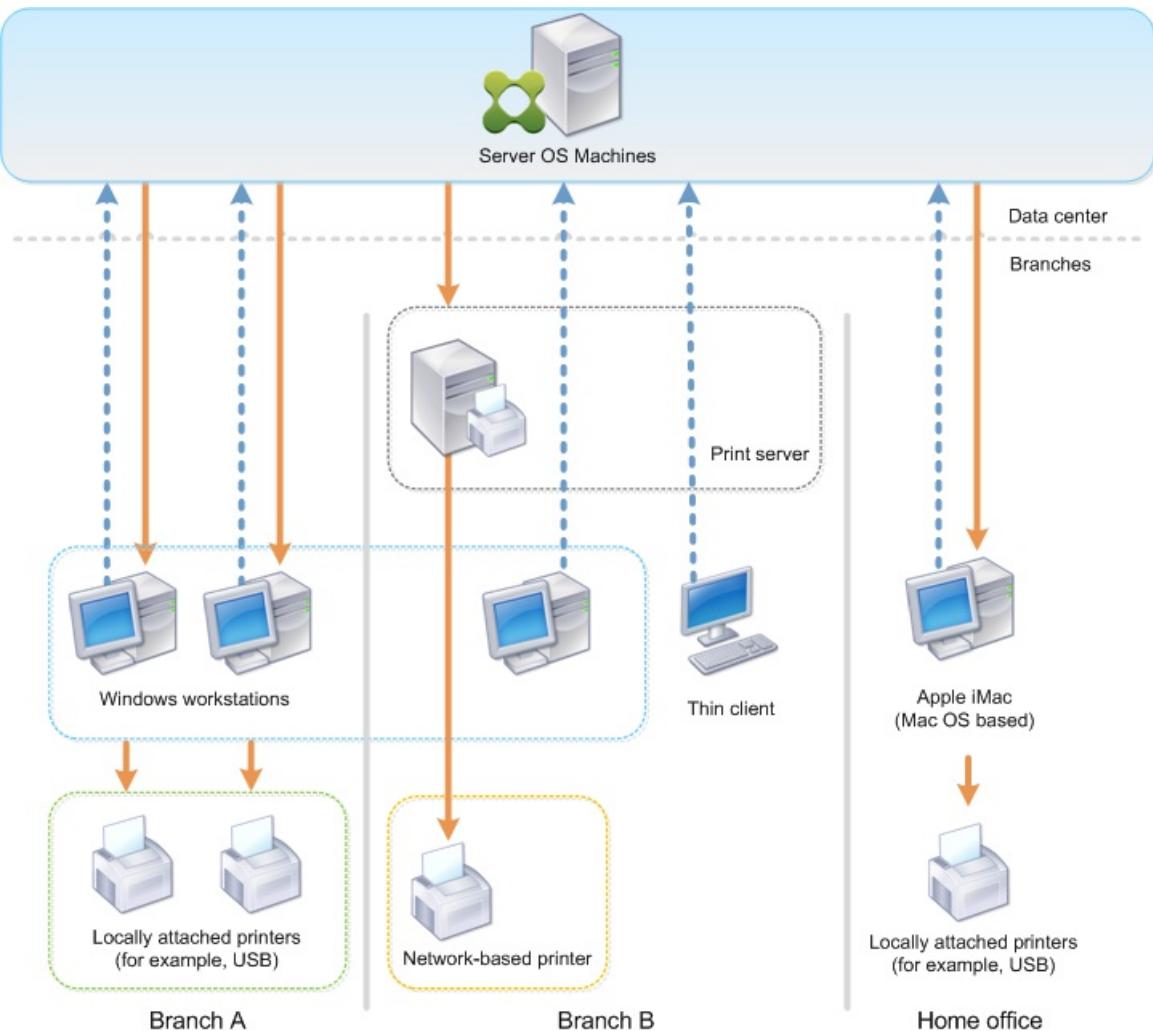
- Whether your organization has security policies that reserve printers for certain users (for example, printers for Human Resources or payroll).
- Whether users need to print while away from their primary work location, such as workers who move between workstations or travel on business.

When designing your printing configuration, try to give users the same experience in a session as they have when printing from local user devices.

## Example print deployment

The following illustration shows the print deployment for these use cases:

- **Branch A** – A small overseas branch office with a few Windows workstations. Every user workstation has a locally attached, private printer.
- **Branch B** – A large branch office with thin clients and Windows-based workstations. For increased efficiency, the users of this branch share network-based printers (one per floor). Windows-based print servers located within the branch manage the print queues.
- **Home office** – A home office with a Mac OS-based user device that accesses the company's Citrix infrastructure. The user device has a locally attached printer.



The following sections describe the configurations which minimize the complexity of the environment and simplify its management.

#### Auto-created client printers and Citrix Universal printer driver

In Branch A, all users work on Windows-based workstations, therefore auto-created client printers and the Universal printer driver are used. Those technologies provide these benefits:

- Performance – Print jobs are delivered over the ICA printing channel, thus the print data can be compressed to save bandwidth.

To ensure that a single user printing a large document cannot degrade the session performance of other users, a Citrix policy is configured to specify the maximum printing bandwidth.

An alternative solution is to leverage a multi-stream ICA connection, in which the print traffic is transferred within a separate low priority TCP connection. Multi-stream ICA is an option when Quality of Service (QoS) is not implemented on the WAN connection.

- Flexibility – Use of the Citrix Universal printer driver ensures that all printers connected to a client can also be used from a virtual desktop or application session without integrating a new printer driver in the data center.

#### Citrix Universal Print Server

In Branch B, all printers are network-based and their queues are managed on a Windows print server, thus the Citrix Universal Print Server is the most efficient configuration.

All required printer drivers are installed and managed on the print server by local administrators. Mapping the printers into the virtual desktop or application session works as follows:

- For Windows-based workstations – The local IT team helps users connect the appropriate network-based printer to their Windows workstations. This enables users to print from locally-installed applications.
- During a virtual desktop or application session, the printers configured locally are enumerated through autocreation. The virtual desktop or application then connects to the print server as a direct network connection if possible.

The Citrix Universal Print Server components are installed and enabled, thus native printer drivers are not required. If a driver is updated or a printer queue is modified, no additional configuration is required in the data center.

- For thin clients – For thin client users, printers must be connected within the virtual desktop or application session. To provide users with the simplest printing experience, administrators configure a single Citrix Session Printer policy per floor to connect a floor's printer as the default printer.

To ensure the correct printer is connected even if users roam between floors, the policies are filtered based on the subnet or the name of the thin client. That configuration, referred to as proximity printing, allows for local printer driver maintenance (according to the delegated administration model).

If a printer queue needs to be modified or added, Citrix administrators must modify the respective Session printer policy within the environment.

Because the network printing traffic will be sent outside the ICA virtual channel, QoS is implemented. Inbound and outbound network traffic on ports used by ICA/HDX traffic are prioritized over all other network traffic. That configuration ensures that user sessions are not impacted by large print jobs.

#### Auto-created client printers and Citrix Universal printer driver

For home offices where users work on non-standard workstations and use non-managed print devices, the simplest approach is to use auto-created client printers and the Universal printer driver.

#### Deployment summary

In summary, the sample deployment is configured as follows:

- No printer drivers are installed on Server OS machines. Only the Citrix Universal printer driver is used. Fallback to native printing and the automatic installation of printer drivers are disabled.
- A policy is configured to auto-create all client printers for all users. Server OS machines will directly connect to the print servers by default. The only configuration required is to enable the Universal Print Server components.
- A session printer policy is configured for every floor of Branch B and applied to all thin clients of the respective floor.
- QoS is implemented for Branch B to ensure excellent user experience.

# 最佳做法、安全注意事项和默认操作

May 28, 2016

## Best practices

Many factors determine the best printing solution for a particular environment. Some of these best practices might not apply to your Site.

- Use the Citrix Universal Print Server.
- Use the Universal printer driver or Windows-native drivers.
- Minimize the number of printer drivers installed on Server OS machines.
- Use driver mapping to native drivers.
- Never install untested printer drivers on a production site.
- Avoid updating a driver. Always attempt to uninstall a driver, restart the print server, and then install the replacement driver.
- Uninstall unused drivers or use the Printer driver mapping and compatibility policy to prevent printers from being created with the driver.
- Try to avoid using version 2 kernel-mode drivers.
- To determine if a printer model is supported, contact the manufacturer or see the Citrix Ready product guide at [www.citrix.com/ready](http://www.citrix.com/ready).

In general, all of the Microsoft-supplied printer drivers are tested with Terminal Services and guaranteed to work with Citrix. However, before using a third-party printer driver, consult your printer driver vendor to ensure the driver is certified for Terminal Services by the Windows Hardware Quality Labs (WHQL) program. Citrix does not certify printer drivers.

## Security considerations

Citrix printing solutions are secure by design.

- The Citrix Print Manager Service constantly monitors and responds to session events such as logon and logoff, disconnect, reconnect, and session termination. It handles service requests by impersonating the actual session user.
- Citrix printing assigns each printer a unique namespace in a session.
- Citrix printing sets the default security descriptor for auto-created printers to ensure that client printers auto-created in one session are inaccessible to users running in other sessions. By default, administrative users cannot accidentally print to another session's client printer, even though they can see and manually adjust permissions for any client printer.

## Default print operations

By default, if you do not configure any policy rules, printing behavior is as follows:

- The Universal Print Server is disabled.
- All printers configured on the user device are created automatically at the beginning of each session.  
This behavior is equivalent to configuring the Citrix policy setting Auto-create client printers with the Auto-create all client printers option.
- The system routes all print jobs queued to printers locally attached to user devices as client print jobs (that is, over the ICA channel and through the user device).
- The system routes all print jobs queued to network printers directly from Server OS machines. If the system cannot route the jobs over the network, it will route them through the user device as a redirected client print job.  
This behavior is equivalent to disabling the Citrix policy setting Direct connection to print servers.
- The system attempts to store printing properties, a combination of the user's printing preferences and printing device-

specific settings, on the user device. If the client does not support this operation, the system stores printing properties in user profiles on the Server OS machine.

This behavior is equivalent to configuring the Citrix policy setting Printer properties retention with the Held in profile only if not saved on client option.

- The system uses the Windows version of the printer driver if it is available on the Server OS machine. If the printer driver is not available, the system attempts to install the driver from the Windows operating system. If the driver is not available in Windows, it uses a Citrix Universal print driver.

This behavior is equivalent to enabling the Citrix policy setting Automatic installation of in-box printer drivers and configuring the Universal printing setting with the Use universal printing only if requested driver is unavailable.

Enabling Automatic installation of in-box printer drivers might result in the installation of a large number of native printer drivers.

Note: If you are unsure about what the shipping defaults are for printing, display them by creating a new policy and setting all printing policy rules to Enabled. The option that appears is the default.

#### Always-On logging

XenApp and XenDesktop include an Always-On logging feature for the print server and printing subsystem on the VDA.

In order to collate the logs as a ZIP for emailing, or to automatically upload to Citrix Insights Services, use the PowerShell cmdlet (Start-TelemetryUpload) supplied with the VDA installer.

# 打印策略和首选项

May 28, 2016

When users access printers from published applications, you can configure Citrix policies to specify:

- How printers are provisioned (or added to sessions)
- How print jobs are routed
- How printer drivers are managed

You can have different printing configurations for different user devices, users, or any other objects on which policies are filtered.

Most printing functions are configured through the Citrix Printing policies. Printing settings follow standard Citrix policy behavior.

The system can write printer settings to the printer object at the end of a session or to a client printing device, provided the user's network account has sufficient permissions. By default, Receiver uses the settings stored in the printer object in the session, before looking in other locations for settings and preferences.

By default, the system stores, or retains, printer properties on the user device (if supported by the device) or in the user profile on the Server OS machine. When a user changes printer properties during a session, those changes are updated in the user profile on the machine. The next time the user logs on or reconnects, the user device inherits those retained settings. That is, printer property changes on the user device do not impact the current session until after the user logs off and then logs on again.

## Printing preference locations

In Windows printing environments, changes made to printing preferences can be stored on the local computer or in a document. In this environment, when users modify printing settings, the settings are stored in these locations:

- **On the user device itself** – Windows users can change device settings on the user device by right-clicking the printer in the Control Panel and selecting Printing Preferences. For example, if Landscape is selected as page orientation, landscape is saved as the default page orientation preference for that printer.
- **Inside of a document** – In word-processing and desktop-publishing programs, document settings, such as page orientation, are often stored inside documents. For example, when you queue a document to print, Microsoft Word typically stores the printing preferences you specified, such as page orientation and the printer name, inside the document. These settings appear by default the next time you print that document.
- **From changes a user made during a session** – The system keeps only changes to the printing settings of an auto-created printer if the change was made in the Control Panel in the session; that is, on the Server OS machine.
- **On the Server OS machine** – These are the default settings associated with a particular printer driver on the machine.

The settings preserved in any Windows-based environment vary according to where the user made the changes. This also means that the printing settings that appear in one place, such as in a spreadsheet program, can be different than those in others, such as documents. As result, printing settings applied to a specific printer can change throughout a session.

## Hierarchy of user printing preferences

Because printing preferences can be stored in multiple places, the system processes them according to a specific priority. Also, it is important to note that device settings are treated distinctly from, and usually take precedence over, document settings.

By default, the system always applies any printing settings a user modified during a session (that is, the retained settings) before considering any other settings. When the user prints, the system merges and applies the default printer settings stored on the Server OS machine with any retained or client printer settings.

## Saving user printing preferences

Citrix recommends that you do not change where the printer properties are stored. The default setting, which saves the printer properties on the user device, is the easiest way to ensure consistent printing properties. If the system is unable to save properties on the user device, it automatically falls back to the user profile on the Server OS machine.

Review the Printer properties retention policy setting if these scenarios apply:

- If you use legacy plug-ins that do not allow users to store printer properties on a user device.
- If you use mandatory profiles on your Windows network and want to retain the user's printer properties.

# 置备打印机

May 28, 2016

There are three printer provisioning methods:

- [Citrix Universal Print Server](#)
- [Auto-created client printers](#)
- [Assign network printers to users](#)

## Citrix Universal Print Server

When determining the best print solution for your environment, consider the following:

- The Universal Print Server provides features not available for the Windows Print Provider: Image and font caching, advanced compression, optimization, and QoS support.
- The Universal print driver supports the public device-independent settings defined by Microsoft. If users need access to device settings that are specific to a print driver manufacturer, the Universal Print Server paired with a Windows-native driver might be the best solution. With that configuration, you retain the benefits of the Universal Print Server while providing users access to specialized printer functionality. A trade-off to consider is that Windows-native drivers require maintenance.
- The Citrix Universal Print Server provides universal printing support for network printers. The Universal Print Server uses the Universal print driver, a single driver on the Server OS machine that allows local or network printing from any device, including thin clients and tablets.

To use the Universal Print Server with a Windows-native driver, enable the Universal Print Server. By default, if the Windows-native driver is available, it is used. Otherwise, the Universal print driver is used. To specify changes to that behavior, such as to use only the Windows-native driver or only the Universal print driver, update the Universal print driver usage policy setting.

## Install the Citrix Universal Print Server (UPS)

The UPServer component, which you install on print servers, is now supported on Windows Server 2012 R2 and Windows Server 2012.

Check the latest [System Requirements](#) for the UPServer component.

The UPClient component, which you install on XenApp and XenDesktop hosts that provision session network printers, is part of the VDA installation.

User authentication during printing operations requires the Universal Print Server to be joined to the same domain as the Remote Desktop Services VDA.

To install the Citrix Universal Print Server:

1. Using the LTSR CU1 image, install the Universal Print Server component on a print server running Windows Server 2008 R2 SP1 or Windows Server 2012 R2 and 2012. Along with the Universal Print Server component, this also installs the following prerequisites:
  - Microsoft Visual Studio 2013 Runtime (both 32-bit and 64-bit)
  - Microsoft .NET Framework 4.5.1
  - CDF\_x64.msi for 64-bit platforms or CDF\_x86.msi for 32-bit platforms

2. A restart is required after installing the UPServer component.

For environments where you want to deploy the UPClient component separately, for example with **XenApp 6.5**:

1. Download the XenApp and XenDesktop 7.6 FP3 Virtual Delivery Agent (VDA) standalone package for Windows Desktop OS or Windows Server OS.
2. Extract the VDA using the command line instructions described in [Install VDAs using the standalone package](#).
3. Install the pre-requisites from the \Image-Full\Support\VcRedist\_2013\_RTM
  - Vcredist\_x64 / vcredist\_x86
    - Run x86 for 32-bit only, and both for 64-bit deployments
4. Install the cdf pre-requisite from the \Image-Full\x64\Virtual Desktop Components or \Image-Full\x86\Virtual Desktop Components.
  - Cdf\_x64 / Cdf\_x86
    - x86 for 32-bit, x64 for 64-bit
5. Find the UPClient component in \Image-Full\x64\Virtual Desktop Components or \Image-Full\x86\Virtual Desktop Components.
6. Install the UPClient component by extracting and then launching the component's MSI.
7. A restart is required after installing the UPClient component.

### Configure the Universal Print Server

Use the following Citrix policy settings to configure the Universal Print Server. For more information, refer to the on-screen policy settings help.

- **Universal Print Server enable.** Universal Print Server is disabled by default. When you enable Universal Print Server, you choose whether to use the Windows Print Provider if the Universal Print Server is unavailable. After you enable the Universal Print Server, a user can add and enumerate network printers through the Windows Print Provider and Citrix Provider interfaces.
- **Universal Print Server print data stream (CGP) port.** Specifies the TCP port number used by the Universal Print Server print data stream CGP (Common Gateway Protocol) listener. Defaults to **7229**.
- **Universal Print Server web service (HTTP/SOAP) port.** Specifies the TCP port number used by the Universal Print Server listener for incoming HTTP/SOAP requests. Defaults to **8080**.

To change the default port of HTTP 8080 for Universal Print Server communication to XenApp and XenDesktop VDAs, the following registry must also be created and the port number value modified on the Universal Print Server computer(s):

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\PrintingPolicies  
"UpsHttpPort"=DWORD:<portnumber>
```

This port number must match the HDX Policy, Universal Print Server web service (HTTP/SOAP) port, in Studio.

- **Universal Print Server print stream input bandwidth limit (kbps).** Specifies the upper bound (in kilobits-per-second) for the transfer rate of print data delivered from each print job to the Universal Print Server using CGP. Defaults to 0 (unlimited).

### Interactions with other policy settings

The Universal Print Server honors other Citrix printing policy settings and interacts with them as noted in the following table. The information provided assumes that the Universal Print Server policy setting is enabled, the Universal Print Server components are installed, and the policy settings are applied.

Policy setting	Interaction
Client printer redirection, Auto-create client printers	After the Universal Print Server is enabled, client network printers are created using the Universal print driver instead of the native drivers. Users see the same printer name as before.
Session printers	When you use the Citrix Universal Print Server solution, Universal print driver policy settings are honored.
Direct connections to print server	When the Universal Print Server is enabled and the Universal print driver usage policy setting is configured to use universal printing only, a direct network printer can be created to the print server, using the Universal print driver.
UPD preference	Supports EMF and XPS drivers.

### Effects on user interfaces

The Citrix Universal print driver used by the Universal Print Server disables the following user interface controls:

- In the Printer Properties dialog box, the Local Printer Settings button
- In the Document Properties dialog box, the Local Printer Settings and Preview on client buttons

When using the Universal Print Server, the Add Printer Wizard for the Citrix Print Provider is the same as the Add Printer Wizard for the Windows Print Provider, with the following exceptions:

- When adding a printer by name or address, you can provide an HTTP/SOAP port number for the print server. That port number becomes a part of the printer name and appears in displays.
- If the Citrix Universal print driver usage policy setting specifies that universal printing must be used, the Universal print driver name appears when selecting a printer. The Windows Print Provider cannot use the Universal print driver.

The Citrix Print Provider does not support client-side rendering.

For more information about the Universal Print Server, see [CTX200328](#).

### Auto-created client printers

These universal printing solutions are provided for client printers:

- **Citrix Universal Printer** - A generic printer created at the beginning of sessions that is not tied to a printing device. The Citrix Universal Printer is not required to enumerate the available client printers during logon, which can greatly reduce resource usage and decrease user logon times. The Universal Printer can print to any client-side printing device.  
The Citrix Universal Printer might not work for all user devices or Receivers in your environment. The Citrix Universal Printer requires a Windows environment and does not support the Citrix Offline Plug-in or applications that are streamed to the client. Consider using auto-created client printers and the Universal print driver for such environments.

To use a universal printing solution for non-Windows Receivers, use one of the other Universal print drivers that are based on postscript/PCL and installed automatically.

- **Citrix Universal print drivers** - A device-independent printer driver. If you configure a Citrix Universal print driver, the system uses the EMF-based Universal print driver by default.

The Citrix Universal print driver might create smaller print jobs than older or less advanced printer drivers. However, a device-specific driver might be needed to optimize print jobs for a specialized printer.

**Configure universal printing** - Use the following Citrix policy settings to configure universal printing. For more information, refer to the on-screen policy settings help.

- Universal print driver usage. Specifies when to use universal printing.
- Auto-create generic universal printer. Enables or disables auto-creation of the generic Citrix Universal Printer object for sessions when a user device compatible with Universal Printing is in use. By default, the generic Universal Printer object is not auto-created.
- Universal driver preference. Specifies the order in which the system attempts to use Universal print drivers, beginning with the first entry in the list. You can add, edit, or remove drivers and change the order of the drivers in the list.
- Universal printing preview preference. Specifies whether to use the print preview function for auto-created or generic universal printers.
- Universal printing EMF processing mode. Controls the method of processing the EMF spool file on the Windows user device. By default, EMF records are spooled directly to the printer. Spooling directly to the printer allows the spooler to process the records faster and uses fewer CPU resources.

For more policies, see [Optimize printing performance](#). To change the defaults for settings such as paper size, print quality, color, duplex, and the number of copies, see [CTX113148](#).

**Auto-create printers from the user device** - At the start of a session, the system auto-creates all printers on the user device by default. You can control what, if any, types of printers are provisioned to users and prevent autocreation.

Use the Citrix policy setting Auto-create client printers to control autocreation. You can specify that:

- All printers visible to the user device, including network and locally attached printers, are created automatically at the start of each session (default)
- All local printers physically attached to the user device are created automatically
- Only the default printer for the user device is created automatically
- Autocreation is disabled for all client printers

The Auto-create client printers setting requires that the Client printer redirection setting is Allowed (the default).

#### Assign network printers to users

By default, network printers on the user device are created automatically at the beginning of sessions. the system enables you to reduce the number of network printers that are enumerated and mapped by specifying the network printers to be created within each session. Such printers are referred to as session printers.

You can filter session printer policies by IP address to provide proximity printing. Proximity printing enables users within a specified IP address range to automatically access the network printing devices that exist within that same range. Proximity printing is provided by the Citrix Universal Print Server and does not require the configuration described in this section.

Proximity printing might involve the following scenario:

- The internal company network operates with a DHCP server which automatically designates IP addresses to users.
- All departments within the company have unique designated IP address ranges.
- Network printers exist within each department's IP address range.

When proximity printing is configured and an employee travels from one department to another, no additional printing device configuration is required. Once the user device is recognized within the new department's IP address range, it will have access to all network printers within that range.

**Configure specific printers to be redirected in sessions** - To create administrator-assigned printers, configure the Citrix policy setting Session printers. Add a network printer to that policy using one of the following methods:

- Enter the printer UNC path using the format \\servername\printename.
- Browse to a printer location on the network.
- Browse for printers on a specific server. Enter the server name using the format \\servername and click Browse.

Important: The server merges all enabled session printer settings for all applied policies, starting from the highest to lowest priorities. When a printer is configured in multiple policy objects, custom default settings are taken from only the highest priority policy object in which that printer is configured.

Network printers created with the Session printers setting can vary according to where the session was initiated by filtering on objects such as subnets.

**Specify a default network printer for a session** - By default, the user's main printer is used as the default printer for the session. Use the Citrix policy setting Default printer to change how the default printer on the user device is established in a session.

1. On the Default printer settings page, select a setting for Choose client's default printer:
  - Network printer name. Printers added with the Session printers policy setting appear in this menu. Select the network printer to use as the default for this policy.
  - Do not adjust the user's default printer. Uses the current Terminal Services or Windows user profile setting for the default printer. For more information, refer to the on-screen policy settings help.
2. Apply the policy to the group of users (or other filtered objects) you want to affect.

**Configure proximity printing** - Proximity printing is also provided by the Citrix Universal Print Server, which does not require the configuration described here.

1. Create a separate policy for each subnet (or to correspond with printer location).
2. In each policy, add the printers in that subnet's geographic location to the Session printers setting.
3. Set the Default printer setting to Do not adjust the user's default printer.
4. Filter the policies by client IP address. Be sure to update these policies to reflect changes to the DHCP IP address ranges.

# 维护打印环境

May 28, 2016

Maintaining the printing environment includes:

- Managing printer drivers
- Optimizing printing performance
- Displaying printer and managing print queues

## Manage printer drivers

To minimize administrative overhead and the potential for print driver issues, Citrix recommends use of the Citrix Universal print driver.

If auto-creation fails, by default, the system installs a Windows-native printer driver provided with Windows. If a driver is not available, the system falls back to the Universal print driver. For more information about printer driver defaults, refer to [Best practices, security considerations, and default operations](#).

If the Citrix Universal print driver is not an option for all scenarios, map printer drivers to minimize the amount of drivers installed on Server OS machines. In addition, mapping printer drivers enables you to:

- Allow specified printers to use only the Citrix Universal print driver
- Allow or prevent printers to be created with a specified driver
- Substitute good printer drivers for outdated or corrupted drivers
- Substitute a driver that is available on Windows server for a client driver name

**Prevent the automatic installation of printer drivers** - The automatic installation of print drivers should be disabled to ensure consistency across Server OS machines. This can be achieved through Citrix policies, Microsoft policies, or both. To prevent the automatic installation of Windows-native printer drivers, disable the Citrix policy setting Automatic installation of in-box printer drivers.

**Map client printer drivers** - Each client provides information about client-side printers during logon, including the printer driver name. During client printer autocreation, Windows server printer driver names are selected that correspond to the printer model names provided by the client. The autocreation process then uses the identified, available printer drivers to construct redirected client print queues.

Here is the general process for defining driver substitution rules and editing print settings for mapped client printer drivers:

1. To specify driver substitution rules for auto-created client printers, configure the Citrix policy setting Printer driver mapping and compatibility by adding the client printer driver name and selecting the server driver that you want to substitute for the client printer driver from the Find printer driver menu. You can use wildcards in this setting. For example, to force all HP printers to use a specific driver, specify HP\* in the policy setting.
2. To ban a printer driver, select the driver name and choose the Do not create setting.
3. As needed, edit an existing mapping, remove a mapping, or change the order of driver entries in the list.
4. To edit the printing settings for mapped client printer drivers, select the printer driver, click Settings, and specify settings such as print quality, orientation, and color. If you specify a printing option that the printer driver does not support, that option has no effect. This setting overrides retained printer settings the user set during a previous session.
5. Citrix recommends testing the behavior of the printers in detail after mapping drivers, since some printer functionality can be available only with a specific driver.

When users log on the system checks the client printer driver compatibility list before it sets up the client printers.

## Optimize printing performance

To optimize printing performance, use the Universal Print Server and Universal print driver. The following policies control printing optimization and compression:

- Universal printing optimization defaults. Specifies default settings for the Universal Printer when it is created for a session:
  - Desired image quality specifies the default image compression limit applied to universal printing. By default, Standard Quality is enabled, meaning that users can only print images using standard or reduced quality compression.
  - Enable heavyweight compression enables or disables reducing bandwidth beyond the compression level set by Desired image quality, without losing image quality. By default, heavyweight compression is disabled.
  - Image and Font Caching settings specify whether or not to cache images and fonts that appear multiple times in the print stream, ensuring each unique image or font is sent to the printer only once. By default, embedded images and fonts are cached.
  - Allow non-administrators to modify these settings specifies whether or not users can change the default print optimization settings within a session. By default, users are not allowed to change the default print optimization settings.
- Universal printing image compression limit. Defines the maximum quality and the minimum compression level available for images printed with the Universal print driver. By default, the image compression limit is set to Best Quality (lossless compression).
- Universal printing print quality limit. Specifies the maximum dots per inch (dpi) available for generating printed output in the session. By default, no limit is specified.

By default, all print jobs destined for network printers route from the Server OS machine, across the network, and directly to the print server. Consider routing print jobs over the ICA connection if the network has substantial latency or limited bandwidth. To do that, disable the Citrix policy setting Direct connections to print servers. Data sent over the ICA connection is compressed, so less bandwidth is consumed as the data travels across the WAN.

**Improve session performance by limiting printing bandwidth** - While printing files from Server OS machines to user printers, other virtual channels (such as video) may experience decreased performance due to competition for bandwidth especially if users access servers through slower networks. To prevent such degradation, you can limit the bandwidth used by user printing. By limiting the data transmission rate for printing, you make more bandwidth available in the HDX data stream for transmission of video, keystrokes, and mouse data.

Important: The printer bandwidth limit is always enforced, even when no other channels are in use.

Use the following Citrix policy Bandwidth printer settings to configure printing bandwidth session limits. To set the limits for the site, perform this task using Studio. To set the limits for individual servers, perform this task using the Group Policy Management Console in Windows locally on each Server OS machine.

- The Printer redirection bandwidth limit setting specifies the bandwidth available for printing in kilobits per second (kbps).
- The Printer redirection bandwidth limit percent setting limits the bandwidth available for printing to a percentage of the overall bandwidth available.

Note: To specify bandwidth as a percentage using the Printer redirection bandwidth limit percent setting, enable the Overall session bandwidth limit as well.

If you enter values for both settings, the most restrictive setting (the lower value) is applied.

To obtain real-time information about printing bandwidth, use Citrix Director.

## Display printers and manage print queues

The following table summarizes where you can display printers and manage print queues in your environment.

	<b>Printing Pathway</b>	<b>UAC Enabled?</b>	<b>Location</b>
Client printers (Printers attached to the user device)	Client printing pathway	On	Print Management snap-in located in the Microsoft Management Console
		Off	Pre-Windows 8: Control Panel Windows 8: Print Management snap-in
Network printers (Printers on a network print server)	Network printing pathway	On	Print Server > Print Management snap-in located in the Microsoft Management Console
		Off	Print Server > Control Panel
Network printers (Printers on a network print server)	Client printing pathway	On	Print Server > Print Management snap-in located in the Microsoft Management Console
		Off	Pre-Windows 8: Control Panel Windows 8: Print Management snap-in
Local network server printers (Printers from a network print server that are added to a Server OS machine)	Network printing pathway	On	Print Server > Control Panel
		Off	Print Server > Control Panel

Note: Print queues for network printers that use the network printing pathway are private and cannot be managed through the system.

# 许可

Oct 05, 2016

## 注意

Studio and Director do not support Citrix License Server VPX. For more information about Citrix License Server VPX, see the Citrix Licensing documentation.

From Studio, you can manage and track licensing, if the license server is in the same domain as Studio or in a trusted domain. For information about other licensing tasks, see

— *Licensing Your Product*

You must be a full license administrator to complete the tasks described below, except for viewing license information. To view license information in Studio, an administrator must have at least the Read Licensing Delegated Administration permission; the built-in Full Administrator and Read-Only Administrator roles have that permission.

The following table lists the supported editions and license models:

Products	Editions	License models
XenApp	<ul style="list-style-type: none"><li>Platinum</li><li>Enterprise</li><li>Advanced</li></ul>	Concurrent
XenDesktop	<ul style="list-style-type: none"><li>Platinum</li><li>Enterprise</li><li>App</li><li>VDI</li></ul>	<ul style="list-style-type: none"><li>User/Device</li><li>Concurrent</li></ul>

To view license information, in the Studio navigation pane, select Configuration and then Licensing. A summary of license usage and settings for the site is displayed with a list of all the licenses currently installed on the specified license server.

To manage licensing, in the Studio navigation pane, select Configuration and then Licensing. Then:

- To download a license from Citrix:
  1. In the Actions pane, select Allocate Licenses.
  2. Type the License Access Code, which is supplied in an email from Citrix.
  3. Select a product and click Allocate Licenses. All the licenses available for that product are allocated and downloaded.  
After you allocate and download all the licenses for a specific License Access Code, you cannot use that License Access Code again. To perform additional transactions with that code, log on to My Account.
- To add licenses that are stored on your local computer or on the network:
  1. In the Actions pane, select Add Licenses.
  2. Browse to a license file and add it to the license server.
- To change the license server:
  1. In the Actions pane, select Change License Server.

2. Type the address of the license server in the form name:port, where name is a DNS, NetBIOS, or IP address. If you do not specify a port number, the default port (27000) is used.
- To select the type of license to use:
    - When configuring the Site, after you specify the license server, you are prompted to select the type of license to use. If there are no licenses on the server, the option to use the product for a 30-day trial period without a license is automatically selected.
    - If there are licenses on the server, their details are displayed and you can select one of them. Or, you can add a license file to the server and then select that one.
  - To change the product edition and licensing model:
    1. In the Actions pane, select Edit Product Edition.
    2. Update the appropriate options.
  - To access the License Administration Console, in the Actions pane, select License Administration Console. The console either appears immediately, or if the dashboard is configured as password-protected, you are prompted for License Administration Console credentials. For details about how to use the console, see  
*Licensing Your Product*
  - To add a licensing administrator:
    1. In the middle pane, choose the Licensing Administrators tab.
    2. In the Actions pane, select Add licensing administrator.
    3. Browse to the user you want to add as an administrator and choose permissions.
  - To edit or delete a licensing administrator, When you select an administrator, the options to Edit licensing administrator (to change the administrator permissions for that administrator) and Delete licensing administrator appear in the Actions pane.
    1. In the middle pane, choose the Licensing Administrators tab and select the administrator you want to delete or edit.
    2. In the Actions pane, select either Edit licensing administrator or Delete licensing administrator.
  - To add a licensing administrator group:
    1. In the middle pane, choose the Licensing Administrators tab.
    2. In the Actions pane, select Add licensing administrator group.
    3. Browse to the group you want to act as licensing administrators and choose permissions. Adding an Active Directory Group gives licensing administrator permissions to the users within that group.
  - To edit or delete a licensing administrator group:
    1. In the middle pane, choose the Licensing Administrators tab and select the administrator group you want to delete or edit. When you select a licensing administrator group, the options to Edit licensing administrator group (to change the administrator permissions for that group) and Delete licensing administrator group appear in the Actions pane..
    2. In the Actions pane, select either Edit licensing administrator group or Delete licensing administrator group.

# 连接和资源

May 28, 2016

You create your first connection to hosting resources when you create a Site. Later, you can change that connection and create new ones. Read Only Administrators can view connection and resource details; you must be a Full Administrator to perform connection and resource management tasks.

## Create a connection and resources

The hosting resources must be available before you create a connection.

1. Select Configuration > Hosting in the Studio navigation pane.
2. Select Add Connections and Resources in the Actions pane.
3. Select Create a new Connection.
4. On the Connection page:
  - Select the connection type and enter a connection name - choose a name that will help administrators identify the host type and deployment address. Additional required information depends on the selected connection type.

Connection type	Information needed
Citrix XenServer, Microsoft System Center Virtual Machine Manager, VMware vSphere, or Microsoft Configuration Manager Wake On LAN	<p>Enter the connection URL, user name, and password.</p> <ul style="list-style-type: none"><li>• For XenServer, Citrix recommends using HTTPS to secure communications. To use HTTPS, you must replace the default SSL certificate installed with XenServer with one from a trusted certificate authority; see <a href="#">CTX128656</a>.</li><li>• For XenServer, you can edit the new connection and select the high availability hypervisors to be used, if high availability is enabled on XenServer.</li></ul>
Citrix CloudPlatform or Amazon Web Services (AWS)	<p>Enter the connection URL, API key and Secret key.</p> <ul style="list-style-type: none"><li>• You can browse to an import keys file provided by your cloud administrator to fill in the API key and Secret key.</li><li>• The credentials file for the root AWS account (retrieved from the AWS console) is not formatted the same as credentials files downloaded for standard AWS users. Therefore, Studio cannot use the file to populate the API key and Secret key fields. Ensure that you are using AWS IAM credentials files when using Studio in an AWS environment.</li></ul>

- Choose the tools you will use to create virtual machines. For hypervisors that provide GPU resources, choose Studio Tools.
5. On the Storage page, select storage types and devices. When using Machine Creation Services, select the network and storage resources for the new virtual machines. If you use shared storage on XenServer connections, you can enable IntelliCache to reduce load on the storage device. For information about using IntelliCache, see below.
  6. If the Connection has GPU capabilities, select the option to use graphics virtualization and then select a GPU type and group.
  7. Enter a name for the resources.

## Create a connection and resources from an existing connection

1. Select Configuration > Hosting in the Studio navigation pane.

2. Select Add Connection and Resources in the Actions pane.
3. Select Use an existing Connection and then choose the relevant connection.
4. Choose the tools you will use to create virtual machines. For hypervisors that provide GPU resources, choose Studio Tools. If the Connection has GPU capabilities, select the option to use graphics virtualization and then select a GPU type and group.
5. Enter a name for the resources.

## Add storage

1. Select Configuration > Hosting in the Studio navigation pane.
2. Select a connection and then select Add Storage in the Actions pane.
3. Select the storage to add.

## Edit storage

1. Select Configuration > Hosting in the Studio navigation pane.
2. Select a resources entry under a connection and then select Edit Storage in the Actions pane.
3. On the Standard Storage page, select or clear the check boxes for the storage locations that will store virtual machines. If you clear a storage location that was accepting new machines, it will no longer accept new machines. Existing machines will continue using that location (and write data to it); so it is possible for a storage location to become full even after it stops accepting new machines. If PvD storage is used, select or clear the check boxes on the PvD Storage page, too.

## Edit a connection

Do not use this procedure to rename a connection or to create a new connection. Those are different operations.

1. Select Configuration > Hosting in the Studio navigation pane.
2. Select the connection and then select Edit Connection in the Actions pane.
  - To change the connection address and credentials, on the Connection Properties page, click Edit settings and then enter the new information. You cannot change the GPU settings for a connection, because machine catalogs accessing this resource must use an appropriate GPU-specific master image. Create a new connection.
  - To specify the high-availability servers for a XenServer connection, on the Connection Properties page, click Edit HA servers. Citrix recommends that you select all servers in the pool to allow communication with XenServer if the pool master fails.
  - For a Microsoft System Center Configuration Manager (ConfMgr) Wake on LAN connection, on the Advanced page, enter ConfMgr Wake Proxy, magic packets, and packet transmission information.
  - To configure throttling based on thresholds of simultaneous actions on the connection, which can help when power management settings allow too many or too few machines to start at the same time.
    - On the Advanced page, for Simultaneous actions (all types) and Simultaneous Personal Storage inventory updates, specify two values: the maximum absolute number that can occur simultaneously on this connection, and a percentage of all machines using this connection. You must specify both absolute and percentage values, but the actual limit applied is the lower of the configured values. For example, in a deployment with 34 machines, if Simultaneous actions (all types) is set to an absolute value of 10 and a percentage value of 10, the actual limit applied is 3 (that is, 10 percent of 34 rounded to the nearest whole number, which is less than the absolute value of 10 machines).
    - Specify the maximum number of new actions per minute. This is an absolute number.

Note: Enter information in the Connection options field on the Advanced page only under the guidance of a Citrix Support representative.

## Turn maintenance mode on or off for a connection

Turning on maintenance mode for a connection prevents any new power action from affecting any machine stored on the connection. Users cannot connect to a machine when it is in maintenance mode. If users are already connected, maintenance mode takes effect when they log off.

1. Select Configuration > Hosting in the Studio navigation pane.
2. Select the connection. To turn maintenance mode on, select Turn On Maintenance Mode in the Actions pane. To turn maintenance mode off, select Turn Off Maintenance Mode.

You can also turn maintenance mode on or off for individual machines; see below.

## Delete a connection

**Caution:** Deleting a connection can result in the deletion of large numbers of machines and loss of data. Ensure that user data on affected machines is backed up or no longer required.

Before you delete a Connection, ensure that:

- All users are logged off from the machines stored on the connection.
- No disconnected user sessions are running.
- Maintenance mode is turned on for pooled and dedicated machines.
- All machines in machine catalogs are powered off.

1. Select Configuration > Hosting in the Studio navigation pane.
2. Select the connection and then select Delete Connection in the Actions pane.
3. If this connection has machines stored on it, you are asked whether the machines should be deleted. If they are to be deleted, specify what should be done with the associated Active Directory computer accounts.

A machine catalog becomes unusable when you delete a connection that is referenced by that catalog. If this connection is referenced by a catalog, you have the option to delete the catalog. Before you delete a catalog, make sure it is not used by other connections.

## Rename a connection

1. Select Configuration > Hosting in the Studio navigation pane.
2. Select the connection and then select Rename Connection in the Actions pane.

## View machine details on a connection

1. Select Configuration > Hosting in the Studio navigation pane.
2. Select the connection and then select View Machines in the Actions pane.

The upper pane lists the machines accessed through the connection. Select a machine to view its details in the lower pane. Session details are also provided for open sessions.

Use the search feature to find machines quickly. Either select a saved search from the list at the top of the window, or create a new search. You can either search by typing all or part of the machine name, or you can build an expression to use for an advanced search. To build an expression, click Unfold, and then select from the lists of properties and operators.

## Manage machines on a connection

1. Select Configuration > Hosting in the Studio navigation pane.

2. Select a connection and then select View Machines in the Action pane.
3. Select one of the following in the Actions pane. Some actions may not be available, depending on the machine state and the connection host type.
  - Start - Starts the machine if it is powered off or suspended.
  - Suspend - Pauses the machine without shutting it down, and refreshes the list of machines.
  - Shut down - Requests the operating system to shut down.
  - Force shut down - Forcibly powers off the machine, and refreshes the list of machines.
  - Restart - requests the operating system to shut down and then start the machine again. If the operating system cannot comply, the desktop remains in its current state.
  - Enable maintenance mode - To temporarily stop connections to a machine, put it into maintenance mode. Users cannot connect to a machine in this state. If users are connected, maintenance mode takes effect when they log off.

To turn maintenance mode on or off for all machines accessed through a connection, see above.

- Remove from Delivery Group - Removing a machine from a Delivery Group does not delete it from the machine catalog that the Delivery Group uses. You can remove a machine only when no user is connected to it (turn on maintenance mode to temporarily prevent users from connecting while you are removing the machine).
- Delete - When you delete a machine, users no longer have access to it, and the machine is deleted from the machine catalog. Before deleting a machine, ensure that all user data is backed up or no longer required. You can delete a machine only when no user is connected to it (turn on maintenance mode to temporarily stop users from connecting while you are deleting the machine).

For actions that involve machine shutdown, if the machine does not shut down within 10 minutes, it is powered off. If Windows attempts to install updates during shutdown, there is a risk that the machine will be powered off before the updates are complete.

## Delete, rename, or test resources

1. Select Configuration > Hosting in the Studio navigation pane.
2. Select the resource and then select the appropriate entry in the Actions pane: Delete Resources, Rename Resources, or Test Resources.

## Use IntelliCache for XenServer connections

Using IntelliCache, hosted VDI deployments are more cost-effective because you can use a combination of shared storage and local storage. This enhances performance and reduces network traffic . The local storage caches the master image from the shared storage, which reduces the amount of reads on the shared storage. For shared desktops, writes to the differencing disks are written to local storage on the host and not to shared storage.

- Shared storage must be NFS when using IntelliCache.
- Citrix recommends that you use a high performance local storage device to ensure the fastest possible data transfer.

To use IntelliCache, you must enable it in both this product and XenServer.

- When installing XenServer, select Enable thin provisioning (Optimized storage for XenDesktop). Citrix does not support mixed pools of servers that have IntelliCache enabled and servers that do not. For more information, see the XenServer documentation.
- In XenApp and XenDesktop, IntelliCache is disabled by default. You can change the setting only when creating a XenServer connection; you cannot disable IntelliCache later. When you add a XenServer connection from Studio:
  - Select Shared as the storage type.
  - Select the Use IntelliCache check box.

## Connection timers

You can use policy settings to configure three connection timers:

- A maximum connection timer. This setting determines the maximum duration of an uninterrupted connection between a user device and a virtual desktop. Use the Session connection timer and Session connection timer interval policy settings.
- A connection idle timer. This setting determines how long an uninterrupted user device connection to a virtual desktop will be maintained if there is no input from the user. Use the Session idle timer and Session idle timer interval policy settings.
- A disconnect timer. This setting determines how long a disconnected, locked virtual desktop can remain locked before the session is logged off. Use the Disconnected session timer and Disconnected session timer interval policy settings .

When you update any of these settings, ensure they are consistent across your deployment.

# 连接租用

May 28, 2016

To ensure that the Site database is always available, Citrix recommends starting with a fault-tolerant SQL Server deployment by following high availability best practices from Microsoft. However, network issues and interruptions may prevent Delivery Controllers from accessing the database, resulting in users not being able to connect to their applications or desktop.

The connection leasing feature supplements the SQL Server high availability best practices by enabling users to connect and reconnect to their most recently used applications and desktops, even when the Site database is not available.

Although users may have a large number of published resources available, they often use only a few of them regularly. When you enable connection leasing, each Controller caches user connections to those recently used applications and desktops during normal operations (when the database is available).

The leases generated on each Controller are uploaded to the Site database for periodic synchronization to other Controllers on the Site. In addition to leases, each Controller's cache holds application, desktop, icon, and worker information. The lease and related information is stored on each Controller's local disk. If the database becomes unavailable, the Controller enters leased connection mode and "replays" the cached operations when a user attempts to connect or reconnect to a recently used application or desktop from StoreFront.

Connections are cached for a lease period of two weeks. So, if the database becomes unavailable, the desktops and applications that the user launched in the previous two weeks remain accessible to that user through StoreFront. However, desktops and applications that have not been launched during the previous two-week lease period are not accessible when the database is unavailable. For example, if a user last launched an application three weeks ago, its lease has expired, and that user cannot launch that application if the database becomes unavailable now. Leases for long-running active or disconnected application or desktop sessions are extended so that they are not considered expired.

By default, connection leasing affects the entire Site; however, you can revoke all leases for specific users, which prevents them from accessing any applications or desktops when the Controller is in leased connection mode. Several other registry settings apply on a Controller basis.

## Considerations and limitations

While connection leasing can improve connection resiliency and user productivity, there are considerations related to the availability, operation, and performance of other features.

Connection leasing is supported for server-hosted applications and desktops, and static (assigned) desktops; it is not supported for pooled VDI desktops or for users who have not been assigned a desktop when the database becomes unavailable.

When the Controller is in leased connection mode:

- Administrators cannot use Studio, Director, or the PowerShell console.
- Workspace Control is not available. When a user logs on to Receiver, sessions do not automatically reconnect; the user must relaunch the application.
- If a new lease is created immediately before the database becomes unavailable, but the lease information has not yet been synchronized across all Controllers, the user might not be able to launch that resource after the database becomes unavailable.
- Server-hosted application and desktop users may use more sessions than their configured session limits. For example:

- A session may not roam when a user launches it from one device (connecting externally through NetScaler Gateway) when the Controller is not in leased connection mode and then connects from another device on the LAN when the Controller is in leased connection mode.
- Session reconnection may fail if an application launches just before the database becomes unavailable; in such cases, a new session and application instance are launched.
- Static (assigned) desktops are not power-managed. VDAs that are powered off when the Controller enters leased connection mode remain unavailable until the database connection is restored, unless the administrator manually powers them on.
- If session prelaunch and session linger are enabled, new prelaunch sessions are not started. Prelaunched and lingering sessions will not be ended according to configured thresholds while the database is unavailable.
- Load management within the Site may be affected. Server-based connections are routed to the most recently used VDA. Load evaluators (and especially, session count rules) may be exceeded.
- The Controller will not enter leased connection mode if you use SQL Server Management Studio to take the database offline. Instead, use one of the following Transact-SQL statements:
  - ALTER DATABASE <database-name> SET OFFLINE WITH ROLLBACK IMMEDIATE
  - ALTER DATABASE <database-name> SET OFFLINE WITH ROLLBACK AFTER <seconds>
 Either statement cancels any pending transactions and causes the Controller to lose its connection with the database. The Controller then enters leased connection mode.

When connection leasing is enabled, there are two brief intervals during which users cannot connect or reconnect: (1) from the time the database becomes unavailable to when the Controller enters leased connection mode, and (2) from the time the Controller changes from leased connection mode to when database access is fully restored and the VDAs have re-registered.

For more considerations, see [XenDesktop 7.6 Connection Leasing Design Considerations](#).

## Configure and deploy

When configuring your deployment to accommodate connection leasing:

- VDAs must be at minimum version 7.6, and the machine catalogs and Delivery Groups that use those machines must be at that minimum level (or a later supported version).
- The Site database size requirements will increase.
- Each Controller needs additional disk space for the cached lease files.

Connection leasing is enabled by default.

You can turn connection leasing off or on from the PowerShell SDK or the Windows registry. From the PowerShell SDK, you can also remove current leases. The following PowerShell cmdlets affect connection leasing; see the cmdlet help for details.

- Set-BrokerSite -ConnectionLeasingEnabled \$true | \$false - Turns connection leasing on or off. Default = \$true
- Get-BrokerServiceAddedCapability - Outputs "ConnectionLeasing" for the local Controller.
- Get-BrokerLease - Retrieves either all or a filtered set of current leases.
- Remove-BrokerLease - Marks either one or a filtered set of leases for deletion.
- Update-BrokerLocalLeaseCache – Updates the connection leasing cache on the local Controller. The data is resynchronized during the next synchronization.

# 虚拟 IP 和虚拟环回

May 28, 2016

Note: These features are valid only for Windows Server 2008 R2 and Windows Server 2012 R2 machines. They do not apply to Windows Desktop OS machines.

The Microsoft virtual IP address feature provides a published application with a unique dynamically-assigned IP address for each session. The Citrix virtual loopback feature allows you to configure applications that depend on communications with localhost (127.0.0.1 by default) to use a unique virtual loopback address in the localhost range (127.\*).

Certain applications, such as CRM and Computer Telephony Integration (CTI), use an IP address for addressing, licensing, identification, or other purposes and thus require a unique IP address or a loopback address in sessions. Other applications may bind to a static port, so attempts to launch additional instances of an application in a multiuser environment will fail because the port is already in use. For such applications to function correctly in a XenApp environment, a unique IP address is required for each device.

Virtual IP and virtual loopback are independent features. You can use either or both.

Administrator action synopsis:

- To use Microsoft virtual IP, enable and configure it on the Windows server.
- To use Citrix virtual loopback, configure two settings in a Citrix policy.

## Virtual IP

When virtual IP is enabled and configured on the Windows server, each configured application running in a session appears to have a unique address. Users access these applications on a XenApp server in the same way they access any other published application. A process requires virtual IP in either of the following cases:

- The process uses a hard-coded TCP port number
- The process uses Windows sockets and requires a unique IP address or a specified TCP port number

To determine if an application needs to use virtual IP addresses:

1. Obtain the TCPView tool from Microsoft. This tool lists all applications that bind specific IP addresses and ports.
2. Disable the Resolve IP Addresses feature so that you see the addresses instead of host names.
3. Launch the application and use TCPView to see which IP addresses and ports are opened by the application and which process names are opening these ports.
4. Configure any processes that open the IP address of the server, 0.0.0.0, or 127.0.0.1.
5. To ensure that an application does not open the same IP address on a different port, launch an additional instance of the application.

## How Microsoft Remote Desktop (RD) IP virtualization works

- Virtual IP addressing must be enabled on the Microsoft server.

For example, in a Windows Server 2008 R2 environment, from Server Manager, expand Remote Desktop Services > RD Session Host Connections to enable the RD IP Virtualization feature and configure the settings to dynamically assign IP addresses using the Dynamic Host Configuration Protocol (DHCP) server on a per-session or per-program basis. See the Microsoft documentation for instructions.

- After the feature is enabled, at session start-up, the server requests dynamically-assigned IP addresses from the DHCP server.
- The RD IP Virtualization feature assigns IP addresses to remote desktop connections per-session or per-program. If you

assign IP addresses for multiple programs, they share a per-session IP address.

- After an address is assigned to a session, the session uses the virtual address rather than the primary IP address for the system whenever the following calls are made: bind, closesocket, connect, WSAConnect, WSAAccept, getpeername, getsockname, sendto, WSASendTo, WSASocketW, gethostbyaddr, getnameinfo, getaddrinfo

When using the Microsoft IP virtualization feature within the Remote Desktop session hosting configuration, applications are bound to specific IP addresses by inserting a “filter” component between the application and Winsock function calls. The application then sees only the IP address it should use. Any attempt by the application to listen for TCP or UDP communications is bound to its allocated virtual IP address (or loopback address) automatically, and any originating connections opened by the application originate from the IP address bound to the application.

In functions that return an address (such as GetAddrInfo(), which is controlled by a Windows policy), if the local host IP address is requested, virtual IP looks at the returned IP address and changes it to the virtual IP address of the session. Applications that attempt to get the IP address of the local server through such name functions see only the unique virtual IP address assigned to that session. This IP address is often used in subsequent socket calls, such as bind or connect.

Often, an application requests to bind to a port for listening on the address 0.0.0.0. When an application does this and uses a static port, you cannot launch more than one instance of the application. The virtual IP address feature also looks for 0.0.0.0 in these call types and changes the call to listen on the specific virtual IP address, which enables more than one application to listen on the same port on the same computer because they are all listening on different addresses. The call is changed only if it is in an ICA session and the virtual IP address feature is enabled. For example, if two instances of an application running in different sessions both try to bind to all interfaces (0.0.0.0) and a specific port (such as 9000), they are bound to VIPAddress1:9000 and VIPAddress2:9000 and there is no conflict.

## Virtual loopback

Enabling the Citrix virtual IP loopback policy settings allows each session to have its own loopback address for communication. When an application uses the localhost address (default = 127.0.0.1) in a Winsock call, the virtual loopback feature simply replaces 127.0.0.1 with 127.X.X.X, where X.X.X is a representation of the session ID + 1. For example, a session ID of 7 is 127.0.0.8. In the unlikely event that the session ID exceeds the fourth octet (more than 255), the address rolls over to the next octet (127.0.1.0), to the maximum of 127.255.255.255.

A process requires virtual loopback in either of the following cases:

- The process uses the Windows socket loopback (localhost) address (127.0.0.1)
- The process uses a hard-coded TCP port number

Use the [virtual loopback policy settings](#) for applications that use a loopback address for interprocess communication. No additional configuration is required. Virtual loopback has no dependency on Virtual IP, so you do not have to configure the Microsoft server.

- Virtual IP loopback support. When enabled, this policy setting allows each session to have its own virtual loopback address. This setting is disabled by default. The feature applies only to applications specified with the Virtual IP virtual loopback programs list policy setting.
- Virtual IP virtual loopback programs list. This policy setting specifies the applications that use the virtual IP loopback feature. This setting applies only when the Virtual IP loopback support policy setting is enabled.

## Related feature

You can use the following registry settings to ensure that virtual loopback is given preference over virtual IP; this is called preferred loopback. However, proceed with caution:

- Preferred loopback is supported on Windows 2008 R2 only.

- Use preferred loopback only if both Virtual IP and virtual loopback are enabled; otherwise, you may have unintended results.
- Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Run regedit on the servers where the applications reside.

- HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\VIP (HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\VIP for 32-bit machines)
- Name: PreferLoopback, Type: REG\_DWORD, Data: 1
- Name: PreferLoopbackProcesses, Type: REG\_MULTI\_SZ, Data: <list of processes>

# 辅助数据库位置

May 28, 2016

By default, the Configuration Logging and Monitoring databases (the secondary databases) are located on the same server as the Site Configuration database. Initially, all three databases have the same name. Citrix recommends that you change the location of the secondary databases after you create a Site. You can host the Configuration Logging and Monitoring databases on the same server or on different servers. The backup strategy for each database may differ.

When you change the location of the Configuration Logging or Monitoring database:

- The data in the previous database is not imported to the new database.
- Logs cannot be aggregated from both databases when retrieving logs.
- The first log entry in the new database indicates that a database change occurred, but it does not identify the previous database.

Before you change the location of the Configuration Logging or Monitoring database, install a supported version of Microsoft SQL Server on the server where the database will reside. Set up mirror, cluster, or other supported redundancy infrastructures, as needed.

You cannot change the location of the Configuration Logging database when mandatory logging is enabled.

Note: You cannot use this method to change the location of the Site Configuration database.

1. Select Configuration in the Studio navigation pane. The names and addresses of the three databases are listed, plus mirror server addresses, if configured.
2. Select the database for which you want to specify a new location and then select Change Database in the Actions pane.
3. Specify the location of the server containing the new SQL Server installation (using one of the forms in the following table) and the database name.

Database type	What to enter	With this database configuration
Standalone or mirror	servername	The default instance is used and SQL Server uses the default port.
	Servername\INSTANCENAME	A named instance is used and SQL Server uses the default port.
	servername,port-number	The default instance is used and SQL Server uses a custom port. (The comma is required.)
Other	cluster-name	A clustered database.
	availability-group-listener	An Always-On database.

4. If you want Studio to create the database, click OK. When prompted, click OK, and Studio will create the database automatically. Studio attempts to access the database using the current Studio user's credentials; if that fails, you are prompted for the database user's credentials. Studio then uploads the database schema to the database. (The credentials are retained only for the database creation time frame.)
5. If you want to create the database manually, click Generate script. The generated scripts includes instructions for manually creating the database and a mirror database, if needed. Ensure that the database is empty and that at least

one user has permission to access and change the database before uploading the schema.

# Delivery Controller 环境

May 28, 2016

In a deployment, the Delivery Controller is the server-side component that is responsible for managing user access, plus brokering and optimizing connections. Controllers also provide the Machine Creation Services that create desktop and server images.

A Site must have at least one Delivery Controller. After you install the initial Controller and create a Site, you can add additional Controllers. There are two primary benefits from having more than one Controller in a Site.

- Redundancy — As best practice, a production Site should always have at least two Controllers on different physical servers. If one Controller fails, the others can manage connections and administer the Site.
- Scalability — As Site activity grows, so does CPU utilization on the Controller and SQL Server database activity. Additional Controllers provide the ability to handle more users and more applications and desktop requests, and can improve overall responsiveness.

## How Virtual Delivery Agents (VDAs) discover Controllers

Before a VDA can be used, it must register (establish communication) with a Controller on the Site. The VDA finds a Controller by checking a list of Controllers called the ListofDDCs. The ListOfDDCs comprises one or more DNS entries or IP addresses that point the VDA to Controllers on the Site. For load balancing, the VDA automatically distributes connections across all Controllers in the list.

In addition to the ListOfDDCs, the ListOfIDs indicates which machine Security IDs (IDs) the VDA allows to contact it as a Controller. The ListOfIDs can be used to decrease the load on Active Directory or to avoid possible security threats from a compromised DNS server.

It is important to ensure that the ListOfDDCs and ListOfIDs on all VDAs contain current information as Controllers are added and removed in the Site. If the lists are not updated, a VDA might reject session launches that were brokered by an unlisted Controller. Invalid entries can delay the startup of the virtual desktop system software. To keep the lists current, you can:

- Use the auto-update feature, which automatically updates the ListOfDDCs and ListOfIDs as Controllers are added or removed. By default, auto-update is enabled.
- Self-manage – that is, manually update policy or registry settings that identify Controllers.

Information in the ListOfDDCs and ListOfIDs can come from several places in a deployment. The VDA checks the following locations, in order, stopping at the first place it finds the lists:

1. A persistent storage location maintained for the auto-update feature. This location contains Controller information when auto-update is enabled and after the VDA successfully registers for the first time after installation. (This storage also holds machine policy information, which ensures that policy settings are retained across restarts.)  
For its initial registration after installation, or when auto-update is disabled, the VDA checks the following locations.
  2. Policy settings (Controllers, Controller SIDs).
  3. The Controller information under the Virtual Desktop Agent key in the registry. The VDA installer initially populates these values, based on Controller information you specify when installing the VDA.
  4. OU-based Controller discovery. This is a legacy method maintained for backward compatibility.
  5. The Personality.ini file created by Machine Creation Services.

If a ListOfDDCs specifies more than one Controller, the VDA attempts to connect to them in random order. The

ListOfDDCs can also contain Controller groups, which are designated by brackets surrounding two or more Controller entries. The VDA attempts to connect to each Controller in a group before moving to other entries in the ListOfDDCs.

For XenDesktop users who have upgraded from versions earlier than 7.0, the auto-update feature replaces the CNAME function from the earlier version. You can manually re-enable the CNAME function, if desired; however, for DNS aliasing to work consistently, you cannot use both the auto-update feature and the CNAME function. See [CTX137960](#) for information about re-enabling the CNAME functionality.

## Considerations for choosing auto-update or self-manage

The policy setting that enables/disables auto-update is enabled by default.

The following types of deployments cannot use auto-update, and must self-manage.

- Deployments that use Controller groups.
- Deployments that use ListOfSIDs for security reasons. (Deployments that use ListOfSIDs to decrease the Active Directory load can use auto-update.)
- Deployments that use Provisioning Services without a write-back disk.
- Deployments that use the Controllers or Controller SIDs policy setting.

## Use auto-update

The auto-update policy setting is located in the Virtual Delivery Agent category.

- To enable auto-update, enable the Enable auto update of Controllers policy setting. This setting is enabled by default.
- To disable auto-update, disable the Enable auto update of Controllers policy setting.

When auto-update is enabled and you install a VDA, the VDA attempts to register with one of the Controller values you specified when you installed the VDA. The installer writes the Controller information you specify during VDA installation to the ListOfDDCs registry value.

After the VDA registers, the Controller with which it registered sends a list of the current Controller Fully Qualified Domain Names (FQDNs) and Security IDs (SIDs) to the VDA. The VDA writes this list to the auto-update persistent storage. Each Controller also checks the Site Configuration Database every 90 minutes for Controller information – if a Controller has been added or removed since the last check, or if a policy change has occurred, the Controller sends updated lists to its registered VDAs. The VDA will accept connections from all the Controllers in the most recent list it received.

If a VDA receives a list that does not include the Controller it is registered with (in other words, that Controller was removed from the Site), the VDA re-registers, choosing among the Controllers in the list. After a VDA registers or re-registers, it receives an updated list.

For example:

1. A deployment has three Controllers: A, B, and C. A VDA is installed and registers with Controller B (which was specified during VDA installation).
2. Two Controllers (D and E) are added to the Site. Within 90 minutes, VDAs receive updated lists and will accept connections from Controllers A, B, C, D, and E. (The load will not be spread equally to all Controllers until the VDAs are restarted.)
3. Controller B is removed from the Site. Within 90 minutes, VDAs receive updated lists because there has been a Controller change since the last check. The VDA installed in step 1 is registered with Controller B, which is no longer on the list, so that VDA re-registers, choosing among the Controllers in the current list (A, C, D, and E).

## Self-manage

If you do not use auto-update, you must update the Citrix policy setting or registry values for each Virtual Delivery Agent (VDA) in the site (or the VDA image) after you add, move, or remove Delivery Controllers in the Site. Registry changes can also be updated using Group Policy Object.

To self-manage using Citrix policy settings:

1. Update the FQDN values specified in the Controllers policy setting. This policy setting is located in the Virtual Delivery Agent category.
2. If you also use ListOfSIDs in your deployment, update the SID values specified in the Controller SIDs policy setting.

To self-manage using the registry:

Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

1. Update the ListOfDDCs registry key, which lists the FQDNs of all the Controllers in the Site. (This key is the equivalent of the Active Directory Site OU.) Separate multiple values with spaces. Surround Controller groups with brackets.

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfDDCs (REG_SZ)`

If the HKEY\_LOCAL\_MACHINE\Software\Citrix\VirtualDesktopAgent registry location contains both the ListOfDDCs and FarmGUID keys, ListOfDDCs is used for Controller discovery; FarmGUID is present if a site OU was specified during VDA installation.

2. Optionally, update the ListOfSIDs registry key:

`HKEY_LOCAL_MACHINE\Software\Citrix\VirtualDesktopAgent\ListOfSIDs (REG_SZ)`

# 添加、删除或移动 Controller 或者移动 VDA

May 28, 2016

To add, remove, or move a Delivery Controller, you need the following roles or permissions:

Operation	Purpose	Server role	Database role
Database creation	Create suitable empty database	dbcreator	
Schema creation	Create all service-specific schemas and add first Controller to Site	securityadmin *	db_owner
Add Controller	Add Controller (other than the first) to the Site	securityadmin *	db_owner
Add Controller (mirror server)	Add Controller login to the database server currently in the mirror role of a mirrored database	securityadmin *	
Remove Controller	Remove Controller from the Site		db_owner
Schema update	Apply schema updates or hotfixes		db_owner

\* While technically more restrictive, in practice, the securityadmin server role should be treated as equivalent to the sysadmin server role.

When using Studio to perform these operations, the user account must explicitly be a member of the sysadmin server role.

If your deployment uses database mirroring:

- Before adding, removing, or moving a Controller, ensure that the principal and mirrored databases are both running. In addition, if you are using scripts with SQL Server Management Studio, enable SQLCMD mode before executing the scripts.
- To verify mirroring after adding, removing, or moving a Controller, run the `get-configdbconnection` PowerShell cmdlet to ensure that the Failover Partner has been set in the connection string to the mirror.

After you add, remove, or move a Controller:

- If auto-update is enabled, the Virtual Delivery Agents (VDAs) will receive an updated list of Controllers within 90 minutes.
- If auto-update is not enabled, ensure that the Controller policy setting or `ListOfDDCs` registry key are updated for all VDAs. After moving a Controller to another Site, update the policy setting or registry key on both Sites.

## Add a Controller

You cannot add servers installed with an earlier version of this software to a Site that was created with this version.

1. On the server you want to add, run the installer and select the Delivery Controller and any other core components you want to install.
2. In Studio, click Join existing deployment and enter the Site address.

## Remove a Controller

Removing a Controller does not uninstall the Citrix software or any other component; it removes the Controller from the Database so that it can no longer be used to broker connections and perform other tasks. If you remove a Controller, you can later add it back to the same Site or to another Site. A Site requires at least one Controller, so you cannot remove the last one listed in Studio.

Note: Make sure that the Controller is powered on so that Studio loads in less than one hour. Once Studio loads the Controller you want to remove, power off the Controller when prompted to do so.

When you remove a Controller from a Site, the Controller logon to the database server is not removed. This avoids potentially removing a logon that is used by other products' services on the same machine. The logon must be removed manually if it is no longer required; the securityadmin server role permission is needed to remove the logon.

**Important:** Do not remove the Controller from Active Directory until *after* you remove it from the Site.

1. Select Configuration > Controllers in the Studio navigation pane, then select the Controller you want to remove.
2. Select Remove Controller in the Actions pane. If you do not have the correct database roles and permissions, you are offered the option of generating a script that allows your database administrator to remove the Controller for you.
3. You might need to remove the Controller's machine account from the database server. Before doing this, check that another service is not using the account.

After using Studio to remove a Controller, traffic to that Controller might linger for a short amount of time to ensure proper completion of current tasks. If you want to force the removal of a Controller in a very short time, Citrix recommends you shut down the server where it was installed, or remove that server from Active Directory. Then, restart the other Controllers on the Site to ensure no further communication with the removed Controller.

## Move a Controller to another Site

You cannot move a Controller to a Site that was created with an earlier version of this software.

1. On the Site where the Controller is currently located (the old Site), select Configuration > Controllers in the Studio navigation pane, then select the Controller you want to move.
2. Select Remove Controller in the Actions pane. If you do not have the correct database roles and permissions, you are offered the option of generating a script that allows your database administrator to remove the Controller for you. A Site requires at least one Controller, so you cannot remove the last one listed in Studio.
3. On the Controller you are moving, open Studio, reset the services when prompted, select Join existing site, and enter the address of the new Site.

## Move a VDA to another Site

If a VDA was provisioned using Provisioning Services or is an existing image, you can move a VDA to another Site (from Site 1 to Site 2) when upgrading, or when moving a VDA image that was created in a test Site to a production Site. VDAs provisioned using Machine Creation Services (MCS) cannot be moved from one Site to another because MCS does not support changing the ListOfDDCs a VDA checks to register with a Controller; VDAs provisioned using MCS always check the ListOfDDCs associated with the Site in which they were created.

There are two ways to move a VDA to another site: using the installer or Citrix policies.

- **Installer:** Run the installer and add a Controller, specifying the FQDN (DNS entry) of a Controller in Site 2.  
    Important: Specify Controllers in the installer only when the Controllers policy setting is not used.
- **Group Policy Editor:** The following example moves multiple VDAs between Sites.
  1. Create a policy in Site 1 that contains the following settings, then filter the policy to the Delivery Group level to initiate a staged VDA migration between the Sites.
    - Controllers - containing FQDNs (DNS entries) of one or more Controllers in Site 2.

- Enable auto update of Controllers - set to disabled.
2. Each VDA in the Delivery Group is alerted within 90 minutes of the new policy. The VDA ignores the list of Controllers it receives (because auto-update is disabled); it selects one of the Controllers specified in the policy, which lists the Controllers in Site 2.
  3. When the VDA successfully registers with a Controller in Site 2, it receives the Site 2 ListOfDDCs and policy information, which has auto-update enabled by default. Since the Controller with which the VDA was registered in Site 1 is not on the list sent by the Controller in Site 2, the VDA re-registers, choosing among the Controllers in the Site 2 list. From then on, the VDA is automatically updated with information from Site 2.

# 基于 Active Directory OU 的控制器发现

Feb 22, 2017

This Delivery Controller discovery method is supported primarily for backward compatibility, and is valid only for Virtual Delivery Agents (VDAs) for Windows Desktop OS, not VDAs for Windows Server OS. Active Directory-based discovery requires that all computers in a Site are members of a domain, with mutual trusting relationships between the domain used by the Controller and the domain(s) used by desktops. If you use this method, you must configure the GUID of the OU in each desktop registry.

To perform an OU-based Controller discovery, run the Set-ADControllerDiscovery.ps1 PowerShell script on the Controller (each Controller contains this script in the folder \$Env:ProgramFiles\Citrix\Broker\Service\Setup Scripts). To run the script, you must have CreateChild permissions on a parent OU, plus full administration rights.

When you create a Site, a corresponding Organizational Unit (OU) must be created in Active Directory if you want desktops to discover the Controllers in the Site through Active Directory. The OU can be created in any domain in the forest that contains your computers. As best practice, the OU should also contain the Controllers in the Site, but this is not enforced or required. A domain administrator with appropriate privileges can create the OU as an empty container, then delegate administrative authority over the OU to a Citrix administrator.

The script creates several essential objects. Only standard Active Directory objects are created and used. It is not necessary to extend the schema.

- A Controllers security group. The computer account of all Controllers in the Site must be a member of this security group. Desktops in a Site accept data from Controllers only if they are members of this security group.  
Ensure that all Controllers have the 'Access this computer from the network' privilege on all virtual desktops running the VDA. You can do this by giving the Controllers security group this privilege. If Controllers do not have this privilege, VDAs will not register.
- A Service Connection Point (SCP) object that contains information about the Site, such as the Site name. If you use the Active Directory Users and Computers administrative tool to inspect a Site OU, you might need to enable Advanced Features in the View menu to see SCP objects.
- A container called RegistrationServices, which is created in the Site OU. This contains one SCP object for each Controller in the Site. Each time the Controller starts, it validates the contents of its SCP and updates it, if necessary.

If multiple administrators are likely to add and remove Controllers after the initial installation, they need permissions to create and delete children on the RegistrationServices container, and Write properties on the Controllers security group; these permissions are granted automatically to the administrator who runs the Set-ADControllerDiscovery.ps1 script. The domain administrator or the original installing administrator can grant these permissions, and Citrix recommends setting up a security group to do this.

When you are using a Site OU:

- Information is written to Active Directory only when installing or uninstalling this software, or when a Controller starts and needs to update the information in its SCP (for example, because the Controller was renamed or because the communication port was changed). By default, the Set-ADControllerDiscovery.ps1 script sets up permissions on the objects in the Site OU appropriately, giving each Controller Write access to its SCP. The contents of the objects in the Site OU are used to establish trust between desktops and Controllers. Ensure that:
  - Only authorized administrators can add or remove computers from the Controllers security group, using the security group's access control list (ACL).

- Only authorized administrators and the respective Controller can change the information in the controller's SCP.
- If your deployment uses replication, be aware of potential delays; see the Microsoft documentation for details. This is particularly important if you create the Site OU in a domain that has domain controllers in multiple Active Directory sites. Depending on the location of desktops, Controllers, and domain controllers, changes that are made to Active Directory when you are initially creating the Site OU, installing or uninstalling Controllers, or changing Controller names or communication ports might not be visible to desktops until that information is replicated to the appropriate domain controller. The symptoms of such replication delay include desktops that cannot establish contact with Controllers and are therefore not available for user connections.
- This software uses several standard computer object attributes in Active Directory to manage desktops. Depending on your deployment, the machine object's fully qualified domain name, as stored in the desktop's Active Directory record, can be included as part of the connection settings that are returned to the user to make a connection. Ensure that this information is consistent with information in your DNS environment.

## Permissions summary

To create a Site, the Citrix administrator who runs the script must have rights over the Site OU to create objects (SCP, container, and security group).

(If the Site OU is not present, the administrator must have rights to create that as well. Citrix recommends that the AD domain administrator pre-create that OU and delegate rights to it to the Citrix Site administrator identity. Optionally, the script can also create the Site OU. To allow this, the administrator needs the “create OU” right on the new OU’s parent OU. However, as noted, Citrix does not recommend this.)

Later, to add or remove a Controller from the Site, the Citrix administrator must have rights to add/remove a machine from the security group, and create/delete an SCP.

During normal operations, Controllers and VDAs need read rights to all objects in the OU and below. VDAs access the OU as their own machine identity; that machine identity needs at least read rights in the OU to be able to discover Controllers. A Controller also needs the rights to set properties on its own SCP object in the container.

Granting the Citrix administrator full rights to the child OUs will permit all these actions. However, if your deployment has stricter security requirements (such as restricting who can use the script for which action), you can use the Delegation of Control wizard to set specific rights. The following example procedure grants rights to create the Site.

1. Create an OU to contain the child objects (Service Connection Point (SCP), container, and security group).
2. Select the OU, then right-click and select **Delegate Control**.
3. In the Delegation of Control wizard, specify the domain user to delegate control to for the OU.
4. On the **Tasks to Delegate** page, select **Create a custom task to delegate**.
5. On the **Active Directory Object type** page, accept the default **This folder, existing objects in this folder, and creation of new objects in this folder**.
6. On the **Permissions** page, select the **Write** and **Create All Child Objects** check boxes.
7. Finish the wizard to confirm the privileges.

To move a Controller to another Site using OU-based Controller discovery

Follow the directions in [Move a Controller to another Site](#). After you remove the Controller from the old Site (step 2), run the PowerShell script Set-ADControllerDiscovery –sync.

This script synchronizes the OU with the current set of Controllers. After joining the existing Site (step 3), run the same script on any Controller in the new Site.

# 会话管理

May 28, 2016

Maintaining session activity is critical to providing the best user experience. Losing connectivity due to unreliable networks, highly variable network latency, and range limitations of wireless devices can lead to user frustration. Being able to move quickly between workstations and access the same set of applications each time they log on is a priority for many mobile workers such as health-care workers in a hospital.

Use the following features to optimize the reliability of sessions, reduce inconvenience, downtime, and loss of productivity; using these features, mobile users can roam quickly and easily between devices.

- Session reliability
- Auto Client Reconnect
- ICA Keep-Alive
- Workspace control

Session Reliability keeps sessions active and on the user's screen when network connectivity is interrupted. Users continue to see the application they are using until network connectivity resumes.

This feature is especially useful for mobile users with wireless connections. For example, a user with a wireless connection enters a railroad tunnel and momentarily loses connectivity. Ordinarily, the session is disconnected and disappears from the user's screen, and the user has to reconnect to the disconnected session. With Session Reliability, the session remains active on the machine. To indicate that connectivity is lost, the user's display freezes and the cursor changes to a spinning hourglass until connectivity resumes on the other side of the tunnel. The user continues to access the display during the interruption and can resume interacting with the application when the network connection is restored. Session Reliability reconnects users without reauthentication prompts.

Citrix Receiver users cannot override the Controller setting.

You can use Session Reliability with Secure Sockets Layer (SSL). SSL encrypts only the data sent between the user device and NetScaler Gateway.

Enable and configure Session Reliability with the following policy settings:

- The Session reliability connections policy setting allows or prevents session reliability.
- The Session reliability timeout policy setting has a default of 180 seconds, or three minutes. Although you can extend the amount of time Session Reliability keeps a session open, this feature is designed for user convenience and therefore does not prompt the user for reauthentication. As you extend the amount of time a session is kept open, chances increase that a user may get distracted and walk away from the user device, potentially leaving the session accessible to unauthorized users.
- Incoming session reliability connections use port 2598, unless you change the port number in the Session reliability port number policy setting.
- If you do not want users to be able to reconnect to interrupted sessions without having to reauthenticate, use the Auto Client Reconnect feature. You can configure the Auto client reconnect authentication policy setting to prompt users to reauthenticate when reconnecting to interrupted sessions.

If you use both Session Reliability and Auto Client Reconnect, the two features work in sequence. Session Reliability closes, or disconnects, the user session after the amount of time you specify in the Session reliability timeout policy setting. After that, the Auto Client Reconnect policy settings take effect, attempting to reconnect the user to the

disconnected session.

With the Auto Client Reconnect feature, Receiver can detect unintended disconnections of ICA sessions and reconnect users to the affected sessions automatically. When this feature is enabled on the server, users do not have to reconnect manually to continue working.

For application sessions, Receiver attempts to reconnect to the session until there is a successful reconnection or the user cancels the reconnection attempts.

For desktop sessions, Receiver attempts to reconnect to the session for a specified period of time, unless there is a successful reconnection or the user cancels the reconnection attempts. By default, this period of time is five minutes. To change this period of time, edit this registry on the user device:

`HKEYSoftware\Citrix\ICA Client\TransportReconnectRetryMaxTimeSeconds; DWORD;<seconds>`

where <seconds> is the number of seconds after which no more attempts are made to reconnect the session.

Enable and configure Auto Client Reconnect with the following policy settings:

- Auto client reconnect. Enables or disables automatic reconnection by Receiver after a connection has been interrupted.
- Auto client reconnect authentication. Enables or disables the requirement for user authentication after automatic reconnection.
- Auto client reconnect logging. Enables or disables logging of reconnection events in the event log. Logging is disabled by default. When enabled, the server's system log captures information about successful and failed automatic reconnection events. Each server stores information about reconnection events in its own system log; the site does not provide a combined log of reconnection events for all servers.

Auto Client Reconnect incorporates an authentication mechanism based on encrypted user credentials. When a user initially logs on, the server encrypts and stores the user credentials in memory, and creates and sends a cookie containing the encryption key to Receiver. Receiver submits the key to the server for reconnection. The server decrypts the credentials and submits them to Windows logon for authentication. When cookies expire, users must reauthenticate to reconnect to sessions.

Cookies are not used if you enable the Auto client reconnection authentication setting. Instead, users are presented with a dialog box to users requesting credentials when Receiver attempts to reconnect automatically.

For maximum protection of user credentials and sessions, use SSL encryption for all communication between clients and the Site.

Disable Auto Client Reconnect on Citrix Receiver for Windows by using the `icaclient.adm` file. For more information, see the documentation for your Receiver for Windows version.

Settings for connections also affect Auto Client Reconnect:

- By default, Auto Client Reconnect is enabled through policy settings at the Site level, as described above. User reauthentication is not required. However, if a server's ICA TCP connection is configured to reset sessions with a broken communication link, automatic reconnection does not occur. Auto Client Reconnect works only if the server disconnects sessions when there is a broken or timed out connection. In this context, the ICA TCP connection refers to a server's virtual port (rather than an actual network connection) that is used for sessions on TCP/IP networks.
- By default, the ICA TCP connection on a server is set to disconnect sessions with broken or timed out connections. Disconnected sessions remain intact in system memory and are available for reconnection by Receiver.

- The connection can be configured to reset or log off sessions with broken or timed-out connections. When a session is reset, attempting to reconnect initiates a new session; rather than restoring a user to the same place in the application in use, the application is restarted.
- If the server is configured to reset sessions, Auto Client Reconnect creates a new session. This process requires users to enter their credentials to log on to the server.
- Automatic reconnection can fail if Receiver or the plug-in submits incorrect authentication information, which might occur during an attack or the server determines that too much time has elapsed since it detected the broken connection.

Enabling the ICA Keep-Alive feature prevents broken connections from being disconnected. When enabled, if the server detects no activity (for example, no clock change, no mouse movement, no screen updates), this feature prevents Remote Desktop Services from disconnecting that session. The server sends keep-alive packets every few seconds to detect if the session is active. If the session is no longer active, the server marks the session as disconnected.

Note: ICA Keep-Alive works only if you are not using Session Reliability. Session Reliability has its own mechanisms to prevent broken connections from being disconnected. Configure ICA Keep-Alive only for connections that do not use Session Reliability.

ICA Keep-Alive settings override keep-alive settings that are configured in Microsoft Windows Group Policy.

Enable and configure ICA Keep-Alive with the following policy settings:

- ICA keep alive timeout. Specifies the interval (1-3600 seconds) used to send ICA keep-alive messages. Do not configure this option if you want your network monitoring software to close inactive connections in environments where broken connections are so infrequent that allowing users to reconnect to sessions is not a concern. The default interval is 60 seconds: ICA Keep-Alive packets are sent to user devices every 60 seconds. If a user device does not respond in 60 seconds, the status of the ICA sessions changes to disconnected.
- ICA keep alives. Sends or prevents sending ICA keep-alive messages.

Workspace control lets desktops and applications follow a user from one device to another. This ability to roam enables a user to access all desktops or open applications from anywhere simply by logging on, without having to restart the desktops or applications on each device. For example, workspace control can assist health-care workers in a hospital who need to move quickly among different workstations and access the same set of applications each time they log on. If you configure workspace control options to allow it, these workers can disconnect from multiple applications at one client device and then reconnect to open the same applications at a different client device.

Workspace control affects the following activities:

- **Logging on** – By default, workspace control enables users to reconnect automatically to all running desktops and applications when logging on, bypassing the need to reopen them manually. Through workspace control, users can open disconnected desktops or applications, as well as any that are active on another client device. Disconnecting from a desktop or application leaves it running on the server. If you have roaming users who need to keep some desktops or applications running on one client device while they reconnect to a subset of their desktops or applications on another client device, you can configure the logon reconnection behavior to open only the desktops or applications that the user disconnected from previously.
- **Reconnecting** – After logging on to the server, users can reconnect to all of their desktops or applications at any time by clicking **Reconnect**. By default, **Reconnect** opens desktops or applications that are disconnected, plus any that are currently running on another client device. You can configure **Reconnect** to open only those desktops or applications.

that the user disconnected from previously.

- **Logging off** – For users opening desktops or applications through StoreFront, you can configure the Log Off command to log the user off from StoreFront and all active sessions together, or log off from StoreFront only.
- **Disconnecting** – Users can disconnect from all running desktops and applications at once, without needing to disconnect from each individually.

Workspace control is available only for Receiver users who access desktops and applications through a Citrix StoreFront connection. By default, workspace control is disabled for virtual desktop sessions, but is enabled for hosted applications. Session sharing does not occur by default between published desktops and any published applications running inside those desktops.

User policies, client drive mappings, and printer configurations change appropriately when a user moves to a new client device. Policies and mappings are applied according to the client device where the user is currently logged on to the session. For example, if a health care worker logs off from a client device in the emergency room of a hospital and then logs on to a workstation in the hospital's X-ray laboratory, the policies, printer mappings, and client drive mappings appropriate for the session in the X-ray laboratory go into effect at the session startup.

You can customize which printers appear to users when they change locations. You can also control whether users can print to local printers, how much bandwidth is consumed when users connect remotely, and other aspects of their printing experiences.

For information about enabling and configuring workspace control for users, see the StoreFront documentation.

# 在 Studio 中使用搜索

May 28, 2016

Use the Search feature to view information about specific machines, sessions, machine catalogs, applications, or Delivery Groups.

1. Select Search in the Studio navigation pane.

Note: You cannot search within the machine catalogs or Delivery Groups tabs using the Search box. Use the Search node in the navigation pane.

To display additional search criteria in the display, click the plus sign next to the Search drop-down fields. Remove search criteria by clicking the minus button.

2. Enter the name or use the drop-down list to select another search option for the item you want to find.
3. Optionally, save your search by selecting Save as. The search appears in the Saved searches list.

Alternatively, click the Expand Search icon (dual downward angle brackets) to display a drop-down list of search properties; you can perform an advanced search by building an expression from the properties in the drop-down list.

Tips to enhance a search:

- To display additional characteristics to include in the display on which you can search and sort, right click any column and select Select columns.
- To locate a user device connected to a machine, use Client (IP) and Is, and enter the device IP address.
- To locate active sessions, use Session State, Is, and Connected.
- To list all of the machines in a Delivery Group, select Delivery Groups in the navigation pane, then select the group, and then select View Machines in the Actions pane.

# IPv4/IPv6 支持

May 28, 2016

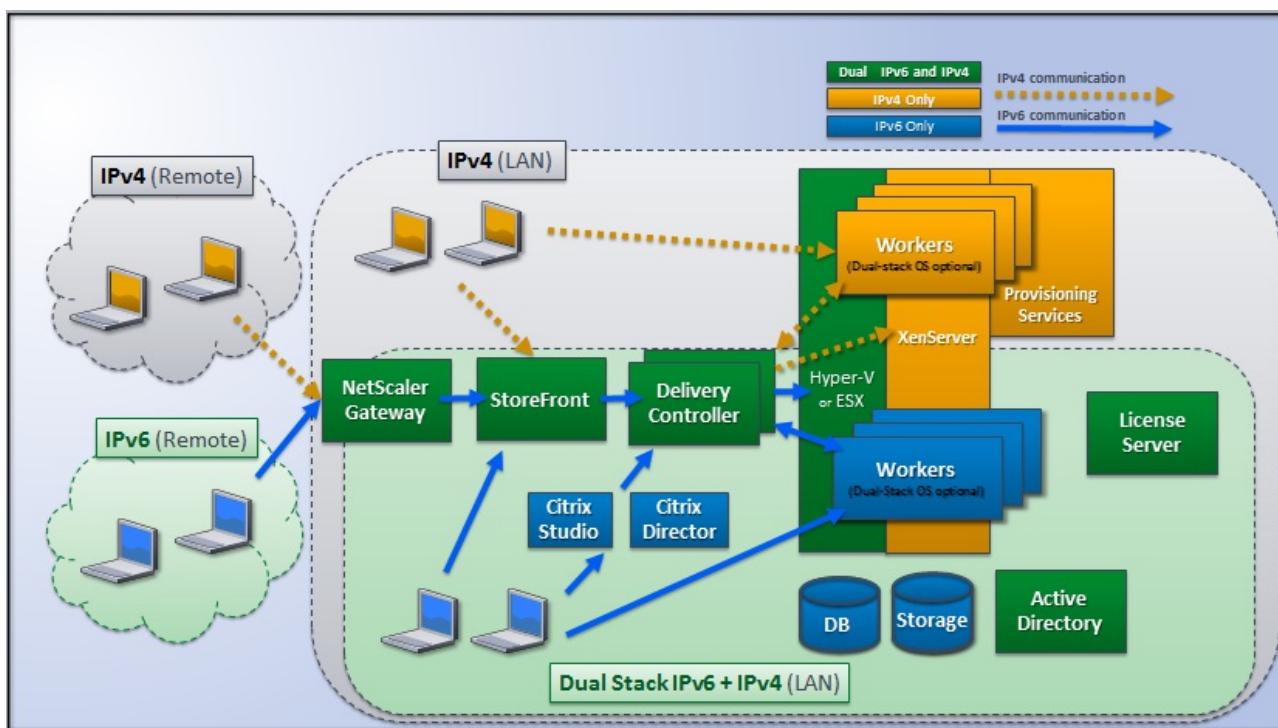
This release supports pure IPv4, pure IPv6, and dual-stack deployments that use overlapping IPv4 and IPv6 networks.

IPv6 communications are controlled with two Virtual Delivery Agent (VDA) connection-related Citrix policy settings:

- A primary setting that enforces the use of IPv6: Only use IPv6 Controller registration.
- A dependent setting that defines an IPv6 netmask: Controller registration IPv6 netmask.

When the Only use IPv6 Controller registration policy setting is enabled, VDAs register with a Delivery Controller for incoming connections using an IPv6 address.

The following figure illustrates a dual-stack IPv4/IPv6 deployment. In this scenario, a worker is a VDA installed on a hypervisor or on a physical system, and is used primarily to enable connections for applications and desktops. Components that support dual IPv6 and IPv4 are running on operating systems that use tunneling or dual protocol software.



These Citrix products, components, and features support only IPv4:

- Provisioning Services
- XenServer Version 6.x
- VDAs not controlled by the Only use IPv6 Controller registration policy setting
- XenApp versions earlier than 7.5, XenDesktop versions earlier than 7, and EdgeSight

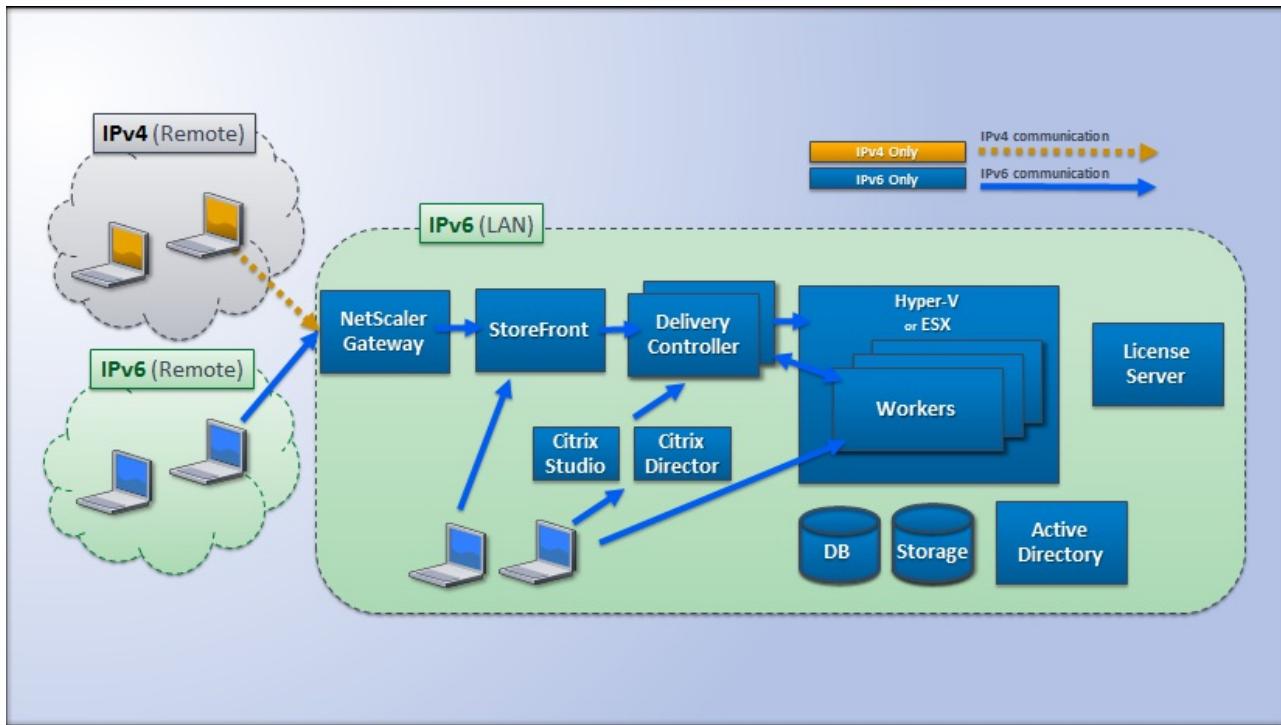
In this deployment:

- If a team frequently uses an IPv6 network and the administrator wants them to use IPv6 traffic, the administrator will publish IPv6 desktops and applications for those users based on a worker image or Organizational Unit (OU) that has the primary IPv6 policy setting turned on (that is, Only use IPv6 Controller registration is enabled).
- If a team frequently uses an IPv4 network, the administrator will publish IPv4 desktops and applications for those users.

based on a worker image or OU that has the primary IPv6 policy setting turned off (that is, Only use IPv6 Controller registration is disabled), which is the default.

The following figure illustrates a pure IPv6 deployment. In this scenario:

- The components are running on operating systems configured to support an IPv6 network.
- The primary Citrix policy setting (Only use IPv6 Controller registration) is enabled for all VDAs; they must register with the Controller using an IPv6 address.



Two Citrix policy settings affect support for a pure IPv6 or dual stack IPv4/IPv6 implementation. Configure the following connection-related policy settings:

- Only use IPv6 Controller registration — Controls which form of address the Virtual Delivery Agent (VDA) uses to register with the Delivery Controller. Default = Disabled
  - When the VDA communicates with the Controller, it uses a single IPv6 address chosen in the following precedence: global IP address, Unique Local Address (ULA), link-local address (only if no other IPv6 addresses are available).
  - When disabled, the VDA registers and communicates with the Controller using the machine's IPv4 address.
- Controller registration IPv6 netmask — A machine can have multiple IPv6 addresses; this policy setting allows administrators to restrict the VDA to only a preferred subnet (rather than a global IP, if one is registered). This setting specifies the network where the VDA will register: the VDA registers only on the first address that matches the specified netmask. This setting is valid only if the Only use IPv6 Controller registration policy setting is enabled. Default = Empty string

**Important:** Use of IPv4 or IPv6 by a VDA is determined solely by these policy settings. In other words, to use IPv6 addressing, the VDA must be controlled by a Citrix policy with the Only use IPv6 Controller registration setting enabled.

If your environment contains both IPv4 and IPv6 networks, you will need separate Delivery Group configurations for the IPv4-only clients and for the clients who can access the IPv6 network. Consider using naming, manual Active Directory

group assignment, or Smart Access filters to differentiate users.

Reconnection to a session may fail if the connection is initiated on an IPv6 network, and then attempts are made to connect again from an internal client that has only IPv4 access.

# 客户端文件夹重定向

May 28, 2016

Client folder redirection changes the way client-side files are accessible on the host-side session. When you enable only client drive mapping on the host-side, client-side full volumes are automatically mapped to the sessions as Universal Naming Convention (UNC) links. When you enable client folder redirection on the host-side and the user configures it on the user device, the portion of the local volume specified by the user is redirected.

Only the user-specified folders appear as UNC links inside sessions instead of the complete file system on the user device. If you disable UNC links through the registry, client folders appear as mapped drives inside the session.

Client folder redirection is supported on Windows Desktop OS machines only.

Client folder redirection for an external USB drive will not be saved on detaching and reattaching the device.

Enable client folder direction on the host-side. Then, on the client device, specify which folders to redirect (the application you use to specify the client folder options is included with the Citrix Receiver supplied with this release).

Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

1. On the host-side:

1. Create a key: HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\Client Folder Redirection.
2. Create a REG\_DWORD value.
  - Name: CFROnlyModeAvailable
  - Type: REG\_DWORD
  - Data: Set to 1

2. On the user device:

1. Ensure the latest version of Receiver is installed.
2. From the Receiver installation directory, start CtxCFRUI.exe.
3. Select the Custom radio button and add, edit, or remove folders.
4. Disconnect and reconnect your sessions for the setting to take effect.

# Personal vDisk 7.x

Jun 21, 2016

The personal vDisk feature retains the single image management of pooled and streamed desktops while allowing users to install applications and change their desktop settings. Unlike traditional Virtual Desktop Infrastructure (VDI) deployments involving pooled desktops, where users lose their customization and personal applications when the administrator changes the master image, deployments using personal vDisks retain those changes. This means administrators can easily and centrally manage their master images while providing users with a customized and personalized desktop experience.

Personal vDisks provide this separation by redirecting all changes made on the user's VM to a separate disk (the personal vDisk), which is attached to the user's VM. The content of the personal vDisk is blended at runtime with the content from the master image to provide a unified experience. In this way, users can still access applications provisioned by their administrator in the master image.

Personal vDisks have two parts, which use different drive letters and are by default equally sized:

- User profile - This contains user data, documents, and the user profile. By default this uses drive P; but you can choose a different drive letter when you create a catalog with machines using personal vDisks. The drive used also depends on the EnableUserProfileRedirection setting.
- Virtual Hard Disk (.vhd) file - This contains all other items, for example applications installed in C:\Program Files. This part is not displayed in Windows Explorer and, since Version 5.6.7, does not require a drive letter.

Personal vDisks support the provisioning of department-level applications, as well as applications downloaded and installed by users, including those that require drivers (except phase 1 drivers), databases, and machine management software. If a user's change conflicts with an administrator's change, the personal vDisk provides a simple and automatic way to reconcile the changes.

In addition, locally administered applications (such as those provisioned and managed by local IT departments) can also be provisioned into the user's environment. The user experiences no difference in usability; personal vDisks ensure all changes made and all applications installed are stored on the vDisk. Where an application on a personal vDisk exactly matches one on a master image, the copy on the personal vDisk is discarded to save space without the user losing access to the application.

Physically, you store personal vDisks on the hypervisor but they do not have to be in the same location as other disks attached to the virtual desktop. This can lower the cost of personal vDisk storage.

During Site creation, when you create a connection, you define storage locations for disks that are used by VMs. You can separate the Personal vDisks from the disks used by the operating system. Each VM must have access to a storage location for both disks. If you use local storage for both, they must be accessible from the same hypervisor. To ensure this requirement is met, Studio offers only compatible storage locations. Later, you can also add personal vDisks and storage for them to existing hosts (but not machine catalogs) from Configuration > Hosting in Studio.

Back up personal vDisks regularly using any preferred method. The vDisks are standard volumes in a hypervisor's storage tier, so you can back them up, just like any other volume.

The following improvements are included in this release:

- This version of personal vDisk contains performance improvements that reduce the amount of time it takes to apply an

image update to a personal vDisk catalog.

The following known issues are fixed in this release:

- Attempting an in-place upgrade of a base virtual machine from Microsoft Office 2010 to Microsoft Office 2013 resulted in the user seeing a reconfiguration window followed by an error message; "Error 25004. The product key you entered cannot be used on this machine." In the past, it was recommended that Office 2010 be uninstalled in the base virtual machine before installing Office 2013. Now, it is no longer necessary to uninstall Office 2010 when performing an in-place upgrade to the base virtual machine (#391225).
- During the image update process, if a higher version of Microsoft .Net exists on the users personal vDisk, it was overwritten by a lower version from the base image. This caused issues for users running certain applications installed on their personal vDisk which required the higher version, such as Visual Studio (#439009).
- A Provisioning Services imaged disk with personal vDisk install and enabled, cannot be used to create a non-personal vdisk machine catalog. This restriction has been removed (#485189).

New in version 7.6:

- Improved personal vDisk error handling and reporting. In Studio, when you display PvD-enabled machines in a catalog, a "PvD" tab provides monitoring status during image updates, plus estimated completion time and progress. Enhanced state displays are also provided.
- A personal vDisk Image Update Monitoring Tool for earlier releases is available from the ISO media (ISO\Support\Tools\Scripts\PvdTool). Monitoring capabilities are supported for previous releases, however the reporting capabilities will not be as robust compared to the current release.
- Provisioning Services test mode allows you to boot machines with an updated image in a test catalog. After you verify its stability, you can promote the test version of the personal vDisk to production.
- A new feature enables you to calculate the delta between two inventories during an inventory, instead of calculating it for each PvD desktop. New commands are provided to export and import a previous inventory for MCS catalogs. (Provisioning Services master vDisks already have the previous inventory.)

Known issues from 7.1.3 fixed in version 7.6:

- Interrupting a personal vDisk installation upgrade can result in corrupting an existing personal vDisk installation. [#424878]
- A virtual desktop may become unresponsive if the personal vDisk runs for an extended period of time and a non-page memory leak occurs. [#473170]

New known issues in version 7.6:

- The presence of antivirus products can affect how long it takes to run the inventory or perform an update. Performance can improve if you add CtxPvD.exe and CtxPvDSvc.exe to the PROCESS exclusion list of your antivirus product. These files are located in C:\Program Files\Citrix\personal vDisk\bin. [#326735]
- Hard links between files inherited from the master image are not preserved in personal vDisk catalogs. [#368678]
- After upgrading from Office 2010 to 2013 on the Personal vDisk master image, Office might fail to launch on virtual machines because the Office KMS licensing product key was removed during the upgrade. As a workaround, uninstall Office 2010 and reinstall Office 2013 on the master image. [#391225]
- Personal vDisk catalogs do not support VMware Paravirtual SCSI (PVSCSI) controllers. To prevent this issue, use the default controller. [#394039]
- For virtual desktops that were created with Personal vDisk version 5.6.0 and are upgraded to 7, users who logged on to the master virtual machine (VM) previously might not find all their files in their pooled VM. This issue occurs because a new user profile is created when they log on to their pooled VM. There is no workaround for this issue. [#392459]

- Personal vDisks running Windows 7 cannot use the Backup and Restore feature when the Windows system protection feature is enabled. If system protection is disabled, the user profile is backed up, but the userdata.v2.vhd file is not. Citrix recommends disabling system protection and using Backup and Restore to back up the user profile. [#360582]
- When you create a VHD file on the base VM using the Disk Management tool, you might be unable to mount the VHD. As a workaround, copy the VHD to the Pvd volume. [#355576]
- Office 2010 shortcuts remain on virtual desktops after this software is removed. To work around this issue, delete the shortcuts. [#402889]
- When using Microsoft Hyper-V, you cannot create a catalog of machines with personal vDisks when the machines are stored locally and the vDisks are stored on Cluster Shared Volumes (CSVs); catalog creation fails with an error. To work around this issue, use an alternative storage setup for the vDisks. [#423969]
- When you log on for the first time to a virtual desktop that is created from a Provisioning Services catalog, the desktop prompts for a restart if the personal vDisk has been reset (using the command ctvpd.exe -s reset). To work around this issue, restart the desktop as prompted. This is a once-only reset that is not required when you log on again. [#340186]
- If you install .NET 4.5 on a personal vDisk and a later image update installs or modifies .NET 4.0, applications that are dependent on .NET 4.5 fail. To work around this issue, distribute .NET 4.5 from the base image as an image update.”
- See also the
  - *Known Issues*
 documentation for the XenApp and XenDesktop 7.6 release.

Known issues from 7.1.1 fixed in version 7.1.3:

- Direct upgrades from personal vDisk 5.6.0 to personal vDisk 7.x may cause the personal vDisk to fail. [#432992]
- Users might only be able to connect intermittently to virtual desktops with personal vDisks. [#437203]
- If a personal vDisk image update operation is interrupted while personal vDisk 5.6.5 or later is upgraded to personal vDisk 7.0 or later, subsequent update operations can fail. [#436145]

Known issues from 7.1 fixed in version 7.1.1:

- Upgrading to Symantec Endpoint Protection 12.1.3 through an image update causes symhelp.exe to report corrupt antivirus definitions. [#423429]
- Personal vDisk can cause pooled desktops to restart if Service Control Manager (services.exe) crashes. [#0365351]

New known issues in version 7.1.1: none

New in version 7.1:

- You can now use Personal vDisk with desktops running Windows 8.1, and event logging has been improved.
- Copy-on-Write (CoW) is no longer supported in this release. When upgrading from Version 7.0 to 7.1 of Personal vDisk, all changes to data managed by CoW are lost. This was an experimental feature in XenDesktop 7 and was disabled by default, so if you did not enable it, you are not affected.

Known issues from 7.0.1 fixed in version 7.1:

- If the value of the Personal vDisk registry key EnableProfileRedirection is set to 1 or ON, and later, while updating the image, you change it to 0 or OFF, the entire Personal vDisk space might get allocated to user-installed applications, leaving no space for user profiles, which remain on the vDisk. If this profile redirection is disabled for a catalog and you enable it during an image update, users might not be able to log on to their virtual desktop. [#381921]
- The Desktop Service does not log the correct error in the Event Viewer when a Personal vDisk inventory update fails.

[#383331]

- When upgrading to Personal vDisk 7.x, modified rules are not preserved. This issue has been fixed for upgrades from Version 7.0 to Version 7.1. When upgrading from Version 5.6.5 to Version 7.1, you must first save the rule file and then apply the rules again after the upgrade. [#388664]
- Personal vDisks running Windows 8 cannot install applications from the Windows Store. An error message stating, "Your purchase couldn't be completed," appears. Enabling the Windows Update Service does not resolve this issue, which has now been fixed. However, user-installed applications must be reinstalled after the system restarts. [#361513]
- Some symbolic links are missing in Windows 7 pooled desktops with personal vDisks. As a result, applications that store icons in C:\Users\All Users do not display these icons in the Start menu. [#418710]
- A personal vDisk does not start if an Update Sequence Number (USN) journal overflow occurs due to a large number of changes made to the system after an inventory update. [#369846]
- A personal vDisk does not start with status code 0x20 and error code 0x20000028. [#393627]
- Symantec Endpoint Protection 12.1.3 displays the message "Proactive Threat Protection is malfunctioning" and this component's Live Update Status is not available. [#390204]

New known issues in version 7.1: See the

— *Known Issues*

documentation for the XenDesktop 7.1 release.

New in version 7.0.1: Personal vDisk is now more robust to environment changes. Virtual desktops with personal vDisks now register with the Delivery Controller even if image updates fail, and unsafe system shutdowns no longer put the vDisks into a permanently disabled state. In addition, using rules files you can now exclude files and folders from the vDisks during a deployment.

Known issues from 5.6.13 fixed in version 7.0.1:

- Changes to a group's membership made by users on a pooled virtual desktop might be lost after an image update. [#286227]
- Image updates might fail with a low disk space error even if the personal vDisk has enough space. [#325125]
- Some applications fail to install on virtual desktops with a personal vDisk, and a message is displayed that a restart is required. This is due to a pending rename operation. [#351520]
- Symbolic links created inside the master image do not work on virtual desktops with personal vDisks. [#352585]
- In environments that use Citrix Profile management and personal vDisk, applications that examine user profiles on a system volume might not function properly if profile redirection is enabled. [#353661]
- The inventory update process fails on master images when the inventory is bigger than 2GB. [#359768]
- Image updates fail with error code 112 and personal vDisks are corrupted even if the vDisks have enough free space for the update. [#363003]
- The resizing script fails for catalogs with more than 250 desktops. [#363365]
- Changes made by users to an environment variable are lost when an image update is performed. [#372295]
- Local users created on a virtual desktop with a personal vDisk are lost when an image update is performed. [#377964]
- A personal vDisk may fail to start if an Update Sequence Number (USN) journal overflow occurred due to a large number of changes made to the system after an inventory update. To avoid this, increase the USN journal size to a minimum of 32 MB in the master image and perform an image update. [#369846]
- An issue has been identified with Personal vDisk that prevents the correct functioning of AppSense Environment Manager registry hiving actions when AppSense is used in Replace Mode. Citrix and AppSense are working together to resolve the issue, which is related to the behavior of the RegRestoreKey API when Personal vDisk is installed. [#0353936]

- When an application installed on a personal vDisk (PvD) is related to another application of the same version that is installed on the master image, the application on the PvD could stop working after an image update. This occurs if you uninstall the application from the master image or upgrade it to a later version, because that action removes the files needed by the application on the PvD from the master image. To prevent this, keep the application containing the files needed by the application on the PvD on the master image.

For example, the master image contains Office 2007, and a user installs Visio 2007 on the PvD; the Office applications and Visio work correctly. Later, the administrator replaces Office 2007 with Office 2010 on the master image, and then updates all affected machines with the updated image. Visio 2007 no longer works. To avoid this, keep Office 2007 in the master image. [#320915]

- When deploying McAfee Virus Scan Enterprise (VSE), use version 8.8 Patch 4 or later on a master image if you use personal vDisk. [#303472]
- If a shortcut created to a file in the master image stops working (because the shortcut target is renamed within PvD), recreate the shortcut. [#367602]
- Do not use absolute/hard links in a master image. [#368678]
- The Windows 7 backup and restore feature is not supported on the personal vDisk. [#360582]
- After an updated master image is applied, the local user and group console becomes inaccessible or shows inconsistent data. To resolve the issue, reset the user accounts on the VM, which requires resetting the security hive. This issue was fixed in the 7.1.2 release (and works for VMs created in later releases), but the fix does not work for VMs that were created with an earlier version and then upgraded. [#488044]
- When using a pooled VM in an ESX hypervisor environment, users see a restart prompt if the selected SCSI controller type is "VMware Paravirtual." For a workaround, use an LSI SCSI controller type. [#394039]
- After a PvD reset on a desktop created through Provisioning Services, users may receive a restart prompt after logging on to the VM. As a workaround, restart the desktop. [#340186]
- Windows 8.1 desktop users might be unable to log on to their PvD. An administrator might see message "PvD was disabled due to unsafe shutdown" and the PvDActivation log might contain the message "Failed to load reg hive [\Device\lvmVhdDisk00000001\CitrixPvD\Settings\RingCube.dat]." This occurs when a user's VM shuts down unsafely. As a workaround, reset the personal vDisk. [#474071]

# 安装和升级

Aug 02, 2016

Personal vDisk 7.x is supported on XenDesktop version 5.6 through the current version. The "System requirements" documentation for each XenDesktop version lists the supported operating systems for Virtual Delivery Agents (VDAs), and the supported versions of hosts (virtualization resources), and Provisioning Services. For details about Provisioning Services tasks, see the Provisioning Services documentation.

PvD is installed automatically when you install or upgrade a VDA for Desktop OS on a machine. If you update the PvD software after installing the VDA, use the PvD MSI provided [here](#) (Citrix account credentials required).

Enabling PvD:

- If you are using Machine Creation Services (MCS), PvD is enabled automatically when you create a machine catalog of desktop OS machines that will use a personal vDisk.
- If you are using Provisioning Services (PVS), PvD is enabled automatically when you run the inventory during the master (base) image creation process, or when auto-update runs the inventory for you.

VDA installation offers options to enable PvD (by selecting the “Personal vDisk” checkbox in the graphical interface or by specifying the /baseimage option in the command line interface). However, omitting this action during the VDA install (which is the default) still allows you to use the same image to create both PvD desktops and non-PvD desktops, because PvD is enabled during the catalog creation process.

You add personal vDisks to hosts when you configure a Site. You can choose to use the same storage on the host for VMs and personal vDisks, or you can use different storage for personal vDisks.

Later, you can also add personal vDisks and their storage to existing hosts (connections), but not machine catalogs.

1. Select Configuration > Hosting in the Studio navigation pane.
2. Select Add Personal vDisk storage in the Actions pane, and specify the storage location.

The easiest way to upgrade personal vDisk from an earlier 7.x version is to simply upgrade your desktop OS VDAs to the version provided with the most recent XenDesktop version. Then, run the PvD inventory.

You can also upgrade just PvD using the PvD MSI from [here](#).

You can use one of two ways to remove the PvD software:

- Uninstall the VDA; this removes the PvD software as well.
- If you updated PvD using the PvD MSI, then you can uninstall it from the Programs list.

If you uninstall PvD and then want to reinstall the same or a newer version, first back up the registry key HKLM\Software\Citrix\personal vDisk\config, which contains environment configuration settings that might have changed. Then, after installing PvD, reset the registry values that might have changed, by comparing them with the backed-up version.

# 配置与管理

May 28, 2016

This topic covers items you should consider when configuring and managing a personal vDisk (PvD) environment. It also covers best practice guidelines and task descriptions.

For procedures that include working in the Windows registry:

Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

The following factors affect the size of the main personal vDisk volume:

- **Size of the applications that users will install on their PvDs**

At restarts, PvD determines the free space remaining in the application area (UserData.v2.vhd). If this falls below 10%, the application area is expanded into any unused profile area space (by default, the space available on the P: drive). The space added to the application area is approximately 50% of the combined free space remaining in both the application area and the profile area.

For example, if the application area on a 10 GB PvD (which by default is 5 GB) reaches 4.7 GB and the profile area has 3 GB free, the increased space that is added to the application area is calculated as follows:

$$\text{increased space} = (5.0 - 4.7)/2 + 3.0/2 = 1.65 \text{ GB}$$

The space added to the application area is only approximate because a small allowance is made for storing logs and for overhead. The calculation and the possible resizing is performed on each restart.

- **Size of users' profiles (if a separate profile management solution is not used)**

In addition to the space required for applications, ensure there is sufficient space available on personal vDisks to store users' profiles. Include any non-redirected special folders (such as My Documents and My Music) when calculating space requirements. Existing profile sizes are available from the Control Panel (sysdm.cpl).

Some profile redirection solutions store stub files (sentinel files) instead of real profile data. These profile solutions might appear to store no data initially but actually consume one file directory entry in the file system per stub file; generally, approximately 4 KB per file. If you use such a solution, estimate the size based on the real profile data, not the stub files.

Enterprise file sharing applications (such as ShareFile and Dropbox) might synchronize or download data to users' profile areas on the personal vDisks. If you use such applications, include enough space in your sizing estimates for this data.

- **Overhead consumed by the template VHD containing the PvD inventory**

The template VHD contains the PvD inventory data (sentinel files corresponding to the master image content). The PvD application area is created from this VHD. Because each sentinel file or folder comprises a file directory entry in the file system, the template VHD content consumes PvD application space even before any applications are installed by the end user. You can determine the template VHD size by browsing the master image after an inventory is taken.

Alternatively, use the following equation for an approximate calculation:

$$\text{template VHD size} = (\text{number of files on base image}) \times 4 \text{ KB}$$

Determine the number of files and folders by right-clicking the C: drive on the base VM image and selecting Properties.

For example, an image with 250,000 files results in a template VHD of approximately 1,024,000,000 bytes (just under 1 GB). This space will be unavailable for application installations in the PvD application area.

- **Overhead for PvD image update operations**

During PvD image update operations, enough space must be available at the root of the PvD (by default, P:) to merge the changes from the two image versions and the changes the user has made to their PvD. Typically, PVD reserves a few hundred megabytes for this purpose, but extra data that was written to the P: drive might consume this reserved space, leaving insufficient for the image update to complete successfully. The PvD pool statistics script (located on the XenDesktop installation media in the Support/Tools/Scripts folder) or the PvD Image Update Monitoring Tool (in the Support/Tools/Scripts\PvdTool folder) can help identify any PvD disks in a catalog that are undergoing an update and that are nearly full.

The presence of antivirus products can affect how long it takes to run the inventory or perform an update. Performance can improve if you add CtxPvD.exe and CtxPvDSvc.exe to the exclusion list of your antivirus product. These files are located in C:\Program Files\Citrix\personal vDisk\bin. Excluding these executables from scanning by the antivirus software can improve inventory and image update performance by up to a factor of ten.

- **Overhead for unexpected growth (unexpected application installations, and so on)**

Consider allowing extra (either a fixed amount or a percentage of the vDisk size) to the total size to accommodate unexpected application installations that the user performs during deployment.

You can manually adjust the automatic resizing algorithm that determines the size of the VHD relative to the P: drive, by setting the initial size of the VHD. This can be useful if, for example, you know users will install a number of applications that are too big to fit on the VHD even after it is resized by the algorithm. In this case, you can increase the initial size of the application space to accommodate the user-installed applications.

Preferably, adjust the initial size of the VHD on a master image. Alternatively, you can adjust the size of the VHD on a virtual desktop when a user does not have sufficient space to install an application. However, you must repeat that operation on each affected virtual desktop; you cannot adjust the VHD initial size in a catalog that is already created.

Ensure the VHD is big enough to store antivirus definition files, which are typically large.

Locate and set the following registry keys in HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\personal vDisk\Config. (Do not modify other settings in this registry key.) All settings must be specified on the master image (except for MinimumVHDSIZEInMB, which can be changed on an individual machine); settings specified on the master image are applied during the next image update.

- **MinimumVHDSIZEMB**

Specifies the minimum size (in megabytes) of the application part (C:) of the personal vDisk. The new size must be greater than the existing size but less than the size of the disk minus PvDReservedSpaceMB.

Increasing this value allocates free space from the profile part on the vDisk to C:. This setting is ignored if a lower value than the current size of the C: drive is used, or if EnableDynamicResizeOfAppContainer is set to 0.

Default = 2048

- **EnableDynamicResizeOfAppContainer**

Enables or disables the dynamic resizing algorithm.

- When set to 1, the application space (on C:) is resized automatically when the free space on C: falls below 10%.

Allowed values are 1 and 0. A restart is required to effect the resize.

- When set to 0, the VHD size is determined according to the method used in XenDesktop versions earlier than 7.x  
Default = 1

- **EnableUserProfileRedirection**

Enables or disables redirecting the user's profile to the vDisk.

- When set to 1, PvD redirects users' profiles to the personal vDisk drive (P: by default). Profiles are generally redirected to P:\Users, corresponding to a standard Windows profile. This redirection preserves the profiles in case the PvD desktop must be reset.
- When set to 0, all of the space on the vDisk minus PvDReservedSpaceMB is allocated to C; the application part of the vDisk, and the vDisk drive (P:) is hidden in Windows Explorer. Citrix recommends disabling redirection by setting the value to 0, when using Citrix Profile management or another roaming profile solution.

This setting retains the profiles in C:\Users instead of redirecting them to the vDisk, and lets the roaming profile solution handle the profiles.

This value ensures that all of the space on P: is allocated to applications.

It is assumed that if this value is set to 0, a profile management solution is in place. Disabling profile redirection without a roaming profile solution in place is not recommended because subsequent PvD reset operations result in the profiles being deleted.

Do not change this setting when the image is updated because it does not change the location of existing profiles, but it will allocate all the space on the Personal vDisk to C: and hide the PvD.

Configure this value before deploying a catalog. You cannot change it after the catalog is deployed.

Important: Beginning with XenDesktop 7.1, changes to this value are not honored when you perform an image update. Set the key's value when you first create the catalogs from which the profiles will originate. You cannot modify the redirection behavior later.

Default = 1

- **PercentOfPvDForApps**

Sets the split between the application part (C:) and the profile part of the vDisk. This value is used when creating new VMs, and during image updates when EnableDynamicResizeOfAppContainer is set to 0.

Changing PercentOfPvDForApps makes a difference only when EnableDynamicResizeOfAppContainer is set to 0. By default, EnableDynamicResizeOfAppContainer is set to 1 (enabled), which means is that the AppContainer (which you see as the C drive) only expands when it is close to being full (that is, dynamic) - when less than 10% free space remains.

Increasing PercentOfPvDForApps only increases the maximum space for which the Apps portion is allowed to expand. It does not provision that space for you immediately. You must also configure the split allocation in the master image, where it will be applied during the next image update.

If you have already generated a catalog of machines with EnableDynamicResizeOfAppContainer set to 1, then change that setting to 0 in the master image for the next update, and configure an appropriate allocation split. The requested split size will be honored as long as it is larger than the current allocated size for the C drive.

If you want to maintain complete control over the space split, set this value to 0. This allows full control over the C drive size, and does not rely on a user consuming space below the threshold to expand the drive.

Default = 50% (allocates equal space to both parts)

- **PvDReservedSpaceMB**

Specifies the size of the reserved space (in megabytes) on the vDisk for storing Personal vDisk logs and other data.

If your deployment includes XenApp 6.5 (or an earlier version) and uses application streaming, increase this value by the size of the Rade Cache.

Default = 512

- **PvDResetUserGroup**

Valid only for XenDesktop 5.6 - Allows the specified group of users to reset a Personal vDisk. Later XenDesktop releases use Delegated Administration for this.

Other settings:

- **Windows Update Service** - Ensure that you set Windows updates to Never Check for Update and the Windows update service to Disabled in the master image. In the event Windows Update Service needs to run on the PvD, setting it to Never Check for Update helps prevent the updates from being installed on the associated machines. Windows 8 Store needs this service to run to install any Modern-style application.
- **Windows updates** - These include Internet Explorer updates and must be applied on the master image.
- **Updates requiring restarts** - Windows updates applied to the master image might require multiple restarts to fully install, depending on the type of patches delivered in those updates. Ensure you restart the master image properly to fully complete the installation of any Windows updates applied to it before taking the PvD inventory.
- **Application updates** - Update applications installed on the master image to conserve space on users' vDisks. This also avoids the duplicate effort of updating the applications on each user's vDisk.

Some software might conflict with the way that PvD composites the user's environment, so you must install it on the master image (rather than on the individual machine) to avoid these conflicts. In addition, although some other software might not conflict with the operation of PvD, Citrix recommends installing it on the master image.

Applications that must be installed on the master image:

- Agents and clients (for example, System Center Configuration Manager Agent, App-V client, Citrix Receiver)
- Applications that install or modify early-boot drivers
- Applications that install printer or scanner software or drivers
- Applications that modify the Windows network stack
- VM tools such as VMware Tools and XenServer Tools

Applications that should be installed on the master image:

- Applications that are distributed to a large number of users. In each case, turn off application updates before deployment:
  - Enterprise applications using volume licensing, such as Microsoft Office, Microsoft SQL Server
  - Common applications, such as Adobe Reader, Firefox, and Chrome
- Large applications such as SQL Server, Visual Studio, and application frameworks such as .NET

The following recommendations and restrictions apply to applications installed by users on machines with personal vDisks.

Some of these cannot be enforced if users have administrative privileges:

- Users should not uninstall an application from the master image and reinstall the same application on their personal vDisk.
- Take care when updating or uninstalling applications on the master image. After you install a version of an application on

the image, a user might install an add-on application (for example, a plug-in) that requires this version. If such a dependency exists, updating or uninstalling the application on the image might make the add-on malfunction. For example, with Microsoft Office 2010 installed on a master image, a user installs Visio 2010 on their personal vDisk. A later upgrade of Office on the master image might make the locally-installed Visio unusable.

- Software with hardware-dependent licenses (either through a dongle or signature-based hardware) is unsupported.

When using Provisioning Services with PvD:

- The Soap Service account must be added to the Administrator node of Studio and must have the Machine Administrator or higher role. This ensures that the PvD desktops are put into the Preparing state when the Provisioning Services (PVS) vDisk is promoted to production.
- The Provisioning Service versioning feature must be used to update the personal vDisk. When the version is promoted to production, the Soap Service puts the PvD desktops into the Preparing state.
- The personal vDisk size should always be larger than the Provisioning Services write cache disk (otherwise, Provisioning Services might erroneously select the personal vDisk for use as its write cache).
- After you create a Delivery Group, you can monitor the personal vDisk using the [PvD Image Update Monitoring Tool](#) or the [Resize and poolstats scripts](#) (personal-vdisk-poolstats.ps1).

Size the write cache disk correctly. During normal operation, PvD captures most user writes (changes) and redirects them to the personal vDisk. This implies that you can reduce the size of the Provisioning Services write cache disk. However, when PvD is not active (such as during image update operations), a small Provisioning Services write cache disk can fill up, resulting in machine crashes.

Citrix recommends that you size Provisioning Services write cache disks according to Provisioning Services best practice and add space equal to twice the size of the template VHD on the master image (to accommodate merge requirements). It is extremely unlikely that a merge operation will require all of this space, but it is possible.

When using Provisioning Services to deploy a catalog with PvD-enabled machines:

- Follow the guidance in the Provisioning Services documentation.
- You can change the power action throttling settings by editing the connection in Studio; see below.
- If you update the Provisioning Services vDisk, after you install/update applications and other software and restart the vDisk, run the PvD inventory and then shut down the VM. Then, promote the new version to Production. The PvD desktops in the catalog should automatically enter the Preparing state. If they do not, check that the Soap Service account has machine administrator or higher privileges on the Controller.

The Provisioning Services test mode feature enables you to create a test catalog containing machines using an updated master image. If tests confirm the test catalog's viability, you can promote it to production.

When using Machine Creation Services (MCS) to deploy a catalog with PvD-enabled machines:

- Follow the guidance in the XenDesktop documentation.
- Run a PvD inventory after you create the master image and then power off the VM (PvD will not function correctly if you do not power off the VM). Then, take a snapshot of the master image.
- In the Create Machine Catalog wizard, specify the personal vDisk size and drive letter.
- After you create a Delivery Group, you can monitor the personal vDisk using the [PvD Image Update Monitoring Tool](#) or the [Resize and poolstats scripts](#) (personal-vdisk-poolstats.ps1).
- You can change the power action throttling settings by editing the connection in Studio; see below.

- If you update the master image, run the PvD inventory after you update the applications and other software on the image, and then power off the VM. Then, take a snapshot of the master image.
- Use the PvD Image Update Monitoring Tool or the personal-vdisk-poolstats.ps1 script to validate that there is sufficient space on each PvD-enabled VM that will use the updated master image.
- After you update the machine catalog, the PvD desktops enter the Preparing state as they individually process the changes in the new master image. The desktops are updated according to the rollout strategy specified during the machine update.
- Use the PvD Image Update Monitoring Tool or the personal-vdisk-poolstats.ps1 script to monitor the PvD in the Preparing state.

Use the rules files to exclude files and folders from the vDisks. You can do this when the personal vDisks are in deployment. The rules files are named custom\_\*\_rules.template.txt and are located in the \config folder. Comments in each file provide additional documentation.

When you enable PvD and after any update to the master image after installation, it is important to refresh the disk's inventory (called "run the inventory") and create a new snapshot.

Because administrators, not users, manage master images, if you install an application that places binary files in the administrator's user profile, the application is not available to users of shared virtual desktops (including those based on pooled machine catalogs and pooled with PvD machine catalogs). Users must install such applications themselves.

It is best practice to take a snapshot of the image after each step in this procedure.

1. Update the master image by installing any applications or operating system updates, and performing any system configuration on the machine.

For master images based on Windows XP that you plan to deploy with Personal vDisks, check that no dialog boxes are open (for example, messages confirming software installations or prompts to use unsigned drivers). Open dialog boxes on master images in this environment prevent the VDA from registering with the Delivery Controller. You can prevent prompts for unsigned drivers using the Control Panel. For example, navigate to System > Hardware > Driver Signing, and select the option to ignore warnings.

2. Shut down the machine. For Windows 7 machines, click Cancel when Citrix Personal vDisk blocks the shutdown.
3. In the Citrix Personal vDisk dialog box, click Update Inventory. This step may take several minutes to complete.  
Important: If you interrupt the following shutdown (even to make a minor update to the image), the Personal vDisk's inventory no longer matches the master image. This causes the Personal vDisk feature to stop working. If you interrupt the shutdown, you must restart the machine, shut it down, and when prompted click Update Inventory again.
4. When the inventory operation shuts down the machine, take a snapshot of the master image.

You can export an inventory to a network share and then import that inventory to a master image. For details, see [Export and import a PvD inventory](#).

The Citrix Broker Service controls the power state of the machines that provide desktops and applications. The Broker Service can control several hypervisors through a Delivery Controller. Broker power actions control the interaction between a Controller and the hypervisor. To avoid overloading the hypervisor, actions that change a machine's power state are assigned a priority and sent to the hypervisor using a throttling mechanism. The following settings affect the throttling. You

specify these values by editing a connection (Advanced page) in Studio.

To configure connection throttling values:

1. Select Configuration > Hosting in the Studio navigation pane.
2. Select the connection and then select Edit Connection in the Actions pane.
3. You can change the following values:

- **Simultaneous actions (all types)** - The maximum number of simultaneous in-progress power actions allowed. This setting is specified as both an absolute value and as a percentage of the connection to the hypervisor. The lower of the two values is used.

Default = 100 absolute, 20%

- **Simultaneous Personal vDisk inventory updates** - The maximum number of simultaneous Personal vDisk power actions allowed. This setting is specified as both an absolute value and a percentage of the connection. The lower of the two values is used.

Default = 50 absolute, 25%

To calculate the absolute value: determine the total IOPS (TIOPS) supported by the end-user storage (this should be specified by the manufacturer or calculated). Using 350 IOPS per VM (IOPS/VM), determine the number of VMs that should be active at any given time on the storage. Calculate this value by dividing total IOPS by IOPS/VM.

For example, if the end-user storage is 14000 IOPS, the number of active VMs is  $14000 \text{ IOPS} / 350 \text{ IOPS/VM} = 40$ .

- **Maximum new actions per minute** - The maximum number of new power actions that can be sent to the hypervisor per minute. Specified as an absolute value.

Default = 10

To help identify optimal values for these settings in your deployment:

1. Using the default values, measure the total response time for an image update of a test catalog. This is the difference between the start of an image update (T1) and when the VDA on the last machine in the catalog registers with the Controller (T2). Total response time = T2 - T1.
2. Measure the input/output operations per second (IOPS) of the hypervisor storage during the image update. This data can serve as a benchmark for optimization. (The default values may be the best setting; alternatively, the system might max out of IOPS, which will require lowering the setting values.)
3. Change the “Simultaneous Personal vDisk inventory updates” value as described below (keeping all other settings unchanged).
  1. Increase the value by 10 and measure the total response time after each change. Continue to increase the value by 10 and test the result, until deterioration or no change in the total response time occurs.
  2. If the previous step resulted in no improvement by increasing the value, decrease the value in increments of 10 and measure the total response time after each decrease. Repeat this process until the total response time remains unchanged or does not improve further. This is likely the optimal PvD power action value.
4. After obtaining the PvD power action setting value, tweak the simultaneous actions (all types) and maximum new actions per minute values, one at a time. Follow the procedure described above (increasing or decreasing in increments) to test different values.

System Center Configuration Manager (Configuration Manager) 2012 requires no special configuration and can be installed in the same way as any other master image application. The following information applies only to System Center Configuration Manager 2007. Configuration Manager versions earlier than Configuration Manager 2007 are not supported.

Complete the following to use Configuration Manager 2007 agent software in a PvD environment.

1. Install the Client Agent on the master image.
  1. Install the Configuration Manager client on the master image.
  2. Stop the ccmexec service (SMS Agent) and disable it.
  3. Delete SMS or client certificates from the local computer certificate store as follows:
    - Mixed mode: Certificates (Local Computer)\SMS\Certificates
    - Native mode
      - Certificates (Local Computer)\Personal\Certificates
      - Delete the client certificate that was issued by your certificate authority (usually, an internal Public Key Infrastructure)
  4. Delete or rename C:\Windows\smscfg.ini.
2. Remove information that uniquely identifies the client.
  1. (Optional) Delete or move log files from C:\Windows\System32\CCM\Logs.
  2. Install the Virtual Delivery Agent (if not installed previously), and take the PvD inventory.
  3. Shut down the master image, take a snapshot, and create a machine catalog using this snapshot.
3. Validate personal vDisk and start services. Complete these steps once on each PvD desktop, after it has been started for the first time. This can be done using a domain GPO, for example.
  - Confirm that PvD is active by checking for the presence of the registry key HKLM\Software\Citrix\personal vDisk\config\virtual.
  - Set the ccmexec service (SMS agent) to Automatic and start the service. The Configuration Manager client contacts the Configuration Manager server, and retrieves new unique certificates and GUIDs.

# 工具

May 28, 2016

You can use the following tools and utilities to tailor, expedite, and monitor PvD operations.

The custom rule files provided with PvD let you modify the default behavior of PvD image updates in the following ways:

- The visibility of files on the PvD
- How changes made to the files are merged
- Whether the files are writable

For detailed instructions on the custom rules files and the CoW feature, refer to the comments in the files located in C:\ProgramData\Citrix\personal vDisk\Config on the machine where PvD is installed. The files named "custom\_%" describe the rules and how to enable them.

Two scripts are provided to monitor and manage the size of PvDs; they are located in the Support\Tools\Scripts folder on the XenDesktop installation media. You can also use the PvD Image Update Monitoring Tool, which is located in the Support\Tools\Scripts\PvdTool folder; see <http://blogs.citrix.com/2014/06/02/introducing-the-pvd-image-update-monitoring-tool/> for details.

Use resize-personalvdisk-pool.ps1 to increase the size of the PvDs in all of the desktops in a catalog. The following snap-ins or modules for your hypervisor must be installed on the machine running Studio:

- XenServer requires XenServerPSSnapin
- vCenter requires vSphere PowerCli
- System Center Virtual Machine Manager requires the VMM console

Use personal-vdisk-poolstats.ps1 to check the status of image updates and to check the space for applications and user profiles in a group of PvDs. Run this script before updating an image to check whether any desktop is running out of space, which helps prevent failures during the update. The script requires that Windows Management Instrumentation (WMI-In) firewall is enabled on the PvD desktops. You can enable it on the master image or through GPO.

If an image update fails, the entry in the Update column gives the reason.

If a desktop becomes damaged or corrupted (by installing a broken application or some other cause), you can revert the application area of the PvD to a factory-default (empty) state. The reset operation leaves user profile data intact.

To reset the application area of the PvD, use one of the following methods:

- Log on to the user's desktop as Administrator. Launch a command prompt, and run the command C:\Program Files\Citrix\Personal vDisk\bin\CtxPvD.exe -s Reset.
- Locate the user's desktop in Citrix Director. Click Reset Personal vDisk and then click OK.

The image update process is an integral part of rolling out new images to PvD desktops; it includes adjusting the existing Personal vDisk to work with the new base image. For deployments that use Machine Creations Services (MCS), you can

export an inventory from an active VM to a network share, and then import it into a master image. A differential is calculated using this inventory in the master image. Although using the export/import inventory feature is not mandatory, it can improve the performance of the overall image update process.

To use the export/import inventory feature, you must be an administrator. If required, authenticate to the file share used for the export/import with “net use.” The user context must be able to access any file shares used for the export/import.

- To export an inventory, run the export command as an administrator on a machine containing a VDA with PvD enabled (minimum version 7.6):

