关于此版本

新增功能

-
-
-
-
-
-
-
-
-
  -
  -
  -
-
-
-

-
  -
    -
    -
    -
    -
-
-
-
-
-
-
-
-
-
-
-
-

本版本中已修复的问题

本版本中的已知问题

Citrix Receiver for Windows 4.2 已修复的问题

Receiver for Windows 4.2.100

-
-
-
-
  -
  -

-
-
-
  -
  -
  -
-
-
-
-
-
-

-
-
-
-
-
-
-
-
-
-
-
-

-
-
-
-
-
-

Receiver for Windows 4.2

-
-
-
-
-

-
-
-
-
-
-
-
-
-
-
-
  -
  -

-
-
-
-
-
-
-
-
-
-
-
-

-
-
-
-
-
-
-
-
-
-
-
  -
  -
  -
  -
-

-
-
-

Citrix Receiver for Windows 4.2 的已知问题

已知问题

-
-
-
-
-
-
-
-
-
-
-

-
-
-
-
-
-
    -
    -

-

系统要求

设备

操作系统

-
-
-
-
-
-
-
-
-
-

硬件

-
-
-

支持触摸的设备

Citrix 服务器

-
  -
  -
  -
  -
  -
  -
-
  -
  -
  -
  -
  -
  -

浏览器

连接

-
-
-

关于安全连接和证书

身份验证

升级

其他

-
  -
  -
  -
-
-
  -
  -

安装 Receiver for Windows

-
  -
  -
  -
-
  -
-
  -

手动升级到 Receiver for Windows

-
-
-
-

升级注意事项

从版本 3.4 升级到 4.2.100 时的重要注意事项

手动安装和卸载 Receiver for Windows

删除 Receiver for Windows

使用命令行参数配置和安装 Receiver for Windows

-
-
-
-
-
  -
  -
  -

-
-
-

-
-
-
-
-
-
-

-
  -
  -
  -
  -
    元素中的 URL。
  -
  -
  -
  -
  -

CitrixReceiver.exe /silent STORE0="AppStore;https://testserver.net/Citrix/MyStore/discovery;on;HR App Store" STORE1="BackUpAppStore;https://testserver.net/Citrix/MyBackupStore/discovery;on;Backup HR App Store"

CitrixReceiver.exe /INCLUDESSON /STORE0="PNAgent;https://testserver.net/Citrix/PNAgent/config.xml;on;My PNAgent Site"

从命令行启动虚拟桌面或应用程序

使用 Active Directory 和示例启动脚本部署 Receiver for Windows

-
-

修改示例脚本

- 设置 DesiredVersion= 3.3.0.XXXX
-
-
-

添加“每计算机启动脚本”

每计算机部署 Receiver

每计算机删除 Receiver

设置“每用户启动脚本”

-
-

每用户部署 Receiver

每用户删除 Receiver

从 Receiver for Web 部署 Receiver for Windows

从 Web Interface 登录屏幕部署 Receiver for Windows

配置 Receiver for Windows

-
-
-
  -
  -
  -
-
-

配置自助服务模式

-

-

配置 StoreFront

配置应用程序交付

-
-
-

配置自助服务模式

-
-
-

自定义应用程序快捷方式的位置

SelfServiceMode true SelfServiceMode false

- SelfServiceMode false
-
-
-
- UseCategoryAsStartMenuPath
- [/DESKTOPDIR="Dir_name"] CategoryPath
- AutoReInstallModifiedApps

使用组策略对象模板自定义应用程序快捷方式的位置

-
-
-
-
-
-
-

使用注册表项自定义应用程序快捷方式的位置

使用 StoreFront 帐户设置自定义应用程序快捷方式的位置

-
-
-

-
-
-
-
-

使用 XenApp 和 XenDesktop 7.x 中的每应用程序设置自定义应用程序快捷方式的位置

使用 XenApp 7.6 中的每应用程序设置自定义应用程序快捷方式的位置

缩短枚举延迟或对应用程序存根进行数字签名

示例用例

配置本地应用程序访问应用程序

-

-

配置 XenDesktop 环境

为 XenDesktop 和 XenApp 连接配置 USB 支持

-
-
-

-
-
-
-

-
-
-
-
-
-

USB 支持的工作原理

大容量存储设备

默认情况下允许连接的 USB 设备类

-
-
-
-

-
  -
  -
  -
  -
  -
  -
-
-
-
-
-

默认情况下拒绝连接的 USB 设备类

-
-
-
-
-
-

更新可进行远程连接的 USB 设备列表

配置 Bloomberg 键盘

-
-

防止 Desktop Viewer 窗口变暗

-
-

-

-

配置面向多个用户和设备的设置

-
-
-

配置 StoreFront

配置 StoreFront

使用组策略对象模板配置 Receiver

-
-
-
-

Sales Store;https://sales.mycompany.com/Citrix/Store/discovery;On;Store for Sales staff

向用户提供帐户信息

-
-
-

配置基于电子邮件的帐户发现

向用户提供置备文件

-

向用户提供需手动输入的帐户信息

-
-
  -
  - NetScalerGatewayFQDN?MyStoreName

优化 Receiver 环境

缩短应用程序启动时间

-
-
-
-

HKLM 注册表值

HKCU 注册表值

映射客户端设备

-
-
-

关闭用户设备映射

重定向客户端文件夹

将客户端驱动器映射到主机端驱动器盘符

HDX Plug and Play USB 设备重定向

将客户端 COM 端口映射到服务器 COM 端口

支持 DNS 名称解析

对特定用户设备禁用 DNS 名称解析

将代理服务器与 XenDesktop 连接结合使用

Nov 19, 2015

如果在您的环境中没有使用代理服务器，请更正在 Windows XP 上运行 Internet Explorer 7.0 的任意用户设备上的 Internet Explorer 代理设置。默认情况下，此配置会自动检测代理设置。如果未使用代理服务器，用户将在检测过程中遇到不必要的延迟。有关更改代理设置的说明，请参考您的 Internet Explorer 文档。或者，您也可以使用 Web Interface 更改代理设置。有关详细信息，请参阅 Web Interface 文档。

提升用户体验

Nov 19, 2015

可以通过以下功能提升用户的体验：

Receiver 支持多客户端麦克风输入。本地安装的麦克风可用于：

- 实时活动，例如软件电话通话和网络会议。
- 托管的录制应用程序，例如听写程序。
- 视频和音频录制。

Receiver 用户可以选择是否要通过更改连接中心设置使用连接到其设备的麦克风。XenDesktop 用户还可以使用 XenDesktop Viewer 首选项禁用自己的麦克风和网络摄像机。

最多可以将八个监视器与 Receiver 结合使用。

会话可以按照以下两种方式跨多个监视器进行：

- 全屏模式，会话中显示多个监视器，应用程序如同在本地一样显示到这些监视器中。
  XenDesktop：要跨任何矩形排列的监视器子集显示 Desktop Viewer 窗口，请跨这些监视器的任意部分调整窗口的大小，然后按最大化按钮。
- 窗口模式，会话中显示单个监视器图像，应用程序不会显示到各个监视器中。

XenDesktop：当同一分配（以前称为“桌面组”）中的任意桌面随后启动时，窗口设置会保留，该桌面会跨相同的监视器显示。如果监视器按矩形排列，则一台设备上可以显示多个虚拟桌面。如果 XenDesktop 会话使用设备上的主监视器，该监视器将成为会话中的主监视器。否则，会话中编号最小的监视器将成为主监视器。

要启用多监视器支持，请确保满足以下各项：

- 用户设备配置为支持多个监视器。
- 用户设备的操作系统必须能够检测到每个监视器。在 Windows 平台上，要验证此检测过程是否发生，请在用户设备上查看显示属性对话框中的设置选项卡，确认每个监视器都单独显示出来。
- 检测到监视器之后：
  - **XenDesktop：**使用 Citrix 计算机策略设置显示内存限制来配置图形内存限制。
  - **XenApp：**根据所安装的 XenApp 服务器的版本执行以下操作：
    - 使用 Citrix 计算机策略设置显示内存限制配置图形内存限制。
    - 在 XenApp 服务器的 Citrix 管理控制台中选择场，在任务窗格中依次选择修改服务器属性 > 修改所有属性 > 服务器默认值 > HDX Broadcast > 显示（或修改服务器属性 > 修改所有属性 > 服务器默认值 > ICA > 显示），并设置用于每个会话的图形的最大内存。

请确保设置足够大的值（以 KB 为单位），以提供足够的图形内存。如果设置的值不够大，已发布应用程序会限制在不超出指定大小的一部分监视器内。

有关为 XenApp 和 XenDesktop 计算会话内存图形要求的信息，请参阅 ctx115637。

如果启用了通用打印优化默认值策略设置允许非管理员修改这些设置，用户可以覆盖在该策略设置中指定的图像压缩和图像和

字体缓存选项。

覆盖用户设备上的打印机设置

1. 在用户设备上，从应用程序中提供的打印菜单中选择属性。
2. 在客户端设置选项卡上，单击高级优化，并对图像压缩和图像和字体缓存选项进行更改。

Receiver 会在您激活文本输入字段时以及设备处于帐篷模式或平板电脑模式时自动显示屏幕键盘，以允许您从 Windows 平板电脑触控访问虚拟应用程序和桌面。

在某些情况下的某些设备上，Receiver 无法准确检测设备的模式，并且屏幕键盘可能会在您不希望其显示时出现。

要在使用可转换设备（带有可拆卸键盘的平板电脑）时禁止显示屏幕键盘，请在 HKLM\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver 中创建 REG_DWORD 值 DisableKeyboardPopup，并将该值设置为 1。
注意：在 64 位计算机上，请在 HKLM\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver 中创建该值

可以配置 Receiver 解释为具有特殊功能的组合键。启用键盘快捷方式策略之后，可以指定 Citrix 热键映射、Windows 热键的行为以及会话的键盘布局。

1. 以管理员身份从开始菜单本地运行 gpedit.msc（将策略应用于单台计算机时）或者使用组策略管理控制台（应用域策略时），打开组策略编辑器。

   注意：如果已将 icaclient 模板导入到“组策略编辑器”中，可以忽略步骤 2 到 5。
2. 在组策略编辑器的左窗格中，选择“管理模板”文件夹。
3. 在操作菜单中，选择添加/删除模板。
4. 选择添加，浏览到 Receiver 的 Configuration 文件夹（路径通常为 C:\Program Files\Citrix\ICA Client\Configuration），然后选择 icaclient.adm。
5. 选择打开以添加模板，然后选择关闭以返回到组策略编辑器。
6. 在组策略编辑器中，依次转至管理模板 > 经典管理模板(ADM) > Citrix 组件 > Citrix Receiver > 用户体验 > 键盘快捷方式。
7. 在操作菜单中，依次选择属性、已启用，然后选择所需的选项。

Receiver 支持 32 位高位颜色图标，并且可以为 Citrix 连接中心对话框、“开始”菜单以及任务栏中可见的应用程序自动选择颜色深度，以提供无缝应用程序。

警告：注册表编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因“注册表编辑器”使用不当导致出现的问题能够得以解决。使用“注册表编辑器”需自担风险。在编辑注册表之前，请务必进行备份。
要设置首选的颜色深度，可以将名为 TWIDesiredIconColor 的字符串注册表项添加到 HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Preferences 中，并将其设置为所需的值。图标可能的颜色深度为 4、8、16、24 和 32 位/像素。如果网络连接速度较慢，用户可以为图标选择较低的颜色深度。

不同的企业会有不同的企业需求。您对用户访问虚拟桌面的方式的要求也因用户的不同和企业需求的变化而不同。连接到虚拟桌面时的用户体验以及用户参与配置连接的程度取决于您如何设置 Receiver for Windows。

当用户需要与其虚拟桌面交互时，请使用 **Desktop Viewer**。用户的虚拟桌面可以是已发布的虚拟桌面，也可以是共享或专用桌面。在这种访问方案中，Desktop Viewer 工具栏功能允许用户在窗口中打开虚拟桌面并在其本地桌面内平移和缩放该桌面。用户可以使用同一用户设备上的多个 XenDesktop 连接来设置首选项和使用多个桌面。

