# 关于此版本

Mar 08, 2016

通过 Citrix Receiver for Windows，用户可以安全地自助访问 XenDesktop 和 XenApp 提供的虚拟桌面和应用程序。

## 此版本中的新增功能

**增强的 RealTime Media Engine (RTME) 集成**

本版本通过将 RTME 集成到一个下载和安装包中，引入了 Citrix Receiver for Windows 安装范例的增强功能。 以前，用户需要安装 Citrix Receiver，然后启动独立的 MSI 安装包才能在 Receiver 中集成 RTME 功能。

这使得用户体验的满意度不高，阻碍了 HDX RealTime Optimization Pack 在某些组织中的广泛应用；BYOD 用户（和远程工作人员）需要先安装 Citrix Receiver，然后返回到 Citrix 下载页面才能调用 HDX RTME 的另一个独立安装程序。 单个安装程序中现在同时包含最新版本的 Citrix Receiver for Windows 和 HDX RTME 安装程序。

有关使用在一个可执行文件中包含 HDX RTME 的最新 Citrix Receiver 安装程序的信息，请参阅安装文章。

**使用会话可靠性组策略设置透明度级别**

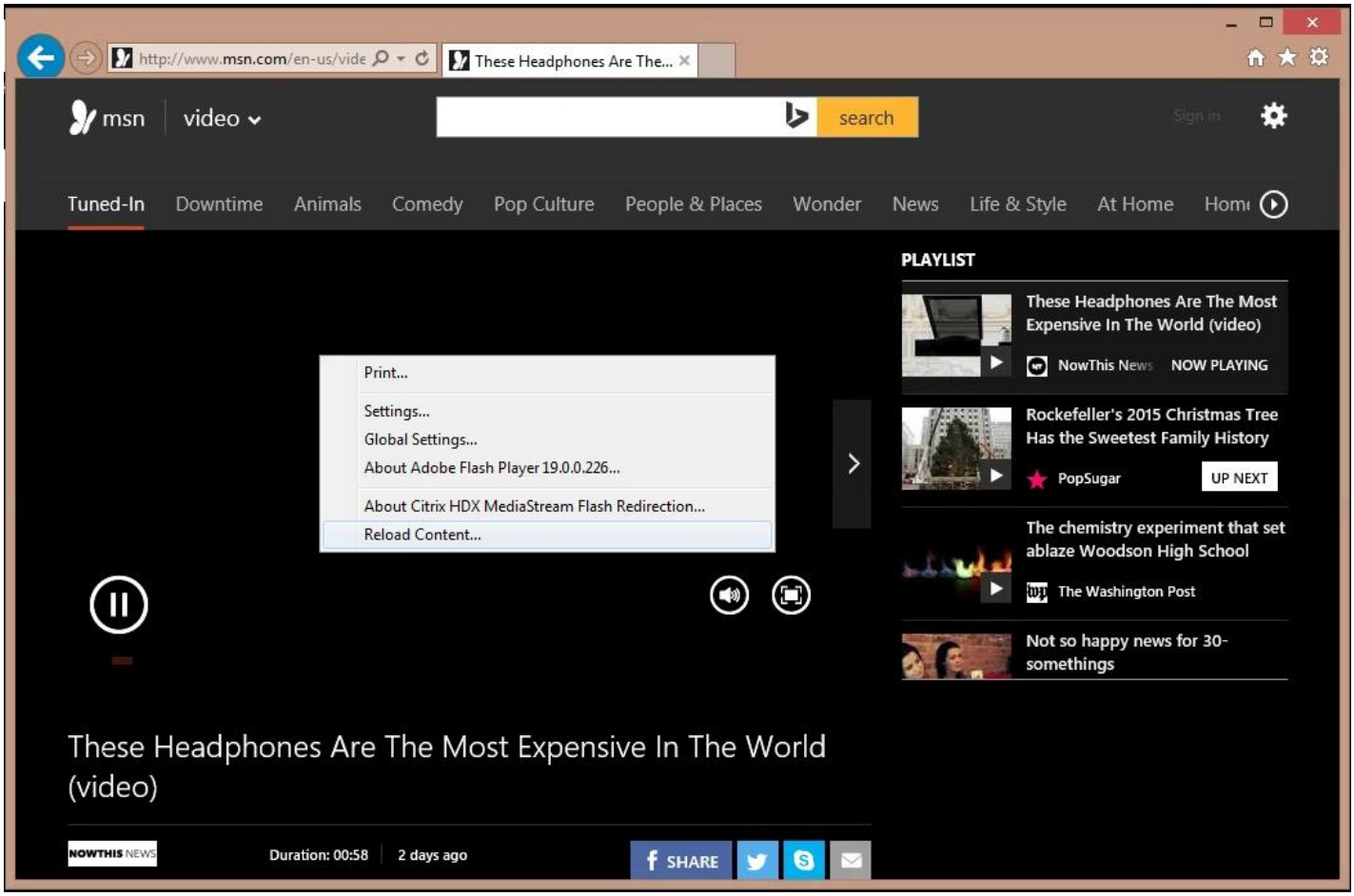
本版本引入了会话可靠性组策略的增强功能。 配置会话可靠性组策略时，您现在可以在会话可靠性重新连接期间设置适用于已发布的应用程序（或桌面）的透明度级别。 有关详细信息，请参阅**使用组策略对象模板配置 Receiver** 中的会话可靠性和组策略。

**手动回退至服务器呈现**

在本版本中，Citrix Receiver 实现了在客户端手动回退到服务器呈现的功能。 在某些情况下查看 Flash 内容时，客户端可能会遇到黑屏问题，并且无法通过任何方式查看 Flash 视频。 在大多数情况下，如果 Flash 无法在客户端呈现，则会自动回退到服务器端呈现。 但是，在某些情况下，客户端呈现失败，并且无法回退。

要解决此类情况，Citrix Receiver for Windows 现在向用户提供手动刷新屏幕并强制在服务器端呈现 Flash 内容的选项。 要手动回退，请将光标置于黑色 Flash 窗口中，单击鼠标右键以显示包含“重新加载内容”选项的上下文菜单。 下图说明了这一新增功能。

> **注意**
>
> 管理员设置的视频保护策略将强制在客户端执行。 有关详细信息，请参阅多媒体策略设置和 Flash 重定向策略设置。




**请升级 SSL SDK 库以支持 NIST SP800-52。**

Citrix Receiver 现在提供升级的 SSL SDK 库以支持 NIST SP800-52。 此功能允许 Receiver 支持 TLS 连接的 NIST SP800-52 兼容模式。 有关详细信息，请参阅设置客户端权限主题中的“启用 NIST SP800-52 兼容模式”。 有关会话可靠性的更多信息，请参阅**使用组策略对象模板配置 Receiver** 主题中的会话可靠性和组策略。

**改进了升级过程**

本版本的 Citrix Receiver for Windows 提供的更新后的安装程序保留了现有的客户端设置，改进了从早期版本的 Citrix Receiver 移动时的用户体验。 此外，更新后的安装程序将从以前安装的版本无缝升级。

**客户端自动重新连接和会话可靠性改进功能**

这些改进功能提升了与 CloudBridge 和 NetScaler Gateway 的互操作性。 会话可以使用客户端自动重新连接和会话可靠性进行重新连接，不受连接路径影响。 本版本具体的改进功能如下：

- 改进的连接消息会告知用户其连接状态并通知其断开连接的时间以及需要执行的操作。
- 倒计时器（以分钟/秒为单位）现在显示会话多久后超时。 倒计时器到期时会话终止。 默认情况下，超时值设置为 2 分钟。可以在 TransportReconnectMaxRetrySeconds ICA 文件设置中更改默认值。

**改进了 HDX 的性能**

Citrix Receiver 已更新，增强了客户端硬件加速功能。 此功能通过启用硬件加速改进了客户端上的 HDX 3D Pro 性能。 有关配置此功能的详细信息，请参阅“用户体验”一文中的硬件解码部分。

**授权平台增强功能**

Citrix Receiver for Windows 现在集成的功能改进了通过特定 TLS 版本验证客户端连接到服务器的方式，包括与特定加密算法、模式、密钥大小以及是否启用 SecureICA 有关的验证。 使用此功能，您还可以在活动会话期间查看客户端当前使用的身份验证证书。 有关详细信息，请参阅 XenApp - XenDesktop 文章，该文章探讨了如何使用密码。

**改进了启动对话框消息**

本版本改进了通知用户与系统有关的更改和更新时 Citrix Receiver for Windows 使用启动对话框的方式。 本版本现在提供简单通知，替换了启动会话时显示的庞大的系统级通知。

**增强了诊断信息收集功能**

本版本集成了改进的诊断工具，您可以使用该工具快速收集系统信息，以及通过创建简单的可以轻松传输或上载至 CIS 等服务的压缩包来分发信息。

## 本版本中已修复的问题

重要：如果您使用的是 XenApp 或 XenDesktop 7.6，请考虑安装 CTX142037、CTX142094 和 CTX142095 上提供的 VDA 修补程序。 此修补程序解决了会话重新连接后出现的音频问题、图形响应问题、图片质量问题以及某些情况下的屏幕损坏问题。

# Citrix Receiver for Windows 4.4 已修复的问题

Jan 20, 2017

Receiver for Windows 4.4 CU3 (4.4.3000)

比较对象：Citrix Receiver for Windows 4.4 CU2 (4.4.2000)

Receiver for Windows 4.4 CU3 (4.4.3000) 包含 Receiver for Windows 4.0、4.0.1、4.1、4.1.2、4.1.100、4.1.200、4.2、4.2.100、4.3、4.3.100、4.4、4.4 CU1 (4.4.1000) 和 4.4 CU2 (4.4.2000) 中的所有修复以及以下新修复：



**本地应用程序访问**

- 使用本地应用程序访问时，某些软件电话应用程序或 Chrome 可能无法正确显示。

  [#LC4327]

- 从本地应用程序访问 (LAA) 桌面断开连接并连接到全屏非 LAA 桌面后，客户端任务栏可能会在全屏非 LAA 桌面上方显示。

  [#LC5966]

- 将会话窗口从全屏模式切换到窗口化模式时，不显示指示以下内容的对话框：
  会话已窗口化。 某些 LAA 功能在此模式下可能不起作用。
  在窗口化模式下启动应用程序时，不显示指示以下内容的对话框：
  应用程序启动失败。 会话处于窗口化模式。 LAA 应用程序启动在此模式下被禁止。 请切换到全屏模式以继续启动。

  [#LC6291]

- 启用本地应用程序访问时，将强制桌面会话在全屏模式下启动。

  [#LC6294]

**内存、CPU 优化**

- SelfServicePlugin.exe 进程会占用高内存。

  [#LC4509]

**会话/连接**

- 使用远程用户配置文件登录并打开已发布的应用程序时，文件类型关联可能不起作用。

[#LC5184]

- 对 SpeechMike 以及其他语音识别应用程序听写时，SpeechMike 可能会停止运行。

  [#LC5632]

- 在无提示开关打开时使用 CleanUp.exe 进程将无法正确地重新加载 Citrix Receiver。

  [#LC6039]

- HDX Engine 可能会意外退出。

  [#LC6047]

- 尝试通过 NetScaler Gateway 11 从 Wyse 瘦客户端启动桌面可能会导致显示以下错误消息：

  Your client has experienced a problem with authentication to the server.（您的客户端在对服务器进行身份验证时遇到问题。）

  [#LC6145]

- 连续不断地移动会话窗口时会话可能会挂起或冻结。

  [#LC6403]

**智能卡**

- 安装了 Citrix Receiver for Windows 4.4 时，在 XenApp 6.5 上发布的应用程序可能会向智能卡发送事务处理请求以结束不活动的事务。 Citrix Receiver for Windows 可能会错误地响应此请求，导致 XenApp 服务器永久等待响应或者设置的事务超时值过期。

  [#LC5772]

**用户体验**

- 此修复在使用客户端音频的实时模式时改进了对播放一小段时间的声音的支持。 此修复仅适用于中质量音频。

  [#LC4941]

- 使用 Windows 8.1 和 Windows Server 2012 R2 时，文件类型关联可能无法将该类型的文件连接到正确的图标和应用程序。应用此修复后，“自助服务”下引入了两个组策略。
  1. 启用默认 FTA - 启用或禁用 FTA 的默认行为
  2. 启用 FTA - 启用或禁用 FTA 功能
  要获取正确的文件类型关联图标，请禁用组策略“启用默认 FTA”。

  [#LC5485]

- 登录到已发布的桌面时，或者如果您重置了 Citrix Receiver for Windows 的配置，文件类型关联 (FTA) 图标的行为可能会与默认 Citrix Receiver for Windows FTA 图标相似。

  [#LC5730]

- Surface Pro 4 和 HP Elite 网络摄像头可能不会重定向到某个会话。 注意：如果网络摄像头不支持屏幕分辨率，网络摄像头重定向可能也会失败。

要修复此问题，请使用以下注册表项：
HKEY_CURRENT_USER\Software\Citrix\HdxRealTime
名称：DefaultWidth
类型：Dword
值：<网络摄像头支持的分辨率> 示例 (Surface Pro 4)：1920

HKEY_CURRENT_USER\Software\Citrix\HdxRealTime
名称：DefaultHeight
类型：Dword
值：<网络摄像头支持的分辨率> 示例 (Surface Pro 4)：1080

[#LC5750]

- 在自助服务窗口中无法正确枚举根据客户端名称分配的桌面。 使用 StoreFront 统一体验时会出现此问题。

  [#LC5773]

## Receiver for Windows 4.4 CU2 (4.4.2000)

比较对象：Citrix Receiver for Windows 4.4 CU1 (4.4.1000)

Receiver for Windows 4.4 CU2 (4.4.2000) 包含 Receiver for Windows 4.0、4.0.1、4.1、4.1.2、4.1.100、4.1.200、4.2、4.2.100、4.3、4.3.100、4.4 和 4.4 CU1 (4.4.1000) 中的所有修复以及以下新修复：



**HDX MediaStream Flash 重定向**

- 启用了 SOLFileHook 时，Flash 内容无法从 ProofHQ.com 正确播放。

  [#LC4866]

- 使用 Adobe Flash Player 22 或 18.0.0.360 浏览包含 Flash 内容的 Web 站点时，Web 站点 URL 将添加到动态黑名单中，并在服务器（而非用户设备）上呈现。

  [#LC5626]

**键盘**

- 如果启用了“键盘快捷方式”策略，并且用户设备上正在运行 wfica32 进程，则通过远程桌面连接进行连接时，可能会显

示“Tip: Exiting Full Screen Mode”（提示: 正在退出全屏模式）对话框窗口。 该对话框窗口无法接受键盘和鼠标输入。

[#LC4445]

