关于此版本

新增功能

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

4.1 中已修复的问题

4.0 中已修复的问题

Citrix Receiver for Windows 4.1、4.0 已修复的问题

Receiver for Windows 4.1.200

-
-
-
-

-

Receiver for Windows 4.1.100

-
-
  -
  -

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

-
-
-
-
-
-
-
-
-
-

-
-
-
-
-
-
-
-
-

-
-

Receiver for Windows 4.1.2

-
-
-
-
-
-

-
-
-
-

-
-
-
-
-
-
-
-
-
-

-
  -
  -
-
-
-
-
-
-
-
-

-
-
-
-

Receiver for Windows 4.0.1

-

Receiver for Windows 4.0

-
-
  -
  -
-
-
  -
  -
-

-
-
  -
  -
-
-
-
-
-
-
-

-
-
-
-
-
-
-

-
-
-
-
-
-
-
-
-
-

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

-
-
-
-

Citrix Receiver for Windows 4 的已知问题

已知问题

-
-
-
-

安装和升级问题

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

常规问题

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

桌面连接

-

-
-
-

Microsoft Lync 2013 VDI 插件问题

-
-
-
-
-
-

系统要求

设备

操作系统

-
-
-
-

-
-

-
-
-
-
-

硬件

-
-
-

服务器

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

浏览器

连接

-
-
-
-
-
-

关于安全连接和 SSL 证书

身份验证

-
-

-
-
-
-
-

-
-
-
-

-
-
-
-
-
-
-

升级

Receiver for Windows 4.0 功能的可用性

其他

-
-
  -
  -
  -
-
-

-
-
-

安装 Receiver for Windows

-
  -
  -
  -
  -
-
  -
  -
-
  -
  -

升级到 Receiver for Windows 4.0

-
-
-

-
-

升级注意事项

为池桌面禁用自动更新

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 和示例启动脚本交付 Receiver

-
-

修改示例脚本

- set DesiredVersion= 3.3.0.XXXX
-
-
-

添加“每计算机启动脚本”

每计算机部署 Receiver

使用每用户示例启动脚本

-
-

从 Receiver for Web 部署 Receiver

从 Web Interface 登录屏幕部署 Receiver

配置 Receiver for Windows

-
-
-
-

配置应用程序交付

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

-

为 XenDesktop 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 和 App Controller

配置 StoreFront

配置 App Controller

使用组策略对象模板配置 Receiver

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

Nov 20, 2015

对于使用 Citrix XML Service 的 Receiver，可以将其配置为请求服务器的域名服务 (DNS) 名称，而非 IP 地址。

重要：除非 DNS 环境被明确配置为使用这一功能，否则，Citrix 建议不要在服务器场中启用 DNS 名称解析。

通过 Web Interface 与已发布应用程序连接的 Receiver 也是使用 Citrix XML Service。对于通过 Web Interface 连接的 Receiver，由 Web 服务器代表 Receiver 对 DNS 名称进行解析。

默认情况下，DNS 名称解析在服务器场中处于禁用状态，而在 Receiver 上处于启用状态。如果在服务器场中禁用了 DNS 名称解析，则 Receiver 的任何 DNS 名称请求都将返回一个 IP 地址。在 Receiver 上不需禁用 DNS 名称解析。

对特定用户设备禁用 DNS 名称解析

如果服务器部署使用 DNS 名称解析，则当您遇到特定用户设备出现问题时，可以对相应的设备禁用 DNS 名称解析。

警告：注册表编辑器如果使用不当，会导致可能需要重新安装操作系统的严重问题。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。

1. 将字符串注册表项 xmlAddressResolutionType 添加到 HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Application Browsing 中。
2. 将其值设置为 IPv4-Port。
3. 对用户设备的每个用户重复此操作。

将代理服务器与 XenDesktop 连接结合使用

Nov 20, 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。有关更多信息，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：

- 客户端麦克风输入
- 多监视器支持
- 设备上的打印机设置替代
- 键盘快捷方式
- Receiver 对 32 位色图标的支持
- 向 Receiver 用户提供虚拟桌面
- Desktop Viewer 会话中的键盘输入
- 连接到虚拟桌面

客户端麦克风输入

Nov 20, 2015

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。

多监视器支持

Nov 20, 2015

最多可以将八个监视器与 Receiver 结合使用。

多监视器配置中的每个监视器各自具有制造商所设计的分辨率。在会话期间，监视器可以具有不同的分辨率和方向。

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 计算会话图形内存要求的信息，请参阅 ctx115637。

设备上的打印机设置替代

Nov 20, 2015

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。

键盘快捷方式

Nov 20, 2015

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），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，依次展开“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 对 32 位色图标的支持

Nov 20, 2015

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，可能导致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。

向 Receiver 用户提供虚拟桌面

Nov 20, 2015

不同的企业会有不同的企业需求，而且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。可以通过两种方式向用户提供对虚拟桌面的访问权限：使用 Desktop Viewer 或 Citrix Desktop Lock。

如果用户需要与其本地桌面以及虚拟桌面进行交互，应使用 Desktop Viewer。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。
有关 Desktop Lock 的详细信息（仅受 CitrixReceiverEnterprise.exe 支持），请参阅 eDocs 中的 XenDesktop 7 文档。

Desktop Viewer 会话中的键盘输入

Nov 20, 2015

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。

连接到虚拟桌面

Nov 20, 2015

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。

配置智能卡身份验证

Nov 20, 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）。双模式身份验证需要使用 StoreFront 和 NetScaler Gateway 配置。
- **多个证书 –** 如果正在使用多个证书，则可将其用于单个智能卡。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 不会保存用户 PIN 或证书选择。
- 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。
- 不支持通过直接智能卡身份验证访问 App Controller。但是，您可以将 App Controller 部署在 StoreFront 之后，以便使用 StoreFront 证书身份验证服务。使用客户端证书身份验证的 Web 应用程序需要单独的智能卡提示，以便浏览器创建其自己的 SSL 连接。
- 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。

为智能卡身份验证启用 Single Sign-On

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\

配置 StoreFront：

- 在 StoreFront 服务器上的 default.ica 文件中，将 Set DisableCtrlAltDel 设置为 false。
- 在 StoreFront 服务器上配置身份验证服务时，选中域直通复选框，并保持不选中智能卡复选框。
  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。