```
Ctxpvdsvc.exe exportinventory "<path-to-export-location>"
```

The software detects the current inventory's location and exports the inventory to a folder named “ExportedPvdInventory” to the specified location. Here's an excerpt from the command output:

```
C:\Program Files\Citrix\personal vDisk\bin> .\CtxPvDSvc.exe exportinventory
```

```
\share location\ExportedInventory
```

```
Current inventory source location C:\CitrixPvD\Settings\Inventory\VER-LAS
```

```
...
```

```
Exporting current inventory to location \\\\....
```

```
...
```

```
Deleting any pre-existing inventory folder at \\\\....
```

```
.Successfully exported current inventory to location \\\\.... Error code = OPS
```

- To import a previously-exported inventory, run the import command as an administrator on the master image:

To import

Run the import command as an administrator on the master image.

```
Ctxpvdsvc.exe importinventory "<path-to-exported-inventory>"
```

The <path to exported inventory> should be the full path to the inventory files, which is usually <network location\ExportedPvdInventory>.

The inventory is obtained from the import location (where it was previously exported using the exportinventory option) and imports the inventory to the inventory store on the master image. Here's an excerpt of the command output:

```
C:\Program Files\Citrix\personal vDisk\bin> .\CtxPvDSvc.exe importinventory
```

```
\share location\ExportedInventory\ExportedPvdInventory
```

```
Importing inventory \share location\ExportedInventory\ExportedPvdInventory
```

```
...
```

```
Successfully added inventory \share location\ExportedInventory\ExportedPvdInventory to the  
store at c:\ProgramData\Citrix\personal vDisk\InventoryStore
```

After the export, the network share should include the following filenames. After the import, the inventory store on the master image should include the same file names.

- Components.DAT
- files\_rules
- folders\_rules
- regkey\_rules
- RINGTHREE.DAT
- S-1-5-18.DAT
- SAM.DAT
- SECURITY.DAT

- SNAPSHOT.DAT
- SOFTWARE.DAT
- SYSTEM.CurrentControlSet.DAT
- VDCATALOG.DAT
- vDiskJournalData

Important: The scripts do not move PvDs to the new storage location. You must perform that operation in some other way.

Two PowerShell scripts supplied on the product installation media (in the Support\Tools\Scripts folder) allow you to back up and restore Personal vDisks. Use the backup and restore scripts to migrate existing PvDs and user associations from one catalog to another. This can be useful if you are changing your PvD storage. The backup script creates an .xml file with metadata from an existing catalog. The metadata contains the current location of the PvDs on the storage, and the user associations with the PvDs. The restore script uses the .xml file to associate the PvDs with a new catalog and assign the correct users to them.

- migration-backup.ps1 captures the mapping between each user and their Personal vDisk in a machine catalog and stores this information in an .xml file
- migration-restore.ps1 uses the .xml file to re-create a user's desktop in a machine catalog

Before backing up and restoring, note the following:

- The scripts work with the hypervisor API so the hypervisor's PowerShell snap-in must be installed on the Controller where the scripts are executed
- Run the scripts from a location that has access to the Controller where the machine catalog was created
- The scripts are supported on the following hypervisor platforms: Citrix XenServer, Microsoft Hyper-V, and VMware ESX

### **Back up a machine catalog**

Perform a backup when a change is made to a machine catalog. You can perform a backup while the machines in the catalog are active.

Use migration-backup.ps1 to back up any machine catalog containing Personal vDisks. The script asks for the name of the machine catalog and connection information for the hypervisor. It then iterates through all of the user-assigned machines in the machine catalog and, for each machine, stores the mapping between the Personal vDisk storage and the assigned user. This information is located in an .xml file, which has the following structure:

```
<PVDMigration>
<hypervisor>
<type></type>
</hypervisor>
<PVD>
<DiskId></DiskId>
<DiskName></DiskName>
<SRName></SRName>
<SRID></SRID>
<UserName></UserName>
<UserSid></UserSid>
<State></State>
</PVD>
</PVDMigration>
```

- PvDMigration.hypervisor.Type supports VMware ESX, Citrix XenServer, and Microsoft Hyper-V.

- PvDMigration.PVD stores information on where the Personal vDisk is stored and the user associated with it.
- PvDMigration.PVD.DiskId is the unique identifier of the vDisk on the hypervisor on which the backup was taken.
- PvDMigration.PVD.DiskName is the name of the .vhd or .vmdk file.
- PvDMigration.PVD.SRName is the name of the storage provider when the backup was taken.
- PvDMigration.PVD.SRID is the unique identifier of the storage provider on the hypervisor on which the backup was taken.
- PvDMigration.PVD.UserName is the name of the user associated with this vDisk.
- PvDMigration.PVD.UserId is the SID of the user associated with this vDisk.
- PvDMigration.PVD.State indicates the state of this vDisk. This can be either "backed up" or "processed." It is "backed up" after the initial backup; the state changes to "processed" after the .xml file is used for restoring from the backup.

## Restore a machine catalog

Before restoring, note the following:

- You can only restore a machine catalog that shares the same master image as that of the backed-up machine catalog
- You must create a new master image by updating the inventory of the master image that the backed-up machine catalog was created from

Use migration-restore.ps1 to restore any machine catalog containing Personal vDisks. The script takes the following inputs:

- The .xml file created during the backup process
- The name of the machine catalog to restore
- The name of the location where the unattached Personal vDisks are stored. This is listed in the .xml file
- Hypervisor connection information

The migration-restore.ps1 script finds any unassigned machines in the machine catalog and assigns users to them. It also attaches users' Personal vDisks to the machines.

### Example scenario 1: Restore a machine catalog and its Personal vDisks using new machine names

In this scenario, an entire machine catalog and the Personal vDisks attached to the machines in it are restored. The machines are given new names. This scenario might occur when your hypervisor or a storage host has failed, or when you migrate users to a new infrastructure.

1. Run migration-backup.ps1 to capture the user-to-Personal-vDisk mapping in the .xml file.
2. Using a backup solution, move or capture the Personal vDisks from the original machine catalog on to a disk:
  - VMware ESX or Microsoft Hyper-V: Personal vDisks are located on the storage specified by the Controller, in a folder containing the name of the machine to which the vDisk is attached.
  - Citrix XenServer: Personal vDisks are located in the root of the storage specified by the Controller. The name of each vDisk is a GUID.
3. Restore the Personal vDisks from the original machine catalog using a storage backup solution:
  - ESX or Hyper-V: Locate the vDisks in a new folder of the new storage resource. Alternatively, leave the vDisks in the original path on the new storage resource.
  - XenServer: Locate the vDisks in the root of the new storage resource.
4. Create a Provisioning Services vDisk or a Machine Creation Services snapshot from the master image, which you used to create the failed machine catalog.
5. Run Update Inventory from the Start menu on the vDisk or snapshot.
6. Re-create the machine catalog in Studio using a different naming convention as the failed (original) machine catalog. This generates a catalog of new machines, each with a new Personal vDisk, that the site database recognizes.
7. Verify that the re-created machine catalog is assigned to the correct Delivery Group.
8. Verify that the Delivery Group is in maintenance mode and the machines in it are shut down.

9. Edit the .xml file generated by the backup script:
  - ESX or Hyper-V: If you restored the vDisks to a new folder on the new storage resource in Step 3, for every PVD section in the file, replace the folder name in DiskName with the location of the restored vDisks. If you restored the vDisks to the original path on the new storage, skip this step.
  - XenServer: Skip this step.
10. On the Controller, run migration-restore.ps1, specifying the name of the .xml file and the location where the backed-up vDisks are stored.

#### **Example scenario 2: Restore a machine catalog and its Personal vDisks reusing existing machine names**

In this scenario, an entire machine catalog and the Personal vDisks attached to the machines in it are restored. Existing (failed) machine names are reused. This scenario might occur when your hypervisor or a storage host has failed.

1. Run migration-backup.ps1 to capture the user-to-Personal-vDisk mapping.
2. Using a backup solution, move or capture the Personal vDisks from the original machine catalog on to a disk:
  - ESX or Hyper-V: Personal vDisks are located on the storage specified by the Controller, in a folder containing the name of the machine to which the vDisk is attached.
  - XenServer: Personal vDisks are located in the root of the storage specified by the Controller. The name of each vDisk is a GUID.
3. Restore the Personal vDisks from the original machine catalog using a storage backup solution:
  - ESX or Hyper-V: Locate the vDisks in a new folder of the new storage resource.
  - XenServer: Locate the vDisks in the root of the new storage resource.
4. Create a Provisioning Services vDisk or a Machine Creation Services snapshot from the master image that you used to create the failed machine catalog.
5. Run Update Inventory from the Start menu on the vDisk or snapshot.
6. Re-create the machine catalog in Studio using the same naming convention as the failed machine catalog. This generates a catalog of new machines, each with a new Personal vDisk, that the site database recognizes.
7. Verify that the re-created machine catalog is assigned to the correct Delivery Group.
8. Verify that the Desktop Group is in maintenance mode and the machines in it are shut down.
9. Edit the .xml file generated by the backup script:
  - ESX or Hyper-V: For every PVD section in the file, replace the folder name in DiskName with the location of the restored vDisks.
  - XenServer: Skip this step.
10. Run the migration-restore.ps1 script on the Controller with the modified .xml file as an input. The script attaches the vDisks without moving them.
11. Verify the users' data has been successfully restored.

#### **Example scenario 3: Restore a subset of Personal vDisks in a machine catalog**

In this scenario, some, but not all, of the Personal vDisks in a machine catalog have failed and are restored. The virtual machines in the catalog have not failed.

1. Run migration-backup.ps1 to capture the user-to-Personal-vDisk mapping in the .xml file.
2. The .xml file has a PVD section for each user in the machine catalog. For any users whose Personal vDisks do not need restoring, remove the users and their associated sections from the file.
3. Restore the Personal vDisks from the original machine catalog using a backup solution, as described in the one of the other scenarios:
  - To use new machine names, follow example scenario 1.
  - To preserve machine names, follow example scenario 2.
4. Ensure there are enough unassigned machines in the catalog. Add machines if necessary. You need one new machine for

each user whose vDisk you want to restore.

5. Verify that the Desktop Group is in maintenance mode and the machines in it are shut down.
6. On the Controller, run migration-restore.ps1 with the modified .xml file as an input.
7. Verify the users' data has been successfully restored.

# 显示、消息和故障排除

May 28, 2016

In Studio, when you choose a PvD-enabled machine in a machine catalog, the "PvD" tab provides monitoring status during image updates, plus estimated completion time and progress. The possible state displays during an image update are: Ready, Preparing, Waiting, Failed, and Requested.

An image update can fail for different reasons, including lack of space or a desktop not finding the PvD in sufficient time. When Studio indicates that an image update failed, an error code with descriptive text is provided to help troubleshooting. Use the Personal vDisk Image Update Monitoring Tool or the personal-vdisk-poolstats.ps1 script to monitor image update progress and obtain error codes associated with the failure.

If an image update fails, the following log files can provide further troubleshooting information:

- PvD service log - C:\ProgramData\Citrix\personal vDisk\Logs\PvDSvc.log.txt
- PvD activation log i- P:\PVDLOGS\PvDActivation.log.txt

The most recent content is at the end of the log file.

The following errors are valid for PvD version 7.6 and later:

- **An internal error occurred. Review the Personal vDisk logs for further details. Error code %d (%s)**  
This is a catch-all for uncategorized errors, so it has no numeric value. All unexpected error encountered during inventory creation or Personal vDisk update are indicated by this error code.
  - Collect logs and contact Citrix support.
  - If this error occurs during catalog update, roll back the catalog to the previous version of the gold image.
- **There are syntax errors in the rule files. Review the logs for further details.**  
Error code 2. The rule file contains syntax errors. The Personal vDisk log file contains the name of the rule file and line number where the syntax error was found. Fix the syntax error in the rule file and retry the operation.
- **The inventory stored in the Personal vDisk corresponding to the previous version of the master image is corrupt or unreadable.**  
Error code 3. The last inventory is stored in "UserData.V2.vhd" in "\ProgramData\CitrixPvD\Settings\Inventory\VER-LAST". Restore the inventory corresponding to the last version of the master image by importing the 'VER-LAST' folder from a known working PvD machine associated with the previous version of the master image.
- **The inventory stored in the Personal vDisk corresponding to the previous version of the master image is higher version.**  
Error code 4. This is caused by personal vDisk version incompatibility between the last master image and the current master image. Retry updating the catalog after installing the latest version of personal vDisk in the master image.
- **Change journal overflow was detected.**  
Error code 5. A USN journal overflow was caused by a large number of changes made to the master image while creating the inventory. If this continues to occur after multiple attempts, use procmon to determine if third party software is creating/deleting a large number of files during inventory creation.
- **The Personal vDisk could not find a disk attached to the system for storing user data.**  
Error code 6. First, verify that the PvD disk is attached to the VM through the hypervisor console. This error typically happens due to "Data Leak Prevention" software preventing access to the PvD disk. If the PvD disk is attached to the

VM, try adding an exception for “attached disk” in the “Data Leak Prevention” software configuration.

- **The system has not been rebooted post-installation. Reboot to implement the changes.**  
Error code 7. Restart the desktop and retry the operation.
- **Corrupt installation. Try re-installing Personal vDisk.**  
Error code 8. Install personal vDisk and try again.
- **Personal vDisk inventory is not up to date. Update the inventory in the master image, and then try again.**  
Error code 9. The personal vDisk inventory was not updated in the master image before shutting down the desktop. Restart the master image and shut down the desktop through the “Update personal vDisk” option, and then create a new snapshot; use that snapshot to update the catalog.
- **An internal error occurred while starting the Personal vDisk. Review the Personal vDisk logs for further details.**  
Error code 10. This could be caused by the PvD driver failing to start a virtualization session due to an internal error or personal vDisk corruption. Try restarting the desktop through the Controller. If the problem persists, collect the logs and contact Citrix Support.
- **The Personal vDisk timed out while trying to find a storage disk for users' personalization settings.**  
Error code 11. This error occurs when the PvD driver fails to find the PvD disk within 30 seconds after restart. This is usually caused by an unsupported SCSI controller type or storage latency. If this occurs with all desktops in the catalog, change the SCSI controller type associated with the “Template VM” / “Master VM” to a type supported by personal vDisk technology. If this occurs with only some desktops in the catalog, it might be due to spikes in storage latency due to a large number of desktops starting at the same time. Try limiting the maximum active power actions setting associated with the host connection.
- **The Personal vDisk has been de-activated because an unsafe system shutdown was detected. Restart the machine.**  
Error code 12. This could be due to a desktop failing to complete the boot process with PvD enabled. Try restarting the desktop. If the problem persists, watch the desktop startup through the hypervisor console and check if the desktop is crashing. If a desktop crashes during startup, restore the PvD from backup (if you maintain one) or reset the PvD.
- **The drive letter specified for mounting the Personal vDisk is not available.**  
Error code 13. This could be caused by PvD failing to mount the PvD disk at the mount specified by the administrator. The PvD disk will fail to mount if the drive letter is already used by other hardware. Select a different letter as the mount point for the personal vDisk.
- **Personal vDisk kernel mode drivers failed to install.**  
Error code 14. Personal vDisk installs drivers during the first inventory update after installation. Some antivirus products prevent installation of the driver when attempted outside the context of an installer. Temporarily disable the antivirus real time scan or add exceptions in the antivirus for PvD drivers during the first time inventory creation.
- **Cannot create a snapshot of the system volume. Make sure that the Volume Shadow Copy service is enabled.**  
Error code 15. This could occur because the Volume Shadow Copy service is disabled. Enable the Volume Shadow Copy service and retry taking an inventory.
- **The change journal failed to activate. Try again after waiting for few minutes.**  
Error code 16. Personal vDisk uses change journal for tracking changes made to master image. During an inventory

update, if PvD detects that the change journal is disabled, it attempts to enable it; this error occurs when that attempt fails. Wait for few minutes and retry.

- **There is not enough free space in the system volume.**

Error code 17. There is not enough free space available on the C drive of the desktop for the image update operation. Expand the system volume or removed unused files to free space in the system volume. The image update should begin again after the next restart.

- **There is not enough free space in the Personal vDisk storage. Expand Personal vDisk storage to provide more space.**

Error code 18. There is not enough free space available on the personal vDisk drive when performing an image update operation. Expand personal vDisk storage or remove unused files to free space in the personal vDisk storage. The image update should restart after next reboot.

- **Personal vDisk storage is over-committed. Expand Personal vDisk storage to provide more space.**

Error code 19. There is not enough free space available on the personal vDisk drive to fully accommodate thick provisioned "UserData.V2.vhd". Expand the personal vDisk storage or remove unused files to free space in the personal vDisk storage.

- **Corrupt system registry.**

Error code 20. The system registry is corrupt, damaged, missing, or unreadable. Reset the personal vDisk or restore it from an earlier backup.

- **An internal error occurred while resetting the Personal vDisk. Check Personal vDisk logs for further details.**

Error code 21. This is a catch-all for all the errors encountered during a personal vDisk reset. Collect the logs and contact Citrix Support.

- **Failed to reset the Personal vDisk because there is not enough free space in the personal vDisk storage.**

Error code 22. There is not enough free space available on the Personal vDisk drive when performing a reset operation. Expand the personal vDisk storage or remove unused files to free space in the personal vDisk storage.

The following errors are valid for PvD 7.x versions earlier than 7.6:

- **Startup failed. Personal vDisk was unable to find a storage disk for user personalization settings.**

The PvD software could not find the Personal vDisk (by default, the P: drive) or could not mount it as the mount point selected by the administrator when they created the catalog.

- Check the PvD service log for following entry: "PvD 1 status --> 18:183".
- If you are using a version of PvD earlier than Version 5.6.12, upgrading to the latest version resolves this issue.
- If you are using Version 5.6.12 or later, use the disk management tool (diskmgmt.msc) to determine whether the P: drive is present as an unmounted volume. If present, run chkdsk on the volume to determine if it is corrupt, and try to recover it using chkdsk.

- **Startup failed. Citrix Personal vDisk failed to start. For further assistance .... Status code: 7, Error code: 0x70**

Status code 7 implies that an error was encountered while trying to update the PvD. The error could be one of the following:

Error code	Description
0x20000001	Failed to save the diff package, most likely due to lack of free disk space inside the VHD.

0x20000004	Failed to acquire required privileges for updating the PvD.
0x20000006	Failed to load hive from the PvD image or from PvD inventory, most likely due to corrupt PvD image or inventory.
0x20000007	Failed to load the file system inventory, most likely due to a corrupt PvD image or inventory.
0x20000009	Failed to open the file containing file system inventory, most likely due to a corrupt PvD image or inventory.
0x2000000B	Failed to save the diff package, most likely due to lack of free disk space inside the VHD.
0x20000010	Failed to load the diff package.
0x20000011	Missing rule files.
0x20000021	Corrupt PvD inventory.
0x20000027	The catalog "MojoControl.dat" is corrupt.
0x2000002B	Corrupt or missing PvD inventory.
0x2000002F	Failed to register user installed MOF on image update, upgrade to 5.6.12 to fix the issue.
0x20000032	Check the PvDactivation.log.txt for the last log entry with a Win32 error code.
0x20	Failed to mount application container for image update, upgrade to 5.6.12 to fix the issue.
0x70	There is not enough space on the disk.

- **Startup failed. Citrix Personal vDisk failed to start [or Personal vDisk encountered an internal error]. For further assistance ... Status code: 20, Error code 0x20000028**  
The personal vDisk was found but a PvD session could not be created.

Collect the logs and check SysVol-lvmSupervisor.log for session creation failures:

1. Check for the following log entry " IvmpNativeSessionCreate: failed to create native session, status XXXXX".
2. If the status is 0xc00002cf, fix the problem by adding a new version of the master image to the catalog. This status code implies that the USN Journal overflowed due to a large number of changes after an inventory update.
3. Restart the affected virtual desktop. If the problem persists, contact Citrix Technical Support.

- **Startup failed. Citrix Personal vDisk has been deactivated because an unsafe system shutdown was detected. To retry, select Try again. If the problem continues, contact your system administrator.**

The pooled VM cannot complete its startup with the PvD enabled. First determine why startup cannot be completed.

Possible reasons are that a blue screen appears because:

- An incompatible antivirus product is present, for example old versions of Trend Micro, in the master image.
- The user has installed software that is incompatible with PvD. This is unlikely, but you can check it by adding a new machine to the catalog and seeing whether it restarts successfully.
- The PvD image is corrupt. This has been observed in Version 5.6.5.

To check if the pooled VM is displaying a blue screen, or is restarting prematurely:

- Log on to the machine through the hypervisor console.

- Click Try Again and wait for the machine to shut down.
- Start the machine through Studio.
- Use the hypervisor console to watch the machine console as it starts.

Other troubleshooting:

- Collect the memory dump from the machine displaying the blue screen, and send it for further analysis to Citrix Technical Support.
- Check for errors in the event logs associated with the PvD:
  1. Mount UserData.V2.vhd from the root of the P: drive using DiskMgmt.msc by clicking Action > Attach VHD.
  2. Launch Eventvwr.msc.
  3. Open the system event log (Windows\System32\winevt\logs\system.evtx) from UserData.V2.vhd by clicking Action > Open saved logs.
  4. Open the application event log (Windows\System32\winevt\logs\application.evtx) from UserData.V2.vhd by clicking Action > Open saved logs.
- **The Personal vDisk cannot start. The Personal vDisk could not start because the inventory has not been updated. Update the inventory in the master image, then try again. Status code: 15, Error code: 0x0**  
 The administrator selected an incorrect snapshot while creating or updating the PvD catalog (that is, the master image was not shut down using Update Personal vDisk when creating the snapshot).

If Personal vDisk is not enabled, you can view the following events in Windows Event Viewer. Select the Applications node in the left pane; the Source of the events in the right pane is Citrix Personal vDisk. If Personal vDisk is enabled, none of these events are displayed.

An Event ID of 1 signifies an information message, an ID of 2 signifies an error. Not all events may be used in every version of Personal vDisk.

Event ID	Description
1	Personal vDisk Status: Update Inventory Started.
1	Personal vDisk Status: Update Inventory completed. GUID: %s.
1	Personal vDisk Status: Image Update Started.
1	Personal vDisk Status: Image Update completed.
1	Reset in progress.
1	OK.
2	Personal vDisk Status: Update Inventory Failed with: %s.
2	Personal vDisk Status: Image Update Failed with: %s.
2	Personal vDisk Status: Image Update Failed with Internal Error.
2	Personal vDisk Status: Update Inventory Failed with: Internal Error.
2	Personal vDisk has been disabled because of an improper shutdown.

Event ID	Description
2	Image update failed. Error code %d.
2	Personal vDisk encountered an internal error. Status code[%d] Error code[0x%X].
2	Personal vDisk reset failed.
2	Unable to find disk for storing user personalization settings.
2	There is not enough space available on the storage disk to create a Personal vDisk container.

# 用户配置文件

May 28, 2016

By default, Citrix Profile management is installed silently on master images when you install the Virtual Delivery Agent, but you do not have to use Profile management as a profile solution.

To suit your users' varying needs, you can use XenApp and XenDesktop policies to apply different profile behavior to the machines in each Delivery Group. For example, one Delivery Group might require Citrix mandatory profiles, whose template is stored in one network location, while another Delivery Group requires Citrix roaming profiles stored in another location with several redirected folders.

- If other administrators in your organization are responsible for XenApp and XenDesktop policies, work with them to ensure that they set any profile-related policies across your Delivery Groups.
- Profile management policies can also be set in Group Policy, in the Profile management .ini file, and locally on individual virtual machines. These multiple ways of defining profile behavior are read in the following order:
  1. Group Policy (.adm or .admx files)
  2. XenApp and XenDesktop policies in the Policy node
  3. Local policies on the virtual machine that the user connects to
  4. Profile management .ini file

For example, if you configure the same policy in both Group Policy and the Policy node, the system reads the policy setting in Group Policy and ignores the XenApp and XenDesktop policy setting.

Whichever profile solution you choose, Director administrators can access diagnostic information and troubleshoot user profiles. For more information, see the Director documentation.

If you use the Personal vDisk feature, Citrix user profiles are stored on virtual desktops' Personal vDisks by default. Do not delete the copy of a profile in the user store while a copy remains on the Personal vDisk. Doing so creates a Profile management error, and causes a temporary profile to be used for logons to the virtual desktop.

The desktop type is automatically detected, based on the Virtual Delivery Agent installation and, in addition to the configuration choices you make in Studio, sets Profile management defaults accordingly.

The policies that Profile management adjusts are shown in the table below. Any non-default policy settings are preserved and are not overwritten by this feature. Consult the Profile management documentation for information about each policy. The types of machines that create profiles affect the policies that are adjusted. The primary factors are whether machines are persistent or provisioned, and whether they are shared by multiple users or dedicated to just one user.

Persistent systems have some type of local storage, the contents of which can be expected to persist when the system turns off. Persistent systems may employ storage technology such as storage area networks (SANs) to provide local disk mimicking. In contrast, provisioned systems are created "on the fly" from a base disk and some type of identity disk. Local storage is usually mimicked by a RAM disk or network disk, the latter often provided by a SAN with a high speed link. The provisioning technology is generally Provisioning Services or Machine Creation Services (or a third-party equivalent).

Sometimes provisioned systems have persistent local storage, which may be provided by Personal vDisks; these are classed as persistent.

Together, these two factors define the following machine types:

- **Both persistent and dedicated** -- Examples are Desktop OS machines with a static assignment and a Personal vDisk

that are created with Machine Creation Services, desktops with Personal vDisks that are created with VDI-in-a-Box, physical workstations, and laptops

- **Both persistent and shared** -- Examples are Server OS machines that are created with Machine Creation Services
- **Both provisioned and dedicated** -- Examples are Desktop OS machines with a static assignment but without a Personal vDisk that are created with Provisioning Services
- **Both provisioned and shared** -- Examples are Desktop OS machines with a random assignment that are created with Provisioning Services and desktops without Personal vDisks that are created with VDI-in-a-Box

The following Profile management policy settings are suggested guidelines for the different machine types. They work well in most cases, but you may want to deviate from these as your deployment requires.

Important: Delete locally cached profiles on logoff, Profile streaming, and Always cache are enforced by the auto-configuration feature. Adjust the other policies manually.

#### Persistent machines

Policy	Both persistent and dedicated	Both persistent and shared
Delete locally cached profiles on logoff	Disabled	Enabled
Profile streaming	Disabled	Enabled
Always cache	Enabled (note 1)	Disabled (note 2)
Active write back	Disabled	Disabled (note 3)
Process logons of local administrators	Enabled	Disabled (note 4)

#### Provisioned machines

Policy	Both provisioned and dedicated	Both provisioned and shared
Delete locally cached profiles on logoff	Disabled (note 5)	Enabled
Profile streaming	Enabled	Enabled
Always cache	Disabled (note 6)	Disabled
Active write back	Enabled	Enabled
Process logons of local administrators	Enabled	Enabled (note 7)

1. Because Profile streaming is disabled for this machine type, the Always cache setting is always ignored.
2. Disable Always cache. However, you can ensure that large files are loaded into profiles as soon as possible after logon by enabling this policy and using it to define a file size limit (in MB). Any file this size or larger is cached locally as soon as possible.
3. Disable Active write back except to save changes in profiles of users who roam between XenApp servers. In this case, enable this policy.
4. Disable Process logons of local administrators except for Hosted Shared Desktops. In this case, enable this policy.
5. Disable Delete locally cached profiles on logoff. This retains locally cached profiles. Because the machines are reset at logoff but are assigned to individual users, logons are faster if their profiles are cached.
6. Disable Always cache. However, you can ensure that large files are loaded into profiles as soon as possible after logon by enabling this policy and using it to define a file size limit (in MB). Any file this size or larger is cached locally as soon as possible.
7. Enable Process logons of local administrators except for profiles of users who roam between XenApp and XenDesktop servers. In this case, disable this policy.

Folder redirection lets you store user data on network shares other than the location where the profiles are stored. This reduces profile size and load time but it might impact network bandwidth. Folder redirection does not require that Citrix user profiles are employed. You can choose to manage user profiles on your own, and still redirect folders.

Configure folder redirection using Citrix policies in Studio.

- Ensure that the network locations used to store the contents of redirected folders are available and have the correct permissions. The location properties are validated.
- Redirected folders are set up on the network and their contents populated from users' virtual desktops at logon.

Note: Configure folder redirection using only Citrix Policies or Active Directory Group Policy Objects, not both. Configuring folder redirection using both policy engines may result in unpredictable behavior.

In deployments with multiple operating systems (OSs), you might want some of a user's profile to be shared by each OS. The rest of the profile is not shared and is used only by one OS. To ensure a consistent user experience across the OSs, you need a different configuration for each OS. This is advanced folder redirection. For example, different versions of an application running on two OSs might need to read or edit a shared file, so you decide to redirect it to a single network location where both versions can access it. Alternatively, because the Start Menu folder contents are structured differently in two OSs, you decide to redirect only one folder, not both. This separates the Start Menu folder and its contents on each OS, ensuring a consistent experience for users.

If your deployment requires advanced folder redirection, you must understand the structure of your users' profile data and determine which parts of it can be shared between OSs. This is important because unpredictable behavior can result unless folder redirection is used correctly.

To redirect folders in advanced deployments:

- Use a separate Delivery Group for each OS.
- Understand where your virtual applications, including those on virtual desktops, store user data and settings, and understand how the data is structured.
- For shared profile data that can safely roam (because it is structured identically in each OS), redirect the containing folders in each Delivery Group.
- For non-shared profile data that cannot roam, redirect the containing folder in only one of the Desktop Groups, typically

the one with the most used OS or the one where the data is most relevant. Alternatively, for non-shared data that cannot roam between OSs, redirect the containing folders on both systems to separate network locations.

**Example advanced deployment** - This deployment has applications, including versions of Microsoft Outlook and Internet Explorer, running on Windows 8 desktops and applications, including other versions of Outlook and Internet Explorer, delivered by Windows Server 2008. To achieve this, you have already set up two Delivery Groups for the two OSs. Users want to access the same set of Contacts and Favorites in both versions of those two applications.

Important: The following decisions and advice are valid for the OSs and deployment described. In your organization, the folders you choose to redirect and whether you decide to share them depend on a number of factors that are unique to your specific deployment.

- Using policies applied to the Delivery Groups, you choose the following folders to redirect.

Folder	Redirected in Windows 8?	Redirected in Windows Server 2008?
My Documents	Yes	Yes
Application Data	No	No
Contacts	Yes	Yes
Desktop	Yes	No
Downloads	No	No
Favorites	Yes	Yes
Links	Yes	No
My Music	Yes	Yes
My Pictures	Yes	Yes
My Videos	Yes	Yes
Searches	Yes	No
Saved Games	No	No
Start Menu	Yes	No

- For the shared, redirected folders:
  - After analyzing the structure of the data saved by the different versions of Outlook and Internet Explorer, you decide it is safe to share the Contacts and Favorites folders
  - You know the structure of the My Documents, My Music, My Pictures, and My Videos folders is standard across OSs, so it is safe to store these in the same network location for each Delivery Group
- For the non-shared, redirected folders:
  - You do not redirect the Desktop, Links, Searches, or Start Menu folders folder in the Windows Server Delivery Group because data in these folders is organized differently in the two OSs. It therefore cannot be shared.
  - To ensure predictable behavior of this non-shared data, you redirect it only in the Windows 8 Delivery Group. You choose this, rather than the Windows Server Delivery Group, because Windows 8 will be used more often by users in

their day-to-day work; they will only occasionally access the applications delivered by the server. Also, in this case the non-shared data is more relevant to a desktop environment rather than an application environment. For example, desktop shortcuts are stored in the Desktop folder and might be useful if they originate from a Windows 8 machine but not from a Windows Server machine.

- For the non-redirected folders:
  - You do not want to clutter your servers with users' downloaded files, so you choose not to redirect the Downloads folder
  - Data from individual applications can cause compatibility and performance issues, so you decide not to redirect the Application Data folder

For more information on folder redirection, see <http://technet.microsoft.com/en-us/library/cc766489%28v=ws.10%29.aspx>.

In Citrix Profile management (but not in Studio), a performance enhancement allows you to prevent folders from being processed using exclusions. If you use this feature, do not exclude any redirected folders. The folder redirection and exclusion features work together, so ensuring no redirected folders are excluded allows Profile management to move them back into the profile folder structure again, while preserving data integrity, if you later decide not to redirect them. For more information on exclusions, see [To include and exclude items](#).

# HDX

Oct 05, 2016

Citrix HDX includes a broad set of technologies that provide a high-definition user experience.

At the device	HDX leverages the computing capacity of user devices to enhance and optimize the user experience. HDX MediaStream technology ensures users receive a smooth, seamless experience with multimedia content in their virtual desktops or applications. Workspace control enables users to pause virtual desktops and applications and resume working from a different device at the point where they left off.
On the network	HDX incorporates advanced optimization and acceleration capabilities to deliver the best performance over any network, including low-bandwidth and high-latency WAN connections.  HDX features adapt to changes in the environment, balancing performance and bandwidth by applying the best technologies for each unique user scenario, whether the desktop or application is accessed locally on the corporate network or remotely from outside the corporate firewall.
In the datacenter	HDX leverages the processing power and scalability of servers to deliver advanced graphical performance, regardless of the capabilities of the client device. Compressed multimedia information is sent directly to the user device in its native format.  HDX channel monitoring provided by Citrix Director displays the status of connected HDX channels on user devices.  HDX Insight, the integration of EdgeSight Network Inspector and EdgeSight Performance management with Director, captures data about ICA traffic and provides a dashboard view of real-time and historical details such as client-side and server-side ICA session latency, bandwidth use of ICA channels, and the ICA round trip time value of each session.

To experience HDX capabilities from your virtual desktop:

- See how HDX delivers rich video content to virtual desktops: View a video on a web site containing high definition videos, such as <http://www.microsoft.com/silverlight/iis-smooth-streaming/demo/>.
- See how Flash Redirection accelerates delivery of Flash multimedia content:
  1. Download Adobe Flash player (<http://get.adobe.com/flashplayer/>) and install it on both the virtual desktop and the user device.
  2. On the Desktop Viewer toolbar, click Preferences. In the Desktop Viewer Preferences dialog box, click the Flash tab and select Optimize content.
  3. To experience how Flash Redirection accelerates the delivery of Flash multimedia content to virtual desktops, view a video on your desktop from a web site containing Flash videos, such as YouTube. Flash Redirection is designed to be seamless so that users do not know when it is running. You can check to see whether Flash Redirection is being used by looking for a block of color that appears momentarily before the Flash player starts.
- See how HDX delivers high definition audio:
  1. Configure your Citrix client for maximum audio quality; see the Receiver documentation for details.
  2. Play music files with a digital audio player (such as iTunes) on your desktop.

HDX provides a superior graphics and video experience for most users by default, with no configuration required. Citrix

policy settings that provide the best out-of-the-box experience for the majority of use cases are enabled by default.

- HDX automatically selects the best delivery method based on the client, platform, application, and network bandwidth, and then self-tunes based on changing conditions.
- HDX optimizes the performance of 2D and 3D graphics and video.
- HDX delivers a Windows Aero experience to virtual desktop users on any client.
- HDX enables user devices to stream multimedia files directly from the source provider on the Internet or Intranet, rather than through the host server. If the requirements for this client-side content fetching are not met, media delivery falls back to Windows Media redirection to play media run-time files on user devices rather than the host server. In most cases, no adjustments to the Windows Media feature policies are needed.

Good to know:

- For support and requirements information for HDX features, see [System requirements for XenApp and XenDesktop 7.6 LTSR](#). Except where otherwise noted, HDX features are available for supported Windows Server OS and Windows Desktop OS machines, plus Remote PC Access desktops.
- This content describes how to further optimize the user experience, improve server scalability, or reduce bandwidth requirements. For information about working with Citrix policies and policy settings, see the *Citrix policies* documents for this release.
- For instructions that include working with the registry, use caution: editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

By default, HDX delivers a highly responsive Windows Aero or Windows 8 desktop experience to virtual desktops accessed from supported Windows user devices. To do that, HDX leverages the graphics processing unit (GPU) or integrated graphics processor (IGP) on the user devices for local DirectX graphics rendering. This feature, named desktop composition redirection, maintains high scalability on the server. For details, see What to do with all these choices in <http://blogs.citrix.com/2013/11/06/go-supersonic-with-xendesktop-7-x-bandwidth-supercodecs/>.

To reduce the bandwidth required in user sessions, consider adjusting the following Citrix policy settings. Keep in mind that changing these settings can reduce the quality of the user experience.

- **Desktop Composition Redirection.** Applies only to Windows Desktop OS machines accessed from Windows user devices and applies only to the composition of the Windows desktop. Application windows are rendered on the server unless the Citrix policy setting Allow local app access (LTSR: not supported) is Allowed.
- **Desktop Composition Redirection graphics quality.** Uses high-quality graphics for desktop composition unless seamless applications or Local App Access (LTSR: not supported) are enabled. To reduce bandwidth requirements, lower the graphics quality.
- **Dynamic windows preview.** Controls the display of seamless windows in Flip, Flip 3D, taskbar preview, and peek window preview modes. To reduce bandwidth requirements, disable this policy setting.

The following visual display policy settings control the quality of images sent from virtual desktops to user devices.

- Visual quality. Controls the visual quality of images displayed on the user device: medium, high, always lossless, build to lossless (default = medium).
- Target frame rate. Specifies the maximum number of frames per second that are sent from the virtual desktop to the user device (default = 30). In many circumstances, you can improve the user experience by specifying a higher value. For

devices with slower CPUs, specifying a lower value can improve the user experience.

- **Display memory limit.** Specifies the maximum video buffer size for the session in kilobytes (default = 65536 KB). For connections requiring more color depth and higher resolution, increase the limit. You can calculate the maximum memory required. Color depths other than 32-bit are available only if the Legacy graphics mode policy setting is enabled.

HDX webcam video compression improves bandwidth efficiency and latency tolerance for webcams during video conferencing in a session. This technology streams webcam traffic over a dedicated multimedia virtual channel; this uses significantly less bandwidth compared to the isochronous HDX Plug-n-Play support, and works well over WAN connections.

Receiver users can override the default behavior by choosing the Desktop Viewer Mic & Webcam setting **Don't use my microphone or webcam**. To prevent users from switching from HDX webcam video compression, disable USB device redirection with the policy settings under ICA policy settings > USB Devices policy settings.

HDX webcam video compression is enabled by default on Receiver for Windows but must be configured on Receiver for Linux. For more information, refer to the Receiver documentation. HDX webcam video compression requires that the following policy settings be enabled (all are enabled by default).

- Client audio redirection
- Client microphone redirection
- Multimedia conferencing
- Windows Media Redirection

If a webcam supports H.264 hardware encoding, HDX video compression uses the hardware encoding by default. Hardware encoding uses additional bandwidth and is not suitable for a low bandwidth network. To force software compression over low bandwidth networks, add the following DWORD key value to the registry key: HKCU\Software\Citrix\HdxRealTime: DeepCompress\_ForceSWEncode=1.

For deployments where server scalability is of greater concern than user experience, you can use the legacy graphics system by adding the Legacy graphics mode policy setting and configuring the individual legacy graphics policy settings. Use of the legacy graphics system affects the user experience over WAN and mobile connections.

# Thinwire 兼容模式

Oct 03, 2016

Thinwire Compatibility Mode uses new screen decomposition and caching techniques, which achieve low bandwidth usage and high server scalability without compromising the end-user experience.

Thinwire Compatibility Mode includes the following features:

- Intelligent bitmap matching for a bitmap-only provider.
  - Bitmap translation analysis for efficient window movement and scrolling.
- Backwards compatible. There is no requirement for client or Citrix Receiver upgrades or hardware acceleration.
  - Tested on a range of older thin clients up to and over 5 years old.
- Optimized for very low server CPU usage and improved server scalability.
- An emulated 16-bit mode, which reduces bandwidth by a further 15-20% for typical workloads.
- Transient detection for server-rendered video content.
  - Multi-transient handling for an improved multimedia experience. For example, when watching multiple videos or ticker tapes.
  - Selective sharpening for regions that leave a transient state.
- Optimized for CloudBridge acceleration. In tests, we have seen up to a 6:1 ratio of bandwidth reduction on Office-type workloads.
- Adaptive display, which can be tuned through policy settings. For more information see [Moving image compression in Moving image policy settings](#).
- VDA's and Windows OS's up to and including Windows 10 VDA are supported.
- New "Build to Lossless" mode for 3D Pro, which improves responsiveness, interactivity, and interruptible sharpening for a better user experience on low bandwidth.
- Default static photographic imagery quality is higher than in Legacy Graphics Mode.

For Visual Quality settings "Low", "Medium" (default) and "High", the transient detector dynamically evaluates screen updates to decide whether highly-animated areas should be sent at lower quality, in accordance with the Adaptive Display policy, to improve client performance and reduce bandwidth usage.

For the **Build to lossless** visual quality, Thinwire Compatibility Mode uses a "fuzzy-first" approach for large screen updates. This setting is targeted at 3D Pro users who are manipulating 3D models or other graphic-intensive applications. If the activity continues, a transient mode is assumed and the affected area is sharpened and cached once transient activity stops. For the initial large change, some lightweight image analysis is performed on the change area to determine whether to use "fuzzy transient" or "sharp transient" (lossless) - for example, when rotating a wireframe. It is more efficient, for FPS (Frames Per Second) and bandwidth, to encode simple imagery using the Citrix lossless codec and no loss in quality occurs.

The sharpen-to-lossless step in Build to lossless is also different. Rather than sharpening the affected area in one step, the area is sharpened in pre-determined blocks to help maintain interactivity and a smooth user experience. Sharpening a large change area mid-transient, for example moving a 3D model which is stopped briefly, then moved again, would previously cause a "stall", especially over a low bandwidth line. The size of the sharpening blocks depends on how far the quality was reduced to try and maintain the target minimum frame rate, which is an Adaptive Display policy setting. If the quality was significantly reduced, the sharpening block size will be smaller, with a minimum size of 128 x 128 pixels. If the quality was not reduced, for example, when the client has adequate processing power and bandwidth, the sharpening block size can be a maximum size of 384 x 384 pixels.

# HDX 3D Pro

Oct 03, 2016

HDX 3D Pro enables you to deliver desktops and applications that perform best with a graphics processing unit (GPU) for hardware acceleration, including 3D professional graphics applications based on OpenGL and DirectX. (The standard VDA supports GPU acceleration of DirectX only.)

Examples of 3D professional applications include:

- Computer-aided design, manufacturing, and engineering (CAD/CAM/CAE) applications
- Geographical Information System (GIS) software
- Picture Archiving Communication System (PACS) for medical imaging
- Applications using the latest OpenGL, DirectX, NVidia CUDA, and OpenCL versions
- Computationally-intensive non-graphical applications that use NVIDIA Compute Unified Device Architecture (CUDA) GPUs for parallel computing

HDX 3D Pro provides the best user experience over any bandwidth:

- On wide area network (WAN) connections: Deliver an interactive user experience over WAN connections with bandwidths as low as 1.5 Mbps.
- On local area network (LAN) connections: Deliver a user experience equivalent to that of a local desktop on LAN connections with bandwidths of 100 Mbps.

You can replace complex and expensive workstations with simpler user devices by moving the graphics processing into the data center for centralized management.

HDX 3D Pro provides GPU acceleration for Windows Desktop OS machines and Windows Server OS machines. When used with Citrix XenServer and NVIDIA GRID GPUs, HDX 3D Pro provides Virtual GPU (vGPU) acceleration for Windows Desktop OS machines. For the supported XenServer versions, see [Citrix Virtual GPU Solution](#).

Use the HDX Monitor tool (which replaces the Health Check tool) to validate the operation and configuration of HDX visualization technologies and to diagnose and troubleshoot HDX issues. To download the tool and learn more about it, see <https://taas.citrix.com/hdx/download/>.

# Flash 重定向

May 25, 2017

Flash Redirection offloads the processing of most Adobe Flash content (including animations, videos, and applications) to users' LAN- and WAN-connected Windows devices, which reduces server and network load. This results in greater scalability while ensuring a high definition user experience. Configuring Flash Redirection requires both server-side and client-side settings.

Caution: Flash Redirection involves significant interaction between the user device and server components. Use this feature only in environments where security separation between the user device and server is not required. Additionally, configure user devices to use this feature only with trusted servers. Because Flash Redirection requires the Flash Player to be installed on the user device, enable this feature only if the Flash Player itself is secured.

The legacy and second generation versions of Flash Redirection are independent solutions and run in separate virtual channels.

- Legacy Flash Redirection features are supported on the client side only. If an earlier version of the Flash Player is installed on the user device, or if the Flash Player cannot be installed, Flash content renders on the server.
- Second generation Flash Redirection is supported on both clients and servers. If the client supports second generation Flash Redirection, Flash content renders on the client. Second generation Flash Redirection features include support for user connections over WAN, intelligent fallback, and a URL compatibility list; see below for details.

Flash Redirection uses Windows event logging on the server to log Flash events. The event log indicates whether Flash Redirection is being used and provides details about issues. The following are common to all events logged by Flash Redirection:

- Flash Redirection reports events to the Application log.
- On Windows 8 and Windows 7 systems, a Flash Redirection-specific log appears in the Applications and Services Logs node.
- The Source value is Flash.
- The Category value is None.

For the latest updates to HDX Flash compatibility, see Knowledge Center article [CTX136588](#).

To configure Flash Redirection on the server, use the following Citrix policy settings. For details, see [Flash Redirection policy settings](#).

- Flash default behavior establishes the default behavior of Flash acceleration. By default, Flash Redirection is enabled. To override this default behavior for individual web pages and Flash instances, use the Flash URL compatibility list setting.
- Flash intelligent fallback - detects instances of small Flash movies (such as those frequently used to play advertisements) and renders them on the server instead of redirecting them for rendering on the user device. It does not cause any interruption or failure in the loading of the web page or the Flash application. By default, Flash intelligent fallback is enabled. To redirect all instances of Flash content for rendering on the user device, disable this policy setting.
- Flash server-side content fetching URL list allows you to specify websites whose Flash content can be downloaded to the server and then transferred to the user device for rendering. (By default, Flash Redirection downloads Flash content to the user device, where it is played.) This setting works with (and requires) the Enable server-side content fetching setting on the user device and is intended for use with Intranet sites and internal Flash applications; see below for details. It also works with most Internet sites and can be used when the user device does not have direct access to the Internet (for example, when the XenApp or XenDesktop server provides that connection).

Note: Server-side content fetching does not support Flash applications using Real Time Messaging Protocols (RTMP); instead, server-side rendering is used, which supports HTTP and HTTPS.

- Flash URL compatibility list - specifies where Flash content from listed websites is rendered: on the user device, on the server, or blocked.
- Flash background color list - enables you to match the colors of web pages and Flash instances, which improves the appearance of the web page when using Flash Redirection.

Install Citrix Receiver and Adobe Flash Player on the user device. No further configuration is required on the user device.

You can change the default settings using Active Directory Group Policy Objects. Import and add the HDX MediaStream Flash Redirection - Client administrative template (HdxFlashClient.adm), which is available in the following folders:

- For 32-bit computers: %Program Files%\Citrix\ICA Client\Configuration\language
- For 64-bit computers: %Program Files (x86)%\Citrix\ICA Client\Configuration\language

The policy settings appear under Administrative Templates > Classic Administrative Templates (ADM) > HDX MediaStream Flash Redirection - Client. See the Microsoft Active Directory documentation for details about GPOs and templates.

#### **Change when Flash Redirection is used**

Together with server-side settings, the Enable HDX MediaStream Flash Redirection on the user device policy setting controls whether Adobe Flash content is redirected to the user device for local rendering. By default, Flash Redirection is enabled and uses intelligent network detection to determine when to play Flash content on the user device.

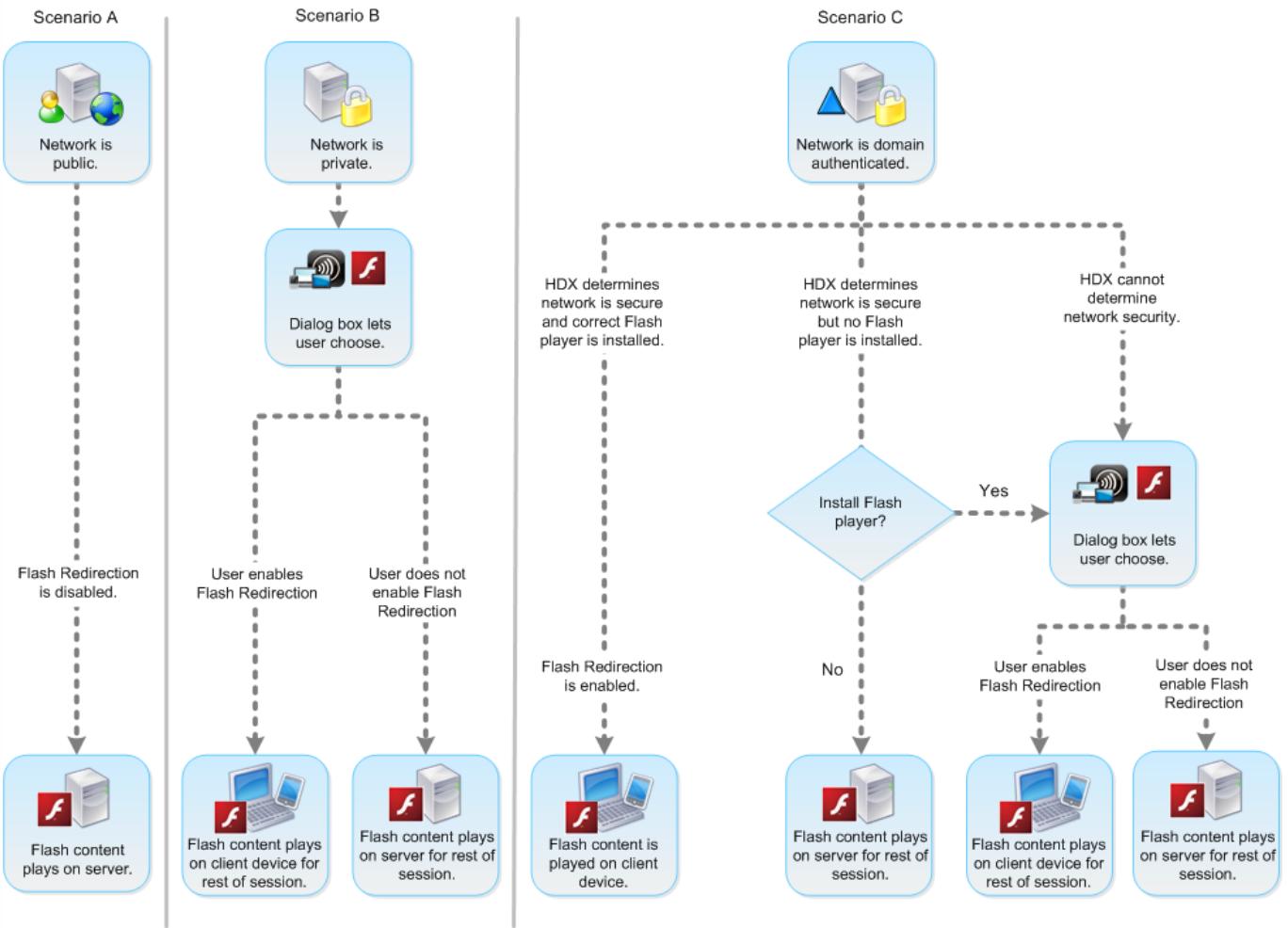
If no configuration is set and Desktop Lock is used, Flash Redirection is enabled on the user device by default.

To change when Flash Redirection is used or to disable Flash Redirection on the user device:

1. From the Setting list, select Enable HDX MediaStream Flash Redirection on the user device and click policy setting.
2. Select Not Configured, Enabled (the default), or Disabled.
3. If you select Enabled, choose an option from the Use HDX MediaStream Flash Redirection list:
  - To use the latest Flash Redirection functionality when the required configuration is present, and revert to server-side rendering when it is not, select Only with Second Generation.
  - To always use Flash Redirection, select Always. Flash content plays on the user device.
  - To never use Flash Redirection, select Never. Flash content plays on the server.
  - To use intelligent network detection to assess the security level of the client-side network to determine when using Flash Redirection is appropriate, select Ask (the default). If the security of the network cannot be determined, the user is asked whether to use Flash Redirection. If the network security level cannot be determined, the user is prompted to choose whether to use Flash Redirection.

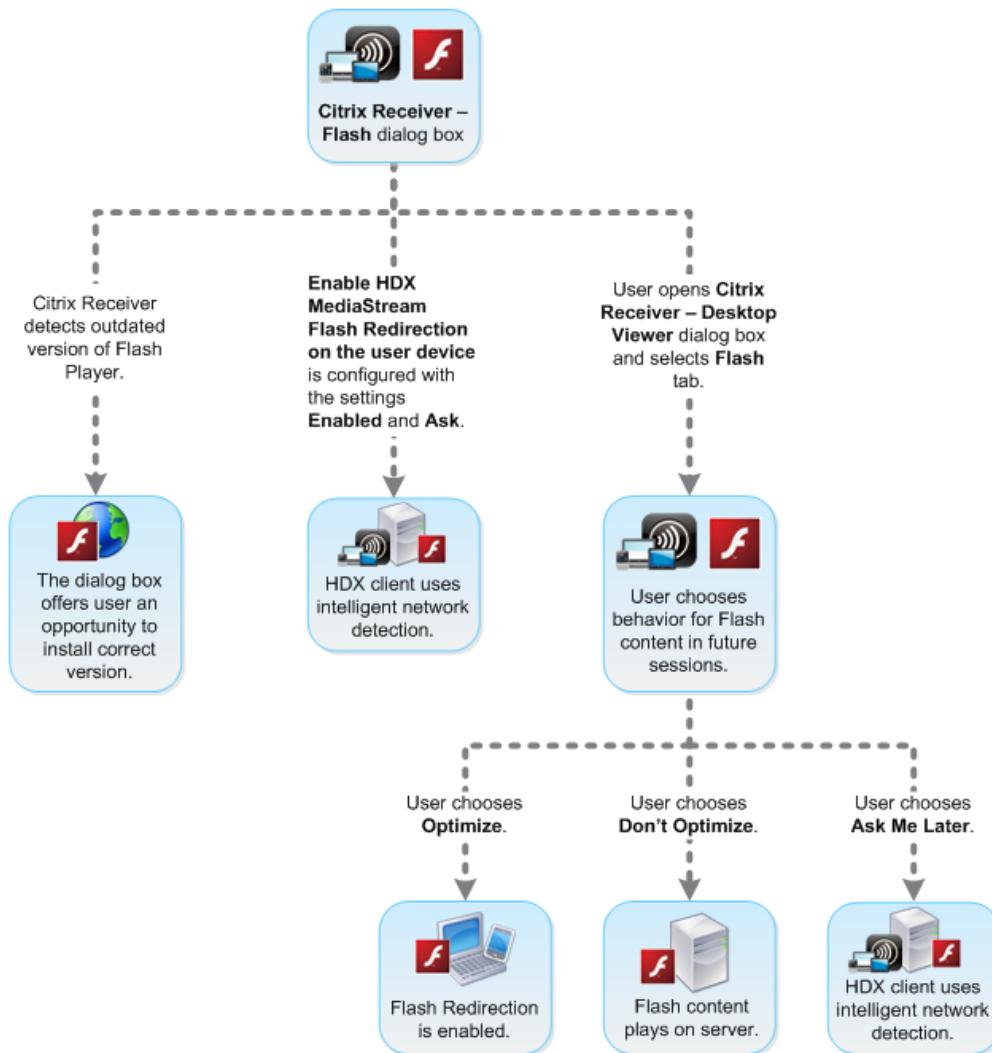
The following illustration indicates how Flash Redirection is handled for various network types.

## Intelligent Network Detection for Flash Redirection



Users can override intelligent network detection from the Citrix Receiver - Desktop Viewer Preferences dialog box by selecting Optimize or Don't Optimize in the Flash tab. The choices available vary depending on how Flash Redirection is configured on the user device, as shown in the following illustration.

## User control of Flash redirection



### Synchronize client-side HTTP cookies with the server-side

Synchronization of the client-side HTTP cookies with the server-side is disabled by default. Enable synchronization to download HTTP cookies from the server; those HTTP cookies are then used for client-side content fetching and are available as needed by sites containing Flash content.

Note: Client-side cookies are not replaced during the synchronization; they remain available even if the synchronization policy is later disabled.

1. From the Setting list, select Enable synchronization of the client-side HTTP cookies with the server-side and click policy setting.
2. Select Not Configured, Enabled, or Disabled (the default).

### Enable server-side content fetching

By default, Flash Redirection downloads Adobe Flash content to the user device, where it is played. Enabling server-side content fetching causes the Flash content to download to the server and then be sent to the user device. Unless there is an overriding policy (such as a site blocked with the Flash URL compatibility list policy setting), the Flash content plays on the user device.

Server-side content fetching is frequently used when the user device connects to internal sites through NetScaler Gateway and when the user device does not have direct access to the Internet.

Note: Server-side content fetching does not support Flash applications using Real Time Messaging Protocols (RTMP). Instead, server-side rendering is used for such sites.

Second generation Flash Redirection supports three enabling options for server-side content fetching. Two of these options include the ability to cache server-side content on the user device, which improves performance because content that is reused is already available on the user device for rendering. The contents of this cache are stored separately from other HTTP content cached on the user device.

With second generation Flash redirection, fallback to server-side content fetching begins automatically when any of the enabling options is selected and client-side fetching of .swf files fails.

Enabling server-side content fetching requires settings on both the client device and the server.

1. From the Setting list, select Enable server-side content fetching and click policy setting.
2. Select Not Configured, Enabled, or Disabled (the default). If you enable this setting, choose an option from the Server-side content fetching state list:

Option	Description
Disabled	Disables server-side content fetching, overriding the Flash server-side content fetching URL list setting on the server. Server-side content fetching fallback is also disabled.
Enabled	Enables server-side content fetching for web pages and Flash applications identified in the Flash server-side content fetching URL list. Server-side content fetching fallback is available, but Flash content is not cached.
Enabled (persistent caching)	Enables server-side content fetching for web pages and Flash applications identified in the Flash server-side content fetching URL list. Server-side content fetching fallback is available. Content obtained through server-side fetching is cached on the user device and stored from session to session.
Enabled (temporary caching)	Enables server-side content fetching for web pages and Flash applications identified in the Flash server-side content fetching URL list. Server-side content fetching fallback is available. Content obtained through server-side fetching is cached on the user device and deleted at the end of the session.

3. On the server, enable the Flash server-side content fetching URL list policy setting and populate it with target URLs.

#### Redirect user devices to other servers for client-side content fetching

To redirect an attempt to obtain Flash content, use the URL rewriting rules for client-side content fetching setting, which is a second generation Flash Redirection feature. When configuring this feature, you provide two URL patterns; when the user device attempts to fetch content from a website matching the first pattern (the URL match pattern), it is redirected to the website specified by the second pattern (the rewritten URL format).

You can use this setting to compensate for content delivery networks (CDN). Some websites delivering Flash content use CDN redirection to enable the user to obtain the content from the nearest of a group of servers containing the same content. When using Flash Redirection client-side content fetching, the Flash content is requested from the user device, while the rest of the web page on which the Flash content resides is requested by the server. If CDN is in use, the server request is redirected to the nearest server, and the user device request follows to the same location. This may not be the location closest to the user device; depending on distance, there could be a noticeable delay between the loading of the web page and the playing of the Flash content.

1. From the Setting list, select URL rewriting rules for client-side content fetching and click policy setting.
2. Select Not Configured, Enabled, or Disabled. Not Configured is the default; Disabled causes any URL rewriting rules specified in the next step to be ignored.
3. If you enable the setting, click Show. Using Perl regular expression syntax, type the URL match pattern in the Value name box and the rewritten URL format in the Value box.

You can add registry settings to specify the minimum version required for Flash redirection for client devices accessing VDAs using Receiver for Windows or Receiver for Linux.

## 警告

Editing the Registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

**ServerFlashPlayerVersionMinimum** is a string value that specifies the minimum version of the Flash Player required on the ICA Server (VDA).

**ClientFlashPlayerVersionMinimum** is a string value that specifies the minimum version of the Flash Player required on the ICA Client (Citrix Receiver).

These version strings can be specified as "10" or "10.2" or "10.2.140". Currently, only the major, minor and build numbers will be compared. The revision number will be ignored. For example, for a version string specified as "10" with only the major number specified, the minor and build numbers will be assumed to be zero.

**FlashPlayerVersionComparisonMask** is a DWORD value that when set to zero will disable comparing the version of the Flash Player on the ICA Client against the Flash Player on the ICA Server. The comparison mask has other values, but these should not be used because the meaning of any non-zero mask may change. It is recommended to only set the comparison mask to zero for the desired clients. It is not recommended to set the comparison mask under the client agnostic settings. If a comparison mask is not specified, Flash redirection will require that the ICA Client has a Flash Player with greater or equal version to the Flash Player on the ICA Server. It will do so by comparing only the major version number of the Flash Player.

In order for redirection to occur the client and server minimum checks need to be successful in addition to the check using the comparison mask.

The subkey ClientID0x51 specifies the Linux ICA Client. The subkey ClientID0x1 specifies the Windows ICA Client. This subkey is named by appending the hexadecimal Client Product ID (without any leading zeros) to the string "ClientID". A full list of Client IDs can be found in the Mobile SDK for Windows Apps documentation <https://www.citrix.com/community/citrix-developer/mobile-sdk-for-windows-apps.html>.

### 32-bit VDA example registry configuration

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer] Client agnostic settings

"ClientFlashPlayerVersionMinimum"="13.0" Minimum version required for the ICA client

"ServerFlashPlayerVersionMinimum"="13.0" Minimum version required for the ICA server

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x1] Windows ICA

## Client settings

"ClientFlashPlayerVersionMinimum"="16.0.0" This specifies the minimum version of the Flash Player required for the Windows client [HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x51] Linux ICA Client settings

"FlashPlayerVersionComparisonMask"=dword:00000000 This disables the version comparison-check for the linux client (checking to see that the client has a more recent Flash Player than the server) "ClientFlashPlayerVersionMinimum"="11.2.0" This specifies the minimum version of the Flash Player for the Linux client.

## 64-bit VDA example registry configuration

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer]
"ClientFlashPlayerVersionMinimum"="13.0" "ServerFlashPlayerVersionMinimum"="13.0"
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x1]
"ClientFlashPlayerVersionMinimum"="16.0.0"
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Server\PseudoServer\ClientID0x51]
"FlashPlayerVersionComparisonMask"=dword:00000000 "ClientFlashPlayerVersionMinimum"="11.2.0"
```

# 主机到客户端重定向

Oct 03, 2016

Content redirection allows you to control whether users access information with applications published on servers or with applications running locally on user devices.

**Host to client redirection** is one kind of content redirection. It is supported only on Server OS VDAs (not Desktop OS VDAs).

- When host to client redirection is enabled, URLs are intercepted at the server VDA and sent to the user device. The web browser or multimedia player on the user device opens these URLs.
- If you enable host to client redirection and the user device fails to connect to a URL, the URL is redirected back to the server VDA.
- When host to client redirection is disabled, users open the URLs with web browsers or multimedia players located on the server VDA.
- When host to client redirection is enabled, users cannot disable it.

Host to client redirection was previously known as **server to client redirection**.

You might consider using host to client redirection in specific but uncommon cases, for performance, compatibility, or compliance. Normally, other forms of content redirection are better.

## Performance

You can use host to client redirection for performance, so that whenever an application is installed on the user device, it is used in preference to an application on the VDA.

Keep in mind that host to client redirection will improve performance only under specific conditions, because the VDA already optimizes Adobe Flash and other types of multimedia content. First, consider using the other approaches (policy settings) noted in the tables below, rather than host to client redirection; they offer more flexibility and usually give a better user experience, particularly for less-powerful user devices.

## Compatibility

You can use host to client redirection for compatibility in the following use cases:

- You use content types other than HTML or multimedia (for example, a custom URL type).
- You use a legacy media format (such as Real Media) that is not supported by the VDA's multimedia player with multimedia redirection.
- The application for the content type is used by only a small number of users who already have the application installed on their user device.
- The VDA cannot access certain web sites (for example, web sites internal to another organization).

## Compliance

You can use host to client redirection for compliance in the following use cases:

- The application or content licensing agreement does not permit publishing via the VDA.

- Organizational policy does not permit a document being uploaded to the VDA.

Some situations are more likely in complex environments, and also if the user device and the VDA belong to different organizations.

Environments may have many different types of user devices.

User device	Situation or environment	Content redirection approach
Tablet	-	Any approach (see next table)
Laptop PC	-	Any approach (see next table)
Desktop PC	Users use a wide range of apps installed on the user device	Any approach (see next table)
Desktop PC	Users use only a few known apps that are installed on the user device	Local App Access
Desktop PC	Users use no apps installed on the user device	Multimedia redirection and/or Flash redirection
Desktop appliance	Vendor supports multimedia redirection and/or Flash redirection	Multimedia redirection and/or Flash redirection
Thin client	Vendor supports multimedia redirection, Flash redirection, and host to client redirection	Any approach (see next table)
Zero client	Vendor supports multimedia redirection and/or Flash redirection	Multimedia redirection and/or Flash redirection

Use the following examples to help guide your content redirection approach.

URLs link	Situation or environment	Content redirection approach
A web page or document	The VDA cannot access the URL	Host to client redirection
A web page	The web page contains Adobe Flash	Flash redirection

A multimedia file or stream	The VDA has a compatible multimedia player	Multimedia redirection
A multimedia file or stream	The VDA does not have a compatible multimedia player	Host to client redirection
A document	The VDA does not have an application for that document type	Host to client redirection
A document	The document must not be downloaded to the user device	No redirection
A document	The document must not be uploaded to the VDA	Host to client redirection
A custom URL type	The VDA does not have an application for that custom URL type	Host to client redirection

Host to client redirection is supported by Citrix Receiver for Windows, Receiver for Mac, Receiver for Linux, Receiver for HTML5, and Receiver for Chrome.

To use host to client redirection, the user device must have a web browser, multimedia player, or other application that is suitable for the content. If the user device is a desktop appliance, thin client, or zero client, confirm that it has suitable applications and is sufficiently powerful.

User devices enabled for Local App Access use a different mechanism for content redirection, and do not require host to client content redirection.

You can use Citrix policies to prevent host to client content redirection for unsuitable devices.

Host to client redirection is used when URLs are:

- Embedded as hyperlinks in an application (for example, in an email message or document).
- Selected through a VDA application's menus or dialogs, provided that the application uses the Windows ShellExecuteEx API.
- Entered in the Windows Run dialog.

Host to client redirection is not used for URLs in a web browser (either in a web page or entered in the address bar of the web browser).

## 注意

If users change their default web browser on the VDA (for example, by using Set Default Programs), that change can interfere with host to client redirection for applications.

When host to client content redirection is enabled, the app that is used to open the URL depends on the configuration of the user device for both the URL type and the content type. For example:

- An HTTP URL with an HTML content type will open in the default web browser.
- An HTTP URL with a PDF content type might open in the default web browser, or it might open in another application.

This user device configuration is not controlled by host to client content redirection. If you do not control the configuration of the user device, consider using Flash redirection and multimedia redirection, rather than host to client content redirection.

The following URL types are opened locally through user devices when host to client redirection is enabled:

- HTTP (Hypertext Transfer Protocol)
- HTTPS (Secure Hypertext Transfer Protocol)
- RTSP (Real Player and QuickTime)
- RTSPU (Real Player and QuickTime)
- PNM (Legacy Real Player)
- MMS (Microsoft Media Format)

You can change the list of URL types for host to client redirection, to remove and add URL types, including custom URL types.

Enabling host to client redirection starts with enabling a Citrix policy setting.

The Host to client redirection policy setting is located in the [File Redirection policy settings](#) section. By default, this setting is disabled.

In addition, you may need to set registry keys and Group Policy for the server VDAs, depending on the VDA's OS.

- If the server VDA is Windows Server 2008 R2 SP1, you do not need to set registry keys or Group Policy.
- If the server VDA is Windows Server 2012, Windows Server 2012 R2, or Windows Server 2016, you must set registry keys and Group Policy.

## 警告

Using Registry Editor incorrectly can cause serious problems that might require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

1. Copy the text between "Reg file start" and "Reg file end" below, and paste it in Notepad.
2. Save the Notepad file with "Save As" as type All Files and the name ServerFTA.reg.
3. Distribute the **ServerFTA.reg** file to the servers using Active Directory Group Policy.

**- Reg file start --**

Windows Registry Editor Version 5.00

[HKEY\_CLASSES\_ROOT\ServerFTAHTML\shell\open\command]

@= "\"C:\\Program Files (x86)\\Citrix\\system32\\iexplore.exe\" %1"

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ServerFTA]

@="ServerFTA"

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ServerFTA\Capabilities]

"ApplicationDescription"="Server FTA URL."

"ApplicationIcon"="C:\\Program Files (x86)\\Citrix\\system32\\iexplore.exe,0"

"ApplicationName"="ServerFTA"

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ServerFTA\Capabilities\URLAssociations]

"http"="ServerFTAHTML"

"https"="ServerFTAHTML"

[HKEY\_LOCAL\_MACHINE\SOFTWARE\RegisteredApplications]

"Citrix.ServerFTA"="SOFTWARE\\Citrix\\ServerFTA\\Capabilities"

**-- Reg file end --**

Create an XML file. Copy the text between "xml file start" and "xml file end" below, paste it in the XML file, and then save the file as **ServerFTAdefaultPolicy.xml**.

```
-- xml file start --

<?xml version="1.0" encoding="UTF-8"?>

<DefaultAssociations>

<Association Identifier="http" ProgId="ServerFTAHTML" ApplicationName="ServerFTA" />

<Association Identifier="https" ProgId="ServerFTAHTML" ApplicationName="ServerFTA" />

</DefaultAssociations>

-- xml file end --
```

From the current Group Policy Management Console, navigate to: **Computer configuration > Administrative Templates > Windows Components > File Explorer > Set a default associations configuration file**, and provide the ServerFTAdefaultPolicy.xml file you created.

To change the list of URL types for host to client redirection, set the following registry key on the server VDA.

Key: HKLM\Software\Wow6432Node\Citrix\SFTA

To remove URL types from the list, set DisableServerFTA and NoRedirectClasses:

Name: DisableServerFTA

Type: REG\_DWORD

Data: 1

Name: NoRedirectClasses

Type: REG\_MULTI\_SZ

Data: Specify any combination of the values: http, https, rtsp, rtspu, pnm, or mms. Enter multiple values on separate lines. For example:

http

https

rtsp

To add URL types to the list, set ExtraURLProtocols:

Name: ExtraURLProtocols

Type: REG\_MULTI\_SZ

Data: Specify any combination of URL types. Each URL type must include the // suffix; separate multiple values with semicolons. For example:

customtype1://;customtype2://

To enable host to client redirection for a specific set of web sites, set the following registry key on the server VDA.

Key: HKLM\Software\Wow6432Node\Citrix\SFTA

Name: ValidSites

Type: REG\_MULTI\_SZ

Data: Specify any combination of fully-qualified domain names (FQDNs). Enter multiple FQDNs on separate lines. An FQDN may include a wildcard in the leftmost position only. This matches a single level of domain, which is consistent with the rules in RFC 6125. For example:

www.example.com

\*.example.com

# 适用于 Windows 桌面操作系统的 GPU 加速

May 28, 2016

With HDX 3D Pro you can deliver graphically intensive applications as part of hosted desktops or applications on Desktop OS machines. HDX 3D Pro supports physical host computers (including desktop, blade, and rack workstations) and XenServer VMs with GPU Passthrough and XenServer VMs with Virtual GPU (vGPU).

Using XenServer GPU Passthrough, you can create VMs with exclusive access to dedicated graphics processing hardware. You can install multiple GPUs on the hypervisor and assign VMs to each of these GPUs on a one-to-one basis.

Using XenServer vGPU, multiple virtual machines can directly access the graphics processing power of a single physical GPU. The true hardware GPU sharing provides full Windows 7 or Windows 2008 R2 SP1 desktops suitable for users with complex and demanding design requirements. Supported for NVIDIA GRID K1 and K2 cards, the GPU sharing uses the same NVIDIA graphics drivers that are deployed on non-virtualized operating systems.

HDX 3D Pro offers the following features:

- Adaptive H.264-based deep compression for optimal WAN and wireless performance. HDX 3D Pro uses CPU-based deep compression as the default compression technique for encoding. This provides optimal compression that dynamically adapts to network conditions.  
The H.264-based deep compression codec no longer competes with graphics rendering for CUDA cores on the NVIDIA GPU. The deep compression codec runs on the CPU and provides bandwidth efficiency.
- Lossless compression option for specialized use cases. HDX 3D Pro also offers a CPU-based lossless codec to support applications where pixel-perfect graphics are required, such as medical imaging. Lossless compression is recommended only for specialized use cases because it consumes significantly more network and processing resources.

When using lossless compression:

- The lossless indicator, a system tray icon, notifies the user if the screen displayed is a lossy frame or a lossless frame. This helps when the Visual Quality policy setting specifies Build to lossless. The lossless indicator turns green when the frames sent are lossless.
- The lossless switch enables the user to change to Always Lossless mode anytime within the session. To select or deselect Lossless anytime within a session, right-click the icon or use the shortcut ALT+SHIFT+1.

For lossless compression: HDX 3D Pro uses the lossless codec for compression regardless of the codec selected through policy.

For lossy compression: HDX 3D Pro uses the original codec, either the default or the one selected through policy.

Lossless switch settings are not retained for subsequent sessions. To use lossless codec for every connection, select Always lossless in the Visual quality policy setting.

- You can override the default shortcut, ALT+SHIFT+1, to select or deselect Lossless within a session. Configure a new registry setting at HKLM\SOFTWARE\Citrix\HDX3D\LLIndicator.
  - Name: HKLM\_HotKey, Type: String
  - The format to configure a shortcut combination is C=0|1, A=0|1, S=0|1, W=0|1, K=val. Keys must be comma "," separated. The order of the keys does not matter.
  - A, C, S, W and K are keys, where C=Control, A=ALT, S=SHIFT, W=Win, and K=a valid key. Allowed values for K are 0-9, a-z, and any virtual key code. For more information on virtual key codes, see [Virtual-Key Codes](#) on MSDN.
  - For example:
    - For F10, set K=0x79
    - For Ctrl + F10, set C=1, K=0x79
    - For Alt + A, set A=1, K=a or A=1, K=A or K=A, A=1
    - For Ctrl + Alt + 5, set C=1, A=1, K=5 or A=1, K=5, C=1
    - For Ctrl + Shift + F5, set A=1, S=1, K=0x74

**Caution:** Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

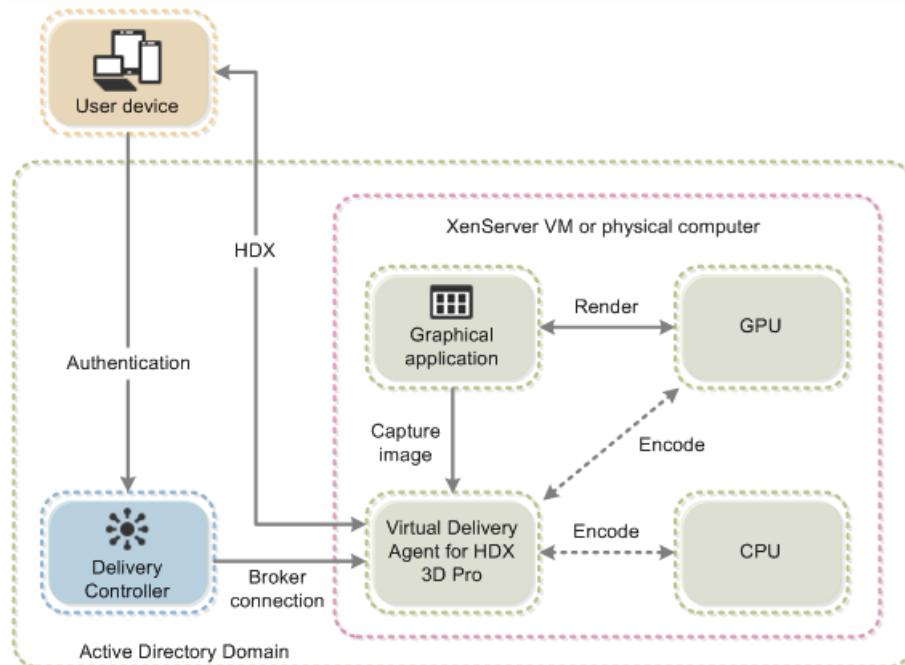
- Multiple and high resolution monitor support. For Windows 7 and Windows 8 desktops, HDX 3D Pro supports user devices with up to four monitors. Users can arrange their monitors in any configuration and can mix monitors with different resolutions and orientations. The number of monitors is limited by the capabilities of the host computer GPU, the user device, and the available bandwidth. HDX 3D Pro supports all monitor resolutions and is limited only by the capabilities of the GPU on the host computer.  
HDX 3D Pro also provides limited support for dual-monitor access to Windows XP desktops. For more information about this, see [VDAs on machines running Windows XP or Windows Vista](#).
- Dynamic resolution. You can resize the virtual desktop or application window to any resolution. **Note:** The only supported method to change the resolution is by

resizing the VDA session window. Changing resolution from within the VDA session (using Control Panel > Appearance and Personalization > Display > Screen Resolution) is not supported.

- Support for NVIDIA Kepler architecture. HDX 3D Pro supports NVIDIA GRID K1 and K2 cards for GPU passthrough and GPU sharing. NVIDIA GRID vGPU enables multiple VMs to have simultaneous, direct access to a single physical GPU, using the same NVIDIA graphics drivers that are deployed on non-virtualized operating systems.
- Support for VMware vSphere and VMware ESX using Virtual Direct Graphics Acceleration (vDGA) - You can use HDX 3D Pro with vDGA for both RDS and VDI workloads. When using HDX 3D Pro with Virtual Shared Graphics Acceleration (vSGA), support is limited to one monitor. Using vSGA with large 3D models can result in performance issues due to its use of API intercept technology. For more information, see [VMware vSphere 5.1 - Citrix Known Issues](#).

As shown in the following figure:

- The host computer must reside within the same Active Directory domain as the Delivery Controller.
  - When a user logs on to Citrix Receiver and accesses the virtual application or desktop, the Controller authenticates the user and contacts the VDA for HDX 3D Pro to broker a connection to the computer hosting the graphical application.
- The VDA for HDX 3D Pro uses the appropriate hardware on the host to compress views of the complete desktop or of just the graphical application.
- The desktop or application views and the user interactions with them are transmitted between the host computer and the user device through a direct HDX connection between Citrix Receiver and the VDA for HDX 3D Pro.



When you use the installer's graphical interface to install a VDA for Windows Desktop OS, simply select Yes on the HDX 3D Pro page. When using the command line interface, include the /enable\_hdx\_3d\_pro option with the XenDesktop VdaSetup.exe command.

To upgrade HDX 3D Pro, uninstall both the separate HDX 3D for Professional Graphics component and the VDA before installing the VDA for HDX 3D Pro. Similarly, to switch from the standard VDA for Windows Desktop OS to the HDX 3D Pro VDA, uninstall the standard VDA and then install the VDA for HDX 3D Pro.

The NVIDIA GRID API provides direct access to the frame buffer of the GPU, providing the fastest possible frame rate for a smooth and interactive user experience. If you install NVIDIA drivers before you install a VDA with HDX 3D Pro, NVIDIA GRID is enabled by default.

To enable NVIDIA GRID on a VM, disable Microsoft Basic Display Adapter from the Device Manager. Run the following

command and then restart the VDA: Montereyenable.exe -enable -noreset

If you install NVIDIA drivers after you install a VDA with HDX 3D Pro, NVIDIA GRID is disabled. Enable NVIDIA GRID by using the Montereyenable tool provided by NVIDIA.

To disable NVIDIA GRID, run the following command and then restart the VDA: Montereyenable.exe -disable -noreset

To use HDX 3D Pro with multiple monitors, ensure that the host computer is configured with at least as many monitors as are attached to user devices. The monitors attached to the host computer can be either physical or virtual.

Do not attach a monitor (either physical or virtual) to a host computer while a user is connected to the virtual desktop or application providing the graphical application. Doing so can cause instability for the duration of a user's session.

Let your users know that changes to the desktop resolution (by them or an application) are not supported while a graphical application session is running. After closing the application session, a user can change the resolution of the Desktop Viewer window in the Citrix Receiver - Desktop Viewer Preferences.

When multiple users share a connection with limited bandwidth (for example, at a branch office), Citrix recommends that you use the Overall session bandwidth limit policy setting to limit the bandwidth available to each user. This ensures that the available bandwidth does not fluctuate widely as users log on and off. Because HDX 3D Pro automatically adjusts to make use of all the available bandwidth, large variations in the available bandwidth over the course of user sessions can negatively impact performance.

For example, if 20 users share a 60 Mbps connection, the bandwidth available to each user can vary between 3 Mbps and 60 Mbps, depending on the number of concurrent users. To optimize the user experience in this scenario, determine the bandwidth required per user at peak periods and limit users to this amount at all times.

For users of a 3D mouse, Citrix recommends that you increase the priority of the Generic USB Redirection virtual channel to 0. For information about changing the virtual channel priority, see Knowledge Center article [CTX128190](#).

# Windows Server 操作系统 GPU 加速

May 28, 2016

HDX 3D Pro allows graphics-heavy applications running in Windows Server OS sessions to render on the server's graphics processing unit (GPU). By moving OpenGL, DirectX, Direct3D, and Windows Presentation Foundation (WPF) rendering to the server's GPU, the server's CPU is not slowed by graphics rendering. Additionally, the server is able to process more graphics because the workload is split between the CPU and GPU.

When using HDX 3D Pro, multiple users can share graphics cards. When HDX 3D Pro is used with XenServer GPU Passthrough, a single server hosts multiple graphics cards, one per virtual machine.

For procedures that involve editing the registry, use caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

GPU Sharing enables GPU hardware rendering of OpenGL and DirectX applications in remote desktop sessions; it has the following characteristics:

- Can be used on bare metal or virtual machines to increase application scalability and performance.
- Enables multiple concurrent sessions to share GPU resources (most users do not require the rendering performance of a dedicated GPU).
- Requires no special settings.

You can install multiple GPUs on a hypervisor and assign VMs to each of these GPUs on a one-to-one basis: either install a graphics card with more than one GPU, or install multiple graphics cards with one or more GPUs each. Mixing heterogeneous graphics cards on a server is not recommended.

Virtual machines require direct passthrough access to a GPU, which is available with Citrix XenServer or VMware vSphere. When HDX 3D Pro is used with GPU Passthrough, each GPU in the server supports one multi-user virtual machine.

GPU Sharing does not depend on any specific graphics card.

- When running on a hypervisor, select a hardware platform and graphics cards that are compatible with your hypervisor's GPU Passthrough implementation. The list of hardware that has passed certification testing with XenServer GPU Passthrough is available at [GPU Passthrough Devices](#).
- When running on bare metal, it is recommended to have a single display adapter enabled by the operating system. If multiple GPUs are installed on the hardware, disable all but one of them using Device Manager.

Scalability using GPU Sharing depends on several factors:

- The applications being run
- The amount of video RAM they consume
- The graphics card's processing power

For example, scalability figures in the range of 8-10 users have been reported on NVIDIA Q6000 and M2070Q cards running applications such as ESRI ArcGIS. These cards offer 6 GB of video RAM. Newer NVIDIA GRID cards offer 8 GB of video RAM and significantly higher processing power (more CUDA cores). With the NVIDIA GRID K2 cards, good performance has been observed with up to 20 users per GRID K2 card. Other applications may scale much higher, achieving 32 concurrent users on a high-end GPU.

Some applications handle video RAM shortages better than others. If the hardware becomes extremely overloaded, this could cause instability or a crash of the graphics card driver. Limit the number of concurrent users to avoid such issues.

To confirm that GPU acceleration is occurring, use a third-party tool such as GPU-Z. GPU-Z is available at <http://www.techpowerup.com/gpuz/>.

DirectX, Direct3D, and WPF rendering is only available on servers with a GPU that supports a display driver interface (DDI) version of 9ex, 10, or 11.

- On Windows Server 2008 R2, DirectX and Direct3D require no special settings to use a single GPU.
- On Windows Server 2012, Remote Desktop Services (RDS) sessions on the RD Session Host server use the Microsoft Basic Render Driver as the default adapter. To use the GPU in RDS sessions on Windows Server 2012, enable the Use the hardware default graphics adapter for all Remote Desktop Services sessions setting in the group policy Local Computer Policy > Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Remote Session Environment.
- To enable WPF applications to render using the server's GPU, create the following settings in the registry of the server running Windows Server OS sessions:
  - [HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\CtxHook\ApplInit\_Dlls\Multiple Monitor Hook]  
"EnableWPFHook"=dword:00000001
  - [HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\ApplInit\_Dlls\Multiple Monitor Hook]  
"EnableWPFHook"=dword:00000001

Experimental support is provided for GPU acceleration of CUDA and OpenCL applications running in a user session. This support is disabled by default, but you can enable it for testing and evaluation purposes.

To use the experimental CUDA acceleration features, enable the following registry settings:

- [HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\CtxHook\ApplInit\_Dlls\Graphics Helper] "CUDA"=dword:00000001
- [HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\ApplInit\_Dlls\Graphics Helper]  
"CUDA"=dword:00000001

To use the experimental OpenCL acceleration features, enable the following registry settings:

- [HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\CtxHook\ApplInit\_Dlls\Graphics Helper] "OpenCL"=dword:00000001
- [HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\CtxHook\ApplInit\_Dlls\Graphics Helper]  
"OpenCL"=dword:00000001

# OpenGL Software Accelerator

May 28, 2016

The OpenGL Software Accelerator is a software rasterizer for OpenGL applications such as ArcGIS, Google Earth, Nehe, Maya, Blender, Voxler, CAD, and CAM. In some cases, the OpenGL Software Accelerator can eliminate the need to use graphics cards to deliver a good user experience with OpenGL applications.

Important: The OpenGL Software Accelerator is provided "as is" and must be tested with all applications. It might not work with some applications and is intended as a solution to try if the Windows OpenGL rasterizer does not provide adequate performance. If the OpenGL Software Accelerator works with your applications, it can be used as a way to avoid the cost of GPU hardware.

The OpenGL Software Accelerator is provided in the Support folder on the installation media, and is supported on all valid VDA platforms.

When should you try the OpenGL Software Accelerator?

- If the performance of OpenGL applications running in virtual machines on XenServer or other hypervisors is an issue, try using OpenGL Accelerator. For some applications, the OpenGL Accelerator outperforms the Microsoft OpenGL software rasterizer that is included with Windows because the OpenGL Accelerator leverages SSE4.1 and AVX. OpenGL Accelerator also supports applications using OpenGL versions up to 2.1.
- For applications running on a workstation, first try the default version of OpenGL support provided by the workstation's graphics adapter. If the graphics card is the latest version, in most cases it will deliver the best performance. If the graphics card is an earlier version or does not deliver satisfactory performance, then try the OpenGL Software Accelerator.
- 3D OpenGL applications that are not adequately delivered using CPU-based software rasterization may benefit from OpenGL GPU hardware acceleration. This feature can be used on bare metal or virtual machines.

# 音频功能

May 28, 2016

You can configure and add the following Citrix policy settings to a policy that optimizes HDX audio features. For usage details plus relationships and dependencies with other policy settings, see [Audio policy settings](#) and [Bandwidth policy settings](#) and [Multi-stream connections policy settings](#).

**Important:** Most audio features are transported using the ICA stream and are secured in the same way as other ICA traffic. User Datagram Protocol (UDP) audio uses a separate, unsecured, transport mechanism when NetScaler Access Gateway is not in path. If NetScaler Access Gateway is configured to access XenApp and XenDesktop resources, then audio traffic between the endpoint device and NetScaler Access Gateway is secured using DTLS protocol.

In general, higher sound quality consumes more bandwidth and server CPU utilization by sending more audio data to user devices. Sound compression allows you to balance sound quality against overall session performance; use Citrix policy settings to configure the compression levels to apply to sound files.

By default, the Audio quality policy setting is set to High - high definition audio. This setting provides high fidelity stereo audio, but consumes more bandwidth than other quality settings. Do not use this audio quality for non-optimized voice chat or video chat applications (such as softphones), because it may introduce latency into the audio path that is not suitable for real-time communications.

Consider creating separate policies for groups of dial-up users and for those who connect over a LAN or WAN. Over dial-up connections, where bandwidth typically is limited, download speed is often more important to users than sound quality. Therefore, you may want to create one policy for dial-up connections that applies high compression levels to sound, and another for LAN or WAN connections that applies lower compression levels.

For setting details, see [Audio policy settings](#). Remember to enable Client audio settings on the user device; see [Audio setting policies for user devices](#).

To allow users to receive audio from an application on a server through speakers or other sound devices (such as headphones) on the user device, add the Client audio redirection setting, which is Allowed by default.

Client audio mapping may cause a heavy load on the servers and the network; however, prohibiting client audio redirection disables all HDX audio functionality.

For setting details see [Audio policy settings](#). Remember to enable client audio settings on the user device; see [Audio setting policies for user devices](#).

To allow users to record audio using input devices such as microphones on the user device add the Client microphone redirection setting, which is Allowed by default.

For security, users are alerted when servers that are not trusted by their user devices try to access microphones, and can choose to accept or reject access prior to using the microphone. Users can disable this alert on Citrix Receiver.

For setting details, see [Audio policy settings](#). Remember to enable Client audio settings on the user device; see [Audio](#)

[setting policies for user devices](#).

The Audio Plug N Play policy setting allows or prevents the use of multiple audio devices to record and play sound. This setting is Enabled by default.

This setting applies only to Windows Server OS machines.

For setting details, see [Audio policy settings](#).

The Audio redirection bandwidth limit policy setting specifies the maximum bandwidth (in kilobits per second) for a playing and recording audio in a session. The Audio redirection bandwidth limit percent setting specifies the maximum bandwidth for audio redirection as a percentage of the total available bandwidth. By default, zero (no maximum) is specified for both settings. If both settings are configured, the one with the lowest bandwidth limit is used.

For setting details, see [Bandwidth policy settings](#). Remember to enable Client audio settings on the user device; see [Audio setting policies for user devices](#).

By default, **Audio over UDP Real-time Transport** is allowed (when selected at time of installation), opening up a UDP port on the server for connections that use Audio over UDP Real-time Transport. Citrix recommends configuring UDP/RTP for audio, to ensure the best possible user experience in the event of network congestion or packet loss.

**Important:** Audio data transmitted with UDP is not encrypted when NetScaler Access Gateway is not in path. If NetScaler Access Gateway is configured to access XenApp and XenDesktop resources then audio traffic between the endpoint device and NetScaler Access Gateway is secured using DTLS protocol.

The **Audio UDP port range** specifies the range of port numbers that the Virtual Delivery Agent (VDA) uses to exchange audio packet data with the user device.

By default, the range is 16500 - 16509.

For setting details about Audio over UDP Real-time Transport, see [Audio policy settings](#); for details about Audio UDP port range, see [Multi-stream connections policy settings](#). Remember to enable **Client audio settings** on the user device; see [Audio setting policies for user devices](#).

1. Load the group policy templates by following [Configure Receiver with the Group Policy Object template](#).
2. In the Group Policy Editor, expand Administrative Templates > Citrix Componentes > Citrix Receiver > User Experience.
3. For Client audio settings, select Not Configured, Enabled, or Disabled.
  - **Not Configured.** By default Audio Redirection is enabled with high quality audio or previously configured custom audio settings.
  - **Enabled.** Audio redirection is enabled with selected options.
  - **Disabled.** Audio redirection is disabled.
4. If you select **Enabled**, choose a sound quality. For UDP audio, use Medium (default).
5. For UDP audio only, select **Enable Real-Time Transport** and then set the range of incoming ports to open in the local Windows firewall.

6. To use UDP Audio with NetScaler Access Gateway, select **Allow Real-Time Transport Through gateway**. NetScaler Access Gateway should be configured with DTLS. For more information, see [UDP Audio Through a Netscaler Gateway](#).

As an Administrator, if you do not have control on endpoint devices to make these changes, for example in the case of BYOD or home computers, then use the default.ica attributes from StoreFront to enable UDP Audio.

1. On the StoreFront machine, open C:\inetpub\wwwroot\Citrix\<Store Name>\App\_Data\default.ica with an editor such as notepad.
2. Make the entries below under the [Application] section.

```
; This is to enable Real-Time Transport
EnableRtpAudio=true

; This is to Allow Real-Time Transport Through gateway
EnableUDPTroughGateway=true

; This is to set audio quality to Medium
AudioBandwidthLimit=1-

; UDP Port range
RtpAudioLowestPort=16500

RtpAudioHighestPort=16509
```

If UDP Audio is enabled by editing default.ica, then UDP audio will be enabled for all users who are using that store.

Users in audio or video conferences may hear an echo. Echoes usually occur when speakers and microphones are too close to each other. For that reason, Citrix recommends the use of headsets for audio and video conferences.

HDX provides an echo cancellation option (enabled by default) that minimizes echo. The effectiveness of echo cancellation is sensitive to the distance between the speakers and the microphone; devices should not be too close or too far away from each other.

You can change a registry setting to disable echo cancellation. When working in the registry, use caution: editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot

guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

1. Using the Registry Editor on the user device, navigate to one of the following:

- 32-bit computers: HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\ICA  
Client\Engine\Configuration\Advanced\Modules\ClientAudio\EchoCancellation
- 64-bit computers: HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA  
Client\Engine\Configuration\Advanced\Modules\ClientAudio\EchoCancellation

2. Change the Value data field to FALSE.

# 网络流量优先级

May 28, 2016

Priorities are assigned to network traffic across multiple connections for a session with quality of service (QoS)-supported routers. Four TCP/IP streams (real-time, interactive, background, and bulk) and one UDP/RTP stream (for voice) are available to carry ICA traffic between the user device and the server. Each virtual channel is associated with a specific priority and transported in the corresponding connection. You can set the channels independently, based on the TCP port number used for the connection.

Multiple channel streaming connections are supported for Virtual Delivery Agents (VDAs) installed on Windows 8 and Windows 7 machines. Work with your network administrator to ensure the Common Gateway Protocol (CGP) ports configured in the Multi-Port Policy setting are assigned correctly on the network routers.

Quality of service (QoS) is supported only when multiple session reliability ports, or the CGP ports, are configured.

Caution: Use transport security when using this feature. Citrix recommends using Internet Protocol Security (IPsec) or Secure Sockets Layer (SSL). SSL connections are supported only when the connections traverse a NetScaler Gateway that supports multi-stream. On an internal corporate network, multi-stream connections with SSL are not supported.

To set quality of service for multiple streaming connections, add the following Citrix policy settings to a policy (see [Multi-stream connections policy settings](#) for details):

- Multi-Port policy - This setting specifies ports for ICA traffic across multiple connections, and establishes network priorities.
  - Select a priority from the CGP default port priority list; by default, the primary port (2598) has a High priority.
  - Enter additional CGP ports in CGP port1, CGP port2, and CGP port3 as needed, and identify priorities for each. Each port must have a unique priority.

Explicitly configure the firewalls on VDAs to allow the additional TCP traffic.

- Multi-Stream computer setting - This setting is disabled by default. If you use Citrix Cloudbridge with Multi-Stream support in your environment, you do not need to configure this setting. Configure this policy setting when using third-party routers or legacy Branch Repeaters to achieve the desired Quality of Service (QoS).
- Multi-Stream user setting - This setting is disabled by default.

For policies containing these settings to take effect, users must log off and then log on to the network.

# USB 和客户端设备注意事项

May 28, 2016

Using HDX USB device redirection, a user can connect a flash drive to a local computer and access it remotely from within a virtual desktop or a desktop hosted application. During a session, users can use plug and play devices, including Picture Transfer Protocol (PTP) devices such as digital cameras, Media Transfer Protocol (MTP) devices such as digital audio players or portable media players, and point-of-sale (POS) devices.

Double-hop USB is not supported for desktop hosted application sessions.

USB redirection is available for the Receiver for Windows and the Receiver for Linux.

By default, USB redirection is allowed for certain classes of USB devices, and denied for others; see the Receiver documentation for details. You can restrict the types of USB devices made available to a virtual desktop by updating the list of USB devices supported for redirection.

## Important

In environments where security separation between the user device and server is needed, provide guidance to users about the types of USB devices to avoid.

Optimized virtual channels are available to redirect most popular USB devices, and provide performance and bandwidth efficiency over a WAN. The level of support provided depends on the Receiver installed on the user device. Optimized virtual channels are usually the best option, especially in high latency environments.

For USB redirection purposes, the product handles a SMART board the same as a mouse.

The product supports optimized virtual channels with USB 3.0 devices and USB 3.0 ports, such as a CDM virtual channel used to view files on a camera or to provide audio to a headset). The product also supports Generic USB Redirection of USB 3.0 devices connected to a USB 2.0 port.

Specialty devices for which there is no optimized virtual channel are supported by falling back to a Generic USB virtual channel that provides raw USB redirection. For information on USB devices tested with XenDesktop, see [CTX123569](#).

Some advanced device-specific features, such as Human Interface Device (HID) buttons on a webcam, may not work as expected with the optimized virtual channel; if this is an issue, use the Generic USB virtual channel.

Certain devices are not redirected by default, and are available only to the local session. For example, it would not be appropriate to redirect a network interface card that is attached to the user device's system board by internal USB.

The following Citrix policy settings control USB support:

- **Client USB device optimization rules.** The optimization mode is supported for input devices for class=03, for example, signature devices and drawing tablets. If no rule is specified, then the device is handled as Interactive mode (02). Capture mode (04) is the recommended mode for signature devices.
- **Client USB device redirection.** The default is Prohibited.
- **Client USB device redirection rules.** Rules only apply to devices using Generic USB redirection; therefore, the rules do not apply to devices using specialized or optimized redirection, such as CDM.
- **Client USB Plug and Play device redirection.** The default is Allowed, to permit plug-and-play of PTP, MTP, and POS

devices in a user session.

- **Client USB device redirection bandwidth limit.** The default is 0 (no maximum).
- **Client USB device redirection bandwidth limit percent.** The default is 0 (no maximum).

## About USB Generic Redirection

Generic USB Redirection is for specialty USB devices for which there is no optimized virtual channel. This functionality redirects arbitrary USB devices from client machines to virtual desktops; with this feature, end users have the ability to interact with a wide selection of generic USB devices in the desktop session as if the devices were physically attached.

With Generic USB Redirection:

- users do not need to install device drivers on the user device
- USB client drivers are installed on the VDA machine

This feature is supported for desktop sessions from VDA for Desktop OS 7.6.

This feature is also supported for desktop sessions from VDA for Server OS 7.6, with these restrictions:

- The VDA machine must be running Windows Server 2012 R2
- Only single-hop scenarios are supported
- The USB client drivers must be compatible with RDSH for Windows 2012 R2
- USB storage devices, audio devices, smartcard reader, and devices that are not fully virtualized are not supported

For more information on configuring Generic USB Redirection, see [CTX137939](#).

## Enable USB support

1. Add the Client USB device redirection setting to a policy and set its value to Allowed.
2. (Optional) To update the list of USB devices available for remoting, add the Client USB device redirection rules setting to a policy and specify the USB policy rules.
3. Enable USB support when you install Receiver on user devices. If you specified USB policy rules for the Virtual Delivery Agent in the previous step, specify those same policy rules for Receiver. For thin clients, consult the manufacturer for details of USB support and any required configuration.

## Update the list of USB devices available for remoting (Receiver for Windows 4.2)

USB devices are automatically redirected when USB support is enabled and the USB user preference settings are set to automatically connect USB devices. USB devices are also automatically redirected when operating in Desktop Appliance mode and the connection bar is not present. In some instances, however, you might not want to automatically redirect all USB devices. For more information, see [CTX123015](#).

Users can explicitly redirect devices that are not automatically redirected by selecting them from the USB device list. To prevent USB devices from ever being listed or redirected, you can specify device rules on the client and the VDA, as explained below.

You can update the range of USB devices available for remoting by specifying USB device redirection rules for both Receiver and the VDA to override the default USB policy rules.

- Edit the user device registry. An Administrative template (ADM file) is included on the installation media so you can change the user device through Active Directory Group Policy: dvd root \os\lang\Support\Configuration\icaclient\_usb.adm.
- Edit the administrator override rules for the Server OS machines through group policy rules. The Group Policy

Management Console is included on the installation media:

- For x64: dvd root \os\lang\x64\Citrix Policy\ CitrixGroupPolicyManagement\_x64.msi
- For x86: dvd root \os\lang\x86\Citrix Policy\ CitrixGroupPolicyManagement\_x86.msi

## 警告

Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

The product default rules are stored in HKLM\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRules. Do not edit these product default rules. Instead, use them as a guide for creating administrator override rules as explained below. The GPO overrides are evaluated before the product default rules.

The administrator override rules are stored in HKLM\SOFTWARE\Policies\Citrix\PortICA\GenericUSB\DeviceRules. GPO policy rules take the format {Allow:|Deny:} followed by a set of tag=value expressions separated by white space. The following tags are supported:

Tag	Description
VID	Vendor ID from the device descriptor
PID	Product ID from the device descriptor
REL	Release ID from the device descriptor
Class	Class from either the device descriptor or an interface descriptor; see the USB Web site at <a href="http://www.usb.org/">http://www.usb.org/</a> for available USB Class Codes
SubClass	Subclass from either the device descriptor or an interface descriptor
Prot	Protocol from either the device descriptor or an interface descriptor

When creating new policy rules, note the following:

- Rules are case-insensitive.
- Rules may have an optional comment at the end, introduced by #. A delimiter is not required, and the comment is ignored for matching purposes.
- Blank and pure comment lines are ignored.
- White space is used as a separator, but cannot appear in the middle of a number or identifier. For example, Deny: Class = 08 SubClass=05 is a valid rule, but Deny: Class=0 Sub Class=05 is not.
- Tags must use the matching operator =. For example, VID=1230.
- Each rule must start on a new line or form part of a semicolon-separated list.