- 使用配备了外部 USB 或无线键盘的 Microsoft Surface Pro 设备过程中，每次输入文本时，Citrix Receiver for Windows 会话中都可能会显示本地屏幕键盘。

  [#LC5093]

**本地应用程序访问**

- 启用了本地应用程序访问时，如果应用程序是在远程会话内部在全屏模式或窗口模式下启动的，VDA 会话的任务栏中可能不会显示应用程序图标。 端点设备可能会在任务栏上显示多个应用程序图标，而不是显示一个。

  [#LC4217]

- 在启用了本地应用程序访问的情况下启动已发布的桌面会话时，Desktop Viewer 工具栏可能会消失。

  [#LC5064]

- 如果连接到启用了本地应用程序访问的 VDA，则当您按 Alt+Tab 键时，端点设备的任务切换器有时会在 VDA 会话中显示。

  [#LC5084]

- 从窗口模式更改为全屏模式时，启用了本地应用程序访问的桌面可能无法正确呈现。

  [#LC5091]

- 断开启用了本地应用程序访问的 VDA 的连接时，任务栏可能会保留在“自动隐藏”模式。

  [#LC5183]

**会话/连接**

- 在 NetScaler 客户端证书身份验证设置为“可选”的情况下尝试取消证书提示会导致启动已发布的应用程序失败，并显示未知客户端错误 1110。

  [#LC4169]

- 重新连接到客户端计算机后，快速切换用户的多屏幕会话可能仅在一个屏幕上显示该会话。

  [#LC4382]

- 如果从用户设备 1 启动无缝应用程序，然后通过 RDP 从用户设备 2 连接到该用户设备，启动的无缝应用程序可能会进入全屏模式，并且用户设备 1 的任务栏重叠。 即使在最小化并还原应用程序窗口后，该问题仍然存在。

  [#LC4682]

- 占用高带宽时，通过 NetScaler Gateway 连接的会话可能无响应。

  [#LC4710]

- 使用某些第三方软件（例如 Cisco WAAS）时，Citrix Receiver for Windows 会话可能会断开连接。

  [#LC4805]

- 此修复解决了基础组件中的内存问题。

  [#LC4903]

- 升级到 Citrix Receiver for Windows 4.4 后，首次登录时，尝试启动应用程序有时可能会失败，直至重新启动 Citrix Receiver for Windows。 此时将显示以下错误消息：

  “无法启动应用程序。 请与技术支持人员联系。”

  [#LC4975]

- 在某些用户设备上，尝试通过 Citrix Receiver 从 StoreFront 访问应用程序可能会失败。 成功添加应用商店后，枚举过程中可能会显示以下错误消息：

  无法连接到服务器
  请检查您的网络并重试
  重试

  [#LC5039]

- Single Sign-On 进程 (SSONSvr.exe) 可能会意外退出，或者凭据可能会自动传递到登录屏幕，导致显示手动输入凭据的提示。

  [#LC5123]

- Citrix Receiver 忽略 Internet Explorer 中的代理跳过列表。

  [#LC5131]

- 安装 Citrix Receiver for Windows 并通过注册表项或组策略对象 (GPO) 配置应用商店后，当您在重新启动虚拟机 (VM) 后首次登录时，应用程序可能无法枚举。

  [#LC5198]

- 如果在 Microsoft Internet Explorer 中启用了“自动检测设置”选项，Citrix Receiver 中的应用程序枚举可能会非常缓慢。

  [#LC5224]

- 启用了 Framehawk 后，鼠标上的滚动按钮在 XenDesktop 7.8 VDA 会话中可能无法执行任何操作。 XenDesktop 7.9 提供了相应的 VDA 端修复。

  [#LC5302]

- 尝试通过单击“开始”菜单中的图标启动应用程序有时会失败，即使您已登录也是如此。

  [#LC5306]

- 使用 Citrix Receiver for Windows 4.4 过程时，如果用户设备为 Android 设备，wfica32.exe 进程在第一个跃点会话中可能会意外退出。 在用户会话中，尝试在双跃点场景中启动已发布的应用程序时会出现此问题。

  [#LC5391]

- 执行触控并拖动手势过程中，使用无缝 EPIC 应用程序时鼠标按钮可能会保留在按下状态。 在无缝 EPIC 应用程序窗口外部松开触控输入时，会话可能会无响应。

[#LC5644]

**系统异常**

- Citrix Receiver for Windows 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。）

  [#LC4100]

- 在 Windows Media Player 中重复播放 .avi 文件时，wfica32.exe 进程可能会遇到死锁问题，并且可能会意外退出。

  [#LC4587]

- 通过代理启动已发布的应用程序时，Citrix Receiver for Windows 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。）

  [#LC5149]

- 在 Windows Vista 上安装 Citrix Receiver for Windows 4.4 后尝试添加帐户时，Citrix Authentication Manager (AuthMgrSvr.exe) 可能会意外退出。

  [#LC5242]

**用户体验**

- 如果启用了本地应用程序访问，则当您从最大化状态还原时，会话窗口可能会定位到 Desktop Viewer 窗口外部。

  [#LC2930]

- 执行触控并拖动手势过程中，来自 Citrix Receiver for Windows 的触控输入可能会向服务器发送某些无意中进行的鼠标事件。 这会导致无缝 EPIC 应用程序无响应。

  [#LC5459]

**用户界面**

- 尝试通过具有统一体验的 StoreFront 打开未订阅的内容可能会失败，并显示以下错误消息：

  所需的软件未安装，无法启动您的应用程序。

  [#LC4308]

- 在非英语操作系统中，在 Receiver for Windows 中显示的协议错误 1030 的文本可能会出现乱码。

  [#LC4687]

- 在外观模式下使用 VLC Media Player 时，如果启用了本地应用程序访问，端点设备可能会显示多个任务快捷方式，而不是显示一个。

  [#LC4744]

- 在无缝模式下，在 Microsoft Internet Explorer 的已发布实例中使用 GoToMeeting URL 打开时，GoToMeeting 图标可能不在任务栏中显示。

[#LC4810]

- 在 FastConnect API 用户之间切换时，将显示以下错误消息：

  您的应用程序当前不可用。 请在几分钟后重试。

  此外，当您使用 FastConnect API 登录时，不会从桌面中删除以前的用户应用程序快捷方式。

  [#LC5602]

**Web Interface**

- 如果用户设备上安装了早期版本的 Citrix Receiver，Web Interface 中将不显示 Citrix Receiver for Windows 安装页面。

  [#LC4242]

**其他**

- wfica32.exe 进程会占用 100% 的 CPU。

  [#LC4520]

- 使用 SelfService.exe -init –createprovider 命令（例如，C:\Program Files (x86)\Citrix\ICA Client\SelfServicePlugin\SelfService.exe -init -createprovider store https://<StoreFrontURL>/Citrix/store/discovery）创建应用商店时，会正确创建相关注册表项。 但是，如果单击通知区域中的 Receiver 图标以访问自助服务用户界面，则会从注册表中删除应用商店，并且可能会显示“添加帐户”对话框。

  [#LC5096]

- wfica32.exe 进程会占用 100% 的 CPU。

  [#LC5189]

- 可能不会保留 Client Selective Trust (CST) 设置，并且“HDX 文件访问”提示可能会针对第一次以及后续的启动显示，即使在选中“Do not ask me again for this virtual desktop”（对此虚拟桌面不再询问）选项后也是如此。 无论何时在注册表项“HKEY_Current_User\Software\Citrix\Ica Client\Client Selective Trust”下为相同的 VDA 创建新注册表，都会出现此问题，即使在选中该选项后也是如此。

  [#LC5598]

- 将 NetScaler 配置为 TLSv1.2 会阻止外部 Windows 7 用户设备添加 StoreFront 帐户。 此时可能会显示以下错误消息：

  无法联系身份验证服务。

  [#LC5737]

## Receiver for Windows 4.4 CU1 (4.4.1000)

比较：Citrix Receiver for Windows 4.4

Receiver for Windows 4.4 CU1 (4.4.1000) 包含 Receiver for Windows 4.0、4.0.1、4.1、4.1.2、4.1.100、4.1.200、4.2、4.2.100、4.3、4.3.100 和 4.4 中的所有修复以及以下新修复：



| | |
|---|---|
| HDX MediaStream | 会话/连接 |
| 安装、卸载、升级 | 系统异常 |
| 键盘 | 用户体验 |
| 本地应用程序访问 | 用户界面 |
| 打印 | |

**客户端设备问题**

- 使用 Citrix Receiver for Windows 4.3 时，通过 USB 3.0 连接的设备（包括键盘和鼠标设备）可能会停止运行并显示错误 DRIVER_POWER_STATE_FAILURE (0x9f)。

  [#LC4542]

- Surface Pro Type/Touch Cover 设备可用于 USB 重定向。 执行 USB 重定向后，鼠标光标/键盘可能不再在会话外部工作。 目前，已在安装时添加拒绝规则，以阻止 Surface Pro Type/Touch Cover 设备进行重定向。 有关这些规则的工作原理的更多详细信息，请参阅 CTX137939。

  注意：当前修复仅适用于全新安装的 Receiver。 对于升级版本，需要手动将以下拒绝规则添加到下列注册表。

  对于 32 位操作系统：
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB

  对于 64 位操作系统：
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\GenericUSB

  编辑 DeviceRules 值并添加适用于 USB 设备的特定拒绝规则。
  DENY:vid=045e pid=079A # Microsoft Surface Pro TouchCover
  DENY:vid=045e pid=079c # Microsoft Surface Pro Type Cover
  DENY:vid=045e pid=07dc # Microsoft Surface Pro 3 Type Cover
  DENY:vid=045e pid=07e4 # Microsoft Surface Pro 4 Type Cover with fingerprint reader
  DENY:vid=03eb pid=8209 # Surface Pro Atmel maXTouch Digitizer

  请按照相同的过程进行操作，为这些设备添加保证阻止重定向的 VID 和 PID。
  适用于特定设备的 DENY: vid=xxxx pid=xxxx 规则必须位于设备规则列表首位。

  [#LC4992]

**HDX MediaStream**

- 在本地应用程序访问会话内部打开 Internet Explorer 并浏览到包含 Flash 内容的 Web 页面时，如果打开并最大化某个应用程序，浏览器的 Flash 容器的内容会保留在屏幕上。

  [#LC4527]

**安装、卸载、升级**

- 尝试按照知识库文章 CTX135438 中的说明隐藏“添加帐户”窗口可能会失败。 应用此修复后，如果重置或重新启动 Citrix Receiver，“添加帐户”窗口有时在关闭后可能会再次弹出。

  [#LC4593]

**键盘**

- 如果已发布的应用程序使用 Ctrl+Alt+[Key] 的热键组合，并且如果 Alt+[Key] 或 Ctrl+[Key] 属于 Citrix 热键，则不会将该组合发送到服务器。

  [#LC3592]

- 使用无缝会话或应用程序时，鼠标单击有时不按预期运行。

  [#LC4779]

**本地应用程序访问**

- 安装适用于 Mozilla Firefox 便携式浏览器的 URL 重定向插件后，浏览器的下部可能会显示一个大白框。

  [#LC4351]

- 在会话中运行 redirector.exe 以注册/取消注册浏览器时，可能会显示一个弹出窗口，其中包含大多数用户确认没有价值的信息。 启用此增强功能后，不再显示该弹出窗口，除非运行带 /verbose 选项的 redirector.exe 命令。

  [#LC4480]

- 启用了本地应用程序访问的已发布桌面进行连接时，会话窗口可能不响应，或者可能会消失。

  [#LC4689]

- 在 Citrix Receiver 中同时启用了本地应用程序访问和 USB 重定向时，CDViewer.exe 进程可能不响应。

  [#LC5018]

**打印**

- 对 EMF 打印机驱动程序使用嵌入了符号的字体时，字体嵌入有时会失败。

  [#LC3334]

**无缝窗口**

- 启动并最小化无缝窗口时，无法从任务栏还原或最大化。

  [#LC3990]

**会话/连接**

- 无法使用 WPAD 通过代理正确重新连接会话。 重新连接到断开的会话时，显示以下消息：“The network connection to your application was interrupted. Try to access your application later or contact your help desk.”（与应用程序的网络连接已中断。请稍后再尝试访问您的应用程序，或者与技术支持人员联系。）

[#LC3077]

- 无法向与该区域的可信站点的特定配置不同的区域添加 StoreFront URL。

  [#LC3281]

- 要使用本地文件类型关联，请使用以下注册表项。 以下注册表项默认设置为 true。 该注册表项设置为 true 时，如果客户端计算机上没有与该文件关联的任何其他程序，本地文件图标将更改为 Citrix Receiver 图标。
  HKEY_CURRENT_USER\Software\Citrix\Dazzle\EnabledDefaultFTAs=false (REG_SZ)

  [#LC4096]

- “会话可靠性”和“客户端自动重新连接”超时断开连接后，会话启动延迟，并且会话共享不起作用。

  [#LC4143]

- 映射的客户端驱动器的大小可能无法正确显示，如果文件超过 1 TB，则无法将其复制到驱动器。 应用此修复后，如果超过 1 TB，驱动器将显示为 0.99 TB。 映射的客户端驱动器的大小仅在启用了旧版客户端驱动器映射选项时显示。

  [#LC4214]

- 启用本地应用程序访问 (LAA) 和桌面锁定后，重新连接到全屏模式的已发布服务器桌面会话会导致会话失去焦点，不再响应。

  [#LC4253]

- 使用“切换用户”Windows 登录选项会改变虚拟桌面的会话分辨率。

  [#LC4452]

- 使用 Citrix Receiver 时，应用程序启动可能不适用于 ICO SDK。

  [来自 RcvrForWin4.4_14.4.1000][#LC4550]

- 用户通过自助服务插件登录 StoreFront 时，SelfService.exe 进程可能会间歇性每隔一小时从其他活动窗口中获取焦点。

  [#LC4628]

- 切换网络时，Epic 应用程序有时会失去焦点。

  [#LC4731]

- 尝试启动应用程序时，wfica32.exe 进程可能会意外退出，并显示以下错误消息：The connection to failed with status (Unknown client error 0)（连接到 失败，状态为(未知客户端错误 0)）。

  [#LC4768]

- NotificationDelay 注册表设置控制无缝连接的连接进度条外观的延迟。 使用自助服务插件启动应用程序时，设置此注册表有时不起作用。 此修复解决了该问题。

  在 32 位 Windows 上：
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  名称：NotificationDelay
  类型：REG_DWORD

数据：<延迟，单位为毫秒>

在 64 位 Windows 上：
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432node\Citrix\ICA Client
名称：NotificationDelay
类型：REG_DWORD
数据：<延迟，单位为毫秒>

[#LC4969]

**系统异常**

- 通过 GPO 更新 XenApp 服务 URL 并应用新 GPO 或使用新应用商店名称（例如，store1 和 store2）更新同一 GPO 时，Citrix Receiver for Windows 可能会意外退出。