使用户设备支持使用智能卡

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。

更改证书的选择方式

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 SSL 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一个证书。

- 将以下注册表项值添加到注册表项 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。

使用 CSP PIN 提示

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。
- 将以下注册表项值添加到注册表项 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 20, 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 SSL/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) 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。

站点不在“可信站点”或“Intranet”区域中时启用直通身份验证

Nov 20, 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，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 20, 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。

配置域直通身份验证以结合使用 Kerberos 和智能卡

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Set DisableCtrlAltDel设置为false。
- 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。

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 代理服务器或 SSL 隧道代理服务器）。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。
- 仅适用于 XenApp 或 Web Interface 部署，不适用于 XenDesktop 7：SSL Relay 解决方案，采用安全套接字层 (SSL) 和传输层安全 (TLS) 协议。

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 20, 2015

要支持远程用户通过 NetScaler Gateway 进行连接，请将 NetScaler Gateway 配置为与 StoreFront 和 App Controller（XenMobile App Edition 的一个组件）配合工作。

- 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。
- 对于 App Controller 部署：通过将 NetScaler Gateway 和 App Controller 集成允许远程用户连接到 App Controller。此部署允许用户连接到 App Controller 以获取其 Web 和软件即服务 (SaaS) 应用程序，并为 Receiver 用户提供 ShareFile Enterprise 服务。用户通过 Receiver 或 NetScaler Gateway 插件连接。

有关配置上述连接的信息，请参考 Citrix eDocs 中的 Integrating NetScaler Gateway with XenMobile App Edition（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 eDocs 中的 Providing Access to Published Applications and Virtual Desktops Through the Web Interface（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 19, 2015

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 eDocs 中的 Integrating Access Gateway with CloudGateway（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 连接到 Web Interface 部署，请将 Access Gateway 配置为与 Web Interface 配合使用，如 Citrix eDocs 中 Configuring Access Gateway Enterprise Edition to Communicate with the Web Interface（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 Normal（普通）模式或 Relay（中继）模式下使用 Secure Gateway，来为 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 SSL）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。）

如果使用 SSL 进行连接，应按 https://CN 格式添加服务器名（其中的 CN 是指在 SSL 证书中显示的“公用名”）。否则，应使用 Receiver 在连接时所用的格式；例如，如果 Receiver 使用 IP 地址进行连接，则应添加服务器的 IP 地址。

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. 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 Relay 进行连接

Nov 19, 2015

本节不适用于 XenDesktop 7。

可以将 Receiver 与 Secure Sockets Layer (SSL) Relay Service 集成在一起。Receiver 同时支持 SSL 和 TLS 协议。

- SSL 提供了强加密功能，可以增强 ICA 连接的隐私性，同时它还提供基于证书的服务器身份验证，可以确保您要连接的服务器是正版服务器。
- 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。由于 SSL 版本 3.0 与 TLS 版本 1.0 之间只有一些微小的技术差异，所以在软件安装过程中用于 SSL 的证书也同样适用于 TLS。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 SSL/TLS 安全通信。SSL Relay 收到 SSL/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 SSL/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 SSL/TLS 的客户端与服务器之间。在 Program Neighborhood 连接中心中，采用 SSL/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 以确保安装安全的信息，请参阅 XenApp 文档中的配置服务器和客户端之间的 SSL/TLS。

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 支持的最大证书密钥长度是 4096 位。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 Receivers for SSL 和 TLS

Nov 19, 2015

本主题不适用于 XenDesktop 7。

SSL 和 TLS 采用相同的配置方式和证书，并且可以同时启用。

启用 SSL 和 TLS 后，每次启动连接时，Receiver 都会先尝试使用 TLS，然后再尝试 SSL。如果插件无法通过 SSL 进行连接，连接就会失败，系统将显示一条错误消息。

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 SSL/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 SSL/TLS 的 Receiver 与服务器场之间，如果要使用 SSL/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 SSL/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），打开“组策略编辑器”。
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“SSL/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。如果使用 TLS 进行连接失败，则 Receiver 将使用 SSL 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，可以忽略第 3 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，然后从下拉式菜单中选择正确的设置。
   - 将 SSL/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。如果使用 TLS 进行连接失败，则 Receiver 将尝试使用 SSL 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 SSL/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 SSL/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 SSL/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 SSL/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。

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 SSL/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 SSL/TLS。有关详细信息，请参阅浏览器的联机帮助。

在用户设备上安装根证书

Nov 19, 2015

在启用了 SSL/TLS 的 Receiver 与服务器场之间，如果要使用 SSL/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。

将 Web Interface 配置为对 Receiver 使用 SSL/TLS

Nov 19, 2015

1. 要使用 SSL/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。

配置 TLS 支持

Nov 19, 2015

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，然后从下拉式菜单中选择 TLS 设置。
   - 将“SSL/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。如果使用 TLS 进行连接失败，则 Receiver 将使用 SSL 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)。

在 Web Interface 上使用组策略模板以满足 FIPS 140 安全性要求

Nov 19, 2015

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，可以忽略第 3 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，然后从下拉式菜单中选择正确的设置。
   - 将 SSL/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。如果使用 TLS 进行连接失败，则 Receiver 将尝试使用 SSL 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。

将 Web Interface 配置为使用 SSL/TLS 与 Citrix Receiver 进行通信

Nov 19, 2015

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 SSL/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。

将 Citrix XenApp 配置为在与 Citrix Receiver 通信时使用 SSL/TLS

Nov 19, 2015

可以将 XenApp 服务器配置为使用 SSL/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 SSL/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。

将 Citrix Receiver 配置为在与运行 Web Interface 的服务器通信时使用 SSL/TLS

Nov 19, 2015

可以将 Receiver 配置为使用 SSL/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 SSL/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 SSL/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 20, 2015

本主题仅适用于使用旧管理模板的 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），以打开组策略编辑器。
   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 过程将被这些过程替代。
警告：注册表编辑不当会导致严重问题，可能导致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。

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 下载注册表设置并执行注册表更改。 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。

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
PdaSecurityPermission	PDA 设备
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