## Important

If you are using the ADM template file, you must create rules on a single line, as a semicolon-separated list

When working with optimized devices such as mass storage, you usually redirect the device using the specialized CDM channel rather than with policy rules. However, you can override this behavior in one of the following ways:

- Manually redirect optimized device using Generic USB redirection, choose Switch to Generic from the Devices tab of the Preferences dialog box.
- Automatically redirect optimized device using Generic USB redirection, set auto-redirection for storage device (for example, AutoRedirectStorage = 1) and set USB user preference settings to automatically connect USB devices; for more information, see [CTX123015](#).

Examples:

- The following example shows an administrator-defined USB policy rule for vendor and product identifiers:  
Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse  
Deny: VID=046D # Deny all Logitech products

- The following example shows an administrator-defined USB policy rule for a defined class, sub-class, and protocol:  
Deny: Class=EF SubClass=01 Prot=01 # Deny MS Active Sync devices  
Allow: Class=EF SubClass=01 # Allow Sync devices  
Allow: Class=EF # Allow all USB-Miscellaneous devices

## Update the list of USB devices available for remoting

By default, USB devices are automatically redirected when USB support is enabled and the USB user preference settings are set to automatically connect USB devices. USB devices are also automatically redirected for Desktop Appliance sites or desktop hosted applications. In some instances, however, you might not want to automatically redirect all USB devices. For more information, see [CTX123015](#).

Desktop Viewer users can redirect devices that are not automatically redirected by selecting them from the USB device list. To prevent USB devices from being listed or redirected, specify device rules on the user device and the VDA.

You can update the range of USB devices available for remoting by specifying USB device redirection rules for both Receiver and the VDA to override the default USB policy rules. Device rules are enforced for both Receiver and the VDA. Be sure to change both so that device remoting works as you intend.

- Edit the user device registry (or the .ini files in the case of the Receiver for Linux). An Administrative template (ADM file) is included on the installation media so you can change the user device through Active Directory Group Policy: dvd root \os\lang\Support\Configuration\icaclient\_usb.adm.
- Edit the administrator override rules in the VDA registry on the Server OS machines. An ADM file is included on the installation media so you can change the VDA through Active Directory Group Policy: dvd root \os\lang\Support\Configuration\vda\_usb.adm.

### 警告

Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

The product default rules are stored in HKLM\SOFTWARE\Citrix\PortICA\GenericUSB\DeviceRules. Do not edit these product default rules. Instead, use them as a guide for creating administrator override rules as explained below. The GPO overrides are evaluated before the product default rules.

The administrator override rules are stored in HKLM\SOFTWARE\Policies\Citrix\PortICA\GenericUSB\DeviceRules. GPO policy rules take the format {Allow:|Deny:} followed by a set of tag=value expressions separated by white space. The following tags are supported:

Tag	Description
VID	Vendor ID from the device descriptor
PID	Product ID from the device descriptor
REL	Release ID from the device descriptor
Class	Class from either the device descriptor or an interface descriptor; see the USB Web site at <a href="http://www.usb.org/">http://www.usb.org/</a> for available USB Class Codes
SubClass	Subclass from either the device descriptor or an interface descriptor
Prot	Protocol from either the device descriptor or an interface descriptor

When creating new policy rules, note the following:

- Rules are case-insensitive.
- Rules may have an optional comment at the end, introduced by #. A delimiter is not required, and the comment is ignored for matching purposes.
- Blank and pure comment lines are ignored.
- White space is used as a separator, but cannot appear in the middle of a number or identifier. For example, Deny: Class = 08 SubClass=05 is a valid rule, but Deny: Class=0 Sub Class=05 is not.
- Tags must use the matching operator =. For example, VID=1230.
- Each rule must start on a new line or form part of a semicolon-separated list.

## Important

If you are using the ADM template file, you must create rules on a single line, as a semicolon-separated list

When working with optimized devices such as mass storage, you usually redirect the device using the specialized CDM channel rather than with policy rules. However, you can override this behavior in one of the following ways:

- Manually redirect optimized device using Generic USB redirection, choose Switch to Generic from the Devices tab of the Preferences dialog box.
- Automatically redirect optimized device using Generic USB redirection, set auto-redirection for storage device (for example, AutoRedirectStorage = 1) and set USB user preference settings to automatically connect USB devices; for more information, see [CTX123015](#).

Examples:

- The following example shows an administrator-defined USB policy rule for vendor and product identifiers:

Allow: VID=046D PID=C626 # Allow Logitech SpaceNavigator 3D Mouse

Deny: VID=046D # Deny all Logitech products

- The following example shows an administrator-defined USB policy rule for a defined class, sub-class, and protocol:
 

```
Deny: Class=EF SubClass=01 Prot=01 # Deny MS Active Sync devices
      Allow: Class=EF SubClass=01 # Allow Sync devices
      Allow: Class=EF # Allow all USB-Miscellaneous devices
```

## Use and remove USB devices

Users can connect a USB device before or after starting a virtual session.

When using Receiver for Windows, the following apply:

- Devices connected after a session starts appear immediately in the USB menu of the Desktop Viewer.
- If a USB device is not redirecting properly, you can try to resolve the problem by waiting to connect the device until after the virtual session starts.
- To avoid data loss, use the Windows "Safely Remove Hardware" icon before removing the USB device.

## USB mass storage devices

For mass storage devices only, remote access is also available through client drive mapping, where the drives on the user device are automatically mapped to drive letters on the virtual desktop when users log on. The drives are displayed as shared folders with mapped drive letters. To configure client drive mapping, use the Client removable drives setting in the File Redirection Policy Settings section of the ICA Policy Settings.

The main differences between the two types of remoting policy are:

Feature	Client drive mapping	Generic USB redirection
Enabled by default	Yes	No
Read-only access configurable	Yes	No
Safe to remove device during a session	No	Yes, provided users follow operating system recommendations for safe removal

If both Generic USB and the client drive mapping policies are enabled and a mass storage device is inserted either before or after a session starts, it will be redirected using client drive mapping. When both Generic USB and the client drive mapping policies are enabled and a device is configured for automatic redirection (see Knowledge Center article [CTX123015](#)) and a mass storage device is inserted either before or after a session starts, it will be redirected using Generic USB.

### 注意

USB redirection is supported over lower bandwidth connections, for example 50 Kbps, however copying large files will not work.

## File access for mapped client drives

You can control whether users can copy files from their virtual environments to their user devices. By default, files and folders on mapped client-drives are available in read/write mode from within the session.

To prevent users from adding or modifying files and folders on mapped client-devices, enable the Read-only client drive access policy setting. When adding this setting to a policy, make sure the Client drive redirection setting is set to Allowed and is also added to the policy.

# 监视

May 28, 2016

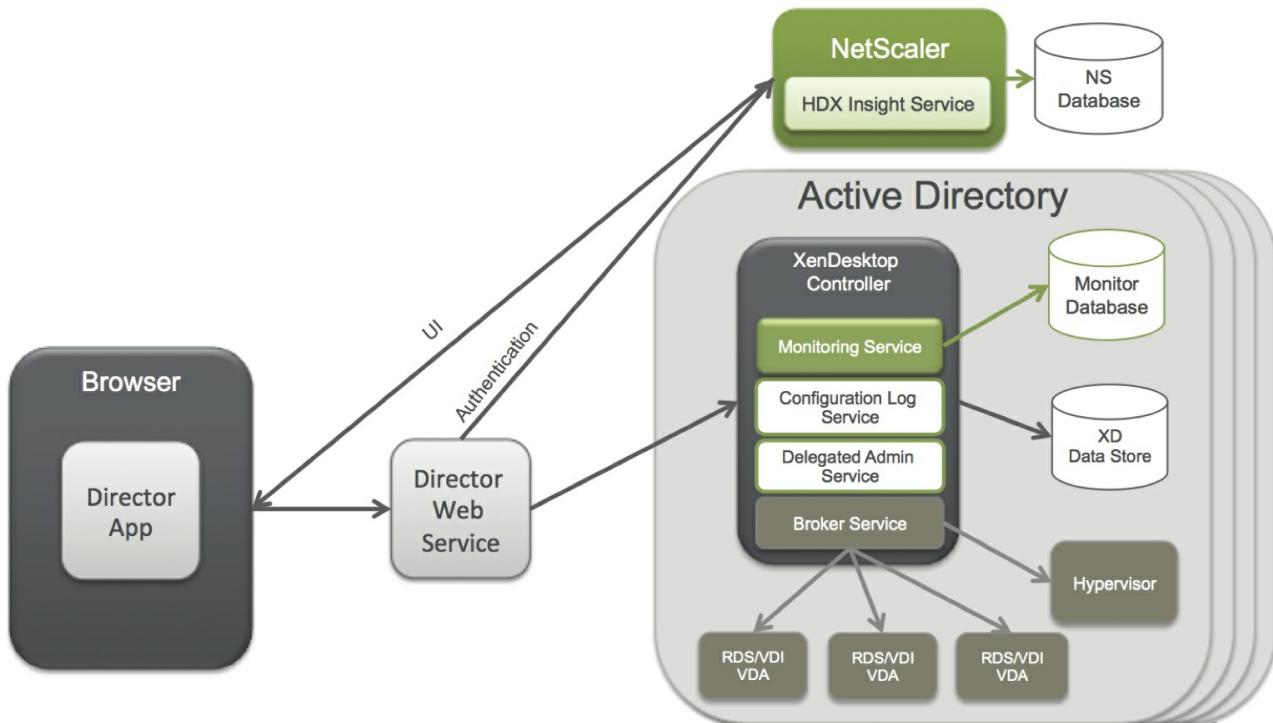
Administrators and help-desk personnel can monitor XenApp and XenDesktop Sites with Director, where administrators can access the Configuration Logging database, or by using the Site's Monitor Service's API using the OData protocol.

Administrators can monitor:

- Session usage
- Logon performance
- Connection and machine failure
- Load evaluation
- Historical trends
- Infrastructure
- User sessions
- Machines

Director

Director is a real-time web tool that allows administrators to monitor, troubleshoot, and perform support tasks for end users.



Director can access:

- Real-time data from the Broker Agent using a unified console integrated with EdgeSight features, Performance Manager, and Network Inspector.
- EdgeSight features include performance management for health and capacity assurance, and historical trending and network analysis, powered by NetScaler HDX Insight, to identify bottlenecks due to the network in your XenApp or

XenDesktop environment.

- Historical data stored in the Monitor database to access the Configuration Logging database.
- ICA data from the NetScaler Gateway using HDX Insight.
  - Gain visibility into end-user experience for virtual applications, desktops, and users for XenApp or XenDesktop.
  - Correlate network data with application data and real-time metrics for effective troubleshooting.
  - Integrate with XenDesktop 7 Director monitoring tool.
- Personal vDisk Data that allows for runtime monitoring showing base allocation and gives help-desk IT the ability to reset the Personal vDisk (to be used only as a last resort).
  - The command line tool CtxPvdDiag.exe is used to gather the user log information into one file for troubleshooting.

Director uses a troubleshooting dashboard that provides real-time health monitoring of the XenApp or XenDesktop site. This feature allows administrators to see failures in real time, providing a better idea of what the end user is experiencing.

## Session Recording

Session Recording allows you to record the on-screen activity of any user's session, over any type of connection, from any server running XenApp subject to corporate policy and regulatory compliance. Session Recording records, catalogs, and archives sessions for retrieval and playback.

Session Recording uses flexible policies to trigger recordings of application sessions automatically. This enables IT to monitor and examine user activity of applications — such as financial operations and healthcare patient information systems — supporting internal controls for regulatory compliance and security monitoring. Similarly, Session Recording also aids in technical support by speeding problem identification and time-to-resolution.

## Configuration Logging

Configuration Logging is a feature that allows administrators to keep track of administrative changes to a XenApp or XenDesktop Site. Configuration Logging can help administrators diagnose and troubleshoot problems after configuration changes are made, assist change management and track configurations, and report administration activity.

Configuration Logging can be viewed in Director with the Trend View interface to provide notifications of configuration changes to administrators who do not have access to XenDesktop Citrix Studio.

Trends View gives historical data of configuration changes over a period of time so administrators can assess what changes were made to the Sites, when they were made, and who made them to find the cause of an issue. This view breaks down configuration information in three categories.

- Connection Failures
- Failed Desktop Machines
- Failed Server Machines

## OData API

Administrators can use the Site's Monitor Service's API to search historical data using the OData protocol. This allows IT to analyze historical trends for planning purposes, to perform detailed troubleshooting of connection and machine failures, and extract information for feeding into other tools and processes.

The Monitor Service schema provides the following types of data:

- Data relating to connection failures
- Machines in a failure state

- Session usage
- Logon duration
- Load balancing data

## Related content

- Director
- Session Recording
- Monitor Personal vDisks
- Configuration Logging
- Monitor Service OData API

# Director

May 28, 2016

Director provides different views of the interface tailored to particular administrators. Product permissions determine what is displayed and the commands available.

For example, help desk administrators see an interface tailored to help desk tasks. Director allows help desk administrators to search for the user reporting an issue and display activity associated with that user, such as the status of the user's applications and processes. They can resolve issues quickly by performing actions such as ending an unresponsive application or process, shadowing operations on the user's machine, restarting the machine, or resetting the user profile.

In contrast, full administrators see and manage the entire site and can perform commands for multiple users and machines. The Dashboard provides an overview of the key aspects of a deployment, such as the status of sessions, user logons, and the site infrastructure. Information is updated every minute. If issues occur, details appear automatically about the number and type of failures that have occurred.

## Deploy and configure Director

Director is installed by default as a website on the Delivery Controller. For prerequisites and other details, see the System requirements documentation for this release.

This release of Director is not compatible with XenApp deployments earlier than 6.5 or XenDesktop deployments earlier than 7.

When Director is used in an environment containing more than one Site, be sure to synchronize the system clocks on all the servers where Controllers, Director, and other core components are installed. Otherwise, the Sites might not display correctly in Director.

**Tip:** If you intend to monitor XenApp 6.5 in addition to XenApp 7.5 or XenDesktop 7.x Sites, Citrix recommends installing Director on a separate server from the Director console that is used to monitor XenApp 6.5 sites.

**Important:** To protect the security of user names and passwords sent using plain text through the network, Citrix strongly recommends that you allow Director connections using only HTTPS, and not HTTP. Certain tools are able to read plain text user names and passwords in HTTP (unencrypted) network packets, which creates a security risk for users.

## To configure permissions

To log on to Director, administrators with permissions for Director must be Active Directory domain users and must have the following rights:

- Read rights in all Active Directory forests to be searched (see [Advanced configuration](#)).
- Configured Delegated Administrator roles (see [Delegated Administration and Director](#)).
- To shadow users, administrators must be configured using a Microsoft group policy for Windows Remote Assistance. In addition:
  - When installing VDAs, ensure the Windows Remote Assistance feature is enabled on all user devices (selected by default).
  - When you install Director on a server, ensure that Windows Remote Assistance is installed (selected by default). However, it is disabled on the server by default. The feature does not need to be enabled for Director to provide assistance to end users. Citrix recommends leaving the feature disabled to improve security on the server.
  - To enable administrators to initiate Windows Remote Assistance, grant them the required permissions by using the appropriate Microsoft Group Policy settings for Remote Assistance. For information, see [CTX127388: How to Enable](#)

## [Remote Assistance for Desktop Director](#)

- For user devices with VDAs earlier than 7, additional configuration is required. See [Configure permissions for VDAs earlier than XenDesktop 7](#).

## **To install Director**

**Note:** To allow Director to find all the XenApp workers in the farm, you will need to add a reverse DNS zone for the subnets where the XenApp servers reside on the DNS servers used by the farm.

Install Director using the installer, which checks for prerequisites, installs any missing components, sets up the Director website, and performs basic configuration. The default configuration provided by the installer handles typical deployments. If Director was not included during installation, use the installer to add Director. To add any additional components, rerun the installer and select the components to install. For information on using the installer, see the Installation documentation. Citrix recommends that you install using the product installer only, not the .MSI file.

When Director is installed on the Controller, it is automatically configured with localhost as the server address, and Director communicates with the local controller by default.

To install Director on a dedicated server that is remote from a Controller, you are prompted to enter the FQDN or IP address of a Controller. Director communicates with that specified Controller by default. Specify only one Controller address for each Site that you will monitor. Director automatically discovers all other Controllers in the same Site and falls back to those other Controllers if the Controller you specified fails.

Note: Director does not load balance between Controllers.

To secure the communications between the browser and the Web server, Citrix recommends that you implement SSL on the IIS website hosting Director. Refer to the Microsoft IIS documentation for instructions. Director configuration is not required to enable SSL.

## **To log on to Director**

The Director website is located at https or http://<Server\_FQDN>/Director.

If one of the Sites in a multi-site deployment is down, the logon for Director takes a little longer while it attempts to connect to the Site that is down.

# 委派管理和 Director

May 28, 2016

Delegated Administration uses three concepts: administrators, roles, and scopes. Permissions are based on an administrator's role and the scope of this role. For example, an administrator might be assigned a Help Desk administrator role where the scope involves responsibility for end-users at one site only.

For information about creating delegated administrators, see the main [Delegated Administration](#) document.

Administrative permissions determine the Director interface presented to administrators and the tasks they can perform.

Permissions determine:

- The views the administrator can access, collectively referred to as a view.
- The desktops, machines, and sessions that the administrator can view and interact with.
- The commands the administrator can perform, such as shadowing a user's session or enabling maintenance mode.

The built-in roles and permissions also determine how administrators use Director:

Administrator Role	Permissions in Director
Full Administrator	Full access to all views and can perform all commands, including shadowing a user's session, enabling maintenance mode, and exporting trends data.
Delivery Group Administrator	Full access to all views and can perform all commands, including shadowing a user's session, enabling maintenance mode, and exporting trends data.
Read Only Administrator	Can access all views and see all objects in specified scopes as well as global information. Can download reports from HDX channels and can export Trends data using the Export option in the Trends view. Cannot perform any other commands or change anything in the views.
Help Desk Administrator	Can access only the Help Desk and User Details views and can view only objects that the administrator is delegated to manage. Can shadow a user's session and perform commands for that user. Can perform maintenance mode operations. Can use power control options for Desktop OS Machines. Cannot access the Dashboard, Trends, or Filters views. Cannot use power control options for Server OS machines.
Machine Catalog Administrator	No access. This administrator is not supported for Director and cannot view data. This user can access the Machine Details page (Machine-based search).
Host Administrator	No access. This administrator is not supported for Director and cannot view data.

## To configure custom roles for Director administrators

In Studio, you can also configure Director-specific, custom roles to more closely match the requirements of your organization and delegate permissions more flexibly. For example, you can restrict the built-in Help Desk administrator role so that this administrator cannot log off sessions.

If you create a custom role with Director permissions, you must also give that role other generic permissions:

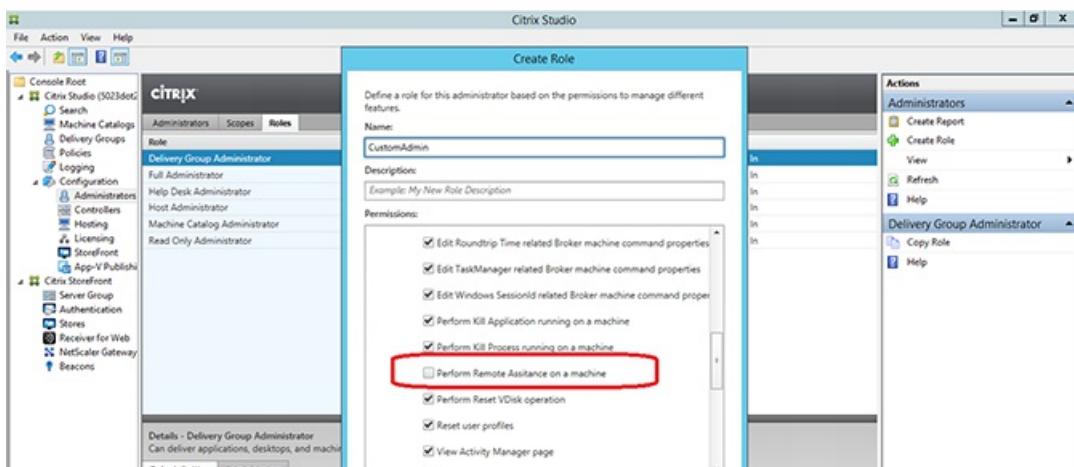
- Delivery Controller permission to log on to Director.
- Permissions to Delivery Groups to view the data related to those Delivery Groups in Director.

Alternatively, you can create a custom role by copying an existing role and include additional permissions for different views. For example, you can copy the Help Desk role and include permissions to view the Dashboard or Filters pages.

Select the Director permissions for the custom role, which include:

- Perform Kill Application running on a machine
- Perform Kill Process running on a machine
- Perform Remote Assistance on a machine
- Perform Reset vDisk operation
- Reset user profiles
- View Client Details page
- View Dashboard page
- View Filters page
- View Machine Details page
- View Trends page
- View User Details page

In this example, Shadowing (Perform Remote Assistance on a machine) is turned off.



In addition, from the list of permissions for other components, consider these permissions:

- From Delivery Groups:
  - Enable/disable maintenance mode of a machine using Delivery Group membership
  - Perform power operations on Windows Desktop machines using Delivery Group membership
  - Perform session management on machines using Delivery Group membership

# 为 XenDesktop 7 之前版本的 VDA 配置权限

May 28, 2016

If users have VDAs earlier than XenDesktop 7 installed on their devices, Director supplements information from the deployment with real-time status and metrics through Windows Remote Management (WinRM).

In addition, use this procedure to configure WinRM for use with Remote PC in XenDesktop 5.6 Feature Pack1.

By default, only local administrators of the desktop machine (typically domain administrators and other privileged users) have the necessary permissions to view the real-time data.

For information about installing and configuring WinRM, see [CTX125243](#).

To enable other users to view the real-time data, you must grant them permissions. For example, suppose there are several Director users (HelpDeskUserA, HelpDeskUserB, and so on) who are members of an Active Directory security group called HelpDeskUsers. The group has been assigned the Help Desk administrator role in Studio, providing them with the required Delivery Controller permissions. However, the group also needs access to the information from the desktop machine.

To provide the necessary access, you can configure the required permissions in one of two ways:

- Grant permissions to the Director users (impersonation model)
- Grant permissions to the Director service (trusted subsystem model)

## **To grant permissions to the Director users (impersonation model)**

By default, Director uses an impersonation model: The WinRM connection to the desktop machine is made using the Director user's identity. It is therefore the user that must have the appropriate permissions on the desktop.

You can configure these permissions in one of two ways (described later in this document):

1. Add users to the local Administrators group on the desktop machine.
2. Grant users the specific permissions required by Director. This option avoids giving the Director users (for example, the HelpDeskUsers group) full administrative permissions on the machine.

## **To grant permissions to the Director service (trusted subsystem model)**

Instead of providing the Director users with permissions on the desktop machines, you can configure Director to make WinRM connections using a service identity and grant only that service identity the appropriate permissions.

With this model, the users of Director have no permissions to make WinRM calls themselves. They can only access the data using Director.

The Director application pool in IIS is configured to run as the service identity. By default, this is the APPPOOL\Director virtual account. When making remote connections, this account appears as the server's Active Directory computer account; for example, MyDomain\DirectorServer\$. You must configure this account with the appropriate permissions.

If multiple Director websites are deployed, you must place each web server's computer account into an Active Directory security group that is configured with the appropriate permissions.

To set Director to use the service identity for WinRM instead of the user's identity, configure the following setting, as described in [Advanced configuration](#):

Service.Connector.WinRM.Identity = Service

You can configure these permissions in one of two ways:

1. Add the service account to the local Administrators group on the desktop machine.
2. Grant the service account the specific permissions required by Director (described next). This option avoids giving the service account full administrative permissions on the machine .

### To assign permissions to a specific user or group

The following permissions are required for Director to access the information it requires from the desktop machine through WinRM:

- Read and execute permissions in the WinRM RootSDDL
- WMI namespace permissions:
  - root/cimv2 — remote access
  - root/citrix — remote access
  - root/RSOP — remote access and execute
- Membership of these local groups:
  - Performance Monitor Users
  - Event Log Readers

The ConfigRemoteMgmt.exe tool, used to automatically grant these permissions, is on the installation media in the x86\Virtual Desktop Agent and x64\Virtual Desktop Agent folders and on the installation media in the tools folder. You must grant permissions to all Director users.

To grant the permissions to an Active Directory security group, user, computer account, or for actions like End Application and End Process, run the tool with administrative privileges from a command prompt using the following arguments:

ConfigRemoteMgmt.exe /configwinrmuser domain\name

where name is a security group, user, or computer account.

To grant the required permissions to a user security group:

ConfigRemoteMgmt.exe /configwinrmuser domain\HelpDeskUsers

To grant the permissions to a specific computer account:

ConfigRemoteMgmt.exe /configwinrmuser domain\DirectorServer\$

For End Process, End Application, and Shadow actions:

ConfigRemoteMgmt.exe /configwinrmuser domain\name /all

To grant the permissions to a user group:

ConfigRemoteMgmt.exe /configwinrmuser domain\HelpDeskUsers /all

To display help for the tool:

ConfigRemoteMgmt.exe

# 配置 HDX Insight

May 28, 2016

Note: The availability of this feature depends on your organization's license and your administrator permissions. HDX Insight is the integration of EdgeSight network analysis and EdgeSight performance management with Director.

- EdgeSight network analysis leverages HDX Insight to provide an application and desktop contextual view of the network. With this feature, Director provides advanced analytics of ICA traffic in their deployment.
- EdgeSight performance management provides the historical retention and trend reporting. With historical retention of data versus the real-time assessment, you can create Trend reports, including capacity and health trending.

After you enable this feature in Director, HDX Insight provides Director with additional information:

- The Trends page shows latency and bandwidth effects for applications, desktops, and users across the entire deployment.
- The User Details page shows latency and bandwidth information specific to a particular user session.

## Limitations

- ICA session Round Trip Time (RTT) shows data correctly for Receiver for Windows 3.4 or higher and the Receiver for Mac 11.8 or higher. For earlier versions of these Receivers, the data does not display correctly.
- In the Trends view, HDX connection logon data is not collected for VDAs earlier than 7. For earlier VDAs, the chart data is displayed as 0.

## To configure the EdgeSight network analysis feature on Director

EdgeSight provides network analysis by leveraging NetScaler HDX Insight to provide the Citrix application and desktop administrators the ability to troubleshoot and correlate issues that can be attributed to poor network performance.

NetScaler Insight Center must be installed and configured in Director to enable EdgeSight network analysis. Insight Center is a virtual machine (appliance) downloaded from Citrix.com. Using EdgeSight network analysis, Director communicates and gathers the information that is related to your deployment. This information is leveraged from HDX Insight, which provides robust analysis of the Citrix ICA protocol between the client and the back-end Citrix infrastructure.

1. On the server where Director is installed, locate the DirectorConfig command line tool in C:\inetpub\wwwroot\Director\tools, and run it with parameter /confignetscaler in command line prompt.
2. When prompted, configure the NetScaler Insight Center machine name (FQDN or IP address), username, password, and HTTP or HTTPS connection type.
3. To verify the changes, log off and log back on.

# 高级配置

May 28, 2016

In this article:

[To support users across multiple Active Directory domains and forests](#)

[To add sites to Director](#)

[To disable the visibility of running applications in the Activity Manager](#)

Some advanced Director configuration, such as supporting multiple sites or multiple Active Directory forests, is controlled through settings in Internet Information Services (IIS) Manager.

Important: When you change a setting in IIS, the Director service automatically restarts and logs off users.

To configure advanced settings using IIS:

1. Open the Internet Information Services (IIS) Manager console.
2. Go to the Director website under the Default website.
3. Double-click **Application Settings**.
4. Double-click a setting to edit it.

Platinum licenses retain data for 90 days by default. For more information on configurations see, [Data granularity and retention](#).

[To support users across multiple Active Directory domains and forests](#)

Director uses Active Directory to search for users and to look up additional user and machine information. By default, Director searches the domain or forest in which:

- The administrator's account is a member.
- The Director web server is a member (if different).

Director attempts to perform searches at the forest level using the Active Directory global catalog. If the administrator does not have permissions to search at the forest level, only the domain is searched.

To search or look up data from another Active Directory domain or forest requires that you explicitly set the domains or forests to be searched. Configure the following setting:

`Connector.ActiveDirectory.Domains = (user),(server)`

The value attributes user and server represent the domains of the Director user (the administrator) and Director server respectively.

To enable searches from an additional domain or forest, add the name of the domain to the list, as shown in this example:

`Connector.ActiveDirectory.Domains =  
(user),(server),<domain1>,<domain2>`

For each domain in the list, Director attempts to perform searches at the forest level. If the administrator does not have permissions to search at the forest level, only the domain is searched.

[To add sites to Director](#)

If Director is already installed, configure it to work with multiple sites. To do this, use the IIS Manager Console on each

Director server to update the list of server addresses in the application settings.

Add an address of a controller from each site to the following setting:

**Service.AutoDiscoveryAddresses = SiteAController,SiteBController**

where SiteAController and SiteBController are the addresses of Delivery Controllers from two different sites.

For XenApp 6.5 sites, add an address of a controller from each XenApp farm to the following setting:

**Service.AutoDiscoveryAddressesXA = FarmAController,FarmBController**

where FarmAController and FarmBController are the addresses of XenApp controllers from two different farms.

For XenApp 6.5 sites, another way to add a controller from a XenApp farm:

**DirectorConfig.exe /xenapp FarmControllerName**

To disable the visibility of running applications in the Activity Manager

By default, the Activity Manager in Director displays a list of all the running applications for the user's session. This information can be viewed by all administrators that have access to the Activity Manager feature in Director. For Delegated Administrator roles, this includes Full administrator, Delivery Group administrator, and Help Desk Administrator.

To protect the privacy of users and the applications they are running, you can disable the Applications tab from listing running applications.

Caution: Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

1. On the VDA, modify the registry key located at HKLM\Software\Citrix\Director\TaskManagerDataDisplayed. By default, the key is set to 1. Change the value to 0, which means the information will not be displayed in the Activity Manager.
2. On the server with Director installed, modify the setting that controls the visibility of running applications. By default, the value is true, which allows visibility of running applications in the Applications tab. Change the value to false, which disables visibility. This option affects only the Activity Manager in Director, not the VDA.

Modify the value of the following setting:

**UI.TaskManager.EnableApplications = false**

Important: To disable the view of running applications, Citrix recommends making both changes to ensure the data is not displayed in Activity Manager.

# 监视部署

Nov 21, 2016

With full administrator permissions, when you open Director, the Dashboard provides a centralized location to monitor the health and usage of a site.

If there are currently no failures and no failures have occurred in the past 60 minutes, panels stay collapsed. When there are failures, the specific failure panel automatically appears.

Note: Depending on your organization's license and your Administrator privileges, some options or features might not be available.

Panel	Description
User Connection Failures	Connection failures over the last 60 minutes. Click the categories next to the total number to view metrics for that type of failure. In the adjacent table, that number is broken out by Delivery Groups.
Failed Desktop OS Machines or Failed Server OS Machines	Total failures in the last 60 minutes broken out by Delivery Groups. Failures broken out by types, including failed to start, stuck on boot, and unregistered. For Server OS machines, failures also include machines reaching maximum load.
Licensing Status	<ul style="list-style-type: none"><li>License Server alerts are sent by the License Server and also display the actions required to resolve the alert.</li><li>Delivery Controller alerts display the details of the licensing state as seen by the controller and are sent by the Delivery Controller.</li></ul> <p>You can set the threshold for alerts in Studio.</p> <p>License Server and/or Delivery Controller alerts do not display if your License Server version is earlier than 11.12.1 and/or your Delivery Controller is older than XenApp 7.6 or XenDesktop 7.6.</p>
Sessions Connected	Connected sessions across all Delivery Groups for the last 60 minutes.
Average Logon Duration	Logon data for the last 60 minutes. The large number on the left is the average logon duration across the hour. Logon data for VDAs earlier than XenDesktop 7.0 is not included in this average.
Infrastructure	Health status of your site's hosts, controllers, and infrastructure. View performance alerts. For hosts, the connection status and the health of the CPU, memory, bandwidth (network usage), and storage (disk usage) are monitored using information from XenServer or VMware.  For example, you can configure XenCenter to generate performance alerts when CPU, network I/O or disk I/O usage go over a specified threshold on a managed server or virtual machine. By default, the alert repeat interval is 60 minutes, but you can configure this as well. For details, in the XenServer

Panel	Description
-------	-------------

Note: If no icon appears for a particular metric, this indicates that this metric is not supported by the type of host you are using. For example, no health information is available for System Center Virtual Machine Manager (SCVMM) hosts, AWS and CloudStack.

Continue to troubleshoot issues using these options (which are documented below):

- Control user machine power
- Prevent connections to machines

## Monitor sessions

If a session becomes disconnected, it is still active and its applications continue to run, but the user device is no longer communicating with the server.

Action	Description
View a user's currently connected machine or session	From the Activity Manager and User Details views, view the user's currently connected machine or session and a list of all machines and sessions to which this user has access. To access this list, click the session switcher icon in the user title bar. See <a href="#">Restore sessions</a> .
View the total number of connected sessions across all Delivery Groups	From the Dashboard, in the Sessions Connected pane, view the total number of connected sessions across all Delivery Groups for the last 60 minutes. Then click the large total number, which opens the Filters view, where you can display graphical session data based on selected Delivery Groups and ranges and usage across Delivery Groups.
View data over a longer period of time	On the Trends view, select the Sessions tab to drill down to more specific usage data for connected and disconnected sessions over a longer period of time (that is, session totals from earlier than the last 60 minutes). To view this information, click View historical trends.

Note: If the user device is running a legacy Virtual Delivery Agents (VDA), such as a VDA earlier than version 7, Director cannot display complete information about the session. Instead, it displays a message that the information is not available in the User Details view and Activity Manager panel.

## Filter data to troubleshoot failures

When you click numbers on the Dashboard or select a predefined filter from the Filter menu, the Filter view opens to display the data based on the selected machine or failure type.

Predefined filters cannot be edited, but you can save a predefined filter as a custom filter and then modify it. Additionally, you can create custom filtered views of machines, connections, and sessions across all Delivery Groups.

### 1. Select a view:

- Machines — Select Desktop OS Machines or Server OS Machines. These views show the number of configured machines. The Server OS Machines tab also includes the load evaluator index, which indicates the distribution of performance counters and tool tips of the session count if you hover over the link.
- Sessions — You can also see the session count from the Machines view.

- Connections — Filter connections by different time periods, including last 60 minutes, last 24 hours, or last 7 days.
2. For Failure by, select the criteria.
  3. Use the additional tabs for each view, as needed, to complete the filter.
  4. Select additional columns, as needed, to troubleshoot further.
  5. Save and name your filter.

To open filter later, from the Filter menu, select the failure type (Machines, Sessions, or Connections), and then select the saved filter.

6. If needed, for Machines or Connections views, use power controls for all the machines you select in the filtered list. The failure reasons and recommended actions for the Machine and Connection failures are available in [Citrix Director 7.6 Failure Reasons Troubleshooting Guide](#).
7. For the Sessions view, use the session controls or option to send messages.

Continue to troubleshoot issues using these options (which are documented below):

- Control user machine power
- Prevent connections to machines

#### Monitor historical trends across a site - Feature Pack 1

The Trends view accesses historical trend information for sessions, connection failures, machine failures, logon performance, and load evaluation for each site. To locate this information, click from the Dashboard or Filters view, click Trends.

The zoom-in drilldown feature lets you navigate through trend charts by zooming in on a time period (clicking on a data point in the graph) and drilling down to see the details associated with the trend. This feature enables you to better understand the details of who or what has been affected by the trends being displayed.

To change the default scope of each graph, apply a different filter to the data.

Action	Description
Export graph data	Select the tab containing the data to export. Click Export and select the file format: PDF, Excel, or CSV.
View trends for sessions	From the Sessions tab, select the Delivery Group and time period to view more detailed information about the concurrent session count.
View trends for connection failures	From the Connection Failures tab, select the machine type, failure type, Delivery Group, and time period to view a graph containing more detailed information about the user connection failures across your site.
View trends for machine failures	From the Desktop OS Machine Failures tab or Server OS Machines tab, select the failure type, Delivery Group, and time period to view a graph containing more detailed information about the machine failures across your site.

View trends for logon performance	<p>From the Logon Performance tab, select the Delivery Group and time period to view a graph containing more detailed information about the duration of user logon times across your site and whether the number of logons affects the performance. This view also shows the average duration of the logon phases, such as brokering duration, VM start time, and so on.</p> <p>This data is specifically for user logons and does not include users trying to reconnect from disconnected sessions.</p>
View trends for load evaluation	<p>From the Load Evaluator Index tab, view a graph containing more detailed information about the load that is distributed among Server OS machines. The filter options for this graph include the Delivery Group or Server OS machine in a Delivery Group, Server OS machine (available only if Server OS machine in a Delivery Group was selected), and range.</p>
View hosted applications usage	<p>The availability of this feature depends on your organization's license.</p> <p>From the Hosted Applications Usage tab, select the Delivery Group and time period to view a graph displaying peak concurrent usage and a table displaying application based usage. From the Application Based Usage table, you can choose a specific application to see details and a list of users who are using, or have used, the application.</p>
View virtual machine usage	<p>From the Machine Usage tab, select Desktop OS Machines or Server OS Machines to obtain real-time view of your VM usage, enabling you to quickly assess your site's capacity needs.</p> <p>Desktop OS availability — displays the current state of Desktop OS machines (VDIs) by availability for the entire site or specific Delivery Group.</p> <p>Server OS availability — displays the current state of Server OS machines by availability for the entire site or specific Delivery Group.</p>
View network analysis data using HDX Insight	<p>The availability of this feature depends on your organization's license and your administrator permissions.</p> <p>From the Network tab, monitor your network analysis, which provides a user, application, and desktop contextual view of the network. With this feature, Director provides advanced analytics of ICA traffic in your deployment.</p>

The flag icons on the graph indicate significant events or actions for that specific time range. Hover the mouse over the flag and click to list events or actions.

Note:

- HDX connection logon data is not collected for VDAs earlier than 7. For earlier VDAs, the chart data is displayed as 0.

- Sessions, failures and logon performance trend information is available as graphs and tables when time period is set to Last month or shorter. When time period is set to Last Year, the trend information is available as graphs but not as tables.
- Export of large data in Director can timeout or produce an unexpected error. This can typically happen when the site monitored by Director has a large number of configured sessions and the data requested for export exceeds 500K rows.

Continue to troubleshoot issues using these options (which are documented below):

- Control user machine power
- Prevent connections to machines

### Monitor historical trends across a site - XenApp 7.6 and XenDesktop 7.6

The Trends view accesses historical trend information for sessions, connection failures, machine failures, logon performance, and load evaluation for each site. To locate this information, click from the Dashboard or Filters view, click Trends.

To change the default scope of each graph, apply a different filter to the data.

Action	Description
Export graph data	Select the tab containing the data to export. Click Export and select the file format: PDF or CSV.
View trends for sessions	From the Sessions tab, select the Delivery Group and time period to view more detailed information about the concurrent session count.
View trends for connection failures	From the Connection Failures tab, select the machine type, failure type, Delivery Group, and time period to view a graph containing more detailed information about the user connection failures across your site.
View trends for machine failures	From the Desktop OS Machine Failures tab or Server OS Machines tab, select the failure type, Delivery Group, and time period to view a graph containing more detailed information about the machine failures across your site.
View trends for logon performance	From the Logon Performance tab, select the Delivery Group and time period to view a graph containing more detailed information about the duration of user logon times across your site and whether the number of logons affects the performance. This view also shows the average duration of the logon phases, such as brokering duration, VM start time, and so on. This data is specifically for user logons and does not include users trying to reconnect from disconnected sessions.
View trends for load evaluation	From the Load Evaluator Index tab, view a graph containing more detailed information about the load that is distributed among Server OS machines. The filter options for this graph include the Delivery Group or Server OS machine in a Delivery Group, Server OS machine (available only if Server OS machine in a Delivery Group was selected), and range.
View hosted applications	The availability of this feature depends on your organization's license. From the Hosted Applications Usage tab, select the Delivery Group and time period to view a graph

<b>Action</b>	<b>Description</b> displaying peak concurrent usage and a table displaying application based usage. From the Application Based Usage table, you can choose a specific application to see details and a list of users who are using, or have used, the application.
View network analysis data using HDX Insight	The availability of this feature depends on your organization's license and your administrator permissions. From the Network tab, monitor your network analysis, which provides a user, application, and desktop contextual view of the network. With this feature, Director provides advanced analytics of ICA traffic in your deployment.

The flag icons on the graph indicate significant events or actions for that specific time range. Hover the mouse over the flag and click to list events or actions.

Note:

- HDX connection logon data is not collected for VDAs earlier than 7. For earlier VDAs, the chart data is displayed as 0.
- Sessions, failures and logon performance trend information is available as graphs and tables when the time period is set to Last month or shorter. When the time period is set to Last Year, the trend information is available as graphs but not as tables.
- Export of large data in Director can time out or produce an unexpected error. This can typically happen when the site monitored by Director has a large number of configured sessions and the data requested for export exceeds 500K rows.

Continue to troubleshoot issues using these options (which are documented below):

- Control user machine power
- Prevent connections to machines

#### Monitor hotfixes

To view the hotfixes installed on a specific machine VDA (physical or VM), choose the Machine Details view.

#### Control user machine power states

To control the state of the machines that you select in Director, use the Power Control options. These options are available for Desktop OS machines, but might not be available for Server OS machines.

Note: This functionality is not available for physical machines or machines using Remote PC Access.

<b>Command</b>	<b>Function</b>
<b>Restart</b>	Performs an orderly (soft) shutdown of the VM. and all running processes are halted individually before restarting the VM. For example, select machines that appear in Director as "failed to start," and use this command to restart them.
<b>Force Restart</b>	Restarts the VM without first performing any shut-down procedure. This command works in the same way as unplugging a physical server and then plugging it back in and turning it back on.
<b>Shut Down</b>	Performs an orderly (soft) shutdown of the VM; all running processes are halted individually.

<b>Force Command Shutdown</b>	Shuts down the VM without first performing any shut-down procedure. This command works in the same way as unplugging a physical server. It may not always shut down all running processes, and you risk losing data if you shut down a VM in this way.
<b>Suspend</b>	Suspends a running VM in its current state and stores that state in a file on the default storage repository. This option allows you to shut down the VM's host server and later, after rebooting it, resume the VM, returning it to its original running state.
<b>Resume</b>	Resumes a suspended VM and restores its original running state.
<b>Start</b>	Starts a VM when it is off (also called a cold start).

If power control actions fail, hover the mouse over the alert, and a pop-up message appears with details about the failure.

### Prevent connections to machines

Use maintenance mode to prevent new connections temporarily while the appropriate administrator performs maintenance tasks on the image.

When you enable maintenance mode on machines, no new connections are allowed until you disable it. If users are currently logged on, maintenance mode takes effect as soon as all users are logged off. For users who do not log off, send a message informing them that machines will be shut down at a certain time, and use the power controls to force the machines to shut down.

1. Select the machine, such as from the User Details view, or a group of machines in the Filters view.
2. Select Maintenance Mode, and turn on the option.

If a user tries to connect to an assigned desktop while it is in maintenance mode, a message appears indicating that the desktop is currently unavailable. No new connections can be made until you disable maintenance mode.

# 对用户问题进行故障排除

May 28, 2016

Use the Director's **Help Desk** view (**Activity Manager** page) to view information about the user:

- Check for details about the user's logon, connection, and applications.
- Shadow the user's machine.
- Troubleshoot the issue with the recommended actions in the following table, and, if needed, escalate the issue to the appropriate administrator.

## Troubleshooting tips

User's issue	See these suggestions:
Logon takes a long time or fails intermittently or repeatedly	<a href="#">Diagnose user logon issues</a>
Application is slow or won't respond	<a href="#">Resolve application failures</a>
Connection failed	<a href="#">Restore desktop connections</a>
Session is slow or not responding	<a href="#">Restore sessions</a>
Video is slow or poor quality	<a href="#">Run HDX channel system reports</a>

Note: To make sure that the machine is not in maintenance mode, from the User Details view, review the Machine Details panel.

## Search tips

When you type the user's name in a Search field, Director searches for users in Active Directory for users across all sites configured to support Director.

When you type a multiuser machine name in a Search field, Director displays the Machine Details for the specified machine.

When you type an endpoint name in a Search field, Director uses the unauthenticated (anonymous) and authenticated sessions that are connected to a specific endpoint, which enables troubleshooting unauthenticated sessions. Ensure that endpoint names are unique to enable troubleshooting of unauthenticated sessions.

The search results also include users who are not currently using or assigned to a machine.

- Searches are not case-sensitive.
- Partial entries produce a list of possible matches.
- After you type a few letters of a two-part name (username, family name and first name, or display name), separated by a space, the results include matches for both strings. For example, if you type jo rob, the results might include strings such as "John Robertson" or Robert, Jones.

To return to the landing page, click the Director logo.

## Upload troubleshooting information to Citrix Technical Support

Run Citrix Scout from a single Delivery Controller or VDA to capture key data points and Citrix Diagnosis Facility (CDF) traces

to troubleshoot selected computers. After capturing this information, Scout securely uploads the data points to Citrix Technical Support. The Tools As a Service (TaaS) platform uses this information to reduce the time to resolve customer-reported issues.

Scout is installed with XenApp or XenDesktop components. Scout appears in the Windows Start Menu or Windows 8 or 8.1 Start Screen when you install or upgrade to XenDesktop 7.1, XenDesktop 7.5, or XenApp 7.5.

To start Scout, from the Start Menu or Start Screen, select Citrix > Citrix Scout.

For information on using and configuring Scout, and for frequently asked questions, see  
<http://support.citrix.com/article/CTX130147>.

The following video summarizes how to use Scout.

# 重影用户

May 28, 2016

From Director, use the shadow user feature to view and work directly on a user's virtual machine or session. The user must be connected to the machine that you want to shadow. Verify this by checking the machine name listed in the user title bar.

1. In the User Details view, select the user session.
2. Activate shadowing for the selected user session:
  - For machine monitoring, in the Activity Manager view, click Shadow.
  - For session monitoring, in the User Details view, locate the Session Details panel and click Shadow.
3. After the connection initializes, a dialog box prompts you to open or save the .msrcincident file.
4. Open the incident file with the Remote Assistance Viewer, if not already selected by default. A confirmation prompt appears on the user device.
5. Instruct the user to click Yes to start the machine or session sharing.

For additional control, ask the user to share keyboard and mouse control.

## Streamline Microsoft Internet Explorer browsers for shadowing

Configure your Microsoft Internet Explorer browser to automatically open the downloaded Microsoft Remote Assistance (.msra) file with the Remote Assistance client.

To do this, you must enable the Automatic prompting for file downloads setting in the Group Policy editor:

Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page > Internet Zone > Automatic prompting for file downloads.

By default, this option is enabled for sites in the Local intranet zone. If the Director site is not in the Local intranet zone, consider manually adding the site to this zone.

# 向用户发送消息

May 28, 2016

From Director, send a message to a user who is connected to one or more machines. For example, use this feature to send immediate notices about administrative actions such as impending desktop maintenance, machine log-offs and restarts, and profile resets.

1. In the Activity Manager view, select the user and click Details.
2. In the User Details view, locate the Session Details panel and click Send Message.
3. Type your message information in the Subject and Message fields, and click Send.

If the message is sent successfully, a confirmation message appears in Director. If the user's machine is connected, the message appears there.

If the message is not sent successfully, an error message appears in Director. Troubleshoot the problem according to the error message. When you have finished, type the subject and message text again and click Try again.

# 诊断用户登录问题

May 28, 2016

Use these general steps:

1. From the User Details view, troubleshoot the logon state using the Logon Duration panel.
  - If the user is logging on, the view reflects the process of logging on.
  - If the user is currently logged on, the Logon Duration panel displays the time it took for the user to log on to the current session.
2. Ask the user to log off and then log on again so that you can observe the Logon Duration data. The panel typically updates after about 3 minutes, but it could take longer depending on the time taken for the logon to complete.
3. Examine the phases of the logon process:
  - **Brokering** — Time taken to decide which desktop to assign to the user.
  - **VM start** — Time taken to boot the desktop.
  - **HDX connection** — Time taken for HDX connection establishment, dependent on the network.
  - **GPOs** — Time taken to apply group policy objects.
  - **Login scripts** — Time taken for scripts.
  - **Profile load** — Time taken to load the user profile.
  - **Interactive session** — Time taken to establish an interactive user session.

The total logon time is not an exact sum of these phases. For example, some phases occur in parallel, and in some phases, additional processing occurs that might result in a longer logon duration than the sum.

Tip: To identify unusual or unexpected values in the graph, compare the amount of time taken in each phase of the current session with the average duration for this user for the last seven days, and the average duration for all users in this Delivery Group for the last seven days.

Escalate as needed. For example, if the VM startup is slow, the issue could be in the hypervisor, so you can escalate it to the hypervisor administrator. Or, if the brokering time is slow, you can escalate the issue to the Site administrator to check the load balancing on the Delivery Controller.

**Troubleshooting tips:** Examine unusual differences, including:

- Missing (current) logon bars
- Major discrepancy between the current duration and this user's average duration. Causes could include:
  - A new application was installed.
  - An operating system update occurred.
  - Configuration changes were made.
- Major discrepancy between the user's logon numbers (current and average duration) and the Delivery Group average duration.

If needed, click Restart to observe the user's logon process to troubleshoot issues, such as VM Start or Brokering.

# 解决应用程序故障

May 28, 2016

In the Activity Manager view, click the Applications tab. You can view all the applications on all machines to which this user has access, including local and hosted applications for the currently connected machine, and the current status of each.

Note: If the Applications tab is greyed out, contact an administrator with the permission to enable the tab.

The list includes only those applications that were launched within the session.

For Server OS machines and Desktop OS machines, applications are listed for each disconnected session. If the user is not connected, no applications are displayed.

Action	Description
End the application that is not responding.	Choose the application that is not responding and click End Application. Once the application is terminated, ask the user to launch it again.
End processes that are not responding.	If you have the required permission, click the Processes tab. Select a process that is related to the application or using a high amount of CPU resources or memory, and click End Process. However, if you do not have the required permission to terminate the process, attempting to end a process will fail.
Restart the user's machine.	For Desktop OS machines only, for the selected session, click Restart. Alternatively, from the Machine Details view, use the power controls to restart or shut down the machine. Instruct the user to log on again so that you can recheck the application.  For Server OS machines, the restart option is not available. Instead, log off the user and let the user log on again.
Put the machine into maintenance mode.	If the machine's image needs maintenance, such as a patch or other updates, put the machine into maintenance mode and escalate the issue to the appropriate administrator. Click , and from the Machine Details view, click Details and turn on the maintenance mode option. Escalate to the appropriate administrator.

# 还原桌面连接

May 28, 2016

From Director, check the user's connection status for the current machine in the user title bar.

If the desktop connection failed, the error that caused failure is displayed and can help you decide how to troubleshoot.

Action	Description
Ensure that the machine is not in maintenance mode.	On the User Details page, make sure maintenance mode is turned off.
Restart the user's machine.	Select the machine and click Restart. Use this option if the user's machine is unresponsive or unable to connect, such as when the machine is using an unusually high amount of CPU resources, which can make the CPU unusable.

# 还原会话

May 28, 2016

If a session becomes disconnected, it is still active and its applications continue to run, but the user device is no longer communicating with the server.

In the User Details view, troubleshoot session failures in the Session Details panel. You can view the details of the current session, indicated by the session ID.

Action	Description
End applications or processes that are not responding.	Click the Applications tab. Select any application that is not responding and click End Application. Similarly, select any corresponding process that is not responding and click End Process. Also, end processes that are consuming an unusually high amount of memory or CPU resources, which can make the CPU unusable.
Disconnect the Windows session.	Click Session Control and then select Disconnect. This option is available only for brokered Server OS machines. For non-brokered sessions, the option is disabled.
Log off the user from the session.	Click Session Control and then select Log Off.

To test the session, the user can attempt to log back onto it. You can also shadow the user to more closely monitor this session.

Note: If user devices are running Virtual Delivery Agents (VDAs) earlier than XenDesktop 7, Director cannot display complete information about the session; instead, it displays a message that the information is not available. These messages might appear in the User Details page and Activity Manager.

# 运行 HDX 通道系统报告

May 28, 2016

In the User Details view, check the status of the HDX channels on the user's machine in the HDX panel. This panel is available only if the user machine is connected using HDX.

If a message appears indicating that the information is not currently available, wait for one minute for the page to refresh, or select the Refresh button. HDX data takes a little longer to update than other data.

Click an error or warning icon for more information.

Tip: You can view information about other channels in the same dialog box by clicking the left and right arrows in the left corner of the title bar.

HDX channel system reports are used mainly by Citrix Support to troubleshoot further.

1. In the HDX panel, click Download System Report.
2. You can view or save the .xml report file.
  - To view the .xml file, click Open. The .xml file appears in the same window as the Director application.
  - To save the .xml file, click Save. The Save As window appears, prompting you for a location on the Director machine to download the file to.

# 重置 Personal vDisk

May 28, 2016

Caution: When you reset the disk, the settings revert back to their factory default values and all data on it is deleted, including applications. The profile data is retained unless you modified the Personal vDisk default (of redirecting profiles from the C: drive), or you are not using a third-party profile solution.

To reset, the machine with the Personal vDisk must be running; however, the user does not have to be logged on to it.

This option is available only for Desktop OS machines; it is disabled for Server OS machines.

1. From the Help Desk view, choose the targeted Desktop OS machine.
2. From this view or in the Personalization panel of the User Details view, click Reset Personal vDisk.
3. Click Reset. A message appears warning that the user will be logged off. After the user is logged off (if the user was logged on), the machine restarts.

If the reset is successful, the Personal vDisk status field value in the Personalization panel of the User Details view is Running. If the reset is unsuccessful, a red X to the right of the Running value appears. When you point to this X, information about the failure appears.

# 重置用户配置文件

May 28, 2016

Caution: When a profile is reset, although the user's folders and files are saved and copied to the new profile, most user profile data are deleted (for example, the registry is reset and application settings might be deleted).

1. From Director, search for the user whose profile you want to reset and select this user's session.
2. Click **Reset Profile**.
3. Instruct the user to log off from all sessions.
4. Instruct the user to log on again. The folders and files that were saved from the user's profile are copied to the new profile.

Important: If the user has profiles on multiple platforms (such as Windows 8 and Windows 7), instruct the user to log back on first to the same desktop or app that the user reported as a problem. This ensures that the correct profile is reset.

If the profile is a Citrix user profile, the profile is already reset by the time the user's desktop appears. If the profile is a Microsoft roaming profile, the folder restoration might still be in progress for a brief time. The user must stay logged on until the restoration is complete.

Note: The preceding steps assume you are using XenDesktop (desktop VDA). If you are using XenApp (server VDA) you will need to be logged on to perform the profile reset. The user then needs to log off, and log back on to complete the profile reset.

If the profile is not successfully reset (for example, the user cannot successfully log back on to the machine or some of the files are missing), you must manually restore the original profile.

The folders (and their files) from the user's profile are saved and copied to the new profile. They are copied in the listed order:

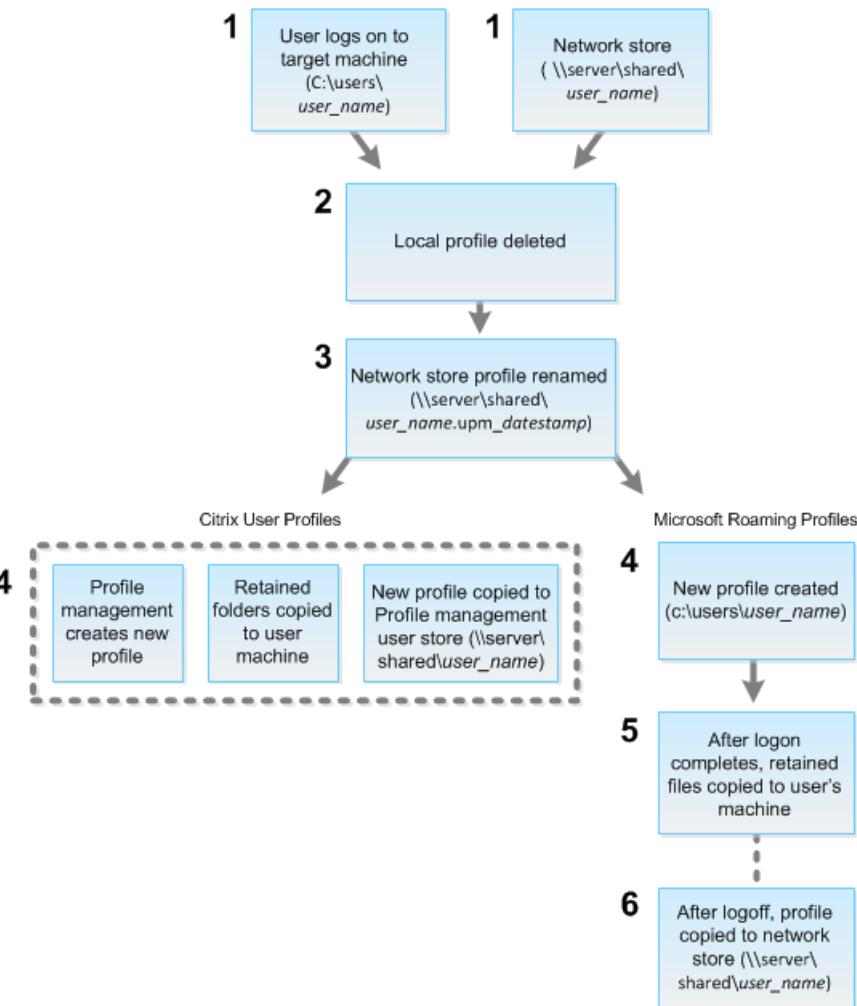
- Desktop
- Cookies
- Favorites
- Documents
- Pictures
- Music
- Videos

Note: In Windows 8 and later, cookies are not copied when profiles are reset.

## How reset profiles are processed

Any Citrix user profile or Microsoft roaming profile can be reset. After the user logs off and you select the reset command (either in Director or using the PowerShell SDK), Director first identifies the user profile in use and issues an appropriate reset command. Director receives the information through Profile management, including information about the profile size, type, and logon timings.

The next time the user logs on, this diagram illustrates the processing that occurs.



1. The reset command issued by Director specifies the profile type. The Profile management service then attempts to reset a profile of that type and looks for the appropriate network share (user store). If the user is processed by Profile management, but receives a roaming profile command, it is rejected (or vice versa).
2. If a local profile is present, it is deleted.
3. The network profile is renamed.
4. The next action depends on whether the profile being reset is a Citrix user profile or a Microsoft roaming profile.
  - For Citrix user profiles, the new profile is created using the Profile management import rules, and the folders are copied back to the network profile, and the user can log on proceed as normal. If a roaming profile is used for the reset, any registry settings in the roaming profile are preserved in the reset profile.

Note: You can configure Profile management so that a template profile overrides the roaming profile, if required.

  - For Microsoft roaming profiles, a new profile is created by Windows, and when the user logs on, the folders are copied back to the user device. When the user logs off again, the new profile is copied to the network store.

To manually restore a profile after a failed reset

1. Instruct the user to log off from all sessions.
2. Delete the local profile if one exists.
3. Locate the archived folder on the network share that contains the date and time appended to the folder name, the folder with a .upm\_datestamp extension.
4. Delete the current profile name; that is, the one without the upm\_datestamp extension.
5. Rename the archived folder using the original profile name; that is, remove the date and time extension. You have returned the profile to its original, pre-reset state.



# Session Recording

May 28, 2016

Session Recording allows you to record the on-screen activity of any user session hosted from a Server OS VDA machine, over any type of connection, subject to corporate policy and regulatory compliance. Session Recording records, catalogs, and archives sessions for retrieval and playback.

Session Recording uses flexible policies to trigger recordings of application sessions automatically. This enables IT to monitor and examine user activity of applications — such as financial operations and healthcare patient information systems — supporting internal controls for regulatory compliance and security monitoring. Similarly, Session Recording also aids in technical support by speeding problem identification and time-to-resolution.

## Benefits

**Enhanced security through logging and monitoring.** Session Recording allows organizations to record on-screen user activity for applications that deal with sensitive information. This is especially critical in regulated industries such as health care and finance. Where personal information that must not be recorded is involved, policy controls allow selective recording.

**Powerful activity monitoring.** Session Recording captures and archives screen updates, including mouse activity and the visible output of keystrokes in secured video recordings to provide a record of activity for specific users, applications, and servers.

Session Recording is not designed or intended to contribute to the collection of evidence for legal proceedings. Citrix recommends that organizations using Session Recording use other techniques for evidence collection, such as conventional video records combined with traditional text-based eDiscovery tools.

**Faster problem resolution.** When users call with a problem that is hard to reproduce, help desk support staff can enable recording of user sessions. When the issue recurs, Session Recording provides a time-stamped visual record of the error, which can then be used for faster troubleshooting.

# Session Recording 入门

May 28, 2016

After you perform the following steps, you can begin recording and reviewing XenApp sessions.

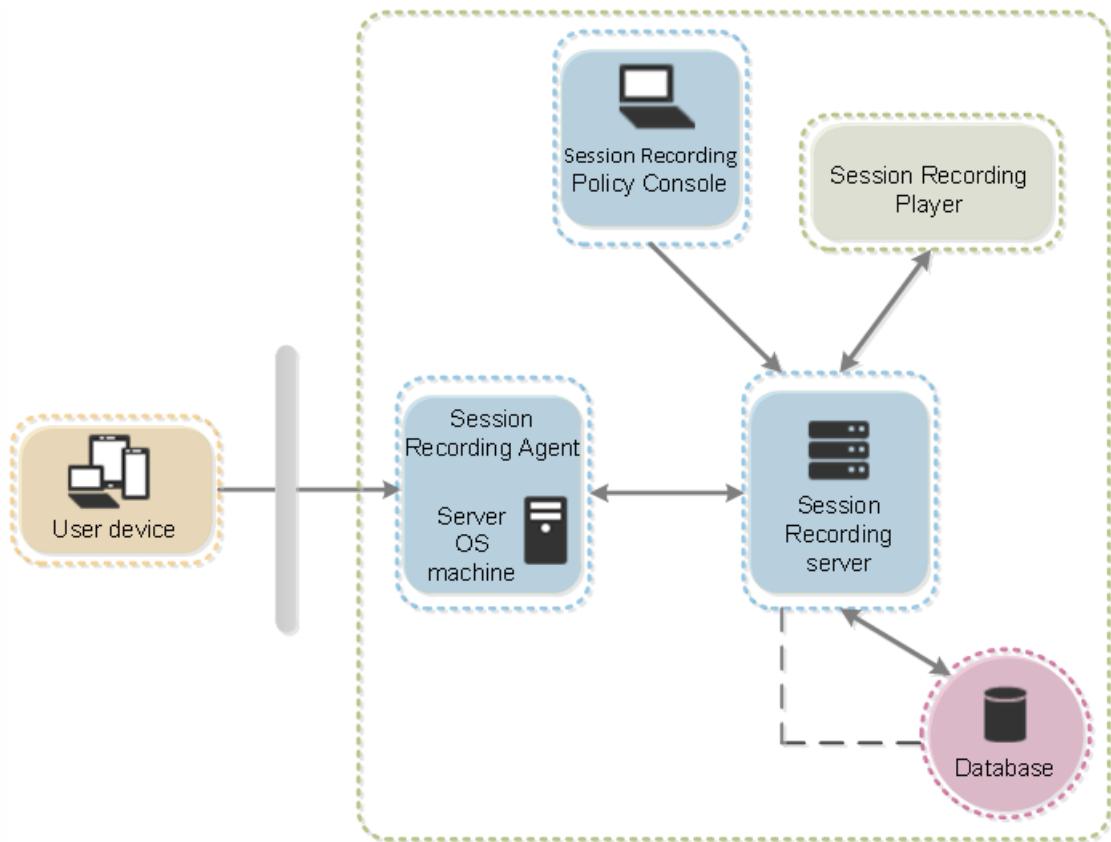
1. Become familiar with the Session Recording components.
2. Select the deployment scenario for your environment.
3. Verify the installation requirements.
4. Install Session Recording.
5. Configure the Session Recording components to permit recording and viewing of sessions.

Session Recording consists of five components:

- **Session Recording Agent.** A component installed on each Server OS machine to enable recording. It is responsible for recording session data.
- **Session Recording Server.** A server that hosts:
  - The Broker. An IIS 6.0+ hosted Web application that handles the search queries and file download requests from the Session Recording Player, handles policy administration requests from the Session Recording Policy Console, and evaluates recording policies for each XenApp session.
  - The Storage Manager. A Windows service that manages the recorded session files received from each Session Recording-enabled computer running XenApp.
- **Session Recording Player.** A user interface that users access from a workstation to play recorded XenApp session files.
- **Session Recording Database.** An SQL database for storing recorded session data.
- **Session Recording Policy Console.** A console used to create policies to specify which sessions are recorded.

This illustration shows the Session Recording components and their relationship with each other:

In the deployment example illustrated here, the Session Recording Agent, Session Recording Server, Session Recording Database, Session Recording Policy Console, and Session Recording Player all reside behind a security firewall. The Session Recording Agent is installed on a Server OS machine. A second server hosts the Session Recording Policy Console, a third server acts as the Session Recording Server, and a fourth server hosts the Session Recording Database. The Session Recording Player is installed on a workstation. A client device outside the firewall communicates with the Server OS machine on which the Session Recording Agent is installed. Inside the firewall, the Session Recording Agent, Session Recording Policy Console, Session Recording Player, and Session Recording Database all communicate with the Session Recording Server.



# 计划部署

May 28, 2016

Depending upon your environment, you can deploy the Session Recording components in different scenarios.

A Session Recording deployment does not have to be limited to a single site. With the exception of the Session Recording Agent, all components are independent of the server site. For example, you can configure multiple sites to use a single Session Recording Server.

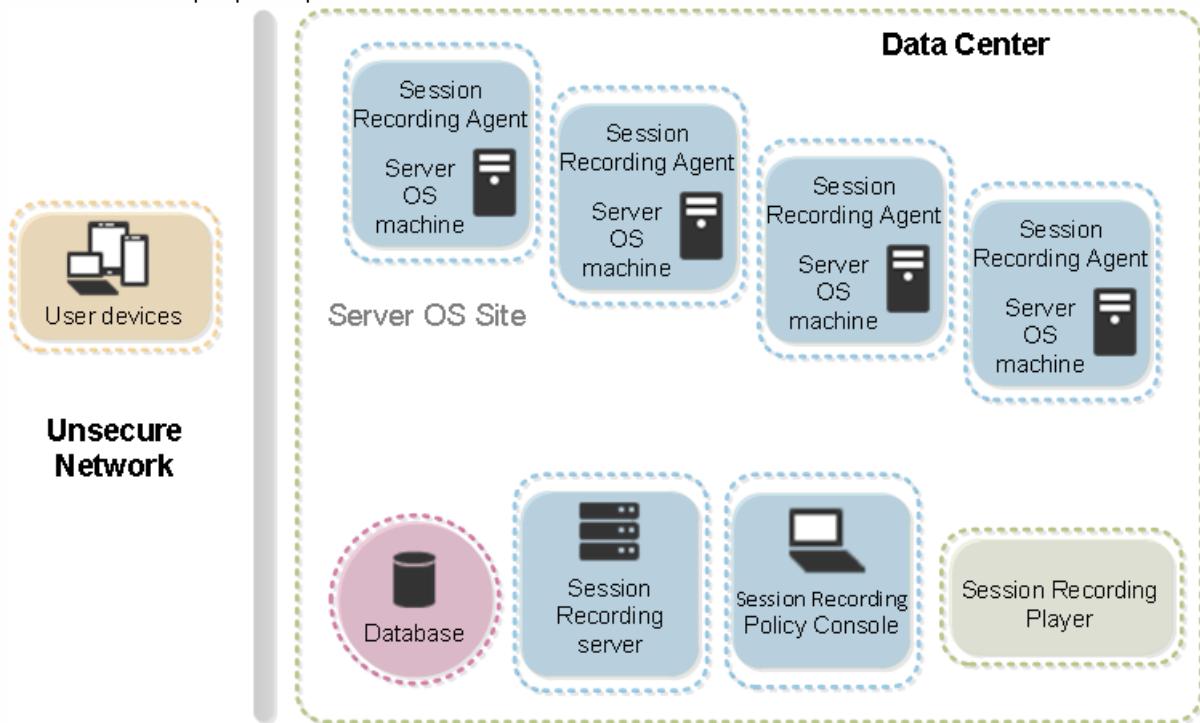
Alternatively, if you have a large site with many agents and plan to record many graphically intense applications (for example, AutoCAD applications), or you have many sessions to record, a Session Recording Server can experience a high performance demand. To alleviate performance issues, you can install multiple Session Recording Servers on different computers and point the Session Recording Agents to the different computers. Keep in mind that an agent can point to only one server at a time.

These are the two suggested configurations for a Session Recording deployment:

- Deploy the Session Recording Agent on single Server OS machine.
- Deploy the Session Recording Agent on multiple Server OS machines on a site.

## Server site deployment

Use this type of deployment for recording sessions for one or more sites. The Session Recording Agent is installed on each Server OS machine in a site. The site resides in a data center behind a security firewall. The Session Recording Administration components (Session Recording Database, Session Recording Server, Session Recording Policy Console) are installed on other servers and the Session Recording Player is installed on a workstation, all behind the firewall but not in the data center. Outside the firewall, in an unsecured network environment, are XenApp clients, such as a workstation, mobile devices, and a laptop computer.



# 安全性建议

Nov 30, 2016

Session Recording is designed to be deployed within a secure network and accessed by administrators, and as such, is secure. Out-of-the-box deployment is designed to be simple and security features such as digital signing and encryption can be configured optionally.

Communication between Session Recording components is achieved through Internet Information Services (IIS) and Microsoft Message Queuing (MSMQ). IIS provides the web services communication link between each Session Recording component. MSMQ provides a reliable data transport mechanism for sending recorded session data from the Session Recording Agent to the Session Recording Server.

Consider these security recommendations when planning your deployment:

- Ensure servers running Session Recording components are physically secure. If possible, lock these computers in a secure room to which only authorized personnel can gain direct access.
- Isolate servers running Session Recording components on a separate subnet or domain.
- Protect the recorded session data from users accessing other servers by installing a firewall between the Session Recording Server and other servers.
- Keep the Session Recording Admin Server and SQL database up to date with the latest security updates from Microsoft.
- Restrict nonadministrators from logging on to the administration machine.
- Strictly limit who is authorized to make recording policy changes and view recorded sessions.
- Install digital certificates, use the Session Recording file signing feature, and set up SSL communications in IIS.
- Set up MSMQ to use HTTPS as its transport by setting the MSMQ protocol listed in the Session Recording Agent Properties dialog box to HTTPS. For more information, see [Troubleshoot MSMQ](#).
- Use TLS 1.0 and disable SSLv2, SSLv3, and RC4 cipher on the Session Recording Server and Session Recording Database. For more information, see the Microsoft articles <http://support.microsoft.com/default.aspx?scid=kb;en-us;187498> and <http://support.microsoft.com/kb/245030/en-us>.
- Use playback protection. Playback protection is a Session Recording feature that encrypts recorded files before they are downloaded to the Session Recording Player. By default, this option is enabled and is in the Session Recording Server Properties.
- Follow NSIT guidance for cryptographic key lengths and cryptographic algorithms.

For information about configuring Session Recording features, see <http://support.citrix.com/article/CTX200868>.

On the computer on which the Session Recording Server is installed, the IIS Web server sends its server certificate to the client when establishing an SSL connection from the Session Recording Agent, Session Recording Player, or Session Recording Policy Console. When receiving a server certificate, the Session Recording Agent, Session Recording Player, or Policy Console determines which Certificate Authority (CA) issued the certificate and if the CA is trusted by the client. If the CA is not trusted, the certificate is declined and an error is logged in the Application Event log for the Session Recording Agent or an error message appears to the user in the Session Recording Player or Policy Console.

A server certificate is installed by gathering information about the server and requesting a CA to issue a certificate for that server. You must specify the correct information when requesting a server certificate and ensure the server name is specified

correctly. If the fully qualified domain name (FQDN) is used for connecting clients (Session Recording Agent, Session Recording Player, and Policy Console) the certificate information specified to the CA must use the FQDN of the server rather than the NetBIOS name. If you specify NetBIOS names, do not specify the FQDN when requesting a server certificate. Install the server certificate into the local server's certificate store. Install the issuing CA certificate on each connecting client.

Your organization may have a private CA that issues server certificates that you can use with Session Recording. If you are using a private CA, ensure each client device has the issuing CA certificate installed. Refer to Microsoft documentation about using certificates and certificate authorities. Alternatively, some companies and organizations currently act as CAs, including VeriSign, Baltimore, Entrust, and their respective affiliates.

All certificates have an expiration date defined by the CA. To find the expiration date, check the properties of the certificate. Ensure certificates are renewed before the expiration date to prevent any errors occurring in Session Recording.

The Session Recording installation is configured to use HTTPS by default and requires that you configure the default Web site with a server certificate issued from a CA. If you need instructions for installing server certificates in IIS, consult your IIS documentation.

# 可扩展性注意事项

May 28, 2016

Installing and running Session Recording requires few additional resources beyond what is necessary to run XenApp. However, if you plan to use Session Recording to record a large number of sessions or if the sessions you plan to record will result in large session files (for example, graphically intense applications), consider the performance of your system when planning your Session Recording deployment.

For more information about building a highly scalable Session Recording system, see <http://support.citrix.com/article/CTX200869>.

In this article:

[Hardware recommendations](#)

[Disk and storage hardware](#)

[Network capacity](#)

[Computer processing capacity](#)

[Deploy multiple Session Recording servers](#)

[Database scalability](#)

Consider how much data you will be sending to each Session Recording Server and how quickly the servers can process and store this data. The rate at which your system can store incoming data must be higher than the data input rate.

To estimate your data input rate, multiply the number of sessions recorded by the average size of each recorded session and divide by the period of time for which you are recording sessions. For example, you might record 5,000 Microsoft Outlook sessions of 20MB each over an 8-hour work day. In this case, the data input rate is approximately 3.5MBps. (5,000 sessions times 20MB divided by 8 hours, divided by 3,600 seconds per hour.)

You can improve performance by optimizing the performance of a single Session Recording Server or by installing multiple Session Recording Servers on different computers.

Disk and storage hardware are the most important factors to consider when planning a Session Recording deployment. The write performance of your storage solution is especially important. The faster data can be written to disk, the higher the performance of the system overall.

Storage solutions suitable for use with Session Recording include a set of local disks controlled as RAID arrays by a local disk controller or by an attached Storage Area Network (SAN).

Note: Session Recording should not be used with Network-Attached Storage (NAS), due to performance and security problems associated with writing recording data to a network drive.

For a local drive set up, a disk controller with built-in cache memory enhances performance. A caching disk controller must have a battery backup facility to ensure data integrity in case of a power failure.

A 100Mbps network link is suitable for connecting a Session Recording Server. A gigabit Ethernet connection may improve performance, but does not result in 10 times greater performance than a 100Mbps link.

Ensure that network switches used by Session Recording are not shared with third-party applications that may compete for available network bandwidth. Ideally, network switches are dedicated for use with the Session Recording Server.

Consider the following specification for the computer on which a Session Recording Server is installed:

- A dual CPU or dual-core CPU is recommended
- 2GB to 4GB of RAM is recommended

Exceeding these specifications does not significantly improve performance.

If a single Session Recording Server does not meet your performance needs, you can install more Session Recording Servers on different machines. In this type of deployment, each Session Recording Server has its own dedicated storage, network switches, and database. To distribute the load, point the Session Recording Agents in your deployment to different Session Recording Servers.

The Session Recording Database requires Microsoft SQL Server 2014, Microsoft SQL Server 2012, or Microsoft SQL Server 2008 R2. The volume of data sent to the database is very small because the database stores only metadata about the recorded sessions. The files of the recorded sessions themselves are written to a separate disk. Typically, each recorded session requires only about 1KB of space in the database, unless the Session Recording Event API is used to insert searchable events into the session.

The Express Editions of Microsoft SQL Server 2014, Microsoft SQL Server 2012, and Microsoft SQL Server 2008 R2 impose a database size limitation of 10GB. At 1KB per recording session, the database can catalog about four million sessions. Other editions of Microsoft SQL Server have no database size restrictions and are limited only by available disk space. As the number of sessions in the database increases, performance of the database and speed of searches diminishes only negligibly.

If you are not making customizations through the Session Recording Event API, each recorded session generates four database transactions: two when recording starts, one when the user logs onto the session being recorded, and one when recording ends. If you used the Session Recording Event API to customize sessions, each searchable event recorded generates one transaction. Because even the most basic database deployment can handle hundreds of transactions per second, the processing load on the database is unlikely to be stressed. The impact is light enough that the Session Recording Database can run on the same SQL Server as other databases, including the XenApp or XenDesktop data store database.

If your Session Recording deployment requires many millions of recorded sessions to be cataloged in the database, follow Microsoft guidelines for SQL Server scalability.

# 重要部署注意事项

May 28, 2016

- To enable Session Recording components to communicate with each other, ensure you install them in the same domain or across trusted domains that have a transitive trust relationship. The system cannot be installed into a workgroup or across domains that have an external trust relationship.
- Session Recording does not support the clustering of two or more Session Recording Servers in a deployment.
- Due to its intense graphical nature and memory usage when playing back large recordings, Citrix does not recommend installing the Session Recording Player as a published application.
- The Session Recording installation is configured for SSL/HTTPS communication. Ensure that you install a certificate on the Session Recording Server and that the root certificate authority (CA) is trusted on the Session Recording components.
- If you install the Session Recording Database on a stand-alone server running SQL Server 2014 Express Edition, SQL Server 2012 Express Edition, or SQL Server 2008 R2 Express Edition, the server must have TCP/IP protocol enabled and SQL Server Browser service running. These settings are disabled by default, but they must be enabled for the Session Recording Server to communicate with the database. See the Microsoft documentation for information about enabling these settings.
- Consider the effects of session sharing when planning your Session Recording deployment. Session sharing for published applications can conflict with Session Recording recording policy rules for published applications. Session Recording matches the active policy with the first published application that a user opens. After the user opens the first application, any subsequent applications opened during the same session continue to follow the policy that is in force for the first application. For example, if a policy states that only Microsoft Outlook should be recorded, the recording commences when the user opens Outlook. However, if the user opens a published Microsoft Word second (while Outlook is running), Word also is recorded. Conversely, if the active policy does not specify that Word should be recorded, and the user launches Word before Outlook (which should be recorded, according to the policy), Outlook is not recorded.