  [#LC4145]

- wfica32.exe 进程可能会遇到访问冲突并意外退出。

  [#LC4482]

- SelfService.exe 进程占用 100% 的 CPU。

  [#LC4494]

- 端点设备上启用了 GPU 切换功能的会话可能无响应。

  [#LC4562]

**用户体验**

- 此修复在使用客户端音频的实时模式时改进了对播放一小段时间的声音的支持。 此修复仅适用于低质量音频。

  [#LC2783]

- 在 XenApp 7.5 中，有时听不见 Windows 系统声音。

  [#LC3926]

- 在不稳定的网络环境中会显示弹出消息，例如，“Your apps are not available at this time. Please try again in a few minutes or contact your help desk with this information: Cannot contact [ServerName].”（您的应用程序当前不可用。请几分钟后再试，或者与技术支持人员联系并提供以下信息: 无法访问 [ServerName]）和“The network connection to your application was interrupted. Try to access your application later or contact your help desk.”（与应用程序的网络连接已中断。请稍后再尝试访问您的应用程序，或者与技术支持人员联系。）。 此修复增加了对允许您禁用弹出消息的以下注册表项的支持。

  在 32 位 Windows 上：
  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle
  名称：SuppressDisconnectMessage
  类型：REG_DWORD
  数据：24(0x18)

  在 64 位 Windows 上：
  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle

名称：SuppressDisconnectMessage
类型：REG_DWORD
数据：24(0x18)

[#LC4378]

**用户界面**

- 如果手动删除快捷方式后刷新应用程序，快捷方式有时不再显示。

  [#LC4020]

## Receiver for Windows 4.4

比较：Citrix Receiver for Windows 4.3.100

Receiver for Windows 4.4 包含 Receiver for Windows 4.0、4.0.1、4.1、4.1.2、4.1.100、4.1.200、4.2、4.2.100、4.3 和 4.3.100 中的所有修复以及以下新修复：



**安装、卸载、升级**

- 卸载 Citrix Receiver 后，Citrix HDX WMI 提供程序可能不运行。

  [#LC3943]

**键盘**

- 启用了会话可靠性时，“对齐”功能将无法在重新连接的会话中运行。 “对齐”功能是您在**控制面板** > **鼠标** > **指针选项** > **自动将鼠标指针移动到对话框中的默认按钮**中配置的一项鼠标/键盘设置。

  [#LC1252]

- 使用 Alt+Tab 键在窗口之间切换将在已发布的桌面会话中激活应用程序菜单。

  [#LC2947]

- Citrix Receiver 和 RDP 会话共享相同的键盘快捷方式“Ctrl+Alt+End”键，用于在终端会话中调用“Ctrl+Alt+Delete”键。 因此，在 Citrix Receiver 会话内部运行时，RDP 会话的键盘快捷方式不起作用。

  应用此修复后，“Ctrl+Alt+End”键的键盘快捷方式将不属于 Citrix Receiver 会话的默认键，并且可以通过设置以下注册表项进

行启用：

- *在 32 位 Windows 上*：

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client
  名称：EnableCtrlAltEnd
  类型：DWORD
  值：1

- *在 64 位 Windows 上*：

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client
  名称：EnableCtrlAltEnd
  类型：DWORD
  值：1（如果值为 0，则将在 RDP 会话内部使用 Ctrl+Alt+End 组合键。）

[#LC3131]

- 升级到 Citrix Receiver 4.2 后，双跳场景中的鼠标单击操作可能不正常。

  [#LC3770]

**本地应用程序访问**

- 启用了本地应用程序访问时，单击鼠标以调整虚拟机上的会话大小会导致虚拟机无响应。

  [#LC1853]

**登录/身份验证**

- 尝试使用缓存的凭据的完全限定域名 (FQDN) 登录时单点登录不起作用。

  [#LC3305]

- Receiver 配置为在已发布的桌面会话中对 Web Interface 或 StoreFront 服务器使用直通身份验证时，Receiver 可能不会传递凭据，而是提示输入凭据。

  [#LC3388]

**会话/连接**

- 配置了会话预启动时，如果尝试重新连接到正在运行已发布应用程序的会话，该已发布应用程序的另一个实例将添加到同一会话中。

  [#LC1701]

- 在前端运行的窗口会话可能会意外丢失焦点。

  [#LC2198]

- 在注册表配置单元 **HKEY_LOCAL_MACHINE\SOFTWARE\\Citrix\AuthManager** 下将策略设置为 **ProxyEnabled = false**，这将跳过在 IE 上配置的代理服务器。 如果使用 32 位操作系统体系结构，**Wow6432Node** 配置单元将不适用。

[#LC3129]

- 在独立端口上配置了音频和视频数据的多端口或多流配置中，音频与视频会不同步。

  [#LC3181]

- 启动 XenApp 已发布的应用程序时，使用智能卡进行身份验证登录 Receiver 4.2 for Windows 的用户可能会看到 PIN 身份验证提示。

  [#LC3187]

- 已发布的应用程序的配置“KEYWORDS:prefer”可能不起作用。 用户注销 Receiver 以及 SelfService.exe 进行意外关闭时会出现此问题。

  [#LC3190]

- 登录 Citrix Receiver 后，应用程序快捷方式可能需要很长时间才能在用户设备的“开始”菜单和桌面上显示。

  [#LC3323]

- 尝试在已发布的 Microsoft Outlook 实例中打开电子邮件消息中的 Windows 媒体 (.wmv) 视频可能会失败。

  [#LC3453]

- Desktop Viewer 从全屏模式切换到窗口模式时，使用 Receiver 过程中 XenDesktop 会话中可能会显示一个浮动工具栏。

  [#LC3526]

- 安装了 Desktop Lock 以及 Receiver 4.3 的系统锁定时，桌面会话可能会断开连接，而非继续保持活动状态。

  要启用此修复，请设置以下注册表项：

  - *在 32 位 Windows 上*：

    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle
    名称：LiveInDesktopDisconnectonLock
    类型：REG_SZ
    值：False
  - *在 64 位 Windows 上*：

    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle
    名称：LiveInDesktopDisconnectonLock
    类型：REG_SZ
    值：False

  [#LC3579]

- 如果为您订阅了 Citrix Receiver 的通过流技术推送到客户端的应用程序，并且该 Receiver 未安装 Citrix 脱机插件，刷新 Citrix Receiver 中的应用程序过程中可能会显示以下错误消息：

  您的应用程序当前不可用

  [#LC3609]

- 通过 Citrix Receiver for Windows 登录时，同一用户的相同交付组中可能会显示不同工作线程上的多个预启动会话。

  [#LC3676]

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

  [#LC3773]

- 如果设备上安装了 4.3 之前的 Receiver for Windows 版本，并且用户将操作系统从 Windows 7、Windows 8 或 Windows 8.1 升级到 Windows 10，通过“添加或删除程序”卸载 Receiver 可能会失败。 尝试升级到 Receiver for Windows 4.3 也会失败。

  [#LC3789]

- 尝试启动新会话过程中，wfica32.exe 进程可能会意外关闭。

  [#LC3795]

- 通过 Citrix Receiver 打开已发布的桌面中的应用程序，并将 %appdata% 文件夹更改为另一个文件服务器时，可能会显示以下错误消息：

  错误 1046: 未加载虚拟驱动程序

  [#LC3981]

- 本地安装的 Lotus Notes 示例的警报窗口可以从已发布的应用程序中获取键盘焦点。

  [#LC3889]

- 图标会同时在“开始”菜单中以及桌面上的类别文件夹中显示。 不应存在桌面的类别文件夹。 使用注册表项 UseCategoryAsStartMenuPath 同时控制“开始”菜单和桌面的类别文件夹中的图标时会出现此问题。

  要启用此项修复，必须设置以下注册表项：

  - 注册表项 UseDifferentPathsforStartmenuAndDesktop 设置为 false 时，注册表项 UseCategoryAsStartMenuPath 将同时控制“开始”菜单和桌面的类别文件夹的创建。
  - 注册表项 UseDifferentPathsforStartmenuAndDesktop 设置为 true 时，注册表项 UseCategoryAsStartMenuPath 将控制“开始”菜单中的图标类别文件夹的创建。 注册表项 UseCategoryAsDesktopPath 将控制桌面上图标类别文件夹的创建。

  [#LC4052]

- 尝试更改 Citrix Receiver 中的密码可能会失败并显示以下错误消息：

  您输入的旧密码不正确。

  [#LC4081]

**系统异常**

- 使用 Microsoft AX Dynamics 2009 或 Excel 2007 时，Citrix Receiver 4.x 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。）

[#LC3776]

**用户体验**

- 尝试将图标快捷方式添加到 Citrix Receiver 会话中的桌面时，某些图标可能不会显示应用程序特定的图标。 而是显示普通的白色页面图标。

  [#LC4097]

- 即使 EnableFTU 设置为 false，也无法禁用 Citrix Receiver 连接向导。

  要阻止显示连接向导，请使用 Receiver.adm/Receiver.admx 禁用“启用 FTU”策略设置：

  **计算机配置 > 管理模板 > Citrix 组件 > Citrix Receiver > 自助服务 > 启用 FTU**

  [#LC4133]

**用户界面**

- 安装适用于 Mozilla Firefox 浏览器的 URL 重定向插件后，浏览器的下部可能会显示一个大型白色框。

  [#LC3409]

- 设置了无缝注册表标志 ENABLE COLOR SYNC 时，无缝会话可能无法从用户设备继承某些颜色，而是显示黑色。

  要启用此修复，请设置以下注册表项：

  HKEY_LOCAL_MACHINE/System/CurrentControlSet/Control/Citrix/wfshell/TWI
  名称：SeamlessFlags
  类型：REG_DWORD
  值：0x10

  [#LC3768]

- 更改 StoreFront URL 时，如果打开并关闭 Citrix Receiver 自助服务插件用户界面，设置为已禁用的应用程序可能会显示为虚影图标，而非显示为灰色。

  [#LC3863]

- 某些应用程序有时无法枚举，此时会显示空白图标，而非显示与这些应用程序关联的图标。

  [#LC4065]

- 如果更改了 Citrix Studio 中已发布应用程序的图标，应用程序的桌面快捷方式将不更新。

  [#LC4124]

**其他**

- 向计算机上位于代理后面的 Citrix Receiver 中添加帐户时，Citrix Receiver 在联系信标时不时用代理设置（位置设置为无，而非外部或内部）。

  [#LC2100]

- 从注册表项中删除注册表值 ConnectionCenter 会导致强制修复 Citrix Receiver：

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

[#LC3751]

**注意**：本版本的 Citrix Receiver 还包括版本 4.3、4.2、4.1 和 4.0 中的所有修复。

# Citrix Receiver for Windows 4.4 的已知问题

Jan 20, 2017

## Citrix Receiver for Windows 4.4 CU3 (4.4.3000) 中的已知问题

在本版本中观察到以下已知问题以及 Citrix Receiver for Windows 4.4、4.4 CU1 (4.4.1000) 和 4.4 CU2 (4.4.2000) 中的已知问题：

- ACR/SR 超时后尝试退出 Citrix Receiver 可能不起作用。 解决方法：注销并重新登录 Citrix Receiver 或退出 wfcrun32 进程。 [#336，#4115]

## Citrix Receiver for Windows 4.4 CU2 (4.4.2000) 中的已知问题

在本版本中观察到以下已知问题以及 Citrix Receiver for Windows 4.4 和 4.4 CU1 (4.4.1000) 中的已知问题：

- 在不具有 Desktop Viewer 工具栏的远程桌面会话中启动已发布的桌面时，可能不会显示“Tip: Exiting Full Screen Mode”（提示: 正在退出全屏模式）对话窗口。 键盘快捷键 Shift+F2 可控制是否显示该会话窗口的标题栏。 要解决此问题，请按下“Shift+F2”查看您的桌面，然后最小化会话窗口。

  [#LC4445，#639585]

## Citrix Receiver for Windows 4.4 CU1 (4.4.1000) 中的已知问题

在本版本中观察到以下已知问题以及 Citrix Receiver for Windows 4.4 中的已知问题：

- 卸载 Citrix Receiver for Windows 后，可能不会删除注册表项 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\（在 32 位系统中）和 HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\（在 64 位系统中）下的注册表值“Installer”。

  [#635242]

## Citrix Receiver for Windows 4.4 中的已知问题

在本版本中发现了以下已知问题：

- 更改 Windows 10 Surface Pro 设备上的托管应用程序的方向时，会显示一个工具提示屏幕，指出“正在退出全屏模式”。 要解决此问题，请通过设置以下注册表项禁用提示对话框消息：

  HKEY_CURRENT_USER\Software\Citrix\ica client\keyboard mappings\tips

  使用值 1 将禁用提示，使用值 0 将启用提示；将此注册表值设置为 1 将禁用所有提示。

  [#608346]

> **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。

- 在白色带阴影的背景显示在屏幕文本后面的位置，Windows 7 客户端上的 VDA 会话可能会遇到显示问题。 客户端未安装最新版本的 GFX 驱动程序时会出现此问题。 在客户端安装了较旧版本的 NVIDIA 驱动程序时解决此问题。

要在客户端安装了较旧版本的 NVIDIA 驱动程序时解决此问题，请执行以下操作：

1. 访问 NVIDIA 控制面板。
2. 访问“Video”（视频）设置。
3. 在“How do you make color adjustments?”（如何调整颜色）部分中，选择“With NVIDIA Settings”（通过 NVIDIA 设置）。
4. 在“NVIDIA settings”（NVIDIA 设置）中，选择“Advanced”（高级）选项卡。
5. 在“Advanced”（高级）选项卡中，将“Dynamic Range”（动态范围）设置为“Full (0-255)”（完整(0-255)）。

也可以通过更新安装了最新 GFX 驱动程序的客户端计算机来跳过建议的解决方法。

[#610197]

> **注意**
>
> 有关 NVIDIA 驱动程序使用情况的详细信息，请参阅 NVIDIA 支持站点上的 Dynamic RGB Range Capability（动态 RGB 范围功能）页面。

- 如果在客户端上启用了硬件解码，连接到处于 H.264 图形模式的 Windows 2008 R2 VDA 时，性能将下降。 Citrix 建议您在 VDA 上使用旧版图形模式以避免此问题。

  [#609292，611580]

- 在客户端上多次断开连接并重新连接后，ACR 无法重新连接到会话，导致强制用户重新登录 StoreFront。

  [#567938]

- NetScaler Gateway End Point Analysis Plugin (EPA) 不支持本机 Windows Receiver。

  [#534790]

- 关闭匿名用户会话时，桌面查看器将显示一条不适用于匿名登录的消息。 在此类情况下，用户断开连接时 Receiver 将自动注销匿名会话。 由于此类登录没有身份验证，因此，匿名会话不支持重新连接、在客户端之间漫游或工作区控制。