值	说明
3	提示用户输入用户名和密码

Receiver for Windows 4.x 已修复的问题

Jan 20, 2017

比较：Citrix Receiver for Windows 4.1.100

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

HDX MediaStream Flash 重定向	会话/连接
打印	系统异常
服务器/场管理	用户体验

HDX MediaStream Flash 重定向

- 浏览某些启用了 HDX MediaStream Flash 重定向功能的 Web 站点可能会导致 Internet Explorer 无响应。

  要启用此修复，还必须在 VDA/XenApp 服务器上安装 VDA/HDX Mediastream for Flash 修复 #LA4151 并设置以下注册表项：

  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://

  [来自 RcvrForWin4.1_14.1.200][#LA5255]

- 在会话中禁用 Flash 智能回退可能会导致 Internet Explorer 无响应。

  [来自 RcvrForWin4.1_14.1.200][#LA5404]

打印

- Citrix 打印机驱动程序 (UPD) 不打印条形码字体。使用 Citrix 打印机驱动程序 (cpviewer.exe) 或条形码打印机打印文档时，此字体显示为空格或随机字符。

  [来自 RcvrForWin4.1_14.1.200][#LC0141]

服务器/场管理

- 如果设置了“文件重定向带宽限制”和“总会话带宽限制”策略，会话可能会意外退出。

  为了解决此问题，必须同时安装包含修复 #LA5925 的服务器更新和 Receiver 更新，然后在服务器上设置以下注册表项：

- 创建以下注册表项：
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\picadm\Parameters
  名称：DisableHighThroughput
  类型：DWORD
  值：1
- 更改以下注册表项：
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\picadm\Parameters
  名称：MaxNetCommands
  类型：DWORD
  值：设置为较小的值

[来自 RcvrForWin4.1_14.1.200][#LA5925]

会话/连接

- 如果 VDA 的网络连接断开后重新连接，鼠标的单击操作不起作用。

  [来自 RcvrForWin4.1_14.1.200][#LA5743]

- COM 端口重定向可能会失败，并显示以下错误消息：

  “Error in OpenPort: Comport 'COM4'”（OpenPort 中出错: COM 端口 COM4）

  [来自 RcvrForWin4.1_14.1.200][#LC0434]

- 连接到 VDA 的端点从睡眠状态恢复时，鼠标和键盘在 VDA 会话中不再可用。

  [来自 RcvrForWin4.1_14.1.200][#LC0085]

- 在前端运行的窗口会话可能会意外丢失焦点。

  [来自 RcvrForWin4.1_14.1.200][#LA5489]

系统异常

- 在直通会话中使用媒体播放器播放视频可能会导致会话意外退出。

  [来自 RcvrForWin4.1_14.1.200][#LC0553]

用户体验

- 全屏无缝应用程序无法顺利移动，移动过程中可能会抖动并且在边框上显示桌面背景。

  [来自 RcvrForWin4.1_14.1.200][#LC0696]

- 在无线网络上，会话窗口可能会临时变为纯灰色。

  [来自 RcvrForWin4.1_14.1.200][#LC0530]

- 如果管理用户会话的策略将会话音频质量设置为**高声音质量；最差性能**（**高级配置** > **属性** > **客户端设备** > **资源** > **音频** > **音频质量** > **高声音质量；最差性能**），则在会话中听不到任何声音。

  [来自 RcvrForWin4.1_14.1.200][#LC0329]

- 在 RDS 桌面会话中循环播放多媒体文件时，经过一个小时或更长时间后，音频和视频流停止。

[来自 RcvrForWin4.1_14.1.200][#LC0641]

- 会话预启动仅在首次启动 Receiver for Windows 时可用，在其配置后不可用。

  [来自 RcvrForWin4.1_14.1.200][#LC0701]

比较：Citrix Receiver for Windows 4.1

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

HDX 3D Pro	服务器/场管理
HDX MediaStream	会话/连接
HDX Plug and Play	系统异常
HDX RealTime	用户体验
安装、卸载、升级	用户界面
打印	其他

HDX 3D Pro

- 在使用 HDX 3D Pro 和 H264 编解码器并且禁用文本跟踪的情况下，使用几个小时后，wfica32.exe 进程的 CPU 占用率达到 100%。

  [来自 RcvrForWin4.1_14.1.100][#LA5554]

HDX MediaStream

- 尝试通过使用已发布的 Web 浏览器（如 Internet Explorer）查看流视频时，可能会由于 HDX MediaStream Flash 重定向功能出现故障而无法进行。

  要启用此修复，请设置以下注册表项：

  - *32 位 Windows*：
    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Client\PseudoContainer
    名称：FallbackIfFlashNotExist
    类型：REG_DWORD
    数据：0
  - *64 位 Windows*：
    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Client\PseudoContainer
    名称：FallbackIfFlashNotExist
    类型：REG_DWORD
    数据：0

[来自 RcvrForWin4.1_14.1.100][#LA5278]

- 在启用了 HDX Mediastream for Flash 1.0（第一代 Flash 重定向）的情况下，如果安装了 Adobe Flash Player 11.8 或更高版本，Microsoft Internet Explorer 可能会意外退出。

  [来自 RcvrForWin4.1_14.1.100][#LA5421]

HDX Plug and Play

- 在 Windows XP SP3 上安装 Receiver for Windows 4.0 后，扩展坞上的 USB 端口无法再重定向。

  [来自 RcvrForWin4.1_14.1.100][#LA4582]

HDX RealTime

- HDX RealTime Webcam Video Compression 重定向可能无法支持 Quarter Video Graphics Array (QVGA) 显示分辨率 (320x240)，并可能会导致 wfica32.exe 进程意外退出。

  [来自 RcvrForWin4.1_14.1.100][#LA5232]

安装、卸载、升级

- 在不连接到 Internet 的情况下将 Receiver for Windows 升级到更新版本时，上一版本无法完全卸载，新版本的安装将失败。

  [来自 RcvrForWin4.1_14.1.100][#LA4896]

打印

- 此修复解决了配置通用打印机驱动程序时双面打印失败而必须手动完成的问题。

  [来自 RcvrForWin4.1_14.1.100][#261552]

- 尝试使用 Internet Explorer 9 打印 HTML 文档可能会导致 Citrix Print Viewer (cpviewer.exe) 中的输出以及某些类型的字体出现乱码。