注意：用户必须使用 Citrix Receiver 更改其虚拟桌面上的屏幕分辨率。无法使用 Windows“控制面板”更改屏幕分辨率。

在 Desktop Viewer 会话中，Windows 徽标键+L 指向本地计算机。

Ctrl+Alt+Delete 指向本地计算机。

激活粘滞键、筛选键和切换键（Microsoft 辅助功能）的按键始终指向本地计算机。

作为 Desktop Viewer 的一项辅助功能，按 Ctrl+Alt+Break 将在弹出窗口中显示 Desktop Viewer 工具栏按钮。

Ctrl+Esc 发送到远程虚拟桌面。

注意：默认情况下，如果将 Desktop Viewer 最大化，Alt+Tab 将在会话内部的窗口之间切换焦点窗口。如果 Desktop Viewer 显示在某个窗口中，Alt+Tab 将在会话外部的窗口之间切换焦点窗口。
热键序列是由 Citrix 设计的键组合。例如，Ctrl+F1 序列将重现 Ctrl+Alt+Delete，Shift+F2 将在全屏模式和窗口模式之间切换应用程序。不能对 Desktop Viewer 中显示的虚拟桌面（即，对 XenDesktop 会话）使用热键序列，但可以对已发布的应用程序（即，对 XenApp 会话）使用热键序列。

在桌面会话中，用户无法连接到同一个虚拟桌面。尝试执行此操作将断开与现有桌面会话的连接。因此，Citrix 建议：

- 管理员不应该将桌面上的客户端配置为指向发布同一桌面的站点
- 用户不应该浏览承载同一桌面，并且已配置为自动将用户重新连接到现有会话的站点。
- 用户不应该浏览承载同一桌面的站点，并尝试启动该站点

请注意，用户本地登录到用作虚拟桌面的计算机会阻止与该桌面进行连接。

如果用户从虚拟桌面连接到使用 XenApp 发布的虚拟应用程序，并且您的组织具有单独的 XenApp 管理员，Citrix 建议您与他们一起协作来定义设备映射，以便在桌面和应用程序会话中的桌面设备映射具有一致性。在桌面会话中，本地驱动器显示为网络驱动器，因此 XenApp 管理员必须更改驱动器映射策略，以包含网络驱动器。

确保连接安全

Nov 19, 2015

为了最大限度地提高环境的安全性，必须保障 Receiver 与您所发布的资源之间的连接安全。可以为 Receiver 软件配置多种类型的身份验证，包括智能卡身份验证、证书吊销列表检查以及 Kerberos 直通身份验证。

Windows 计算机默认支持 Windows NT 质询/响应 (NTLM) 身份验证。

配置域直通身份验证

Nov 19, 2015

本主题介绍了如何通过 XenDesktop 或 XenApp 为 Citrix Receiver 启用域直通身份验证。

注意：在此示例中，在客户端操作系统中安装 Receiver、应用计算机策略以及配置可信站点都是手动完成的。构建组策略对象 (GPO) 模板后，可以将其应用于安装了 Receiver 的任何域客户端计算机。

1. 使用 /includeSSON 开关安装 Citrix Receiver 4.2。
    1. 安装一个或多个 StoreFront 应用商店。可以稍后完成此步骤。安装 StoreFront 应用商店并不是设置域直通身份验证的必备条件。有关添加一个或多个 StoreFront 应用商店的语法信息，请参阅使用命令行参数配置和安装 Receiver for Windows。
    2. 通过启动 Citrix Receiver 检查是否已启用直通身份验证，然后确认 **ssonsvr.exe** 进程是否正在运行。
2. 将本地计算机策略添加到用户的本地计算机上和/或 VDA 桌面黄金映像中。
    1. 打开 **gpedit.msc**。
       注意：组策略编辑器管理单元 gpedit.msc 随 Windows 7 和 Windows 8 Professional、Enterprise 和 Ultimate Edition 提供。
    2. 右键单击计算机配置 > 管理模板，然后选择添加/删除模板。
    3. 添加 **C:\Program Files\Citrix\ICA Client\Configuration\icaclient.adm** 模板。
3. 在用户的本地计算机上和/或 VDA 桌面黄金映像中启用下列本地计算机 GPO：
    1. 选择本地用户名和密码。
    2. 选择已启用。
    3. 选择启用直通身份验证。
    4. 选择允许对所有 ICA 连接执行直通身份验证。
    5. 单击确定。
    6. 重新启动 VDA 桌面黄金映像。
4. 登录交付控制器，然后打开 Windows PowerShell 并执行以下命令，以允许交付控制器信任 StoreFront 发送的 XML 请求。
    1. 如果尚未加载，请加载 Citrix cmdlet，方法是键入asnpCitrix*.（请务必包含 Citrix* 后面的句点）。
    2. 按 Enter 键。
    3. 然后键入Add-PSSnapin citrix.broker.admin.v2并按 Enter 键。
    4. 然后键入Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $True并按 Enter 键。
    5. 关闭 PowerShell。
5. 在本地计算机上和/或 VDA 桌面黄金映像中打开 Internet Explorer。
6. 在 Internet 设置 > 安全 > 可信站点中，将 StoreFront 服务器的完全限定名称（不包含应用商店路径）添加到列表中。例如 https://storefront.example.com
   注意：还可以使用 Microsoft GPO 将 StoreFront 服务器添加到“可信站点”。GPO 名为站点到区域分配列表，可以在计算机配置 > 管理模板 > Windows 组件 > Internet Explorer > Internet 控制面板 > 安全页中找到。
7. 注销并重新登录 Receiver。

Citrix Receiver 打开时，如果当前用户已登录到域，用户的凭据将传递到 StoreFront 并枚举 Citrix Receiver 和用户的“开始”菜单中的应用程序和桌面。用户单击某个图标时，Receiver 会将用户的域凭据传递到交付控制器，此时将打开应用程序或桌面。

站点不在“可信站点”或“Intranet”区域中时启用传递身份验证

Nov 19, 2015

您的用户可能要求使用其用户登录凭据向服务器进行传递身份验证，但无法将站点添加到“可信站点”或“Intranet”区域。启用此设置可允许对除“受限站点”外的所有站点启用传递身份验证。

1. 以管理员身份从开始菜单本地运行 gpedit.msc（将策略应用于单台计算机时）或者使用组策略管理控制台（应用域策略时），打开组策略编辑器。
   注意：如果已将 icaclient 模板导入到“组策略编辑器”中，可以忽略步骤 2 到 5。
2. 在组策略编辑器的左窗格中，选择“管理模板”文件夹。
3. 在操作菜单中，选择添加/删除模板。
4. 选择添加，浏览到 Receiver 的 Configuration 文件夹（路径通常为 C:\Program Files\Citrix\ICA Client\Configuration），然后选择 icaclient.adm。
5. 选择打开以添加模板，然后选择关闭以返回到组策略编辑器。
6. 在组策略编辑器中，转到管理模板 > 经典管理模板(ADM) > Citrix 组件 > Citrix Receiver > 用户身份验证 > 本地用户名和密码。
7. 在本地用户名和密码属性菜单中，选择已启用，然后选择启用直通递身份验证和允许对所有 ICA 连接进行直通身份验证复选框。

使用 Kerberos 配置域直通身份验证

Nov 19, 2015

本主题仅适用于 Receiver 与 StoreFront、XenDesktop 或 XenApp 之间的连接。

Receiver for Windows 支持为使用智能卡的部署采用 Kerberos 进行域直通身份验证。Kerberos 是集成 Windows 身份验证 (IWA) 中包含的一种身份验证方法。

启用 Kerberos 身份验证后，无需 Receiver 的密码 Kerberos 即可进行身份验证，因而防止用户设备上发生特洛伊木马攻击来获取密码的访问权限。用户可以通过任何身份验证方法（例如，指纹读取器之类的生物特征验证器）登录用户设备，而且无需进一步的身份验证即可访问已发布的资源。

当 Receiver、StoreFront、XenDesktop 和 XenApp 配置为使用智能卡身份验证并且用户使用智能卡进行登录时，Receiver 按如下方式使用 Kerberos 处理直通身份验证：

1. Receiver Single Sign-On Service 捕获智能卡 PIN。
2. Receiver 使用 IWA (Kerberos) 向 StoreFront 验证用户身份。然后，StoreFront 向 Receiver 提供有关可用虚拟桌面和应用程序的信息。
   注意：对于此步骤，无需必须使用 Kerberos 身份验证。在 Receiver 上启用 Kerberos 只是为了避免额外的 PIN 提示。如果您不使用 Kerberos 身份验证，Receiver 将使用智能卡凭据向 StoreFront 进行身份验证。
3. HDX Engine（之前称为 ICA 客户端）将智能卡 PIN 传递给 XenDesktop 或 XenApp，从而使用户登录到 Windows 会话。然后，XenDesktop 或 XenApp 交付请求的资源。

要将 Kerberos 身份验证用于 Receiver，请确保您的 Kerberos 配置符合以下条件。

- Kerberos 登录只在 Receiver 与属于相同或可信 Windows 服务器域的服务器之间起作用。服务器还必须启用信任委派，您可以通过“Active Directory 用户和计算机管理”工具配置该选项。
- 必须在域中以及 XenDesktop 和 XenApp 中启用 Kerberos。为增强安全性并确保使用 Kerberos，请在域上禁用任何非 Kerberos IWA 选项。
- Kerberos 登录不适用于配置为使用基本身份验证、始终使用指定的登录信息或始终提示输入密码的远程桌面服务连接。

本主题中的剩余部分介绍适用于大多数常见场景的配置域直通身份验证方法。如果打算从 Web Interface 迁移到 StoreFront，并且之前使用的是自定义身份验证解决方案，请联系 Citrix 支持代表以了解详细信息。

警告：本主题中说明的部分配置涉及注册表编辑操作。“注册表编辑器”使用不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因“注册表编辑器”使用不当导致出现的问题能够得以解决。使用“注册表编辑器”需自担风险。请确保在编辑注册表之前进行备份。

如果您不熟悉 XenDesktop 环境中的智能卡部署，建议您在继续操作之前，阅读 XenDesktop 文档中的确保部署安全性部分。

安装 Receiver 时，请包含以下命令行选项：

- /includeSSON
  此选项在加入域的计算机上安装 Single Sign-On 组件，从而使 Receiver 能够使用 IWA (Kerberos) 向 StoreFront 进行身份验证。Single Sign-On 组件存储智能卡 PIN，然后，HDX Engine 在将智能卡硬件和凭据远程传递到 XenDesktop 时会使用此 PIN。XenDesktop 自动从智能卡选择一个证书并从 HDX Engine 获得此 PIN。

  默认情况下会启用相关选项 ENABLE_SSON，请保留启用此选项。

如果安全策略阻止在设备上启用 Single Sign-On，请通过以下策略配置 Receiver：

管理模板 > 经典管理模板(ADM) > Citrix 组件 > Citrix Receiver > 用户身份验证 > 本地用户名和密码

注意：在此情况下您希望允许 HDX Engine 使用智能卡身份验证而非 Kerberos，因此请勿使用选项 ENABLE_KERBEROS=Yes，此选项会强制 HDX Engine 使用 Kerberos。

要应用这些设置，请在用户设备上重新启动 Receiver。

配置 StoreFront：

- 在 StoreFront 服务器上的 default.ica 文件中，将DisableCtrlAltDel设置为false。
  注意：如果所有客户端计算机都运行 Receiver for Windows 4.2 或更高版本，则无需执行此步骤。
- 在 StoreFront 服务器上配置身份验证服务时，选中域直通复选框。该设置将启用集成 Windows 身份验证。无需选中智能卡复选框，除非您还具有未加入域的客户端使用智能卡连接到 Storefront。

有关将智能卡用于 StoreFront 的详细信息，请参阅 StoreFront 文档中的配置身份验证服务。

配置智能卡身份验证

Nov 19, 2015

Receiver for Windows 支持以下智能卡身份验证特性。有关 XenDesktop 和 StoreFront 配置的信息，请参阅这些组件的文档。本主题介绍适用于智能卡的 Receiver for Windows 配置。

- **直通身份验证 (Single Sign-On)** – 当用户登录到 Receiver 时，直通身份验证可捕获智能卡凭据。Receiver 按以下方式使用捕获的凭据：
  - 使用智能卡凭据登录到 Receiver 的已加入域的设备用户无需再次进行身份验证即可启动虚拟桌面和应用程序。
  - 使用智能卡凭据登录到 Receiver 的未加入域的设备用户必须再次输入凭据才可启动桌面或应用程序。