  [#481561]

- 在某些本地化实例中（例如，运行中文版 Citrix Receiver），本地化的登录凭据的用户名中包含代理项对时，虚拟桌面和应用程序可能无法启动。

  [#556174]

- 如果您以域管理员身份安装了 Receiver，并在安装过程中选择“启用 CEIP”选项，CEIP 窗口在“关于”菜单中将显示会灰色。

  [#556179]

- 由于 RAVE 存在兼容性问题，因此，音量控制对会话内部的 RealTimes for Real Player 可能不起作用。

  [#573549]

- 使用脱机模式时，Receiver 将遇到以下问题：
  - 网络连接断开不导致显示通知用户条件的错误消息。 在脱机模式下使用 Receiver 时，无法刷新应用程序或订阅/取消订阅应用程序。 [#559792，#560091，#560360]
  - 重新建立网络连接时，不同步在 Receiver 处于脱机模式下对应用程序或桌面所做的更改。 [#560362]

- 注销 Receiver，然后重新登录时，用户名不在界面右上角显示。

[#562107]

- 智能卡授权对 XenApp Services 站点不起作用，此功能适用于 StoreFront 站点。 要解决此问题，请将智能卡授权指向 StoreFront 站点。
- 用户界面中的字段标签上可能仍会显示对 SSL 的引用，例如 **TLS and Compliance Mode Configuration**（TLS 和合规模式配置）。 这些内容将在未来的版本中更新。
- 桌面锁定客户端的登录屏幕上不显示语言栏。 解决方法是使用浮动语言兰。

  [#502678]
- 在窗口模式下打开会话时，Citrix Desktop Viewer 中显示的快捷方式选项不起作用。

  [#510529]
- 断开连接期间，Desktop Viewer 警报消息不适用于匿名用户会话。 这是由设计确定的。

  [#481561]
- Receiver for Windows 不能使用用户（非域）帐户安装在 Windows 2012 R2 计算机上。

  要解决此问题，请执行以下操作：

  1. 单击**开始**，键入 **regedit** 并按 **Enter** 键。
  2. 找到以下设置：

  HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\Installer

  创建：DisableMSI 类型：REG_DWORD 值 = 0（0 应允许您进行安装）

  [#492508]
- 在桌面锁定模式下，有时候会显示系统托盘通知。

  [#488620]
- 不自动为终端服务器 VDA 显示虚拟键盘。 解决方法是使用 Desktop Viewer 工具栏上的图标打开虚拟键盘；对于应用程序，则通过任务栏上的虚拟键盘图标来打开虚拟键盘。

  [#502774]
- 远程处理经由通用 USB 的 USB 耳机 (Logitech USB H340) 时，音频质量低于预期质量。 这是由设计确定的。 在 USB 重定向时不执行音频优化。 在将来的版本中，会考虑增强此功能。

  [#469670]
- 在通过 XenApp 和 XenDesktop 7.0 之前的版本远程连接的应用程序上，或 Window 2008 R2 上的 XenApp 和 XenDesktop 7.0 或更高版本上，捏合和缩放手势不起作用。

  [#517877]

# 系统要求和兼容性

Sep 20, 2016

设备

## 操作系统

- Windows 10
- Windows 8.1，32 位和 64 位版本（包括 Embedded Edition）
- Windows 8，32 位和 64 位版本（包括 Embedded Edition）
- Windows 7，32 位和 64 位版本（包括 Embedded Edition）
- Windows Vista，32 位和 64 位版本
- Windows Thin PC
- Windows Server 2012 R2 Standard Edition 和 Datacenter Edition
- Windows Server 2012 Standard Edition 和 Datacenter Edition
- Windows Server 2008 R2（64 位版本）
- Windows Server 2008（32 位和 64 位版本）

## 硬件

- 适用于彩色监视器的 VGA 或 SVGA 视频适配器
- 用于提供声音支持的 Windows 兼容声卡（可选）
- 要实现与服务器场的网络连接，需要网络接口卡 (NIC) 和相应的网络传输软件
- 客户端计算机应安装最新版本的 GFX 驱动程序，才能体验更出色的图形性能。

支持触摸的设备

Citrix Receiver for Windows 4.4 可用于 Windows 7 和 8.1 便携式可触摸计算机、可触摸平板电脑，和使用 XenApp 和 XenDesktop 7 或更高版本以及 Windows 7、8 和 2012 虚拟桌面代理的监视器。

Citrix 服务器

- XenApp（以下任意产品）：
  - Citrix XenApp 7.6
  - Citrix XenApp 7.5
  - Citrix XenApp 6.5 Feature Pack 2 Windows Server 2008 R2
  - Citrix XenApp 6.5 Feature Pack 1 Windows Server 2008 R2
  - Citrix XenApp 6.5 for Windows Server 2008 R2
  - 适用于 Unix 操作系统的 Citrix XenApp 4 Feature Pack 2
- XenDesktop（以下任意产品）：
  - XenDesktop 7.6
  - XenDesktop 7.5
  - XenDesktop 7.1
  - XenDesktop 7.0
- Citrix VDI-in-a-Box
  - VDI-in-a-Box 5.3
  - VDI-in-a-Box 5.2
- 您可以将 Citrix Receiver for Windows 4.4 基于浏览器的访问功能与 StoreFront Receiver for Web 和 Web Interface 结合使用，安装或不安装 NetScaler Gateway 插件均可以。
  StoreFront：

- StoreFront 3.0.x、2.6, 2.5 和 2.1
  用于直接访问 StoreFront 应用商店。
- 配置有 Receiver for Web 站点的 StoreFront
  用于从 Web 浏览器访问 StoreFront 应用商店。 有关此部署的限制，请参阅 Receiver for Web sites（Receiver for Web 站点）上的“Important considerations”（重要注意事项）。

Web Interface 与 NetScaler VPN 客户端结合使用：

- Web Interface 5.4 for Windows Web 站点。
  提供从 Web 浏览器访问虚拟桌面和应用程序的功能。
- Web Interface 5.4 for Windows 与 XenApp Services 或 XenDesktop Services 站点

- 为用户部署 Citrix Receiver 的方法：
  - 允许用户从 receiver.citrix.com 下载，然后结合使用电子邮件或服务地址与 StoreFront。
  - 允许从 Citrix Receiver for Web 站点（配置了 StoreFront）安装。
  - 允许从 Citrix Web Interface 5.4 安装 Receiver。
  - 使用 Active Directory (AD) 组策略对象 (GPOs) 部署。
  - 使用 Microsoft System Center 2012 Configuration Manager 部署。

### 浏览器

- Internet Explorer
  与 Citrix Receiver for Web 或 Web Interface 的连接支持 32 位 Internet Explorer。 有关支持的 Internet Explorer 版本，请参阅 StoreFront 系统要求和 Web Interface 系统要求。

- Mozilla Firefox 18.x（支持的最低版本）
- Google Chrome 21 或 20（需要 StoreFront）。

> **注意**
>
> 有关对 Google Chrome NPAPI 支持所做的更改的信息，请参阅 Citrix 博客文章 Preparing for NPAPI being disabled by Google Chrome（准备 Google Chrome 禁用的 NPAPI）。

### 连接

Citrix Receiver for Windows 支持通过以下任一配置的 HTTPS 和 ICA-over-TLS 连接。

- 对于 LAN 连接：
  - 使用 StoreFront Services 或 Citrix Receiver for Web 站点的 StoreFront
  - Web Interface 5.4 for Windows，使用 Web Interface 或 XenApp Services 站点

  有关已加入域和未加入域的设备的信息，请参阅 XenDesktop 7 文档。

- 对于安全的远程连接或本地连接：
  - Citrix NetScaler Gateway 11.x
  - Citrix NetScaler Gateway 10.5

  支持已加入域的托管 Windows 设备（本地及远程，使用或不使用 VPN 皆可）以及未加入域的设备（使用或不使用 VPN 皆可）。

  有关 StoreFront 支持的 NetScaler Gateway 和 Access Gateway 版本的信息，请参阅 StoreFront 系统要求。

> **注意**
>
> 除非另有指定，否则本主题中 NetScaler Gateway 的参考资料也适用于 Access Gateway。

## 关于安全连接和证书

> **注意**
>
> 有关安全证书的其他信息，请参阅安全连接和安全通信下的主题。

### 私有（自签名）证书

如果远程网关上安装了专用证书，用户设备上必须安装组织的证书颁发机构颁发的根证书，才能使用 Receiver 成功访问 Citrix 资源。

> **注意**
>
> 如果连接时无法验证远程网关的证书（因为本地密钥库中不包含根证书），系统会显示一条警告，指出该证书不受信任。 如果用户选择忽略警告继续，则会显示一个应用程序列表，但应用程序不会启动。

### 在用户设备上安装根证书

有关在用户设备上安装根证书以及配置 Web Interface 以供证书使用的信息，请参阅确保 Receiver 通信安全。

### 通配符证书

通配符证书用于代替同一域内任意服务器的各个服务器证书。 Citrix Receiver for Windows 支持通配符证书，但是，只能在符合组织的安全策略时使用这些证书。 在实际中，可以考虑使用通配符证书的替代选项，如使用者备用名称 (SAN) 扩展中包含服务器名称列表的证书。 此类证书可能由私有证书颁发机构或公共证书颁发机构签发。

### 中间证书与 NetScaler Gateway

如果您的证书链中包含中间证书，必须将该中间证书附加到 NetScaler Gateway 服务器证书。 有关信息，请参阅 Configuring Intermediate Certificates（配置中间证书）。

### 身份验证

对于到 StoreFront 的连接，Citrix Receiver 支持以下身份验证方法：

| | Receiver for Web（使用浏览器） | StoreFront Services 站点（本机） | StoreFront XenApp Services 站点（本机） | NetScaler 到 Receiver for Web（浏览器） | NetScaler 到 StoreFront Services 站点（本机） |
|---|---|---|---|---|---|
| 匿名 | 是 | 是 | | | |
| 域 | 是 | 是 | 是 | 是* | 是* |

| 域直通 | Receiver for Web（使用浏览器） | StoreFront 是 Services 站点（本机） | StoreFront 是 XenApp Services 站点（本机） | NetScaler 到 Receiver for Web（浏览器） | NetScaler 到 StoreFront Services 站点（本机） |
|---|---|---|---|---|---|
| 安全令牌 | | | | 是* | 是* |
| 双因素（域 + 安全令牌） | | | | 是* | 是* |
| SMS | | | | 是* | 是* |
| 智能卡 | 是 | 是 | 否 | | |
| 用户证书 | | | | 是（NetScaler 插件） | 是（NetScaler 插件） |

* 在设备上安装或不安装 NetScaler 插件均可。

> **注意**
>
> Citrix Receiver for Windows 4.4 支持通过 NetScaler Gateway 到 StoreFront 本机服务的 2FA（域 + 安全令牌）。

对于到 Web Interface 5.4 的连接，Citrix Receiver 支持以下身份验证方法（Web Interface 使用术语“显式”表示域和安全令牌身份验证）：

| | Web Interface（浏览器） | Web Interface XenApp Services 站点 | NetScaler 到 Web Interface（浏览器） | NetScaler 到 Web Interface XenApp Services 站点 |
|---|---|---|---|---|
| 匿名 | 是 | | | |
| 域 | 是 | 是 | 是* | |
| 域直通 | 是 | 是 | | |
| 安全令牌 | | | 是* | |
| 双因素（域 + 安全令牌） | | | 是* | |
| SMS | | | 是* | |

| | | | | |
|---|---|---|---|---|
| 智能卡 | 是 | 否 | | |
| 用户证书 | | | 是（NetScaler 插件） | |

* 仅在包含 NetScaler Gateway 的部署中可用，而无论设备上是否已安装关联的插件。

有关身份验证的信息，请参阅 NetScaler Gateway 文档中的配置身份验证和授权以及 StoreFront 文档中的管理主题。 有关 Web Interface 支持的身份验证方法的信息，请参阅为 Web Interface 配置身份验证。

### 升级

可以使用 Citrix Receiver for Windows 4.x 升级 Receiver for Windows 3.x 和 Citrix 联机插件 12.x。 有关升级的详细信息，请参阅升级注意事项。

> **注意**
>
> 如果要从 Citrix Receiver 3.4 升级到版本 4.2.100，请按照 Upgrading from Receiver 3.4 to Receiver 4.2.100 Guide（《从 Receiver 3.4 升级到 Receiver 4.2.100 指南》）中的说明进行操作。 版本 4.2.100 不支持最终用户进行原位升级。 IT 管理员必须准备环境，以便网络中的所有用户都能够成功完成升级。 升级指南中提供的信息中包含逐步升级说明。

### 其他

- **.NET Framework 要求**
  - 自助服务插件需要 .NET 3.5 Service Pack 1，才能允许用户从 Receiver 窗口或命令行订阅和启动桌面和应用程序。 有关详细信息，请参阅使用命令行参数配置和安装 Receiver for Windows。
  - 需要安装 .NET 2.0 Service Pack 1 和 Microsoft Visual C++ 2005 Service Pack 1 可再发行组件包，以确保正确显示 Receiver 图标。 Microsoft Visual C++ 2005 Service Pack 1 软件包包含在 .NET 2.0 Service Pack 1、.NET 3.5 和 .NET 3.5 Service Pack 1 中；也可单独获取此软件包。
  - 对于 XenDesktop 连接：要使用 Desktop Viewer，必需安装 .NET 2.0 Service Pack 1 或更高版本。 要求此版本是因为，如果 Internet 访问不可用，证书吊销校验会放慢连接启动的时间。 使用此版本的 Framework 而非 .NET 2.0 可以关闭校验并改善启动时间。
- 有关将 Receiver 与 Microsoft Lync Server 2013 和 Microsoft Lync 2013 VDI Plug-in for Windows 结合使用的信息，请参阅 XenDesktop、XenApp 和 Citrix Receiver 对 Microsoft Lync 2013 VDI 插件的支持。
- **支持的连接方法和网络传输协议：**
  - TCP/IP+HTTP
    有关可能需要的其他值，请参阅 CTX 134341。
  - TLS+HTTPS

> **Important**
>
> 如果在 StoreFront 中将应用商店的传输类型配置为 HTTP，则必须将以下键值添加到注册表项 HKLM\Software\[Wow6432Node\]Citrix\AuthManager 中：ConnectionSecurityMode=Any。