  [来自 RcvrForWin4.1_14.1.100][#LA3962]

服务器/场管理

- 如果 StoreFront 配置了未经身份验证的应用商店，使用 Receiver for Windows 时，帐户发现可能会失败。

  [来自 RcvrForWin4.1_14.1.100][#LC0004]

- 此增强功能支持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。对于这些应用程序，除现有首选规则之外，自助服务插件还在首选模板目录中搜索快捷方式。如果匹配首选规则，则会将快捷方式复制到用户的开始菜单。

  默认情况下，此目录为以下目录之一：

  - %systemdrive%:\Program Files\Citrix\shortcuts
  - %systemdrive%:\Program Files (x86)\Citrix\shortcuts（适用于按用户设备安装）和
  - %systemdrive%:\Users\<用户名>\AppData\Local\Citrix\SelfService\shortcuts（适用于按用户安装）

  默认首选模板目录的位置可以在注册表中指定。

  HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle or HKEY_CURRENT_USER\Software\Citrix\Dazzle

名称：PreferTemplateDirectory
类型：REG_SZ
数据：任意路径（例如，%systemroot%:\Shortcuts）

如果应用程序随后被取消订阅或从应用商店中删除，从首选目录中复制的快捷方式也会被删除。

[来自 RcvrForWin4.1_14.1.100][#LC0005]

会话/连接

- 在虚拟桌面会话中使用 Citrix Receiver 时，尝试启动通过 XenApp 发布的应用程序失败，并显示以下错误消息：

  “此版本的 Citrix Receiver 不支持所选加密级别。请联系管理员。[错误 1029: 无效的 DLL 负载]。”

  [来自 RcvrForWin4.1_14.1.100][#LA4743]

- 应用 Receiver for Windows 13.4 累积更新 2 后，如果无缝应用程序有焦点，当按 Alt + Tab 切换活动窗口时，语言栏上的输入语言将发生变化。

  [来自 RcvrForWin4.1_14.1.100][#LA4963]

- 在 Windows XP 系统中的任务栏和“开始”菜单属性中选择“将相似任务栏按钮归为一组”后，启动应用程序的速度可能非常缓慢。

  [来自 RcvrForWin4.1_14.1.100][#LA4191]

- 从 Citrix 联机插件 12.2 版升级到 Citrix Receiver for Windows 3.x 版后，如果启用了 NTLM 代理身份验证，与外部 Web 站点的代理连接可能无法启动。

  [来自 RcvrForWin4.1_14.1.100][#LA3781]

- 如果用户设备没有连接网络摄像机，尝试启动已发布的 Microsoft Lync 2010 实例可能会导致应用程序数次建立连接又断开连接，之后才能最终建立连接并启动应用程序。如果在没有安装任何其他网络摄像机的情况下，您安装的应用程序（如 Motorola Bluetooth 软件包）需要安装一个网络摄像机，可能会发生此问题。

  [来自 RcvrForWin4.1_14.1.100][#LA4867]

- 启动已发布的应用程序或桌面时，如果在 IPv4 网络上使用直通身份验证，Kerberos 身份验证可能无法使用。此版本仅为 IPv4 网络修复了此问题。

  [来自 RcvrForWin4.1_14.1.100][#LA5026]

- 此修复解决了与 Microsoft Lync 2013 VDI Plug-in for Windows 相关的音频/视频问题。它可以提升 Lync 用户的用户体验。有关详细信息，请参阅知识中心文章 CTX138408。

  [来自 RcvrForWin4.1_14.1.100][#LA5314]

- 如果 CANcaseXL USB 网络适配器重定向到虚拟桌面，它会在 Windows 设备管理器中显示出现故障。此 USB 设备不支持 Citrix USB 重定向驱动程序。VDA 需要安装修复 #LA5022 才能正常运行。

  [来自 RcvrForWin4.1_14.1.100][#LA5022]

- 此修复修订了修复 #LA1257，#LA1257 无法完全解决以下问题：

如果禁用了 Desktop Viewer，全屏客户端会话不会因为端点上的屏幕分辨率发生变化而调整 Virtual Desktop Agent 的屏幕分辨率。

[来自 RcvrForWin4.1_14.1.100][#LA4000]

- 如果 XenDesktop 会话的连接断开时长超过会话可靠性超时时间，Desktop Viewer 将在屏幕上无限期显示。按照预期，会话本身在会话可靠性超时之后应该从连接中心消失。

  [来自 RcvrForWin4.1_14.1.100][#LA4856]

系统异常

- wfica32.exe 进程可能会意外退出，并显示以下错误消息：

  “Citrix HDX Engine has encountered a problem and needs to close.”（Citrix HDX Engine 遇到问题，需要关闭。）

  [来自 RcvrForWin4.1_14.1.100][#LA3964]

- wfica32.exe 进程可能会意外退出，并显示以下错误消息：

  “Citrix HDX Engine has encountered a problem and needs to close.”（Citrix HDX Engine 遇到问题，需要关闭。）

  [来自 RcvrForWin4.1_14.1.100][#LA4695]

- 在 XenApp 6.5 桌面与 XenApp 4.5 发布的应用程序之间启动直通会话时，wfica32.exe 进程可能会意外退出。

  [来自 RcvrForWin4.1_14.1.100][#LA5193]

- 如果启用了多流策略，访问 COM 端口时应用程序可能无响应。

  [来自 RcvrForWin4.1_14.1.100][#LA5543]

- 在双跳场景中，启动 Microsoft Outlook 或 Communicator 可能会导致 Receiver for Windows 意外退出。

  [来自 RcvrForWin4.1_14.1.100][#LA4813]

用户体验

- 连接或重新连接到托管在 XenApp for Unix 上的会话时，90 秒内屏幕未更新。

  [来自 RcvrForWin4.1_14.1.100][#LA5244]

用户界面

- 联机插件 12.1 中引入了一项对无缝连接的连接进度条显示采用延迟的更改。但是，对于连接到速度较慢的服务器的会话而言，这种行为并不总是可取。此增强功能引入了对以下注册表项的支持，允许您配置延迟的持续时间：

  在 32 位 Windows 上：

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  名称：NotificationDelay
  类型：REG_DWORD
  数据：*<延迟，以毫秒为单位>*