  直通身份验证需要使用 StoreFront 和 Receiver 配置。

- **双模式身份验证** – 双模式身份验证可使用户在使用智能卡和输入用户名和密码之间进行选择。此功能在无法使用智能卡时非常有用（例如，用户将其遗忘在家里或登录证书已过期）。必须根据站点设置专用应用商店以启用此功能，方法是将DisableCtrlAltDel设置为False以允许使用智能卡。双模式身份验证需要 StoreFront 配置。如果解决方案中包含 NetScaler Gateway，也需要此配置。

  双模式身份验证现在还允许 StoreFront 管理员向最终用户提供针对同一个应用商店使用用户名和密码身份验证以及智能卡身份验证的功能，方法是从 StoreFront 控制台中进行选择。请参阅 StoreFront 文档。

- **多个证书** – 如果正在使用多个证书，则其可用于单个智能卡。如果用户将智能卡插入读卡器，则这些证书可用于在用户设备上运行的所有应用程序，包括 Receiver。要更改证书的选择方式，请配置 Receiver。
- **客户端证书身份验证** – 客户端证书身份验证需要使用 NetScaler Gateway/Access Gateway 和 StoreFront 配置。
  - 要通过 NetScaler Gateway/Access Gateway 访问 StoreFront 资源，在移除智能卡后用户可以必须重新进行身份验证。
  - 当 NetScaler Gateway/Access Gateway SSL 配置设置为强制客户端证书身份验证时，操作更加安全。但是，强制客户端证书身份验证与双模式身份验证不兼容。
- **双跳会话** – 如果需要双跳，则需要在 Receiver 和用户的虚拟桌面之间建立更进一步的连接。支持双跳的部署在 XenDesktop 文档中有介绍。
- **支持智能卡的应用程序** – 支持智能卡的应用程序，如 Microsoft Outlook 和 Microsoft Office，允许用户对虚拟桌面或应用程序会话中的文档进行数字签名或加密。

必备条件

本主题假设您熟悉 XenDesktop 和 StoreFront 文档中的智能卡主题。

限制

- 证书必须存储在智能卡上，而非用户设备上。
- Receiver for Windows 不保存用户证书选项，但是可以在配置时存储 PIN。PIN 仅在用户会话期间缓存在非分页内存中，任何时候都 不会存储在磁盘中。
- 插入智能卡后，Receiver for Windows 不会重新连接会话。
- 针对智能卡身份验证进行配置后，Receiver for Windows 不支持虚拟专用网络 (VPN) Single Sign-On 或会话预启动。要将智能卡身份验证与 VPN 隧道结合使用，用户必须安装 NetScaler Gateway 插件并通过 Web 页登录，在每一步都使用智能卡和 PIN 进行身份验证。使用 NetScaler Gateway 插件通过直通身份验证访问 StoreFront 不适用于智能卡用户。
- Receiver for Windows Updater 与 citrix.com 通信，且 Merchandising Server 与 NetScaler Gateway 上的智能卡身份验证不兼容。

警告：本主题中说明的部分配置涉及注册表编辑操作。“注册表编辑器”使用不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因“注册表编辑器”使用不当导致出现的问题能够得以解决。使用“注册表编辑器”需自担风险。请确保在编辑

注册表之前进行备份。

要配置 Receiver，请在安装时包含以下命令行选项：

- ENABLE_SSON=Yes
  Single Sign-On 是另一个用于直通身份验证的术语。启用此设置可阻止 Receiver 第二次显示 PIN 提示。

此外，也可以通过以下策略和注册表更改执行此配置：

- 管理模板 > 经典管理模板(ADM) > Citrix 组件 > Citrix Receiver > 用户身份验证 > 本地用户名和密码
- 如果未安装 Single Sign-On 组件，请在下列任一注册表项中将SSONCheckEnabled设置为false。此注册表项可阻止 Receiver Authentication Manager 查找 Single Sign-On 组件，因此允许 Receiver 向 StoreFront 进行身份验证。
  HKEY_CURRENT_USER\Software\Citrix\AuthManager\protocols\integratedwindows\

  HKEY_LOCAL_MACHINE\Software\Citrix\AuthManager\protocols\integratedwindows\

此外，可以为 Storefront 启用智能卡身份验证，而非 Kerberos。要为 Storefront 启用智能卡身份验证而非 Kerberos，请使用下面的命令行选项安装 Receiver。执行此操作需要管理员权限。计算机无需加入域。

- /includeSSON安装单点登录（直通）身份验证。启用凭据缓存以及使用基于域的直通身份验证。
- 如果用户使用智能卡以外的 Receiver 身份验证方法（如用户名和密码）登录端点，命令行应采用：
  /includeSSON LOGON_CREDENTIAL_CAPTURE_ENABLE=No
  这样可阻止凭据在登录时被捕获，并在登录到 Receiver 时允许 Receiver 存储 PIN。

- 转到“策略”>“管理模板”>“经典管理模板(ADM)”>“Citrix 组件”>“Citrix Receiver”>“用户身份验证”>“本地用户名和密码”。
  启用直通身份验证。根据您的配置和安全设置，您可能需要选择允许对所有 ICA 执行直通身份验证选项才能使用直通身份验证。

配置 StoreFront：

- 配置身份验证服务时，请选中智能卡复选框。

有关将智能卡用于 StoreFront 的详细信息，请参阅 StoreFront 文档中的配置身份验证服务。

1. 将证书颁发机构根证书导入设备的密钥库。
2. 安装供应商的加密中间件。
3. 安装和配置 Receiver for Windows。

默认情况下，如果多个证书有效，则 Receiver 将提示用户从列表中选择证书。或者，可以将 Receiver 配置为使用默认证书（根据智能卡提供商）或近期即将过期的证书。如果没有有效的登录证书，则会向用户发出通知，并提供使用其他可用登录方法的选项。

有效证书必须具备以下所有特点：

- 本地计算机上时钟的当前时间在证书有效期内。
- 使用者公钥必须使用 RSA 算法且密钥长度为 1024、2048 或 4096 位。
- 密钥用法必须包含数字签名。
- 使用者备用名称必须包含用户主体名称 (UPN)。

- 增强型密钥用法必须包含智能卡登录和客户端身份验证或所有密钥用法。
- 证书颁发者链条中的证书颁发机构之一必须匹配服务器在 TLS 握手时发送的允许的可分辨名称 (DN) 之一。

使用以下方法之一可更改证书的选择方式：

- 在 Receiver 命令行中，指定选项 AM_CERTIFICATESELECTIONMODE={ Prompt | SmartCardDefault | LatestExpiry }。默认有提示。对于 SmartCardDefault 或 LatestExpiry，如果有多个证书符合条件，则 Receiver 将提示用户从中选择。
- 将以下键值添加到注册表项 HKCU 或 HKLM\Software\[Wow6432Node\]Citrix\AuthManager：CertificateSelectionMode={ Prompt | SmartCardDefault | LatestExpiry }。在 HKCU 中定义的值优先级高于 HKLM 中的值，可更好地帮助用户选择证书。

默认情况下，向用户显示的 PIN 提示由 Receiver 而不是智能卡加密服务提供程序 (CSP) 提供。Receiver 在需要时提示用户输入 PIN，然后将 PIN 传递给智能卡 CSP。如果您的站点或智能卡有更严格的安全要求，如禁止在每进程或每会话缓存 PIN，则可将 Receiver 配置为使用 CSP 组件以管理 PIN 条目，包括输入 PIN 的提示。

使用以下方法之一更改 PIN 条目的处理方式：

- 在 Receiver 命令行中，指定选项 AM_SMARTCARDPINENTRY=CSP。
- 将以下键值添加到注册表项 HKLM\Software\[Wow6432Node\]Citrix\AuthManager：SmartCardPINEntry=CSP。

启用证书吊销列表检查功能以提高 Receiver 的安全性

Nov 19, 2015

启用证书吊销列表 (CRL) 检查功能后，Receiver 将检查服务器的证书是否已经吊销。通过强制 Receiver 对此进行检查，可以改善服务器的加密身份验证，提高用户设备与服务器之间 TLS 连接的总体安全性。

可以启用多个级别的 CRL 检查。例如，可以将 Receiver 配置为只检查其本地证书列表，也可以配置为同时检查本地和网络证书列表。此外，还可以将证书检查机制配置为只有在验证了所有 CRL 之后才允许用户登录。

在本地计算机中进行这一更改时，如果 Receiver 正在运行，请先退出。确保包括连接中心在内的所有 Receiver 组件都已关闭。

1. 以管理员身份从开始菜单本地运行 gpedit.msc（将策略应用于单台计算机时）或者使用组策略管理控制台（应用域策略时），打开组策略编辑器。
   注意：如果已将 icaclient 模板导入到“组策略编辑器”中，可以忽略步骤 2 到 5。
2. 在组策略编辑器的左窗格中，选择“管理模板”文件夹。
3. 在操作菜单中，选择添加/删除模板。
4. 选择添加，浏览到 Receiver 的 Configuration 文件夹（路径通常为 C:\Program Files\Citrix\ICA Client\Configuration) 并选择 icaclient.adm。
5. 选择打开以添加模板，然后选择关闭以返回到组策略编辑器。
6. 在组策略编辑器中，依次前往管理模板 > 经典管理模板(ADM) > Citrix 组件 > Citrix Receiver > 网络路由 > TLS/SSL 数据加密和服务器标识。
7. 在操作菜单中，选择属性，然后选择已启用。
8. 在 CRL 验证下拉式菜单中，选择其中一个选项。
   - 已禁用。不执行证书吊销列表检查。
   - 只检查存储在本地的 CRL。 在证书验证中使用先前安装或下载的 CRL。如果证书被吊销，则连接会失败。
   - 需要 CRL 才能进行连接。 检查本地的和网络上来自相关证书颁发者的 CRL。如果证书被吊销或找不到，则连接会失败。
   - 从网络获取 CRL。 检查来自相关证书颁发者的 CRL。如果证书被吊销，则连接会失败。

   如果没有设置 CRL 验证，默认为只检查存储在本地的 CRL。

确保 Receiver 通信安全

Nov 19, 2015

要确保 XenDesktop 站点或 XenApp 服务器场与 Receiver 之间的通信安全，可以使用以下安全技术集成 Receiver 连接：

- Citrix NetScaler Gateway 或 Access Gateway。有关信息，请参阅本部分中的主题以及 NetScaler Gateway、Access Gateway 和 StoreFront 文档。
  注意：Citrix 推荐使用 NetScaler Gateway 来确保 StoreFront 服务器与用户设备之间的通信安全。
- 防火墙。网络防火墙可以根据目标地址和端口允许或阻止数据包通过。在使用 Receiver 时，如果要经过将服务器内部网络 IP 地址映射到外部 Internet 地址（即网络地址转换，或 NAT）的网络防火墙，则应配置外部地址。
- 可信服务器配置。
- 仅适用于 XenApp 或 Web Interface 部署；不适用于 XenDesktop 7：SOCKS 代理服务器或安全代理服务器（也称为安全性代理服务器、HTTPS 代理服务器）。可以使用代理服务器来限制网络的入站和出站访问，并处理 Receiver 与服务器之间的连接。Receiver 支持 SOCKS 和安全代理协议。
- （仅限 XenApp 或 Web Interface 部署）不适用于 XenDesktop 7、XenDesktop 7.1、XenDesktop 7.5 或 XenApp 7.5：使用传输层安全性 (TLS) 协议的 SSL Relay 解决方案。
- 对于 XenApp 7.6 和 XenDesktop 7.6，您可以直接在用户与 VDA 之间启用 SSL 连接。（有关为 XenApp 7.6 或 XenDesktop 7.6 配置 SSL 的信息，请参阅 SSL。）

Receiver 与使用 Microsoft Specialized Security - Limited Functionality (SSLF) 桌面安全模板的环境兼容，并可在其中正常运行。Microsoft Windows XP、Windows Vista 和 Windows 7 平台支持这些模板。有关此模板和相关设置的详细信息，请参阅 Windows XP、Windows Vista 和 Windows 7 安全指南，网址为：http://technet.microsoft.com。

使用 NetScaler Gateway 进行连接

Nov 02, 2016

要允许用户通过 NetScaler Gateway 连接，请配置 NetScaler Gateway 以用于 StoreFront。

- 对于 StoreFront 部署：通过将 NetScaler Gateway 和 StoreFront 集成，允许内部或远程用户通过 NetScaler Gateway 连接到 StoreFront。 此部署允许用户连接到 StoreFront 以便访问虚拟桌面和应用程序。 用户通过 Receiver 进行连接。