> **警告**
>
> “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。

# 安装

Aug 25, 2016

可以通过以下方式安装 CitrixReceiver.exe 安装软件包：

- 由用户从 Citrix.com 或自有下载站点安装
  - 从 Citrix.com 或自有下载站点获取 Receiver 的 Receiver 新用户可以通过输入电子邮件地址（而非服务器 URL）来设置一个帐户。 Receiver 会确定与电子邮件地址相关联的是 NetScaler Gateway（或 Access Gateway）还是 StoreFront 服务器，然后提示用户登录并继续安装。 此功能称为“基于电子邮件的帐户发现”。
    注意：首次使用的用户是指未在设备上安装 Receiver 的用户。
  - 如果 Receiver 是从 Citrix.com 以外的站点（例如 Receiver for Web 站点）下载的，则不会对首次使用的用户执行基于电子邮件的发现。
  - 如果您的站点需要配置 Receiver，请使用备用部署方法。
- 从 Receiver for Web 或从 Web Interface 登录屏幕自动完成。
  - 首次使用 Receiver 的用户可以通过输入服务器 URL 或下载置备 (CR) 文件来设置帐户。
- 使用电子软件分发 (Electronic Software Distribution, ESD) 工具安装
  - 第一次使用 Receiver 的用户必须输入服务器 URL 或打开置备文件才能设置帐户。

除非要使用直通身份验证，否则不需要具有管理员权限即可安装 Receiver。

### HDX RealTime Media Engine (RTME)

单个安装程序中现在同时包含最新版本的 Citrix Receiver for Windows 和 HDX RTME 安装程序。 安装本版本的 Citrix Receiver 时，HDX RTME 将包含在可执行文件 (.exe) 中。

> **注意**
>
> 安装最新版本的具有集成 RTME 支持功能的 Citrix Receiver 要求用户在主机上具有管理权限。

安装或升级 Citrix Receiver 时，请注意以下 HDX RTME 问题：

- 最新版本的 Citrix Receiver 包含最新版本的 HDX RTME（版本 1.0.0.1）；如果要安装 RTME，不需要进一步执行任何安装。
- 支持从早期版本的 Receiver 升级到最新的捆绑版本（带 RTME 的 Citrix Receiver）。 以前安装的 RTME 版本将被最新版本覆盖；不支持从相同版本的 Receiver 升级到最新的捆绑版本（例如，从 Receiver 4.4 升级到捆绑版本的带 RTME 的 Receiver 4.4）。
- 如果您已安装早期版本的 RTME，安装最新版本的 Receiver 将自动更新客户端设备上的 RTME。
- 如果存在更新版本的 RTME，安装程序将保留最新版本。

> **Important**
>
> XenApp/XenDesktop 服务器上的 HDX RealTime Connector 的最低版本必须为 2.0.0.417（GA 版本），以便与新 RTME 包兼容；即，不能将 RTME 2.0 与 1.8 RTME Connector 结合使用。

### 手动升级到 Citrix Receiver for Windows

对于使用 StoreFront 的部署情形：

- 对于 BYOD（自带设备）用户，最佳做法是按照产品文档站点上的这些产品的文档中的相关说明配置最新的 NetScaler Gateway 和 StoreFront 版本。 将 StoreFront 创建的置备文件附加到一封电子邮件中，并通知用户如何在安装完 Receiver 后升级和打开此置备文件。
- 提供置备文件的另一个方法是，通知用户输入 NetScaler Gateway（或 Access Gateway Enterprise Edition）的 URL。 或者，如果您按 StoreFront 文档中所述配置了基于电子邮件的帐户发现，则可通知用户输入其电子邮件地址。
- 另一种方法是，按照 StoreFront 文档所述配置 Receiver for Web 站点，然后按照从 Receiver for Web 部署 Receiver for Windows 所述完成配置。 通知用户如何升级 Receiver、访问 Receiver for Web 站点以及从 Receiver for Web 下载置备文件（单击用户名，然后单击“激活”）。

对于使用 Web Interface 的部署情形：

- 升级包含 Receiver for Windows 的 Web Interface 站点，并按照从 Web Interface 登录屏幕部署 Receiver for Windows 所述完成配置。 告知用户如何升级 Receiver。 例如，您可以创建一个下载站点，使用户能够获取重命名的 Receiver 安装程序。

## 升级注意事项

> ### 提示
>
> 对 Receiver for Windows 4.x 配置直通身份验证（单点登录）的过程已更改。 有关信息，请参阅使用命令行参数配置和安装 Receiver for Windows 中关于 /includeSSON 的说明。

可以使用 Citrix Receiver for Windows 4.x 升级 Receiver for Windows 3.x 和 Citrix 联机插件 12.x。

如果以每计算机方式安装了 Receiver for Windows 3.x，则不支持每用户升级方式（由不具有管理权限的用户进行安装）。

如果以每用户方式安装了 Receiver for Windows 3.x，则不支持每计算机升级方式。

# 手动安装和卸载 Receiver for Windows

Feb 02, 2016

可以从安装介质、网络共享、Windows 资源管理器或命令行通过手动运行 CitrixReceiver.exe 安装程序包安装 Receiver。 有关命令行安装参数和空间要求，请参阅使用命令行参数配置和安装 Receiver for Windows。

> **Important**
>
> 对 Receiver for Windows 4.x 配置直通身份验证（单点登录）的过程已更改。 有关信息，请参阅使用命令行参数配置和安装 Receiver for Windows 中关于 /includeSSON 的说明。

如果公司政策禁止您使用 .exe 文件，则请参阅 How to Manually Extract, Install, and Remove Individual .msi Files（如何手动提取、安装和删除各个 .msi 文件）。

**手动安装并配置 Receiver 以实现直通身份验证**

可以在 XenApp 和 XenDesktop 的直通身份验证场景中使用 Receiver。 本部分内容还介绍如何安装和配置 CitrixReciver.exe 以对 Web Interface 或 StoreFront 服务器连接使用直通身份验证。

成功安装并配置后，用户不需要再输入凭据即可访问其 XenApp/XenDesktop 资源。 来自客户端计算机的凭据将被自动传输到端点。

请注意直通身份验证的以下要求：

- Citrix Receiver for Windows 安装包为 CitrixReceiver.exe。
- 相应加载组策略文件：
  - receiver.adm（位于安装了 Citrix Receiver 的 Windows 计算机上的 %SystemDrive%\Program Files (x86)\Citrix\ICA Client\Configuration 文件夹中）；Windows XP,、indows 2003 和瘦客户端中必须存在 receiver.adm 文件。
  - receiver.admx、receiver.adml（位于安装了 Citrix Receiver 的 Windows 计算机上的 %SystemDrive%\Program Files (x86)\Citrix\ICA Client\Configuration 文件夹中）；要将 ADMX 文件加载到 GPO 中，请参阅使用组策略对象模板配置 Receiver 中的“关于 ADMX 模板的使用”部分。
- 需要具有本地管理员权限，才能在客户端设备上安装和配置软件。
  **注意**：仅当瘦客户端运行 XPe 操作系统时才使用 .adm 文件。

不使用企业软件部署工具（例如 Citrix Merchandising Server 或 Microsoft System Center Configuration Manager）时，可以通过两种不同的部署方案实现 XenApp/XenDesktop 的直通身份验证：

1. 分别在各种计算机上手动安装 Citrix Receiver 并使用本地组策略（导入 receiver.adm、receiver.admx、receiver.adml）进行配置。
   **注意**：此方案适用于非常小的环境。

2. 使用 Active Directory 组策略安装 Citrix Receiver（例如，使用 XenApp 随附的 **CheckAndDeployCitrixReceiverEnterpriseStartupScript.bat**）。 然后可以使用 Active Directory 组策略管理控制台将使用 **receiver.adm**、**receiver.admx**、**receiver.adml** 的配置应用到大量集中管理的计算机。

由于复杂度级别更高，因此，本文不介绍此方案。 有关详细信息，请参阅 CTX134280 How to Deploy Citrix Receiver Enterprise for Pass-Through Authentication Using Active Directory Group Policy（如何使用 Active Directory 组策略部署

Citrix Receiver Enterprise 以实现直通身份验证）。

**注意**：Citrix 强烈建议使用之前在非生产环境中彻底测试并验证本文中概述的所有步骤。

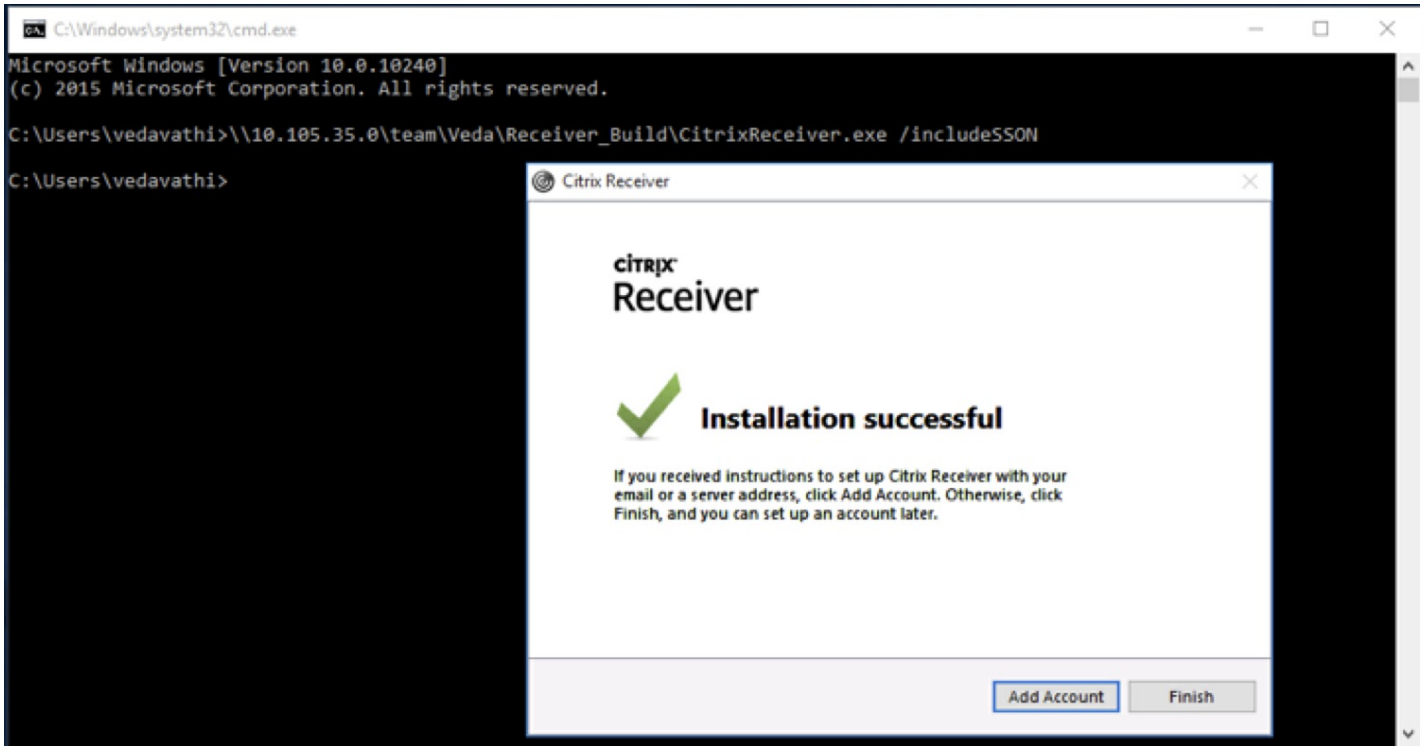
**手动安装并配置 Receiver 以实现直通身份验证**：

1. 在控制器上使用 PowerShell 运行以下命令：**Set-BrokerSite -TrustedRequestsSentToTheXmlServicePort $True**
2. 以具有管理权限的用户身份登录客户端计算机。
3. 开始执行安装过程之前，请从客户端计算机中卸载所有现有的联机插件或 Citrix Receiver for Windows 的安装。
4. 从 Citrix 下载下载 Citrix Receiver for Windows 安装包 (CitrixReceiver.exe)。

   通过命令行或 GUI 使用恰当的安装部署。

**使用命令行**：

1. 打开 **Windows 命令提示窗口**，并更改 CitrixReceiver.exe 所在的目录。
2. 在**命令提示**窗口中，运行以下命令以安装启用了 SSON 功能的 Citrix Receiver：**CitrixReceiver.exe /includeSSON**。 请注意使用命令行参数配置和安装 Receiver for Windows 一文中的信息；参数 /includeSSON 为 Receiver standard (CitrixReceiver.exe) 启用单点登录。 Receiver enterprise (CitrixReceiverEnterprise.exe) 不支持此方案，该版本的 Receiver 默认安装单点登录
3. 安装完成后，将显示一条弹出消息：Installation successful（安装成功）。




**使用 GUI**：

1. 双击 CitrixReceiver.exe。
2. 在“启用单点登录”安装向导中，选中“启用单点登录”复选框以安装启用了 SSON 功能的 Citrix Receiver。 这等同于使用命令行通过 /includeSSON 标志安装 Receiver。