  在 64 位 Windows 上：

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Citrix\ICA Client
名称：NotificationDelay
类型：REG_DWORD
数据：*<延迟，以毫秒为单位>*

[来自 RcvrForWin4.1_14.1.100][#LA0678]

- 将桌面颜色方案从默认的蓝色更改为其他颜色（如橄榄绿或银色）（**桌面** > **属性** >**外观**选项卡 > **配色方案**）后，自助服务插件的文本和背景颜色变为相同，从而导致看不到菜单项。

  [来自 RcvrForWin4.1_14.1.100][#LA5121]

其他

- 使用基于电子邮件的发现后，如果在 DNS 端创建的 SRV 记录包含的端口不是 443，Receiver 会忽略 SRV 记录中指定的端口，并继续使用端口 443 连接到 Access/NetScaler Gateway URL。

  [来自 RcvrForWin4.1_14.1.100][#LA4491]

比较：Citrix Receiver for Windows 4.1

Receiver for Windows 4.1.2 包含 Receiver for Windows 4.0、4.0.1 和 4.1 中的所有修复以及以下新修复：

Microsoft Lync 2013 VDI 插件	安装、卸载、升级

Microsoft Lync 2013 VDI 插件

- 将 Lync 对话窗口移至另一台监视器中后，视频无法显示。

  [#LA5314、#399447]

- 将白板演示窗口移交给另一个用户时，您的会话窗口中不显示其他用户的视频。

  [#LA5314、#399465]

- 在多方视频通话中或在视频会议结束时，Receiver 可能会意外退出。

  [#LA5314、#426035]

- 在某些客户端设备上，采用全屏 VDA 模式的视频通话过程中视频间歇性不可用。

  [#LA5314、#418675]

- 如果移动视频会议窗口，可能会发生视频扭曲。

  [#LA5314、#419898]

安装、卸载、升级

- 在不连接到 Internet 的情况下将 Receiver for Windows 升级到更新版本时，上一版本无法完全卸载，新版本的安装将失败。

[#LA4896]

比较：Citrix Receiver for Windows 4.0.1

Receiver for Windows 4.1 包含 Receiver for Windows 4.0 和 4.0.1 中的所有修复以及以下新修复：

HDX MediaStream Flash 重定向	打印
HDX MediaStream Windows Media 重定向	会话/连接
HDX Plug and Play	系统异常
安装、卸载、升级	用户体验
键盘	用户界面
本地应用程序访问	其他
登录/身份验证	

HDX MediaStream Flash 重定向

- 启用 HDX MediaStream Flash 重定向后，在 http://www.youtube.com/ 上快速连续播放多个多媒体文件时，PseudoContainer2.exe 进程可能会意外退出。

  [#LA3846]

HDX MediaStream Windows Media 重定向

- 在启用了 HDX MediaStream Windows Media 重定向的 Receiver for Windows 3.4 版中，多媒体文件开始通过流技术推送之前，您可能会观察到长达 10 秒钟的延迟。

  [#LA4141]

HDX Plug and Play

- 单击 Desktop Viewer 中的“设备”以选择要使用 HDX Plug-n-Play USB 设备重定向功能远程连接的 USB 设备可能会导致 Desktop Viewer 无响应。

  [#LA3348]

安装、卸载、升级

- 如果 Receiver for Windows 是由管理员安装的，非管理用户尝试升级该 Receiver 可能会导致部分安装 Receiver。

  应用此修复后，非管理用户尝试升级管理员安装的 Receiver 时将收到一条错误消息，安装过程将终止。

[#LA3425]

键盘

- 使用 Receiver for Windows 3.3 版时，按 Alt 键会导致该键保持在按下状态。因此，随后按 E 键可能会调用 Windows Explorer。

  [#LA3288]

- 在全屏模式下按住 Windows 键单击 Desktop Viewer 工具栏，该键可能会保持在按下状态。因此，随后按 E 键将调用 Windows Explorer。

  [#LA3349]

- 此修复解决了可能会导致 Caps Lock、Num Lock 和/或 Scroll Lock 键的状态在 ICA 会话中不同步的问题。此修复引入了一个新参数，该参数允许您强制在客户端与服务器之间同步键盘 LED 状态。要启用此选项，请将条目“KeyboardForceLEDUpdate = On”添加到本地用户配置文件所在位置中的 appsrv.ini 文件或相应 Web Interface 站点中的 default.ica 文件的 [WFClient] 部分。

  [#LA3682]

- 此修复解决了可能会导致 Caps Lock、Num Lock 和/或 Scroll Lock 键的状态在客户端与服务器之间不同步的 LED 同步问题。

  [#LA4293]

本地应用程序访问

- 启用本地应用程序访问功能后，单击 Desktop Viewer 会导致不必要地显示客户端本地任务栏。

  [#LA3049]

登录/身份验证

- 在 Windows Server 2008 R2 上安装 XenDesktop 7 VDA 后，直通身份验证可能会失败。出现此问题的原因是 ssonsvr.exe 进程无法启动。

  [#LA4685]

打印

- 将多个 Adobe Acrobat 打印作业发送到会话打印机时，可能会丢失随机页面或整个打印作业。

  [#LA3643]

- 会话打印机枚举可能需要相当长的时间。

  [#LA3951]

会话/连接

- 如果活动的 XenDesktop 会话运行过程中客户端设备在相当长的时间内处于睡眠或休眠状态，客户端设备恢复时，会话可能无法按预期重新连接，并且卡在重新连接阶段，需要手动关闭会话窗口。

  此修复解决了该问题，因而恢复客户端设备时，即使重新连接失败，会话窗口也能够按预期关闭。

[#LA2748]

- 在无缝模式下启动已发布的应用程序时，进度条窗口保留在后台。

  要启用此修复，请在客户端设置以下注册表项：

  - *Windows 32 位系统：*
    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
    名称：ForegroundProgressBar
    类型：DWORD
    数据：1
  - *Windows 64 位系统：*
    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client
    名称：ForegroundProgressBar
    类型：DWORD
    数据：1

  [#LA3491]

- 每次出现硬件错误或 VM 强制从虚拟机管理程序中关闭时，带有 Desktop Lock 的 Receiver 将显示灰屏。

  [#LA3499]