有关配置上述连接的信息，请参考 Citrix 产品文档中的将 NetScaler Gateway 与 XenMobile App Edition 相集成以及该节点下的其他主题。 以下主题提供了有关 Receiver for Windows 所需设置的信息：

- 为 XenMobile App Edition 配置会话策略和配置文件
- 为 Receiver for XenMobile App Edition 创建会话配置文件
- 配置 Receiver 的自定义无客户端访问策略

要使远程用户能够通过 NetScaler Gateway 连接到您的 Web Interface 部署，请按 Citrix 产品文档中的通过 Web Interface 提供对已发布的应用程序和虚拟桌面的访问及其子主题中所述将 NetScaler Gateway 配置为与 Web Interface 结合使用。

通过 Access Gateway Enterprise Edition 进行连接

Nov 02, 2016

要使远程用户能够通过 Access Gateway 进行连接，请将 Access Gateway 配置为与 StoreFront 和 AppController（CloudGateway 的一个组件）结合使用。

- 对于 StoreFront 部署：允许内部或远程用户通过集成 Access Gateway 与 StoreFront，借助 Access Gateway 连接到 StoreFront。 此部署允许用户连接到 StoreFront 以便访问虚拟桌面和应用程序。 用户通过 Receiver 进行连接。
- 对于 AppController 部署：允许远程用户通过集成 Access Gateway 与 AppController 连接到 AppController。 此部署允许用户连接到 AppController 以获取其 Web 应用程序和软件即服务 (Software as a Service, SaaS) 应用程序，同时向 Receiver 用户提供 ShareFile Enterprise 服务。 用户通过 Receiver 或 Access Gateway 插件进行连接。

有关配置上述连接的信息，请参考 Citrix 产品文档中的将 Access Gateway 与 CloudGateway 相集成以及该节点下的其他主题。 以下主题提供了有关 Receiver for Windows 所需设置的信息：

- 为 CloudGateway 配置会话策略和配置文件
- 创建 Receiver for CloudGateway Enterprise 的会话配置文件
- 创建 Receiver for CloudGateway Express 的会话配置文件
- 配置 Receiver 的自定义无客户端访问策略

要使远程用户能够通过 Access Gateway 连接 Web Interface 部署，应将 Access Gateway 配置为与 Web Interface 配合使用，如 Citrix 产品文档中将 Access Gateway Enterprise Edition 配置为与 Web Interface 通信及其子主题所述。

通过 Secure Gateway 进行连接

Nov 19, 2015

本主题仅适用于使用 Web Interface 的部署。

可以在普通模式或中继模式下使用 Secure Gateway，为 Receiver 与服务器之间的通信提供安全通道。如果在“Normal”（普通）模式下使用 Secure Gateway，并且用户通过 Web Interface 进行连接，则不需要对 Receiver 进行任何配置。

Receiver 使用在运行 Web Interface 的服务器上远程配置的设置连接到运行 Secure Gateway 的服务器。有关为 Receiver 配置代理服务器设置的信息，请参阅与 Web Interface 有关的主题。

如果安全网络中的服务器上安装了 Secure Gateway 代理，则可以在“Relay”（中继）模式下使用 Secure Gateway 代理。有关“Relay”（中继）模式的详细信息，请参阅与 Secure Gateway 相关的主题。

如果使用“Relay”（中继）模式，Secure Gateway 服务器将相当于一个代理，并且必须对 Receiver 进行配置才能使用：

- Secure Gateway 服务器的完全限定的域名 (FQDN)。
- Secure Gateway 服务器的端口号。请注意，Secure Gateway 2.0 版本不支持“Relay”（中继）模式。

FQDN 必须按顺序列出以下三个组成部分：

- 主机名
- 中间域
- 顶级域

例如：my_computer.my_company.com 是一个 FQDN，因为它依次列出主机名 (my_computer)、中间域 (my_company) 和顶级域 (com)。中间域和顶级域的组合 (my_company.com) 通常称为域名。

通过防火墙进行连接

Nov 19, 2015

网络防火墙可以根据目标地址和端口允许或阻止数据包通过。如果在部署中使用防火墙，Receiver 必须能够经由防火墙与 Web 服务器和 Citrix 服务器通信。对于用户设备到 Web 服务器的通信，防火墙必须允许 HTTP 通信（如果正在使用安全 Web 服务器，则通常通过标准 HTTP 端口 80 或 443 进行通信）。对于 Receiver 到 Citrix 服务器的通信，防火墙必须允许在端口 1494 和 2598 上进行入站 ICA 通信。

如果防火墙进行了网络地址转换 (NAT) 配置，您可以使用 Web Interface 定义从内部地址到外部地址的映射和端口。例如，如果 XenApp 或 XenDesktop 服务器未配置有备选地址，则可以将 Web Interface 配置为向 Receiver 提供备选地址。然后，Receiver 使用外部地址和端口号连接服务器。有关详细信息，请参阅 Web Interface 文档。

强制执行信任关系

Nov 19, 2015

可信服务器配置是为标识和实施 Receiver 连接中涉及的信任关系而设计的。这种信任关系可以增强 Receiver 管理员和用户对用户设备上数据完整性的信心，并防止恶意使用 Receiver 连接。

启用此功能后，Receiver 可以指定信任要求，并确定是否信任到服务器的某个连接。例如，以特定连接类型（例如 TLS）连接到某个地址（例如 https://*.citrix.com）的 Receiver 将被定向到服务器上的某个可信区域。

在启用可信服务器配置后，已连接的服务器必须驻留在 Windows“可信站点”区域。（有关将服务器添加到“Windows 受信任站点”区域的操作步骤说明，请参阅 Internet Explorer 的联机帮助。）

启用可信服务器配置

如果在本地计算机上更改此项配置，请关闭所有 Receiver 组件（包括连接中心）。

1. 以管理员身份从开始菜单本地运行 gpedit.msc（将策略应用于单台计算机时）或者使用组策略管理控制台（应用域策略时），打开组策略编辑器。
   注意：如果已将 icaclient 模板导入到“组策略编辑器”中，可以忽略步骤 2 到 5。
2. 在组策略编辑器的左窗格中，选择“管理模板”文件夹。
3. 在操作菜单中，选择添加/删除模板。
4. 选择添加，浏览到 Receiver 的 Configuration 文件夹（路径通常为 C:\Program Files\Citrix\ICA Client\Configuration），然后选择 icaclient.adm。
5. 选择打开以添加模板，然后选择关闭以返回到组策略编辑器。
6. 展开用户配置节点下的管理模板文件夹。
7. 在组策略编辑器中，依次前往管理模板 > 经典管理模板(ADM) > Citrix 组件 > Citrix Receiver > 网络路由 > 配置可信服务器配置。
8. 在操作菜单中，选择属性，然后选择已启用。

提升级别与 wfcrun32.exe

Nov 19, 2015

在运行 Windows 8、Windows 7 或 Windows Vista 的设备上启用了用户访问控制 (UAC) 之后，只有与 wfcrun32.exe 具有相同提升/完整性级别的进程才能启动虚拟应用程序。

示例 1：

以普通用户身份运行 wfcrun32.exe（未提升）时，必须以普通用户身份运行其他进程（例如 Receiver），才能通过 wfcrun32 启动应用程序。

示例 2：

在提升模式下运行 wfcrun32.exe 时，其他进程（例如 Receiver、连接中心以及在非提升模式下使用 ICA Client Object 运行的第三方应用程序）无法与 wfcrun32.exe 进行通信。

通过代理服务器连接 Receiver

Nov 19, 2015

本主题仅适用于使用 Web Interface 的部署。

代理服务器用于限制网络的入站和出站访问，并处理 Receiver 与服务器之间的连接。Receiver 支持 SOCKS 和安全代理协议。

与服务器场进行通信时，Receiver 使用在运行 Receiver for Web 或 Web Interface 的服务器上远程配置的代理服务器设置。有关代理服务器配置的信息，请参阅 StoreFront 或 Web Interface 文档。

在与 Web 服务器进行通信时，Receiver 使用通过用户设备上默认 Web 浏览器的 Internet 设置配置的代理服务器设置。您必须相应地配置用户设备上默认 Web 浏览器的 Internet 设置。

通过 Secure Sockets Layer (SSL) Relay 连接

Nov 19, 2015

本主题不适用于 XenDesktop 7、XenDesktop 7.1、XenDesktop 7.5 或 XenApp 7.5。

可以将 Receiver 与 Secure Sockets Layer (SSL) Relay Service 集成在一起。Receiver 支持 TLS 协议。Receiver for Windows 4.2 仅支持 TLS 1.0。

- TLS（传输层安全性）是 SSL 协议的最新标准化版本。互联网工程工作小组 (IETF) 在接管 SSL 开放式标准的开发任务后，将 SSL 更名为 TLS。TLS 通过提供服务器身份验证、数据流加密和消息完整性检查，来保障数据通信的安全。有些组织（包括美国政府组织）要求使用 TLS 来保障数据通信的安全。这些组织可能还要求使用验证的加密，例如 FIPS 140（联邦信息处理标准）。FIPS 140 是一个加密标准。

默认情况下，Citrix SSL Relay 使用 XenApp 服务器上的 TCP 端口 443 来进行 TLS 安全通信。SSL Relay 收到 TLS 连接时，会先将数据解密，然后再重定向到服务器，或者，如果用户选择了 TLS+HTTPS 浏览，则重定向到 Citrix XML Service。

如果将 SSL Relay 配置为侦听 443 以外的其他端口，则必须将该非标准侦听端口号指定给插件。

可以使用 Citrix SSL Relay 来保障以下情况下的通信安全：

- 在启用了 TLS 的客户端与服务器之间。在 Program Neighborhood 连接中心中，采用 TLS 加密的连接会带有一个挂锁图标的标记。
- 在 XenApp 服务器与 Web 服务器之间（通过运行 Web Interface 的服务器）。

有关配置 SSL Relay 来确保安装安全的信息，请参阅 XenApp 文档。

除系统要求外，还必须确保：

- 客户端设备支持 128 位加密
- 客户端设备安装了根证书，可以检验服务器证书上的证书颁发机构签名
- Receiver 知晓服务器场中 SSL Relay Service 所使用的 TCP 侦听端口号
- 应用了 Microsoft 推荐的任何 Service Pack 或升级

如果您正在使用 Internet Explorer 并且不能确定系统的加密级别，请访问 Microsoft 网站 http://www.microsoft.com，安装能够提供 128 位加密的 Service Pack。

重要：Receiver 支持的证书密钥长度多达 4096 未。请确保证书颁发机构根证书和中间证书的位长度以及服务器证书的位长度都不超出 Receiver 支持的位长度，否则连接可能会失败。

如果在本地计算机上更改此项配置，请关闭所有 Receiver 组件（包括连接中心）。

1. 以管理员身份从开始菜单本地运行 gpedit.msc（将策略应用于单台计算机时）或者使用组策略管理控制台（应用域策略时），打开组策略编辑器。
   注意：如果已将 icaclient 模板导入到“组策略编辑器”中，可以忽略步骤 2 到 5。
2. 在组策略编辑器的左窗格中，选择“管理模板”文件夹。
3. 在操作菜单中，选择添加/删除模板。
4. 选择添加，然后浏览到插件的 Configuration 文件夹（通常位于 C:\Program Files\Citrix\ICA Client\Configuration），并选

择 icaclient.adm。
5. 选择打开以添加模板，然后选择关闭以返回到组策略编辑器。
6. 在组策略编辑器中，依次前往管理模板 > 经典管理模板(ADM) > Citrix 组件 > Citrix Receiver > 网络路由 > TLS/SSL 数据加密和服务器标识。
7. 在操作菜单中，依次选择属性 > 已启用，然后在允许的 SSL 服务器文本框中按以下格式键入一个新的端口号：

server:SSL relay port number

其中，SSL relay port number 为侦听端口号。可以使用通配符指定多个服务器。例如，*.Test.com:SSL relay port number 将匹配通过指定的端口与 Test.com 建立的所有连接。