**注意**：本地管理员进行安装时，“启用单点登录”安装向导仅适用于在加入域的计算机上执行的全新安装。

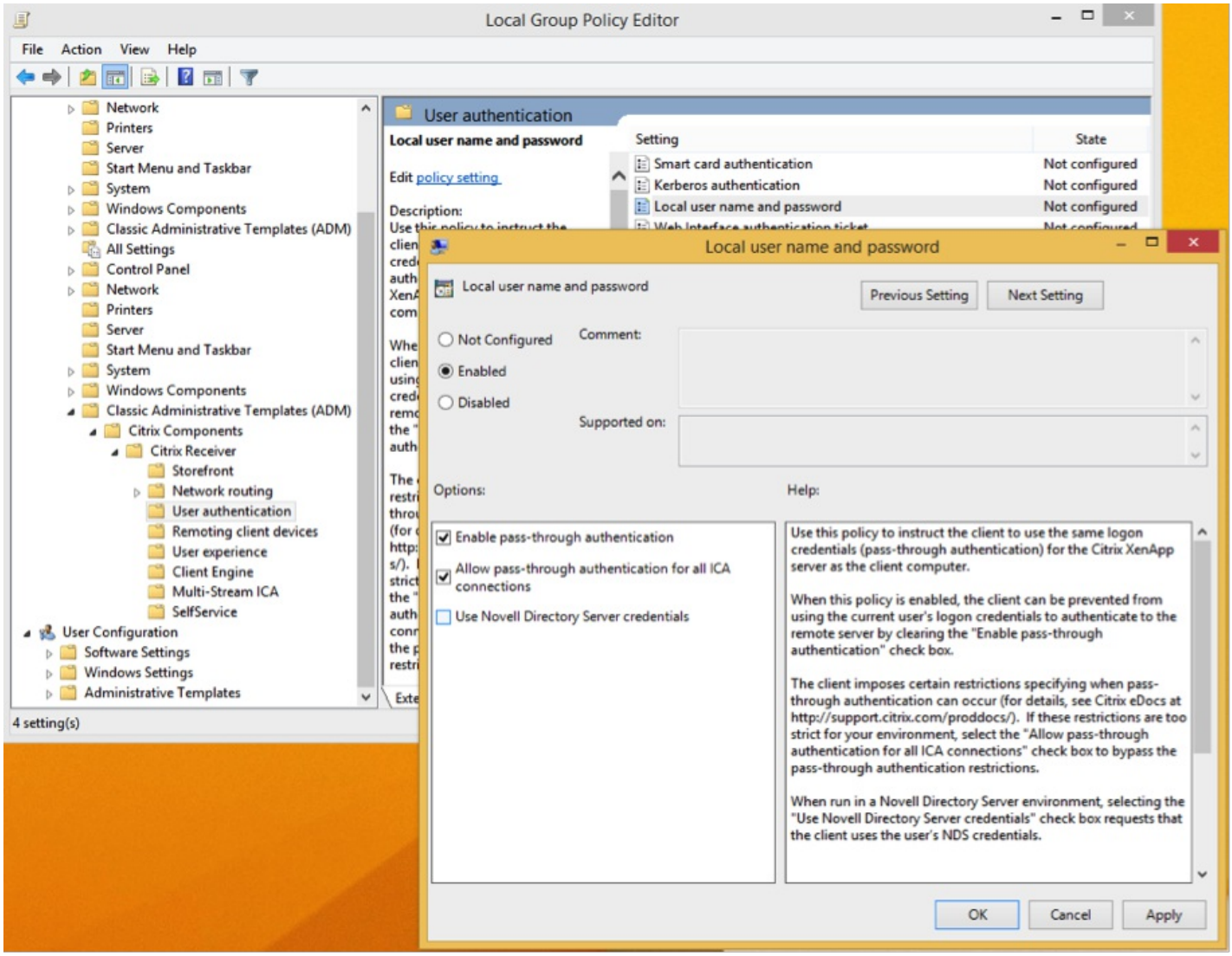

**通过本地组策略编辑器 (GPO) 配置 SSON**

默认情况下，SSON 的组策略为**启用直通身份验证**；不使用 Desktop Viewer 和 Receiver for Web 时，该策略足以使 SSON 起作用。 使用 Desktop Viewer 时，请启用 GPO 以**允许对所有 ICA 连接进行直通身份验证**。

**使用 ADM 文件配置用户身份验证**

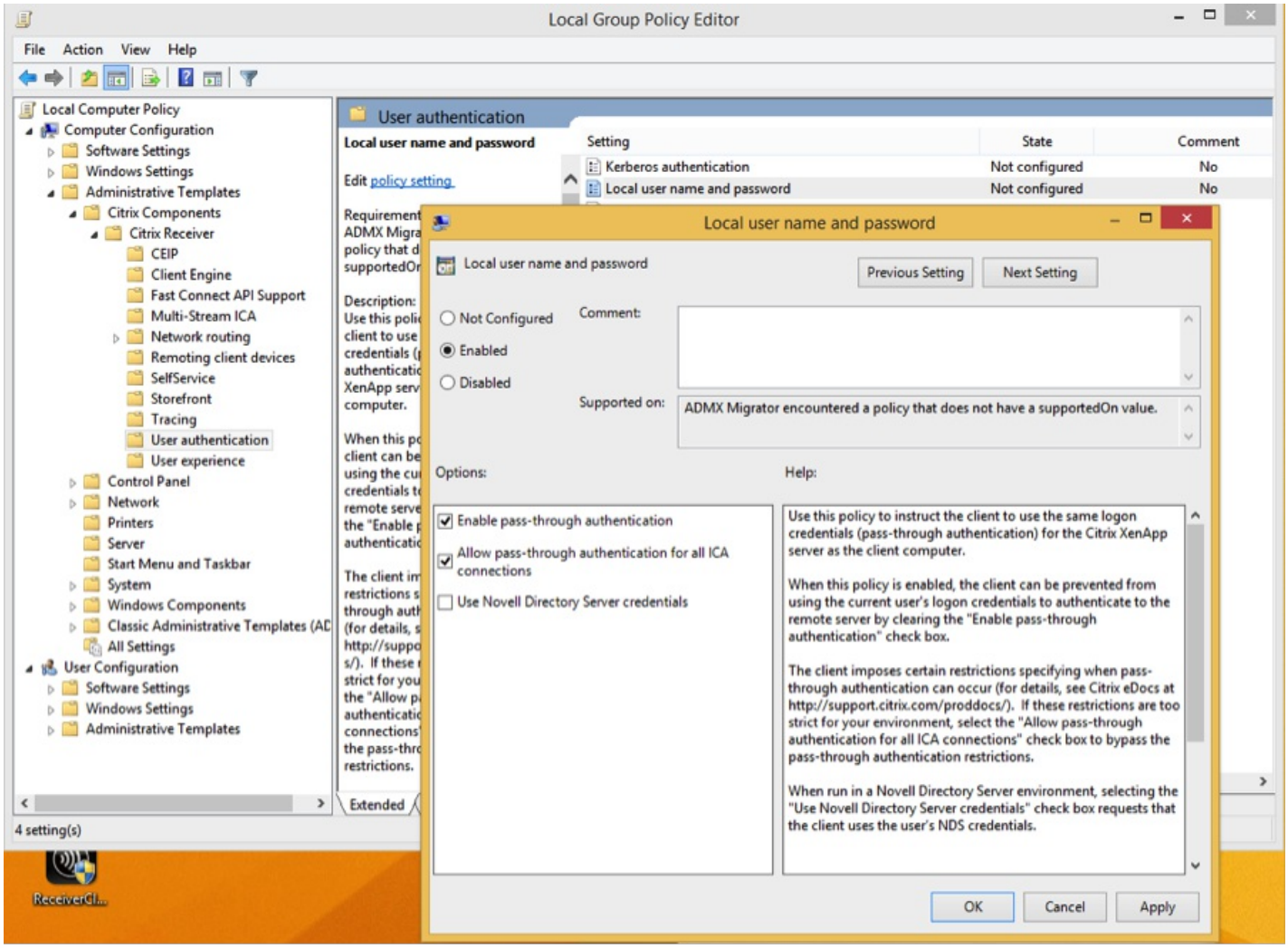
1. 通过运行命令 **gpedit.msc** 或在“开始”菜单中搜索“编辑组策略”，打开本地组策略编辑器。
2. 通过选择“计算机配置”将 receiver.adm 模板添加到本地组策略编辑器，方法是右键单击“管理模板”，然后选择“添加/删除模板”> 单击**添加**。
3. 成功添加 receiver.adm 模板后，依次展开“计算机配置”>“管理模板”>“经典管理模板(ADM)”>“Citrix 组件”>“Citrix Receiver”>“用户身份验证”。

**注意：**根据 StoreFront\Receiver for Web 配置和安全设置，可能必须选择**允许对所有 ICA 进行直通身份验证**，直通身份验证才能起作用。



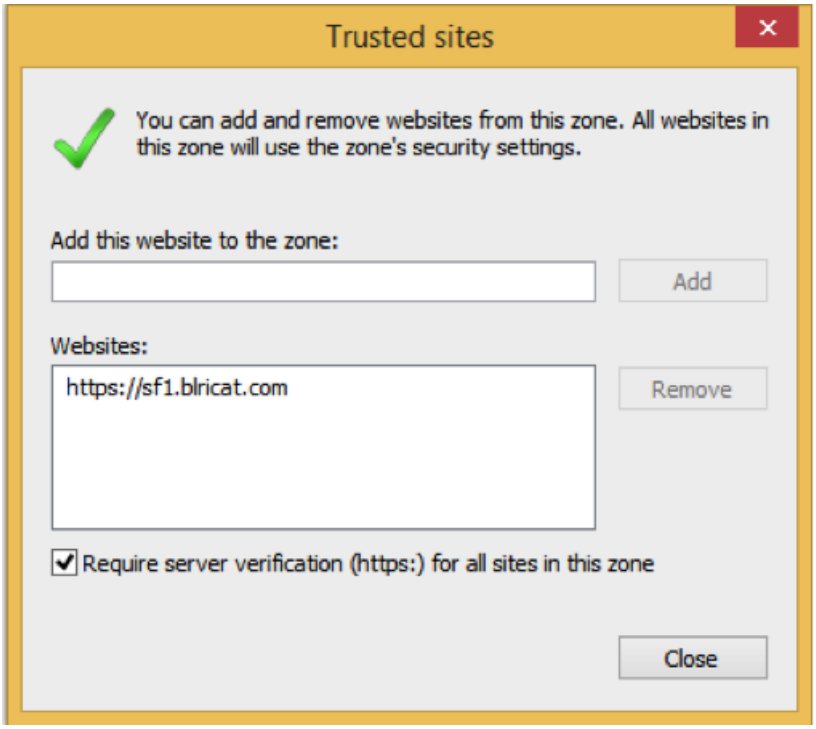

**使用 ADMX 文件进行直通身份验证**

1. 将 receiver.admx 和 receiver.adml 模板添加到本地组策略编辑器。 请参阅使用组策略对象模板配置 Receiver 中的“关于 ADMX 模板的使用”部分。
2. 成功添加 eceiver.admx 和 receiver.adml 模板后，展开“计算机配置”>“管理模板”>“Citrix 组件”>“Citrix Receiver”>“用户身份验证”。
3. 选择**本地用户名密码**设置。
4. 启用上述策略时，请选择“启用直通身份验证”和“允许对所有 ICA 进行直通身份验证”选项。




**将完全限定的域名 (FQDN) 添加到“受信任的站点”列表**

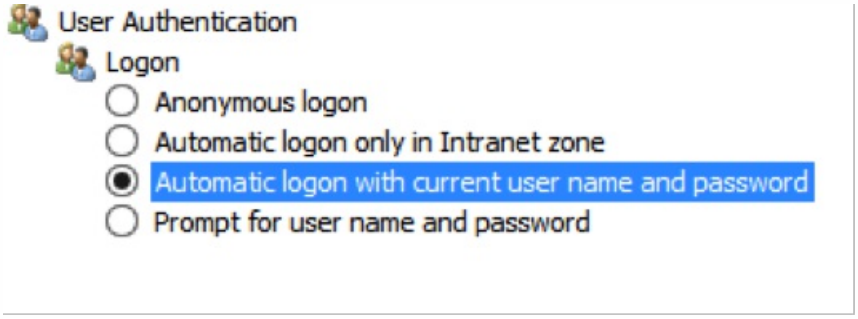
1. 在客户端设备上，启动 Internet Explorer。
2. 在 Internet Explorer 中，单击“工具”>“Internet 选项”>“受信任的站点”。
3. 单击**添加**将 FQDN 添加到“受信任的站点”列表（例如 https://sf1.blricat.com）。 添加后，该站点将显示在“白名单”列表中：




将某个 Web 站点添加到“受信任的站点”列表后，选择恰当的用户身份验证方法：

1. 在“Internet 选项”下的“安全”选项卡中，选择“受信任的站点”。
2. 选择**自定义级别，安全区域**。
3. 滚动到列表底部，然后选择**自动使用当前用户名和密码登录**。
4. 重新启动客户端设备以应用所做的更改。

**注意**：使用当前用户名和密码执行的自动登录是一项每用户设置；如果这些设置不是本地管理员配置的，则每个用户都必须配置此选项；要在全局应用此设置，请配置 GPO，方法是同时在“Internet”和“受信任的站点”中的“自定义级别”下添加此值。




**通过 Single Sign-on (SSON) 进行升级的重要注意事项**

下表包含与使用命令行通过 SSON 升级 Receiver 有关的信息：

| 升级之前安装了 SSON | 新 Receiver 安装期间的 SSON 选项<br><br>（命令行 - /includeSSON 或选中 UI 选项） | 行为 |
| --- | --- | --- |
| | | |

| | | |
|---|---|---|
| 是 | 是 | 已升级 SSON 组件<br>已创建注册表项<br>SSON 功能起作用 – 无需启用任何操作 |
| 是 | 否 | 已升级 SSON 组件<br>已创建注册表项<br>SSON 功能起作用 – 无需启用任何操作 |
| 否 | 是 | 已升级 SSON 组件<br>已创建注册表项<br>SSON 功能已禁用 – 用户需要卸载 Receiver，然后在选中 SSON 的前提下通过命令行选项 /includeSSON 或 GUI 选项重新安装 Receiver |
| 否 | 否 | 未安装 SSON 组件 |

**注意**：升级现有版本的 Citrix Receiver 时，“启用单点登录”安装向导不可用。

### 删除 Receiver for Windows

您可以使用 Windows 的“程序和功能”实用工具（添加/删除程序）卸载 Receiver。

**使用命令行删除 Receiver**

还可以通过键入以下命令从命令行卸载 Receiver：

CitrixReceiver.exe /uninstall

从用户设备上卸载 Receiver 后，由 Receiver.adm/Receiver.adml 或 Receiver.admx 创建的自定义 Receiver 注册表项仍保留在 HKEY_LOCAL_MACHINE 和 HKEY_LOCAL_USER 下的 Software\Policies\Citrix\ICA Client 目录中。 如果重新安装 Receiver，可能会强制实施这些策略，这也许会导致出现异常行为。 要删除这些自定义项，请手动执行删除操作。

> **警告**
>
> “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。

# 使用命令行参数配置和安装 Receiver for Windows

Aug 25, 2016

可以通过指定命令行选项自定义 Citrix Receiver 安装程序。 安装程序包将在启动安装程序前自解压到用户的临时目录中，并且要求 %temp% 目录中大约具有 57.8 MB 的可用空间。 空间要求包括程序文件、用户数据以及启动多个应用程序后使用的临时目录。

> **警告**
>
> “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。

要从命令提示窗口中安装 Citrix Receiver for Windows，请使用以下语法：

**CitrixReceiver.exe [Options]**

显示使用信息

| | |
|---|---|
| **选项** | /? 或 -help |
| **说明** | 此开关显示用法信息 |
| **示例用法** | CitrixReceiver.exe /?<br>CitrixReceiver.exe /help |

禁止在 UI 安装期间重新启动

| | |
|---|---|
| **选项** | /noreboot |
| **说明** | 禁止在 UI 安装期间重新启动。 无提示安装不需要此选项。 如果您禁止显示重新启动提示，Receiver 安装时处于暂停状态的任何 USB 设备在重新启动用户设备后才能被 Receiver 识别。 |
| **示例用法** | CitrixReceiver.exe /noreboot |