- 如果客户端设备上启用了“任务栏分组”，wfica32.exe 中的 TaskbarGrpXpVista.dll 将不必要地向客户端设备查询与该会话中运行的已发布应用程序有关的信息。例如，运行已发布的 cmd.exe 实例时，TaskbarGrpXpVista.dll 将向 C:\windows\system32\cmd.exe 查询与该可执行文件有关的信息。如果已发布的应用程序从远程共享运行，这可能会导致不适当地占用带宽。

  [#LA3661]

- 如果设置了某项 GPO 设置以阻止任务栏分组，单击 Windows XP 和 Vista 客户端设备上的任务栏图标无法将焦点切换到关联窗口。

  [#LA3889]

- 如果您在“Citrix Receiver – 设备访问”对话框显示期间单击 Desktop Viewer 工具栏的“设备”按钮，Receiver 可能会无响应。如果设备访问首选项配置为“每次都询问”而不是“不执行任何操作”，将会显示此对话框。

  [#LA3899]

- 连接到虚拟桌面会话时，Desktop Viewer (CDViewer.exe) 和 wfica32.exe 进程可能会意外退出。

  [#LA3944]

- 应用此修复后，IsReconnectInProgress() API 将集成到 Citrix Fast Connect 2.0。该功能决定启用“自动客户端重新连接”功能时重新连接进程是否正在运行。

  [#LA4080]

- 此修复允许重新连接直通应用程序并为直通应用程序启用工作区控制。

  要启用此项修复，必须设置以下注册表项：

要在直通模式下启用工作区控制，请设置：

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\PNAgent
名称：ForceEnableWSC
类型：DWORD
数据 = 1

要允许重新连接直通应用程序，请设置：

HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client
名称：BypassPassThruMode
类型：DWORD
数据 = 1

注意：此修复仅在以下条件下起作用：

- 在相同的 XenApp Services 站点或场中不能出现两个或多个连接跃点。换句话说，端点 Receiver 可以连接到 XenApp Services 站点 A 上已发布的 XenDesktop VDA，该 VDA 上的直通客户端随后可以连接到*不同的* XenApp Services 站点（即站点 B）上已发布的应用程序或桌面。
- 第二个连接跃点必须是 XenApp 终端会话，不能是 XenDesktop VDA。

[#LA4206]

- 在所发布的客户端屏幕百分比为奇数（非偶数，例如 95%）的桌面中使用远程协助软件时，远程协助会话可能会变形。

  [#LA4313]

- 此兼容性增强功能扩展了对 HDX Plug and Play USB 设备到其他 USB 设备的重定向支持能力。

  [#LA4335]

- wfcrun32.exe 中的死锁会阻止新会话成功启动。

  [#LA4344]

- 尝试使用 Citrix 快速启动工具或指定“HTTPBrowserAddress=服务器或 IP:端口”（例如：“HTTPBrowserAddress=192.168.1.10:8080”）的静态 ICA 文件连接到 XenApp 服务器可能会失败。

  [#LA4585]

系统异常

- wfica32.exe 进程可能会意外退出，并显示以下错误消息：

  “Citrix HDX Engine has encountered a problem and needs to close.”（Citrix HDX Engine 遇到问题，需要关闭。）

  [#LA3412]

- wfica32.exe 进程可能会遇到访问冲突并意外退出。

  [#LA3639]

- wfica32.exe 进程可能会意外退出。

  [#LA4208]

用户体验

- 此修复删除了 Receiver 4.0 与 StoreFront 结合使用时所显示的不必要的登录提示。

  [#LA4652]

用户界面

- 如果应用程序名称与已发布的应用程序的显示名称不匹配，应用程序启动将失败。

  [#LA3891]

其他

- 此版本包含 SSLSDK 的最新版本 - 版本 12.1.13。

  [#LA3804]

- 此修复改进了某些部署中 Receiver for Windows 的 TerminateUser 函数的功能。

  [#LA3881]

比较：Citrix Receiver for Windows 4.0

Receiver for Windows 4.0.1 包含 Receiver for Windows 4.0 中的所有修复以及以下新修复：

- 此修复删除了 Receiver 4.0 与 StoreFront 结合使用时所显示的不必要的登录提示。

  [#LA4652]

比较：Citrix Receiver for Windows 3.4

与 Citrix Receiver for Windows 3.4 相比，Receiver for Windows 4.0 包含以下修复：

HDX MediaStream Flash 重定向	会话/连接
HDX Plug and Play	系统异常
安装、卸载、升级	用户体验
键盘	用户界面
打印	其他
无缝窗口	

HDX MediaStream Flash 重定向

- 在呈现视频文件时，将整个或部分视频窗口移至离屏会导致在屏幕上留下黑暗区域。即使将视频窗口移动回来，黑暗区域仍保留。

  [#LA0599]

- **重要**：在客户端设备上应用此修复前，请参阅知识中心文章 CTX126817，以了解有关“动态黑名单”功能对客户端 Flash 重定向的各种影响的重要信息。

  如果在服务器上启用*启用服务器端内容提取*策略，并且在客户端针对 Flash 重定向策略配置 *Flash 服务器端内容提取 URL 列表*设置，则当内容的 URL 中包含多字节/unicode 字符（例如亚洲语言中常见的此类字符）时，尝试播放 Flash 内容可能会失败

  要完整启用此项修复，必须安装包含修复 #LA1621 的客户端修补程序以及：

  - *对于 XenApp*：包含修复 #LA1621 的 HDX Flash 修补程序
  - *对于 XenDesktop*：包含修复 #LA1621 的 Virtual Desktop Agent 修补程序

  注意：此项修复还要求在客户端和服务器上安装相应语言的代码页。这些代码页由 Windows 操作系统默认安装。例如，日文版 Windows 7 将默认安装日文代码页。但是，如果在英文版 Windows 7 中使用含日文字符的 URL，则必须显式安装日文代码页。这对于客户端和服务器均适用，因为如果启用服务器端内容提取，URL 会从客户端传输到服务器。

  [#LA1621]

- 某些带 Flash 内容的用户交互（例如单击按钮）可能会导致 Pseudocontainer2.exe 意外退出。

  [#LA1948]