# 安装/升级 Session Recording

May 28, 2016

Before you start the installation, ensure that you completed this list:

	Step
	Install the prerequisites before starting the installation. See <a href="#">System Requirements</a> .
	Select the machines where you want to install each Session Recording component and ensure that each computer meets the hardware and software requirements for the component(s) you want to install.
	Download the Session Recording zip file or the LTSR image from the Citrix download page.
	If you use the SSL protocol for communication between the Session Recording components, install the requisite certificates in your environment. See <a href="#">Install certificates</a> .
	Configure Director to create and activate Session Recording policies. For more information, see <a href="#">Configure Director to use the Session Recording Server</a> .

Notes:

- Citrix recommends dividing published applications into separate delivery groups based on the recording policies because session sharing for published applications can conflict with active policies if they are in the same delivery group. Session Recording matches the active policy with the first published application that a user opens.
- If you are planning to use Machine Creation Services (MCS) or Provisioning Services with XenApp, prepare the server for a unique QMId. Failure to do so might result in recording data loss. For more information, see Known Issue #[528678](#).
- SQL server requires TCP/IP to be enabled, the SQL Server Browser service to be running, and Windows Authentication.
- If you want to use HTTPS, configure server certificates for SSL/HTTPS.

## Session Recording installation files

You need the following installation files from the Citrix download page:

- Session Recording Administration files
  - SessionRecordingAdministrationx64.msi
- Session Recording Agent files
  - SessionRecordingAgentx64.msi
- Session Recording Player files
  - SessionRecordingPlayer.msi

Session Recording Administration consists of the following components. You can install the components on a single server or on separate servers.

- Session Recording Database
- Session Recording Server
- Session Recording Policy Console.

Before installing the Session Recording Administration components, ensure you have all the prerequisites installed. See [Session Recording Administration components](#).

To improve security, you can remove these permissions after installing the database.

1. Run the **Broker\_PowerShellSnapIn\_x64.msi** file and follow the instructions to complete the installation. This installer is located in the Citrix Desktop Delivery Controller folder of the installation image.
2. Start the Windows command prompt as an administrator and then type:

```
msiexec /i SessionRecordingAdministrationx64.msi
```

or double click the .msi file.

3. On the installation UI, select Next and accept the license agreement.
4. On the Session Recording Administration Setup screen, select the Session Recording Administration components you want to install.

## Install the Session Recording Database

Before installing the Session Recording Database, ensure you have all prerequisites installed. See [Session Recording Administration components](#).

1. On the Database Configuration page:
  - If you are installing all Administration components on the same server, type **localhost** in the Session Recording Server Name field.
  - If you are installing the Session Recording Server and the Session Recording Database components on separate servers, type the name of the computer hosting the Session Recording Server in the following format: domain\machine-name. The Session Recording Server name is the user account for accessing the database.



If the database instance is not a named instance as you configured when you set up the instance, you can use only the machine name of the SQL Server. If you have named the instance, use machine-name\instance-name as the database instance name. To determine the server instance name you are using, run `select @@servername` on the SQL Server; the return value is the exact database instance name.

2. Click **Test** to test the connection to the SQL server. Make sure the current user account has the public SQL Server role permission; otherwise the test fails for lack of permissions. Then click **Next** to continue the installation.
3. Follow the instructions to complete the installation. During the installation, if the current user account is not a database administrator, a dialog box appears, requiring the credentials of a database administrator with **sysadmin** server role permission. Enter the correct credentials and click **OK** to continue the installation. The installation creates the new Session Recording Database and adds the machine account of the Session Recording Server as **db-owner**.

Note: To improve security, you can remove these permissions after installing the database.

## Install the Session Recording Server

Before installing the Session Recording Server, ensure that you have all prerequisites installed. See [Session Recording Administration components](#).

1. Enter the name of your SQL server in the Database Instance Name text box. If you are using a named instance, enter machine-name\instance-name; otherwise enter a machine-name only.
2. Click **Test** to test the connection to the SQL server. Make sure that the *current useraccount* has the public SQL Server role permission. Otherwise, the test fails for lack of permissions. Then click **Next** to continue and follow the instructions to complete the installation.

At the end of the installation wizard, you can choose to participate in the Citrix Customer Experience Improvement Program. When you join this program, anonymous statistics and usage information is sent to Citrix. For more information, see [About the Citrix Customer Experience Improvement Program \(CEIP\)](#).

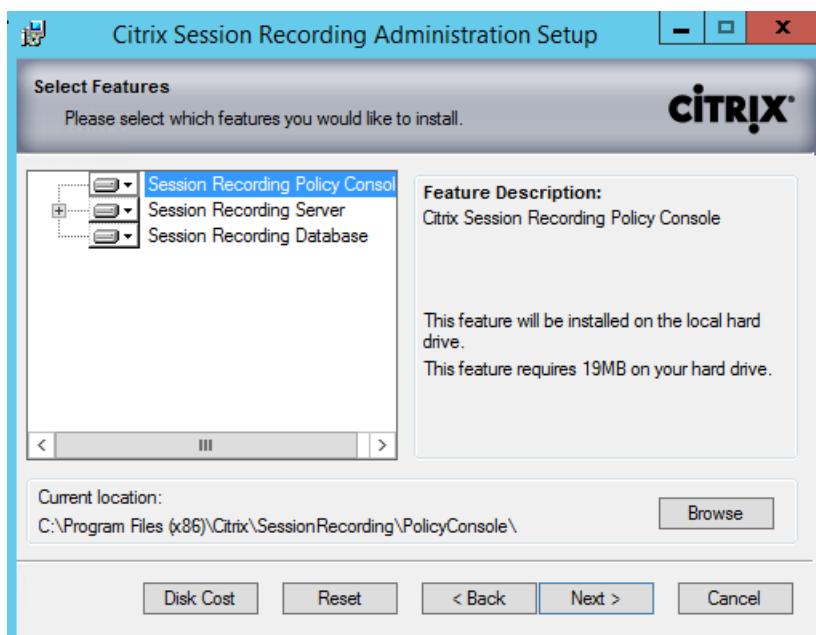
## Configure Director to use the Session Recording Server

You can use the Director console to create and activate Session Recording policies.

1. For an HTTPS connection, install the certificate to trust the Session Recording Server in the Trusted Root Certificates of the Director server.
2. To configure the Director server to use the Session Recording Server, run the `C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configsessionrecording` command.
3. Enter the IP address or FQDN of the Session Recording Server and the port number and connection type (HTTP/HTTPS) that the Session Recording Agent uses to connect to the Session Recording Broker on the Director server.

## Install the Session Recording Policy Console

1. On the Session Recording Administration Setup screen, select the Session Recording Policy Console to install.



2. Click **Next** to begin the installation. You can click **Browse** to change the installation path.

3. Click **Finish** when the installation completes.

## Install the Session Recording Agent

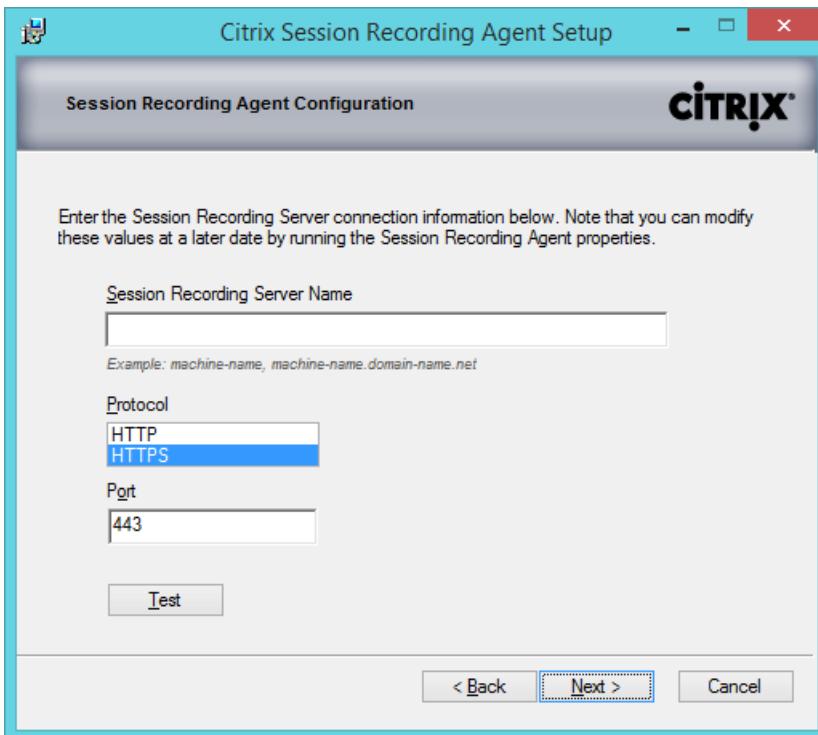
The Session Recording Agent must be installed on the VDA for Server OS on which you want to record sessions.

1. Use the Server Manager to install .NET Framework 3.5 and Microsoft Message Queuing (MSMQ) with HTTP support on the VDA for Server OS.
2. Start the Windows command prompt as an administrator, and then type:

```
msiexec /i SessionRecordingAgentx64.msi
```

or double click the .msi file.

3. On the installation UI, select **Next** and accept the license agreement.
4. In the Session Recording Agent Configuration page, enter the name of the computer where you installed the Session Recording Server and the protocol and port information for the connection to the Session Recording Server.



5. The Session Recording default installation uses HTTPS/SSL to secure communications. If SSL is not configured, use HTTP. To do so, deselect SSL in the IIS Management Console by navigating to the Session Recording Broker site. Open the SSL settings and clear the Require SSL box.

6. Follow the instructions to complete the installation.

Install the Session Recording Player on the Session Recording Server or on one or more workstations in the domain for users who view session recordings.

- Run the **SessionRecordingPlayer.msi** and follow the instructions to complete the installation.

Use Citrix Director to create and activate Session Recording policies.

1. For an https connection, install the certificate to trust the Session Recording Server in the Trusted Root Certificates of the Director server.
2. To configure the Director server to use the Session Recording Server, run the following command:

```
C:\inetpub\wwwroot\Director\tools\DirectorConfig.exe /configsessionrecording
```

3. Enter the IP/FQDN of the Session Recording Server, the port number and the connection type (http/https) between Session Recording Agent and Session Recording Broker on the Director server.

## Upgrade Session Recording

You can upgrade both the Agent and Player components from Version 7.6.100 to 7.6.1000.

- Use the Session Recording installer's graphical or command-line interface to upgrade the existing version of both components.
  - In addition to being a domain user, you must be a local administrator on the machines where you are upgrading the Session Recording components.
  - If there are live recording sessions underway while you upgrade the Session Recording Agent, the recordings will be interrupted.
  - Review the upgrade sequence below so you can plan and mitigate potential outages.
1. Upgrade the Session Recording Agent (on master image).
  2. Upgrade the Session Recording Player.

## Uninstall Session Recording

To remove Session Recording components from a server or workstation, use the uninstall or remove programs capability available through the Windows Control Panel. To remove the Session Recording Database, you must have the same sysadmin SQL server role permissions as when you installed it.

# 自动安装

May 28, 2016

To install Session Recording Agent on multiple servers, write a script that uses silent installation.

The following command line installs the Session Recording Agent and creates a log file to capture the install information.

```
msiexec /i SessionRecordingAgentx64.msi sessionrecordingservername=yourservername  
sessionrecordingbrokerproto=yourbrokerprotocol sessionrecordingbrokerport=yourbrokerport  
/l*v yourinstallationlog /q
```

where:

yourservername is the NetBIOS name or FQDN of the computer hosting the Session Recording Server. If not specified, this value defaults to localhost.

yourbrokerprotocol is either HTTP or HTTPS, and represents the protocol that Session Recording Agent uses to communicate with Session Recording Broker; this value defaults to HTTPS if not specified.

yourbrokerport is an integer representing the port Session Recording Agent uses to communicate with Session Recording Broker. If not specified, this value defaults to zero, which directs Session Recording Agent to use the default port number for the selected protocol: 80 for HTTP or 443 for HTTPS.

/l\*v specifies verbose mode logging

yourinstallationlog is the location of the setup log file created.

/q specifies quiet mode.

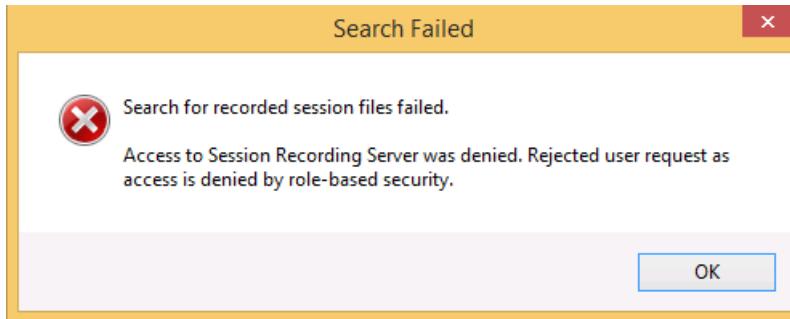
# 配置用于播放和录制会话的 Session Recording

May 28, 2016

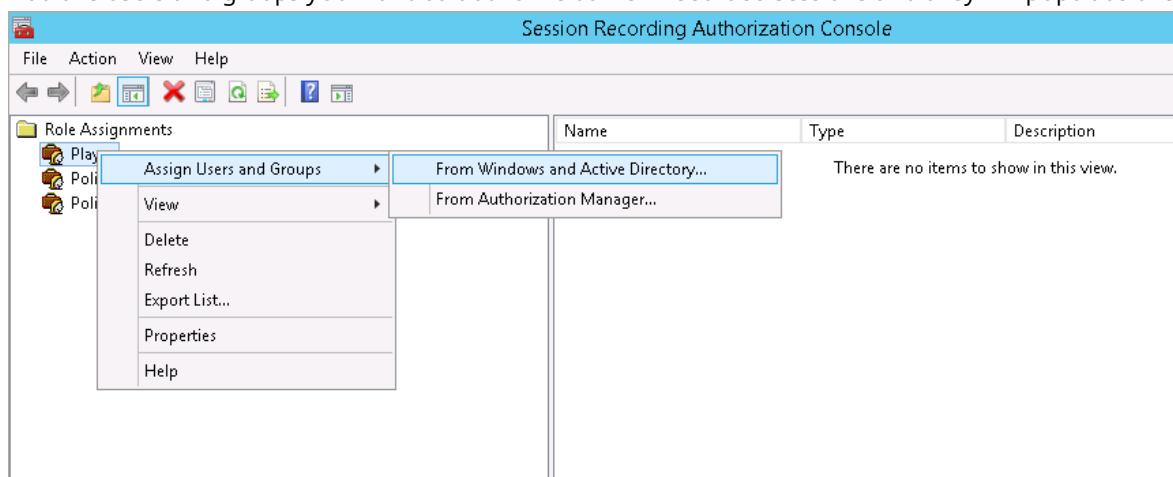
After you install the Session Recording components, perform these steps to configure Session Recording to record XenApp sessions and allow users to view them:

- Authorize users to play recordings
- Authorize users to administer recording policies
- Change the active recording policy to one that records sessions
- Configure Session Recording Player to connect to the Session Recording Server

When you install Session Recording, no users have permission to play recorded sessions. You must assign permission to each user, including the administrator. A user without permission to play recorded sessions receives the following error message when trying to play a recorded session:



1. Log on as administrator to the computer hosting the Session Recording Server.
2. Start the Session Recording Authorization Console.
3. In the Session Recording Authorization Console, select Player.
4. Add the users and groups you want to authorize to view recorded sessions and they will populate the right pane.



When you install Session Recording, domain administrators grant permission to control the recording policies by default. You can change the authorization setting.

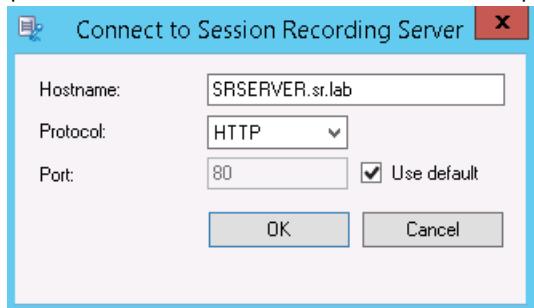
1. Log on as administrator to the machine hosting the Session Recording Server.

2. Start the Session Recording Authorization Console and select PolicyAdministrators.
3. Add the users and groups who can administer recording policies.

The active recording policy specifies session recording behavior on all Server OS VDAs that have Session Recording Agent installed and connected to the Session Recording Server. When you install Session Recording, the active recording policy is Do not record. Sessions cannot be recorded until you change the active recording policy.

1. Log on as an authorized Policy Administrator to the server where the Session Recording Policy Console is installed.
2. Start the Session Recording Policy Console.
3. If you are prompted by a Connect to Session Recording Server pop-up window, ensure that the name of the computer

hosting the Session Recording Server, protocol, and port are correct.



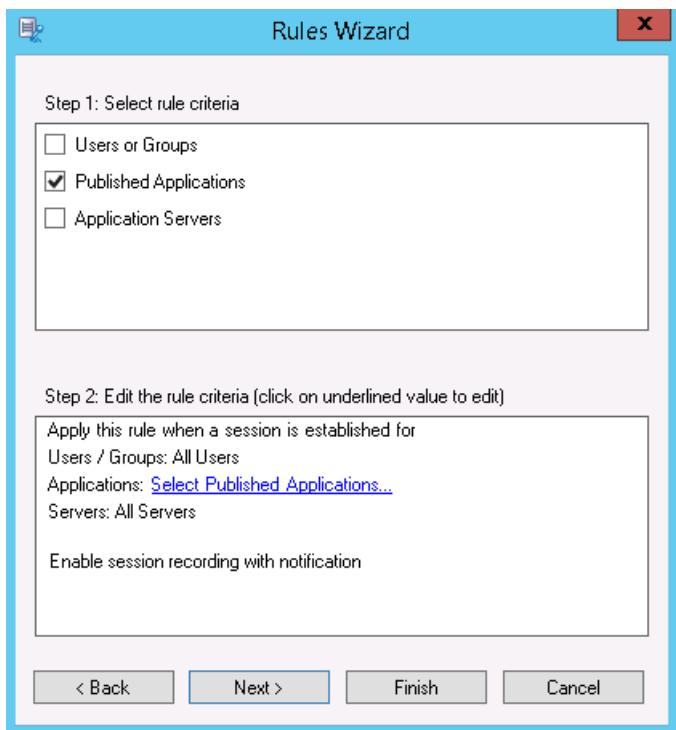
4. In the Session Recording Policy Console, expand Recording Policies. This displays the recording policies available when you install Session Recording, with a check mark indicating which policy is active:
  - Do not record. This is the default policy. If you do not specify another policy, no sessions are recorded.
  - Record everyone with notification. If you choose this policy, all sessions are recorded. A pop-up window appears notifying the user that recording is occurring.
  - Record everyone without notification. If you choose this policy, all sessions are recorded. A pop-up window does not appear notifying the user that recording is occurring.
5. Select the policy you want to make the active policy.
6. From the menu bar, choose Action > Activate Policy.

Note: Session Recording allows you to create your own recording policy. When you create recording policies, they appear in the Recording Policies folder within the Session Recording Policy Console.

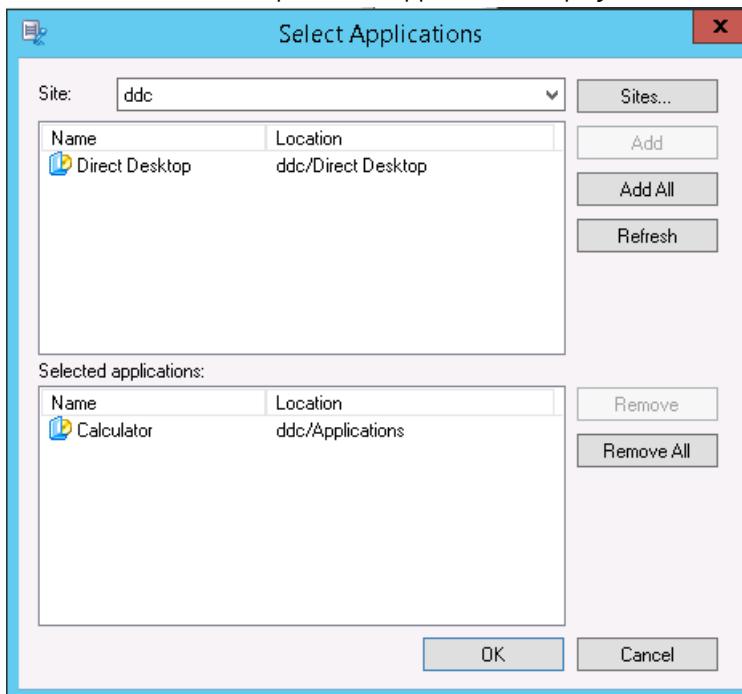
The generic recording policy might not fit your requirements. You can configure policies based on users, VDA servers, and applications.

**Important:** A policy can contain many rules, but there can be only one active policy running at a time.

1. Log on as an authorized Policy Administrator to the server where the Session Recording Policy Console is installed.
2. Start the Session Recording Policy Console and select Recording Policies > Add New Policy.
3. Right click New policy and select Add New Rule.
4. In the Rules wizard, select Enable Session Recording with notification , and then click Next.
5. Check the box Published Applications, and then click the hyperlink for Select Published Applications.



6. On the Select Applications screen, click Sites and Add.
7. Enter the server name of a XenApp 7.6 FP1 Delivery Controller.
8. Click Connect and the site enumerates.
9. Click Close and a list of published applications displays. Add some applications from the list, and then click OK and Finish.



10. Right click on the policy and select Activate. You can rename the policy if you want to.

Before a Session Recording Player can play sessions, you must configure it to connect to the Session Recording Server that stores the recorded sessions. Each Session Recording Player can be configured with the ability to connect to multiple Session Recording Servers, but can connect to only one Session Recording Server at a time. If the Player is configured with

the ability to connect to multiple Session Recording Servers, users can change which Session Recording Server the Player connects to by selecting a check box.

1. Log on to the workstation where Session Recording Player is installed.
2. Start the Session Recording Player.
3. From the Session Recording Player menu bar, choose Tools > Options.
4. In the Connections tab, click Add.
5. In the Hostname field, type the name or Internet protocol (IP) address of the computer hosting the Session Recording Server and select the protocol. By default Session Recording is configured to use HTTPS/SSL to secure communications. If SSL is not configured, select HTTP.
6. If you want to configure the Session Recording Player with the ability to connect to more than one Session Recording Server, repeat Steps 4 and 5 for each Session Recording Server.
7. Ensure that the check box for the Session Recording Server you want to connect to is selected.

# 授予用户访问权限

May 28, 2016

Note: For security reasons, grant users only the rights they need to perform specific functions, such as viewing recorded sessions.

You grant rights to Session Recording users by assigning them to roles using the Session Recording Authorization Console on the Session Recording Server. Session Recording users have three roles:

- **Player.** Grants the right to view recorded XenApp sessions. There is no default membership in this role.
- **PolicyQuery.** Allows the servers hosting the Session Recording Agent to request recording policy evaluations. By default, authenticated users are members of this role.
- **PolicyAdministrator.** Grants the right to view, create, edit, delete, and enable recording policies. By default, administrators of the computer hosting the Session Recording Server are members of this role.

Session Recording supports users and groups defined in Active Directory.

1. Log on to computer hosting the Session Recording Server, as administrator or as a member of the Policy Administrator role.
2. Start the Session Recording Authorization Console.
3. Select the role to which you want to assign users.
4. Choose Action > Assign Windows Users and Groups.
5. Add the users and groups.

Any changes made to the console take effect during the update that occurs once every minute.

# 创建并激活录制策略

May 28, 2016

Use the Session Recording Policy Console to create and activate policies that determine which sessions are recorded.

You can activate system policies available when Session Recording is installed or create and activate your own custom policies. Session Recording system policies apply a single rule to all users, published applications, and servers. Custom policies specifying which users, published applications, and servers are recorded.

The active policy determines which sessions are recorded. Only one policy is active at a time.

Session Recording provides these system policies:

- **Do not record.** If you choose this policy, no sessions are recorded. This is the default policy; if you do not specify another policy, no sessions are recorded.
- **Record everyone with notification.** If you choose this policy, all sessions are recorded. A pop-up window appears notifying the user that recording is occurring.
- **Record everyone without notification.** If you choose this policy, all sessions are recorded. A pop-up window does not appear notifying the user that recording is occurring.

System policies cannot be modified or deleted.

1. Log on to the server where the Session Recording Policy Console is installed.
2. Start the Session Recording Policy Console.
3. If you are prompted by a Connect to Session Recording Server pop-up window, ensure that the name of the Session Recording Server, protocol, and port are correct. Click OK.
4. In the Session Recording Policy Console, expand Recording Policies.
5. Select the policy you want to make the active policy.
6. From the menu bar, choose Action > Activate Policy.

When you create your own policy, you make rules to specify which users and groups, published applications, and servers have their sessions recorded. A wizard within the Session Recording Policy Console helps you create rules. To obtain the list of published applications and servers, you must have the site administrator read permission. Configure that on this site's Delivery Controller.

For each rule you create, you specify a recording action and a rule criteria. The recording action applies to sessions that meet the rule criteria.

For each rule, choose one recording action:

- Do not record. (Choose Disable session recording within the rules wizard.) This recording action specifies that sessions that meet the rule criteria are not recorded.
- Record with notification. (Choose Enable session recording with notification within the rules wizard.) This recording action specifies that sessions that meet the rule criteria are recorded. A pop-up window appears notifying the user that

recording is occurring.

- Record without notification. (Choose Enable session recording without notification within the rules wizard.) This recording action specifies that sessions that meet the rule criteria are recorded. Users are unaware that they are being recorded.

For each rule, choose at least one of the following to create the rule criteria:

- Users or Groups. You create a list of users or groups to which the recording action of the rule applies.
- Published Applications. You create a list of published applications to which the recording action of the rule applies. Within the rules wizard, choose the XenApp site or sites on which the applications are available.
- Applications Servers. You create a list of Server OS machines to which the recording action of the rule applies. Within the rules wizard, choose the XenApp site or sites where the servers reside.

When you create more than one rule in a recording policy, some sessions may match the criteria for more than one rule. In these cases, the rule with the highest priority is applied to the session.

The recording action of a rule determines its priority:

- Rules with the Do not record action have the highest priority
- Rules with the Record with notification action have the next highest priority
- Rules with the Record without notification action have the lowest priority

Some sessions may not meet any rule criteria in a recording policy. For these sessions, the recording action of the policies fallback rule applies. The recording action of the fallback rule is always Do not record. The fallback rule cannot be modified or deleted.

## Using Active Directory Groups

Session Recording allows you to use Active Directory groups when creating policies. Using Active Directory groups instead of individual users simplifies creation and management of rules and policies. For example, if users in your company's finance department are contained in an Active Directory group named Finance, you can create a rule that applies to all members of this group by selecting the Finance group within the rules wizard when creating the rule.

## White Listing Users

You can create Session Recording policies that ensure that the sessions of some users in your organization are never recorded. This is called white listing these users. White listing is useful for users who handle privacy-related information or when your organization does not want to record the sessions of a certain class of employees.

For example, if all managers in your company are members of an Active Directory group named Executive, you can ensure that these users' sessions are never recorded by creating a rule that disables session recording for the Executive group. While the policy containing this rule is active, no sessions of members of the Executive group are recorded. The sessions of other members of your organization are sessions recorded based on other rules in the active policy.

## Create a new policy

Note: When using the rules wizard, you may be prompted to "click on underlined value to edit" when no underlined value appears. Underlined values appear only when applicable. If no underline values appear, ignore the step.

1. Log on to the server where Session Recording Policy Console is installed.
2. Start the Session Recording Policy Console.
3. If you are prompted by a Connect to Session Recording Server pop-up window, ensure that the name of the Session

- Recording Server, protocol, and port are correct. Click OK.
4. In the Session Recording Policy Console, select Recording Policies.
  5. From the menu bar, choose Action > Add New Policy. A policy called New Policy appears in the left pane.
  6. Select the new policy and choose Action > Rename from the menu bar.
  7. Type a name for the policy you are about to create and press Enter or click anywhere outside the new name.
  8. With the policy selected, choose Action > Add New Rule from the menu bar to launch the rules wizard.
  9. Follow the instructions to create the rules for this policy.

## Modify a policy

1. Log on to the server where the Session Recording Policy Console is installed.
2. Start the Session Recording Policy Console.
3. If you are prompted by a Connect to Session Recording Server pop-up window, ensure that the name of the Session Recording Server, protocol, and port are correct. Click OK.
4. In the Session Recording Policy Console, expand Recording Policies.
5. Select the policy you want to modify. The rules for the policy appear in the right pane.
6. Add a new rule, modify a rule, or delete a rule:
  - From the menu bar, choose Action > Add New Rule. If the policy is active, a pop-up window appears requesting confirmation of the action. Use the rules wizard to create a new rule.
  - Select the rule you want to modify, right-click, and choose Properties. Use the rules wizard to modify the rule.
  - Select the rule you want to delete, right-click, and choose Delete Rule.

## Delete a policy

Note: You cannot delete a system policy or a policy that is active.

1. Log on to the server where the Session Recording Policy Console is installed.
2. Start the Session Recording Policy Console.
3. If you are prompted by a Connect to Session Recording Server pop-up window, ensure that the name of the Session Recording Server, protocol, and port are correct. Click OK.
4. In the Session Recording Policy Console, expand Recording Policies.
5. In the left pane, select the policy you want to delete. If the policy is active, you must activate another policy.
6. From the menu bar, choose Action > Delete Policy.
7. Select Yes to confirm the action.

When you activate a policy, the previously active policy remains in effect until the user's session ends; however, in some cases, the new policy takes effect when the file rolls over. Files roll over when they have reached the maximum size limit. For information on maximum file sizes for recordings, see [Specify file size for recordings](#).

The following table details what happens when you apply a new policy while a session is being recorded and a rollover occurs:

If the previous policy was:	And the new policy is:	After a rollover the policy will be:
Do not record	Any other policy	No change. The new policy takes effect only when the user logs on to a new session.

Record without notification If the previous policy was:	Do not record And the new policy is: Record with notification	Recording stops. After a rollover the policy will be: Recording continues and a notification message appears.
Record with notification	Do not record	Recording stops.
	Record without notification	Recording continues. No message appears the next time a user logs on.

# 禁用或启用录制

May 28, 2016

You install the Session Recording Agent on each Server OS machine for which you want to record sessions. Within each agent is a setting that enables recording for the server on which it is installed. After recording is enabled, Session Recording evaluates the active recording policy, which determines which sessions are recorded.

When you install the Session Recording Agent, recording is enabled. Citrix recommends that you disable Session Recording on servers that are not recorded because they experience a small impact on performance, even if no recording takes place.

1. Log on to the server where the Session Recording Agent is installed.
2. From the Start menu, choose Session Recording Agent Properties.
3. Under Session Recording, select or clear the Enable session recording for this Server OS VDA check box to specify whether or not sessions can be recorded for this server.
4. When prompted, restart the Session Recording Agent Service to accept the change.

Note: When you install Session Recording, the active policy is Do not record (no sessions are recorded on any server). To begin recording, use the Session Recording Policy Console to activate a different policy.

# 配置与 Session Recording Server 的连接

May 28, 2016

The connection between the Session Recording Agent and the Session Recording Server is typically configured when the Session Recording Agent is installed. To configure this connection after Session Recording Agent is installed, use Session Recording Agent Properties.

1. Log on to the server where Session Recording Agent is installed.
2. From the Start menu, choose Session Recording Agent Properties.
3. Click the Connections tab.
4. In the Session Recording Server field, type the server name or its Internet protocol (IP) address.
5. In the Session Recording Storage Manager message queue section, select the protocol that is used by the Session Recording Storage Manager to communicate and modify the default port number, if necessary.
6. In the Message life field, accept the default of 7200 seconds (two hours) or type a new value for the number of seconds each message is retained in the queue if there is a communication failure. After this period of time elapses, the message is deleted and the file is playable until the point where the data is lost.
7. In the Session Recording Broker section, select the communication protocol the Session Recording Broker uses to communicate and modify the default port number, if necessary.
8. When prompted, restart the Session Recording Agent Service to accept the changes.

# 创建通知消息

May 28, 2016

If the active recording policy specifies that users are notified when their sessions are recorded, a pop-up window appears displaying a notification message after users type their credentials. The following message is the default notification: "Your activity with one or more of the programs you recently started is being recorded. If you object to this condition, close the programs." The user clicks OK to dismiss the window and continue the session.

The default notification message appears in the language of the operating system of the computers hosting the Session Recording Server.

You can create custom notifications in languages of your choice; however, you can have only one notification message for each language. Your users see the notification message in the language corresponding to their user preferred locale settings.

1. Log on to the computer hosting the Session Recording Server.
2. From the Start menu, choose Session Recording Server Properties.
3. In Session Recording Server Properties, click the Notifications tab.
4. Click Add.
5. Choose the language for the message and type the new message. You can create only one message for each language.

After accepting and activating, the new message appears in the Language-specific notification messages box.

# 启用自定义事件录制

May 28, 2016

Session Recording allows you to use third-party applications to insert custom data, known as events, into recorded sessions. These events appear when the session is viewed using the Session Recording Player. They are part of the recorded session file and cannot be modified after the session is recorded.

For example, an event might contain the following text: “User opened a browser.” Each time a user opens a browser during a session that is being recorded, the text is inserted into the recording at that point. When the session is played using the Session Recording Player, the viewer can locate and count the times that the user opened a browser by noting the number of markers that appear in the Events and Bookmarks list in the Session Recording Player.

To insert custom events into recordings on a server:

- Use Session Recording Agent Properties to enable a setting on each server where you want to insert custom events. You must enable each server separately; you cannot globally enable all servers in a site.
- Write applications built on the Event API that runs within each user’s XenApp session (to inject the data into the recording).

The Session Recording installation includes an event recording COM application (API) that allows you to insert text from third-party applications into a recording. You can use the API from many programming languages including Visual Basic, C++, or C#. The Session Recording Event API .dll is installed as part of the Session Recording installation. You can find it at C:\Program Files\Citrix\SessionRecording\Agent\Bin\Interop.UserApi.dll.

1. Log on to the server where the Session Recording Agent is installed.
2. From the Start menu, choose Session Recording Agent Properties.
3. In Session Recording Agent Properties, click the Recording tab.
4. Under Custom event recording, select the Allow third party applications to record custom data on this XenApp server check box.

# 启用或禁用实时会话播放

May 28, 2016

Using Session Recording Player, you can view a session after or while it is being recorded. Viewing a session that is currently recording is similar to seeing actions happening live; however, there is actually a one to two second delay as the data propagates from the XenApp server.

Some functionality is not available when viewing sessions that have not completed recording:

- A digital signature cannot be assigned until recording is complete. If digital signing is enabled, you can view live playback sessions, but they are not digitally signed and you cannot view certificates until the session is completed.
- Playback protection cannot be applied until recording is complete. If playback protection is enabled, you can view live playback sessions, but they are not encrypted until the session is completed.
- You cannot cache a file until recording is complete.

By default, live session playback is enabled.

1. Log on to the computer hosting the Session Recording Server.
2. From the Start menu, choose Session Recording Server Properties.
3. In Session Recording Server Properties, click the Playback tab.
4. Select or clear the Allow live session playback check box.

# 启用或禁用播放保护

May 28, 2016

As a security precaution, Session Recording automatically encrypts recorded files before they are downloaded for viewing in the Session Recording Player. This playback protection prevents them from being copied and viewed by anyone other than the user who downloaded the file. The files cannot be played back on another workstation or by another user. Encrypted files are identified with an .icle extension; unencrypted files are identified with an .icl extension. The files remain encrypted while they reside in the cache on the workstation where the Session Recording Player is installed until they are opened by an authorized user.

Citrix recommends that you use HTTPS to protect the transfer of data.

By default, playback protection is enabled.

1. Log on to the computer hosting the Session Recording Server.
2. From the Start menu, choose Session Recording Server Properties.
3. In Session Recording Server Properties, click the Playback tab.
4. Select or clear the Encrypt session recording files downloaded for playback check box.

# 启用和禁用数字签名

May 28, 2016

If you installed certificates on the computers on which the Session Recording components are installed, you can enhance the security of your Session Recording deployment by assigning digital signatures to session recording.

By default, digital signing is disabled.

1. Log on to the computer hosting the Session Recording Server.
  2. From the Start menu, choose Session Recording Server Properties.
  3. In Session Recording Server Properties, click the Signing tab.
  4. Browse to the certificate that enables secure communication among the computers on which the Session Recording components are installed.
- 
1. Log on to the computer hosting the Session Recording Server.
  2. From the Start menu, choose Session Recording Server Properties.
  3. In Session Recording Server Properties, click the Signing tab.
  4. Click Clear.

# 指定录制件的存储位置

May 28, 2016

Use Session Recording Server Properties to specify where recordings are stored and where archived recordings are restored.

Note: To archive files or restore deleted files, use the icldb command.

By default, recordings are stored in the drive:\SessionRecordings directory of the computer hosting the Session Recording Server. You can change the directory where the recordings are stored, add additional directories to load-balance across multiple volumes, or make use of additional space. Multiple directories in the list indicates recordings are load-balanced across the directories. You can add a directory multiple times. Load balancing cycles through the directories.

1. Log on to the computer hosting the Session Recording Server.
2. From the Start menu, choose Session Recording Server Properties.
3. In Session Recording Server Properties, click the Storage tab.
4. Use the File storage directories list to manage the directories where recordings are stored.

You can create file storage directories on the local drive, the SAN volume, or a location specified by a UNC network path. Network mapped drive letters are not supported. Do not use Session Recording with Network-Attached Storage (NAS), due to serious performance and security problems associated with writing recording data to a network drive.

By default, archived recordings are restored to the drive:\SessionRecordingsRestore directory of the computer hosting the Session Recording Server. You can change the directory where the archived recordings are restored.

1. Log on to the computer hosting the Session Recording Server.
2. From the Start menu, choose Session Recording Server Properties.
3. In Session Recording Server Properties, click the Storage tab.
4. In the Restore directory for archived files field, type the directory for the restored archive files.

# 指定录制的文件大小

May 28, 2016

As recordings grow in size, the files can take longer to download and react more slowly when you use the seek slider to navigate during playback. To control file size, specify a threshold limit for a file. When the recording reaches this limit, Session Recording closes the file and opens a new one to continue recording. This action is called a rollover.

You can specify two thresholds for a rollover:

- **File size.** When the file reaches the specified number of megabytes, Session Recording closes the file and opens a new one. By default, files roll over after reaching 50 megabytes; however, you can specify a limit from 10 megabytes to one gigabyte.
- **Duration.** After the session records for the specified number of hours, the file is closed and a new file is opened. By default, files roll over after recording for 12 hours; however, you can specify a limit from one to 24 hours.

Session Recording checks both fields to determine which event occurs first to determine when to rollover. For example, if you specify 17MB for the file size and six hours for the duration and the recording reaches 17MB in three hours, Session Recording reacts to the 17MB file size to close the file and open a new one.

To prevent the creation of many small files, Session Recording does not rollover until at least one hour elapses (this is the minimum number that you can enter) regardless of the value specified for the file size. The exception to this rule is if the file size surpasses one gigabyte.

1. Log on to the computer hosting the Session Recording Server.
2. From the Start menu, choose Session Recording Server Properties.
3. In Session Recording Server Properties, click the Rollover tab.
4. Enter an integer between 10 and 1024 to specify the maximum file size in megabytes.
5. Enter an integer between 1 and 24 to specify the maximum recording duration in hours.

# 查看录制

May 28, 2016

Use Session Recording Player to view, search, and bookmark recorded XenApp or XenDesktop sessions.

If sessions are recorded with the live playback feature enabled, you can view sessions that are in progress, with a delay of a few seconds, as well as sessions that are completed.

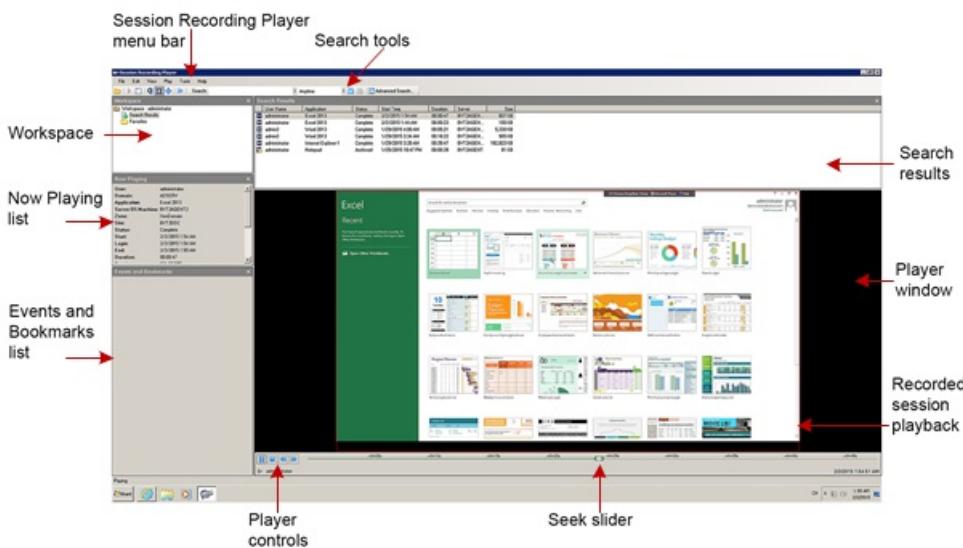
Sessions that have a longer duration or larger file size than the limits configured by your Session Recording administrator appear in more than one session file.

Note: A Session Recording administrator must grant users the right to access to recorded Server OS machine sessions. If you are denied access to viewing sessions, contact your Session Recording administrator.

When Session Recording Player is installed, the Session Recording administrator typically sets up a connection between the Session Recording Player and a Session Recording Server. If this connection is not set up, the first time you perform a search for files, you are prompted to set it up. Contact your Session Recording administrator for set up information.

1. Log on to the workstation where Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.  
The Session Recording Player appears.

This illustration shows the Session Recording Player with callouts indicating its major elements. The functions of these elements are described throughout following articles.



The Session Recording Player has window elements that toggle on and off.

1. Log on to the workstation where the Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. From the Session Recording Player menu bar, choose View.
4. Choose the elements that you want to display. Selecting an element causes it to appear immediately. A check mark indicates that the element is selected.

If the Session Recording administrator set up your Session Recording Player with the ability to connect to more than one Session Recording Server, you can select the Session Recording Server that the Session Recording Player connects to. The Session Recording Player can connect to only one Session Recording Server at a time.

1. Log on to the workstation where the Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. From the Session Recording Player menu bar, choose Tools > Options > Connections.
4. Select the Session Recording Server to which you want to connect.

# 打开和播放录制件

May 28, 2016

You can open session recordings in Session Recording Player in three ways:

- Perform a search using the Session Recording Player. Recorded sessions that meet the search criteria appear in the search results area.
- Access recorded session files directly from your local disk drive or a share drive.
- Access recorded session files from a Favorites folder

When you open a file that was recorded without a digital signature, a warning appears telling you that the origin and integrity of the file was not verified. If you are confident of the integrity of the file, click Yes in the warning pop-up window to open the file.

1. Log on to the workstation where Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. Perform a search.
4. If the search results area is not visible, select Search Results in the Workspace pane.
5. In the search results area, select the session you want to play.
6. Do any of the following:
  - Double-click the session
  - Right-click and select Play
  - From the Session Recording Player menu bar, select Play > Play

Recorded session file names begin with an *i*\_, followed by a unique alphanumeric file ID, followed by the .icl and .icle file extension: .icl for recordings without playback protection applied, .icle for recordings with playback protection applied. Session Recording saves recorded session files in a directory structure that incorporates the date the session was recorded. For example, the file for a session recorded on December 22, 2014, is saved in folder path 2014\12\22.

1. Log on to the workstation where Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. Do any of the following:
  - From the Session Recording Player menu bar, select File > Open and browse for the file
  - Using Windows Explorer, navigate to the file and drag the file into the Player window
  - Using Windows Explorer, navigate to and double-click the file
  - If you created Favorites in the Workspace pane, select Favorites and open the file from the Favorites area in the same way you open files from the search results area

Creating Favorites folders allows you to quickly access recordings that you view frequently. These Favorites folders reference recorded session files that are stored on your workstation or on a network drive. You can import and export these files to other workstations and share these folders with other Session Recording Player users.

Note: Only users with access rights to Session Recording Player can download the recorded session files associated with Favorites folders. Contact your Session Recording administrator for access rights.

To create a Favorites subfolder:

1. Log on to the workstation where Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. In the Session Recording Player, select the Favorites folder in your Workspace pane.
4. From the menu bar, choose File > Folder > New Folder. A new folder appears under the Favorites folder.
5. Type the folder name, then press Enter or click anywhere to accept the new name.

Use the other options that appear in the File > Folder menu to delete, rename, move, copy, import, and export the folders.

# 搜索录制的会话

May 28, 2016

Session Recording Player allows you to perform quick searches, perform advanced searches, and specify options that apply to all searches. Results of searches appear in the search results area of the Session Recording Player.

Note: To display all available recorded sessions, up to the maximum number of sessions that may appear in a search, perform a search without specifying any search parameters.

To perform a quick search

1. Log on to the workstation where Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. Define your search criteria:
  - Enter a search criterion in the Search field. To assist you:
  - Move the mouse pointer over the Search label to display a list of parameters to use as a guideline
  - Click the arrow to the right of the Search field to display the text for the last 64 searches you performed
  - Use the drop-down list to the right of the Search field to select a period or duration specifying when the session was recorded.
4. Click the binocular icon to the right of the drop-down list to start the search.

To perform an advanced search

Tip: Advanced searches might take up to 20 seconds to return results containing more than 150K entities. Citrix recommends using more accurate search conditions such as a date range or user to reduce the result number.

1. Log on to the workstation where Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. In the Session Recording Player window, click Advanced Search on the tool bar or choose Tools > Advanced Search.
4. Define your search criteria in the tabs of the Advanced Search dialog box:
  - Common allows you to search by domain or account authority, site, group, Server OS machine, application, or file ID.
  - Date/Time allows you to search date, day of week, and time of day.
  - Events allows you to search on custom events that your Session Recording administrator inserted to the sessions.
  - Other allows you to search by session name, client name, client address, and recording duration. It also allows you to specify, for this search, the maximum number of search results displayed and whether or not archived files are included in the search.

As you specify search criteria, the query you are creating appears in the pane at the bottom of the dialog box.

5. Click Search to start the search.

Tip: You can save and retrieve advanced search queries. Click Save within the Advanced Search dialog box to save the current query. Click Open within the Advanced Search dialog box to retrieve a saved query. Queries are saved as files with an .isq extension.

To set search options

Session Recording Player search options allow you to limit maximum number of session recordings that appear in search results and to specify whether or not search results include archived session files.

1. Log on to the workstation where Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. From the Session Recording Player menu bar, choose Tools > Options > Search.
4. In the Maximum result to display field, type the number of search results you want to display. A maximum of 500 results

can be displayed.

5. To set whether or not archived files are included in searches, select or clear Include archived files.

# 播放录制的会话

May 28, 2016

After you open a recorded session in the Session Recording Player, you can navigate through the recorded sessions using these methods:

- Use the player controls to play, stop, pause, and increase or decrease playback speed
- Use the seek slider to move forward or backward

If you have inserted markers into the recording or if the recorded session contains custom events, you can also navigate through the recorded session by going to those markers and events.

Note:

- During playback of a recorded session, a second mouse pointer may appear. The second pointer appears at the point in the recording when the user navigated within Internet Explorer and clicked an image that was originally larger than the screen but was scaled down automatically by Internet Explorer. While only one pointer appears during the session, two may appear during playback.
- This version of Session Recording does not support SpeedScreen Multimedia Acceleration for XenApp or the Flash quality adjustment policy setting for XenApp. When this option is enabled, playback displays a black square.
- Session Recording cannot record the Lync webcam video when using the HDX RealTime Optimization Pack for Microsoft Lync.

## Use player controls

You can click the player controls under the Player window or access them by choosing Play from the Session Recording Player menu bar. Use Player controls to:

	Play the selected session file.
	Pause playback.
	Stop playback. If you click Stop, then Play, the recording restarts at the beginning of the file.
	Halve the current playback speed down to a minimum of one-quarter normal speed.
	Double the current playback speed up to a maximum of 32 times normal speed.

## Use the seek slider

Use the seek slider below the Player window to jump to a different position within the recorded session. You can drag the seek slider to the point in the recording you want to view or click anywhere on the slider bar to move to that location.

You can also use the following keyboard keys to control the seek slider:

Key:	Seek action:
Home	Seek to the beginning.
End	Seek to the end.

<b>Key:</b> Right Arrow	<b>Seek action:</b> Seek forward five seconds.
Left Arrow	Seek backward five seconds.
Move mouse wheel one notch down	Seek forward 15 seconds.
Move mouse wheel one notch up	Seek backward 15 seconds.
Ctrl + Right Arrow	Seek forward 30 seconds.
Ctrl + Left Arrow	Seek backward 30 seconds.
Page Down	Seek forward one minute.
Page Up	Seek backward one minute.
Ctrl + Move mouse wheel one notch down	Seek forward 90 seconds.
Ctrl + Move mouse wheel one notch up	Seek backward 90 seconds.
Ctrl + Page Down	Seek forward six minutes.
Ctrl + Page Up	Seek backward six minutes.

Note: To adjust the speed of the seek slider: From the Session Recording Player menu bar, choose Tools > Options > Player and drag the slider to increase or decrease the seek response time. A faster response time requires more memory. The response might be slow depending on the size of the recordings and your machine's hardware.

#### To change the playback speed

You can set Session Recording Player to play recorded sessions in exponential increments from one-quarter normal playback speed to 32 times normal playback speed.

1. Log on to the workstation where the Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. From the Session Recording Player menu bar, choose Play > Play Speed.
4. Choose a speed option.

The speed adjusts immediately. A number indicating the increased or decreased speed appears below the Player window controls. Text indicating the exponential rate appears briefly in green in the Player window.

#### To skip over spaces where no action occurred

Fast review mode allows you to set Session Recording Player to skip the portions of recorded sessions in which no action takes place. This setting saves time for playback viewing; however, it does not skip animated sequences such as animated mouse pointers, flashing cursors, or displayed clocks with second hand movements.

1. Log on to the workstation where Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. From the Session Recording Player menu bar, choose Play > Fast Review Mode.

The option toggles on and off. Each time you choose it, its status appears briefly in green in the Player window.

# 使用事件和书签

May 28, 2016

You can use events and bookmarks to help you navigate through recorded sessions.

Events are inserted to sessions as they are recorded, using the Event API and a third-party application. Events are saved as part of the session file. You cannot delete or alter them using the Session Recording Player.

Bookmarks are markers you insert into the recorded sessions using the Session Recording Player. Bookmarks are associated with the recorded session until you delete them, but they are not saved as part of the session file. By default, each bookmark is labeled with the text Bookmark, but you can change this to any text annotation up to 128 characters long.

Events and bookmarks appear as dots under the Player window. Events appear as yellow dots; bookmarks appear as blue dots. Moving the mouse over these dots displays the text label associated with them. You can also display the events and bookmarks in the events and bookmarks list of the Session Recording Player. They appear in this list with their text labels and the times in the recorded session at which they appear, in chronological order.

You can use events and bookmarks to help you navigate through recorded sessions. By going to an event or bookmark, you can skip to the point in the recorded session where the event or bookmark is inserted.

## To display events and bookmarks in the list

The events and bookmarks list displays the events and bookmarks inserted in the recorded session that is currently playing. It can show events only, bookmarks only, or both.

1. Log on to the workstation where the Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. Move the mouse pointer into the events and bookmarks list area and right-click to display the menu.
4. Choose Show Events Only, Show Bookmarks Only, or Show All.

## To insert a bookmark

1. Log on to the workstation where the Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. Begin playing the recorded session to which you want to add a bookmark.
4. Move the seek slider to the position where you want to insert the bookmark.
5. Move the mouse pointer into the Player window area and right-click to display the menu.
6. Add a bookmark with the default label Bookmark or create an annotation:
  - To add a bookmark with the default label Bookmark, choose Add Bookmark.
  - To add a bookmark with a descriptive text label that you create, choose Add Annotation. Type the text label you want to assign to the bookmark, up to 128 characters. Click OK.

## To add or change an annotation

After a bookmark is created, you can add an annotation to it or change its annotation.

1. Log on to the workstation where Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. Begin playing the recorded session containing the bookmark.
4. Ensure that the events and bookmarks list is displaying bookmarks.
5. Select the bookmark in the events and bookmarks list and right-click to display the menu.

6. Choose Edit Annotation.
7. In the window that appears, type the new annotation and click OK.

#### To delete a bookmark

1. Log on to the workstation where Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. Begin playing the recorded session containing the bookmark.
4. Ensure that the events and bookmarks list is displaying bookmarks.
5. Select the bookmark in the events and bookmarks list and right-click to display the menu.
6. Choose Delete.

#### To go to an event or bookmark

Going to an event or bookmark causes the Session Recording Player to go to the point in the recorded session where the event or bookmark is inserted.

1. Log on to the workstation where the Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. Begin playing a session recording containing events or bookmarks.
4. Go to an event or bookmark:
  - In the area below the Player window, click the dot representing the event or bookmark to go to the event or bookmark.
  - In the events and bookmarks list, double-click the event or bookmark to go to it. To go to the next event or bookmark, select any event or bookmark from the list, right-click to display the menu, and choose Seek to Bookmark.

# 更改播放显示

May 28, 2016

Options allow you to change how recorded sessions appear in the Player window. You can pan and scale the image, show the playback in full-screen mode, display the Player window in a separate window, and display a red border around the recorded session to differentiate it from the Player window background.

## To display the Player window in full-screen format

1. Log on to the workstation where the Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. From the Session Recording Player menu bar, choose View > Player Full Screen.
4. To return to the original size, press ESC or F11.

## To display the Player window in a separate window

1. Log on to the workstation where the Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. From the Session Recording Player menu bar, choose View > Player in Separate Window. A new window appears containing the Player window. You can drag and resize the window.
4. To embed the Player window in the main window, choose View > Player in Separate Window, or press F10.

## To scale the session playback to fit the Player window

1. Log on to the workstation where the Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. From the Session Recording Player menu bar, choose Play > Panning and Scaling > Scale to Fit.
  - Scale to Fit (Fast Rendering) shrinks the image while providing a good quality image. Images are drawn quicker than when using the High Quality option but the images and text are not as sharp. Use this option if you are experiencing performance issues when using the High Quality mode.
  - Scale to Fit (High Quality) shrinks the image while providing high quality images and text. Using this option may cause the images to be drawn more slowly than the Fast Rendering option.

## To pan the image

1. Log on to the workstation where the Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. From the Session Recording Player menu bar, choose Play > Panning and Scaling > Panning. The pointer changes to a hand and a small representation of the screen appears in the top right of the Player window.
4. Drag the image. The small representation indicates where you are in the image.
5. To stop panning, choose one of the scaling options.

## To display a red border around the session recording

1. Log on to the workstation where the Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. From the Session Recording Player menu bar, choose Tools > Options > Player from the menu bar.
4. Select the Show border around session recording check box.

Tip: If the Show border around session recording check box is not selected, you can temporarily view the red border by

clicking and holding down the left mouse button while the pointer is in the Player window.

# 缓存录制的会话文件

May 28, 2016

Each time you open a recorded session file, the Session Recording Player downloads the file from the location where the recordings are stored. If you download the same files frequently, you can save download time by caching the files on your workstation. Cached files are stored on your workstation in this folder.

`userprofile\AppData\Local\Citrix\SessionRecording\Player\Cache`

You can specify how much disk space is used for the cache. When the recordings fill the specified disk space, Session Recording deletes the oldest, least used recordings to make room for new recordings. You can empty the cache at any time to free up disk space.

## To enable caching

1. Log on to the workstation where the Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. From the Session Recording Player menu bar, choose Tools > Options > Cache.
4. Select the Cache downloaded files on local machine check box.
5. If you want to limit the amount of disk space used for caching, select the Limit amount of disk space to use check box and specify the number of megabytes to be used for cache.
6. Click OK.

## To empty cache

1. Log on to the workstation where the Session Recording Player is installed.
2. From the Start menu, choose Session Recording Player.
3. From the Session Recording Player menu bar, choose Tools > Options > Cache.
4. Select the Cache downloaded files on local machine check box.
5. In the Session Recording Player, choose Tools > Options > Cache.
6. Click Purge Cache, then OK to confirm the action.

# Session Recording 故障排除

May 28, 2016

This troubleshooting information contains solutions to some issues you may encounter during and after installing Session Recording components:

- Components failing to connect to each other
- Sessions failing to record
- Problems with the Session Recording Player or Session Recording Policy Console
- Issues involving your communication protocol

## Session Recording Agent cannot connect

When Session Recording Agent cannot connect, the Exception caught while sending poll messages to Session Recording Broker event message is logged, followed by the exception text. The exception text provides the reason why the connection failed. These reasons include:

- The underlying connection was closed. Could not establish a trust relationship for the SSL/TLS secure channel. This exception means that the Session Recording Server is using a certificate that is signed by a CA that the server on which the Session Recording Agent resides does not trust, or have a CA certificate for. Alternatively, the certificate may have expired or been revoked.

Resolution: Verify that the correct CA certificate is installed on the server hosting the Session Recording Agent or use a CA that is trusted.

- The remote server returned an error: (403) forbidden. This is a standard HTTPS error displayed when you attempt to connect using HTTP (nonsecure protocol). The computer hosting the Session Recording Server rejects the connection because it accepts only secure connections.

Resolution: Use Session Recording Agent Properties to change the Session Recording Broker protocol to HTTPS.

The Session Recording Broker returned an unknown error while evaluating a record policy query. Error code 5 (Access Denied). See the Event log on the Session Recording Server for more details. This error occurs when sessions are started and a request for a record policy evaluation is made. The error is a result of the Authenticated Users group (this is the default member) being removed from the Policy Query role of the Session Recording Authorization Console.

Resolution: Add the Authenticated Users group back into this role, or add each server hosting each Session Recording Agent to the PolicyQuery role.

The underlying connection was closed. A connection that was expected to be kept alive was closed by the server. This error means that the Session Recording Server is down or unavailable to accept requests. This could be due to IIS being offline or restarted, or the entire server may be offline.

Resolution: Verify that the Session Recording Server is started, IIS is running on the server, and the server is connected to the network.

## Session Recording Server cannot connect to the Session Recording Database

When the Session Recording Server cannot connect to the Session Recording Database, you may see a message similar to one of the following:

## Event Source:

Citrix Session Recording Storage Manager Description: Exception caught while establishing database connection. This error appears in the applications event log in the Event Viewer of the computer hosting the Session Recording Server.

Unable to connect to the Session Recording Server. Ensure that the Session Recording Server is running. This error message appears when you launch the Session Recording Policy Console.

## Resolution:

- The Express Edition of Microsoft SQL Server 2008 R2, Microsoft SQL Server 2012, or Microsoft SQL Server 2014 is installed on a stand-alone server and does not have the correct services or settings configured for Session Recording. The server must have TCP/IP protocol enabled and SQL Server Browser service running. See the Microsoft documentation for information about enabling these settings.
- During the Session Recording installation (administration portion), incorrect server and database information was given. Uninstall the Session Recording Database and reinstall it, supplying the correct information.
- The Session Recording Database Server is down. Verify that the server has connectivity.
- The computer hosting the Session Recording Server or the computer hosting the Session Recording Database Server cannot resolve the FQDN or NetBIOS name of the other. Use the ping command to verify the names can be resolved.

Logon failed for user 'NT\_AUTHORITY\ANONYMOUS LOGON'. This error message means that the services are logged on incorrectly as .\administrator.

Resolution: Restart the services as local system user and restart the SQL services.

## Sessions are not recording

If your application sessions are not recording successfully, start by checking the application event log in the Event Viewer on the Server OS machine running the Session Recording Agent and Session Recording Server. This may provide valuable diagnostic information.

If sessions are not recording, these issues might be the cause:

- **Component connectivity and certificates.** If the Session Recording components cannot communicate with each other, this can cause session recordings to fail. To troubleshoot recording issues, verify that all components are configured correctly to point to the correct computers and that all certificates are valid and correctly installed.
- **Non-Active Directory domain environments.** Session Recording is designed to run in a Microsoft Active Directory domain environment. If you are not running in an Active Directory environment, you may experience recording issues. Ensure that all Session Recording components are running on computers that are members of an Active Directory domain.
- **Session sharing conflicts with the active policy.** Session Recording matches the active policy with the first published application that a user opens. Subsequent applications opened during the same session continue to follow the policy that is in force for the first application. To prevent session sharing from conflicting with the active policy, publish the conflicting applications on separate Server OS machines.
- **Recording is not enabled.** By default, installing the Session Recording Agent on a Server OS machine enables the server for recording. Recording will not occur until an active recording policy is configured to allow this.
- **The active recording policy does not permit recording.** For a session to be recorded, the active recording policy must permit the sessions for the user, server, or published application to be recorded.
- **Session Recording services are not running.** For sessions to be recorded, the Session Recording Agent service must be running on the Server OS machine and the Session Recording Storage Manager service must be running on the computer hosting the Session Recording Server.

- **MSMQ is not configured.** If MSMQ is not correctly configured on the server running the Session Recording Agent and the computer hosting the Session Recording Server, recording problems may occur.

#### Unable to view live session playback

If you experience difficulties when viewing recordings using the Session Recording Player, the following error message may appear on the screen:

Download of recorded session file failed. Live session playback is not permitted. The server has been configured to disallow this feature. This error indicates that the server is configured to disallow the action.

Resolution: In the Session Recording Server Properties dialog box, choose the Playback tab and select the Allow live session playback check box.

#### Recordings are corrupt or incomplete

When recordings are becoming corrupt or incomplete when viewing them using the Session Recording Player, you may also see warnings in the Event logs on the Session Recording Agent.

**Event Source:** Citrix Session Recording Storage Manager

**Description:** Data lost while recording file <icl file name>

This usually happens when Machine Creation Services (MCS) or Provisioning Services is used to create VDAs with a configured master image and Microsoft Message Queuing (MSMQ) installed. In this condition the VDAs have the same QMIDs for MSMQ.

Resolution: Create the unique QMId for each VDA. A workaround is introduced in [Known Issues](#).

Test connection of the database instance failed when installing the Session Recording Database or Session Recording Server

When you install Session Recording Database or Session Recording Server, the test connection fails with the error message **Database connection test failed. Please correct Database instance name** even if the database instance name is correct.

Resolution: Make sure the current user has the public SQL Server role permission to correct the permission limitation failure.

# 验证组件连接

May 28, 2016

During the setup of Session Recording, the components may not connect to other components. All the components communicate with the Session Recording Server (Broker). By default, the Broker (an IIS component) is secured using the IIS default Web site certificate. If one component cannot connect to the Session Recording Server, the other components may also fail when attempting to connect.

The Session Recording Agent and Session Recording Server (Storage Manager and Broker) log connection errors in the applications event log in the Event Viewer of the computer hosting the Session Recording Server, while the Session Recording Policy Console and Session Recording Player display connection error messages on screen when they fail to connect.

## Verify Session Recording Agent is connected

1. Log on to the server where the Session Recording Agent is installed.
2. From the Start menu, choose Session Recording Agent Properties.
3. In Session Recording Server Properties, click Connection.
4. Verify that the value for Session Recording Server is the correct server name of the computer hosting the Session Recording Server.
5. Verify that the server given as the value for Session Recording Server can be contacted by the Server OS machine.

Note: Check the application event log for errors and warnings.

## Verify Session Recording Server is connected

Caution: Using Registry Editor can cause serious problems that can require you to reinstall the operating system. Citrix cannot guarantee that problems resulting from incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk.

1. Log on to the computer hosting the Session Recording Server.
2. Open the Registry Editor.
3. Browse to HKEY\_LOCAL\_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server.
4. Verify the value of SmAudDatabaseInstance correctly references the Session Recording Database you installed in your SQL Server instance.

## Verify Session Recording Database is connected

1. Using a SQL Management tool, open your SQL instance that contains the Session Recording Database you installed.
2. Open the Security permissions of the Session Recording Database.
3. Verify the Session Recording Computer Account has access to the database. For example, if the computer hosting the Session Recording Server is named SsRecSrv in the MIS domain, the computer account in your database should be configured as MIS\SsRecSrv\$. This value is configured during the Session Recording Database install.

## Test IIS connectivity

Testing connections to the Session Recording Server IIS site by using a Web browser to access the Session Recording Broker Web page can help you determine whether problems with communication between Session Recording components stem from misconfigured protocol configuration, certification issues, or problems starting Session Recording Broker.

## To verify IIS connectivity for the Session Recording Agent

1. Log on to the server where the Session Recording Agent is installed.
2. Launch a Web browser and type the following address:
  - For HTTPS: <https://servername/SessionRecordingBroker/RecordPolicy.rem?wsdl>, where `servername` is the name of the computer hosting the Session Recording Server
  - For HTTP: <http://servername/SessionRecordingBroker/RecordPolicy.rem?wsdl>, where `servername` is the name of the computer hosting the Session Recording Server
3. If you are prompted for NT LAN Manager (NTLM) authentication, log on with a domain administrator account.

If you see an XML document within your browser, this verifies that the computer running the Session Recording Agent is connected to the computer hosting the Session Recording Server using the configure protocol.

## To verify IIS connectivity for the Session Recording Player

1. Log on to the workstation where the Session Recording Player is installed.
2. Launch a Web browser and type the following address:
  - For HTTPS: <https://servername/SessionRecordingBroker/Player.rem?wsdl>, where `servername` is the name of the computer hosting the Session Recording Server
  - For HTTP: <http://servername/SessionRecordingBroker/Player.rem?wsdl>, where `servername` is the name of the computer hosting the Session Recording Server
3. If you are prompted for NT LAN Manager (NTLM) authentication, log on with a domain administrator account.

If you see an XML document within your browser, this verifies that the computer running the Session Recording Player is connected to the computer hosting the Session Recording Server using the configure protocol.

## To verify IIS connectivity for the Session Recording Policy Console

1. Log on to the server where the Session Recording Policy Console is installed.
2. Launch a Web browser and type the following address:
  - For HTTPS: <https://servername/SessionRecordingBroker/PolicyAdministration.rem?wsdl>, where `servername` is the name of the computer hosting the Session Recording Server
  - For HTTP: <http://servername/SessionRecordingBroker/PolicyAdministration.rem?wsdl>, where `servername` is the name of the computer hosting the Session Recording Server
3. If you are prompted for NT LAN Manager (NTLM) authentication, log on with a domain administrator account.

If you see an XML document within your browser, this verifies that the computer running the Session Recording Policy Console is connected to the computer hosting the Session Recording Server using the configure protocol.

### Troubleshoot certificate issues

If you are using HTTPS as your communication protocol, the computer hosting the Session Recording Server must be configured with a server certificate. All component connections to the Session Recording Server must have root certificate authority (CA). Otherwise, attempted connections between the components fail.

You can test your certificates by accessing the Session Recording Broker Web page as you would when testing IIS connectivity. If you are able to access the XML page for each component, the certificates are configured correctly.

Here are some common ways certificate issues cause connections to fail:

- **Invalid or missing certificates.** If the server running the Session Recording Agent does not have a root certificate to trust the server certificate, cannot trust and connect to the Session Recording Server over HTTPS, causing connectivity to fail. Verify that all components trust the server certificate on the Session Recording Server.
- **Inconsistent naming.** If the server certificate assigned to the computer hosting the Session Recording Server is created

using a fully qualified domain name (FQDN), then all connecting components must use the FQDN when connecting to the Session Recording Server. If a NetBIOS name is used, configure the components with a NetBIOS name for the Session Recording Server.

- **Expired certificates.** If a server certificate expired, connectivity to the Session Recording Server through HTTPS fails. Verify the server certificate assigned to the computer hosting the Session Recording Server is valid and has not expired. If the same certificate is used for the digital signing of session recordings, the event log of the computer hosting the Session Recording Server provides error messages that the certificate expired or warning messages when it is about to expire.

# 如果 Session Recording Player 失败，搜索录制件

May 28, 2016

If you experience difficulties when searching for recordings using the Session Recording Player, the following error messages may appear on the screen:

- Search for recorded session files failed. The remote server name could not be resolved: `servername`, where `servername` is the name of the server to which the Session Recording Player is attempting to connect. The Session Recording Player cannot contact the Session Recording Server. Two possible reasons for this are an incorrectly typed server name or the DNS cannot resolve the server name.

Resolution: From the Player menu bar, choose Tools > Options > Connections and verify that the server name in the Session Recording Servers list is correct. If it is correct, from a command prompt, run the ping command to see if the name can be resolved. When the Session Recording Server is down or offline, the search for recorded session files failed error message is Unable to contact the remote server.

- Unable to contact the remote server. This error occurs when the Session Recording Server is down or offline.

Resolution: Verify that the Session Recording Server is connected.

- Access denied error. An access denied error can occur if the user was not given permission to search for and download recorded session files.

Resolution: Assign the user to the Player role using the Session Recording Authorization Console.

- Search for recorded session files failed. The underlying connection was closed. Could not establish a trust relationship for the SSL/TLS secure channel. This exception is caused by the Session Recording Server using a certificate that is signed by a CA that the client device does not trust or have a CA certificate for.

Resolution: Install the correct or trusted CA certificate workstation where the Session Recording Player is installed.

- The remote server returned an error: (403) forbidden. This error is a standard HTTPS error that occurs when you attempt to connect using HTTP (nonsecure protocol). The server rejects the connection because, by default, it is configured to accept only secure connections.

Resolution: From the Session Recording Player menu bar, choose Tools > Options > Connections. Select the server from the Session Recordings Servers list, then click Modify. Change the protocol from HTTP to HTTPS.

## Troubleshoot MSMQ

If your users see the notification message but the viewer cannot find the recordings after performing a search in the Session Recording Player, there could be a problem with MSMQ. Verify that the queue is connected to the Session Recording Server (Storage Manager) and use a Web browser to test for connection errors (if you are using HTTP or HTTPS as your MSMQ communication protocol).

To verify that the queue is connected:

1. Log on to the server hosting the Session Recording Agent and view the outgoing queues.
2. Verify that the queue to the computer hosting the Session Recording Server has a connected state.
  - If the state is “waiting to connect,” there are a number of messages in the queue, and the protocol is HTTP or HTTPS (corresponding to the protocol selected in the Connections tab in the Session Recording Agent Properties dialog box), perform Step 3.
  - If state is “connected” and there are no messages in the queue, there may be a problem with the server hosting the Session Recording Server. Skip Step 3 and perform Step 4.

3. If there are a number of messages in the queue, launch a Web browser and type the following address:
  - For HTTPS: [https://servername/msmq/private\\$/CitrixSmAudData](https://servername/msmq/private$/CitrixSmAudData), where servername is the name of the computer hosting the Session Recording Server
  - For HTTP: [http://servername/msmq/private\\$/CitrixSmAudData](http://servername/msmq/private$/CitrixSmAudData), where servername is the name of the computer hosting the Session Recording ServerIf the page returns an error such as The server only accepts secure connections, change the MSMQ protocol listed in the Session Recording Agent Properties dialog box to HTTPS. Otherwise, if the page reports a problem with the Web site's security certificate, there may be a problem with a trust relationship for the SSL/TLS secure channel. In that case, install the correct CA certificate or use a CA that is trusted.
4. If there are no messages in the queue, log on to the computer hosting the Session Recording Server and view private queues. Select `citrixsmauddata`. If there are a number of messages in the queue (Number of Messages Column), verify that the Session Recording StorageManager service is started. If it is not, restart the service.

# 更改通信协议

May 28, 2016

For security reasons, Citrix does not recommend using HTTP as a communication protocol. The Session Recording installation is configured to use HTTPS. If you want to use HTTP instead of HTTPS, you must change several settings.

## To use HTTP as the communication protocol

1. Log on to the computer hosting the Session Recording Server and disable secure connections for Session Recording Broker in IIS.
2. Change the protocol setting from HTTPS to HTTP in each Session Recording Agent Properties dialog box:
  1. Log on to each server where the Session Recording Agent is installed.
  2. From the Start menu, choose Session Recording Agent Properties.
  3. In Session Recording Agent Properties, choose the Connections tab.
  4. In the Session Recording Broker area, select HTTP from the Protocol drop-down list and choose OK to accept the change. If you are prompted to restart the service, choose Yes.
3. Change the protocol setting from HTTPS to HTTP in the Session Recording Player settings:
  1. Log on to each workstation where the Session Recording Player is installed.
  2. From the Start menu, choose Session Recording Player.
  3. From the Session Recording Player menu bar, choose Tools > Options > Connections, select the server and choose Modify.
  4. Select HTTP from the Protocol drop-down list and click OK twice to accept the change and exit the dialog box.
4. Change the protocol setting from HTTPS to HTTP in the Session Recording Policy Console:
  1. Log on to the server where the Session Recording Policy Console is installed.
  2. From the Start menu, choose Session Recording Policy Console.
  3. Choose HTTP from the Protocol drop-down list and choose OK to connect. If the connection is successful, this setting is remembered the next time you launch the Session Recording Policy Console.

## To revert to HTTPS as the communication protocol

1. Log on to the computer hosting the Session Recording Server and enable secure connections for the Session Recording Broker in IIS.
2. Change the protocol setting from HTTP to HTTPS in each Session Recording Agent Properties dialog box:
  1. Log on to each server where the Session Recording Agent is installed.
  2. From the Start menu, choose Session Recording Agent Properties.
  3. In Session Recording Agent Properties, choose the Connections tab.
  4. In the Session Recording Broker area, select HTTPS from the Protocol drop-down list and choose OK to accept the change. If you are prompted to restart the service, choose Yes.
3. Change the protocol setting from HTTP to HTTPS in the Session Recording Player settings:
  1. Log on to each workstation where the Session Recording Player is installed.
  2. From the Start menu, choose Session Recording Player.
  3. From the Session Recording Player menu bar, choose Tools > Options > Connections, select the server and choose Modify.
  4. Select HTTPS from the Protocol drop-down list and click OK twice to accept the change and exit the dialog box.
4. Change the protocol setting from HTTP to HTTPS in the Session Recording Policy Console:
  1. Log on to the server where the Session Recording Policy Console is installed.
  2. From the Start menu, choose Session Recording Policy Console.

3. Choose HTTPS from the Protocol drop-down list and choose OK to connect. If the connection is successful, this setting is remembered the next time you launch the Session Recording Policy Console.

# 参考：管理您的数据库记录

May 28, 2016

The ICA Log database (ICLDB) utility is a database command-line utility used to manipulate the session recording database records. This utility is installed during the Session Recording installation in the drive:\Program Files\Citrix\SessionRecording\Server\Bin directory at the server hosting the Session Recording Server software.

## Quick reference chart

The following table lists the commands and options that are available for the ICLDB utility. Type the commands using the following format:

icldb [version | locate | dormant | import | archive | remove | removeall] command-options [/l] [/f] [/s] [/?]

Note: More extensive instructions are available in the help associated with the utility. To access the help, from a command prompt, type drive:\Program Files\Citrix\SessionRecording\Server\Bin directory, type icldb ?. To access help for specific commands, type icldb command ?.

Command	Description
archive	Archives the session recording files older than the retention period specified. Use this command to archive files.
dormant	Displays or counts the session recording files that are considered dormant. Dormant files are session recordings that were not completed due to data loss. Use this command to verify if you suspect that you are losing data. You can verify if the session recording files are becoming dormant for the entire database, or only recordings made within the specified number of days, hours, or minutes.
import	Imports session recording files into the Session Recording database. Use this command to rebuild the database if you lose database records.  Additionally, use this command to merge databases (if you have two databases, you can import the files from one of the databases).
locate	Locates and displays the full path to a session recording file using the file ID as the criteria. Use this command when you are looking for the storage location of a session recording file.  It is also one way to verify if the database is up-to-date with a specific file.
remove	Removes the references to session recording files from the database. Use this command (with caution) to clean up the database. Specify the retention period to be used as the criteria.  You can also remove the associated physical file.

<b>removeall</b>	<p><b>Description</b></p> <p>Removes all of the references to session recording files from the Session Recording Database and returns the database to its original state. The actual physical files are not deleted; however you cannot search for these files in the Session Recording Player. Use this command (with caution) to clean up the database. Deleted references can be reversed only by restoring from your backup.</p>
version	Displays the Session Recording Database schema version.
/l	Logs the results and errors to the Windows event log.
/f	Forces the command to run without prompts.
/s	Suppresses the copyright message.
/?	Displays help for the commands.

# 第三方声明

May 28, 2016

Session Recording may include third party software components licensed under the following terms. This list was generated using third party software as of the date listed. This list may change with specific versions of the product and may not be complete; it is provided "As-Is." TO THE EXTENT PERMITTED BY APPLICABLE LAW, CITRIX AND ITS SUPPLIERS MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, WITH REGARD TO THE LIST OR ITS ACCURACY OR COMPLETENESS, OR WITH RESPECT TO ANY RESULTS TO BE OBTAINED FROM USE OR DISTRIBUTION OF THE LIST. BY USING OR DISTRIBUTING THE LIST, YOU AGREE THAT IN NO EVENT SHALL CITRIX BE HELD LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY OTHER DAMAGES WHATSOEVER RESULTING FROM ANY USE OR DISTRIBUTION OF THIS LIST.

MMC .NET Library

Licensed under the Common Public License, Version 1.0

# Personal vDisk

May 28, 2016

You can use a diagnostic tool to monitor the changes made by users to both parts of their Personal vDisks (the user data and the application parts). These changes include applications that users have installed and files they have modified. The changes are stored in a set of reports.