如果在本地计算机上更改此项配置，请关闭所有 Receiver 组件（包括连接中心）。

1. 以管理员身份从开始菜单本地运行 gpedit.msc（将策略应用于单台计算机时）或者使用组策略管理控制台（应用域策略时），打开组策略编辑器。
   注意：如果已将 icaclient 模板添加到“组策略编辑器”，可以忽略第 2 步到第 5 步。
2. 在组策略编辑器的左窗格中，选择“管理模板”文件夹。
3. 在操作菜单中，选择添加/删除模板。
4. 选择添加，浏览到 Receiver 的 Configuration 文件夹（路径通常为 C:\Program Files\Citrix\ICA Client\Configuration），然后选择 icaclient.adm。
5. 选择打开以添加模板，然后选择关闭以返回到组策略编辑器。
6. 在组策略编辑器中，依次前往管理模板 > 经典管理模板(ADM) > Citrix 组件 > Citrix Receiver > 网络路由 > TLS/SSL 数据加密和服务器标识。
7. 在操作菜单中，依次选择属性 > 已启用，然后在允许的 SSL 服务器文本框中按以下格式键入可信服务器和新端口号的列表（逗号分隔）：
   servername:SSL relay port number,servername:SSL relay port number

   其中，SSL relay port number 为侦听端口号。可以指定一个与下例类似的特定可信 SSL 服务器的列表（逗号分隔）：
   csghq.Test.com:443,fred.Test.com:443,csghq.Test.com:444
   该列表在 appsrv.ini 示例文件中将转换为以下形式：
   [Word]

   SSLProxyHost=csghq.Test.com:443

   [Excel]

   SSLProxyHost=csghq.Test.com:444

   [Notepad]

   SSLProxyHost=fred.Test.com:443

配置并启用 Receiver for TLS

Nov 19, 2015

本主题不适用于 XenDesktop 7、XenDesktop 7.1、XenDesktop 7.5 或 XenApp 7.5。

要强制 Receiver 通过 TLS 进行连接，必须在 Secure Gateway 服务器或 SSL Relay Service 上指定 TLS。有关详细信息，请参阅 Secure Gateway 或 SSL Relay Service 文档。

此外，请确保用户设备满足所有系统要求。

要对所有 Receiver 通信使用 TLS 加密，请配置用户设备、Receiver 以及运行 Web Interface 的服务器（如果使用 Web Interface）。有关确保 StoreFront 通信安全的信息，请参阅 StoreFront 文档中“安全”下的主题。

在启用了 TLS 的 Receiver 与服务器场之间，如果要使用 TLS 来确保通信安全，用户设备上必须要有可以验证服务器证书上的证书颁发机构签名的根证书。

Receiver 支持 Windows 操作系统所支持的证书颁发机构。这些证书颁发机构的根证书随 Windows 一起安装，并通过 Windows 实用程序进行管理。它们就是 Microsoft Internet Explorer 所使用的根证书。

如果使用自己的证书颁发机构，则必须从该证书颁发机构获得一个根证书，并将其安装在每个客户端设备上。之后，Microsoft Internet Explorer 和 Receiver 都会使用并信任该根证书。

或许也可以使用其他管理或部署方法来安装根证书，例如：

- 使用 Microsoft Internet Explorer 管理工具包 (IEAK) 配置向导和配置文件管理器
- 使用第三方部署工具

请确保 Windows 操作系统所安装的证书能够满足组织的安全要求，否则就应使用组织的证书颁发机构所颁发的证书。

1. 要使用 TLS 对在 Receiver 与运行 Web Interface 的服务器之间所传递的应用程序枚举和启动数据进行加密，请使用 Web Interface 配置相应的设置。必须包括托管 SSL 证书的 XenApp 服务器的计算机名称。
2. 要使用安全 HTTP (HTTPS) 对在 Receiver 与运行 Web Interface 的服务器之间所传递的配置信息进行加密，请按格式 https://servername 输入服务器 URL。在 Windows 通知区域中的 Receiver 图标上单击鼠标右键，然后选择首选项。
3. 在插件状态中的联机插件条目上单击鼠标右键，然后选择更改服务器。

如果在本地计算机上更改此项配置，请关闭所有 Receiver 组件（包括连接中心）。

1. 以管理员身份从开始菜单本地运行 gpedit.msc（该配置应用于单个计算机时）或者使用组策略管理控制台（使用 Active Directory 时），以打开“组策略编辑器”。
   注意：如果已将 icaclient 模板导入到“组策略编辑器”中，可以忽略步骤 2 到 5。
2. 在组策略编辑器的左窗格中，选择“管理模板”文件夹。
3. 在操作菜单中，选择添加/删除模板。
4. 选择添加，浏览到 Receiver 的 Configuration 文件夹（路径通常为 C:\Program Files\Citrix\ICA Client\Configuration），然后选择 icaclient.adm。
5. 选择打开以添加模板，然后选择关闭以返回到组策略编辑器。

6. 在组策略编辑器中，依次前往管理模板 > 经典管理模板(ADM) > Citrix 组件 > Citrix Receiver > 网络路由 > TLS/SSL 数据加密和服务器标识。
7. 在操作菜单中，依次选择属性、已启用，然后从下拉式菜单中选择 TLS 设置。
   - 将“TLS 版本”设置为 TLS 或全部检测，以启用 TLS。如果选择了全部检测，Receiver 将使用 TLS 加密进行连接。
   - 将 SSL 密码集设置为检测版本，使 Receiver 能够从“Government”（政府）和“Commercial”（商业）密码集中协商一个适当的密码集。可以将密码集限定为“Government”（政府）或“Commercial”（商业）。
   - 将 CRL 验证设置为需要 CRL 才能进行连接，以要求 Receiver 尝试检索来自相关证书颁发者的证书吊销列表 (Certificate Revocation Lists, CRL)。

如果在本地计算机上更改此项配置，请关闭所有 Receiver 组件（包括连接中心）。

要满足 FIPS 140 安全性要求，请使用“组策略”模板来配置参数，或者将这些参数加入到运行 Web Interface 的服务器上的 Default.ica 文件中。有关 Default.ica 文件的其他信息，请参阅 Web Interface 相关信息。

1. 以管理员身份从开始菜单本地运行 gpedit.msc（将策略应用于单台计算机时）或者使用组策略管理控制台（应用域策略时），打开组策略编辑器。
   注意：如果已将 icaclient 模板导入到“组策略编辑器”中，可以忽略步骤 3 到 5。
2. 在组策略编辑器的左窗格中，选择“管理模板”文件夹。
3. 在操作菜单中，选择添加/删除模板。
4. 选择添加，浏览到 Receiver 的 Configuration 文件夹（路径通常为 C:\Program Files\Citrix\ICA Client\Configuration），然后选择 icaclient.adm。
5. 选择打开以添加模板，然后选择关闭以返回到组策略编辑器。
6. 在组策略编辑器中，依次前往管理模板 > 经典管理模板(ADM) > Citrix 组件 > Citrix Receiver > 网络路由 > TLS/SSL 数据加密和服务器标识。
7. 在操作菜单中，选择属性，再选择已启用，然后从下拉式菜单中选择正确的设置。
   - 将 TLS 版本设置为 TLS 或全部检测，以启用 TLS。如果选择了全部检测，Receiver 将尝试使用 TLS 加密进行连接。
   - 将 SSL 密码集设置为 Government（政府）。
   - 将 CRL 验证设置为需要 CRL 才能进行连接。

使用 Web Interface 时，应指定 SSL 证书托管服务器的计算机名称。有关使用 TLS 来确保 Receiver 与 Web 服务器之间通信安全的详细信息，请参阅与 Web Interface 相关的信息。

1. 在 Configuration settings（配置设置）菜单中，选择 Server Settings（服务器设置）。
2. 选择 Use SSL/TLS for communications between clients and the Web server（使用 SSL/TLS 实现客户端与 Web 服务器之间的通信）。
3. 保存所做的更改。

选择 SSL/TLS 后，所有 URL 会改为使用 HTTPS 协议。

可以将 XenApp 服务器配置为使用 TLS 来确保 Receiver 与服务器之间的通信安全。

1. 从 XenApp 服务器的 Citrix 管理控制台中，打开要确保其安全的应用程序对应的属性对话框。
2. 选择高级 > 客户端选项，并确保选择启用 SSL 和 TLS 协议。
3. 对要保护的每个应用程序重复这些步骤。

使用 Web Interface 时，应指定 SSL 证书托管服务器的计算机名称。有关使用 TLS 来确保 Receiver 与 Web 服务器之间通信安全的详细信息，请参阅与 Web Interface 相关的信息。

可以将 Receiver 配置为使用 TLS 来确保 Receiver 与运行 Web Interface 的服务器之间的通信安全。

请确保用户设备上已安装了有效的根证书。有关详细信息，请参阅在用户设备上安装根证书。

1. 在 Windows 通知区域中的 Receiver 图标上单击鼠标右键，然后选择首选项。
2. 在插件状态中的联机插件条目上单击鼠标右键，然后选择更改服务器。
3. 更改服务器屏幕中会显示当前配置的 URL。使用 TLS 加密配置数据，请以 https://servername 格式在文本框中键入服务器 URL。
4. 单击更新应用所做的更改。
5. 在用户设备浏览器中启用 TLS。有关详细信息，请参阅浏览器的联机帮助。

ICA 文件签名可阻止启动来自不可信服务器的应用程序或桌面

Nov 19, 2015

本主题仅适用于使用管理模板的 Web Interface 的部署。

ICA 文件签名功能可帮助保护用户免于启动未经授权的应用程序或桌面。Citrix Receiver 可根据管理策略确认由可信源生成该应用程序或桌面启动，并防止从不受信任的服务器进行启动。可以使用组策略对象、Storefront 或 Citrix Merchandising Server 为应用程序或桌面启动签名验证配置此 Receiver 安全策略。默认情况下，不启用 ICA 文件签名。有关为 StoreFront 启用 ICA 文件签名功能的信息，请参阅 StoreFront 文档。

对于 Web Interface 部署，Web Interface 可在启动过程中使用 Citrix ICA File Signing Service 启用并配置应用程序或桌面启动，使其包含签名。该服务可以使用计算机的个人证书存储中的证书签署 ICA 文件。

带 Receiver 的 Citrix Merchandising Server 可以使用 Citrix Merchandising Server 管理员控制台 > 交付向导启用并配置启动签名验证功能，从而添加可信证书指纹。

要使用组策略对象启用并配置应用程序或桌面启动签名验证，请执行下述过程：

1. 以管理员身份从开始菜单本地运行 gpedit.msc（将策略应用于单台计算机时）或者使用组策略管理控制台（应用域策略时），打开组策略编辑器。
   注意：如果已将 ica-file-signing.adm 模板导入到“组策略编辑器”中，可以忽略第 2 步到第 5 步。
2. 在组策略编辑器的左窗格中，选择“管理模板”文件夹。
3. 在操作菜单中，选择添加/删除模板。
4. 选择添加，然后浏览到 Receiver 的 Configuration 文件夹（通常位于 C:\Program Files\Citrix\ICA Client\Configuration），并选择 ica-file-signing.adm。
5. 选择打开以添加模板，然后选择关闭以返回到组策略编辑器。
6. 在组策略编辑器中，依次前往管理模板 > 经典管理模板(ADM) > Citrix 组件 > Citrix Receiver，然后导航到启用 ICA 文件签名。
7. 如果选择已启用，则通过单击显示并使用显示内容屏幕，可以将签名证书指纹添加到可信证书指纹白名单中，或者从该白名单中删除签名证书指纹。 可以从签名证书属性中复制并粘贴签名证书指纹。使用策略下拉式菜单选择仅允许已签名的启动(比较安全) 或向用户提示未签名的启动(不太安全)。

选项	说明
仅允许已签名的启动(比较安全)	仅允许来自可信服务器且已正确签名的应用程序或桌面启动。如果应用程序或桌面启动的签名无效，系统将在 Receiver 中向用户显示一条安全警告消息。用户将无法继续，并且未经授权的启动会受到阻止。
向用户提示未签名的启动(不太安全)	未签名或签名无效的应用程序或桌面每次尝试启动时都会提示用户。用户可以继续应用程序启动或终止启动（默认设置）。

选择数字签名证书时，Citrix 建议您从下面已排好优先级顺序的列表中进行选择：

1. 从公共证书颁发机构 (CA) 购买一个代码签名证书或 SSL 签名证书。

2. 如果您的企业具有专用 CA，请使用该专用 CA 创建一个代码签名证书或 SSL 签名证书。
3. 使用现有的 SSL 证书，例如 Web Interface 服务器证书。
4. 创建一个新的根 CA 证书，并使用 GPO 或通过手动安装将其分发给用户设备。

配置 Web 浏览器和 ICA 文件以启用 Single Sign-On 并管理与可信服务器的安全连接

Nov 19, 2015

本主题仅适用于使用 Web Interface 的部署。

要使用 Single Sign-On (SSO) 并管理与可信服务器的安全连接，请将 Citrix 服务器的站点地址添加到用户设备上 Internet Explorer 工具 > Internet 选项 > 安全下的本地 Intranet 或可信站点区域中。该地址可以包括 Internet 安全管理器 (ISM) 支持的通配符 (*) 格式，也可以是 protocol\://URL[:port] 格式的具体地址。