无提示安装

| | |
|---|---|
| **选项** | /silent |
| **说明** | 禁用错误和进度对话框以执行完全无提示安装。 |
| **示例用法** | CitrixReceiver.exe /silent |

| | |
|---|---|
| | |

启用单点登录身份验证

| | |
|---|---|
| **选项** | /includeSSON |
| **说明** | 安装单点登录（直通）身份验证。 智能卡单点登录需要此选项。<br><br>命令行中包含 /includeSSON 时，启用相关选项 ENABLE_SSON。 如果要使用 ADDLOCAL= 指定各项功能，并希望安装 Single Sign-On，则还必须指定值 ENABLE_SSON。<br><br>要为用户设备启用直通身份验证，必须从包含选项 /includeSSON 的命令行通过本地管理员权限安装 Receiver。 在用户设备上，还必须启用“管理模板”>“经典管理模板(ADM)”>“Citrix 组件”>“Citrix Receiver”>“用户身份验证”中的以下策略：<br><br>● 本地用户名和密码<br>● 启用直通身份验证<br>● 允许对所有 ICA 执行直通身份验证（可能需要，具体取决于 Web Interface 配置和安全设置）<br><br>在完成更改后，重新启动用户设备。 有关详细信息，请参阅 How to Manually Install and Configure Citrix Receiver for Pass-Through Authentication（如何手动安装和配置 Citrix Receiver 以实现直通身份验证）。<br><br>注意：智能卡、Kerberos 和本地用户名和密码策略相互依赖。配置顺序非常重要。 建议首先禁用不需要的策略，然后启用所需的策略。 请仔细验证结果。 |
| **示例用法** | CitrixReceiver.exe /includeSSON |

在指定了 /includeSSON 时启用单点登录

| | |
|---|---|
| **选项** | ENABLE_SSON={Yes \| No} |
| **说明** | 在指定了 /includeSSON 时启用单点登录。 默认值为 Yes。 在同时指定了 /includeSSON 时启用单点登录。 智能卡单点登录需要此属性。 请注意，启用带有单点登录身份验证的安装之后，用户必须注销并重新登录其设备。 需要具有管理员权限。 |
| **示例用法** | CitrixReceiver.exe /ENABLE_SSON=Yes |

AlwaysOn 跟踪

| | |
|---|---|
| **选** | |

| | |
|---|---|
| **项** | /EnableTracing={true \| false} |
| **说明** | 默认情况下启用此功能。 使用此属性可明确启用或禁用 AlwaysOn 跟踪功能。 AlwaysOn 跟踪功能可帮助收集与连接时间有关的关键日志。 解决间歇性出现的连接问题时，这些日志证明非常有用。 AlwaysOn 跟踪策略将覆盖此设置。<br><br>默认情况下，AlwaysOn 跟踪日志文件位于 *C:\Users\\AppData\Local\Temp\CTXReceiverLogs\\xxx.et*/目录中。 |
| **示例用法** | CitrixReceiver.exe /EnableTracing=true |

使用 Citrix 客户体验改善计划 (CEIP)

| | |
|---|---|
| **选项** | /EnableCEIP={true \| false} |
| **说明** | 如果允许参与 Citrix 客户体验改善计划 (CEIP)，匿名统计数据和使用信息将发送给 Citrix 以帮助 Citrix 改进其产品质量和性能。 |
| **示例用法** | CitrixReceiver.exe /EnableCEIP=true |

指定安装目录

| | |
|---|---|
| **选项** | INSTALLDIR=<安装目录> |
| **说明** | 指定安装路径，其中安装目录为大多数 Citrix Receiver 软件的安装位置。 默认值为 C:\Program Files\Citrix\Receiver。 以下 Receiver 组件将安装在路径 C:\Program Files\Citrix 中：身份验证管理器、Citrix Receiver 和自助服务插件。<br><br>如果您使用此选项并指定了一个安装目录，则必须在安装目录 \Receiver 目录中安装 RIInstaller.msi，并在安装目录中安装其他 .msi 文件。 |
| **示例用法** | CitrixReceiver.exe INSTALLDIR=c:\Citrix\Test |

识别连接到服务器场的用户设备

| | |
|---|---|
| **选项** | CLIENT_NAME=<*ClientName*> |
| **说明** | 指定客户端名称，其中 ClientName 用来识别连接到服务器场的用户设备的名称。 默认值为 %COMPUTERNAME% |

| | |
|---|---|
| **示例用法** | CitrixReceiver.exe CLIENT_NAME=%COMPUTERNAME%. |

动态客户端名称

| | |
|---|---|
| **选项** | ENABLE_CLIENT_NAME=Yes \| No |
| **说明** | 动态客户端名称功能可以使客户端名称始终与计算机名称相同。 当用户更改其计算机名称时，客户端名称会随之相应更改。 默认值为 Yes。 要禁用动态客户端名称支持，请将此属性设置为 No，并为 CLIENT_NAME 属性指定一个值。 |
| **示例用法** | CitrixReceiver.exe DYNAMIC_NAME=Yes |

安装指定的组件

| | |
|---|---|
| **选项** | ADDLOCAL= |
| **说明** | 安装一个或多个指定的组件。 指定多个参数时，请用逗号分隔每个参数，并且参数之间不能有空格。 名称区分大小写。 如果未指定此参数，则默认安装所有组件。<br><br>注意：ReceiverInside 和 ICA_Client 是所有其他组件的必备项，必须安装。<br><br>注意：未指定 ADDLOCAL 时，将安装除 SSON 以外的所有其他默认组件。<br><br>这些组件包括：<br><br>● ReceiverInside – 安装 Citrix Receiver 体验（Receiver 操作的必需组件）。<br>● ICA_Client – 安装标准 Citrix Receiver（Receiver 操作的必需组件）。<br>● WebHelper – 安装 WebHelper 组件。此组件用于从 StoreFront 中获取 ICA 文件并将其传递给 HDX Engine。此外，还用于验证环境参数并将其与 StoreFront 共享（与 ICO 客户端检测类似）。<br>● SSON – 安装单点登录。 需要具有管理员权限。<br>● AM – 安装身份验证管理器。<br>● SELFSERVICE – 安装自助服务插件。 必须在命令行中指定 AM 值，且必须在用户设备上安装 .NET 3.5 Service Pack 1。 自助服务插件对 Windows Thin PC 设备不可用，该设备不支持 .NET 3.5。<br>● 有关为自助服务插件 (SSP) 编写脚本和 Receiver for Windows 4.2 及更高版本中可用参数列表的信息，请参阅 http://support.citrix.com/article/CTX200337。<br>● 自助服务插件允许用户从 Receiver 窗口或命令行访问虚拟桌面和应用程序，如本部分后面的“从命令行启动虚拟桌面或应用程序”中所述。<br>● USB – 安装 USB 支持功能。 需要具有管理员权限。<br>● DesktopViewer – 安装 Desktop Viewer。<br>● Flash – 安装 HDX Media Stream for Flash。<br>● Vd3d – 启用 Windows Aero 体验（面向支持此功能的操作系统）。 |
| **示** | |

| | |
|---|---|
| **例用法** | CitrixReceiver.exe ADDLOCAL=ReceiverInside, ICA_Client, SSON |

配置未通过 Merchandising Server 交付对象配置的应用商店

| | |
|---|---|
| **选项** | ALLOWADDSTORE={N \| S \| A} |
| **说明** | 指定用户是否能够添加和删除未通过 Merchandising Server 交付对象配置的应用商店；用户可以启用或禁用通过 Merchandising Server 交付对象配置的应用商店，但不能删除这些应用商店或者更改名称或 URL。默认值为 S。 选项包括：<br>● N – 不允许用户添加或删除自己的应用商店。<br>● S – 仅允许用户添加或删除安全应用商店（已配置 HTTPS）。<br>● A – 允许用户添加或删除安全应用商店 (HTTPS) 和非安全应用商店 (HTTP)。 如果 Citrix Receiver 是按每用户方式安装的，则不适用。<br>也可以通过更新注册表项 HKLM\Software\[Wow6432Node\]Citrix\Dazzle\AllowAddStore 控制此功能。<br>注意：默认情况下仅允许安全 (HTTPS) 应用商店并建议将其用于生产环境。 在测试环境中，您可以通过以下配置使用 HTTP 应用商店连接：<br>1. 将 HKLM\Software\[Wow6432Node\]Citrix\Dazzle\AllowAddStore 设置为 A 以允许用户添加非安全应用商店。<br>2. 将 HKLM\Software\[Wow6432Node\]Citrix\Dazzle\AllowSavePwd 设置为 A 以允许用户保存非安全应用商店的密码。<br>3. 要添加在 StoreFront 中配置的 TransportType 为 HTTP 的应用商店，请将值 ConnectionSecurityMode（REG_SZ 类型）添加到 HKLM\Software\[Wow6432Node\]Citrix\AuthManager 并将其设置为 Any。<br>4. 退出并重新启动 Citrix Receiver。 |
| **示例用法** | CitrixReceiver.exe ALLOWADDSTORE=N |

使用 PNAgent 协议在本地保存应用商店的凭据

| | |
|---|---|
| **选项** | ALLOWSAVEPWD={N \| S \| A} |
| | 指定用户是否能够添加和删除未通过 Merchandising Server 交付对象配置的应用商店；用户可以启用或禁用通过 Merchandising Server 交付对象配置的应用商店，但不能删除这些应用商店或者更改名称或 URL。默认值为 S。 选项包括：<br>● N – 不允许用户保存密码。<br>● S – 仅允许用户保存安全应用商店的密码（已配置 HTTPS）。<br>● A – 允许用户保存安全应用商店 (HTTPS) 和非安全应用商店 (HTTP) 的密码。 |

| | |
|---|---|
| **说明** | 也可以通过更新注册表项 HKLM\Software\[Wow6432Node]\Citrix\Dazzle\AllowSavePwd 控制此功能。<br><br>注意：如果 AllowSavePwd 不起作用，则必须手动添加以下注册表项。<br><br>• 32 位操作系统客户端的注册表项：HKLM\Software\Citrix\AuthManager<br>• 64 位操作系统客户端的注册表项：HKLM\Software\wow6432node\Citrix\AuthManager<br>• 类型：REG_SZ<br>• 值：never – 绝不允许用户保存密码。 secureonly – 仅允许用户保存安全应用商店的密码（通过 HTTPS 配置）。 always – 允许用户保存安全应用商店 (HTTPS) 和不安全应用商店 (HTTP) 的密码。 |
| **示例用法** | CitrixReceiver.exe ALLOWSAVEPWD=N |

选择证书

| | |
|---|---|
| **选项** | AM_CERTIFICATESELECTIONMODE={Prompt \| SmartCardDefault \| LatestExpiry} |
| **说明** | 使用此选项选择证书。默认值为 Prompt，该值将提示用户从列表中选择证书。 更改此属性可选择默认证书（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。<br><br>还可以通过更新注册表项 HKCU 或 HKLM\Software\[Wow6432Node\]Citrix\AuthManager: CertificateSelectionMode={ Prompt \| SmartCardDefault \| LatestExpiry } 控制此功能。 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。 |
| **示例用法** | CitrixReceiver.exe AM_CERTIFICATESELECTIONMODE=Prompt |

使用 CSP 组件管理智能卡 PIN 条目

| | |
|---|---|
| **选项** | AM_SMARTCARDPINENTRY=CSP |
| **说明** | 使用 CSP 组件管理智能卡 PIN 条目。 默认情况下，向用户显示的 PIN 提示由 Citrix 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。 指定此属性可使用 CSP 组件管理 PIN 条目，包括提示输入 PIN。 |
| **示例用法** | CitrixReceiver.exe AM_SMARTCARDPINENTRY=CSP |

使用 Kerberos

| | |
|---|---|
| **选项** | ENABLE_KERBEROS={Yes \| No} |
| **说明** | 默认值为 No。 指定 HDX 引擎是否应使用 Kerberos 身份验证，并仅在启用了单点登录（直通）身份验证时应用。有关详细信息，请参阅配置使用 Kerberos 的域直通身份验证。 |
| **示例用法** | CitrixReceiver.exe ENABLE_KERBEROS=No |

显示旧 FTA 图标

| | |
|---|---|
| **选项** | LEGACYFTAICONS={False \| True} |
| **说明** | 使用此选项显示旧 FTA 图标。 默认值为 False。 指定是否为与订购的应用程序具有文件类型关联的文档显示应用程序图标。 如果此参数设置为 False，Windows 将为未向其分配特定图标的文档生成图标。 Windows 生成的图标由较小版本的应用程序图标覆盖的通用文档图标组成。 如果您计划向运行 Windows 7 的用户交付 Microsoft Office 应用程序，Citrix 建议启用此选项。 |
| **示例用法** | CitrixReceiver.exe LEGACYFTAICONS=False |

启用预启动功能

| | |
|---|---|
| **选项** | ENABLEPRELAUNCH={False \| True} |
| **说明** | 默认值为 False。 有关会话预启动的信息，请参阅缩短应用程序启动时间。 |
| **示例用法** | CitrixReceiver.exe ENABLEPRELAUNCH=False |

指定“开始”菜单快捷方式的目录

| | |
|---|---|
| **选项** | STARTMENUDIR={Directory Name} |
| | 默认情况下，应用程序显示在开始 > 所有程序下。 可以将程序文件夹下的相对路径指定为包含已订阅应用程序的快捷方式。 例如，要将快捷方式放置在“开始”>“所有程序”>“Receiver”下，请指定 STARTMENUDIR=\Receiver\。 用户可以随时更改文件夹名称或删除该文件夹。<br><br>还可以通过注册表项控制此功能：为 StartMenuDir 创建一个注册表项 REG_SZ，并将其值设置为 \相对路径。 位置：<br><br>HKLM\Software\[Wow6432Node\]Citrix\Dazzle |

| | |
|---|---|
| **说明** | HKCU\Software\Citrix\Dazzle<br><br>对于通过指定了客户端应用程序文件夹（也称为 Program Neighborhood 文件夹）的 XenApp 发布的应用程序，可以按如下所述将客户端应用程序文件夹指定为附加到快捷方式路径：为 UseCategoryAsStartMenuPath 创建一个注册表项 REG_SZ，并将其值设置为 true。 使用如上所述的相同注册表位置。<br><br>注意：Windows 8/8.1 不允许在“开始”菜单中创建嵌入式文件夹。 “应用程序”将单独显示或在根文件夹下显示，不在通过 XenApp 定义的“类别”子文件夹中显示。<br><br>示例<br><br>• 如果客户端应用程序文件夹为 \office，UseCategoryAsStartMenuPath 为 true，并且未指定 StartMenuDiris，则会将快捷方式放置在“开始”>“所有程序”>“Office”下。<br>• 如果客户端应用程序文件夹为 \Office，UseCategoryAsStartMenuPath 为 true，StartMenuDir 为 \Receiver，则会将快捷方式放置在“开始”>“所有程序”>“Receiver”>“Office”下。<br><br>对这些设置所做的更改不会影响已创建的快捷方式。 要删除快捷方式，必须卸载并重新安装应用程序。 |
| **示例用法** | CitrixReceiver.exe STARTMENUDIR=\Office |