1. On the machine that you want to monitor, run C:\Program Files\Citrix\personal vDisk\bin\CtxPvdDiag.exe.
2. Browse to a location where you want to store the reports and logs, select which reports to generate, and click OK. The following reports are available:

Report or Log	Generated Files	Changes Monitored
Software hive report	Software.Dat.Report.txt, Software.Dat.delta.txt	<p>Software.Dat.Report.txt records the changes made by the user to the HKEY_LOCAL_MACHINE\Software hive. It consists of the following sections:</p> <ul style="list-style-type: none"><li>• <b>List of Applications installed on the base</b> — The applications that were installed in Layer 0.</li><li>• <b>List of user installed software</b> — the applications that were installed by the user on the application part of the vDisk.</li><li>• <b>List of software uninstalled by user</b> — the applications removed by the user that were originally present in Layer 0.</li></ul> <p>See Hive delta report for information on Software.Dat.delta.txt.</p>
System hive report	SYSTEM.CurrentControlSet.DAT.Report.txt	<p>This file records the changes made by the user to the HKEY_LOCAL_MACHINE\System hive. It contains the following sections:</p> <ul style="list-style-type: none"><li>• <b>List of user installed services</b> — the services and drivers installed by the user.</li><li>• <b>Startup of following services were changed</b> — the services and drivers whose start type was modified by the user.</li></ul>
Security hive report	SECURITY.DAT.Report.txt	<p>This file monitors all changes that the user makes in the HKEY_LOCAL_MACHINE\Security hive.</p>
Security Account Manager(SAM) hive report	SAM.DAT.Report.txt	<p>This file monitors all changes that the user makes in the HKEY_LOCAL_MACHINE\SAM hive.</p>
Hive delta report	Software.Dat.delta.txt	<p>This file records all registry keys and values added or removed, and all values modified, by the user in the</p>

Report or Log	Generated Files	HKEY_LOCAL_MACHINE\Software hive. <b>Changes Monitored</b>
Personal vDisk logs	Pud-IvmSupervisor.log, PvDActivation.log, PvDSvc.log, PvDWMI.log, SysVol-IvmSupervisor.log, vDeskService-<#>.log	These files are generated by default in P:\Users\<user account>\AppData\Local\Temp\PVDLOGS but are moved to the selected location.
Windows operating system (OS) log	EvtLog_App.xml, EvtLog_System.xml, setupapi.app.log, setuperr.log, setupapi.dev.log, msinfo.txt	<p>EvtLog_App.xml and EvtLog_System.xml are the application and system event logs in XML format from the Personal vDisk volume.</p> <p>Setupapi.app.log and setuperr.log contain log messages from when msieexec.exe was run during Personal vDisk installation.</p> <p>Setupapi.dev.log contains device installation log messages.</p> <p>Msinfo.txt contains the output of msinfo32.exe. For information on this output, see your Microsoft documentation.</p>
File system report	FileSystemReport.txt	<p>This file records changes made by the user to the file system. It consists of the following sections:</p> <ul style="list-style-type: none"> <li>● <b>Files Relocated</b> — the files in Layer 0 that were moved by the user to the vDisk. Layer 0 files are those that were inherited from the master image by the machine to which the Personal vDisk is attached.</li> <li>● <b>Files Removed</b> — the files in Layer 0 that were hidden by a user's action (for example, removing an application).</li> <li>● <b>Files Added (MOF,INF,SYS)</b> — the files with .mof, .inf, or .sys extensions that the user added to the vDisk (for example, when they installed an application such as Visual Studio 2010 that registers a .mof file for autorecovery).</li> <li>● <b>Files Added Other</b> — Other files that the user added to the vDisk (for example, when they installed an application).</li> <li>● <b>Base Files Modified But Not Relocated</b> — the files in Layer 0 that the user modified but that the Personal vDisk Kernel-Mode drivers did not capture in the vDisk.</li> </ul>

# 配置日志记录

May 28, 2016

Configuration Logging captures Site configuration changes and administrative activities to the Database. You can use the logged content to:

- Diagnose and troubleshoot problems after configuration changes are made; the log provides a breadcrumb trail
- Assist change management and track configurations
- Report administration activity

You set Configuration Logging preferences, display configuration logs, and generate HTML and CSV reports from Citrix Studio. You can filter configuration log displays by date ranges and by full text search results. Mandatory logging, when enabled, prevents configuration changes from being made unless they can be logged. With appropriate permission, you can delete entries from the configuration log. You cannot use the Configuration Logging feature to edit log content.

Configuration Logging uses a PowerShell 2.0 SDK and the Configuration Logging Service. The Configuration Logging Service runs on every Controller in the Site; if one Controller fails, the service on another Controller automatically handles logging requests.

By default, the Configuration Logging feature is enabled, and uses the Database that is created when you create the Site (the Site Configuration Database). Citrix strongly recommends that you change the location of the database used for Configuration Logging as soon as possible after creating a Site. The Configuration Logging Database supports the same high availability features as the Site Configuration Database.

Access to Configuration Logging is controlled through Delegated Administration, with the Edit Logging Preferences and View Configuration Logs permissions.

Configuration logs are localized when they are created. For example, a log created in English will be read in English, regardless of the locale of the reader.

## What is logged

Configuration changes and administrative activities initiated from Studio, Director, and PowerShell scripts are logged.

Examples of logged configuration changes include working with (creating, editing, deleting, assigning):

- Machine Catalogs
- Delivery Groups (including changing power management settings)
- Administrator roles and scopes
- Host resources and connections
- Citrix policies through Studio

Examples of logged administrative changes include:

- Power management of a virtual machine or a user desktop
- Studio or Director sending a message to a user

The following operations are not logged:

- Autonomic operations such as pool management power-on of virtual machines.
- Policy actions implemented through the Group Policy Management Console (GPMC); use Microsoft tools to view logs of those actions.
- Changes made through the registry, direct access of the Database, or from sources other than Studio, Director, or PowerShell.

- When the deployment is initialized, Configuration Logging becomes available when the first Configuration Logging Service instance registers with the Configuration Service. Therefore, the very early stages of configuration are not logged (for example, when the Database schema is obtained and applied, when a hypervisor is initialized).

# 管理配置日志记录

May 28, 2016

By default, Configuration Logging uses the database that is created when you create a Site (also known as the Site Configuration Database). Citrix recommends that you change the location of the database used for Configuration Logging (and the database used for the Monitoring Service, which also uses the Site Configuration Database by default) after creating a Site, for the following reasons:

- The backup strategy for the Configuration Logging Database is likely to differ from the backup strategy for the Site Configuration Database.
- The volume of data collected for Configuration Logging (and the Monitoring Service) could adversely affect the space available to the Site Configuration database.
- It splits the single point of failure for the three databases.

Note: Product editions that do not support Configuration Logging do not have a Logging node in Studio. For more information, see [XenDesktop 7.6 and XenApp 7.6 Features and Entitlements](#).

## Enable and disable Configuration Logging and mandatory logging

By default, Configuration Logging is enabled, and mandatory logging is disabled.

1. Select Logging in the Studio navigation pane.
2. Select Preferences in the Actions pane. The Configuration Logging dialog box contains database information and indicates whether Configuration Logging and mandatory logging are enabled or disabled.
  - To enable Configuration Logging, select the Enable logging radio button. This is the default setting. If the database cannot be written to, the logging information is discarded, but the operation continues.
  - To disable Configuration Logging, select the Disable logging radio button. If logging was previously enabled, existing logs remain readable with the PowerShell SDK.
  - To enable mandatory logging, clear the Allow changes when the database is disconnected checkbox. No configuration change or administrative activity that would normally be logged will be allowed unless it can be written in the database used for Configuration Logging.

You can enable mandatory logging only when Configuration Logging is enabled, that is, when the Enable Configuration Logging radio button is selected. If the Configuration Logging Service fails, and high availability is not in use, mandatory logging is assumed. In such cases, operations that would normally be logged are not performed.

- To disable mandatory logging, select the Allow changes when the database is disconnected check box. Configuration changes and administrative activities are allowed, even if the database used for Configuration Logging cannot be accessed. This is the default setting.

## Change the Configuration Logging database location

Note: You cannot change the database location when mandatory logging is enabled, because the location change includes a brief disconnect interval that cannot be logged.

1. Create a database server, using a supported SQL Server version.
2. Select Logging in the Studio navigation pane.
3. Select Preferences in the Actions pane.
4. In the Logging Preferences dialog box, select Change logging database.
5. In the Change Logging Database dialog box, specify the location of the server containing the new database server (using one of the forms in the following table) and the database name.

<b>Database type</b>	<b>What to enter</b>	<b>With this database configuration</b>
Standalone or mirror	servername	The default instance is used and SQL Server uses the default port.
	servername\INSTANCENAME	A named instance is used and SQL Server uses the default port.
	servername,port-number	The default instance is used and SQL Server uses a custom port. (The comma is required.)
Other	cluster-name	A clustered database.
	availability-group-listener	An Always-On database.

- To allow Studio to create the database, click OK. When prompted, click OK, and the database will be created automatically. Studio attempts to access the database using the current Studio user's credentials; if that fails, you are prompted for the database user's credentials. Studio then uploads the database schema to the database. (The credentials are retained only during database creation.)
- To create the database manually, click Generate database script. The generated script includes instructions for manually creating the database. Ensure that the database is empty and that at least one user has permission to access and change the database before uploading the schema.

The Configuration Logging data in the previous database is not imported to the new database. Logs cannot be aggregated from both databases when retrieving logs. The first log entry in the new Configuration Logging database will indicate that a database change occurred, but it does not identify the previous database.

#### Display configuration log content

When initiating configuration changes and administrative activities, the high level operations created by Studio and Director are displayed in the upper middle pane in Studio. A high level operation results in one or more service and SDK calls, which are low level operations. When you select a high level operation in the upper middle pane, the lower middle pane displays the low level operations.

If an operation fails before completion, the log operation might not be completed in the Database; for example, a start record will have no corresponding stop record. In such cases, the log indicates that there is missing information. When you display logs based on time ranges, incomplete logs are shown if the data in the logs matches the criteria. For example, if all logs for the last five days are requested and a log exists with a start time in the last five days but has no end time, it is included.

When using a script that calls PowerShell cmdlets, if you create a low level operation without specifying a parent high level operation, Configuration Logging will create a surrogate high level operation.

To display configuration log content, select Logging in the Studio navigation pane. By default, the display in the center pane lists the log content chronologically (newest entries first), separated by date.

<b>To filter the display by</b>	<b>Complete this action</b>
Search	Enter text in the Search box at the top of the middle pane. The filtered display includes the number of

<b>To filter the display by results</b>	search results. To return to the standard logging display, clear the text in the Search box. <b>Complete this action</b>
<b>Column by heading</b>	Click a column heading to sort the display by that field.
A date range	Select an interval from the drop down list box next to the Search box at the top of the middle pane.

## Generate reports

You can generate CSV and HTML reports containing configuration log data.

- The CSV report contains all the logging data from a specified time interval. The hierarchical data in the database is flattened into a single CSV table. No aspect of the data has precedence in the file. No formatting is used and no human readability is assumed. The file (named MyReport) simply contains the data in a universally consumable format. CSV files are often used for archiving data or as a data source for a reporting or data manipulation tool such as Microsoft Excel.
- The HTML report provides a human-readable form of the logging data for a specified time interval. It provides a structured, navigable view for reviewing changes. An HTML report comprises two files, named Summary and Details. Summary lists high level operations: when each operation occurred, by whom, and the outcome. Clicking a Details link next to each operation takes you to the low level operations in the Details file, which provides additional information.

To generate a configuration log report, select Logging in the Studio navigation pane, and then select Create custom report in the Actions pane.

- Select the date range for the report.
- Select the report format: CSV, HTML, or both.
- Browse to the location where the report should be saved.

## Delete configuration log content

To delete the configuration log, you must have certain Delegated Administration and SQL Server database permissions.

- **Delegated Administration** — You must have a Delegated Administration role that allows the deployment configuration to be read. The built-in Full administrator role has this permission. A custom role must have Read Only or Manage selected in the Other permissions category.

To create a backup of the configuration logging data before deleting it, the custom role must also have Read Only or Manage selected in the Logging Permissions category.

- **SQL Server database** — You must have a SQL server login with permission to delete records from the database. There are two ways to do this:
  - Use a SQL Server database login with a sysadmin server role, which allows you to perform any activity on the database server. Alternatively, the serveradmin or setupadmin server roles allow you to perform deletion operations.
  - If your deployment requires additional security, use a non-sysadmin database login mapped to a database user who has permission to delete records from the database.
    1. In SQL Server Management Studio, create a SQL Server login with a server role other than 'sysadmin.'
    2. Map the login to a user in the database; SQL Server automatically creates a user in the database with the same name as the login.
    3. In Database role membership, specify at least one of the role members for the database user: ConfigurationLoggingSchema\_ROLE or dbowner.

For more information, see the SQL Server Management Studio documentation.

To delete the configuration logs:

1. Select Logging in the Studio navigation pane.
2. Select Delete logs in the Actions pane.
3. You are asked if you want to create a backup of the logs before they are deleted. If you choose to create a backup, browse to the location where the backup archive should be saved. The backup is created as a CSV file.

After the configuration logs are cleared, the log deletion is the first activity posted to the empty log. That entry provides details about who deleted the logs, and when.

# Monitor Service OData API

May 28, 2016

Documentation for the Monitor Service OData API is available in [Citrix Developer Documentation](#).

# XenApp 和 XenDesktop SDK

May 28, 2016

Documentation for the XenApp and XenDesktop SDK is available [here](#).

# 针对 XenApp and XenDesktop 7.6 LTSR 的 Citrix VDI 最佳实践

Feb 10, 2017

PDF

Citrix VDI Handbook and Best Practices for the XenApp and XenDesktop 7.6 Long Term Service Release

## Introduction

In traditional business environments, workers suffer from productivity loss in many ways, including downtime during PC refreshes, patches and updates, or simply when they are away from the office. Application and desktop virtualization centralizes apps and desktops in the datacenter, rather than on local devices. This allows IT to deliver apps and desktops to users on demand, to any device, anywhere.

Unfortunately, organizations sometimes struggle to achieve this level of success. Why does one organization succeed while another organization struggles?

If we compare the factors between success and failure between desktop virtualization and other technology related projects, we see that there is little difference:

- Lack of justification – Without a solid business reason, desktop virtualization is simply a new way to deliver a desktop. A business justification gives the project team a goal to strive towards.
- Lack of a methodology – Many people who try and struggle to deploy a desktop virtualization solution do so because they jump right in without understanding or implementing the appropriate prerequisites. A structured methodology provides the path for the project.
- Lack of experience – For many who embark on a desktop virtualization project, there is a lack of experience, which creates a lack of confidence in the design. Architects begin to second-guess themselves and the project stalls.

Our hope is that this handbook can alleviate the anxiety associated with desktop virtualization by showing how challenges can be resolved in a manner that is technically sound, but also feasible and effective for organizations facing deadlines and other organizational challenges.

Citrix has successfully employed the methodology, experience and best practices shared within this handbook across thousands of desktop virtualization projects.

## Methodology

The Citrix VDI Handbook follows the Citrix Consulting methodology. A proven methodology that has been successfully employed across thousands of desktop virtualization projects. Each phase includes guidance on the important questions to ask, what tools to use and tips to help you succeed. The Citrix Consulting methodology consists of five phases:

Define – Builds the business case for desktop virtualization by creating a high-level project roadmap, prioritizing activities and estimating storage and hardware requirements.

Assess – Key business drivers are rated so that work effort can be prioritized accordingly. In addition, the current environment is reviewed for potential problems and to identify use cases for the project. This information will be used to set the direction of the Citrix deployment, upgrade, or expansion.

Design – Define architecture required to satisfy key business drivers and success criteria identified during the assess phase.

Topics such as environment scalability, redundancy and high availability are addressed.

Deploy – During the deploy phase, the infrastructure is installed and configured as described in the design phase. All components of the infrastructure should be thoroughly unit and regression tested before users are provided with access to the environment.

Monitor – Define architectural and operational processes required to maintain the production environment.

The Citrix Consulting methodology follows an iterative Assess > Design > Deploy process for each major initiative of your project. In doing so, your organization is left with tangible improvements to the environment at the end of each engagement. For example, high priority user groups can progress through the assess, design and deploy phases earlier than other user groups

**Note:** The VDI Handbook provides content on the Assess, Design and Monitor phases of the Citrix Consulting methodology.

# 评估

Feb 10, 2017

## Overview

Creating an app and desktop delivery solution begins with a proper assessment. Architects that fail to properly assess the current environment find that they require the assess information later on, forcing them to backtrack, which can potentially stall and put the project at risk.

By gathering all of the information from the outset, the architect will gain an appreciation for the current environment and be able to work from the beginning on properly aligning business and user requirements with the overall solution.

The assess phase is a four-step, simple to follow process:



### Step 1: Define the Organization

The first step in your virtual desktop project should be to understand and prioritize the strategic imperatives of the organization. This enables the project management team to define success criteria and allows the design team to create a tailored and optimized architecture.

Requirements can be captured during meetings or by distributing questionnaires. Meetings are more time consuming, but allow for follow-up questions to be asked and help to simplify the prioritization process. It is important that this exercise be completed jointly by both business managers and IT decision makers since both groups will have significantly different viewpoints. Take the following examples of what certain organizations faced, which drove their selection of desktop virtualization.

#### Experience from the Field

**Finance** – A large financial institution had a base of operations in the city designated as the host city for an upcoming G8 summit. As these types of meetings historically include riots, protests and other issues that can disrupt business and the safety of their employees, the financial organization needed an alternative allowing their users to work from the safety of their homes.

**Agriculture** – Due to thin margins, an agriculture organization wanted to save money by extending the life of desktop PCs while still being able to run the latest applications.

**Healthcare** – A large healthcare organization was in need of a solution to simplify application updates as the main application required updates on a weekly basis. Due to the distributed nature of the endpoint devices, the organization was in need of a better application delivery solution.

These are just a few examples, but they demonstrate how organizations think about their priorities. Most organizations do not focus on technology, they focus on the needs of the user and of the organization. These needs can be met with technical solutions but it is imperative the team understands the “Why” of the project.

In addition to the three real-world examples, the following table identifies a few other priorities often stated from many organizations:

Requester	Requirement
Business managers	Better IT agility and responsiveness – Flexible desktop solution that is capable of accommodating periods of change such as rapid growth or downsizing. For example, enabling the business to setup project offices or temporary points of sale very rapidly without long delays or IT notification periods.
	Bring your own device – Empower employees to choose their own devices to improve productivity, collaboration and mobility.
	Collaboration – With an increase in both globalization and mobility, team members are often dispersed across multiple physical locations. Powerful collaboration capabilities are required to ensure high levels of productivity, efficiency and quality.
	Work from anywhere – The business needs to support home workers in order to attract and retain top talent, and / or travelling employees.
IT decision makers	Better desktop management – Simplify the management of desktop infrastructure. IT is not as proactive as they would like and spend too much time "fighting fires".
	Increase security – Data theft or the loss of devices containing sensitive data is a big risk and preventive measures are a top priority.
	Extend desktop hardware lifecycle – Replacing workstations every three to five years in order to keep up with the requirements of the operating system or the applications has been very costly.
	Reducing cost – Cut costs associated with supporting and maintaining traditional desktops.
	Improving user experience - Increasing performance or enabling features which would otherwise not be possible with a geographically dispersed user population

Table 1: Sample Business Drivers

The prioritization process should be completed in collaboration with the project team, business managers and IT managers so that all views are considered.

## Step 2: Define the User Groups

Although there are multiple approaches towards defining user groups, it is often easiest to align user groups with departments as most users within the same department or organizational unit consumes the same set of applications.

### User Segmentation

Depending on the size of the department, there might be a subset of users with unique requirements. Each defined user group should be evaluated against the following criteria to determine if the departmental user group needs to be further divided into more specialized user groups.

- Primary datacenter – Each user will have a primary datacenter assigned that will be used to host their virtual desktop, data, and application servers. Identify the datacenter that the user should be assigned to rather than the datacenter they are currently using. Users will be grouped based on their primary datacenter so that a unique design can be created for each one.
- Personalization – Personalization requirements are used to help determine the appropriate VDI model for each user group. For example, if a user group requires complete personalization, a personal desktop will be recommended as the optimal solution. There are three classifications available:

Personalization	Requirement
None	User cannot modify any user or application settings, for example - kiosk.
Basic	User can modify user-level settings of desktops and applications.
Complete	User can make any change, including installing applications.

Table 2: Personalization Characteristics

- Security – Security requirements are used to help determine the appropriate desktop and policy (or policies) for each user

group. For example, if a user group requires high security, a hosted pooled desktop or a local VM desktop will be recommended as the optimal solution. There are three classifications available:

Security Level	Description
Low	Users are allowed to transfer data in and out of the virtualized environment.
Medium	All authentication and session traffic should be secured; users should not be able to install or modify their virtualized environment.
High	In addition to traffic encryption, no data should leave the data center (such as through printing or copy/paste); all user access to the environment should be audited.

Table 3: Security Characteristics

- Mobility – Mobility requirements are used to help determine the appropriate desktop model for each user group. For example, if a user group faces intermittent network connectivity, then any VDI model requiring an active network connection is not applicable. There are four classifications available:

Mobility	Requirement
Local	Always uses the same device, connected to an internal, high-speed and secured network.
Roaming Local	Connects from different locations on an internal, high-speed, secured network.
Remote	Sometimes connects from external variable-speed, unsecure networks.
Mobile	Often needs access when the network is intermittent or unavailable.

Table 4: Mobility Characteristics

- Desktop Loss Criticality – Desktop loss criticality is used to determine the level of high availability, load balancing and fault tolerance measures required. For example, if there is a high risk to the business if the user's resource is not available, the user should not be allocated a local desktop because if that local desktop fails, the user will not be able to access their resources. There are three classifications available:

Desktop loss criticality	Requirement
Low	No major risk to products, projects or revenue.
Medium	Potential risk to products, projects or revenue.
High	Severe risk to products, projects or revenue.

Table 5: Desktop loss criticality Characteristics

- Workload – Types and number of applications accessed by the user impacts overall density and the appropriate VDI model. Users requiring high-quality graphics will either need to utilize a local desktop implementation or a professional graphics desktop. There are three classifications available:

User Type	Characteristics
Light	1-2 office productivity apps or kiosk.
Medium	2-10 office productivity apps with light multimedia use.
Heavy	Intense multimedia, data processing or application development.

Table 6: Workload Characteristics

## 注意

Performance thresholds are not identified based on processor, memory or disk utilization because these characteristics will change dramatically following the application rationalization and desktop optimization process. In addition, it is likely that the user's management tools and operating system will change during the migration process. Instead, workload is gauged based on the number and type of applications the user runs.

### Experience from the Field

**Utility company** – A large utility company collected data on every user in their organization. During the user segmentation process it was realized that the organization's existing role definitions were sufficiently well defined that all the users within a role shared the same requirements. This allowed a significant amount of time to be saved by reviewing a select number of users per group.

**Government** – A government organization discovered that there was significant deviation between user requirements within each role, particularly around security and desktop loss criticality. As such, each user needed to be carefully reviewed to ensure that they were grouped appropriately.

## Assign VDI Models

As with physical desktops, it is not possible to meet every user requirement with a single type of VDI. Different types of users need different types of resources. Some users may require simplicity and standardization, while others may require high levels of performance and personalization. Implementing a single VDI model across an entire organization will inevitably lead to user frustration and reduced productivity.

Citrix offers a complete set of VDI technologies that have been combined into a single integrated solution. Because each model has different strengths, it is important that the right model is chosen for each user group within the organization.

The following list provides a brief explanation of each VDI model.

- **Windows Apps** – The Windows apps model utilizes a server-based or desktop-based Windows operating system, where only the application interface is seen by the user. This approach provides a seamless way for organizations to deliver a centrally managed and hosted application into the user's local PC. The Windows app model is often utilized when organizations must simplify management of a few line-of-business applications.
- **Browser Apps** – The browser apps model utilizes a server-based Windows operating system to deliver an app as a tab within the user's local, preferred browser. This approach provides a seamless way for organizations to overcome browser compatibility challenges when users have the ability to use their own preferred browser (Internet Explorer, Microsoft Edge, Google Chrome, Mozilla Firefox, etc.).
- **Shared Desktop** – With the shared desktop model, multiple user desktops are hosted from a single, server-based operating system (Windows 2008, 2012, 2016, Red Hat, SUSE, CentOS). The shared desktop model provides a low-cost, high-density solution; however, applications must be compatible with a multi-user server based operating system. In addition, because multiple users share a single operating system instance, users are restricted from performing actions that negatively impact other users, for example installing applications, changing system settings and restarting the operating system.
- **Pooled Desktop** – The pooled desktop model provides each user with a random, temporary desktop operating system. Because each user receives their own instance of an operating system, overall hypervisor density is lower when compared to the shared desktop model. However, pooled desktops remove the requirement that applications must be multi-user aware and support server-based operating systems.
- **Personal Desktop** – The personal desktop model provides each user with a statically assigned, customizable, persistent

desktop operating system. Because each user receives their own instance of an operating system, overall hypervisor density is lower when compared to the shared desktop model. However, personal desktops remove the requirement that applications must be multi-user aware and support server based operating systems.

- **Pro Graphics Desktop** – The pro graphics desktop model provides each user with a hardware-based graphics processing unit (GPU) allowing for higher-definition graphical content.
- **Local Streamed Desktop** – The local streamed desktop model provides each user with a centrally managed desktop, running on local PC hardware.
- **Local VM Desktop** – The local VM desktop model provides each user with a centrally managed desktop, running on local PC hardware capable of functioning with no network connectivity.
- **Remote PC Access** – The remote PC access desktop model provides a user with secure remote access to their statically assigned, traditional PC. This is often the fastest and easiest VDI model to deploy as it utilizes already deployed desktop PCs.

Compare each user group against the following table to determine which VDI model best matches the overall user group requirements. In many environments, a single user might utilize a desktop VDI model and an app VDI model simultaneously.

Segmentation Characteristic	Hosted Windows Apps	Hosted Browser Apps	Hosted Shared Desktop	Hosted Pooled Desktop	Hosted Personal Desktop	Hosted Pro Graphics Desktop	Local Streamed Desktop	Local VM Desktop	Remote PC Access
<b>Workload</b>									
Light	✓	✓	○	○	○	✗	○	○	○
Medium	○	○	✓	✓	○	○	○	○	○
Heavy	✗	✗	✗	✗	○	✓	✓	✓	○
<b>Mobility</b>									
Local	✓	✓	✓	✓	○	○	✓	○	○
Roaming Local	✓	✓	✓	✓	○	○	✗	○	○
Remote	✓	✓	✓	✓	○	○	✗	○	✓
Mobile	✗	✗	✗	✗	✗	✗	✗	✓	✗
<b>Personalization</b>									
None	✓	✓	✓	✓	✗	○	○	○	○
Basic	✓	✓	✓	✓	✗	○	○	○	○
Complete	✗	✗	✗	✗	✓		✗	✓	✓
<b>Security</b>									
Low	○	○	○	○	○	○	○	○	○
Medium	✓	✓	✓	✓	○	○	○	○	○
High	○	○	○	✓	✗	○	✓	✓	✗
<b>Desktop Loss Criticality</b>									
Low	○	○	○	○	○	○	○	○	○
Medium	✓	✓	✓	✓	○	○	○	○	✗
High	✓	✓	✓	✓	✗	○	○	✗	✗

"✓": Recommended, "✗": Not Recommended, "○": Viable

Table 7: VDI Model Capability Comparison

Don't forget to follow these top recommendations from Citrix Consulting based on years of experience:

### Citrix Consulting Tips for Success

1. **Start with Windows apps, shared and pooled desktops** - As you can see in the VDI capability table above, the Windows apps, hosted shared and pooled desktop models can be used in the majority of situations. The local streamed and local VM desktop models should only be used on an exception basis. By reducing the number of VDI models required, you will help to reduce deployment time and simplify management.
2. **Perfect match** - It may not be possible to select a VDI model that is a perfect match for the user group. For example, you can't provide users with a desktop that is highly secure and offers complete personalization at the same time. In these situations, select the VDI model which is the closest match to the organization's highest priorities for the user group.
3. **Desktop loss criticality** - There are only three VDI models that meet the needs of a high desktop loss criticality user

group (backup desktops available) – none of which allow for complete personalization. If a high-desktop loss criticality user group also requires the ability to personalize their desktop they could be provided with a pool of backup desktops (hosted shared, pooled) in addition to their primary desktop. Although these desktops would not include customizations made to their primary desktop, they would allow users to access core applications such as mail, Internet and Microsoft Office.

4. **Consider Operations & Maintenance** - The ongoing support of each VDI model should be factored in when deciding on a VDI model. For example, pooled desktops can be rebooted to a known good state which often leads to reduced maintenance versus a personal desktop where each desktop is unique.

## Step 3: Define the Applications

Once the users have been divided up into groups the next step is to determine which applications they require.

This is a two-step process:

1. **Application rationalization** - Help to simplify the application assessment by removing redundant applications from the inventory that were captured during the data capture.
2. **Link apps to users** - Use the results from the data capture process to map applications to user groups.

### Application Rationalization

The number of applications identified during the inventory is often surprising, even for organizations that believe they have a high-level of control over applications. To help reduce complexity as well as overall time required, it's important to take the time to consolidate the list of applications.

The following guidelines will help ensure that your application list is consolidated appropriately:

- **Multiple versions** - Different versions of the same application may have been identified during the inventory. There are various reasons for this, including an inconsistent patching or upgrade process, decentralized application management, limited licenses and situations where users require specific application versions for compatibility with other applications, macros and document formats. Where possible, work with the application owners to reduce the number of versions required. The leading practice is to standardize on a single version of each application, typically the latest.
- **Non-business applications** - Applications that are not required by the business should be removed from the application inventory to reduce resource requirements and to help simplify the overall project. Non-business related applications are typically found in an application inventory when users have been provided with the ability to install their own applications and typically include games, communication clients, screen savers, peripheral software and media players.
- **Legacy applications** - The inventory may identify legacy applications that have since been retired or that are no longer required within the business. These applications may not have been removed from the desktops because there is no established process to do so or because there are always more highpriority activities to complete. These applications should be consolidated during the rationalization stage of the application assessment.
- **Management applications** - The antivirus, application delivery, monitoring, inventory, maintenance and backup applications will be completely re-designed across the organization during the desktop virtualization project. These applications should also be consolidated during this stage.

#### Experience from the Field

**Government:** A government organization identified that there were 2,660 applications installed across their desktop estate. Most of which were installed by users with local administrative rights. By following the application rationalization recommendations above, it was possible to reduce the number of applications required to 160.

## Application Categorization

Each application included in the project should be categorized based on certain criteria, which will help determine the most appropriate way to host and integrate the app. Each application can be installed directly into the image, virtualized in an isolated container and streamed to the desktop (Microsoft App-V), captured in a unique layer and attached to the virtual machine (Citrix AppDisk) or installed locally on the user's endpoint device and seamlessly integrated into the user's virtual desktop (Citrix Local App Access). Due to the uniqueness of every application, many large-scale deployments simultaneously utilize multiple approaches.

Each application should be categorized as follows:

- **Common Apps** - Every organization includes a suite of applications utilized by almost every user, Microsoft Office for example. This suite of applications is often the most utilized application in a desktop VDI model.
- **Departmental Apps** - A certain set of applications are only relevant for a unique business unit or department. For example, an engineering department will often require software development applications.
- **User Apps** - Often making up the largest grouping of apps are the apps used by very few individual users. In a traditional PC implementation, these applications are installed by the user as a temporary requirement or a personal requirement, often not directly impacting the business.
- **Management Apps** - Many desktop deployments include a combination of antivirus, monitoring, inventory, maintenance and backup applications. Many of these applications have unique virtualization requirements and are often required across the entire organization.

## Application Characterization

The following characteristics should be identified for each application so that the right application delivery model can be selected during the design phase of the project:

- **Complex** - An application should be classified as technically challenging if it is complex to set up, has extensive dependencies on other applications or requires a specialized configuration, for example an Electronic Medical Records (EMR) application. Technically challenging applications need to be identified during the application assessment because they are not generally appropriate for installation into a base desktop image or delivery by application streaming. Delivering technically challenging applications as a hosted Windows app will help to reduce the complexity of the base desktop image.
- **Demanding** - Collecting application resource requirements allows the virtualization infrastructure to be sized and an appropriate application delivery model to be selected. For example, resource intensive applications will not be delivered via a hosted shared desktop because there is limited control over how the resources are shared between users. There are two classifications available in the user assessment worksheet:

Workload	Requirement
Resource Intensive	Application requires 1GB+ of RAM or averages 50%+ CPU utilization.
None	The application is not resource intensive.

Table 8: Application Workload Characteristics

- **Mobile** - Some user groups may require the ability to work while mobile, sometimes when offline. If so, it is important that the design can determine which applications will work without a network connection and which ones will not. Applications that require backend infrastructure such as web and database servers are not typically available offline.
- **Peripherals** - If applications require connectivity with peripheral devices, identify the interface required so that it can be made available to the application when it is run from a virtual session.
- **Restrictions** - Application access may need to be restricted due to insufficient licenses / resources and to protect sensitive data / tools. For example, applications with a limited number of licenses should not be installed on a base image that is shared with unlicensed users. There are three restricted access categories in the application assessment workbook:

Restricted Access	Requirement
No	There are no restrictions for the application and it can be accessed by any user within the organization.
User group	The application may be installed on a multi-user operating system but only a specific group of users should be provided with an icon.
Virtual machine	Application should only be installed on a virtual machine that is accessible by authorized users.

Table 9: Restricted Access Characteristics

## Step 4: Define the Project Team

Desktop virtualization is a fundamental change that requires close collaboration between various business and technical teams in order to be successful. For example, the virtualization and desktop teams need to work together to ensure that the virtual desktop image meets user needs while also being optimized for the datacenter. Failure to build a cohesive project team that consists of the right roles and skillsets can negatively impact performance, availability, user experience and supportability while also increasing costs and risk.

The following tables identify the business and technical roles required during an enterprise virtual desktop deployment. Although the list may seem quite large, many of these roles are only required for a short time and multiple roles may be performed by a single person. The project manager and Citrix architect are considered to be full time roles with other team members being brought in only when required. The project manager role is key to ensuring that the right people are involved in the project at the right time.

### Business Roles

Role	Description	Example Responsibilities
Project sponsor	The project sponsor is a senior company executive who recognizes the benefits that desktop virtualization will bring to the business. The project sponsor role is often performed by the chief technology officer (CTO).	<p><b>Pre-project</b></p> <ul style="list-style-type: none"> <li>• Promote desktop virtualization within business</li> <li>• Identify members of the steering committee</li> </ul> <p><b>Secure funding</b></p> <ul style="list-style-type: none"> <li>• Assess general costs associated with</li> </ul>

Role	Description	<ul style="list-style-type: none"> <li>• Identify and prioritize key business drivers</li> </ul> <b>Responsibilities</b>
Project Manager	<p>The project manager directs the project team and is responsible for ensuring that project objectives are completed on time and within budget.</p>	<p><b>All steps</b></p> <ul style="list-style-type: none"> <li>• Define key project milestones</li> <li>• Create and update project plan</li> <li>• Track progress against plan</li> <li>• Track expenditure against budget</li> <li>• Maintain issue and risk register</li> <li>• Manage scope changes</li> <li>• Create weekly project reports</li> <li>• Brief steering committee on progress</li> <li>• Organize project workshops and meetings</li> <li>• Ensure project teams are synchronized</li> <li>• Ensure pre-requisites are in place</li> <li>• Creates change control requests</li> </ul>
Business Manager	<p>Depending on company structure and size, business managers oversee planning and performance at a department, region or company level. A business manager understands the requirements necessary for their employees to be successful.</p>	<p><b>Assess</b></p> <ul style="list-style-type: none"> <li>• Assist with application consolidation project</li> <li>• Provide details on connectivity requirements of user group, including offline usage</li> <li>• Provide details on risk tolerance of user group</li> <li>• Identify requirements for peripherals</li> </ul> <p><b>Deploy</b></p> <ul style="list-style-type: none"> <li>• Promote benefits of desktop virtualization</li> <li>• Assist with coordinating the rollout</li> </ul>

Role	Description	<b>Example</b> <b>Responsibilities</b>
Business continuity manager	<p>The business continuity manager ensures that an organization can continue to function after a disruptive event such as natural disaster, crime or human/computer error.</p>	<p><b>Example</b>  <b>Responsibilities</b></p> <p>with detailed understanding of the current business continuity plan</p> <p><b>Design</b></p> <ul style="list-style-type: none"> <li>Update business continuity plan to incorporate the new Citrix infrastructure</li> </ul> <p><b>Deploy</b></p> <ul style="list-style-type: none"> <li>Test business continuity plan</li> </ul>
Test Manager	<p>The test manager is responsible for ensuring that the test and user acceptance environments match the production environments as closely as possible. The test manager helps to reduce risk by ensuring that changes are fully tested before being implemented in production.</p>	<p><b>Assess</b></p> <ul style="list-style-type: none"> <li>Provide Citrix architect with detailed understanding of current testing infrastructure and processes</li> </ul> <p><b>Design</b></p> <ul style="list-style-type: none"> <li>Work with Citrix architect to design an appropriate testing infrastructure and test plan for new Citrix environment</li> </ul> <p><b>Deploy</b></p> <ul style="list-style-type: none"> <li>Ensure that testing design is implemented correctly and new Citrix infrastructure is fully tested before rollout</li> </ul>
	<p>An application owner is a subject matter expert on specific applications deployed</p>	<p><b>Assess</b></p> <ul style="list-style-type: none"> <li>Assist with application consolidation project</li> <li>Identify application licensing limitations</li> <li>Provide details on security restrictions</li> <li>Provide details on application</li> </ul>

Role	<b>Description</b> Owners with the applications are resolved and that upgrades/updates are performed without issue. Application owners are also responsible for managing support agreements with the application vendors.	<b>Example</b> <b>Responsibilities</b> <b>Deploy</b> <ul style="list-style-type: none"> <li>Provide location of back-end resources</li> </ul>
Service desk manager	<p>The service desk manager helps to improve productivity and end-user satisfaction by ensuring that production issues are logged, escalated and resolved in a timely manner. The service desk manager is also responsible for reporting on common issues, call volumes and service desk performance.</p>	<b>Assess</b> <ul style="list-style-type: none"> <li>Identify common issues with existing environment</li> <li>Provide details on support tools currently used</li> </ul> <b>Design</b> <ul style="list-style-type: none"> <li>Assist Citrix architect with designing a delegated administration model</li> <li>Participate in operations and support design workshops</li> <li>Work with training manager to identify training requirements</li> </ul> <b>Deploy</b> <ul style="list-style-type: none"> <li>Monitor helpdesk calls for rollout related issues</li> </ul>
Training manager	<p>The training manager ensures that support staff and end-users are proficient with new areas of technology. The training manager also has responsibility for ensuring that the training plan is up-to-date and followed appropriately.</p>	<b>Assess</b> <ul style="list-style-type: none"> <li>Determine current skill set for support staff and end users</li> </ul> <b>Design</b> <ul style="list-style-type: none"> <li>Create training plan for support staff and end users</li> </ul> <b>Deploy</b> <ul style="list-style-type: none"> <li>Implement training plan for support staff and end users</li> </ul>

Role	Description	Design Example Work with project manager to create communications plan
Communications manager	The communication manager is responsible for disseminating key information throughout the organization.	<b>Deploy</b> <ul style="list-style-type: none"> <li>• Relay benefits of desktop virtualization</li> <li>• Inform users of key migration dates</li> <li>• Ensure expectations are set accordingly</li> </ul>

## Technical Roles

Role	Description	Example Responsibilities
Citrix desktop architect	The Citrix architect acts as the design authority for all Citrix products and liaises with other architects to ensure that the Citrix infrastructure is successfully integrated into the organization.	<p><b>Assess</b></p> <ul style="list-style-type: none"> <li>• Work with project sponsor and key stakeholders to identify and prioritize key business drivers</li> <li>• Oversee user segmentation and app. assessment</li> <li>• Map VDI models to user groups</li> <li>• Perform capabilities assessment to determine current state of readiness</li> <li>• Identify areas of risk and provides remedial actions</li> </ul> <p><b>Design</b></p> <ul style="list-style-type: none"> <li>• Create Citrix design that includes hardware and storage estimates</li> <li>• Coordinate with other architects to integrate Citrix infrastructure into organization</li> <li>• Work with monitoring architect to ensure that Citrix environment is monitored appropriately</li> <li>• Create operations and support design</li> <li>• Create implementation and rollout design</li> <li>• Create test plan</li> </ul> <p><b>Deploy</b></p> <ul style="list-style-type: none"> <li>• Ensure that the Citrix environment is implemented in accordance with design</li> <li>• Verify that implementation passes test plan</li> <li>• Ensure that the Citrix design is implemented correctly</li> </ul>
Active directory	Design authority on Microsoft Active Directory, including Organizational Units (OU) and Group Policy	<p><b>Assess</b></p> <ul style="list-style-type: none"> <li>• Provide Citrix architect with detailed understanding of current Active Directory architecture</li> </ul> <p><b>Design</b></p> <ul style="list-style-type: none"> <li>• Work with the Citrix architect to design OU structure, group policies, permissions, service accounts, etc. for new Citrix environment</li> </ul>

Role	Description	
		<p>centralization of user data and accounts</p> <p><b>Example Responsibilities</b></p> <p><b>Deploy</b></p> <ul style="list-style-type: none"> <li>• Ensure that Active Directory design is implemented correctly</li> </ul>
Virtualization architect	Design authority on server and desktop virtualization using Citrix XenServer, Microsoft Hyper-V, Nutanix Acropolis or VMware vSphere.	<p><b>Assess</b></p> <ul style="list-style-type: none"> <li>• Provide Citrix architect with detailed understanding of current virtualization architecture</li> </ul> <p><b>Design</b></p> <ul style="list-style-type: none"> <li>• Work with Citrix architect to design hardware, networking, storage, high availability, etc. for server and desktop virtualization</li> <li>• Work with monitoring architect to ensure that virtualization environment is monitored appropriately</li> </ul> <p><b>Deploy</b></p> <ul style="list-style-type: none"> <li>• Ensure that the virtualization design is implemented correctly</li> </ul>
Network architect	Design authority on networking, including routing, VLANs, DHCP, DNS, VPN and firewalls.	<p><b>Assess</b></p> <ul style="list-style-type: none"> <li>• Provide Citrix architect with detailed understanding of current networking architecture</li> </ul> <p><b>Design</b></p> <ul style="list-style-type: none"> <li>• Work with Citrix architect to design physical network, virtual networks, routing, firewalls, quality of service, remote access, network optimization, etc. for new Citrix environment</li> <li>• Work with monitoring architect to ensure that network is monitored appropriately</li> </ul> <p><b>Deploy</b></p> <ul style="list-style-type: none"> <li>• Ensure that network design is implemented correctly</li> </ul>
Desktop architect	Design authority on Microsoft desktop operating systems, including Windows XP, Windows 7 and Windows 8.	<p><b>Assess</b></p> <ul style="list-style-type: none"> <li>• Provide Citrix architect with detailed understanding of current desktop environment</li> </ul> <p><b>Design</b></p> <ul style="list-style-type: none"> <li>• Work with Citrix architect to design core desktop virtual image, core applications, desktop optimizations, etc. for new Citrix environment</li> <li>• Work with monitoring architect to ensure that the virtual desktops are monitored appropriately</li> </ul> <p><b>Deploy</b></p> <ul style="list-style-type: none"> <li>• Ensure that desktop design is implemented correctly</li> </ul>
		<p><b>Assess</b></p> <ul style="list-style-type: none"> <li>• Provide Citrix architect with detailed understanding of</li> </ul>

Role	Description	Example Responsibilities
Storage architect	Design authority on storage solutions, including direct-attached storage, storage-attached networks and network attached storage.	<p><b>Example Responsibilities</b></p> <ul style="list-style-type: none"> <li>Work with Citrix architect to design storage architecture, tiers, sizing, connectivity, etc. for new Citrix environment</li> <li>Work with monitoring architect to ensure that storage is monitored appropriately</li> </ul> <p><b>Deploy</b></p> <ul style="list-style-type: none"> <li>Ensure that storage design is implemented correctly</li> </ul>
Backup architect	Design authority on backup and recovery, including virtual machines, desktops, servers, user data and databases.	<p><b>Assess</b></p> <ul style="list-style-type: none"> <li>Provide Citrix architect with detailed understanding of current backup architecture and processes</li> </ul> <p><b>Design</b></p> <ul style="list-style-type: none"> <li>Work with Citrix architect and disaster recovery architect to design backup architecture, process, schedule, retention, etc. for new Citrix environment</li> </ul> <p><b>Deploy</b></p> <ul style="list-style-type: none"> <li>Ensure that backup design is implemented correctly</li> </ul>
Application packaging architect	Design authority on packaging applications for deployment through the systems management team.	<p><b>Assess</b></p> <ul style="list-style-type: none"> <li>Provide Citrix architect with detailed understanding of current application packaging process and status</li> </ul> <p><b>Design</b></p> <ul style="list-style-type: none"> <li>Ensure that all required applications are packaged according to design</li> </ul>
Monitoring architect	Design authority on monitoring, including hardware, network, servers, storage and security appliances.	<p><b>Assess</b></p> <ul style="list-style-type: none"> <li>Provide Citrix architect with detailed understanding of current monitoring architecture and processes</li> </ul> <p><b>Design</b></p> <ul style="list-style-type: none"> <li>Work with Citrix architect to design monitoring architecture, metrics, alerts, etc. for new Citrix environment and supporting infrastructure</li> </ul> <p><b>Deploy</b></p> <ul style="list-style-type: none"> <li>Ensure that monitoring design is implemented correctly</li> <li>Provide regular reports on capacity and trends during rollout</li> </ul>
Systems management architect	Design authority on systems management, including server/desktop build process, patching and automated application installation.	<p><b>Assess</b></p> <ul style="list-style-type: none"> <li>Provide Citrix architect with a detailed understanding of the current systems management processes</li> </ul> <p><b>Design</b></p> <ul style="list-style-type: none"> <li>Works with Citrix architect to define server/desktop build process, patching and application delivery strategy for new Citrix environment</li> </ul>

Role	Description	<b>Example Responsibilities</b> <ul style="list-style-type: none"> <li>• Ensure that the systems management designs</li> </ul>
Security architect	Design authority on security, including desktops, servers, networks and VPNs.	<p><b>Assess</b></p> <ul style="list-style-type: none"> <li>• Provide Citrix architect with detailed understanding of current security policy</li> </ul> <p><b>Design</b></p> <ul style="list-style-type: none"> <li>• Work with Citrix architect to design security standards for new Citrix environment, including authentication, encryption, port numbers, firewall rules, etc.</li> </ul> <p><b>Deploy</b></p> <ul style="list-style-type: none"> <li>• Ensure that security design is implemented correctly</li> </ul>

# 设计

Jan 25, 2017

## Overview

Designing a desktop virtualization solution is simply a matter of following a proven process and aligning technical decisions with organizational and user requirements. Without the standardized and proven process, architects tend to randomly jump from topic to topic, which leads to confusion and mistakes. The recommended approach focuses on working through five distinct layers:

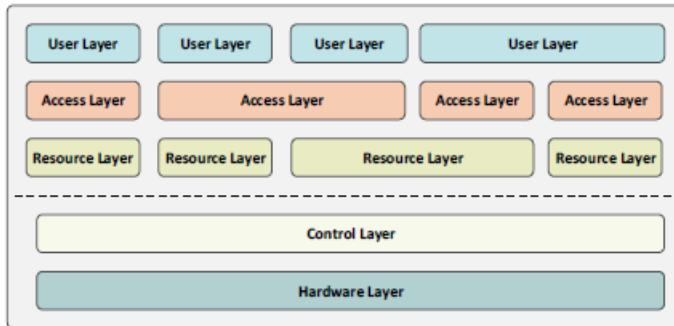


Figure 3: Five-Layer Design Model

The top three layers are designed for each user group independently, which were identified during the user segmentation section of the assess phase. These layers define the users' resources and how users access their resources. Upon completion of these three layers, the foundational layers (control and hardware) are designed for the entire solution.

This process guides the design thinking in that decisions made higher up impact lower level design decisions.

### Layer 1: The User Layer

The top layer of the design methodology is the user layer, which is defined for each unique user group.

The user layer appropriately sets the overall direction for each user group's environment. This layer incorporates the assessment criteria for business priorities and user group requirements in order to define effective strategies for endpoints and Citrix Receiver. These design decisions impact the flexibility and functionality for each user group.

### Endpoint Selection

There are a variety of endpoint devices available, all with differing capabilities, including:

- Tablet based
- Laptop
- Desktop PC
- Thin client
- Smartphone

The user's primary endpoint device must align with the overall business objectives as well as each user's role and associated requirements. In many circumstances, multiple endpoints may be suitable, each offering differing capabilities.

### Decision: Endpoint Ownership

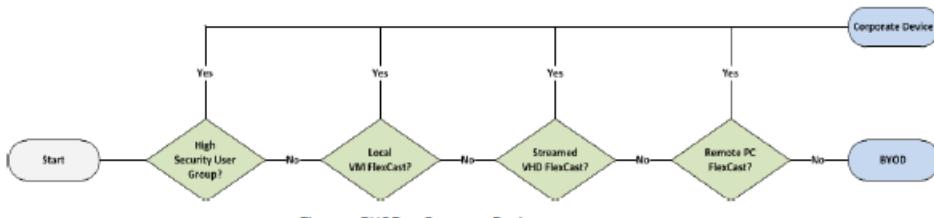
In many organizations, endpoint devices are corporate owned and managed. However, more and more organizations are now introducing bring your own device (BYOD) programs to improve employee satisfaction, reduce costs and to simplify device management. Even if BYOD is a business priority, it does not mean that every user should be allowed to use a

personal device in the corporate environment.

Certain user requirements, which were identified during the user segmentation, can greatly impact the suitability of personal devices:

- **Security** – Users requiring a high-level of security might not be able to bring a personal device into the secured environment for risk of data theft.
- **Mobility** – Users operating in a disconnected mode might not be able to use a personal device, as the local VM desktop VDI model associated with this type of requirement can have specific hardware requirements, or special maintenance requirements.
- **Desktop loss criticality** – Users with a high desktop loss criticality rating might require redundant endpoints in the event of failure. This would require the user to have an alternative means for connecting in the event their personal device fails, likely making these users poor candidates for a BYOD program.
- **VDI models** – A personal device should not be recommended for user groups utilizing a local VDI model like a local streamed desktop, local VM desktop or Remote PC Access. These VDI models typically require a specific hardware configuration or installation that will restrict device selection.

The following diagram provides guidance on when user owned devices could be used:



#### Decision: Endpoint Lifecycle

Organizations may choose to repurpose devices in order to extend refresh cycles or to provide overflow capacity for contract workers. Endpoints now offer more capabilities allowing them to have longer useful lifespans. In many cases, these hardware capabilities vastly outstrip the needs of a typical user. When coupled with the ability to virtualize application and desktop workloads, this provides new options to administrators such as repurposing existing workstations. These options go well beyond the simple three-year PC refresh cycle. However, the benefits of repurposing or reallocating a workstation should be balanced against the following considerations.

- **Minimum standards** - While cost factors of repurposing existing workstations may be compelling, certain minimum standards should be met to guarantee a good user experience. At a minimum, it is recommended that repurposed workstations have a 1GHz processor, 1GB of RAM, 16GB of free disk space and a GPU that is capable of supporting HDX features.
- **Business drivers** - Priorities underpin the success of any major project. Those organizations that have prioritized reducing capital expenditure by means of prolonging the hardware refresh cycle can benefit from repurposing hardware. Conversely, if an organization's business drivers include reducing power consumption as part of an overall green initiative, purchasing newer endpoints may be beneficial in order to take advantage of the latest generation of power management capabilities available in the most modern devices.
- **Workload** - The type of work and VDI model for an end user can determine whether they are a good candidate for a repurposed endpoint, or may be better served with a new device. If the work performed by the individual involves locally installed applications, the individual may be best served by a new endpoint that offers the most powerful and recently updated processor and graphics architecture. However, if a user is largely performing tasks associated with virtualized applications that do not involve the latest multimedia capabilities such as webcams, VoIP and media redirection, then a

repurposed workstation should be a viable alternative.

The following planning matrix outlines considerations when repurposing existing hardware:

Endpoint Provisioning Criteria	Repurpose Existing	Procure New
Capital restrained environment	✓	
High number of virtualized applications	✓	
Desire to prolong hardware refresh cycle	✓	
High failure rate among existing desktops		✓
Outmoded client-side feature set		✓
Power consumption or green initiative(s)		✓

Table 12: Endpoint Procurement Criteria

### Decision: Endpoint Form Factor

The capabilities of endpoints have grown along with efficiencies offered in thin client form factors. Even mid-range thin clients now have graphics capabilities that allow utilization of HDX features such as multi-monitor support while offering management and power efficiency benefits. Citrix has developed a three-tiered classification for thin clients based on their HDX capabilities: HDX Ready, HDX Premium, and HDX 3D Pro, which can be used to help narrow the field of appropriate thin client devices based on the use case requirements. This expansion of capabilities has given IT administrators more options and flexibility than ever before.

Most organizations will likely deploy a mixture of fully featured clients as well as thin clients. However, certain endpoint devices are more appropriate when used in combination with certain VDI models as explained in the following table:

VDI Model	Thin Clients	Desktop PC	Laptop	Tablet	Smartphone
Hosted Windows Apps	✓	✓	✓	✓	✓
Hosted Browser Apps	✓	✓	✓	✓	✓
Hosted Shared Desktop	✓	✓	✓	○	○
Hosted Pooled Desktop	✓	✓	✓	○	○
Hosted Personal Desktop	✓	✓	✓	○	○
Hosted Pro Graphics Desktop	✓	✓	○	○	○
Local Streamed Desktop	✗	✓	✗	✗	✗
Local VM Desktop	✗	○	✓	✗	✗
Remote PC Access	✗	✓	✓	○	○

"✓": Recommended, "✗": Not Recommended, "○": Viable

Table 13: Primary Endpoint Selection

#### Experience from the Field

Large systems integrator – A large systems integrator recommended that a customer deploy a single type of low-end, limited capability endpoint for all users. Upon deployment to production, users immediately complained that they received a poor user experience when viewing multimedia content over the WAN. At great cost, the systems integrator and customer re-assessed the environment and chose to deploy endpoints that supported HDX MediaStream. The mistake caused a schism between systems integrator and the customer, resulting in lost time, capital and the end of a business relationship that was fostered over many years. It is critical that the endpoints assigned to each user group can support their requirements.

### Receiver Selection

Citrix Receiver is an easy-to-install software client that provides access to applications, desktops and data easily and securely from any device, including smartphones, tablets, PCs and Macs.

The following section provides a series of design decisions that should be considered when deploying Citrix Receiver.

### Decision: Receiver Type

While most organizations should simply deploy the latest Citrix Receiver compatible with their endpoint, it is important to recognize that there are certain differences between editions. The following table should be referenced to determine the most appropriate edition of Citrix Receiver for each user group. For the latest feature matrix, please refer to [Receiver Feature Matrix](#).

### Decision: Initial Deployment

There are several deployment options available for delivering Citrix Receiver to an endpoint. Although it is usually a best practice to have a full version of Citrix Receiver deployed to an endpoint to provide the greatest level of functionality, it is important to consider fallback options such as the HTML5 Receiver for those situations where the installation of Citrix Receiver is simply not possible. Note that although the HTML5 Receiver can be used as a fallback option, like the Java client was with Web Interface, it is not generally recommended as the primary Receiver for enterprises to standardize on due to the limited feature set and common browser restrictions around unsecured WebSockets connections (see [CTX134123](#) for more information).

#### Experience from the Field

Furniture distributor – A furniture distributor maintains a configurator application for various furniture options. The configurator application is accessed via a limited functionality kiosk that is deployed at various furniture outlets, including small, independent retailers with little to no IT staff present. The kiosks are completely locked down in many situations, to the point where even the running of Java applications is limited. The kiosks do feature a modern browser (Google Chrome), and therefore, are able to utilize the HTML5 Receiver in order to provide access to the configurator application.

County government – A government IT organization provides services to all agencies operating in the county. A mixture of full desktops and applications are deployed to both Windows based desktops and iPads. Since the desktops are joined to the Active Directory domain, GPOs are utilized to deploy and configure Citrix Receiver. Mobile users accessing the Citrix environment via an iPad install and configure Receiver from the App Store. To allow for seamless provisioning, email based discovery was configured. This allows users to configure Receiver for both internal and external access through NetScaler Gateway by entering in their email address.

The following mechanisms are commonly used to deploy and update Citrix Receiver:

- **StoreFront** - If Citrix StoreFront is available, administrators can deploy Citrix Receiver via a Receiver for Web site by enabling the “Client Detection” feature. When deployed, a Receiver for Web site enables users to access StoreFront stores through a web page. If the Receiver for Web site detects that a user does not have a compatible version of Citrix Receiver, the user is prompted to download and install Citrix Receiver. The Receiver clients can be hosted on the StoreFront server, or users can be directed to [citrix.com](http://citrix.com) for the latest Receiver files.
- **Internal download site** - Users may be prevented from downloading software from the Internet, even if they have permission to install applications. Administrator can create an internal website for supported Citrix Receivers or host them on a common software distribution point for a more seamless user experience. This could be an alternative to enabling Client Detection on the StoreFront Receiver for Web site, which can result in an inconsistent user experience depending on browser’s ActiveX settings.
- **Markets and stores** - Citrix Receiver is available on the Windows, Android and iOS stores..
- **Enterprise software deployment** - Many organizations employ an enterprise software deployment (ESD) or Mobile Application Management (MAM) solution. ESD/MAM solutions can be used to deploy Citrix Receiver to managed endpoint devices. Employee-owned devices can only be managed if the user successfully registered the device with the management tool.
- **Master image** - Most organizations have a group of master desktop images, which are deployed to each business

owned desktop, laptop, server, or virtual desktop. A common mechanism to ensure access to virtual desktops and applications is to include a supported version of Citrix Receiver in the master image. Subsequent updates to Citrix Receiver are handled either by enterprise software deployment tools or manually.

- **Group policy** - For customers without a robust ESD solution, it is possible to deploy and configure Citrix Receiver via Microsoft Group Policy. Sample start-up scripts that deploy and remove Citrix Receiver are available on Citrix XenApp and XenDesktop media:

#### *Citrix Receiver and Plugins|Windows|Receiver|Startup\_Logon\_Scripts*

- **Manual install** - All supported versions of Citrix Receiver are available from the Citrix Receiver Download site. Upon landing on this site, client detection is performed and a platform and operating system specific link is provided to allow users to download an appropriate edition of Citrix Receiver. It is important to note that no configuration will be accomplished via this download, so users will receive the first time use prompt to enter a server URL or email address. This option is likely to be utilized in a BYOD environment.

Selecting the appropriate deployment method is based on the type of Citrix Receiver selected. The following table should be referenced to help identify the appropriate deployment options for Citrix Receiver.

Deployment Options	Thin clients	Desktop PC	Laptop	Tablet	Smartphone
Base image	✓	✓	✓	✗	✗
ESD / MAM	✗	✓	✓	✗	✗
Group Policy	✗	✓	✓	✗	✗
Receiver for Web Site	✗	✓	✓	✗	✗
Internal Download Site	✗	✓	✓	✗	✗
App Store	✗	✗	✗	✓	✓

"✓": Recommended, "✗": Not Recommended

Table 14: Receiver Deployment Options

## Decision: Initial Configuration

Citrix Receiver must be configured in order to provide access to enterprise resources. The method of configuration varies by Citrix Receiver edition, the form factor of the device, and lastly the access method (local or remote) that is involved. Several methods may be viable for an organization. The method utilized is contingent on the resources (people, systems, time) available as well as larger organizational initiatives such as BYOD programs.

The following methods can be used to configure Citrix Receiver:

- **Email-based discovery** - The latest releases of Citrix Receiver can be configured by entering an email address. Email based discovery requires Citrix StoreFront as well as an SRV DNS record which points to the FQDN of the StoreFront server.

**Note:** Any DNS platform should support email-based discovery, however only Windows DNS has been explicitly tested.

For remote access, NetScaler Gateway must be utilized with the corresponding SRV record in external DNS. A valid server certificate on the NetScaler Gateway appliance or StoreFront server must be present in order to enable email-based account discovery. This configuration assumes that the portion of the email address after the "@" is the DNS namespace that should be queried for this SRV record. This can be challenging for customers with different external and internal namespaces or email addresses that are different from DNS namespaces.

- **Group policy** - Microsoft Group Policy can be used to configure Citrix Receiver. This can be done via start up scripts used to deploy Receiver by ensuring there is a value for the SERVER\_LOCATION=Server\_URL parameter or by using the ADMX/ADML template files included with the installation of Citrix Receiver to set the StoreFront Account List option in

conjunction with another Receiver deployment method. Provide the URL of the server running Citrix StoreFront in the format <https://baseurl/Citrix/storename/discovery>.

- **Provisioning file** - For environments running StoreFront, it is possible to provide users with a provisioning file that contains store information. Provisioning files are exported from the StoreFront console. The file is saved with a “\*.cr” extension and can then be placed on a shared network resource, a Receiver for Web site, or other web based resource or emailed to users. The file can then be launched from an endpoint, which automatically configures Citrix Receiver to use the store(s). If users browse to the Receiver for Web site and select the “Activate” option under their username, this also automatically downloads this same “.cr” file and configure the Receiver client for users.
- **Manually** - If allowed, it is usually possible to configure Citrix Receiver manually by entering the server URL. This method should be reserved for administrators or users that have advanced knowledge.
- **Studio** - In addition to the above methods, in order to configure Receiver deployed on a virtual desktop or server image (within a XenDesktop or XenApp environment), it is possible to set the StoreFront address via the properties of the Delivery Group.

#### Decision: Updates

Citrix Receiver is in active development. As such, periodic updates are released that provide enhanced functionality or address user issues. As with any actively developed product, the latest version of these products should be deployed to the endpoints so that users benefit from the latest functionality and to maintain compliance with product support lifecycles. There are multiple methods available to update Citrix Receiver and, if applicable, associated plug-ins.

- **Enterprise software deployment** - ESD tools provide an organization with direct control over the time/frequency of Receiver updates to managed devices. Additional thought must be given to updating unmanaged devices and endpoints outside of the corporate firewall.
- **Manual updates** - When no automated solution is available, manual methods can be used to update Citrix Receiver. Whether deployed on Receiver for Web site, StoreFront, an internal Citrix Receiver site, or an external site, these options will require user involvement in updating Citrix Receiver. Due to the involved nature of manual updates coupled with the opportunity for a user mistake, this option should only be considered as a last resort.

## Layer 2: The Access Layer

The second layer of the design methodology is the access layer, which is defined for each user group.

Creating an appropriate design for the access layer is an important part of the desktop virtualization process. This layer handles user validation through authentication and orchestrates access to all components necessary to establish a secure virtual desktop connection.

The access layer design decisions are based on the mobility requirements of each user group as well as the endpoint devices used.

#### Authentication

Getting access to resources is based on the user's identity. Defining the authentication strategy takes into account the user's entry point into the environment as well as how the user will authenticate.

#### Decision: Authentication Point

Before a user connects to a virtual resource, they must first authenticate. The place of authentication is often determined by the user group's mobility requirements, which were defined during the user segmentation process. There are two authentication points available in XenDesktop 7.6:

- **StoreFront** - Citrix StoreFront provides authentication and resource delivery services for Citrix Receiver, enabling centralized enterprise stores to deliver desktops, applications and other resources.
- **NetScaler Gateway** - NetScaler Gateway is an appliance providing secure application access and granular application-level policy controls to applications and data while allowing users to work from anywhere.

The following table lists preferred authentication points according to user group mobility requirements:

User Group's Mobility Requirement	Preferred Authentication Point
Local	StoreFront
Roaming local	StoreFront
Remote	NetScaler Gateway
Mobile	NetScaler Gateway

Table 15: Preferred Authentication Point

Authentication for user groups with a mobility requirement of remote or mobile may occur directly on StoreFront where required. For example, DMZ security policies may prohibit access from the NetScaler Gateway to the domain, which is required to support SmartCard client certificate authentication. Access to StoreFront for authentication may then be delivered via a NetScaler SSL\_BRIDGE virtual server, which provides a conduit for https traffic. Typically, the virtual server would be hosted alongside a NetScaler Gateway on the same NetScaler configured to provide HDX Proxy access to the virtual desktop environment. Although such a use case may sometimes be necessary, the recommended best practice is to authenticate external users via NetScaler Gateway.

### Decision: Authentication Policy

Once the authentication point has been identified, the type of authentication must be determined. The following options are the primary methods available:

- **StoreFront** - Supports a number of different authentication methods, although not all are recommended depending on the user access method, security requirements and network location. Note that by default StoreFront authenticates users directly with Active Directory, not via XML as Web Interface did. StoreFront 3.0+ can be optionally configured to delegate authentication to XML if required (such as if the StoreFront servers are in a domain that does not trust the user domains).
- **User name and password** - Requires users to logon directly to the site by entering a user name and password.
- **Domain pass-through** - Allows pass-through of domain credentials from users' devices. Users authenticate to their domain-joined Windows computers and are automatically logged on when they access their stores.
- **NetScaler Gateway pass-through** - Allows pass-through authentication from NetScaler Gateway. Users authenticate to NetScaler Gateway and are automatically logged on when they access their stores.
- **Smart card** - Allows users to authenticate using smart cards and PINs through Citrix Receiver for Windows and NetScaler Gateway. To enable smart card authentication, user accounts must be configured either within the Microsoft Active Directory domain containing the StoreFront servers or within a domain that has a direct two-way trust relationship with the StoreFront server domain. Multi-forest deployments involving one-way trust or trust relationships of different types are not supported.
- **Anonymous** - Allow users to access applications and desktops without presenting credentials to StoreFront or Citrix Receiver. Local anonymous accounts are created on demand on the Server VDA when sessions are launched. This requires a StoreFront store configured for authenticated access, a Server OS based VDA, and a XenApp 7.6 (or later) Delivery Group configured for unauthenticated users.
- NetScaler Gateway - The NetScaler Gateway supports several authentication methods. The list below includes those primarily used in virtual desktop environments. Each may be used individually, but are often combined to provide multi-factor authentication.
  - **LDAP** - The lightweight directory access protocol (LDAP) is used to access directory information services such Microsoft Active Directory. NetScaler Gateway uses LDAP to authenticate users and extract their group membership information.
  - **RADIUS (token)** - Remote authentication dial in user service (RADIUS) is a UDP based network security protocol that provides authentication, authorization and accounting. A network access server (NetScaler Gateway in this case) forwards credentials to a RADIUS server that can either check the credentials locally, or check them against a directory service. The RADIUS server could then accept the connection, reject the connection, or challenge and

request a second form of authentication such as a token.

- **Client certificate** - Users logging on to a NetScaler Gateway virtual server can also be authenticated based on the attributes of a client certificate presented to the virtual server. Client certificates are usually disseminated to users in the form of smartcards or common access cards (CACs) that are read by a reader attached to each user's device.

The authentication type for a user group is often determined based on security requirements as well as the authentication point used. The following table helps define the appropriate solution for each user group based on the level of security required:

Authentication Point	Security Requirement	Authentication Type
StoreFront	Low	<ul style="list-style-type: none"><li>• LDAP Username and Password</li><li>• Pass-through</li></ul>
	Medium	<ul style="list-style-type: none"><li>• LDAP Username and Password</li><li>• Pass-through</li></ul>
	High	<ul style="list-style-type: none"><li>• LDAP and/or Smartcard</li></ul>
NetScaler Gateway	Low	<ul style="list-style-type: none"><li>• LDAP Username and Password</li></ul>
	Medium	<ul style="list-style-type: none"><li>• LDAP Username and Password</li></ul>
	High	<ul style="list-style-type: none"><li>• LDAP and Token</li><li>• LDAP and Smartcard</li><li>• Token and Smartcard</li></ul>

Table 16: Authentication Policy Guidance

#### Experience from the Field

Retail – A small private retail company provides virtual desktop users with access to non-sensitive data such as marketing catalogs and email. They are not required to adhere to security regulations such as Sarbanes Oxley. Therefore, LDAP authentication has been implemented based on user name and password.

Financial – A medium financial enterprise provides their virtual desktop users with access to confidential data such as banking transaction records. They are governed by security regulations such as the Statement on Accounting Standards (SAS) 70 and are required to utilize multi-factor authentication for remote access users. LDAP authentication has been implemented based on user name and password along with RADIUS authentication using tokens.

Government – A large federal institution provides virtual desktop users with access to highly confidential data such as private citizens' personal records. They are subject to regulation by Department of Defense (DOD) security standards. LDAP authentication has been implemented based on user name and password, along with Client Certificate authentication using CAC cards.

Healthcare - A hospital is using XenApp to deliver their EMR application to users. ThinClient devices on stationary and mobile carts are being used by doctors and nurses to capture and retrieve patient data. Unauthenticated access has been configured to prevent medical staff from having to authenticate to the domain as well as the EMR application.

## StoreFront

Citrix StoreFront authenticates users to XenApp and XenDesktop resources. StoreFront enumerates and aggregates available desktops and applications into a single interface that users access through Citrix Receiver for Windows, iOS, Android, or the StoreFront web site.

### Decision: High Availability

If the server hosting StoreFront is unavailable, users cannot start new virtual desktops, published applications or manage their subscriptions. Therefore, deploy at least two StoreFront servers to prevent this component from becoming a single point of failure. By implementing a load balancing solution, users will not experience an interruption in their service. Options include:

- **Hardware load balancing** - An intelligent appliance, which is capable of verifying the availability of the StoreFront service and actively load balance user requests appropriately. Citrix NetScaler is a great example of a hardware load

balancer. Citrix NetScaler is an ideal load balancer, coming pre-configured with StoreFront health checks.

- **DNS round robin** - Provides rudimentary load balancing across multiple servers without performing any checks on availability. If a StoreFront server becomes unavailable, DNS round robin would still route users to the failed server. Because of this, DNS round robin is not recommended by Citrix.
- **Windows network load balancing** – A Windows service capable of performing rudimentary checks to verify the server is available but cannot determine the status of individual services. This can cause users to be forwarded to StoreFront servers which are not able to process new requests. The user would then not be able to access applications or desktops.

#### **Decision: Delivery Controller Reference**

To provide users with desktops and applications, StoreFront must be configured with the IP address or DNS name of at least one Controller in each XenDesktop and XenApp site. For fault tolerance, multiple controllers should be entered for each site and/or farm specified. By default, StoreFront treats a list of servers in failover order (active/passive).

For large deployments or environments with a high logon load an active distribution of the user load (active/active) is recommended. This can be achieved by means of a load balancer with built-in XML monitors, such as Citrix NetScaler or by configuring StoreFront to load balance the list of Controllers instead of treating them as an ordered list.

#### **Decision: Beacons**

Citrix Receiver uses beacons (websites) to identify whether a user is connected to an internal or external network. Internal users are connected directly to StoreFront for authentication while external users are connected via Citrix NetScaler Gateway. It is possible to control what a user sees by restricting applications due to which beacon they have access to.

The internal beacon should be a site that is not resolvable externally. By default, the internal beacon is the StoreFront base URL. This will have to be adjusted if the same external and internal URL is configured. The external beacon can be any external site that produces an http response. Citrix Receiver continuously monitors the status of network connections (for example, link up, link down or change of the default gateway). When a status change is detected, Citrix Receiver first verifies that the internal beacon points can be accessed before moving on to check the accessibility of external beacon points. StoreFront provides Citrix Receiver with the http(s) addresses of the beacon points during the initial connection/configuration download process and provides updates as necessary.

It is necessary to specify at least two highly available external beacons that can be resolved from public networks.

#### **Decision: Resource Presentation**

By default, StoreFront allows users to choose (subscribe) to the resources they want to regularly use after they logon (favorites). This approach, deemed “Self-Service,” allows users to restrict the resources that they see on their home screen to the ones that they use on a regular basis. The resources chosen by every user for each store are recorded by the subscription store service and stored locally on each StoreFront server (synced automatically between servers in the same server group) so that they can be displayed on the Citrix Receiver home screen from any device that the user connects from. Although by default subscriptions are per store and per server group, administrators can configure two stores within a server group to share a subscription database and/or sync subscriptions between two identically named stores in two separate server groups on a defined schedule if required.

Administrators should determine which applications should always be displayed to users on their home screen or the featured tab. In general, these applications are common applications such as the Microsoft Office Suite and any other applications that every user in an environment may need. StoreFront can filter/present these resources using Keywords defined within the published application properties Description field.

The following table explores the Keyword options:

Keyword	Description
Auto	Automatically subscribes all users of a store to an application. When users log on to the store, the application is automatically provisioned without users needing to manually subscribe to the application. Users can choose to subsequently remove this subscription if desired.
Mandatory	New in StoreFront 2.5, the Mandatory keyword will make applications automatically be subscribed to users of the store. However, users will not have the option to remove the application. This setting is useful when creating a core set of applications which must always be presented to all users.
Featured	Advertise applications to users or make commonly used applications easier to find by listing them in the Receiver Featured list.
Prefer	Specify a locally installed application should be used instead of an application available in Receiver. Receiver searches for the specified name/path to determine if the application is installed locally. If it is, Receiver subscribes the application and does not create a shortcut. When the user starts the application from the Receiver window, Receiver starts the locally installed (preferred) application. If a user uninstalls a preferred application outside of Receiver, the application is unsubscribed during the next Receiver refresh. If a user uninstalls a preferred application from the Receiver window, Receiver unsubscribes the application but does not uninstall it.
TreatAsApp	By default, XenDesktop VDI desktops and XenApp hosted shared desktops are treated like other desktops by Receiver for Web sites. By using the keyword "TreatAsApp," the desktop will be displayed in the application views of Receiver for Web sites rather than the desktop views. Users are required to subscribe before they can access the desktop.
Primary	When in a multi-site deployment, using this keyword ensures that an application is delivered from a designated site. If an application is available from multiple sites, with the same name, the application from the secondary site will only be displayed if the application is not available from the primary site.
Secondary	A same property as the "Primary" keyword, except it designates an application in the secondary site.

Table 17: Keywords for Application Delivery

## Decision: Scalability

The number of Citrix Receiver users supported by a single StoreFront server depends on the resources assigned and level of user activity. Note that Receiver for Web users will consume more RAM on average than native Receiver users, but a minimum of 4 GB of RAM is recommended per StoreFront server in all cases as a baseline. Additionally, more sites/farms enumerated per store will increase both CPU utilization and server response time, with XenApp IMA farms having a greater scalability impact than XenApp/XenDesktop FMA site.

StoreFront deployment	CPU Usage	Simultaneous activities
<ul style="list-style-type: none"> <li>• Standalone deployment</li> <li>• 4 CPUs</li> <li>• 4 GB RAM</li> <li>• Heavy Usage (logon, enumerate, subscribe, unsubscribe, logoff)</li> </ul>	75%	• 291 per second
	90%	• 375 per second
<ul style="list-style-type: none"> <li>• Cluster StoreFront deployment</li> <li>• 2 Nodes each with:           <ul style="list-style-type: none"> <li>◦ 4 CPUs</li> <li>◦ 4 GB RAM</li> <li>◦ Heavy Usage (logon, enumerate, subscribe, unsubscribe, logoff)</li> </ul> </li> </ul>	75%	• 529 per second
	90%	• 681 per second

Table 18: StoreFront Scalability

Tests have shown diminishing returns after a single StoreFront deployment grows beyond 3-4 StoreFront nodes with a maximum of 5-6 servers supported in a single server group.

## NetScaler Gateway

Selection of the network topology is central to planning the remote access architecture to ensure that it can support the necessary functionality, performance, and security. The design of the remote access architecture should be completed in

collaboration with the security team to ensure adherence to corporate security requirements. There are two primary topologies to consider, each of which provides increasing levels of security:

### Decision: Topology

Selection of the network topology is central to planning the remote access architecture to ensure that it can support the necessary functionality, performance and security. The design of the remote access architecture should be completed in collaboration with the security team to ensure adherence to corporate security requirements. There are two primary topologies to consider, each of which provides increasing levels of security:

- **1-Arm (normal security)** - With a 1-arm topology, the NetScaler Gateway utilizes one physical or logical bonded interface, with associated VLAN and IP subnet, to transport both frontend traffic for users and backend traffic for the virtual desktop infrastructure servers and services.

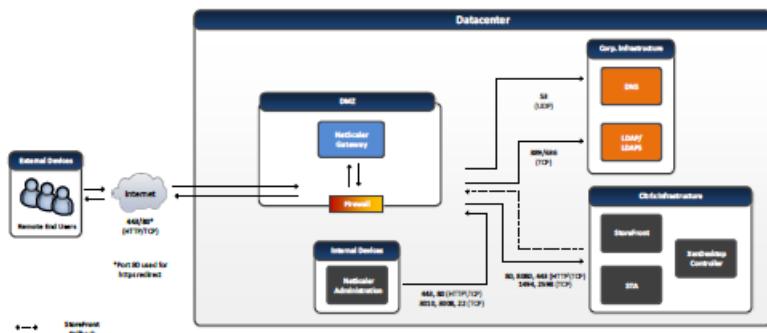


Figure 5: 1-Arm Topology

- **2-Arm (high security)** - With a 2-arm topology, the NetScaler Gateway utilizes two or more physically or logically bonded interfaces, with associated VLANs and IP subnets. Transport of the frontend traffic for users is directed to one of these interfaces. The frontend traffic is isolated from backend traffic, between the virtual desktop infrastructure servers and services, which is directed to a second interface. This allows the use of separate demilitarized zones (DMZs) to isolate frontend and backend traffic flows along with granular firewall control and monitoring.

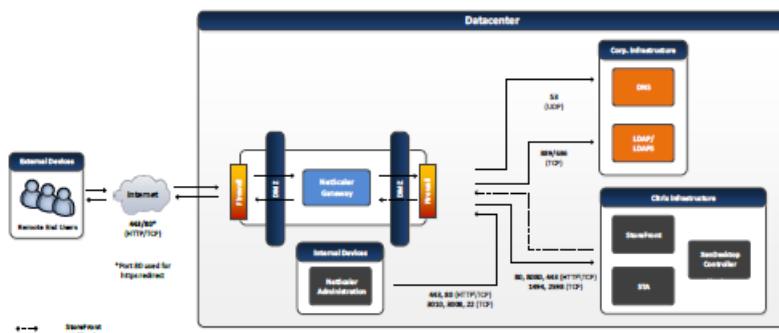


Figure 6: 2-Arm Topology

### Decision: High Availability

If the NetScaler Gateway is unavailable, remote users will not be able to access the environment. Therefore, at least two NetScaler Gateway hosts should be deployed to prevent this component from becoming a single point of failure.

When configuring NetScaler Gateway in a high availability (active/passive) pair, the secondary NetScaler Gateway monitors the first appliance by sending periodic messages, also called a heartbeat message or health check, to determine if the first appliance is accepting connections. If a health check fails, the secondary NetScaler Gateway tries the connection again for a specified amount of time until it determines that the primary appliance is not working. If the secondary appliance confirms the health check failure, the secondary NetScaler Gateway takes over for the primary NetScaler Gateway.