在 ICA 文件和站点条目中，必须使用相同的地址格式。例如，如果在 ICA 文件中使用完全限定域名 (FQDN)，则在站点区域条目中也必须使用 FQDN。XenDesktop 连接仅使用桌面组名称格式。

http[s]://10.2.3.4

http[s]://10.2.3.*

http[s]://hostname

http[s]://fqdn.example.com

http[s]://*.example.com

http[s]://cname.*.example.com

http[s]://*.example.co.uk

desktop://group-20name

ica[s]://xaserver1

ica[s]://xaserver1.example.com

在站点区域中添加 Web Interface 站点的确切地址。

Web 站点地址示例

https://my.company.com

http://10.20.30.40

http://server-hostname:8080

https://SSL-relay:444

以 desktop://Desktop Group Name 格式添加地址。如果桌面组名称中包含空格，应将每个空格替换为 -20。

在 ICA 文件中对 Citrix 服务器站点地址使用以下一种格式。使用相同格式将其添加到用户设备上 Internet Explorer 工具 > Internet 选项 > 安全下的本地 Intranet 或可信站点区域中：

ICA 文件 HttpBrowserAddress 条目示例

HttpBrowserAddress=XMLBroker.XenappServer.example.com:8080

ICA 文件 XenApp 服务器地址条目示例

如果 ICA 文件仅包含 XenApp 服务器**地址**字段，应使用以下一种条目格式：

icas://10.20.30.40:1494

icas://my.xenapp-server.company.com

ica://10.20.30.40

设置客户端资源权限

Nov 19, 2015

本主题仅适用于使用 Web Interface 的部署。

可以使用“可信站点”和“受限站点”区域通过以下操作设置客户端资源权限：

- 将 Web Interface 站点添加到“可信站点”列表
- 更改新注册表设置

注意：由于 Receiver 的增强功能，插件/Receiver 早期版本中的 .ini 进行将被这些进程替代。

警告：注册表编辑不当会导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因“注册表编辑器”使用不当导致出现的问题能够得以解决。使用“注册表编辑器”需自担风险。在编辑注册表之前，请务必进行备份。

将 Web Interface 站点添加到“可信站点”列表

1. 从 Internet Explorer 的工具菜单中，依次选择 Internet 选项 > 安全。
2. 选择可信站点图标，然后单击站点按钮。
3. 在将该网站添加到区域文本字段中，键入 Web Interface 站点的 URL，然后单击添加。
4. 从 http://support.citrix.com/article/CTX133565 下载注册表设置并注册表做任何更改。 对于 Win32 用户设备，请使用 SsonRegUpx86.reg，对于 Win64 用户设备，请使用 SsonRegUpx64.reg。
5. 注销并重新登录到用户设备。

在注册表中更改客户端资源权限

1. 从 http://support.citrix.com/article/CTX133565 下载注册表设置，并将这些设置导入到每个用户设备。 对于 Win32 用户设备，请使用 SsonRegUpx86.reg，对于 Win64 用户设备，请使用 SsonRegUpx64.reg。
2. 在“注册表编辑器”中，导航至 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Client Selective Trust，并在相应区域中将以下所有资源的默认值更改为所需的访问权限值：

资源键	资源说明
FileSecurityPermission	客户端驱动器
MicrophoneAndWebcamSecurityPermission	麦克风和网络摄像机
ScannerAndDigitalCameraSecurityPermission	USB 设备及其他设备

值	说明
0	无访问权限
1	只读访问权限
2	完全访问权限
3	提示用户输入用户名和密码

值	说明

Receiver Desktop Lock

Nov 19, 2015

当用户不需要与本地桌面进行交互时，可以使用 Receiver Desktop Lock。用户仍可以使用 Desktop Viewer（如已启用），但是，工具栏上仅具有必需的一组选项：Ctrl+Alt+Del、首选项、设备和断开连接。

Receiver Desktop Lock 在加入域的计算机上运行，这些计算机已启用 SSON (Single Sign-On) 并且已配置应用商店。不支持 PNA 站点。升级到 Receiver for Windows 4.2.x 后不再支持以前的 Desktop Lock 版本。

必须通过/includeSSON标志安装 Citrix Receiver for Windows。必须使用 adm 文件或 cmdline 选项配置应用商店和 Single Sign-On。

然后，以管理员身份使用 citrix.com/downloads 上提供的 CitrixReceiverDesktopLock.MSI 安装 Receiver Desktop Lock。

Citrix Receiver Desktop Lock 的系统要求

- 在 Windows XP (Embedded Edition)、Windows 7（包括 Embedded Edition）、Windows 7 Thin PC、Windows 8 和 Windows 8.1 上受支持。
- 仅限通过本机协议连接到 StoreFront。
- 加入域的终端。
- 用户设备必须连接到局域网 (LAN) 或广域网 (WAN)。

注意：Microsoft 已于 2014 年 4 月 8 日终止对 Windows XP 的扩展支持，至此不再支持 Windows XP。

本地应用程序访问

警告:启用本地应用程序访问可能允许本地桌面访问，除非已使用组策略对象模板或类似策略应用了完全锁定。请参阅 XenApp 和 XenDesktop 中的配置本地应用程序访问和 URL 重定向以了解详细信息。

使用 Receiver Desktop Lock

- 可以将 Receiver Desktop Lock 与以下 Receiver for Windows 功能结合使用：
  - 3Dpro、Flash、USB、HDX Insight、Microsoft Lync 2013 插件和本地应用程序访问
  - 仅限域、双因素或智能卡身份验证
- 断开 Receiver Desktop Lock 会话的连接将注销终端设备。
- Flash 重定向在 Windows 8 及更高版本中处于禁用状态。Flash 在 Windows 7 上处于启用状态。
- Desktop Viewer 针对 Receiver Desktop Lock 优化，不具有“主页”、“还原”、“最大化”和“显示”属性。
- Ctrl+Alt+Del 在 Viewer 工具栏上可用。
- 大多数 Windows 快捷键均传递到远程会话，Windows+L 除外。有关详细信息，请参阅将 Windows 快捷键传递到远程会话。
- 禁用连接或 Desktop Viewer 进行桌面连接时，Ctrl+F1 会触发 Ctrl+Alt+Del。

安装 Receiver Desktop Lock

下面的过程将安装 Receiver for Windows，以便使用 Receiver Desktop Lock 显示虚拟桌面。有关使用智能卡的部署，请参阅配置智能卡以与运行 Receiver Desktop Lock 的设备结合使用。

1. 使用本地管理员帐户登录。
2. 在命令提示窗口，运行以下命令（位于安装介质上的 Citrix Receiver 和插件 > Windows > Receiver 文件夹中）。
   对于 Receiver for Windows 4.2：
   CitrixReceiver.exe /includeSSON STORE0="*DesktopStore*;https://*my.storefront.server*/Citrix/MyStore/discovery;on;*Desktop Store*"
   有关命令详细信息，请参阅 Receiver for Windows 安装文档中的使用命令行参数配置和安装 Receiver for Windows。
3. 在安装介质上的同一文件夹中，双击 CitrixReceiverDesktopLock.MSI。Desktop Lock 向导将打开。按照提示进行操作。
4. 安装完成时，重新启动用户设备。如果您有权访问桌面并以域用户身份登录，请使用 Receiver Desktop Lock 显示该设备。

要在安装之后允许管理用户设备，需要从替换 Shell 阶段排除安装 CitrixReceiverDesktopLock.msi 所用的帐户。如果稍后删除该帐

户，您将无法登录和管理设备。

要运行 Receiver Desktop Lock 的**静默安装**，请使用以下命令行：msiexec /i CitrixReceiverDesktopLock.msi /qn

配置 Receiver Desktop Lock

仅应向每位用户授予一个运行 Receiver Desktop Lock 的虚拟桌面的访问权限。

使用 Active Directory 策略，阻止用户使虚拟桌面进入休眠状态。

使用安装时所用的管理员帐户配置 Receiver Desktop Lock。

- 确保 icaclient.adm 和 icaclient_usb.adm 文件加载到组策略中（此时，策略出现在“计算机配置”或“用户配置”>“管理模板”>“经典管理模板(ADM)”>“Citrix 组件”中）。.adm 文件位于 %Program Files%\Citrix\ICA Client\Configuration\ 中。
- USB 首选项 - 用户插入某个 USB 设备时，该设备会自动远程连接到虚拟桌面；无需用户交互。虚拟桌面负责控制 USB 设备并在用户界面中显示该设备。
  - 启用 USB 策略规则。
  - 在“Citrix Receiver”>“远程连接客户端设备”>“通用 USB 远程连接”中，启用并配置现有 USB 设备和新 USB 设备策略。
- 驱动器映射 - 在“Citrix Receiver”>“远程连接客户端设备”中，启用并配置客户端驱动器映射策略。
- 麦克风 - 在“Citrix Receiver”>“远程连接客户端设备”中，启用并配置客户端麦克风策略。

配置智能卡以与运行 Receiver Desktop Lock 的设备结合使用

1. 配置 StoreFront。
   1. 将 XML Service 配置为使用 DNS 地址解析，以获取 Kerberos 支持。
   2. 配置 StoreFront 站点以进行 HTTPS 访问、创建由域证书颁发机构签署的服务器证书，并向默认 Web 站点中添加 HTTPS 绑定。
   3. 确保启用通过智能卡直通（默认启用）。
   4. 启用 Kerberos。
   5. 启用 Kerberos 和使用智能卡进行直通身份验证。
   6. 在 IIS 默认 Web 站点上启用匿名访问并使用集成 Windows 身份验证。
   7. 确保 IIS 默认 Web 站点不需要 SSL 并忽略客户端证书。
2. 使用组策略管理控制台配置用户设备上的本地计算机策略。
   1. 从 %Program Files%\Citrix\ICA Client\Configuration\ 导入 icaclient.adm 模板。
   2. 依次展开管理模板 > 经典管理模板(ADM) > Citrix 组件 > Citrix Receiver > 用户身份验证。
   3. 启用智能卡身份验证。
   4. 启用本地用户名和密码。
3. 安装 Receiver Desktop Lock 之前，配置用户设备。
   1. 将 Delivery Controller 的 URL 添加到 Windows Internet Explorer 的可信站点列表中。
   2. 以 desktop://交付组名称格式将第一个交付组的 URL 添加到 Internet Explorer 可信站点列表中。
   3. 启用 Internet Explorer 以使用可信站点的自动登录功能。

当用户设备上安装了 Receiver Desktop Lock 时，会强制执行一致的智能卡移除策略。例如，如果桌面的 Windows 智能卡移除策略设置为强制注销，则不管用户设备上的 Windows 智能卡移除策略设置为何，用户都必须从该用户设备注销。这样可确保用户设备处于一致状态。这仅适用于具有 Receiver Desktop Lock 的用户设备。

删除 Receiver Desktop Lock

确保删除下面列出的两个组件。

1. 使用安装和配置 Receiver Desktop Lock 时所用的本地管理员帐户登录。
2. 使用专门用于删除或更改程序的 Windows 功能：
   - 删除 Citrix Receiver Desktop Lock。
   - 删除 Citrix Receiver。

将 Windows 快捷键传递到远程会话

大多数 Windows 快捷键都传递到远程会话。本部分重点介绍部分常用快捷键。

Windows

- Win+D - 最小化桌面上的所有窗口。
- Alt+Tab - 更改活动的窗口。
- Ctrl+Alt+Delete - 经由 Ctrl+F1 和 Desktop Viewer 工具栏。
- Alt+Shift+Tab
- Windows+Tab
- Windows+Shift+Tab
- Windows+所有字符键

Windows 8

- Win+C -“打开”超级按钮。
- Win+Q -“搜索”超级按钮。
- Win+H -“共享”超级按钮。
- Win+K -“设备”超级按钮。
- Win+I -“设置”超级按钮。
- Win+Q - 搜索应用程序。
- Win+W - 搜索设置。
- Win+F - 搜索文件。

Windows 8 应用程序

- Win+Z - 转至应用程序选项。
- Win+.- 应用程序左对齐。
- Win+Shift+.- 应用程序右对齐。
- Ctrl+Tab - 循环浏览应用程序历史记录。
- Alt+F4 - 关闭应用程序。