- 对于某些类型的 Flash 内容，客户端内容重定向可能会失败，并恢复到服务器端呈现，其中包括以下情况：

  1. Flash 内容尝试下载另一个不存在或找不到的 Flash 文件
  2. Adobe Captive 创建的 Flash 内容不满足客户端内容重定向功能的逻辑检查
  3. Flash 内容导致客户端内容重定向功能向服务器远程连接不受支持的界面
  4. 即使将 Flash 内容的 URL 配置在 ServerContentFetching URL 黑名单中，客户端仍尝试提取此 Flash 内容

  要启用此项修复，必须安装一个 HDX Flash 和一个包含修复 #LA2198 的 Receiver for Windows 修补程序。要为上面的第 1 个问题启用此修复，还必须在客户端设备上设置以下注册表项：

  - *32 位 Windows：*
    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Client\PseudoContainer
    名称：FallbackIfFlashNotExist
    类型：REG_DWORD
    数据：0
  - *64 位 Windows：*
    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\HdxMediaStreamForFlash\Client\PseudoContainer
    名称：FallbackIfFlashNotExist
    类型：REG_DWORD
    数据：0

  [#LA2198]

- 将焦点从 Flash 窗口（运行无缝窗口的 Web 浏览器的子窗口）切换到本地窗口，然后再将焦点切换回无缝浏览器窗口的地址栏时，尝试在浏览器的地址栏中键入可能会失败。

[#LA2685]

- 重要：在客户端设备上应用此修复前，请参阅知识中心文章 CTX126817，以了解有关“动态黑名单”功能对客户端 Flash 重定向的各种影响的重要信息。

  HDX MediaStream Flash 重定向功能可能无法对有错误的 Dailymotion 视频 (http://www.dailymotion.com) 起作用。客户端和服务器位于不同地理位置时将出现此问题。

  要启用此修复，必须创建以下注册表项：

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\HdxMediaStreamForFlash\Client
  名称：DisableRegionFiltering
  类型：REG_DWORD
  数据：1

  [#LA3134]

HDX Plug and Play

- 此增强功能修改了默认 USB 重定向行为，如下所述：
  - 启用 Desktop Viewer 时，用户可以手动重定向 USB 设备。
  - 不启用 Desktop Viewer 时，USB 设备自动重定向。

  [#LA0108]

- 尝试将某些 USB 设备映射到虚拟桌面会话失败后，这些设备会从设备管理器中消失，直到重新启动端点。

  [#LA0954]

- 单击 Desktop Viewer 中的“设备”以选择要使用 HDX Plug-n-Play USB 设备重定向功能远程连接的 USB 设备可能会导致 Desktop Viewer 无响应。

  [#LA3348]

安装、卸载、升级

- 升级到 Receiver 3.*x* 后，用户无法启动已发布的应用程序并显示以下错误消息：

  “此版本的 Citrix Receiver 不支持所选加密级别。请联系管理员。错误 1046：未加载虚拟驱动程序。”

  [#LA3120]

键盘

- 通过单击 Desktop Viewer 上的“主页”将虚拟桌面会话最小化可能会断断续续地导致 Tab 键在端点设备上不起作用，直至会话断开连接。

  [#LA2925]

- 截至 Receiver for Windows 3.0 版，在 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\LockdownProfiles\All Regions\Lockdown\Virtual Channels\Keyboard 下设置的 KeyboardTimer 设置值不再有效。此修复恢复了该功能。

  [#LA2949]

- 此修复解决了可能会导致在前台运行的直通会话中 Caps Lock、Num Lock 和/或 Scroll Lock 键的状态在客户端与服务器之间不同步的问题。

  [#LA3288]

- 此修复解决了可能会导致在后台运行的直通会话中 Caps Lock、Num Lock 和/或 Scroll Lock 键的状态在客户端与服务器之间不同步的问题。

  [#LA3310]

打印

- 单击 **Client Settings**（客户端设置）选项卡上的 **Local Printer Settings**（本地打印机设置），将显示 UPD 打印机的 **Properties**（属性）页，之后关闭设置对话框会导致 **Properties**（属性）页无响应。

  [#259485]

无缝窗口

- 存在未保存数据的情况下，使用连接中心或 Web Interface 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。使用“Cancel”（取消）按钮后，Citrix 建议保存您的数据，然后注销会话，以防止进一步出现性能延迟。

  [#LA0318]

会话/连接

- 与虚拟桌面会话断开连接再重新连接后，尝试在会话内录制音频可能会失败。要完全启用此修复，必须同时安装包含修复 #LA0821 的服务器和客户端修补程序。

  [#LA0821]

- 在客户端会话中文件传输所需的时间可能比在 RDP 会话中长。

  要完全启用此修复，必须同时安装包含修复 #LA1263 的服务器和客户端修补程序。

  [#LA1263]

- 在某些情况下，如果在虚拟桌面会话意外断开连接（例如，由于网络中断）之前更改该会话的分辨率，可能会导致重新连接之后会话分辨率与预期分辨率不同。

  [#LA1377]

- 串行端口条形码扫描仪无法处理标签数据大小超过 512 字节的标签。要启用此项修复，必须设置以下注册表项：

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  名称：CommBufferSize
  类型：REG_DWORD
  数据：512（最小值）至 2048（最大值）之间的数字

[#LA1695]

- 按照知识中心文章 CTX131577 所述禁用 Network List Service 和/或 Network Location Awareness Service 导致联机插件 12.3 版丢失连接。

  [#LA2024]

- 尝试通过低带宽连接启动发布到 UNC 路径的无缝应用程序可能需要两分钟以上的时间才能完成。

  [#LA2170]

- 通过单击 Ctrl + Shift 调用无缝会话的输入方法可能也会改变客户端本地输入法。要阻止此问题，必须设置以下注册表项：

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  名称：Showlocallanguagebar
  类型：REG_DWORD
  数据：1 *<显示本地语言栏>*；0 *<隐藏本地语言栏>*

  [#LA2180]

- 启用自动客户端重定向时，选择“休眠”后，如果客户端自动关闭，重新连接尝试可能会失败。

  利用此修复，可以使用 USB 设备重定向将系统暂停或置于“休眠”模式，系统从“待机”模式返回后可以自动重新连接。

  [#LA3061]