Note that in firmware 10.5 and above, clustering is also possible with multiple NetScaler Gateway instances to provide high availability, although support for spotted versus stripped configurations varies by firmware and Gateway configuration (full SSL VPN versus ICA proxy). (<http://docs.citrix.com/en-us/netscaler/11->

### Decision: Platform

In order to identify an appropriate NetScaler platform to meet project requirements, the key resource constraints must be identified. Since all remote access traffic will be secured using the secure sockets layer (SSL), transported by Hypertext Transfer Protocol (HTTP) in the form of HTTPS, there are two resource metrics that should be targeted:

- SSL throughput – The SSL throughput is the gigabits of SSL traffic that may be processed per second (Gbps).
- SSL transactions per second (TPS) – The TPS metric identifies how many times per second an Application Delivery Controller (ADC) may execute an SSL transaction. The capacity varies primarily by the key length required. TPS capacity is primarily a consideration during the negotiation phase when SSL is first setup and it is less of a factor in the bulk encryption / decryption phase, which is the majority of the session life. While TPS is an important metric to monitor, field experience has shown that SSL throughput is the most significant factor in identifying the appropriate NetScaler Gateway.

The SSL bandwidth overhead average is often considered negligible relative to the volume of virtual desktop traffic and is not typically accounted for as part of required SSL throughput. However, making provisions for SSL bandwidth will help ensure the total throughput estimated is sufficient. The fixed bandwidth added to packet headers can vary according to the encryption algorithms used and the overall percentage of bandwidth may vary widely according to packet size. Ideally, the overhead should be measured during a proof of concept or pilot. However, in the absence of such data incrementing the workload bandwidth by 2% is a reasonable rule of thumb. Therefore, to determine the SSL throughput required by a NetScaler platform, multiply the maximum concurrent bandwidth for a datacenter by 1.02:

$$h \quad h = \quad h * 1.02$$

For example, assuming 128Mbps maximum concurrent bandwidth, the appropriate NetScaler model can be determined as follows:

$$\sim 130 \quad = 128 \quad * 1.02$$

The SSL throughput value should be compared to the throughput capabilities of various NetScaler platforms to determine the most appropriate one for the environment. There are three main platform groups available, each of which provides broad scalability options.

- **VPX** - A NetScaler VPX device provides the same full functionality as hardware NetScalers. However, NetScaler VPXs can leverage 'off the shelf' servers for hosting and are suitable for small to medium sized environments. Typically, organizations create a baseline cap for the VPX instances at 500 users.
- **MDX** - A NetScaler MDX is the hardware version of the NetScaler devices. The MDX device is more powerful than the virtual NetScaler and can support network optimizations for larger scale enterprise deployments, particularly when SSL offload will be configured as this is done in software on the VPX versus dedicated SSL chips on the MPX.
- **SDX** - A NetScaler SDX is a blend between the virtual and physical NetScaler devices. An SDX machine is a physical device capable of hosting multiple virtual NetScaler devices. This consolidation of devices aids with reducing required shelf space and device consolidation. NetScaler SDXs are suitable for handling network communications for large enterprise deployments and/or multi-tenant hosting providers.

SSL throughput capabilities of the NetScaler platforms may be found in the Citrix NetScaler data sheet. Therefore, based on the example calculation above, a NetScaler MPX 5550 appliance would be sufficient to handle the required load. However, actual scalability will depend on security requirements. NetScaler SSL throughput decreases with the use of increasingly complex encryption algorithms and longer key lengths. Also, this calculation represents a single primary NetScaler. At a minimum, N+1 redundancy is recommended which would call for an additional NetScaler of the identical platform and model.

**Note:** The Citrix NetScaler data sheet typically represents throughput capabilities under optimal conditions for performance. However, performance is directly affected by security requirements. For example, if the RC4 encryption algorithm and a 1k key length are used, a VPX platform may be able to handle more than 500 HDX proxy connections. However, if a 3DES encryption algorithm and 2k key length are used (which are becoming more common), the throughput may be halved.

### Decision: Pre-Authentication Policy

An optional pre-authentication policy can be applied to user groups with NetScaler Gateway as their authentication point. Pre-authentication policies limit access to the environment based on whether the endpoint meets certain criteria through Endpoint Analysis (EPA) Scans.

Pre-authentication access policies can be configured to test antivirus, firewall, operating system, or even registry settings. These policies can be used to prevent access entirely or can be used by XenDesktop to control session features such as clipboard mapping, printer mapping and even the availability of specific applications and desktops. For example, if a user device does not have antivirus installed, a filter can be set to hide sensitive applications.

The following figure provides an overview of how multiple policies can be used to customize the features of a virtualization resource:

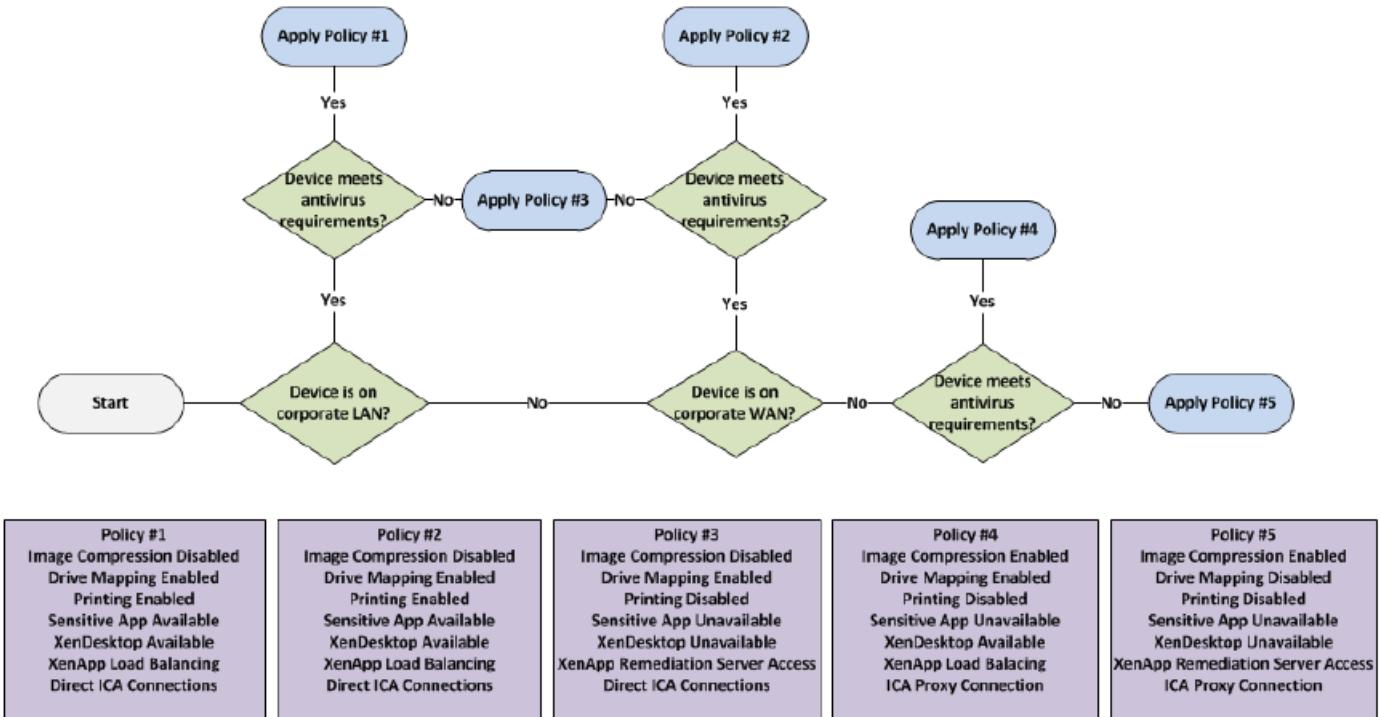


Figure 7: Simplified SmartAccess Decision Logic

### Experience from the Field

**Retail** – A small private retail company use EPA to scan for the presence of updated antivirus definitions prior to allowing access.

**Financial** – A medium financial enterprise use EPA scans of the Domain SID to verify that users are members of the enterprise domain prior to allowing access.

**Government** – A large federal institution use EPA to scan endpoint devices to ensure that a specific certificate (or set of certificates) has been installed on the device prior to allowing access.

### Decision: Session Policy

User groups with NetScaler Gateway as their authentication point must have corresponding session policies defined. Session policies are used to define the overall user experience post-authentication.

Organizations create sessions policies based on the type of Citrix Receiver used. For the purpose of session policy assignment, devices are commonly grouped as either non-mobile (such as Windows, Mac and Linux OS based), or mobile (such as iOS or Android). Therefore a decision on whether to provide support for mobile devices, non-mobile devices, or both should be made based on client device requirements identified during the assess phase.

To identify devices session policies, include expressions such as ([Configuring Session Policies and Profiles for App Controller and StoreFront](#)):

- **Mobile devices** - The expression is set to REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver which is given a higher priority than the non-mobile device policy to ensure mobile devices are matched while non-mobile devices are not.
- **Non-mobile devices** – The expression is set to ns\_true which signifies that it should apply to all traffic that is sent to it.

An alternative use of session policies is to apply endpoint analysis expressions. These session policies are applied post

authentication yet mimic the previously mentioned pre-authentication policies. Use of session policies is an option to provide a fallback scenario to endpoints that do not meet full security requirements such read-only access to specific applications.

## Decision: Session Profile

Each session policy must have a corresponding session profile defined. The session profile defines details required for the user group to gain access to the environment. There are two primary forms of session profiles that determine the access method to the virtual desktop environment:

- **SSLVPN** - Users create a virtual private network and tunnel all traffic configured by IP addresses through the internal network. The user's client device is able to access permitted intranet resources as if it were on the internal network. This includes XenDesktop sites and any other internal traffic such as file shares or intranet websites. This is considered a potentially less secure access method since network ports and routes to services outside of the virtual desktop infrastructure may be opened leaving the enterprise susceptible to risks that may come with full VPN access. These risks may include denial of service attacks, attempts at hacking internal servers, or any other form of malicious activity that may be launched from malware, trojan horses, or other viruses via an Internet based client against vulnerable enterprise services via routes and ports.

Another decision to consider when SSLVPN is required is whether to enable split tunneling for client network traffic. By enabling split tunneling, client network traffic directed to the intranet by Citrix Receiver may be limited to routes and ports associated with specific services. By disabling split tunneling, all client network traffic is directed to the intranet, therefore both traffic destined for internal services as well as traffic destined for the external services (Internet) traverses the corporate network. The advantage of enabling split tunneling is that exposure of the corporate network is limited and network bandwidth is conserved. The advantage of disabling split tunneling is that client traffic may be monitored or controlled through systems such as web filters or intrusion detection systems.

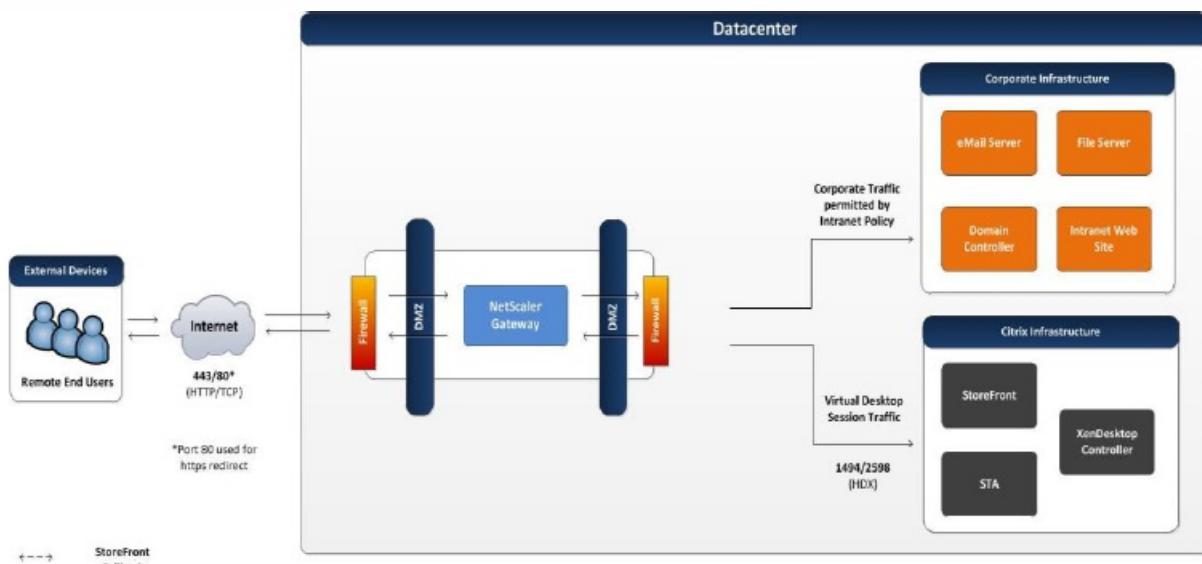


Figure 8: SSL VPN

- **HDX proxy** - With HDX Proxy, users connect to their virtual desktops and applications through the NetScaler Gateway without exposing internal addresses externally. In this configuration, the NetScaler Gateway acts as a micro VPN and only handles HDX traffic. Other types of traffic on the client's endpoint device, such as private mail or personal Internet traffic do not use the NetScaler Gateway.

Based on the endpoint and Citrix Receiver used, a decision must be made as to whether this method is supported for each user group. HDX Proxy is considered a secure access method for remote virtual desktop access since only traffic specific to the desktop session is allowed to pass through to the corporate infrastructure. Most Citrix Receivers support HDX Proxy and it is the preferred method:

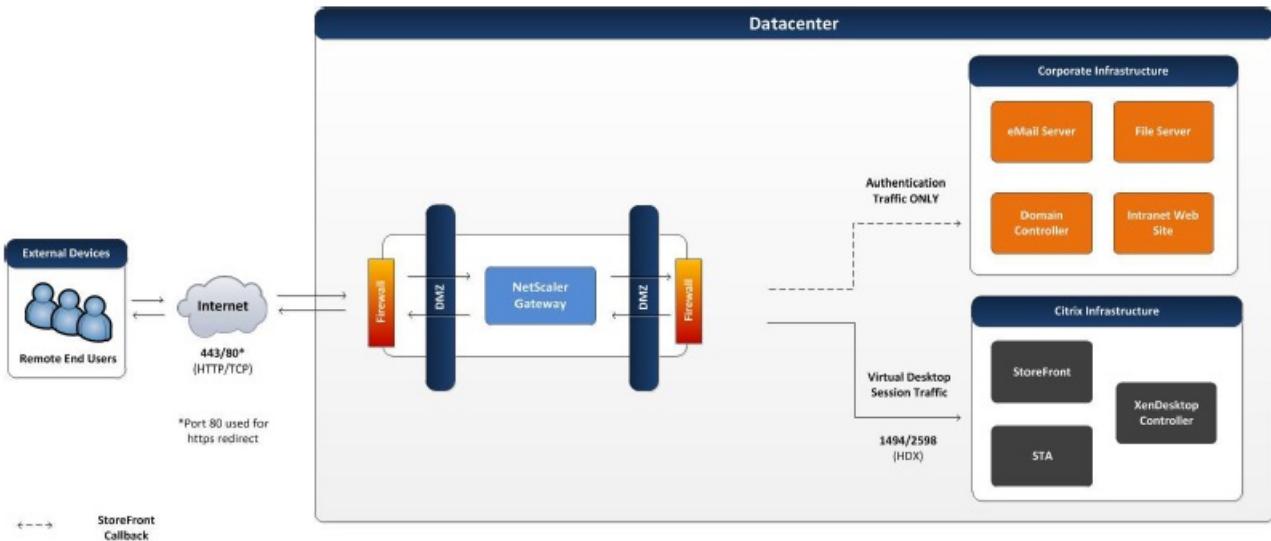


Figure 9: HDX Proxy

#### Decision: Preferred Datacenter

Enterprises often have multiple active datacenters providing high availability for mission critical applications. Some virtual desktops or applications may fall into that category while others may only be accessed from a specific preferred datacenter. Therefore, the initial NetScaler Gateway that a user authenticates to in a multi-active datacenter environment may not be within the preferred datacenter corresponding to the user's VDI resources. StoreFront is able to determine the location of the user's assigned resources and direct the HDX session to those resources; however, the resulting path may be sub-optimal (WAN connection from the NetScaler Gateway to the virtual desktop/application resources as opposed to LAN connection).

There are static and dynamic methods available to direct HDX sessions to their virtual desktop resources in their primary datacenter. The decision regarding which method to select should be based on the availability of technology to dynamically assign sites links such as Global Server Load Balancing (GSLB) along with the network assessment of intranet and Internet bandwidth as well as Quality of Service (QoS) capabilities.

**Note:** For more information on configuring the static and dynamic methods of GSLB, please refer to Citrix Product Documentation - [Configuring GSLB for Proximity](#).

- **Static**

- **Direct** - The user can be given a FQDN mapped to an A record that is dedicated to the primary datacenter NetScaler Gateway(s) allowing them to access their virtual desktop directly wherever they are in the world. This approach eliminates a layer of complexity added with dynamic allocation. However, it also eliminates fault tolerance options such as the ability to access the virtual desktop through an alternative intranet path when a primary datacenter outage is limited to the access infrastructure.

- **Dynamic**

- **Intranet** - For most dynamic environments, the initial datacenter selected for authentication is the one closest to the user. Protocols such as GSLB dynamic proximity calculate the least latency between the user's local DNS server and the NetScaler Gateway. Thereafter, by default, the HDX session is routed through the same NetScaler Gateway to whichever datacenter is hosting the user's virtual desktops and applications. The advantage of this approach is that the majority of the HDX session would traverse the corporate WAN where quality of service may be used.

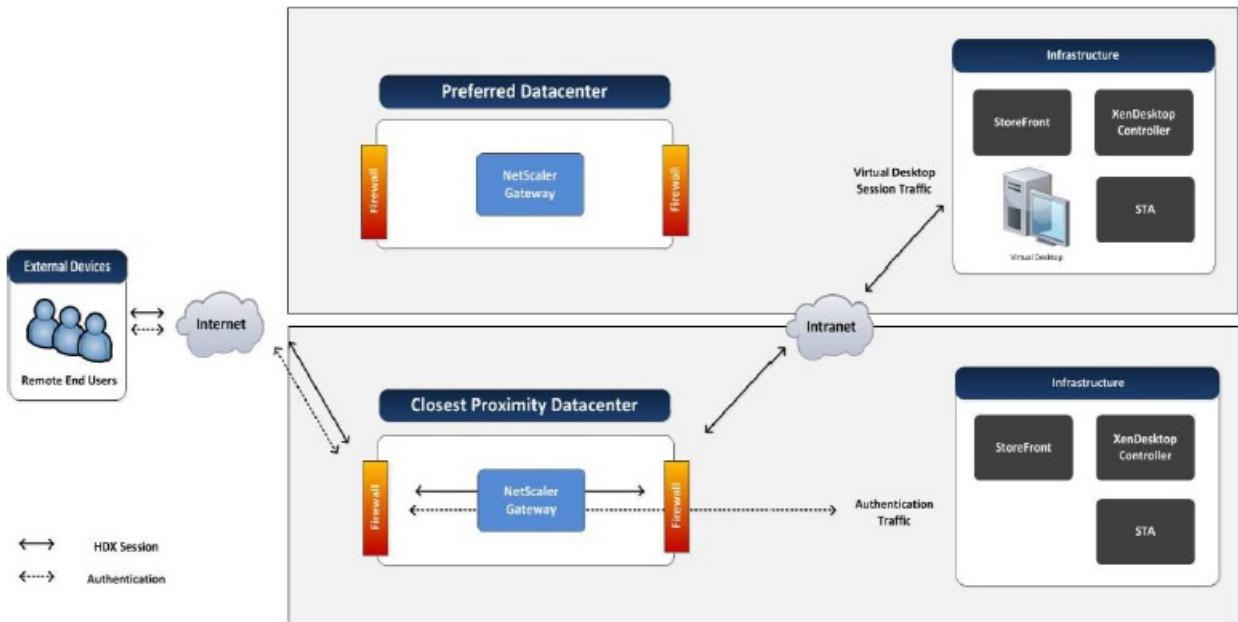


Figure 10: Intranet Connection

- **Internet** - Alternatively, the HDX session can be re-routed through an alternate NetScaler Gateway proximate to the backend VDI desktop / XenApp server, resulting in most of the HDX session travelling over the Internet. For example, a user with a dedicated desktop in the United States, traveling in Europe may be directed to a NetScaler Gateway hosted in a European datacenter based on proximity. However, when the user launches their desktop, an HDX connection will be established to the virtual desktop via a NetScaler Gateway hosted in the preferred datacenter in the United States.

This conserves WAN network usage (at the cost of QoS) and is recommended in cases where the user's Internet connection may provide a more reliable experience than the corporate WAN.

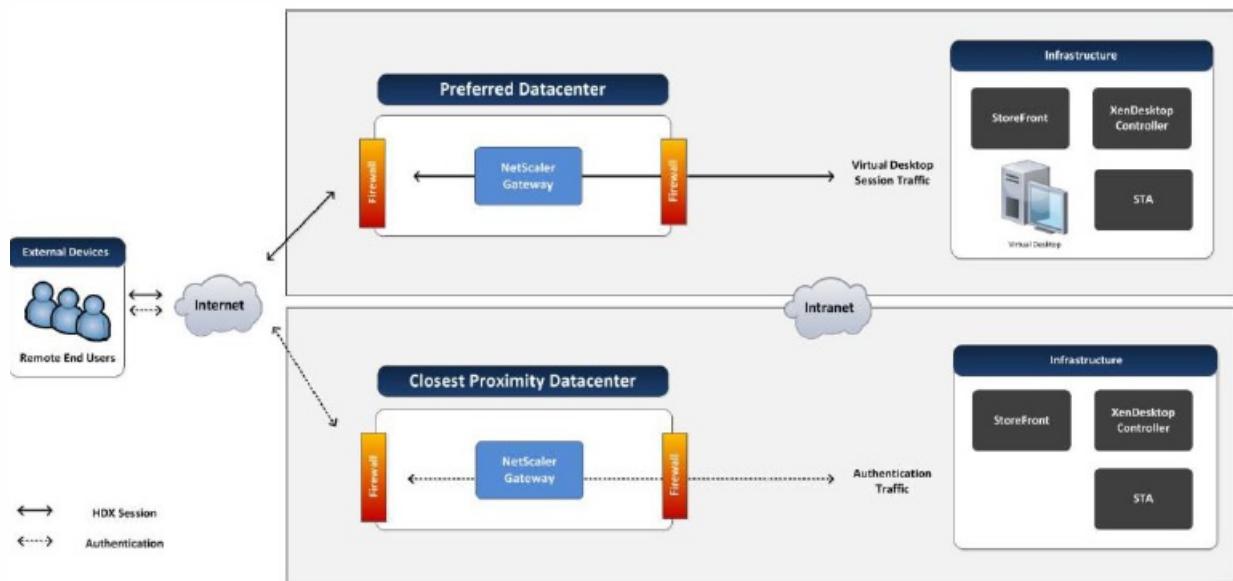


Figure 11: Internet Connection

Some customers will use a combination of these methods, such as geo-specific dynamic URLs such that fault tolerance is provided within a geographic area (such as North America) without incurring the complexity of global GSLB.

### Layer 3: The Resource Layer

The resource layer is the third layer of the design methodology and the final layer focused specifically on the user groups.

The overall user acceptance of the solution is defined by the decisions made within the resource layer. Profiles, printing, applications and overall desktop image design play a pivotal role in how well the desktop is aligned with the user group's requirements, which were identified within the assess phase.

## User Profiles

A user's profile plays a critical role in delivering a consistently positive experience within a virtual desktop or virtual application scenario. Even a well-designed virtual desktop solution can fail if users are frustrated due to lengthy logon times or lost settings.

The user profile solution chosen must align with the personalization characteristics of the user group captured during the assess phase as well as the VDI model selected.

### Decision: Profile Type

This section provides an overview on the different profile types available and provides guidance on the optimal user profile for each VDI model.

- **Local profiles** - Local profiles are stored on each server or desktop operating system and are initially created based on the default user profile. Therefore, a user accessing these resources would create an independent profile on each system. Users are able to retain changes to their local profile on each individual system, but changes are only accessible for future sessions on that system. Local profiles require no configuration; if a user logging into a server or desktop operating system does not have a profile path administratively defined, a local profile is created by default.
- **Roaming profiles** - Roaming profiles are stored in a centralized network repository for each user. Roaming profiles differ from local profiles in that the information in the profile (whether it is a printer, a registry setting, or a file stored in the documents folder) can be made available to user sessions accessed from all systems in the environment. Configuring a user for a roaming profile requires an administrator to designate the user's profile path (for virtual desktops) or terminal server profile path to a particular network share. The first time the user logs on to a server or desktop operating system, the default user profile is used to create the user's roaming profile. During logoff, the profile is copied to the administrator-specified network location.
- **Mandatory profiles** - Mandatory profiles are typically stored in a central location for many users. However, the user's changes are not retained at logoff. Configuring a user for a mandatory profile requires an administrator to create a mandatory profile file (NTUSER.MAN) from an existing roaming or local profile and assign users' with a terminal services profile path. This can be achieved by means of Microsoft Group Policy, customizing the user properties in Active Directory or Citrix Profile Management.
- **Hybrid profiles** - Hybrid profiles combine a robust profile core (a mandatory profile or a local default profile) with user specific registry keys or files that are merged during logon. This technique enables administrators to tightly control which changes are retained and to keep the user profiles small in size. Furthermore, hybrid profiles address the last write wins issue using mature queuing techniques that automatically detect and prevent simultaneous writes that could potentially overwrite changes made in another session. Thus minimizing, user frustration resulting from lost profile changes when accessing multiple servers or virtual desktops simultaneously. In addition, they capture and record only the changes within the profile, rather than writing the entire profile at logoff. A good example of a hybrid profile solution is Citrix Profile Management, which will be discussed in detail within this chapter.

The following table compares the capabilities of each profile type:

In order to select the optimal profile type for each user group, it is important to understand their personalization requirements in addition to the FlexCast model assigned.

The following table provides recommendations on selecting the appropriate user profile type based on VDI resource:

	Local	Roaming	Mandatory	Hybrid
<b>User setting persistence required (personalization characteristic: basic / complete)</b>				
Hosted Windows App	✗	✓	✗	✓
Hosted Browser App	✗	✓	✗	✓
Hosted Shared Desktop	✗	✓	✗	✓
Hosted Pooled Desktop	✗	✓	✗	✓
Hosted Personal Desktop	◦	✓	✗	✓
Hosted Pro Graphics Desktop	◦	✓	✗	✓
Local Streamed Desktop	✗	✓	✗	✓
Local VM Desktop	✓	◦	✗	◦
Remote PC Access	✓	◦	✗	◦
<b>User setting persistence <u>not</u> required or <u>not</u> desired (personalization characteristic: none)</b>				
Hosted Windows App	✗	✗	✓	✗
Hosted Browser App	✗	✗	✓	✗
Hosted Shared Desktop	✗	✗	✓	✗
Hosted Pooled Desktop	✓	✗	✓	✗
Hosted Personal Desktop	✗	✗	✓	✗
Hosted Pro Graphics Desktop	◦	✗	✓	✗
Local Streamed Desktop	✓	✗	✓	✗
Local VM Desktop	◦	✗	✓	✗
Remote PC Access	◦	✗	✓	✗

"✓": Recommended "◦": Viable "✗": Not Recommended

Table 20: Profile Type Selection

### Decision: Folder Redirection

Redirecting special folders can supplement any of the described profile types. While redirecting profile folders, such as user documents and favorites, to a network share is a good practice to minimize profile size, architects need to be aware that applications may frequently read and write data to profile folders such as AppData, causing potential issues with file server utilization and responsiveness. It is important to thoroughly test profile redirection before implementation in production to avoid these issues. Therefore, it is important to research profile read / write activities and to perform a pilot before moving to production. Microsoft Outlook is an example of an application that regularly performs profile read activities, as the user signature is read from the user profile every time an email is created.

The following table provides general recommendations to help identify the appropriate folders to redirect:

Folder	Local	Roaming	Mandatory	Hybrid
Application Data	✗	○	✗	○
Contacts	✗	✓	✗	○
Desktop	✗	✓	✗	○
Downloads	✗	○	✗	○
Favorites	○	✓	○	✓
Links	✗	✓	✗	○
My Documents	○	✓	○	✓
My Music	○	✓	○	○
My Pictures	○	✓	○	○
My Videos	○	✓	○	○
Saved Games	✗	○	✗	○
Searches	✗	✓	✗	○
Start Menu	✗	✗	✗	✗

"✓": Recommended "○": Optional "✗": Not recommended

Table 21: Folder Redirection Matrix

### Decision: Folder Exclusion

Excluding folders from being persistently stored as part of a roaming or hybrid profile can help to reduce profile size and logon times. By default Windows excludes the AppData\Local and AppData\LocalLow folders, including all subfolders, such as History, Temp and Temporary Internet Files. In addition, the downloads and saved games folders should also be excluded. All folders that are redirected should be excluded from the profile solution.

### Decision: Profile Caching

Local caching of roaming or hybrid user profiles on a server or virtual desktop is default Windows behavior and can reduce login times and file server utilization / network traffic. With profile caching, the system only has to download changes made to the profile. The downside of profile caching is that it can consume significant amounts of local disk storage on multi-user systems, such as a hosted shared desktop hosts.

In certain VDI models and configurations, the VDI resource is reset to a pristine state. Having locally cached profiles be deleted upon logoff is an unnecessary consumption of resources. Based on this, the leading recommendation is to not deleting locally cached profiles for the following VDI models:

- Hosted Personal Desktops
- Hosted Pooled Desktops - only in situations where a reboot occurs after logoff.
- Local VM Desktops
- Remote PC Access

Configuring the “Delay before deleting cached profiles” Citrix policy sets an optional extension to the delay before locally cached profiles are deleted at logoff. Extending the delay is useful if a process keeps files or the user registry hive open during logoff. This can also reduce logoff times for large profiles.

### Decision: Profile Permissions

For security reasons, administrators, by default, cannot access user profiles. While this level of security may be required for organizations that deal with very sensitive data, it is unnecessary for most environments and can complicate operations and maintenance. Therefore, consider enabling the “Add the Administrators security group to roaming user profiles” policy

setting. The configuration of this policy should be aligned with the security characteristics of the user groups captured during the assess phase. For more information on the permissions required for the file share hosting user profiles and data, please refer to Microsoft TechNet - Deploying Roaming Profiles.

## Decision: Profile Path

Determining the network path for the user profiles is one of the most significant decisions during a user profile design process. In general it is strongly recommended to leverage a redundant and high performance file server or NAS device.

There are four topics that must be considered for the profile share:

- **Performance** - File server performance will affect logon and logoff times, and depending on other decisions such as redirected folders and profile streaming, can impact the user's experience within the session. For large virtual desktop infrastructures, a single file server cluster may not be sufficient to handle periods of peak activity. In order to distribute the load across multiple file servers, the file server address and share name will need to be adjusted.
- **Location** - User profiles are transferred over the network by means of the SMB protocol, which does not perform well on high-latency network connections. Furthermore, WAN connections are typically bandwidth constrained, which can add additional delay to the profile load process. Therefore, the file server should be located in close proximity to the servers and virtual desktops to minimize logon times.
- **Operating system platforms** - User profiles have a tight integration with the underlying operating system and it is not supported to reuse a single user profile on different operating systems or different platforms like 64-Bit (x64) and 32-Bit (x86). For more information, please refer to the Microsoft knowledge base article KB2384951 – Sharing 32 and 64-bit User Profiles. Windows 2008 and Windows Vista introduced a new user profile structure, which can be identified by .V2 profile directory suffix, which makes older user profiles incompatible with newer operating systems such as Windows 2012, 7 and 8. In order to ensure that a separate profile is used per platform, the profile directory has to be adapted.
- **Indexing capabilities** - To take full advantage of Windows Search functionality on a user's redirected data, Windows file servers that index the user's data must be used, as opposed to a share on a NAS appliance. This is important for use cases that are heavily dependent on Windows Search or are especially sensitive to perception of slowness or latency.

There are two methods that can be used to address these challenges that are based on Windows built-in technology:

- **User object** - For every user object in Active Directory, an individual profile path, which contains file server name and profile directory, can be specified. Since only a single profile path can be specified per user object, it is not possible to ensure that a separate profile is loaded for each operating system platform.
- **Computer group policy or system variables** - The user profile path can also be configured by means of computer specific group policies or system variables. This enables administrators to ensure that a user profile is dedicated to the platform. Since computer specific configurations affect all users of a system, all user profiles will be written to the same file server. To load balance user profiles across multiple servers dedicated XenDesktop delivery groups have to be created per file server.

**Note:** Microsoft does not support DFS-N combined with DFS-R for actively used user profiles. For more information, please refer to the Microsoft articles:

- [Information about Microsoft support policy for a DFS-R and DFS-N deployment scenario](#)
- [Microsoft's Support Statement Around Replicated User Profile Data](#)

When using Citrix Profile Management, a third option is available to address these challenges:

- **User object attributes and variables** - Citrix Profile Management enables the administrator to configure the profile path by means of a computer group policy using attributes of the user object in Active Directory to specify the file server

dynamically. In order to achieve this, three steps are required:

1. Create a DNS alias (for example, fileserver1) that refers to the actual file server
2. Populate an empty LDAP attribute of the user object (for example, L or UID) with the DNS Alias
3. Configure Citrix Profile Management by means of GPO to use a profile path that refers to the LDAP attribute (for example, If attribute UID is used the profile path becomes \\#UID#\Profiles\profiledirectory)

In addition, Citrix Profile Management automatically populates variables to specify the profile path dynamically based on the operating system platform. Valid profile management variables are:

- **!CTX\_PROFILEVER!** - Expands to v1 or v2 depending on the profile version.
- **!CTX\_OSBITNESS!** - Expands to x86 or x64 depending on the bit-level of the operating system.
- **!CTX\_OSNAME!** - Expands to the short name of the operating system, for example Win7

By combining both capabilities of Citrix Profile Management, a fully dynamic user profile path can be created, which can be load balanced across multiple file servers and ensure profiles of different operating system platforms are not mixed. An example of a fully dynamic user profile path is shown below:

\\#UID#\profiles\$\%USERNAME%.%USERDOMAIN%\!CTX\_OSNAME!CTX\_OSBITNESS!

### Decision: Profile Streaming

**Note:** The following design decision only applies to those environments that use Citrix Profile Management.

With user profile streaming, files and folders contained in a profile are fetched from the user store (file server) to the local computer when a user accesses them. During the logon process, Citrix Profile Management immediately reports that the profile load process has completed reducing profile load time to almost zero.

Citrix recommends enabling profile streaming for all scenarios. If it is desired to keep a local cached copy of the user profile for performance reasons, it is recommended to enable the “Always Cache” setting and configure a size of 0. This ensures that the user profile is downloaded in the background and enables the system to use this cached copy going forward.

**Note:** Profile streaming is not required and does not work with the personal vDisk feature of Citrix XenDesktop. Even if explicitly enabled by means of Group Policy, the profile streaming setting is automatically disabled.

#### Experience from the Field

**General –** Some poorly written applications might load faster if their AppData has already been streamed to the VDI resource. Enabling the “Always Cache” option for profile streaming can help improve performance when the AppData folder is not redirected.

### Decision: Active Write Back

**Note:** The following design decision only applies to those environments that use Citrix Profile Management.

By enabling the active write back feature, Citrix Profile Manager detects when an application has written and closed a file and copies the file back to the network copy of the profile during idle periods. In scenarios where a single user leverages multiple virtual desktops or hosted shared desktops simultaneously, this feature can be tremendously beneficial. However, Citrix Profile Management does not copy any registry changes back to the network, except during an ordered logoff. As such, there is a risk that the registry and files may get out of alignment on non-persistent systems, where locally cached profile information is wiped upon reboot. Therefore, it is recommended to disable active write back functionality for non-persistent scenarios.

## **Decision: Configuration Approach**

**Note:** The following design decision only applies to those environments that use Citrix Profile Management.

Citrix Profile Management can be configured by means of an “.ini” file, Microsoft Group Policy and Citrix Policy (Citrix Profile Management 5.0 and newer). While each option offers the same configuration settings, Group Policy is recommended because it allows administrators to perform Windows and Citrix profile configurations from a single point, minimizing the tools necessary for profile management.

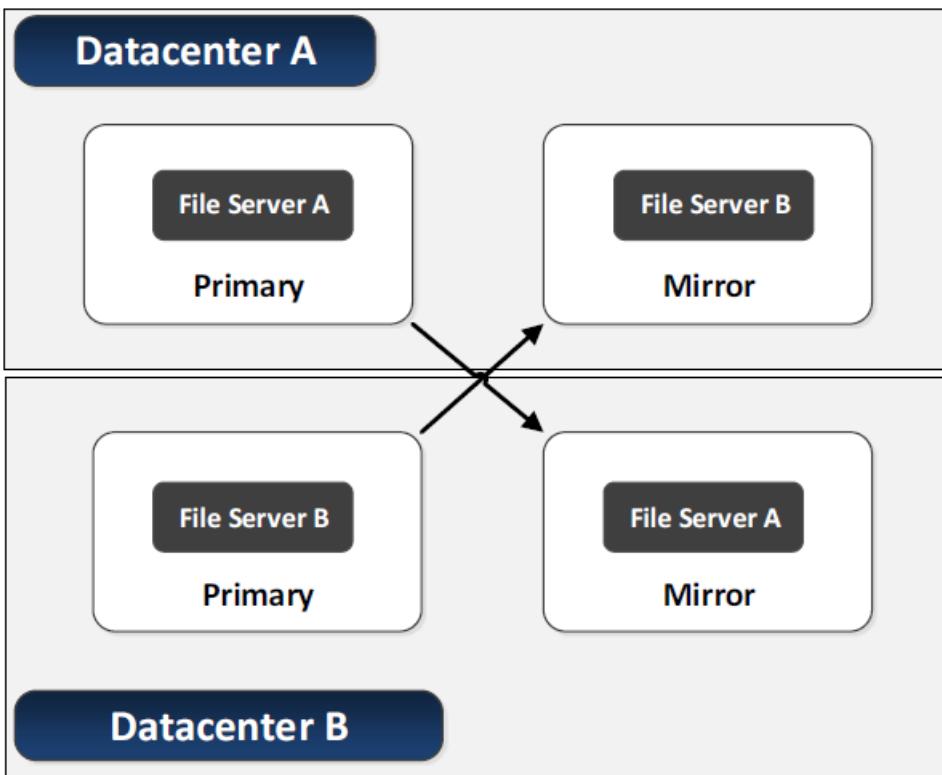
**Note:** With Citrix Profile Management 5.0 and newer, the desktop type is automatically detected and Citrix Profile Management policies set accordingly. For more information, please refer to Citrix eDocs – How automatic configuration works.

## **Decision: Replication**

While having an active/active datacenter on a network level is easily accomplished with GSLB, the replication of user data makes having a fully active/active deployment complex in most situations. To have an active/active configuration where users are not statically assigned to a specific datacenter, will require users to have no form of personalization requirements. This will limit the user’s ability to make any configuration changes and will not allow them to create any documents or persistent data. The exception to this is when a high-speed low latency connection such as dark fibre is available between datacenters. This will let resources in both locations point to the same file server allowing for a true active/active solution. Also, an active/active configuration can be accomplished when applications are used that rely solely on a backend database that is actively replicated between datacenters and do not store any data in the user profile.

For redundancy and failover purposes, user data such as Windows profiles and documents should be synchronized between datacenters. Although it is recommended to replicate user data between datacenters, the replication would be an active/passive configuration. This means the data can only be actively consumed from a single datacenter. The reason for this limitation is the distributed file locking method inside Windows that only allows a single user to actively write to a file. Therefore, active/active replication of user data is not supported. Any supported configuration consists of a one-way replication of data that is active in a single datacenter at any point in time.

For example, the figure below describes a scenario where user data is passively replicated from Datacenter A to Datacenter B. In this example, File Server A is the primary location for user data in Datacenter A and File Server B is the primary location in Datacenter B. One-way replication of the user data occurs for each fileserver to allow for the user data to be available in the opposite datacenter if a failover occurs. Replication technologies such as Microsoft DFS can be configured to mirror user profiles and documents to a file server in another datacenter. DFS Namespaces can also be used to have a seamless path for the location of the user data. However, implementing a replication solution like this requires an administrator familiar with Microsoft DFS and user profiles.



## Policies

Policies provide the basis to configure and fine tune XenApp and XenDesktop environments, allowing organizations to control connection, security and bandwidth settings based on various combinations of users, devices or connection types.

When making policy decisions it is important to consider both Microsoft and Citrix policies to ensure that all user experience, security and optimization settings are considered. For a list of all Citrix-related policies, please refer to the Citrix Policy Settings Reference.

### **Decision: Preferred Policy Engine**

Organizations have the option to configure Citrix policies via Citrix Studio or through Active Directory group policy using Citrix ADMX files, which extend group policy and provide advanced filtering mechanisms.

Using Active Directory group policy allows organizations to manage both Windows policies and Citrix policies in the same location, and minimizes the administrative tools required for policy management. Group policies are automatically replicated across domain controllers, protecting the information and simplifying policy application.

Citrix administrative consoles should be used if Citrix administrators do not have access to Active Directory policies. Architects should select one of the above two methods as appropriate for their organization's needs and use that method consistently to avoid confusion with multiple Citrix policy locations.

It is important to understand how the aggregation of policies, known as policy precedence flows in order to understand how a resultant set of policies is created. With Active Directory and Citrix policies, the precedence is as follows:

Policy Precedence	Policy Type
Processed first (lowest precedence)	Local server policies
Processed second	Citrix policies created using the Citrix administrative consoles
Processed third	Site level AD policies
Processed fourth	Domain level AD policies
Processed fifth	Highest level OU in domain
Processed sixth and subsequent	Next level OU in domain
Processed last (highest precedence)	Lowest level OU containing object

Table 22: Policy Precedence

Policies from each level are aggregated into a final policy that is applied to the user or computer. In most enterprise deployments, Citrix administrators do not have rights to change policies outside their specific OUs, which will typically be the highest level for precedence. In cases where exceptions are required, the application of policy settings from higher up the OU tree can be managed using “block inheritance” and “no override” settings. Block inheritance stops settings from higher-level OUs (lower precedence) from being incorporated into the policy. However, if a higher-level OU policy is configured with no override, the block inheritance setting will not be applied. Given this, care must be taken in policy planning, and available tools such as the “Active Directory Resultant Set of Policy” tool or the “Citrix Group Policy Modeling” wizard should be used to validate the observed outcomes with the expected outcomes.

**Note:** Some Citrix policy settings, if used, need to be configured through Active Directory group policy, such as Controllers and Controller registration port, as these settings are required for VDAs to register.

### Decision: Policy Integration

When configuring policies, organizations often require both Active Directory policies and Citrix policies to create a completely configured environment. With the use of both policy sets, the resultant set of policies can become confusing to determine. In some cases, particularly with respect to Windows Remote Desktop Services (RDS) and Citrix policies, similar functionality can be configured in two different locations. For example, it is possible to enable client drive mapping in a Citrix policy and disable client drive mapping in a RDS policy. The ability to use the desired feature may be dependent upon the combination of RDS and Citrix policy. It is important to understand that Citrix policies build upon functionality available in Remote Desktop Services. If the required feature is explicitly disabled in RDS policy, Citrix policy will not be able to affect a configuration as the underlying functionality has been disabled.

In order to avoid this confusion, it is recommended that RDS policies only be configured where required and there is no corresponding policy in the XenApp and XenDesktop configuration, or the configuration is specifically needed for RDS use within the organization. Configuring policies at the highest common denominator will simplify the process of understanding resultant set of policies and troubleshooting policy configurations.

### Decision: Policy Scope

Once policies have been created, they need to be applied to groups of users and/or computers based on the required outcome. Policy filtering provides the ability to apply policies against the requisite user or computer groups. With Active Directory based policies, a key decision is whether to apply a policy to computers or users within site, domain or organizational unit (OU) objects. Active Directory policies are broken down into user configuration and computer configuration. By default, the settings within the user configuration apply to users who reside within the OU at logon, and

settings within the computer configuration are applied to the computer at system startup, and will affect all users who logon to the system. One challenge of policy association with Active Directory and Citrix deployments revolves around three core areas:

- **Citrix environment specific computer policies** - Citrix servers and virtual desktops often have computer policies that are created and deployed specifically for the environment. Applying these policies is easily accomplished by creating separate OU structures for the servers and the virtual desktops. Specific policies can then be created and confidently applied to only the computers within the OU and below and nothing else. Based upon requirements, virtual desktops and servers may be further subdivided within the OU structure based on server roles, geographical locations or business units.
- **Citrix specific user policies** -- When creating policies for XenApp and XenDesktop there are a number of policies specific to user experience and security that are applied based on the user's connection. However, the user's account could be located anywhere within the Active Directory structure, creating difficulty with simply applying user configuration based policies. It is not desirable to apply the Citrix specific configurations at the domain level as the settings would be applied to every system any user logs on to. Simply applying the user configuration settings at the OU where the Citrix servers or virtual desktops are located will also not work, as the user accounts are not located within that OU. The solution is to apply a loopback policy, which is a computer configuration policy that forces the computer to apply the assigned user configuration policy of the OU to any user who logs onto the server or virtual desktop, regardless of the user's location within Active Directory. Loopback processing can be applied with either merge or replace settings. Using replace overwrites the entire user GPO with the policy from the Citrix server or virtual desktop OU. Merge will combine the user GPO with the GPO from the Citrix server or desktop OU. As the computer GPOs are processed after the user GPOs when merge is used, the Citrix related OU settings will have precedence and be applied in the event of a conflict. For more information, please refer to the Microsoft TechNet article - [Understand User Group Policy Loopback Mode](#).
- **Active Directory policy filtering** - In more advanced cases, there may be a need to apply a policy setting to a small subset of users such as Citrix administrators. In this case, loopback processing will not work, as the policy should only be applied to a subset of users, not all users who logon to the system. Active Directory policy filtering can be used to specify specific users or groups of users to which the policy is applied. A policy can be created for a specific function, and then a policy filter can be set to apply that policy only to a group of users such as Citrix administrators. Policy filtering is accomplished using the security properties of each target policy.

Citrix policies created using Citrix Studio have specific filter settings available, which may be used to address policy-filtering situations that cannot be handled using group policy. Citrix policies may be applied using any combination of the following filters:

Filter Name	Filter Description	Scope
Access control	Applies a policy based on access control conditions through which a client is connecting. For example, users connecting through a Citrix NetScaler Gateway can have specific policies applied.	User settings
Citrix CloudBridge	Applies a policy based on whether or not a user session was launched through Citrix CloudBridge.	User settings
Client IP address	Applies a policy based on the IPv4 or IPv6 address of the user device used to connect the session. Care must be taken with this filter if IPv4 address ranges are used in order to avoid unexpected results.	User settings
Client name	Applies a policy based on the name of the user device used to connect the session.	User settings
Delivery group	Applies a policy based on the delivery group membership of the desktop running the session	User and computer settings
Delivery group type	Applies a policy based on the type of machine running the session. For example, different policies can be set depending upon whether a desktop is pooled, dedicated or streamed.	User and computer settings
Organizational unit	Applies a policy based on the OU of the desktop or server running the session.	User and computer settings
Tag	Applies a policy based on any tags applying to the desktop running the session. Tags are strings that can be added to virtual desktops in XenDesktop environments that can be used to search for or limit access to desktops.	User and computer settings
User or group	Applies a policy based on the Active Directory group membership of the user connecting to the session.	User settings

Table 23: Citrix Policy Filters

**Note:** Citrix policies in XenDesktop 7.x provide a merged view of settings that apply at the user and computer level. In table 24, the Scope column identifies whether the specified filter applies to user settings, computer settings, or both.

### Decision: Baseline Policy

A baseline policy should contain all common elements required to deliver a high-definition experience to the majority of users within the organization. A baseline policy creates the foundation for user access, and any exceptions that may need to be created to address specific access requirements for groups of users. It should be comprehensive to cover as many use cases as possible and should have the lowest priority, for example 99 (a priority number of “1” is the highest priority), in order to create the simplest policy structure possible and avoid difficulties in determining the resultant set of policies. The unfiltered policy set provided by Citrix as the default policy may be used to create the baseline policy as it is applied to all users and connections. In the baseline configuration, all Citrix policy settings should be enabled, even those that will be configured with the default value, in order to explicitly define desired/expected behavior, and to avoid confusion should default settings change over time.

Citrix Policy templates can be used to configure Citrix policies to effectively manage the end-user experience within an environment and can serve as an initial starting point for a baseline policy. Templates consist of pre-configured settings that optimize performance for specific environments or network conditions. The built-in templates included in XenDesktop are shown below:

Built-in Templates	
High definition user experience	Includes settings for providing high quality audio, graphics, and video to users.
High server scalability	Includes settings for providing an optimized user experience while hosting more users on a single server.
Optimized bandwidth for WAN	Includes settings for providing an optimized experience to users with low bandwidth or high latency connections.
Security and control	Includes settings for disabling access to peripheral devices, drive mapping, port redirection, and Flash acceleration on user devices.

Table 24: XenDesktop 7 Built-in Policy Templates

For more information on Citrix policy templates, please refer to Citrix eDocs - Manage Citrix Policy Templates.

A baseline policy configuration should also include Windows policies. Windows policies reflect user specific settings that optimize the user experience and remove features that are not required or desired in a XenDesktop environment. For example, one common feature turned off in these environments is Windows update. In virtualized environments, particularly where desktops and servers may be streamed and non-persistent, Windows update creates processing and network overhead, and changes made by the update process will not persist a restart of the virtual desktop or application server. Also in many cases, organizations use Windows software update service (WSUS) to control Windows updates. In these cases, updates are applied to the master disk and made available by the IT department on a scheduled basis.

In addition to the above considerations, an organization's final baseline policy may include settings specifically created to address security requirements, common network conditions, or to manage user device or user profile requirements:

## Printing

Citrix XenApp and Citrix XenDesktop support a variety of different printing solutions. In order to plan and successfully implement the proper printing solution it is important to understand the available technologies as well as their benefits and limitations.

### Decision: Printer Provisioning

The process of creating printers at the start of a XenApp or XenDesktop session is called printer provisioning. There are multiple approaches available:

- **User Added** - Allowing users to manually add printers gives them the flexibility to select printers by convenience. The drawback to manually adding network-based printers is that it requires the users to know the network name or path of the printers. There is also a chance that the native print driver is not installed in the operating system and the Citrix Universal Print Driver is not compatible, thereby requiring the user to seek administrative assistance. Manually adding printers is best suited in the following situations:
  - Users roam between different locations using the same client device (i.e. laptop, tablet).
  - Users work at assigned stations or areas whose printer assignments will rarely change.
  - Users have personal desktops with sufficient rights to install necessary printer drivers.
- **Auto Created** - Auto-creation is a form of dynamic provisioning that attempts to create some or all of the available printers on the client device at the start of a user session. This includes locally attached printers as well as network-based printers. Auto-creating all client printers can increase the session logon time as each printer is enumerated during the logon process.
- **Session-Based** - Session printers are a set of network-based printers assigned to users through a Citrix policy at the start of each session.

- Proximity Based: Session printers filtered by IP subnet. The network printers created under this policy may vary based on where the user's endpoint device is located. Proximity printing is recommended in situations where: Users roam between different locations using the same endpoint device (i.e. laptop, tablet) and where thin clients are used, which do not have the ability to connect to network-based printers directly.
- Session printers can be assigned using the "Session Printer" policy or the "Printer Assignments" policy. The "Session printer" policy is intended to be used to set default printers for a farm, site, large group, or OU. The "Printer Assignments" policy is used to assign a large group of printers to multiple users. If both policies are enabled and configured, the session printers will be merged into a single list.
- **Universal Printer** - The Citrix Universal Printer is a generic printer object that is auto-created at the start of a session and is not linked to a printing device. When using the Citrix Universal Printer it is not required to enumerate the available client printers during logon, which can greatly reduce resource usage and decrease user logon times. By default the Citrix Universal Printer will print to the client's default printer, however the behavior can be modified to allow the user to select any of their compatible local or network-based printers.

The Citrix Universal Printer is best suited for the following scenarios:

- The user requires access to multiple printers both local and network-based which may vary with each session.
- The user's logon performance is a priority and the Citrix policy "Wait for printers to be created" must be enabled due to application compatibility.
- The user is working from a Windows based device or thin client.

**Note:** Other options for provisioning printers, such as Active Directory group policy, "follow-me" centralized print queue solutions, and other 3rd party print management solutions can be used to provision printers into a Citrix session.

### Decision: Printer Drivers

Managing print drivers in XenApp and XenDesktop can be a tedious task, especially in large environments with hundreds of printers. In XenApp and XenDesktop there are several methods available to assist with print driver management.

- **User Installed** - When adding a printer within a XenApp or XenDesktop session and the native print driver is not available, the drivers can be installed manually, by the user. Many different print drivers can potentially be installed on different resources creating inconsistencies within the environment. Troubleshooting printing problems and maintenance of print drivers can become very challenging since every hosted resource may have different sets of print drivers installed. To ensure consistency and simplify support and troubleshooting, user installed drivers is not recommended.
- **Automatic Installation** - When connecting a printer within a XenApp or XenDesktop session, a check is made to see if the required print driver is already installed in the operating system. If the print driver is not already installed, the native print driver, if one exists, will be installed automatically. If users roam between multiple endpoints and locations, this can create inconsistencies across sessions since users may access a different hosted resource every time they connect. When this type of scenario occurs, troubleshooting printing problems and maintenance of print drivers can become very challenging since every hosted resource may have different sets of print drivers installed. To ensure consistency and simplify support and troubleshooting, automatic installed drivers is not recommended.
- **Universal Print Driver** - The Citrix Universal Printer Driver (UPD) is a device independent print driver, which has been designed to work with most printers. The Citrix Universal Printer Driver (UPD) simplifies administration by reducing the number of drivers required on the master image. For autocreated client printers, the driver records the output of the application and sends it, without any modification, to the end-point device. The endpoint uses local, device-specific drivers to finish printing the job to the printer. The UPD can be used in conjunction with the Citrix Universal Print Server (UPServer) to extend this functionality to network printers.

### Decision: Printer Routing

Print jobs can be routed along different paths: through a client device or through a print server.

- **Client Device Routing** - Client devices with locally attached printers (printers attached through USB, LPT, COM, TCP, etc.) will route print jobs directly from the client device to the printer.
- **Windows Print Server Routing** - By default, print jobs sent to auto-created network-based printers will be routed from the user's session to the print server. However, the print job will take a fallback route through the client device when any of the following conditions are true:
  - The session cannot contact the print server
  - The print server is on a different domain without a trust established
  - The native print driver is not available within the user's session
- **Citrix Universal Print Server Routing** - Print job routing follows the same process as Windows Print Server Routing except that the Universal Print Driver is used between the user's session and the Citrix Universal Print Server.

The specifics with print job routing are based on the printer provisioning method. Auto-created and user-added printers can route print jobs based on the following diagrams:

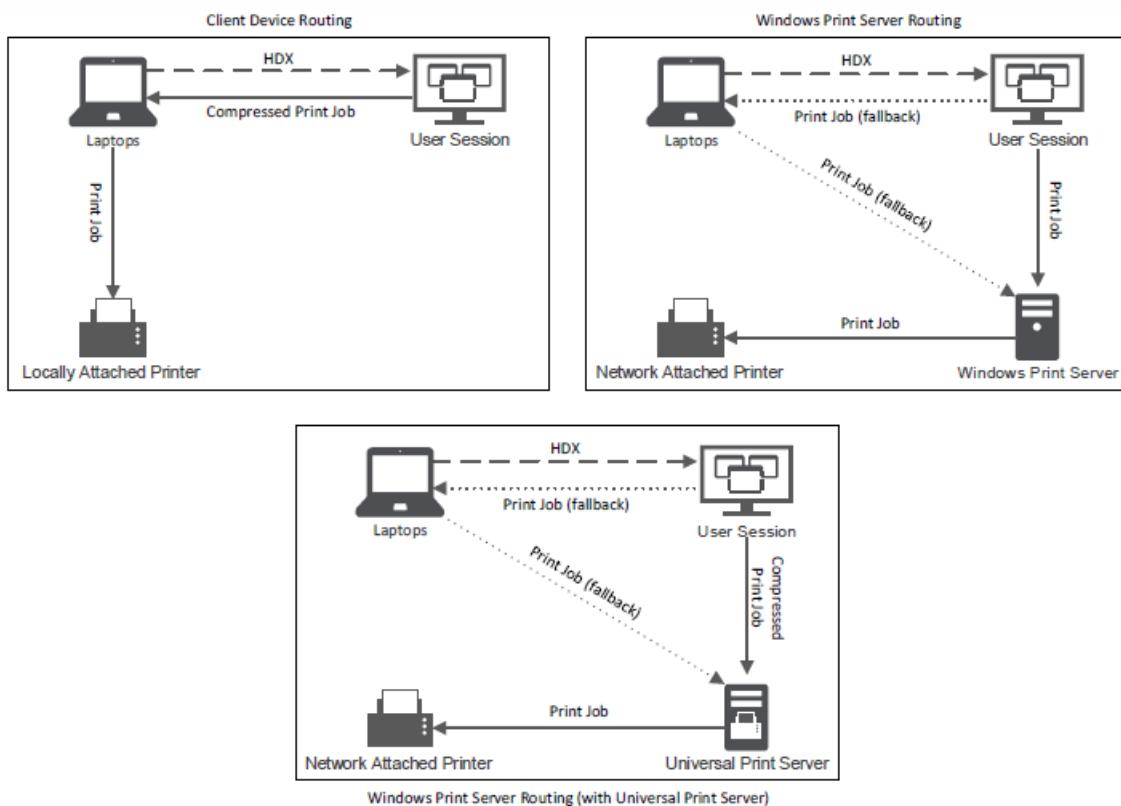


Figure 12: Auto-created and User-Added Print Job Routing

However, if the printers are provisioned as session printers, the print job routing options change slightly. The jobs are no longer able to route through the user's endpoint device.

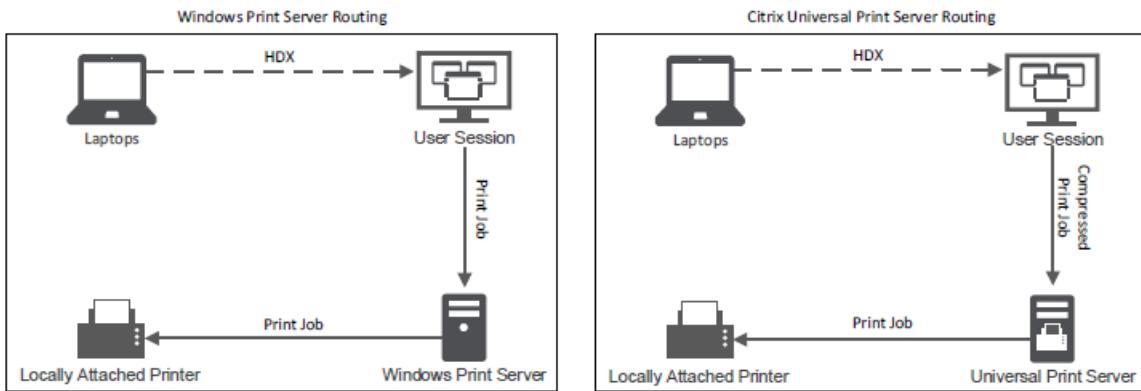


Figure 13: Session Printers Print Job Routing

The recommended option is based on the network location of the endpoint device, the user's session and the print server.

- Client Device Routing
  - Use for locally attached printer implementations.
  - Use if a Windows endpoint device and printer are on the same high-speed, low-latency network as the Windows Print Server.
- Windows Print Server Routing
  - Use if the printer is on the same high-speed, low-latency network as the Windows Print Server and user session.
- Windows Print Server Routing (with Universal Print Server)
  - Use if non-Windows endpoint device and printer are on the same high-speed, low-latency network as the Windows Print Server.

### **Decision: Print Server Redundancy**

Network-based printers, managed with a Microsoft print server or the Citrix Universal Print Server should be configured with redundancy in order to eliminate a single point of failure. The Citrix Universal Print Server should be defined within a Citrix Policy.

## Experience from the Field

A print media company leverages Thin Clients and Windows-based workstations at the company headquarters. Network based printers are placed throughout the building (one per floor). Windows print servers reside in the datacenter and manage the network printers. XenDesktop and XenApp servers also reside in the datacenter.

A regional office has numerous Windows, Linux and Mac endpoints with network attached printers.

A remote branch office has a few Windows workstations with locally attached printers.

Three different print strategies are applied:

### Headquarters

A Citrix Universal Print Server is used for printing within the XenApp and XenDesktop session. Native print drivers are not required on the Windows based workstations. A session printer policy is configured per floor which connects the floor printer as the default printer. The policies are filtered based on the subnet of the thin client for proximity printing.

Quality of Service (QoS) policies are implemented. Inbound and outbound network traffic on ports TCP 1494 and TCP 2598 are prioritized over all other network traffic. This will prevent HDX user sessions from being impacted by large print jobs.

### Regional Office

A Universal Print Server is deployed within the regional office. The print job uses the Universal Print Driver and is compressed and delivered from the user's session to the Universal Print Server, across the WAN. The job is then sent to the network-attached printer in the office.

### Branch Office

Since all branch users work on Windows based workstations, auto-created client printers in conjunction with the Citrix Universal Printer Driver are used. Since the print job is delivered over ICA, the print data is compressed which saves bandwidth. The Citrix Universal Printer Driver ensures all printers connected to the client can be used within the XenApp or XenDesktop session without concern of the printer model used.

## Applications

Properly integrating an application requires understanding compatibility and how the user/business requirements influences the appropriate delivery method.

### Decision: Compatibility

VDI typically requires significant changes to be made to an organization's application delivery and management strategy. For example, many organizations will take the opportunity to upgrade their desktop operating system and to simplify management by reducing the number of applications installed into the base image using techniques such as application streaming and application layering. These are significant changes that require comprehensive compatibility testing. Important compatibility requirements that may need to be verified include:

- **Operating system** - the application must be compatible with the preferred operating system.
- **Multi-User** - Some applications may be more appropriate for delivery via a hosted shared desktop or a hosted Windows App. In these situations, the compatibility of the application must be verified against the multi-user capabilities of a server operating system like Windows Server 2012R2.
- **Application architecture** - It is important to understand whether the application includes 16-bit, 32-bit or 64-bit code so that an appropriate operating system can be selected. 16-bit code cannot be executed on a 64-bit operating system. However, a 16-bit application can be delivered to users as a Hosted Windows App from a 32-bit desktop-based operating system like x86 editions of Windows 7, 8 or 10.
- **Interoperability** - Some applications may experience complications if they coexist on the same operating system.

Possible causes include shared registry hives, dll files or INI files as well as incompatible dependencies. Application interoperability issues should be identified so that appropriate remediation steps can be taken or an alternative delivery model selected.

- **Dependency** - Applications may need to interact with each other to provide the users with a seamless experience. For example, applications that present information in a PDF format require a suitable PDF viewer to be available. Many times, the dependent (child) applications are version specific to the parent application.
- **Application virtualization** - The use of application virtualization techniques, like streaming and layering, helps to simplify image management by reducing the number of applications installed into the base image. However, not all applications are suitable for streaming and layering because they may install device drivers, use COM+ or form part of the operating system.

Application compatibility can be achieved by doing a combination of manual, user testing, utilizing pre-verified lists maintained by the software vendor, or using an automated application compatibility solution, like Citrix AppDNA which runs through thousands of tests to verify compatibility.

### **Decision: Application Delivery Method**

It is unlikely that a single delivery method will meet all requirements. Based on the outcome of the application categorization assessment process, several application delivery methods can be considered.

Choosing one of the appropriate application delivery method helps improve scalability, management and user experience.

- **Installed app** - The application is part of the base desktop image. The install process involves dll, exe and other files being copied to the image drive as well as registry modifications.
- **Streamed App (Microsoft App-V)** - The application is profiled and delivered to the desktops across the network on-demand. Application files and registry settings are placed in a container on the virtual desktop and are isolated from the base operating system and each other, which helps to address compatibility issues.
- **Hosted Windows App** - The application is installed on a multi-user XenApp host and deployed as an application and not a desktop. The hosted Widnwos app is accessed seamless from the user's VDI desktop or endpoint device, hiding the fact that the app is executing remotely.
- **Local App** - The application is deployed on the endpoint device. The application interface appears within the user's hosted VDI session even though it executes on the endpoint.

The following table provides recommendations on the preferred approaches for integrating applications into the overall solution:

App Category	Installed App	Streamed App	Hosted Windows App	Local App
Common	✓	◦	◦	✗
Departmental	◦	✓	✓	✗
User	✗	◦	◦	✓
Management	✓	✗	◦	✗

"✓": Recommended, "✗": Not Recommended, "◦": Viable

Table 25: App Deployment Recommendations

### Experience from the Field

**Energy** – An energy company installs applications on the base image for the majority of users and streams departmental applications as required.

**Financial** – A banking customer maintains and deploys multiple desktop images containing user group focused applications as required by various departments.

## Virtual Machines

Virtual resources require proper allocation of the processor, memory and disk. These decisions have a direct impact on the amount of hardware required as well as the user experience.

The key to successful resource allocation is to ensure that virtual desktops and applications offer similar levels of performance to physical desktops. Otherwise, productivity and overall user satisfaction will be affected. Allocating resources to the virtual machines above their requirements however is inefficient and expensive for the business.

The resources allocated should be based on the workload characteristic of each user group, identified during the assess phase.

### Decision: Virtual Processor (vCPU)

For hosted desktop-based VDI models (hosted pooled desktops and hosted personal desktops), the general recommendation is two or more vCPUs per virtual machine so that multiple threads can be executed simultaneously. Although a single vCPU could be assigned for extremely light workloads, users are more likely to experience session hangs.

For hosted server-based VDI models (hosted Windows apps, hosted browser apps, hosted shared desktops), the proper vCPU allocation is based on the Non-Uniform Memory Access (NUMA) architecture of the processors.

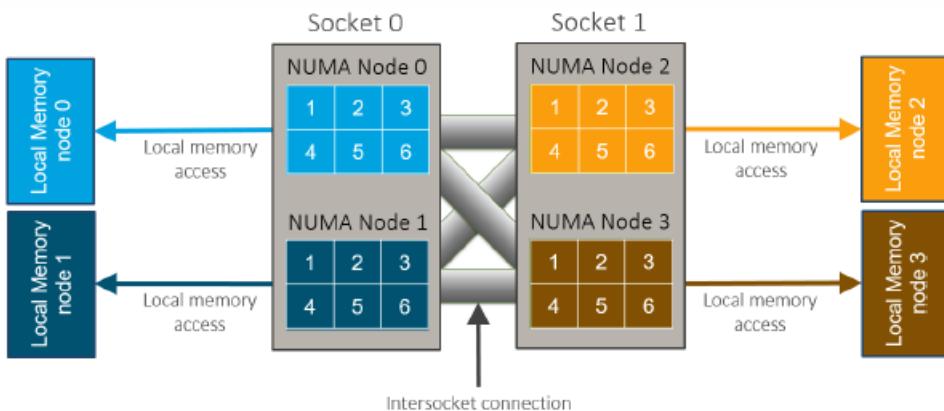


Figure 14: NUMA Architecture

Each socket is divided into one or more NUMA nodes. Hosted server-based VDI models will often utilize 4 or more processors. Allocating more vCPU than the NUMA node contains results in a performance hit. Allocating a portion of a NUMA node to a virtual machine results in a performance hit if the portion allocated is not easily divisible by the size of the NUMA node. It is often ideal to allocate the number of cores within a NUMA node to a virtual machine or allocate ½ of the cores to a virtual machine, while doubling the number of virtual machines.

User Workload	Operating System	vCPU Configured for Scale	vCPU Configured for Experience
Light	Windows 7	2 vCPU	2 vCPU
	Windows 10	2 vCPU	2 vCPU
	Windows 2012R2	NUMA or $\frac{1}{2}$ of NUMA	NUMA or $\frac{1}{2}$ of NUMA
Medium	Windows 7	2 vCPU	3 vCPU
	Windows 10	2 vCPU	3 vCPU
	Windows 2012R2	NUMA or $\frac{1}{2}$ of NUMA	NUMA or $\frac{1}{2}$ of NUMA
Heavy	Windows 7	3 vCPU	4 vCPU
	Windows 10	3 vCPU	4 vCPU
	Windows 2012R2	NUMA or $\frac{1}{2}$ of NUMA	NUMA or $\frac{1}{2}$ of NUMA

Table 26: vCPU Allocation

**Note:** Windows 2012R2 recommendations are based on the hosted Windows app, hosted browser app and hosted shared desktop VDI model.

### Decision: Virtual Memory (vRAM)

The amount of memory allocated to each resource is a function of the user's expected workload and application footprint. Assigning insufficient memory to the virtual machines will cause excessive paging to disk, resulting in a poor user experience; allocating too much RAM increases the overall cost of the solution.

The following table provides guidance on the virtual RAM that should be assigned based on workload:

User Workload	Operating System	vRAM Configured for Scale	vRAM Configured for Experience
Light	Windows 7	2 GB	3 GB
	Windows 10	2 GB	3 GB
	Windows 2012R2	256 MB per user	
Medium	Windows 7	3 GB	4 GB
	Windows 10	3 GB	4 GB
	Windows 2012R2	512 MB per user	
Heavy	Windows 7	6 GB	8 GB
	Windows 10	6 GB	8 GB
	Windows 2012R2	1024 MB per user	

Table 27: vRAM Allocation

**Note:** Windows 2012R2 recommendations are based on the hosted Windows app, hosted browser app and hosted shared desktop VDI model.

**Note:** Memory allocation above 4GB requires a 64-bit operating system.

**Note:** If used, the Machine Creation Services and Provisioning Services cache in RAM amount should be added onto the virtual machine RAM specifications.

### Decision: Disk Cache

The amount of storage that each VM requires will vary based on the workload and the image type. If creating hosted personal desktop without leveraging an image management solution, each VM will require enough storage for the entire OS and locally installed applications.

Deploying machines through Machine Creation Services or Provisioning Services can substantially reduce the storage

requirements for each virtual machine. Disk space requirements for the write cache and difference disk will depend on application usage and user behavior. However, the following table provides a starting point for estimating disk space requirements based on machine sized with vCPU and vRAM as per the guidelines above:

User Workload	Operating System	Storage Space (Differencing Disk / Write Cache Disk)
Light	Windows 7	10 GB
	Windows 10	10 GB
	Windows 2012R2	40 GB
Medium	Windows 7	15 GB
	Windows 10	15 GB
	Windows 2012R2	40 GB
Heavy	Windows 7	20 GB
	Windows 10	20 GB
	Windows 2012R2	40 GB

Table 28: Disk Cache Allocation

### Decision: RAM Cache

Provisioning Services and Machine Creation Services have the capability to utilize a portion of the virtual machine's RAM as a buffer for the storage cache. The RAM cache is used to improve the performance of traditional storage by sharing the virtual machine's non-paged pool memory

User Workload	Operating System	RAM Cache Configured for Scale	RAM Cache Configured for Experience
Light	Windows 7	128 MB	256 MB
	Windows 10	128 MB	256 MB
	Windows 2012R2	2 GB	
Medium	Windows 7	256 MB	512 MB
	Windows 10	256 MB	512 MB
	Windows 2012R2	2 GB	
Heavy	Windows 7	512 MB	1024 MB
	Windows 10	512 MB	1024 MB
	Windows 2012R2	2 GB	

Table 29: RAM Cache Allocation

**Note:** If used, the Machine Creation Services and Provisioning Services cache in RAM amount should be added onto the virtual machine RAM specifications.

**Note:** If additional RAM is available on the host, the RAM Cache amounts can be increased to provide even greater levels of performance.

### Decision: Storage IOPS

Storage performance is limited by the number of operations it can handle per second, referred to as IOPS. Underallocating storage IOPS results in a VDI desktop where apps, web pages and data are slow to load.

The following table provides guidance on the number of storage IOPS generated per user based on workload and operating system. Storage IO activity will be higher during user logon/logoff.

User Workload	Operating System	Storage IOPS (without RAM-Based Cache)	Storage IOPS (with RAM-Based Cache)
Light	Windows 7	10 IOPS	1 IOPS
	Windows 10	12 IOPS	1 IOPS
	Windows 2012R2	3 IOPS	0.5 IOPS
Medium	Windows 7	15 IOPS	1 IOPS
	Windows 10	20 IOPS	1.5 IOPS
	Windows 2012R2	4 IOPS	0.5 IOPS
Heavy	Windows 7	25 IOPS	2 IOPS
	Windows 10	35 IOPS	3 IOPS
	Windows 2012R2	5 IOPS	1.5 IOPS

Table 30: IOPS Allocation

### Decision: Graphics (GPU)

Without a graphical processing unit (GPU), graphical processing is rendered with software by the CPU. A graphical processing unit (GPU) can be leveraged to improve server scalability and user experience or enable the use of graphically intensive applications. During the desktop design it is important to decide how the GPU (if used) will be mapped to the virtual machines. There are three methods available.

- **Pass-Through GPU** - Each physical GPU is passed through to a single virtual machine (hosted apps or hosted desktops).
- **Hardware Virtualized GPU** - Using a hypervisor's vGPU technology, an NVIDIA GRID or Intel Iris Pro is virtualized and shared between multiple machines. Each virtual machine has the full functionality of GPU drivers and direct access to the GPU.
- **Software Virtualized GPU** - The GPU is managed by the hypervisor and intercepts requests made by the VDI desktops. This process is used if a GPU is not installed within the host.

	Pass-Through GPU	Hardware Virtualized GPU (Nvidia)	Hardware Virtualized GPU (Intel)	Software Emulated GPU
<b>Citrix XenServer</b>				
XenDesktop	✓	✓	✓	✓
XenApp	✓	✓	✓	✓
<b>Microsoft Hyper-V</b>				
XenDesktop	✓	✗	✗	✓
XenApp	✓	✗	✗	✓
<b>VMware vSphere</b>				
XenDesktop	✓	✓	✗	✓
XenApp	✓	✓	✗	✓

"✓": Available "✗": Not Supported

Table 31 GPU Allocation Options

User groups with a heavy use of graphical applications will often require the use of a NVidia hardware virtualized GPU. User groups who rely on office-based applications can have an observable benefit with the use of a hardware virtualized GPU from Intel.

### Layer 4: The Control Layer

## Active Directory

### Decision: Forest Design

Multi-forest deployments, by default, do not have inter-domain trust relationships between the forests. An Active Directory administrator can establish trust relationships between the multiple forests, allowing the users and computers from one forest to authenticate and access resources in another forest.

For forests that have inter-domain trusts, Citrix recommends that the appropriate settings be configured to allow the Delivery Controllers to communicate with both domains. When the appropriate trusts are not configured, multiple XenDesktop sites for each forest must be configured. This section outlines the storage requirements on a per product basis and provides sizing calculations. For more information, please refer to Citrix article: [CTX134971 - Successfully Deploying XenDesktop in a Complex Active Directory Environment](#).

### Decision: Organizational Unit Structure

Infrastructure components for a XenApp and XenDesktop deployment should reside within their own dedicated organizational units (OUs); separating workers and controllers for management purposes. By having their own OUs, the objects inside will have greater flexibility with their management while allowing Citrix administrators to be granted delegated control.

A sample Citrix OU structure can be seen below.

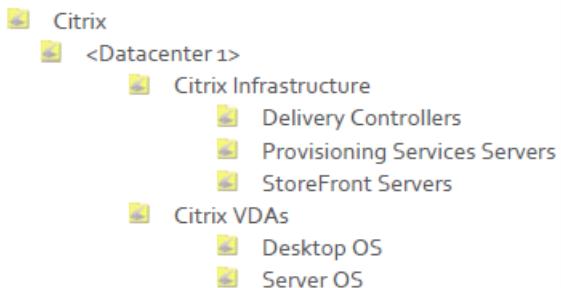


Figure 15: Example Citrix OU Structure

### Decision: User Groups

Whenever possible, permissions and authorization should be assigned to user groups rather than individual users, thereby eliminating the need to edit a large amount of resource permissions and user rights when creating, modifying, or deleting user accounts.

Permission application example:

- An application published to one group of 1,000 users requires the validation of only one object for all 1,000 users.
- The same application published to 1,000 individual user accounts requires the validation of all 1,000 objects.

## Database

The majority of Citrix products discussed within this document require a database. The following table outlines the usage on a per product basis:

Product	Configuration Data	Runtime Data	Audit / Change Log Data	Monitoring Data
XenDesktop	✓	✓	✓	✓
Provisioning Services	✓		①	
XenClient	✓	✓	✓	

"①": Optional

Table 32: Database usage

## Decision: Edition

There are multiple editions of Microsoft SQL Server 2012: Express, Web, Standard, Business Intelligence, and Enterprise. Based on the capabilities of the various SQL Server editions available, the Standard edition is often used for hosting the XenApp and XenDesktop databases in production environments.

The Standard edition provides an adequate amount of features to meet the needs of most environments. For more information on the databases supported with Citrix products please refer to the Citrix Database Support Matrix. Different versions of Citrix products support different versions of the SQL server; therefore it is important to check the support matrix to ensure the version of SQL server used is compatible with the Citrix product being deployed.

## Decision: Database Server Sizing

The SQL server must be sized correctly to ensure the performance and stability of an environment. Since every Citrix product uses SQL server in a different way, no generic all-encompassing sizing recommendations can be provided. Instead, per-product SQL server sizing recommendations are provided below.

### XenApp and XenDesktop

XenApp and XenDesktop Brokers use the database as a message bus for broker communications, storing configuration data and storing monitoring and configuration log data. The databases are constantly in use and the performance impact on the SQL server can be considered as high.

Based on results from Citrix internal scalability testing the following SQL server specification for a server hosting all XenDesktop databases are recommended:

- 2 Cores / 4 GB RAM for environments up to 5,000 users
- 4 Cores / 8 GB RAM for environments up to 15,000 users
- 8 Cores / 16 GB RAM for environments with 15,000+ users

The database files and transaction logs should be hosted on separate hard disk subsystems in order to cope with a high number of transactions. For example, registering 20,000 virtual desktops during a 15 minute boot storm causes ~500 transactions / second and 20,000 users logging on during a 30 minute logon storm causes ~800 transactions / second on the XenDesktop Site Database.

### Provisioning Services

In addition to static configuration data provisioning servers store runtime and auditing information in the database. Depending on the boot and management pattern, the performance impact of the database can be considered as low to medium.

Based on this categorization, a SQL server specification of 4 Cores and 4 GB RAM is recommended as a good starting point. The SQL server should be carefully monitored during the testing and pilot phase in order to determine the

optimal configuration of the SQL server.