桌面

- Win+D - 打开桌面。
- Win+, - 浏览桌面。
- Win+B - 返回桌面。

其他

- Win+U - 打开“轻松使用设置中心”。
- Ctrl+Esc - 启动屏幕。
- Win+Enter - 打开 Windows 讲述人。
- Win+X - 打开系统工具设置菜单。
- Win+PrintScrn - 创建屏幕快照并保存到“图片”。
- Win+Tab - 打开切换列表。
- Win+T - 预览工具栏中打开的窗口。

Citrix Receiver for Windows 4.x 已修复的问题

Jan 20, 2017

Receiver for Windows 4.2.100

比较：Citrix Receiver for Windows 4.2

Receiver for Windows 4.2.100 包含 Receiver for Windows 4.0、4.0.1、4.1、4.1.2、4.1.100、4.1.200 和 4.2 中包含的所有修复以及下列新修复：

键盘

- 当用户在已发布的 Receiver 会话中收到通过按 Ctrl + Alt + End 组合键更改密码的提示时，此按键组合不起作用。

  [来自 RcvrForWin4.2_14.2.100][#LC0862]

本地应用程序访问

- 在 XenApp 7.5 和 StoreFront 2.5 中，对任一应用程序使用本地应用程序访问功能“KEYWORDS:prefer="*模式*"”时，Receiver 可能会遇到问题。此外，通过使用“首选模板目录”自动创建首选应用程序的快捷方式时，可能会出现问题。

  [来自 RcvrForWin4.2_14.2.100][#LC2153]

会话/连接

- 使用 FastConnect Scripting API 切换用户时，凭据提示不会关闭。

  [来自 RcvrForWin4.2_14.2.100][#LC2299]

- 如果用户以全屏模式启动桌面会话，并且禁用了 Desktop Viewer，插入第二个显示器时，可能会显示滚动条。

  要启用此修复，请设置以下注册表项：

  - *Windows 32 位系统*：
    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
    名称：ProcessWM_SETTINGCHANGE
    类型：DWORD
    值：1（默认值为零）（此修复仅适用于禁用 CDViewer Bar 并且以全屏模式运行桌面的用户）
  - *Windows 64 位系统*：
    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client
    名称：ProcessWM_SETTINGCHANGE
    类型：DWORD

值：1（默认值为零）（此修复仅适用于禁用 CDViewer Bar 并且以全屏模式运行桌面的用户）
下列注册表项为可选。默认情况下，此值为 0，且仅在默认配置无法解决问题时才需要。

- *Windows 32 位系统*：
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  名称：MonitorLayoutUpdateDelay
  类型：DWORD
  值：0 到 4（默认值为零）
- *Windows 64 位系统*：
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client
  名称：MonitorLayoutUpdateDelay
  类型：DWORD
  值：0 到 4（默认值为零）

[来自 RcvrForWin4.2_14.2.100][#LA5746]

- 利用此增强功能，当用户连接到 NetScaler Gateway 并且部署中包含 CloudBridge 或 HDX Insight 时，如果 Receiver for Windows 使用 XenApp 6.5 和运行 VDA 7.x 版的服务器操作系统，则支持“客户端自动重新连接”功能。

  注意：如果在服务器上启用了多流和多端口策略，并且满足以下任意或全部条件，会话可靠性和自动客户端重新连接将不可用：

  - 在 NetScaler Gateway 上禁用会话可靠性
  - NetScaler 设备上出现故障转移
  - CloudBridge 与 NetScaler Gateway 结合使用

  [来自 RcvrForWin4.2_14.2.100][#LC1779]

- 在向用户设备插入多个 USB 设备的情况下运行 Receiver 时，如果重新启动设备或连接新的 USB 设备，会显示以下错误消息：

  “USB Hub Power Exceeded”（超过 USB 集线器功率）

  [来自 RcvrForWin4.2_14.2.100][#LC1904]

- 如果池桌面组为每个用户配置了多个桌面，使用 Receiver for Windows 时，只可以启动第一个桌面。如果用户单击其他桌面的图标，桌面可能会显示“正在连接”对话框，然后连接失败。第一个桌面会话显示在前台。

  [来自 RcvrForWin4.2_14.2.100][#LC0780]

- 按照知识中心文章 CTX133565 的说明导入客户端选择性信任注册表项文件，并配置可信区域和 Intranet 区域时，如果在 Web Interface 或 StoreFront 中启用了 Desktop Viewer，注册表项可能不起作用。如果在浏览器中将 Web Interface 或 StoreFront URL 配置为可信区域，访问客户端驱动器映射 (Client Drive Mapping, CDM) 目录时，会错误地显示文件安全提示。

  [来自 RcvrForWin4.2_14.2.100][#LC0904]

- 从桌面会话注销后，如果用户尝试从 Windows XP Embedded 瘦客户端注销，将显示错误消息“End program concentr.exe”（结束程序 concentr.exe）。

  [来自 RcvrForWin4.2_14.2.100][#LC2556]

- 用户使用 Receiver for Windows 登录时，时区不正确。为了使此修补程序生效，必须满足以下要求：

- 用户设备和服务器上必须安装相同的 Microsoft 时区更新修补程序。例如，如果用户设备上安装了 Microsoft 修补程序 KB2998527，服务器上也应安装此修补程序。
- 如果服务器操作系统为 Windows Server 2008 R2 Service Pack 1，则必须在此服务器上安装 Microsoft 修补程序 KB2870165。
- 必须在 XenApp 服务器上安装修复 #LC1061。

[来自 RcvrForWin4.2_14.2.100][#LC1392]

- 此修复启用了 FastConnect Scripting API 支持，并且未与自助服务插件集成。此选项可以通过以下步骤启用：使用 **ADM** > **Citrix 组件** > **Citrix Receiver** > **FastConnect API Support**（FastConnect API 支持）> **Manage FastConnectAPI support**（管理 FastConnectAPI 支持）下面的组策略对象，然后取消选中“Integrate Self Service plugin with FastConnect”（将自助服务插件与 FastConnect 集成）选项。您也可以将 HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\Dazzle 下的注册表项“FastConnectUsingSSP”设置为“False”。

  [来自 RcvrForWin4.2_14.2.100][#LC2580]

- 将“SelfServiceMode”设置为“False”时，将为后台会话（如预启动应用程序）创建“开始”菜单快捷方式。

  [来自 RcvrForWin4.2_14.2.100][#LC1760]

- 此修复解决了以下问题：

  - 启动已发布的无缝应用程序时，应用程序可能会在 Windows 任务栏的后面打开。
  - 将 Windows 任务栏移动到其他位置时，无缝会话无法调整大小，任务栏可能会叠加到无缝应用程序的上面。

  要启用此修复，还必须安装服务器端修复 #LC1342。

  [来自 RcvrForWin4.2_14.2.100][#LC1645]

- 在 Windows XP Embedded 客户端上的 Receiver for Windows 4.2 中启动会话时，可能会显示错误消息。

  [来自 RcvrForWin4.2_14.2.100][#LC1929]

- 此修复通过设置“FastConnectAPISupportEnabled=True”在安装过程中启用 FastConnect Scripting API 支持。您也可以通过“Manage FastConnectAPI support”（管理 FastConnectAPI 支持）下的“Enable FastConnect API Functionality”（启用 FastConnect API 功能）组策略对象启用此设置。

  [来自 RcvrForWin4.2_14.2.100][#LC2131]

- Receiver for Windows 4.2 可能会由于程序死锁停止发送网络数据包。从而导致发生以下情况：

  - 可能无法建立会话。
  - 如果桌面屏幕分辨率发生变化，Citrix HDX Engine 可能变为无响应。

  [来自 RcvrForWin4.2_14.2.100][#LC2105]

- 在 Receiver for Windows 4.2 累积更新 1 中，此增强功能提供对 TLS 1.1 版和1.2 版的支持。

  [来自 RcvrForWin4.2_14.2.100][#LC1931]

- 在跨场的随机会话中，EdgeSight 代理的 ICA 会话行程往返时间可能会较长。

  [来自 RcvrForWin4.2_14.2.100][#LC1725]

- 利用此增强功能，修改了“icaclient.adm”文件，改善了对 Fast Connect 变更的处理。

[来自 RcvrForWin4.2_14.2.100][#LC2575]

- 将 Receiver 会话调整为“缩放以适应窗口”模式后，鼠标和键盘在会话中不起作用。

  [来自 RcvrForWin4.2_14.2.100][#LC2219]

- 此增强功能改进了关于 Fast Connect 功能的 Citrix Diagnostic Facility (CDF) 跟踪日志，使其不会在没有失败的情况下报告失败。

  [来自 RcvrForWin4.2_14.2.100][#LC2573]

- 通过命令行安装 Receiver 之后，停止并重新启动 Receiver 时，会自动在自助服务插件中添加新应用商店。

  此问题出现在以下情况下：HKEY_CURRENT_USER\Software\Citrix 下的“Dazzle”注册表项存在名为“Properties”的子项，“RegDeleteKey”无法删除包含子项的注册表项，从而创建了重复的应用商店注册表项。

  [来自 RcvrForWin4.2_14.2.100][#LC2154]

- 用户使用 Fast Connect Scripting API 注销后，应用程序快捷方式保留在桌面快捷方式文件夹中或“开始”菜单上。

  [来自 RcvrForWin4.2_14.2.100][#LC2590]

- 通过使用 FastConnect Scripting API 注销时，可能会针对未经身份验证的请求显示多个登录提示。

  [来自 RcvrForWin4.2_14.2.100][#LC2300]

- 如果在安装 Receiver 前创建了与 Receiver 相关的注册表条目，标准版用户可以安装 Receiver for Windows，并且不会出现任何错误，但是，应用程序可能无法启动。

  [来自 RcvrForWin4.2_14.2.100][#LC0410]

- 在 FastConnect Scripting API 中，可能无法将用户切换到显式身份验证。

  [来自 RcvrForWin4.2_14.2.100][#LC2127]

- 此增强功能包括“Per App shortcut management”（每应用程序快捷方式管理）选项。通过使用应用程序属性，可以在用户的桌面和“开始”菜单上创建特定已发布应用程序的快捷方式。

  注意：应用程序属性的“开始”菜单文件夹仅在用户通过使用 Web Interface 而非 StoreFront 连接到场或交付组时有效。

  [来自 RcvrForWin4.2_14.2.100][#LC1930]

- 用户通过使用 Fast Connect 从 Receiver 注销时，应用程序的订阅列表继续显示在侧窗格中。

  [来自 RcvrForWin4.2_14.2.100][#LC2574]

- 如果没有为 Receiver for Windows 配置帐户，则无法通过使用断开连接自助服务命令断开应用程序连接。

  [来自 RcvrForWin4.2_14.2.100][#LC2128]

系统异常

- Receiver 可能会遇到访问冲突并异常关闭。出现此问题时，用户无法通过单击 Web Interface 中的应用程序图标启动会话。

  [来自 RcvrForWin4.2_14.2.100][#LC0650]

- 在本地打印机连接到用户设备的情况下，启动已发布的应用程序时，Receiver for Windows 可能会异常关闭，并显示以下错误消息：

  “Citrix HDX Engine has stopped working”（Citrix HDX Engine 已停止运行）

  [来自 RcvrForWin4.2_14.2.100][#LC1170]

用户体验

- 用户登录 StoreFront 或 Web Interface 时，Receiver 可能需要很长时间才能创建应用程序的桌面快捷方式。

  [来自 RcvrForWin4.2_14.2.100][#LC2263]

- 利用此修复，读取会话的配置时，组策略对象设置的优先级高于主应用商店。

  [来自 RcvrForWin4.2_14.2.100][#LC2698]

用户界面

- 使用命令行安装 Receiver 后，将应用商店名称和说明设置为现有值。如果重新启动 Receiver，应用商店名称和说明可能会自动更改为其他值。但是，URL 保持不变，连接可以正常使用。

  出现此问题是由于，处理 Receiver 站点时，应用商店名称并非从注册表获取，而是根据应用商店 URL 生成新应用商店名称。

  [来自 RcvrForWin4.2_14.2.100][#LC1231]

- 利用此增强功能，如果应用程序不再是已发布的应用程序或已被禁用，将不再显示从应用程序列表删除应用程序和删除快捷方式的提示。

  [来自 RcvrForWin4.2_14.2.100][#LC2157]