- 对于 Citrix Receiver for Windows 3.x，如果使用 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\TCP/IP Compress=Off 将 ICA 压缩设置为“OFF”（关），已发布的应用程序可能无法启动。

  [#LA3072]

- 在多显示器环境中，在全屏模式下将显示切换到辅助显示器时，Desktop Viewer 工具栏可能不再可见。

  [#LA3083]

- 在连接到 Virtual Desktop Agent 的双显示器配置中，如果主显示器是一台便携式计算机，关闭其显示屏后再打开导致会话随后仅在主显示器上显示。

  [#LA3202]

- 在运行 Internet Explorer 8 的 Windows XP 工作站上使用 3.3 版的累积更新 1 或 Receiver for Windows 3.4 版时，可能无法从 Web Interface 启动初始应用程序。

  [#LA3234]

- 尝试使用 Receiver for Linux 重新连接到断开的虚拟桌面会话时，控制台和 XenDesktop 会话可能会无响应（卡在“欢迎”屏幕）。在 Virtual Desktop Agent 上启用了 WDDM 驱动程序，但另一个虚拟桌面会话正在该会话中运行时，将发生此问题。

  [#LA3241]

- 如果客户端 Windows 7 系统的“区域和语言选项”设置为“哈萨克语(哈萨克斯坦)”，Receiver for Windows 3.4 版可能无法启动。

[#LA3517]

系统异常

- 在部署了 EdgeSight for Load Testing 的环境中，wfica32.exe 进程可能会意外退出。

  [#LA0289]

- 在部署了 HP LoadRunner 的环境中，wfcrun.exe 进程可能会意外退出。

  [#LA0859]

- 将音频策略设置为高清声音后，在已发布应用程序的“声音”控制面板中播放随机采样声音文件时，wfica32.exe 进程可能会意外退出。

  [#LA1000]

- 在 Microsoft Excel 2007 电子表格处于打开状态的情况下，从 Web Interface 站点断开会话连接时，联机插件 12.3 版可能会意外退出。

  [#LA2274]

- 启用本地应用程序访问功能后，如果为 Virtual Desktop Agent 配置了法律声明，尝试连接到 Virtual Desktop Agent 可能会失败。

  [#LA2351]

- 重新连接到会话时 Pnamain.exe 进程可能会意外退出。

  [#LA2704]

- 在启用了 aero 的单显示器 Windows 客户端设备上运行的会话可能会意外断开连接。将预览（动态窗口预览功能的一部分）发送到客户端时可能会发生此问题；此时，twi3.dll 线程可能会终止 Winlogon.exe 进程，进而导致会话断开连接。

  要完全解决此问题，必须同时安装包含修复 #LA2858 的 XenApp 和 Receiver 修补程序。

  [#LA2858]

- wfica32.exe 进程可能会意外退出。发生此问题的原因是内存取消引用无效。

  [#LA2860]

- 在某些双跳场景中打印时，将显示以下错误消息且 Wfica32.exe 进程意外退出：“Citrix HDX Engine was stopped working.”（Citrix HDX Engine 已停止运行。）如果端口名称的长度超过 260 个字符，将导致出现此问题。

  要解决此问题，必须同时安装包含修复 #LA3009（XA650R01W2K8R2X64056；RcvrForWin3.3_13.3.104 或其替代修补程序）的服务器和 Receiver 修补程序。

  [#LA3009]

- Citrix Receiver 可能会生成 selfserviceplugin.exe 进程的多个实例，导致系统内存不足。

  [#LA3460]

- Desktop Viewer 在注销过程中可能会意外退出。

[#LA3567]

- 将联机插件用作直通客户端时，PNMain.exe 可能会意外退出。

  [#LA0785]

用户体验

- 使用 USB 重定向时，USB SpaceMouse 设备在使用几个小时后可能会从虚拟桌面会话中消失。

  [#LA2256]

- 利用 eceiver for Windows 3.4 版的增强功能，您可以禁止为 VPN 登录显示以下身份验证消息，当用户在网络连接之间切换时会显示该消息。

  要禁止显示此消息，请创建以下注册表项：

  - *32 位 Windows*：
    HKEY_CURRENT_USER\Software\Citrix\Receiver
    名称：AutoSecureConnection
    类型：REG_DWORD
    值：0（禁止显示 VPN 提示）
  - *64 位 Windows*：
    HKEY_CURRENT_USER\Software\Wow6432Node\Citrix\Receiver
    名称：AutoSecureConnection
    类型：REG_DWORD
    值：0（禁止显示 VPN 提示）

  [#LA3772]

用户界面

- 此修复修改了 Desktop Viewer 工具栏上“Home Desktop”图标标题的韩语翻译，使其意思更明确。

  [#232198]

- 单击在端点上运行桌面组快捷方式时显示的身份验证对话框中的**取消**时，会显示以下不正确的具有误导性的错误消息：

  “应用程序或桌面无法启动。请检查您的网络连接。”

  [#259081]

- 在最大化会话窗口中，如果在“会话连接”屏幕消失*后*单击 USBMultiInsertDialogue 对话框中的**连接**，Desktop Viewer 工具栏可能无法正确描绘。

  [#260390]

- icaclient.adm 的“客户端驱动器映射帮助”主题错误地声明策略不会覆盖用户的选择。但是，策略确实会覆盖用户的选择。

  [#LA0398]

- 使用某些自定义应用程序时，Speed Screen Latency Reduction 的本地文本回显编辑框在键入时显示黑条。

  [#LA0544]

- 首次通过 Merchandising Server 成功交付后无法显示欢迎和/或完成消息。

  [#LA2277]

- 启动已发布的应用程序时，Windows 任务栏的通知区域中 Tivoli Access Manager for Enterprise Single Sign-On (TAM ESSO) 的图标可能会意外消失。

  [#LA3190]

- 如果将本地任务栏设置为自动隐藏，然后将其从默认位置移至屏幕顶部、左侧或右侧，将无法访问该任务栏。

  [#LA3400]

其他

- 播放 UDP 音频流时，wfica32.exe 进程的句柄数量可能会大量增加。

  [#LA3094]

- 此修复删除了仅允许在 Receiver for Web 3.3 中存在一个 Program Neighborhood Web Interface 5.4 站点的限制。

  [#LA3142]