## Decision: Instance Sizing

When sizing a SQL database, two aspects are important:

- **Database file** - Contains the data and objects such as tables, indexes, stored procedures and views stored in the database.
- **Transaction log file** - Contains a record of all transactions and database modifications made by each transaction. The transaction log is a critical component of the database and, if there is a system failure, the transaction log might be required to bring the database back to a consistent state. The usage of the transaction log varies depending on which database recovery model is used:
  - **Simple recovery** - No log backups required. Log space is automatically reclaimed, to keep space requirements small, essentially eliminating the need to manage the transaction log space. Changes to the database since the most recent backup are unprotected. In the event of a disaster, those changes must be redone.
  - **Full recovery** - Requires log backups. No work is lost due to a lost or damaged database data file. Data of any arbitrary point in time can be recovered (for example, prior to application or user error). Full recovery is required for database mirroring.
  - **Bulk-logged** - Requires log backups. This is an adjunct of the full recovery model that permits high-performance bulk copy operations. It is typically not used for Citrix databases.

For further information, please refer to the [Microsoft Developer Network – SQL Server Recovery Models](#).

In order to estimate storage requirements, it is important to understand the disk space consumption for common database entries. This section outlines the storage requirements on a per product basis and provides sizing calculations. For more information, please refer to Citrix article: CTX139508 – [XenDesktop 7.x Database Sizing](#).

## XenDesktop General

XenApp 7.x and XenDesktop 7.x use three distinct databases:

- **Site Configuration database** - Contains static configuration and dynamic runtime data
- **Monitoring database** - Contains monitoring data which is accessible through Director
- **Configuration logging database** - Contains a record for each administrative change performed within the site (accessible through Studio)

## Site Database

Since the database of a XenApp or XenDesktop site contains static configuration data and dynamic runtime data, the size of the database file depends not only on the physical size of the environment but also user patterns. The following factors all impact the size of the database file:

- The number of connected sessions
- The number of configured and registered VDAs
- The number of transactions occurring during logon
- The VDA heartbeat transactions

The size of the Site Database is based on the number of VDAs and active sessions. The following table shows the typical maximum database size Citrix observed when scale testing XenApp and XenDesktop with a sample number of users, applications, and desktop delivery methods.

Users	Applications	Desktop Types	Expected Maximum Size (MB)
1,000	50	Hosted Shared	30
10,000	100	Hosted Shared	60
100,000	200	Hosted Shared	330
1,000	N/A	Hosted Pooled	30
10,000	N/A	Hosted Pooled	115
40,000	N/A	Hosted Pooled	390

Table 33: XenDesktop Site DB sample size calculations

**Note:** This sizing information is a guide only. Actual database sizes may differ slightly by deployment due to how databases are maintained.

Determining the size of the transaction log for the Site database is difficult due to factors that can influence the log including:

- The SQL Database recovery model
- The launch rate at peak times
- The number of desktops being delivered

During XenDesktop scalability testing, Citrix observed the transaction log growth rate at 3.5MB an hour when the system is idle, and a per user per day growth rate of ~32KB. In a large environment, transaction log usage requires careful management and a regular backup, to prevent excessive growth. This can be achieved by means of scheduled jobs or maintenance plans

## Monitoring Database

Of the three databases, the Monitoring database is expected to be the largest since it contains historical information for the site. Its size is dependent on many factors including:

- Number of Users
- Number of sessions and connections
- Number of workers
- Retention period configuration – Platinum customers can keep data for over a year (default 90 days). Non-platinum customers can keep data for up to 7 days (default 7 days).
- Number of transaction per second. Monitoring service tends to execute updates in batches. It is rare to have the number of transactions per second go above 20.
- Background transaction caused by regular consolidation calls from the Monitoring service.
- Overnight processing carried out to remove data outside the configured retention period.

The following table shows the estimated size of the Monitoring database over a period of time under different scenarios. This data is an estimate based on data seen within scale testing XenApp and XenDesktop (assuming a 5 day working week).

Estimates with 1 connection and 1 session per user with a 5 day work week					
Users	Type	1 week (MB)	1 month (MB)	3 months (MB)	1 year (MB)
1,000	HSD	20	70	230	900
10,000	HSD	160	600	1,950	7,700
100,000	HSD	1,500	5,900	19,000	76,000
1,000	VDI	15	55	170	670
10,000	VDI	120	440	1,400	5,500
40,000	VDI	464	1,700	5,400	21,500
Estimates with 2 connections and 1 session per user with a 5 day work week					
Users	Type	1 week (MB)	1 month (MB)	3 months (MB)	1 year (MB)
1,000	HSD	30	100	330	1,300
10,000	HSD	240	925	3,000	12,000
100,000	HSD	2,400	9,200	30,000	119,000
1,000	VDI	25	85	280	1,100
10,000	VDI	200	750	2,500	9,800
40,000	VDI	800	3,000	9,700	38,600

Table 34: Monitoring DB size estimations

**Note:** The 100,000 HSD tests are based on a test environment consisting of:

- 2 Delivery Controllers
- 43 Hosted Shared Desktop workers
- 3 SQL servers, configured with databases held within one Always On Availability Group

For more information please see the Citrix Support article [XenDesktop 7.x Database Sizing](#).

The size of the transaction log for the Monitoring Database is very hard to estimate, but XenApp and XenDesktop scalability testing showed a growth rate of about 30.5 MB an hour when the system is idle, and a per user per day growth rate of ~9 KB.

## Configuration Logging Database

The Configuration Logging Database is typically the smallest of the three databases. Its size and the size of the related transaction log depends on the daily administrative activities initiated from Studio, Director or PowerShell scripts, therefore its size is difficult to estimate. The more configuration changes are performed, the larger the database will grow. Some factors that can affect the size of the database include:

- The number of actions performed in Studio, Director and PowerShell.
- Minimal transactions which occur on the database when no configuration changes are taking place.
- The transaction rate during updates. Updates are batched whenever possible.
- Data manually removed from the database. Data within the Configuration Logging Database is not subject to any retention policy, therefore it is not removed unless done so manually by an administrator.
- Activities that have an impact on sessions or users, for example, session logoff and reset.
- The mechanism used for deploying desktops.

In XenApp environments not using MCS, the database size tends to fall between 30 and 40MB. For MCS environments, database size can easily exceed 200MB due to the logging of all VM build data.

## Temporary Database

In addition to the Site, Monitoring, and Configuration Logging databases, a system-wide temporary database (tempdb) is provided by SQL Server. This temporary database is used to store Read-Committed Snapshot Isolation data. XenApp 7.x and XenDesktop 7.x uses this SQL Server feature to reduce lock contention on the XenApp and XenDesktop databases. Citrix recommends that all XenApp 7.x and XenDesktop 7.x databases use Read-Committed Snapshot Isolation. For more information please see How to Enable Read-Committed Snapshot in XenDesktop.

The size of the tempdb database will depend on the number of active transactions, but in general it is not expected to grow more than a few MBs. The performance of the tempdb database does not impact the performance of XenApp and XenDesktop brokering, as any transactions that generate new data require tempdb space. XenApp and XenDesktop tend to have short-lived transactions, which help keep the size of the tempdb small.

The tempdb is also used when queries generate large intermediate result sets. Guidance and sizing the tempdb can be found on the Microsoft TechNet article Optimizing tempdb Performance.

## Provisioning Services

The Provisioning Services farm database contains static configuration and configuration logging (audit trail) data. The record size requirements outlined below can be used to help size the database:

Configuration Item	DB Space Required (KB)	Number of Items (Example)	Total (KB)
Base farm configuration	112	-	112
User group w/ farm access	50	10	250
Site	4	5	20
Device collection	10	50	500
Farm view	4	10	40
Farm view to device relationship	5	1	5,000
Site View	4	5	20
Site view to device relationship	5	1	5,000
Device	2	5,000	10,000
Device bootstrap	10	-	-
Device to disk relationship	35	1	175,000
Device printer relationship	1	-	-
Device personality data	1	-	-
Device status (when booted)	1	5,000	5,000
Device custom property	2	-	-
vDisk	1	20	20
vDisk version	3	5	300
Disk locator	10	1	200
Disk locator custom property	2	-	-
Server	5	10	50
Server IP	2	1	20
Server status (when booted)	1	20	20
Server custom property	2	-	-
vDisk store	8	5	40
vDisk store to server relationship	4	1	40
Connection to XenServer (VirtualHostingPool)	4	-	-
vDisk update task	10	10	100
Administrative change (auditing enabled)	1	10,000	10,000
<b>Total</b>			<b>211,732KB (~212MB)</b>

Table 35: Provisioning Services Farm DB sample size calculations

During the PVS farm setup, a database with an initial file size of 20MB is created. Due to the nature of the data in the PVS

farm database the transaction log is not expected to grow very quickly, unless a large amount of configuration is performed.

In contrast to XenApp, which also offers the ability to track administrative changes, the related information is not written to a dedicated database but directly to the Provisioning Services farm database. In order to limit the size of the Provisioning Services database it is recommended to archive the audit trail data on a regular schedule.

### Decision: Database Location

By default, the Configuration Logging and Monitoring databases are located within the Site Configuration database. Citrix recommends changing the location of these secondary databases as soon as the configuration of the site has been completed, in order to simplify sizing, maintenance and monitoring. All three databases can be hosted on the same server or on different servers. An ideal configuration would be to host the Monitoring database on a different server from the Site Configuration and Configuration Logging databases since it records more data, changes occur more frequently and the data is not considered to be as critical as the other databases. For more information, please see [Change secondary database locations](#) in the Citrix Product Documentation.

**Note:** The location of the Configuration Logging database cannot be changed when mandatory logging is enabled.

### Decision: High-Availability

The following table highlights the impact to XenApp, XenDesktop and Provisioning Services when there is a database outage:

Component	Impact of Database Outage
Site configuration database	<p>Users will be unable to connect or reconnect to a virtual desktop.</p> <p><i>Note: Connection leasing in XenApp and XenDesktop 7.6 allows users with Hosted Shared Desktops, Hosted Windows and Browser Applications, and Personal Desktops to reconnect to their most recently used applications and desktops even when the site database is unavailable.</i></p>
Monitoring database	<p>Director will not display any historical data and Studio cannot be started.</p> <p>Brokering of incoming user requests and existing user sessions will not be affected.</p>
Configuration logging database	<p>If allow changes when the database is disconnected has been enabled within XenApp and XenDesktop logging preferences, an outage of the configuration logging database will have no impact (other than configuration changes not being logged). Otherwise, administrators will be unable to make any changes to the XenApp and XenDesktop site configuration. Users are not impacted.</p>
Provisioning Services farm database	<p>When offline database support is enabled and the database becomes unavailable, the stream process uses a local copy of the database to retrieve information about the provisioning server and the target devices supported by the server. This allows provisioning servers and the target devices to remain operational. However, when the database is offline, the console and the management functions listed below become unavailable:</p> <ul style="list-style-type: none"><li>• AutoAdd target devices</li><li>• vDisk creation and updates</li><li>• Active Directory password changes</li><li>• Stream process startup</li><li>• Image update service</li><li>• PowerShell and MCLI based management</li></ul> <p>If offline database support has not been enabled, all management functions become unavailable and the boot and failover of target devices will fail.</p>

Table 36: Impact of a database outage

**Note:** Please review HA options for 3rd party databases (for example, App-V, SCVMM or vCenter) with the respective

software vendor.

In addition to the built-in database redundancy options, Microsoft SQL Server, as well as the underlying hypervisor (in virtual environments), offer a number of high availability features. These enable administrators to ensure single server outages will have a minimal impact (if any) on the XenApp and XenDesktop infrastructure. The following the SQL / hypervisor high availability features are available:

**VM-level HA** - This high availability option is available for virtual SQL servers only, which need to be marked for High Availability at the hypervisor layer. In case of an unexpected shutdown of the virtual machine or the underlying hypervisor host, the hypervisor will try to restart the VM immediately on a different host. While VM-level HA can minimize downtimes in power-outage scenarios, it cannot protect from operating system level corruption. This solution is less expensive than mirroring or clustering because it uses a built-in hypervisor feature. However, the automatic failover process is slower, as it can take time detect an outage and start the virtual SQL server on another host. This may interrupt the service to users.

- **Mirroring** - Database mirroring increases database availability with almost instantaneous failover. Database mirroring can be used to maintain a single standby or mirror database, for a corresponding principal or production database. Database mirroring runs with either synchronous operation in high-safety mode, or asynchronous operation in high-performance mode. In high-safety mode with automatic failover (recommended for XenDesktop) a third server instance, known as a witness, is required, which enables the mirror server to act as a hot standby server. Failover from the principal database to the mirror database happens automatically and is typically completed within a few seconds. It is a good practice to enable VM-level HA (or a similar automatic restart functionality) for at least the witness to ensure SQL service availability in case of a multi-server outage.

**Note:** Microsoft is planning to remove mirroring as a high availability option in a future release of SQL Server and is discouraging its use in new network development. Please refer to the Microsoft article [Database Mirroring \(SQL Server\)](#) for more information.

- **AlwaysOn Failover Cluster Instances** - Failover clustering provides high-availability support for an entire instance of Microsoft SQL Server. A failover cluster is a combination of two or more nodes, or servers, using a shared storage. A Microsoft SQL Server AlwaysOn Failover Cluster Instance, introduced in SQL Server 2012, appears on the network as a single computer, but has functionality that provides failover from one node to another if the current node becomes unavailable. The transition from one node to the other node is seamless for the clients connected to the cluster. AlwaysOn Failover cluster Instances require a Windows Server Failover Clustering (WSFC) resource group. The number of nodes supported in the WSFC resource group will depend on the SQL Server edition. (Please refer to the table in the Decision: Edition earlier in this chapter.) For more information please refer to MSDN – AlwaysOn Failover Cluster Instances (SQL Server).
- **AlwaysOn Availability Groups** - AlwaysOn Availability Groups is an enterprise-level high-availability and disaster recovery solution introduced in Microsoft SQL Server 2012, which enables administrators to maximize availability for one or more user databases. AlwaysOn Availability Groups require that the Microsoft SQL Server instances reside on Windows Server failover clustering (WSFC) nodes. Similar to failover clustering a single virtual IP / network name is exposed to the database users. In contrast to failover clustering, shared storage is not required since the data is transferred using a network connection. Both synchronous and asynchronous replication to one or more secondary servers is supported. As opposed to mirroring or clustering secondary servers can be actively used for processing incoming read-only requests, backups or integrity checks. This feature can be used to offload user resource enumeration requests to a secondary SQL server in XenDesktop environments to essentially scale-out a SQL server infrastructure. Since the data on active secondary servers can lag multiple seconds behind the primary server, the read-only routing feature cannot be used for other XenDesktop database requests at this point in time. For more information, please refer to MSDN – AlwaysOn Availability Groups (SQL Server).

The following table outlines the recommended high availability features for Citrix databases:

Component	VM-Level HA	Mirroring	AlwaysOn Failover Cluster Instances	AlwaysOn Availability Groups
Site database	①	✓	○	○
Configuration logging database	①	○	○	○
Monitoring database	①	✓	○	○
Provisioning Services farm database	①	✓	○	✗
XenClient database	①	✗	○	○

"✓": Recommended "○": Viable "✗": Not Supported "①": Recommended for test environments only

Table 37: Recommended SQL high availability options

### Decision: Connection Leasing

Connection leasing is a new XenApp and XenDesktop 7.6 feature that allows Hosted Shared, Hosted Windows and Browser Apps and Personal VDI users to connect and reconnect to their most recently used applications and desktops, even when the site database is unavailable. Connection Leasing is not available for users with a Pooled VDI desktop.

The lease information along with the application, desktop, icon, and worker information is stored on the controller's local disk and synchronized between controllers in the site. If the site database becomes unavailable, the controllers enter a "leased connection mode" and replay cached operations from an XML file on the local disk to connect or reconnect users to a recently used application or desktop.

Administrators familiar with the local host cache in XenApp 6.5 and earlier should understand the similarities and differences with connection leasing because it can have an impact on the design and scalability of the XenApp and XenDesktop 7.6 solution. In XenApp 6.5 and earlier, the IMA service is responsible for synchronizing the local host cache with the data store. In XenApp and XenDesktop 7.6, the FMA service caches the brokering operations (leases) to an XML file containing the address of the VDA, application path, and other details required for the session to launch. The FMA also caches dynamic information such as user sessions, VDA registrations, and load. These files are uploaded to the SQL database and synchronized between all controllers in the site. The controllers will download the files on a regular basis so that any other controller in the site can connect a user to their session.

Each controller needs additional disk space for the cached lease files. At a minimum, 4KB is required for each lease file. Each resource entry in the enumeration lease will take anywhere from 200 bytes to a few KBs depending on the number of entries and resources published. Citrix testing has shown that 200,000 leased connections for server hosted applications and desktops required approximately 3GB of disk space. 40,000 leased connections for assigned desktops required approximately 156MB of disk space.

By default, connection leases have an expiration period of two weeks. Applications and desktops must have been launched within the two last weeks to still be accessible when the database is unavailable. The expiration period is configurable using PowerShell cmdlets or editing the registry and can be set from 0 minutes to several years. Setting the expiration period too short will prevent users from connecting to their virtual desktops and applications in the event of an outage. Setting the expiration period too long will increase storage requirement on the controllers.

By default, connection leasing affects the entire site, however, leases can be revoked for specific users, which prevents them from accessing any applications or desktops when the site database is unavailable.

### Citrix Licensing

Citrix offers organizations the flexibility of multiple licensing models that align with common usage scenarios. The different licensing models vary based on the Citrix product used, but can include per user/device and per concurrent user. Several Citrix products use the license server, while other products require a license to be installed on the product itself.

For more information on XenDesktop 7.x licensing, refer to CTX128013 - XenDesktop Licensing.

For more information on Microsoft Licensing, refer to the Microsoft document – Licensing Microsoft’s Virtual Desktop Infrastructure Technology.

### **Decision: Sizing**

Internal scalability testing has shown that a single virtual license server with two cores and 2GB of RAM can issue approximately 170 licenses per second or 306,000 licenses per half hour. If necessary, the specification of the license server can be scaled out to support a higher number of license requests per second.

### **Decision: High Availability**

For a typical environment, a single license server is sufficient. Should the license server become unavailable, dependent Citrix products will enter a 30-day grace period, which provides more than enough time to resolve connectivity issues and/or restore or rebuild the license server.

Note: If the license server and the Citrix product do not communicate within 2 heartbeats (5-10 min), the Citrix product will enter a grace period and will allow connections for up to 30 days. Once communication with the license server is re-established, the license server will reconcile the temporary and actual licenses.

Note: A CNAME record in DNS is a convenient way to reference the license server. Using CNAMEs allows the license server name to be changed without updating the Citrix products.

If additional redundancy is required, Citrix supports the following high availability solutions for the license server.

- Windows Clustering – Cluster servers are groups of computers that work together in order to increase availability. Clustering allows the license server role to automatically failover in the event of a failure. For more information on clustering, please see the Citrix eDocs article – Clustered License Servers.
- Duplication of license server – Create a VM level backup of the license server. This backup should not be stored on the same host as the license server. Instead, it should be stored in a safe location, such as a highly available storage solution, or backed up to tape or disk. The duplicate server is not active, and will remain on standby until the need arises to restore the active license server. Should the license server be restored using this backup, any new licenses must be re-downloaded to the server.

Each method allows an administrator to exchange a single license server for another without an interruption in service; assuming that the change occurs during the grace period and that the following limitations are considered.

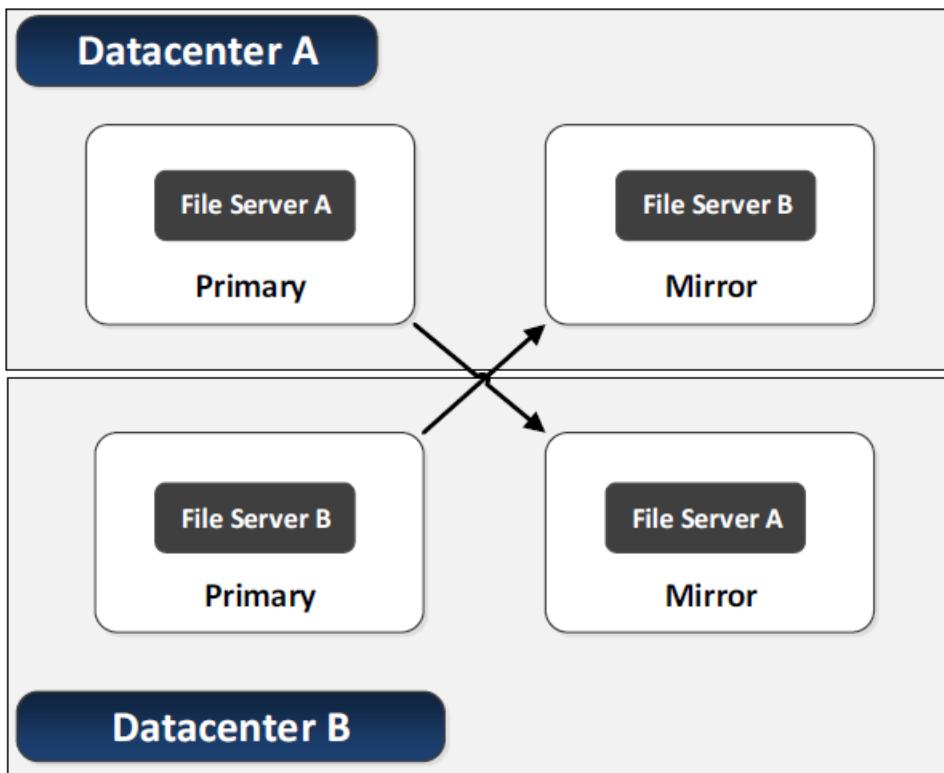
- License files will reference the server specified during the allocation process. This means that the license files can only be used on a server with the same binding information (Hostname) as the server that was previously specified.
- Two Windows-based, domain joined license servers cannot share the same name and be active in the environment at the same time.
- Because license servers do not communicate with each other, any additional licenses must be placed on both the active and backup license server.

### **Decision: Optimization**

License server performance can be optimized by tuning the number of “receive” and “processing” threads. If the thread count is set too low, requests will be queued until a thread becomes available. Conversely, if the thread count is set too high, the license server will become overloaded. The optimal values are dependent on the server hardware, site configuration, and license request volume. Citrix recommends testing and evaluating different values to determine the proper configuration. Setting the maximum number of processing threads to 30 and the maximum number of receiving threads to 15 is a good starting point for large scale deployments. This optimization will improve the Citrix License Server’s ability to provide licenses by increasing its ability to receive and process license requests.

# 监视

Jan 25, 2017



## Policies

Policies provide the basis to configure and fine tune XenApp and XenDesktop environments, allowing organizations to control connection, security and bandwidth settings based on various combinations of users, devices or connection types.

When making policy decisions it is important to consider both Microsoft and Citrix policies to ensure that all user experience, security and optimization settings are considered. For a list of all Citrix-related policies, please refer to the Citrix Policy Settings Reference.

### Decision: Preferred Policy Engine

Organizations have the option to configure Citrix policies via Citrix Studio or through Active Directory group policy using Citrix ADMX files, which extend group policy and provide advanced filtering mechanisms.

Using Active Directory group policy allows organizations to manage both Windows policies and Citrix policies in the same location, and minimizes the administrative tools required for policy management. Group policies are automatically replicated across domain controllers, protecting the information and simplifying policy application.

Citrix administrative consoles should be used if Citrix administrators do not have access to Active Directory policies. Architects should select one of the above two methods as appropriate for their organization's needs and use that method consistently to avoid confusion with multiple Citrix policy locations.

It is important to understand how the aggregation of policies, known as policy precedence flows in order to understand how a resultant set of policies is created. With Active Directory and Citrix policies, the precedence is as follows:

Policy Precedence	Policy Type
Processed first (lowest precedence)	Local server policies
Processed second	Citrix policies created using the Citrix administrative consoles
Processed third	Site level AD policies
Processed fourth	Domain level AD policies
Processed fifth	Highest level OU in domain
Processed sixth and subsequent	Next level OU in domain
Processed last (highest precedence)	Lowest level OU containing object

Table 22: Policy Precedence

Policies from each level are aggregated into a final policy that is applied to the user or computer. In most enterprise deployments, Citrix administrators do not have rights to change policies outside their specific OUs, which will typically be the highest level for precedence. In cases where exceptions are required, the application of policy settings from higher up the OU tree can be managed using “block inheritance” and “no override” settings. Block inheritance stops settings from higher-level OUs (lower precedence) from being incorporated into the policy. However, if a higher-level OU policy is configured with no override, the block inheritance setting will not be applied. Given this, care must be taken in policy planning, and available tools such as the “Active Directory Resultant Set of Policy” tool or the “Citrix Group Policy Modeling” wizard should be used to validate the observed outcomes with the expected outcomes.

**Note:** Some Citrix policy settings, if used, need to be configured through Active Directory group policy, such as Controllers and Controller registration port, as these settings are required for VDAs to register.

### Decision: Policy Integration

When configuring policies, organizations often require both Active Directory policies and Citrix policies to create a completely configured environment. With the use of both policy sets, the resultant set of policies can become confusing to determine. In some cases, particularly with respect to Windows Remote Desktop Services (RDS) and Citrix policies, similar functionality can be configured in two different locations. For example, it is possible to enable client drive mapping in a Citrix policy and disable client drive mapping in a RDS policy. The ability to use the desired feature may be dependent upon the combination of RDS and Citrix policy. It is important to understand that Citrix policies build upon functionality available in Remote Desktop Services. If the required feature is explicitly disabled in RDS policy, Citrix policy will not be able to affect a configuration as the underlying functionality has been disabled.

In order to avoid this confusion, it is recommended that RDS policies only be configured where required and there is no corresponding policy in the XenApp and XenDesktop configuration, or the configuration is specifically needed for RDS use within the organization. Configuring policies at the highest common denominator will simplify the process of understanding resultant set of policies and troubleshooting policy configurations.

### Decision: Policy Scope

Once policies have been created, they need to be applied to groups of users and/or computers based on the required outcome. Policy filtering provides the ability to apply policies against the requisite user or computer groups. With Active Directory based policies, a key decision is whether to apply a policy to computers or users within site, domain or organizational unit (OU) objects. Active Directory policies are broken down into user configuration and computer configuration. By default, the settings within the user configuration apply to users who reside within the OU at logon, and

settings within the computer configuration are applied to the computer at system startup, and will affect all users who logon to the system. One challenge of policy association with Active Directory and Citrix deployments revolves around three core areas:

- **Citrix environment specific computer policies** - Citrix servers and virtual desktops often have computer policies that are created and deployed specifically for the environment. Applying these policies is easily accomplished by creating separate OU structures for the servers and the virtual desktops. Specific policies can then be created and confidently applied to only the computers within the OU and below and nothing else. Based upon requirements, virtual desktops and servers may be further subdivided within the OU structure based on server roles, geographical locations or business units.
- **Citrix specific user policies** -- When creating policies for XenApp and XenDesktop there are a number of policies specific to user experience and security that are applied based on the user's connection. However, the user's account could be located anywhere within the Active Directory structure, creating difficulty with simply applying user configuration based policies. It is not desirable to apply the Citrix specific configurations at the domain level as the settings would be applied to every system any user logs on to. Simply applying the user configuration settings at the OU where the Citrix servers or virtual desktops are located will also not work, as the user accounts are not located within that OU. The solution is to apply a loopback policy, which is a computer configuration policy that forces the computer to apply the assigned user configuration policy of the OU to any user who logs onto the server or virtual desktop, regardless of the user's location within Active Directory. Loopback processing can be applied with either merge or replace settings. Using replace overwrites the entire user GPO with the policy from the Citrix server or virtual desktop OU. Merge will combine the user GPO with the GPO from the Citrix server or desktop OU. As the computer GPOs are processed after the user GPOs when merge is used, the Citrix related OU settings will have precedence and be applied in the event of a conflict. For more information, please refer to the Microsoft TechNet article - [Understand User Group Policy Loopback Mode](#).
- **Active Directory policy filtering** - In more advanced cases, there may be a need to apply a policy setting to a small subset of users such as Citrix administrators. In this case, loopback processing will not work, as the policy should only be applied to a subset of users, not all users who logon to the system. Active Directory policy filtering can be used to specify specific users or groups of users to which the policy is applied. A policy can be created for a specific function, and then a policy filter can be set to apply that policy only to a group of users such as Citrix administrators. Policy filtering is accomplished using the security properties of each target policy.

Citrix policies created using Citrix Studio have specific filter settings available, which may be used to address policy-filtering situations that cannot be handled using group policy. Citrix policies may be applied using any combination of the following filters:

Filter Name	Filter Description	Scope
Access control	Applies a policy based on access control conditions through which a client is connecting. For example, users connecting through a Citrix NetScaler Gateway can have specific policies applied.	User settings
Citrix CloudBridge	Applies a policy based on whether or not a user session was launched through Citrix CloudBridge.	User settings
Client IP address	Applies a policy based on the IPv4 or IPv6 address of the user device used to connect the session. Care must be taken with this filter if IPv4 address ranges are used in order to avoid unexpected results.	User settings
Client name	Applies a policy based on the name of the user device used to connect the session.	User settings
Delivery group	Applies a policy based on the delivery group membership of the desktop running the session	User and computer settings
Delivery group type	Applies a policy based on the type of machine running the session. For example, different policies can be set depending upon whether a desktop is pooled, dedicated or streamed.	User and computer settings
Organizational unit	Applies a policy based on the OU of the desktop or server running the session.	User and computer settings
Tag	Applies a policy based on any tags applying to the desktop running the session. Tags are strings that can be added to virtual desktops in XenDesktop environments that can be used to search for or limit access to desktops.	User and computer settings
User or group	Applies a policy based on the Active Directory group membership of the user connecting to the session.	User settings

Table 23: Citrix Policy Filters

**Note:** Citrix policies in XenDesktop 7.x provide a merged view of settings that apply at the user and computer level. In table 24, the Scope column identifies whether the specified filter applies to user settings, computer settings, or both.

### Decision: Baseline Policy

A baseline policy should contain all common elements required to deliver a high-definition experience to the majority of users within the organization. A baseline policy creates the foundation for user access, and any exceptions that may need to be created to address specific access requirements for groups of users. It should be comprehensive to cover as many use cases as possible and should have the lowest priority, for example 99 (a priority number of “1” is the highest priority), in order to create the simplest policy structure possible and avoid difficulties in determining the resultant set of policies. The unfiltered policy set provided by Citrix as the default policy may be used to create the baseline policy as it is applied to all users and connections. In the baseline configuration, all Citrix policy settings should be enabled, even those that will be configured with the default value, in order to explicitly define desired/expected behavior, and to avoid confusion should default settings change over time.

Citrix Policy templates can be used to configure Citrix policies to effectively manage the end-user experience within an environment and can serve as an initial starting point for a baseline policy. Templates consist of pre-configured settings that optimize performance for specific environments or network conditions. The built-in templates included in XenDesktop are shown below:

Built-in Templates	
High definition user experience	Includes settings for providing high quality audio, graphics, and video to users.
High server scalability	Includes settings for providing an optimized user experience while hosting more users on a single server.
Optimized bandwidth for WAN	Includes settings for providing an optimized experience to users with low bandwidth or high latency connections.
Security and control	Includes settings for disabling access to peripheral devices, drive mapping, port redirection, and Flash acceleration on user devices.

Table 24: XenDesktop 7 Built-in Policy Templates

For more information on Citrix policy templates, please refer to Citrix eDocs - Manage Citrix Policy Templates.

A baseline policy configuration should also include Windows policies. Windows policies reflect user specific settings that optimize the user experience and remove features that are not required or desired in a XenDesktop environment. For example, one common feature turned off in these environments is Windows update. In virtualized environments, particularly where desktops and servers may be streamed and non-persistent, Windows update creates processing and network overhead, and changes made by the update process will not persist a restart of the virtual desktop or application server. Also in many cases, organizations use Windows software update service (WSUS) to control Windows updates. In these cases, updates are applied to the master disk and made available by the IT department on a scheduled basis.

In addition to the above considerations, an organization's final baseline policy may include settings specifically created to address security requirements, common network conditions, or to manage user device or user profile requirements:

## Printing

Citrix XenApp and Citrix XenDesktop support a variety of different printing solutions. In order to plan and successfully implement the proper printing solution it is important to understand the available technologies as well as their benefits and limitations.

### Decision: Printer Provisioning

The process of creating printers at the start of a XenApp or XenDesktop session is called printer provisioning. There are multiple approaches available:

- **User Added** - Allowing users to manually add printers gives them the flexibility to select printers by convenience. The drawback to manually adding network-based printers is that it requires the users to know the network name or path of the printers. There is also a chance that the native print driver is not installed in the operating system and the Citrix Universal Print Driver is not compatible, thereby requiring the user to seek administrative assistance. Manually adding printers is best suited in the following situations:
  - Users roam between different locations using the same client device (i.e. laptop, tablet).
  - Users work at assigned stations or areas whose printer assignments will rarely change.
  - Users have personal desktops with sufficient rights to install necessary printer drivers.
- **Auto Created** - Auto-creation is a form of dynamic provisioning that attempts to create some or all of the available printers on the client device at the start of a user session. This includes locally attached printers as well as network-based printers. Auto-creating all client printers can increase the session logon time as each printer is enumerated during the logon process.
- **Session-Based** - Session printers are a set of network-based printers assigned to users through a Citrix policy at the start of each session.

- Proximity Based: Session printers filtered by IP subnet. The network printers created under this policy may vary based on where the user's endpoint device is located. Proximity printing is recommended in situations where: Users roam between different locations using the same endpoint device (i.e. laptop, tablet) and where thin clients are used, which do not have the ability to connect to network-based printers directly.
- Session printers can be assigned using the "Session Printer" policy or the "Printer Assignments" policy. The "Session printer" policy is intended to be used to set default printers for a farm, site, large group, or OU. The "Printer Assignments" policy is used to assign a large group of printers to multiple users. If both policies are enabled and configured, the session printers will be merged into a single list.
- **Universal Printer** - The Citrix Universal Printer is a generic printer object that is auto-created at the start of a session and is not linked to a printing device. When using the Citrix Universal Printer it is not required to enumerate the available client printers during logon, which can greatly reduce resource usage and decrease user logon times. By default the Citrix Universal Printer will print to the client's default printer, however the behavior can be modified to allow the user to select any of their compatible local or network-based printers.

The Citrix Universal Printer is best suited for the following scenarios:

- The user requires access to multiple printers both local and network-based which may vary with each session.
- The user's logon performance is a priority and the Citrix policy "Wait for printers to be created" must be enabled due to application compatibility.
- The user is working from a Windows based device or thin client.

**Note:** Other options for provisioning printers, such as Active Directory group policy, "follow-me" centralized print queue solutions, and other 3rd party print management solutions can be used to provision printers into a Citrix session.

### Decision: Printer Drivers

Managing print drivers in XenApp and XenDesktop can be a tedious task, especially in large environments with hundreds of printers. In XenApp and XenDesktop there are several methods available to assist with print driver management.

- **User Installed** - When adding a printer within a XenApp or XenDesktop session and the native print driver is not available, the drivers can be installed manually, by the user. Many different print drivers can potentially be installed on different resources creating inconsistencies within the environment. Troubleshooting printing problems and maintenance of print drivers can become very challenging since every hosted resource may have different sets of print drivers installed. To ensure consistency and simplify support and troubleshooting, user installed drivers is not recommended.
- **Automatic Installation** - When connecting a printer within a XenApp or XenDesktop session, a check is made to see if the required print driver is already installed in the operating system. If the print driver is not already installed, the native print driver, if one exists, will be installed automatically. If users roam between multiple endpoints and locations, this can create inconsistencies across sessions since users may access a different hosted resource every time they connect. When this type of scenario occurs, troubleshooting printing problems and maintenance of print drivers can become very challenging since every hosted resource may have different sets of print drivers installed. To ensure consistency and simplify support and troubleshooting, automatic installed drivers is not recommended.
- **Universal Print Driver** - The Citrix Universal Printer Driver (UPD) is a device independent print driver, which has been designed to work with most printers. The Citrix Universal Printer Driver (UPD) simplifies administration by reducing the number of drivers required on the master image. For autocreated client printers, the driver records the output of the application and sends it, without any modification, to the end-point device. The endpoint uses local, device-specific drivers to finish printing the job to the printer. The UPD can be used in conjunction with the Citrix Universal Print Server (UPServer) to extend this functionality to network printers.

### Decision: Printer Routing

Print jobs can be routed along different paths: through a client device or through a print server.

- **Client Device Routing** - Client devices with locally attached printers (printers attached through USB, LPT, COM, TCP, etc.) will route print jobs directly from the client device to the printer.
- **Windows Print Server Routing** - By default, print jobs sent to auto-created network-based printers will be routed from the user's session to the print server. However, the print job will take a fallback route through the client device when any of the following conditions are true:
  - The session cannot contact the print server
  - The print server is on a different domain without a trust established
  - The native print driver is not available within the user's session
- **Citrix Universal Print Server Routing** - Print job routing follows the same process as Windows Print Server Routing except that the Universal Print Driver is used between the user's session and the Citrix Universal Print Server.

The specifics with print job routing are based on the printer provisioning method. Auto-created and user-added printers can route print jobs based on the following diagrams:

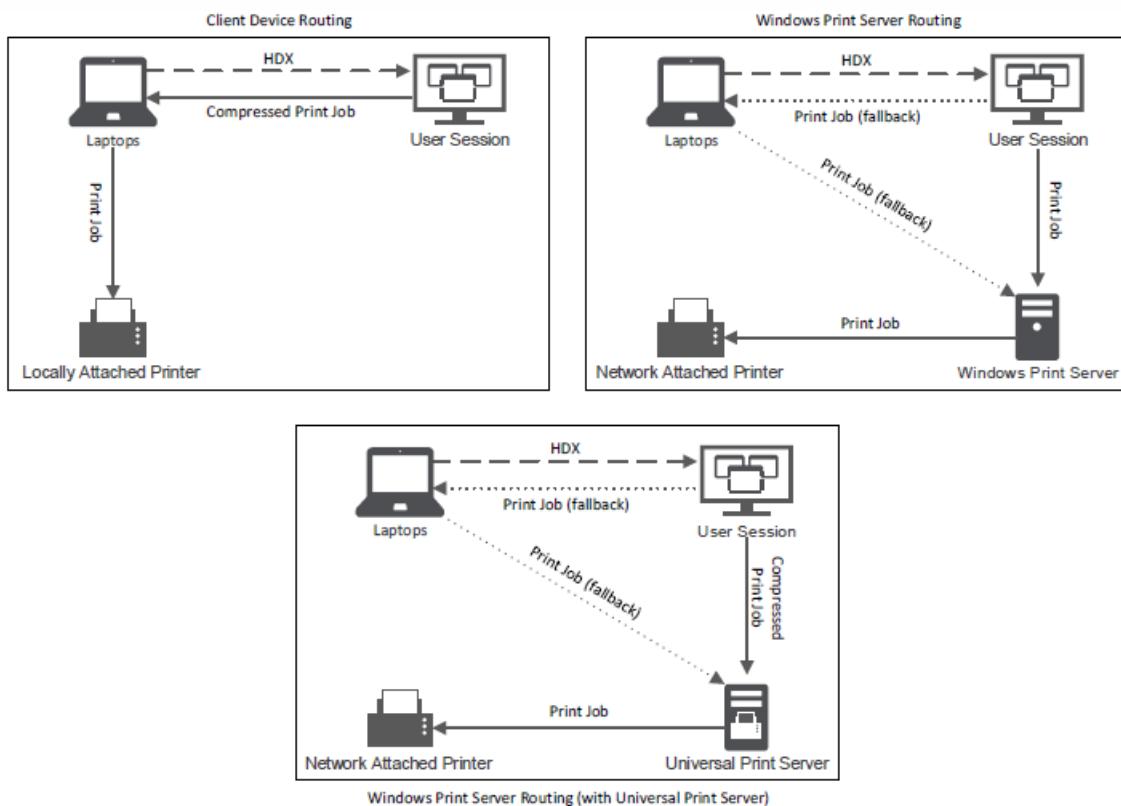


Figure 12: Auto-created and User-Added Print Job Routing

However, if the printers are provisioned as session printers, the print job routing options change slightly. The jobs are no longer able to route through the user's endpoint device.

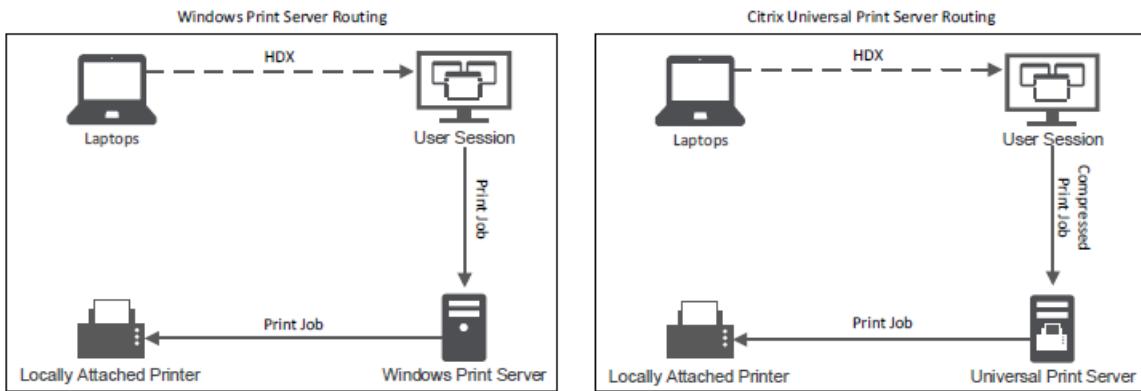


Figure 13: Session Printers Print Job Routing

The recommended option is based on the network location of the endpoint device, the user's session and the print server.

- Client Device Routing
  - Use for locally attached printer implementations.
  - Use if a Windows endpoint device and printer are on the same high-speed, low-latency network as the Windows Print Server.
- Windows Print Server Routing
  - Use if the printer is on the same high-speed, low-latency network as the Windows Print Server and user session.
- Windows Print Server Routing (with Universal Print Server)
  - Use if non-Windows endpoint device and printer are on the same high-speed, low-latency network as the Windows Print Server.

### **Decision: Print Server Redundancy**

Network-based printers, managed with a Microsoft print server or the Citrix Universal Print Server should be configured with redundancy in order to eliminate a single point of failure. The Citrix Universal Print Server should be defined within a Citrix Policy.

## Experience from the Field

A print media company leverages Thin Clients and Windows-based workstations at the company headquarters. Network based printers are placed throughout the building (one per floor). Windows print servers reside in the datacenter and manage the network printers. XenDesktop and XenApp servers also reside in the datacenter.

A regional office has numerous Windows, Linux and Mac endpoints with network attached printers.

A remote branch office has a few Windows workstations with locally attached printers.

Three different print strategies are applied:

### Headquarters

A Citrix Universal Print Server is used for printing within the XenApp and XenDesktop session. Native print drivers are not required on the Windows based workstations. A session printer policy is configured per floor which connects the floor printer as the default printer. The policies are filtered based on the subnet of the thin client for proximity printing.

Quality of Service (QoS) policies are implemented. Inbound and outbound network traffic on ports TCP 1494 and TCP 2598 are prioritized over all other network traffic. This will prevent HDX user sessions from being impacted by large print jobs.

### Regional Office

A Universal Print Server is deployed within the regional office. The print job uses the Universal Print Driver and is compressed and delivered from the user's session to the Universal Print Server, across the WAN. The job is then sent to the network-attached printer in the office.

### Branch Office

Since all branch users work on Windows based workstations, auto-created client printers in conjunction with the Citrix Universal Printer Driver are used. Since the print job is delivered over ICA, the print data is compressed which saves bandwidth. The Citrix Universal Printer Driver ensures all printers connected to the client can be used within the XenApp or XenDesktop session without concern of the printer model used.

## Applications

Properly integrating an application requires understanding compatibility and how the user/business requirements influences the appropriate delivery method.

### Decision: Compatibility

VDI typically requires significant changes to be made to an organization's application delivery and management strategy. For example, many organizations will take the opportunity to upgrade their desktop operating system and to simplify management by reducing the number of applications installed into the base image using techniques such as application streaming and application layering. These are significant changes that require comprehensive compatibility testing. Important compatibility requirements that may need to be verified include:

- **Operating system** - the application must be compatible with the preferred operating system.
- **Multi-User** - Some applications may be more appropriate for delivery via a hosted shared desktop or a hosted Windows App. In these situations, the compatibility of the application must be verified against the multi-user capabilities of a server operating system like Windows Server 2012R2.
- **Application architecture** - It is important to understand whether the application includes 16-bit, 32-bit or 64-bit code so that an appropriate operating system can be selected. 16-bit code cannot be executed on a 64-bit operating system. However, a 16-bit application can be delivered to users as a Hosted Windows App from a 32-bit desktop-based operating system like x86 editions of Windows 7, 8 or 10.
- **Interoperability** - Some applications may experience complications if they coexist on the same operating system.

Possible causes include shared registry hives, dll files or INI files as well as incompatible dependencies. Application interoperability issues should be identified so that appropriate remediation steps can be taken or an alternative delivery model selected.

- **Dependency** - Applications may need to interact with each other to provide the users with a seamless experience. For example, applications that present information in a PDF format require a suitable PDF viewer to be available. Many times, the dependent (child) applications are version specific to the parent application.
- **Application virtualization** - The use of application virtualization techniques, like streaming and layering, helps to simplify image management by reducing the number of applications installed into the base image. However, not all applications are suitable for streaming and layering because they may install device drivers, use COM+ or form part of the operating system.

Application compatibility can be achieved by doing a combination of manual, user testing, utilizing pre-verified lists maintained by the software vendor, or using an automated application compatibility solution, like Citrix AppDNA which runs through thousands of tests to verify compatibility.

### **Decision: Application Delivery Method**

It is unlikely that a single delivery method will meet all requirements. Based on the outcome of the application categorization assessment process, several application delivery methods can be considered.

Choosing one of the appropriate application delivery method helps improve scalability, management and user experience.

- **Installed app** - The application is part of the base desktop image. The install process involves dll, exe and other files being copied to the image drive as well as registry modifications.
- **Streamed App (Microsoft App-V)** - The application is profiled and delivered to the desktops across the network on-demand. Application files and registry settings are placed in a container on the virtual desktop and are isolated from the base operating system and each other, which helps to address compatibility issues.
- **Hosted Windows App** - The application is installed on a multi-user XenApp host and deployed as an application and not a desktop. The hosted Widnwos app is accessed seamless from the user's VDI desktop or endpoint device, hiding the fact that the app is executing remotely.
- **Local App** - The application is deployed on the endpoint device. The application interface appears within the user's hosted VDI session even though it executes on the endpoint.

The following table provides recommendations on the preferred approaches for integrating applications into the overall solution:

App Category	Installed App	Streamed App	Hosted Windows App	Local App
Common	✓	◦	◦	✗
Departmental	◦	✓	✓	✗
User	✗	◦	◦	✓
Management	✓	✗	◦	✗

"✓": Recommended, "✗": Not Recommended, "◦": Viable

Table 25: App Deployment Recommendations

### Experience from the Field

**Energy** – An energy company installs applications on the base image for the majority of users and streams departmental applications as required.

**Financial** – A banking customer maintains and deploys multiple desktop images containing user group focused applications as required by various departments.

## Virtual Machines

Virtual resources require proper allocation of the processor, memory and disk. These decisions have a direct impact on the amount of hardware required as well as the user experience.

The key to successful resource allocation is to ensure that virtual desktops and applications offer similar levels of performance to physical desktops. Otherwise, productivity and overall user satisfaction will be affected. Allocating resources to the virtual machines above their requirements however is inefficient and expensive for the business.

The resources allocated should be based on the workload characteristic of each user group, identified during the assess phase.

### Decision: Virtual Processor (vCPU)

For hosted desktop-based VDI models (hosted pooled desktops and hosted personal desktops), the general recommendation is two or more vCPUs per virtual machine so that multiple threads can be executed simultaneously. Although a single vCPU could be assigned for extremely light workloads, users are more likely to experience session hangs.

For hosted server-based VDI models (hosted Windows apps, hosted browser apps, hosted shared desktops), the proper vCPU allocation is based on the Non-Uniform Memory Access (NUMA) architecture of the processors.

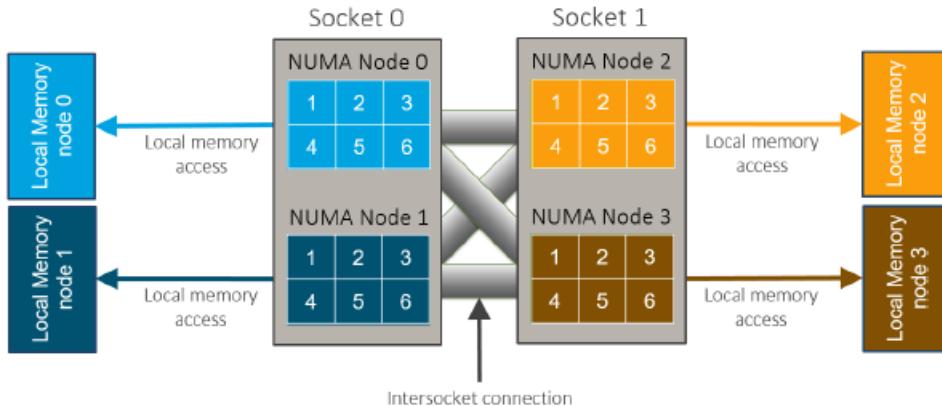


Figure 14: NUMA Architecture

Each socket is divided into one or more NUMA nodes. Hosted server-based VDI models will often utilize 4 or more processors. Allocating more vCPU than the NUMA node contains results in a performance hit. Allocating a portion of a NUMA node to a virtual machine results in a performance hit if the portion allocated is not easily divisible by the size of the NUMA node. It is often ideal to allocate the number of cores within a NUMA node to a virtual machine or allocate ½ of the cores to a virtual machine, while doubling the number of virtual machines.

User Workload	Operating System	vCPU Configured for Scale	vCPU Configured for Experience
Light	Windows 7	2 vCPU	2 vCPU
	Windows 10	2 vCPU	2 vCPU
	Windows 2012R2	NUMA or $\frac{1}{2}$ of NUMA	NUMA or $\frac{1}{2}$ of NUMA
Medium	Windows 7	2 vCPU	3 vCPU
	Windows 10	2 vCPU	3 vCPU
	Windows 2012R2	NUMA or $\frac{1}{2}$ of NUMA	NUMA or $\frac{1}{2}$ of NUMA
Heavy	Windows 7	3 vCPU	4 vCPU
	Windows 10	3 vCPU	4 vCPU
	Windows 2012R2	NUMA or $\frac{1}{2}$ of NUMA	NUMA or $\frac{1}{2}$ of NUMA

Table 26: vCPU Allocation

**Note:** Windows 2012R2 recommendations are based on the hosted Windows app, hosted browser app and hosted shared desktop VDI model.

### Decision: Virtual Memory (vRAM)

The amount of memory allocated to each resource is a function of the user's expected workload and application footprint. Assigning insufficient memory to the virtual machines will cause excessive paging to disk, resulting in a poor user experience; allocating too much RAM increases the overall cost of the solution.

The following table provides guidance on the virtual RAM that should be assigned based on workload:

User Workload	Operating System	vRAM Configured for Scale	vRAM Configured for Experience
Light	Windows 7	2 GB	3 GB
	Windows 10	2 GB	3 GB
	Windows 2012R2	256 MB per user	
Medium	Windows 7	3 GB	4 GB
	Windows 10	3 GB	4 GB
	Windows 2012R2	512 MB per user	
Heavy	Windows 7	6 GB	8 GB
	Windows 10	6 GB	8 GB
	Windows 2012R2	1024 MB per user	

Table 27: vRAM Allocation

**Note:** Windows 2012R2 recommendations are based on the hosted Windows app, hosted browser app and hosted shared desktop VDI model.

**Note:** Memory allocation above 4GB requires a 64-bit operating system.

**Note:** If used, the Machine Creation Services and Provisioning Services cache in RAM amount should be added onto the virtual machine RAM specifications.

### Decision: Disk Cache

The amount of storage that each VM requires will vary based on the workload and the image type. If creating hosted personal desktop without leveraging an image management solution, each VM will require enough storage for the entire OS and locally installed applications.

Deploying machines through Machine Creation Services or Provisioning Services can substantially reduce the storage

requirements for each virtual machine. Disk space requirements for the write cache and difference disk will depend on application usage and user behavior. However, the following table provides a starting point for estimating disk space requirements based on machine sized with vCPU and vRAM as per the guidelines above:

User Workload	Operating System	Storage Space (Differencing Disk / Write Cache Disk)
Light	Windows 7	10 GB
	Windows 10	10 GB
	Windows 2012R2	40 GB
Medium	Windows 7	15 GB
	Windows 10	15 GB
	Windows 2012R2	40 GB
Heavy	Windows 7	20 GB
	Windows 10	20 GB
	Windows 2012R2	40 GB

Table 28: Disk Cache Allocation

### Decision: RAM Cache

Provisioning Services and Machine Creation Services have the capability to utilize a portion of the virtual machine's RAM as a buffer for the storage cache. The RAM cache is used to improve the performance of traditional storage by sharing the virtual machine's non-paged pool memory

User Workload	Operating System	RAM Cache Configured for Scale	RAM Cache Configured for Experience
Light	Windows 7	128 MB	256 MB
	Windows 10	128 MB	256 MB
	Windows 2012R2	2 GB	
Medium	Windows 7	256 MB	512 MB
	Windows 10	256 MB	512 MB
	Windows 2012R2	2 GB	
Heavy	Windows 7	512 MB	1024 MB
	Windows 10	512 MB	1024 MB
	Windows 2012R2	2 GB	

Table 29: RAM Cache Allocation

**Note:** If used, the Machine Creation Services and Provisioning Services cache in RAM amount should be added onto the virtual machine RAM specifications.

**Note:** If additional RAM is available on the host, the RAM Cache amounts can be increased to provide even greater levels of performance.

### Decision: Storage IOPS

Storage performance is limited by the number of operations it can handle per second, referred to as IOPS. Underallocating storage IOPS results in a VDI desktop where apps, web pages and data are slow to load.

The following table provides guidance on the number of storage IOPS generated per user based on workload and operating system. Storage IO activity will be higher during user logon/logoff.

User Workload	Operating System	Storage IOPS (without RAM-Based Cache)	Storage IOPS (with RAM-Based Cache)
Light	Windows 7	10 IOPS	1 IOPS
	Windows 10	12 IOPS	1 IOPS
	Windows 2012R2	3 IOPS	0.5 IOPS
Medium	Windows 7	15 IOPS	1 IOPS
	Windows 10	20 IOPS	1.5 IOPS
	Windows 2012R2	4 IOPS	0.5 IOPS
Heavy	Windows 7	25 IOPS	2 IOPS
	Windows 10	35 IOPS	3 IOPS
	Windows 2012R2	5 IOPS	1.5 IOPS

Table 30: IOPS Allocation

### Decision: Graphics (GPU)

Without a graphical processing unit (GPU), graphical processing is rendered with software by the CPU. A graphical processing unit (GPU) can be leveraged to improve server scalability and user experience or enable the use of graphically intensive applications. During the desktop design it is important to decide how the GPU (if used) will be mapped to the virtual machines. There are three methods available.

- **Pass-Through GPU** - Each physical GPU is passed through to a single virtual machine (hosted apps or hosted desktops).
- **Hardware Virtualized GPU** - Using a hypervisor's vGPU technology, an NVIDIA GRID or Intel Iris Pro is virtualized and shared between multiple machines. Each virtual machine has the full functionality of GPU drivers and direct access to the GPU.
- **Software Virtualized GPU** - The GPU is managed by the hypervisor and intercepts requests made by the VDI desktops. This process is used if a GPU is not installed within the host.

	Pass-Through GPU	Hardware Virtualized GPU (Nvidia)	Hardware Virtualized GPU (Intel)	Software Emulated GPU
<b>Citrix XenServer</b>				
XenDesktop	✓	✓	✓	✓
XenApp	✓	✓	✓	✓
<b>Microsoft Hyper-V</b>				
XenDesktop	✓	✗	✗	✓
XenApp	✓	✗	✗	✓
<b>VMware vSphere</b>				
XenDesktop	✓	✓	✗	✓
XenApp	✓	✓	✗	✓

"✓": Available "✗": Not Supported

Table 31 GPU Allocation Options

User groups with a heavy use of graphical applications will often require the use of a NVidia hardware virtualized GPU. User groups who rely on office-based applications can have an observable benefit with the use of a hardware virtualized GPU from Intel.

### Layer 4: The Control Layer

## Active Directory

### Decision: Forest Design

Multi-forest deployments, by default, do not have inter-domain trust relationships between the forests. An Active Directory administrator can establish trust relationships between the multiple forests, allowing the users and computers from one forest to authenticate and access resources in another forest.

For forests that have inter-domain trusts, Citrix recommends that the appropriate settings be configured to allow the Delivery Controllers to communicate with both domains. When the appropriate trusts are not configured, multiple XenDesktop sites for each forest must be configured. This section outlines the storage requirements on a per product basis and provides sizing calculations. For more information, please refer to Citrix article: [CTX134971 - Successfully Deploying XenDesktop in a Complex Active Directory Environment](#).

### Decision: Organizational Unit Structure

Infrastructure components for a XenApp and XenDesktop deployment should reside within their own dedicated organizational units (OUs); separating workers and controllers for management purposes. By having their own OUs, the objects inside will have greater flexibility with their management while allowing Citrix administrators to be granted delegated control.

A sample Citrix OU structure can be seen below.

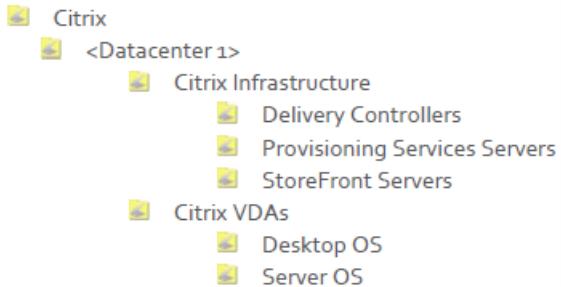


Figure 15: Example Citrix OU Structure

### Decision: User Groups

Whenever possible, permissions and authorization should be assigned to user groups rather than individual users, thereby eliminating the need to edit a large amount of resource permissions and user rights when creating, modifying, or deleting user accounts.

Permission application example:

- An application published to one group of 1,000 users requires the validation of only one object for all 1,000 users.
- The same application published to 1,000 individual user accounts requires the validation of all 1,000 objects.

## Database

The majority of Citrix products discussed within this document require a database. The following table outlines the usage on a per product basis:

Product	Configuration Data	Runtime Data	Audit / Change Log Data	Monitoring Data
XenDesktop	✓	✓	✓	✓
Provisioning Services	✓		①	
XenClient	✓	✓	✓	

"①": Optional

Table 32: Database usage

## Decision: Edition

There are multiple editions of Microsoft SQL Server 2012: Express, Web, Standard, Business Intelligence, and Enterprise. Based on the capabilities of the various SQL Server editions available, the Standard edition is often used for hosting the XenApp and XenDesktop databases in production environments.

The Standard edition provides an adequate amount of features to meet the needs of most environments. For more information on the databases supported with Citrix products please refer to the Citrix Database Support Matrix. Different versions of Citrix products support different versions of the SQL server; therefore it is important to check the support matrix to ensure the version of SQL server used is compatible with the Citrix product being deployed.

## Decision: Database Server Sizing

The SQL server must be sized correctly to ensure the performance and stability of an environment. Since every Citrix product uses SQL server in a different way, no generic all-encompassing sizing recommendations can be provided. Instead, per-product SQL server sizing recommendations are provided below.

### XenApp and XenDesktop

XenApp and XenDesktop Brokers use the database as a message bus for broker communications, storing configuration data and storing monitoring and configuration log data. The databases are constantly in use and the performance impact on the SQL server can be considered as high.

Based on results from Citrix internal scalability testing the following SQL server specification for a server hosting all XenDesktop databases are recommended:

- 2 Cores / 4 GB RAM for environments up to 5,000 users
- 4 Cores / 8 GB RAM for environments up to 15,000 users
- 8 Cores / 16 GB RAM for environments with 15,000+ users

The database files and transaction logs should be hosted on separate hard disk subsystems in order to cope with a high number of transactions. For example, registering 20,000 virtual desktops during a 15 minute boot storm causes ~500 transactions / second and 20,000 users logging on during a 30 minute logon storm causes ~800 transactions / second on the XenDesktop Site Database.

### Provisioning Services

In addition to static configuration data provisioning servers store runtime and auditing information in the database. Depending on the boot and management pattern, the performance impact of the database can be considered as low to medium.

Based on this categorization, a SQL server specification of 4 Cores and 4 GB RAM is recommended as a good starting point. The SQL server should be carefully monitored during the testing and pilot phase in order to determine the

optimal configuration of the SQL server.

## Decision: Instance Sizing

When sizing a SQL database, two aspects are important:

- **Database file** - Contains the data and objects such as tables, indexes, stored procedures and views stored in the database.
- **Transaction log file** - Contains a record of all transactions and database modifications made by each transaction. The transaction log is a critical component of the database and, if there is a system failure, the transaction log might be required to bring the database back to a consistent state. The usage of the transaction log varies depending on which database recovery model is used:
  - **Simple recovery** - No log backups required. Log space is automatically reclaimed, to keep space requirements small, essentially eliminating the need to manage the transaction log space. Changes to the database since the most recent backup are unprotected. In the event of a disaster, those changes must be redone.
  - **Full recovery** - Requires log backups. No work is lost due to a lost or damaged database data file. Data of any arbitrary point in time can be recovered (for example, prior to application or user error). Full recovery is required for database mirroring.
  - **Bulk-logged** - Requires log backups. This is an adjunct of the full recovery model that permits high-performance bulk copy operations. It is typically not used for Citrix databases.

For further information, please refer to the [Microsoft Developer Network – SQL Server Recovery Models](#).

In order to estimate storage requirements, it is important to understand the disk space consumption for common database entries. This section outlines the storage requirements on a per product basis and provides sizing calculations. For more information, please refer to Citrix article: CTX139508 – [XenDesktop 7.x Database Sizing](#).

## XenDesktop General

XenApp 7.x and XenDesktop 7.x use three distinct databases:

- **Site Configuration database** - Contains static configuration and dynamic runtime data
- **Monitoring database** - Contains monitoring data which is accessible through Director
- **Configuration logging database** - Contains a record for each administrative change performed within the site (accessible through Studio)

## Site Database

Since the database of a XenApp or XenDesktop site contains static configuration data and dynamic runtime data, the size of the database file depends not only on the physical size of the environment but also user patterns. The following factors all impact the size of the database file:

- The number of connected sessions
- The number of configured and registered VDAs
- The number of transactions occurring during logon
- The VDA heartbeat transactions

The size of the Site Database is based on the number of VDAs and active sessions. The following table shows the typical maximum database size Citrix observed when scale testing XenApp and XenDesktop with a sample number of users, applications, and desktop delivery methods.

Users	Applications	Desktop Types	Expected Maximum Size (MB)
1,000	50	Hosted Shared	30
10,000	100	Hosted Shared	60
100,000	200	Hosted Shared	330
1,000	N/A	Hosted Pooled	30
10,000	N/A	Hosted Pooled	115
40,000	N/A	Hosted Pooled	390

Table 33: XenDesktop Site DB sample size calculations

**Note:** This sizing information is a guide only. Actual database sizes may differ slightly by deployment due to how databases are maintained.

Determining the size of the transaction log for the Site database is difficult due to factors that can influence the log including:

- The SQL Database recovery model
- The launch rate at peak times
- The number of desktops being delivered

During XenDesktop scalability testing, Citrix observed the transaction log growth rate at 3.5MB an hour when the system is idle, and a per user per day growth rate of ~32KB. In a large environment, transaction log usage requires careful management and a regular backup, to prevent excessive growth. This can be achieved by means of scheduled jobs or maintenance plans

## Monitoring Database

Of the three databases, the Monitoring database is expected to be the largest since it contains historical information for the site. Its size is dependent on many factors including:

- Number of Users
- Number of sessions and connections
- Number of workers
- Retention period configuration – Platinum customers can keep data for over a year (default 90 days). Non-platinum customers can keep data for up to 7 days (default 7 days).
- Number of transaction per second. Monitoring service tends to execute updates in batches. It is rare to have the number of transactions per second go above 20.
- Background transaction caused by regular consolidation calls from the Monitoring service.
- Overnight processing carried out to remove data outside the configured retention period.

The following table shows the estimated size of the Monitoring database over a period of time under different scenarios. This data is an estimate based on data seen within scale testing XenApp and XenDesktop (assuming a 5 day working week).

Estimates with 1 connection and 1 session per user with a 5 day work week					
Users	Type	1 week (MB)	1 month (MB)	3 months (MB)	1 year (MB)
1,000	HSD	20	70	230	900
10,000	HSD	160	600	1,950	7,700
100,000	HSD	1,500	5,900	19,000	76,000
1,000	VDI	15	55	170	670
10,000	VDI	120	440	1,400	5,500
40,000	VDI	464	1,700	5,400	21,500
Estimates with 2 connections and 1 session per user with a 5 day work week					
Users	Type	1 week (MB)	1 month (MB)	3 months (MB)	1 year (MB)
1,000	HSD	30	100	330	1,300
10,000	HSD	240	925	3,000	12,000
100,000	HSD	2,400	9,200	30,000	119,000
1,000	VDI	25	85	280	1,100
10,000	VDI	200	750	2,500	9,800
40,000	VDI	800	3,000	9,700	38,600

Table 34: Monitoring DB size estimations

**Note:** The 100,000 HSD tests are based on a test environment consisting of:

- 2 Delivery Controllers
- 43 Hosted Shared Desktop workers
- 3 SQL servers, configured with databases held within one Always On Availability Group

For more information please see the Citrix Support article [XenDesktop 7.x Database Sizing](#).

The size of the transaction log for the Monitoring Database is very hard to estimate, but XenApp and XenDesktop scalability testing showed a growth rate of about 30.5 MB an hour when the system is idle, and a per user per day growth rate of ~9 KB.

## Configuration Logging Database

The Configuration Logging Database is typically the smallest of the three databases. Its size and the size of the related transaction log depends on the daily administrative activities initiated from Studio, Director or PowerShell scripts, therefore its size is difficult to estimate. The more configuration changes are performed, the larger the database will grow. Some factors that can affect the size of the database include:

- The number of actions performed in Studio, Director and PowerShell.
- Minimal transactions which occur on the database when no configuration changes are taking place.
- The transaction rate during updates. Updates are batched whenever possible.
- Data manually removed from the database. Data within the Configuration Logging Database is not subject to any retention policy, therefore it is not removed unless done so manually by an administrator.
- Activities that have an impact on sessions or users, for example, session logoff and reset.
- The mechanism used for deploying desktops.

In XenApp environments not using MCS, the database size tends to fall between 30 and 40MB. For MCS environments, database size can easily exceed 200MB due to the logging of all VM build data.

## Temporary Database

In addition to the Site, Monitoring, and Configuration Logging databases, a system-wide temporary database (tempdb) is provided by SQL Server. This temporary database is used to store Read-Committed Snapshot Isolation data. XenApp 7.x and XenDesktop 7.x uses this SQL Server feature to reduce lock contention on the XenApp and XenDesktop databases. Citrix recommends that all XenApp 7.x and XenDesktop 7.x databases use Read-Committed Snapshot Isolation. For more information please see How to Enable Read-Committed Snapshot in XenDesktop.

The size of the tempdb database will depend on the number of active transactions, but in general it is not expected to grow more than a few MBs. The performance of the tempdb database does not impact the performance of XenApp and XenDesktop brokering, as any transactions that generate new data require tempdb space. XenApp and XenDesktop tend to have short-lived transactions, which help keep the size of the tempdb small.

The tempdb is also used when queries generate large intermediate result sets. Guidance and sizing the tempdb can be found on the Microsoft TechNet article Optimizing tempdb Performance.

## Provisioning Services

The Provisioning Services farm database contains static configuration and configuration logging (audit trail) data. The record size requirements outlined below can be used to help size the database:

Configuration Item	DB Space Required (KB)	Number of Items (Example)	Total (KB)
Base farm configuration	112	-	112
User group w/ farm access	50	10	250
Site	4	5	20
Device collection	10	50	500
Farm view	4	10	40
Farm view to device relationship	5	1	5,000
Site View	4	5	20
Site view to device relationship	5	1	5,000
Device	2	5,000	10,000
Device bootstrap	10	-	-
Device to disk relationship	35	1	175,000
Device printer relationship	1	-	-
Device personality data	1	-	-
Device status (when booted)	1	5,000	5,000
Device custom property	2	-	-
vDisk	1	20	20
vDisk version	3	5	300
Disk locator	10	1	200
Disk locator custom property	2	-	-
Server	5	10	50
Server IP	2	1	20
Server status (when booted)	1	20	20
Server custom property	2	-	-
vDisk store	8	5	40
vDisk store to server relationship	4	1	40
Connection to XenServer (VirtualHostingPool)	4	-	-
vDisk update task	10	10	100
Administrative change (auditing enabled)	1	10,000	10,000
<b>Total</b>			<b>211,732KB (~212MB)</b>

Table 35: Provisioning Services Farm DB sample size calculations

During the PVS farm setup, a database with an initial file size of 20MB is created. Due to the nature of the data in the PVS

farm database the transaction log is not expected to grow very quickly, unless a large amount of configuration is performed.

In contrast to XenApp, which also offers the ability to track administrative changes, the related information is not written to a dedicated database but directly to the Provisioning Services farm database. In order to limit the size of the Provisioning Services database it is recommended to archive the audit trail data on a regular schedule.

### Decision: Database Location

By default, the Configuration Logging and Monitoring databases are located within the Site Configuration database. Citrix recommends changing the location of these secondary databases as soon as the configuration of the site has been completed, in order to simplify sizing, maintenance and monitoring. All three databases can be hosted on the same server or on different servers. An ideal configuration would be to host the Monitoring database on a different server from the Site Configuration and Configuration Logging databases since it records more data, changes occur more frequently and the data is not considered to be as critical as the other databases. For more information, please see [Change secondary database locations](#) in the Citrix Product Documentation.

**Note:** The location of the Configuration Logging database cannot be changed when mandatory logging is enabled.

### Decision: High-Availability

The following table highlights the impact to XenApp, XenDesktop and Provisioning Services when there is a database outage:

Component	Impact of Database Outage
Site configuration database	<p>Users will be unable to connect or reconnect to a virtual desktop.</p> <p><i>Note: Connection leasing in XenApp and XenDesktop 7.6 allows users with Hosted Shared Desktops, Hosted Windows and Browser Applications, and Personal Desktops to reconnect to their most recently used applications and desktops even when the site database is unavailable.</i></p>
Monitoring database	<p>Director will not display any historical data and Studio cannot be started.</p> <p>Brokering of incoming user requests and existing user sessions will not be affected.</p>
Configuration logging database	<p>If allow changes when the database is disconnected has been enabled within XenApp and XenDesktop logging preferences, an outage of the configuration logging database will have no impact (other than configuration changes not being logged). Otherwise, administrators will be unable to make any changes to the XenApp and XenDesktop site configuration. Users are not impacted.</p>
Provisioning Services farm database	<p>When offline database support is enabled and the database becomes unavailable, the stream process uses a local copy of the database to retrieve information about the provisioning server and the target devices supported by the server. This allows provisioning servers and the target devices to remain operational. However, when the database is offline, the console and the management functions listed below become unavailable:</p> <ul style="list-style-type: none"><li>• AutoAdd target devices</li><li>• vDisk creation and updates</li><li>• Active Directory password changes</li><li>• Stream process startup</li><li>• Image update service</li><li>• PowerShell and MCLI based management</li></ul> <p>If offline database support has not been enabled, all management functions become unavailable and the boot and failover of target devices will fail.</p>

Table 36: Impact of a database outage

**Note:** Please review HA options for 3rd party databases (for example, App-V, SCVMM or vCenter) with the respective

software vendor.

In addition to the built-in database redundancy options, Microsoft SQL Server, as well as the underlying hypervisor (in virtual environments), offer a number of high availability features. These enable administrators to ensure single server outages will have a minimal impact (if any) on the XenApp and XenDesktop infrastructure. The following the SQL / hypervisor high availability features are available:

**VM-level HA** - This high availability option is available for virtual SQL servers only, which need to be marked for High Availability at the hypervisor layer. In case of an unexpected shutdown of the virtual machine or the underlying hypervisor host, the hypervisor will try to restart the VM immediately on a different host. While VM-level HA can minimize downtimes in power-outage scenarios, it cannot protect from operating system level corruption. This solution is less expensive than mirroring or clustering because it uses a built-in hypervisor feature. However, the automatic failover process is slower, as it can take time detect an outage and start the virtual SQL server on another host. This may interrupt the service to users.

- **Mirroring** - Database mirroring increases database availability with almost instantaneous failover. Database mirroring can be used to maintain a single standby or mirror database, for a corresponding principal or production database. Database mirroring runs with either synchronous operation in high-safety mode, or asynchronous operation in high-performance mode. In high-safety mode with automatic failover (recommended for XenDesktop) a third server instance, known as a witness, is required, which enables the mirror server to act as a hot standby server. Failover from the principal database to the mirror database happens automatically and is typically completed within a few seconds. It is a good practice to enable VM-level HA (or a similar automatic restart functionality) for at least the witness to ensure SQL service availability in case of a multi-server outage.

**Note:** Microsoft is planning to remove mirroring as a high availability option in a future release of SQL Server and is discouraging its use in new network development. Please refer to the Microsoft article [Database Mirroring \(SQL Server\)](#) for more information.

- **AlwaysOn Failover Cluster Instances** - Failover clustering provides high-availability support for an entire instance of Microsoft SQL Server. A failover cluster is a combination of two or more nodes, or servers, using a shared storage. A Microsoft SQL Server AlwaysOn Failover Cluster Instance, introduced in SQL Server 2012, appears on the network as a single computer, but has functionality that provides failover from one node to another if the current node becomes unavailable. The transition from one node to the other node is seamless for the clients connected to the cluster. AlwaysOn Failover cluster Instances require a Windows Server Failover Clustering (WSFC) resource group. The number of nodes supported in the WSFC resource group will depend on the SQL Server edition. (Please refer to the table in the Decision: Edition earlier in this chapter.) For more information please refer to MSDN – AlwaysOn Failover Cluster Instances (SQL Server).
- **AlwaysOn Availability Groups** - AlwaysOn Availability Groups is an enterprise-level high-availability and disaster recovery solution introduced in Microsoft SQL Server 2012, which enables administrators to maximize availability for one or more user databases. AlwaysOn Availability Groups require that the Microsoft SQL Server instances reside on Windows Server failover clustering (WSFC) nodes. Similar to failover clustering a single virtual IP / network name is exposed to the database users. In contrast to failover clustering, shared storage is not required since the data is transferred using a network connection. Both synchronous and asynchronous replication to one or more secondary servers is supported. As opposed to mirroring or clustering secondary servers can be actively used for processing incoming read-only requests, backups or integrity checks. This feature can be used to offload user resource enumeration requests to a secondary SQL server in XenDesktop environments to essentially scale-out a SQL server infrastructure. Since the data on active secondary servers can lag multiple seconds behind the primary server, the read-only routing feature cannot be used for other XenDesktop database requests at this point in time. For more information, please refer to MSDN – AlwaysOn Availability Groups (SQL Server).

The following table outlines the recommended high availability features for Citrix databases:

Component	VM-Level HA	Mirroring	AlwaysOn Failover Cluster Instances	AlwaysOn Availability Groups
Site database	①	✓	○	○
Configuration logging database	①	○	○	○
Monitoring database	①	✓	○	○
Provisioning Services farm database	①	✓	○	✗
XenClient database	①	✗	○	○

"✓": Recommended "○": Viable "✗": Not Supported "①": Recommended for test environments only

Table 37: Recommended SQL high availability options

## Decision: Connection Leasing

Connection leasing is a new XenApp and XenDesktop 7.6 feature that allows Hosted Shared, Hosted Windows and Browser Apps and Personal VDI users to connect and reconnect to their most recently used applications and desktops, even when the site database is unavailable. Connection Leasing is not available for users with a Pooled VDI desktop.

The lease information along with the application, desktop, icon, and worker information is stored on the controller's local disk and synchronized between controllers in the site. If the site database becomes unavailable, the controllers enter a "leased connection mode" and replay cached operations from an XML file on the local disk to connect or reconnect users to a recently used application or desktop.

Administrators familiar with the local host cache in XenApp 6.5 and earlier should understand the similarities and differences with connection leasing because it can have an impact on the design and scalability of the XenApp and XenDesktop 7.6 solution. In XenApp 6.5 and earlier, the IMA service is responsible for synchronizing the local host cache with the data store. In XenApp and XenDesktop 7.6, the FMA service caches the brokering operations (leases) to an XML file containing the address of the VDA, application path, and other details required for the session to launch. The FMA also caches dynamic information such as user sessions, VDA registrations, and load. These files are uploaded to the SQL database and synchronized between all controllers in the site. The controllers will download the files on a regular basis so that any other controller in the site can connect a user to their session.

Each controller needs additional disk space for the cached lease files. At a minimum, 4KB is required for each lease file. Each resource entry in the enumeration lease will take anywhere from 200 bytes to a few KBs depending on the number of entries and resources published. Citrix testing has shown that 200,000 leased connections for server hosted applications and desktops required approximately 3GB of disk space. 40,000 leased connections for assigned desktops required approximately 156MB of disk space.

By default, connection leases have an expiration period of two weeks. Applications and desktops must have been launched within the two last weeks to still be accessible when the database is unavailable. The expiration period is configurable using PowerShell cmdlets or editing the registry and can be set from 0 minutes to several years. Setting the expiration period too short will prevent users from connecting to their virtual desktops and applications in the event of an outage. Setting the expiration period too long will increase storage requirement on the controllers.

By default, connection leasing affects the entire site, however, leases can be revoked for specific users, which prevents them from accessing any applications or desktops when the site database is unavailable.

For more information on connection leasing considerations and configuration, please refer to eDocs – Connection Leasing.

## Citrix Licensing

Citrix offers organizations the flexibility of multiple licensing models that align with common usage scenarios. The different licensing models vary based on the Citrix product used, but can include per user/device and per concurrent user. Several Citrix products use the license server, while other products require a license to be installed on the product itself.

# 第三方声明

May 28, 2016

XenApp and XenDesktop 7.6 may include third party software licensed under the terms defined in the following documents:

- [XenApp 7.6 and XenDesktop 7.6 Third Party Notices](#)
- [FlexNet Publisher Documentation Supplement: Software Licenses](#)