- Desktop Viewer 中的“了解更多信息”链接与用户单击导航区域中 Receiver 图标菜单中的“帮助”所指向的帮助文件不同。

  [来自 RcvrForWin4.2_14.2.100][#LC2066]

Receiver for Windows 4.2

比较：Citrix Receiver for Windows 4.1.200

Receiver for Windows 4.2 包含 Receiver for Windows 4.0、4.0.1、4.1、4.1.2、4.1.100 和 4.1.200 中包含的所有修复以及下列新修复：

内容重定向	会话/连接
HDX MediaStream	重影操作
HDX MediaStream Windows Media 重定向	智能卡
HDX Plug and Play	系统异常

安装、卸载、升级 | 用户体验
登录/身份验证 | 用户界面
打印 | 其他
服务器/场管理

内容重定向

- 在已发布的应用程序内访问 URL 时，服务器到客户端的内容重定向可能不起作用，可以在服务器上打开浏览器，但是无法在客户端打开浏览器。

  [#LC0150]

- 有时，如果 Web 服务器无法接受 HEAD 请求，访问 URL 标头中包含“HEAD”请求而非“GET”请求的 Web 站点可能会失败。结果导致服务器到客户端的内容重定向不起作用。

  要启用此修复，请创建以下注册表项：

  HKEY_CURRENT_USER_\Software\Citrix\ICA Client\Engine
  名称：SpecificSites
  类型：REG_MULTI_SZ
  值：Web 站点名称（每行一个 Web 站点）

  注意：GET 请求（而非 HEAD 请求）会发送到值中指定的任何 Web 站点。Web 站点名称区分大小写并且支持通配符“*”。例如，如果在注册表值中指定“*.mycompany.com”，用户同时可以访问 www.mycompany.com 和 support.mycompany.com，二者都是“指定的”Web 站点。

  [#LC0326]

- 此修复是对修复 #LA0803 的增强。在安装了 XenApp 6 Hotfix Rollup Pack 2 和 XenApp 6.5 Hotfix Rollup Pack 3 的服务器上，在已发布的应用程序内访问自定义 URL 时，服务器到客户端的内容重定向不起作用，Web 浏览器在服务器而非用户设备上打开。

  [#LC0428]

HDX MediaStream

- 在具有两个显示器的用户设备上，在 Receiver 会话内通过第一个显示器使用 Windows Media Player 播放视频时，第二个显示器上会额外打开一个黑色窗口。

  [#LC0552]

- 在 Receiver 会话内使用 Windows Media Player 播放视频时，会额外打开一个标题为“Citrix HDX Movie Window”（Citrix HDX 电影窗口）的黑色窗口。关闭此辅助窗口不会影响正在播放的视频。

  [#LC0818]

HDX MediaStream Windows Media 重定向

- 通过 Windows Media Player 播放音频时可能会出现静态噪音。

  [#LA2911]

HDX Plug and Play

- 在会话期间，从端点移除 USB 设备时，Receiver for Windows 可能会变得无响应。

  [#LA4827]

- 有时，从会话注销后没有释放 USB 设备，随后，此设备无法在本地会话中使用。

  [#LC0091]

安装、卸载、升级

- 使用 /includeSSON 命令行开关安装 Receiver 后，SSONSVR.exe 进程无法运行。

  [#LC0138]

- Windows SYSTEM 管理员尝试使用 CitrixReceiver.exe /uninstall 卸载 Receiver 可能会导致显示 UAC 提示。

  [#LC0977]

登录/身份验证

- 在客户端 ADM 模板中自动启用智能身份验证导致在本地策略中将“Local User Name and Password”（本地用户名和密码）设置为“Enabled”（已启用），尽管之前并未配置此策略。

  [#LC0713]

- 安装了累积更新 3 的 Citrix Receiver for Windows 3.4 可能偶尔无法使用域直通身份验证。

  [#LC0865]

打印

- 在 Internet Explorer 8 中将本地打印机设置配置为在一张纸上打印多页时，可能不会采用此设置，而是在一页纸上打印一页。当您从 XenApp 6.5 已发布的桌面连接到 XenApp 6 服务器上发布的 Internet Explorer 8 实例时，会出现此问题。

  [#LA3379]

- 使用 XPS 通用打印机驱动程序时，如果单击“在客户端预览”，Internet Explorer 中会出现以下错误消息：

  “Internet Explorer 无法显示该网页。”

  [#LA5896]

- 每个会话最多可以自动创建 100 个打印机。

  [#LC0031]

- 此增强功能向 LPT 映射客户端组件增加了 CDF 跟踪支持。

  [#LC0823]

服务器/场管理

- 此修复解决了基础组件中的内存问题。

  [#LA5664]

- Receiver for Windows 连接到 NetScaler Gateway，然后将连接传递到 StoreFront 时，StoreFront 的响应中仅包含服务 URL，不包含信标。出现此问题时，用户会收到 HTTP 403 错误，自动发现可能无法使用。

  [#LC0481]

- 如果用户禁用“USB Root Hub”（USB 根集线器）设置，然后在用户设备上通过 Device Manager 再将其启用，当该设备连接到 VDA 时，USB 设备重定向不起作用。

  [#LC0541]

会话/连接

- 登录和注销安装了 Receiver for Windows Enterprise Edition 的 Windows 7 客户端设备可能会出现延迟。通过 GPO 应用登录/注销脚本会出现此问题。每个脚本都可能导致明显延迟。

  [#LA3811]

- 当端点使用 Receiver for Windows 连接到 XenApp 或 XenDesktop 会话时，如果将此端点从睡眠或休眠模式恢复，端点与 Citrix 会话之间的复制/粘贴操作可能会失败。

  [#LA3973]

- 启用多流的情况下，带有 Desktop Lock 功能的 Receiver 可能无法从 VDA 屏幕保护程序恢复，并且无法在 VDA 锁定之后重新连接。

  [#LA4097]

- 尝试从映射到具有只读权限的会话中的客户端驱动器打开 Microsoft Word 或 Microsoft Excel 2003 文件时，文件可能无法打开。

  [#LA4198]

- 启用“Hide Icon”（隐藏图标）策略的情况下，登录客户端设备后，“关于 Citrix Receiver”窗口可能会自动显示。

  [#LA4513]

- 尝试使用自定义虚拟驱动程序启动会话可能会失败。

  要启用此修复，必须创建以下注册表项：

  - *32 位 Windows*
    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
    名称：VdLoadUnLoadTimeOut
    类型：REG_DWORD
    数据：以秒为单位的任何值
  - *64 位 Windows*
    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Citrix\ICA Client

名称：VdLoadUnLoadTimeOut
类型：REG_DWORD
数据：以秒为单位的任何值

[#LA4540]

- 使用 HollyCRM 与 Huawei OpenEye 插件从 PVS 流推送 VDA 执行 VOIP 呼叫时，经过两个小时或更长时间之后，任何一端都听不到对方。

  [#LA4809]

- 当无缝窗口运行在前端时，如果按 Windows 键或单击“开始”按钮打开客户端“开始”菜单，单击本地窗口的任务栏图标会导致焦点保留在无缝会话窗口上，而不是切换到本地窗口。

  [#LA5089]

- 启用 SSL Relay 的情况下，会话可靠性无法用于为利用加密而配置的应用程序。

  [#LA5476]

- 在 XenApp 已发布的桌面会话中更改密码后，已发布的桌面会话内针对已发布应用程序的直通身份验证失败，用户收到询问用户名和密码的提示。

  [#LA5587]

- Receiver 无法通过 Netscaler Gateway 从 Windows Server 2012 R2 连接到 StoreFront。

  [#LC0084]

- 在 Receiver for Windows 4.1 中，当用户尝试通过单击自助服务插件窗口中的桌面图标重新连接到已经断开的会话时，会创建第二个桌面会话。

  [#LC0182]

- 重置 Receiver 时，cleanup.exe 可能会意外退出。

  [#LC0249]

- 在非英语 XenApp 环境中，会话预启动期间，Citrix Receiver 进度条显示但没有响应，并出现以下错误消息：

  “已建立连接。正在协商功能”

  [#LC0306]

- 在已发布的 Microsoft Outlook 实例中键入内容可能会导致会话随机断开连接。

  [#LC0323]

- 尝试使用 TWAIN 设备和任何第三方应用程序传输文件时，应用程序可能会意外退出。

  [#LC0369]

- 用户通过使用 Receiver for Windows 连接到 Windows 7 VDA 时，如果用户通过使用 Desktop Viewer 重定向 SpeechMike，释放麦克风按钮时，重定向可能会失败。

  [#LC0510]

- 尽管配置了文件类型关联，系统还是会提示用户选择打开给定文件所使用的应用程序。

  [#LC0515]

- 尝试通过 PAC 文件使用代理服务器进行连接失败。

  [#LC0529]

- 对于已发布的 SAP 应用程序，Citrix Receiver for Windows 13.4 累积更新 3 可能会意外退出，并显示以下错误消息：

  “Citrix HDX Engine has stopped working”（Citrix HDX Engine 已停止运行）

  [#LC0712]

- 重定向的 COM 端口设备在 Receiver 会话中不可用。

  [#LC0851]

- 如果应用了修复 #LC0031，当用户断开连接或注销时，若存在其他活动会话，Receiver 会话在超过两分钟的时间内变得无响应。

  [#LC0983]

重影操作

- 管理员尝试重影会话会导致启动黑色的重影会话，从而可能无法进行自动重绘。如果重影窗口和被重影窗口的大小相同，会出现此问题。

  [#LA2913]

智能卡

- Citrix Receiver for Windows 可能无法查找有效的智能卡证书，并且可能会在 Authentication Manager 调试日志中显示以下错误消息：

  “ERROR_WINHTTP_CLIENT_AUTH_CERT_NEEDED: Unknown error code '12044'”

  [#LC0783]

系统异常

- 客户端设备从休眠状态恢复时，Receiver for Windows 可能无响应。

  [#LA5023]

- CDViewer 进程的某个问题可能会导致显示黑屏，并触发 .Net 未处理异常。

  [#LC1038]

用户体验

- 在某些配置中，用户会话可能会遇到鼠标闪烁的问题。

  [#LA309]

- 启用“本地文本回显”的情况下，在已发布的 Internet Explorer 实例中输入脱字符可能会闪烁或在高延迟连接下不显示。

[#LA4762]

- 在有些情况下，应用程序在后台启动。

  [#LC0050]

- 如果用户打开多个 Excel 工作簿，并且在注册表中启用了 Excelhook，当关闭最后一个工作簿时，Excel 任务栏图标消失，尽管 Excel 窗口还处于打开状态。

  [#LC0062]

- 除安装 Receiver 的用户以外的任何用户，首次启动 Receiver 时，都会收到“添加帐户”提示。

  [#LC0253]

- 从“关闭显示器”恢复后，会话被重绘为显示器左上角的小屏幕。

  [#LC0319]

- 尝试移动本地 Windows 任务栏后面的已发布应用程序窗口可能会失败。

  [#LC0561]

- 在多个显示器配置中，应用程序窗口可能会错误地重绘。

  [#LC0600]

用户界面

- 如果在应用程序启动过程中关闭 Receiver 应用商店窗口，应用程序启动完成后，进度栏可能仍可见。

  [#LC0464]

- 启动应用程序或桌面过程中，启动对话框在几秒钟内为空，不显示任何活动说明。

  [#LC0624]

- 此修复删除了默认管理模板中的排版错误。

  [#LC0848]

其他

- 此功能是对 Citrix Receive 安装程序日志记录的增强，使您可以：

  - 将日志保存到永久位置
  - 每次安装后保存安装历史记录
  - 实际启动安装之前收集用户环境信息
  - 在安装日志中提供更多调试信息

  [#LA4615]

- CtxCredApi.dll 和 CtxCredApi(64).dll 现在包含在 Citrix Receiver for Windows Enterprise MSI 软件包中。API 现在支持 64 位。将 CtxCredApi64.dll 用于 64 位应用程序。

  [#LA4630]

- 单个用户在用户会话中使用音频时，服务器上所有 wfica 进程的 CPU 使用率可能会增加约 10%。

  [#LA5918]

- 如果证书的组织名称中包含特殊字符，特别是 ASCII 字符集前 128 个字符以外的字符，Receiver 可能无法正确读取该证书的组织名称。

  [#LC0801]

- 使用“wfica32.exe /setup”命令时，wfica.ocx ActiveX 加载项无法注册 Internet Explorer。

  [#LC0927]

注意：本版本的 Citrix Receiver 还包括版本 4.1 和 4.0 中的所有修复。