指定应用商店名称

| | |
|---|---|
| **选项** | STOREx="storename;http[s]://servername.domain/IISLocation/discovery;[On \| Off]; [storedescription]" [STOREy="..."] |
| **说明** | 使用此选项可指定应用商店名称。 最多可以指定 10 个应用商店与 Citrix Receiver 结合使用。 值：<br><br>• x 和 y – 整数 0 到 9。<br>• storename – 默认值为 store。 此名称必须与在 StoreFront 服务器上配置的名称一致。<br>• servername.domain – 托管应用商店的服务器的完全限定域名。<br>• IISLocation – IIS 内的应用商店路径。 应用商店 URL 必须与 StoreFront 置备文件中的 URL 一致。 应用商店 URL 的格式为“/Citrix/store/discovery”。 要获取 URL，请从 Storefront 中导出一个置备文件，在记事本中打开，并复制 元素中的 URL。<br>• On \| Off – 可选 Off 配置设置使您能够交付已禁用的应用商店，从而使用户能够选择是否访问这些应用商店。 如果应用商店状态未指定，则默认设置为 On。<br>• storedescription – 应用商店的可选描述，例如 HR App Store。<br>注意：在本版本中，请务必在应用商店 URL 中包括 /discovery 以成功执行直通身份验证。 |
| **示例用法** | CitrixReceiver.exe STORE0="Store;https://test.xx.com/Citrix/Store/Discovery" |

在用户设备上启用 URL 重定向

| | |
|---|---|
| **选项** | ALLOW_CLIENTHOSTEDAPPSURL=1 |
| **说明** | 在用户设备上启用 URL 重定向功能。 需要具有管理员权限。 需要为所有用户安装 Citrix Receiver。 有关 URL 重定向的信息，请参阅 XenDesktop 7 文档中的本地应用程序访问及其子主题。 |
| **示例用法** | CitrixReceiver.exe ALLOW_CLIENTHOSTEDAPPSURL=1 |

启用自助服务模式

| | |
|---|---|
| **选项** | SELFSERVICEMODE={False \| True} |
| **说明** | 默认值为 True。 如果管理员将 SelfServiceMode 标志设置为 False，用户将不再具有自助服务 Citrix Receiver 用户界面的访问权限。 相反，这些用户可以从“开始”菜单或通过桌面快捷方式（称为“仅快捷方式模式”）访问订阅的应用程序。 |
| **示例用法** | CitrixReceiver.exe SELFSERVICEMODE=False |

指定桌面快捷方式的目录

| | |
|---|---|
| **选项** | DESKTOPDIR=<目录名称> |
| **说明** | 将所有快捷方式放在单个文件夹中。 桌面快捷方式支持类别路径。<br>注意：使用 DESKTOPDIR 选项时，请将 PutShortcutsOnDesktop 注册表项设置为 True。 |
| **示例用法** | CitrixReceiver.exe DESKTOPDIR=\Office |

从不受支持的 Citrix Receiver 版本进行升级

| | |
|---|---|
| **选项** | /rcu |
| **说明** | 允许您将 Citrix Receiver 从不受支持的版本升级到最新版本。 |
| **示例用法** | CitrixReceiver.exe /rcu |

### 在无人参与的安装期间显示安装完成对话框

安装完成时，将显示一个指示安装成功的对话框，然后显示**添加帐户**屏幕。 如果用户首次使用 Citrix Receiver for Windows，“添加帐户”对话框将要求您输入电子邮件或服务器地址以设置帐户。

> **注意**
>
> 如果未通过上述 STOREx 参数或组策略对象配置常用应用商店，之前尚未登录安装了 Citrix Receiver 的计算机的用户可能会看到“添加帐户”对话框。 要取消此对话框，请在注册表项 HKLM\Software\Citrix\Receiver 中创建一个 REG_DWORD 值 EnableX1FTU 并将其值设置为 0。

### 对安装问题进行故障排除

如果安装出现问题，请在用户的 %TEMP%/CTXReceiverInstallLogs 目录中搜索带有前缀 CtxInstall- 或 TrolleyExpress- 的日志。 例如：

CtxInstall-ICAWebWrapper-20141114-134516.log

TrolleyExpress-20090807-123456.log

**命令行安装示例**

无提示安装所有组件并指定两个应用商店：

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"

指定单点登录（直通身份验证）并添加指向 XenApp Services URL 的应用商店：

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

Citrix Receiver 会为每个已订阅桌面或应用程序创建存根应用程序。 您可以使用存根应用程序从命令行启动虚拟桌面或应用程序。 存根应用程序位于 %appdata%\Citrix\SelfService 中。 存根应用程序的文件名即为应用程序的显示名称（删除其中的空格）。 例如 Internet Explorer 的存根应用程序文件名为 InternetExplorer.exe。

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

Feb 02, 2016

可以使用 Active Directory 组策略脚本根据 Active Directory 的组织结构在系统中预部署 Receiver。 Citrix 建议使用脚本而非提取 .msi 文件，因为脚本会为安装、升级和卸载预留一个点，并且脚本合并了“程序和功能”中的 Citrix 条目，使检测已部署的 Receiver 简单易行。 使用计算机配置或用户配置下“组策略管理控制台 (GPMC)”中的脚本设置。 有关启动脚本的常规信息，请参阅 Microsoft 文档。

Citrix 包括用于安装和卸载 CitrixReceiver.exe 的示例每计算机启动脚本。 这些脚本位于 Citrix Receiver 和 Plug-ins\Windows\Receiver\Startup_Logon_Scripts 文件夹中的最新 XenApp 和 XenDesktop 介质上。

- CheckAndDeployReceiverPerMachineStartupScript.bat
- CheckAndRemoveReceiverPerMachineStartupScript.bat

如果在启动或关闭 Active Directory 组策略期间执行脚本，则可能会在系统的默认用户配置文件中创建自定义配置文件。 如果未删除这些配置文件，它们可能会阻止某些用户访问 Receiver 日志目录。 Citrix 示例脚本包括用于正确删除这些配置文件的功能。

**使用启动脚本和 Active Directory 部署 Receiver**

1. 为每个脚本创建一个组织单位 (OU)。
2. 为每个新创建的 OU 创建一个组策略对象 (GPO)。

### 修改示例脚本

可以通过编辑每个文件标题部分中的以下参数来修改脚本：

- **当前的软件包版本**。 指定的版本号已经过验证，即使不存在，部署也将继续。 例如： 设置 DesiredVersion= 3.3.0.XXXX 可精确匹配指定的版本。 如果您指定了部分版本号，例如 3.3.0，该版本号将与具有该前缀（3.3.0.1111、3.3.0.7777 等）的任何版本相匹配。
- **软件包位置/部署目录**。 此参数指定包含软件包的网络共享，但未由脚本进行身份验证。 每位用户都必须对共享文件夹具有读取权限。
- **脚本日志记录目录**。 此参数指定复制安装目录的网络共享，但未由脚本进行身份验证。 每位用户都必须对共享文件夹具有读取和写入权限。
- **软件包安装程序命令行选项**。 这些命令行选项将传递到安装程序。 有关命令行语法，请参阅使用命令行参数配置和安装 Receiver for Windows。

### 添加“每计算机启动脚本”

1. 打开组策略管理控制台。
2. 依次选择计算机配置 > 策略 > Windows 设置 > 脚本(启动/关闭)。
3. 在组策略管理控制台的右侧窗格中，选择启动。
4. 在属性菜单中，单击显示文件，将相应的脚本复制到显示的文件夹，然后关闭该窗口。
5. 在属性菜单中，单击添加，然后使用浏览查找并添加新创建的脚本。

### 每计算机部署 Receiver

1. 将指定接收此部署的用户设备移动到您创建的 OU 中。

2. 重新启动用户设备，并以任意用户身份登录。
3. 验证“程序和功能”（在早期操作系统版本中为“添加或删除程序”）中是否包含新安装的软件包。

### 每计算机删除 Receiver

1. 将为删除操作指定的用户设备移动到您创建的 OU 中。
2. 重新启动用户设备，并以任意用户身份登录。
3. 验证“程序和功能”（在早期操作系统版本中为“添加或删除程序”）中是否已删除之前安装的软件包。

### 使用每用户示例启动脚本

Citrix 建议用户使用每计算机启动脚本。 但是，对于需要 Receiver 每用户部署的情况，两个 Receiver 每用户脚本将包含在 Citrix Receiver 和 Plug-ins\Windows\Receiver\Startup_Logon_Scripts 文件夹中的 XenDesktop 和 XenApp 介质中。

- CheckAndDeployReceiverPerUserLogonScript.bat
- CheckAndRemoveReceiverPerUserLogonScript.bat

## 设置“每用户启动脚本”

1. 打开组策略管理控制台。
2. 依次选择用户配置 > 策略 > Windows 设置 > 脚本。
3. 在组策略管理控制台的右侧窗格中，选择登录。
4. 在登录属性菜单中，单击显示文件，将相应的脚本复制到显示的文件夹，然后关闭该窗口。
5. 在登录属性菜单中，单击添加，然后使用浏览查找并添加新创建的脚本。

## 每用户部署 Receiver

1. 将指定接收此部署的用户移动到您创建的 OU 中。
2. 重新启动用户设备，并以指定的用户身份登录。
3. 验证“程序和功能”（在早期操作系统版本中为“添加或删除程序”）中是否包含新安装的软件包。

## 每用户删除 Receiver

1. 将为删除操作指定的用户移动到您创建的 OU 中。
2. 重新启动用户设备，并以指定的用户身份登录。
3. 验证“程序和功能”（在早期操作系统版本中为“添加或删除程序”）中是否已删除之前安装的软件包。

# 从 Receiver for Web 部署 Receiver for Windows

Feb 02, 2016

可以从 Receiver for Web 部署 Receiver，以确保用户在尝试从浏览器连接到应用程序之前已安装 Receiver。 借助 Receiver for Web 站点，用户可以通过 Web 页面访问 StoreFront 应用商店。 如果 Receiver for Web 站点检测到用户没有 Receiver 的兼容版本，系统会提示用户下载并安装 Receiver。 有关详细信息，请参阅 StoreFront 文档中的 Receiver for Web 站点。

如果已从 Receiver for Web 部署 Receiver，则基于电子邮件的帐户发现不适用。 如果已配置基于电子邮件的帐户发现，而首次使用的用户从 Citrix.com 安装了 Receiver，则 Receiver 将提示该用户输入电子邮件或服务器地址。 输入电子邮件地址时会显示错误消息“您的电子邮件无法用于添加帐户”。如果使用以下配置，则仅提示输入服务器地址。

1. 将 CitrixReceiver.exe 下载到本地计算机。
2. 将 CitrixReceiver.exe 重命名为 CitrixReceiverWeb.exe。
   重要：名称 CitrixReceiverWeb.exe 区分大小写。
3. 使用常规部署方法部署这一重命名的可执行文件。 如果使用 StoreFront，请参阅 StoreFront 文档中的使用配置文件配置 Receiver for Web 站点。

# 从 Web Interface 登录屏幕部署 Receiver for Windows

Feb 02, 2016

此功能仅适用于支持 Web Interface 的 XenDesktop 和 XenApp 版本。

可以从 Web 页面部署 Receiver，以确保用户在尝试使用 Web Interface 之前安装了 Receiver。 Web Interface 提供了客户端检测和部署过程，用于检测可以将哪些 Citrix 客户端部署在用户环境中，然后引导用户完成部署过程。

可以将客户端检测和部署过程配置为在用户访问 XenApp Web 站点时自动运行。 如果 Web Interface 检测到用户没有 Receiver 的兼容版本，则会提示用户下载并安装 Receiver。

有关详细信息，请参阅 Web Interface 文档中的配置客户端部署。

如果已从 Web Interface 部署 Receiver，则基于电子邮件的帐户发现不适用。 如果已配置基于电子邮件的帐户发现，而首次使用的用户从 Citrix.com 安装了 Receiver，则 Receiver 将提示该用户输入电子邮件或服务器地址。 输入电子邮件地址时会显示错误消息“您的电子邮件无法用于添加帐户”。如果使用以下配置，则仅提示输入服务器地址。

1. 将 CitrixReceiver.exe 下载到本地计算机。
2. 将 CitrixReceiver.exe 重命名为 CitrixReceiverWeb.exe。
   重要：名称 CitrixReceiverWeb.exe 区分大小写。
3. 请在 XenApp Web 站点的配置文件中的 ClientIcaWin32 参数中指定所更改的文件名。
   要使用客户端检测和部署过程，Receiver 安装文件必须位于 Web Interface 服务器上。 默认情况下，Web Interface 假定 Receiver 安装文件的文件名与 XenApp 或 XenDesktop 安装介质上提供的文件相同。
4. 请将用于下载 CitrixReceiverWeb.exe 文件的站点添加到“可信站点”区域中。
5. 使用常规部署方法部署这一重命名的可执行文件。

# 配置 Citrix Receiver for Windows

Aug 25, 2016

使用 Receiver for Windows 软件时，用户利用以下配置步骤可访问其托管应用程序和桌面：

- 配置应用程序交付和配置 XenDesktop 环境。 请确保正确配置您的 XenApp 环境。 了解您的选择并向您的用户提供有意义的应用程序说明。
- 通过向 Receiver 中添加 StoreFront 帐户配置自助服务模式。 此模式允许您的用户从 Receiver 用户界面订阅应用程序。
- 配置仅快捷方式模式，包括：
  - 使用组策略对象模板文件自定义快捷方式。
  - 使用注册表项自定义快捷方式。
  - 根据 StoreFront 帐户设置配置快捷方式
- 向用户提供帐户信息。 向用户提供设置托管其虚拟桌面和应用程序的帐户的访问权限所需的信息。 在某些环境中，用户必须手动设置帐户的访问权限。

- 如果有用户从外部网络进行连接（例如，用户从 Internet 或远程位置进行连接），请通过 NetScaler Gateway 配置身份验证。 有关详细信息，请参阅 Netscaler Gateway。

**配置应用程序交付**

通过 XenDesktop 或 XenApp 交付应用程序时，请考虑采用以下方案增强用户访问其应用程序时的体验：

Web 访问模式

如果未执行任何配置，Citrix Receiver for Windows 将提供 Web 访问模式：基于浏览器访问应用程序和桌面。 用户只需要打开浏览器访问 Receiver for Web 或 Web Interface 站点，选择并使用所需的应用程序。 在 Web 访问模式下，不会将任何应用程序快捷方式放置在用户设备上的应用程序文件夹中。

自助服务模式

通过将 StoreFront 或 Web Interface Services 站点帐户添加到 Receiver for Windows，可以配置自助服务模式，在此模式下，您的用户可以通过 Receiver 订阅应用程序。 这种增强的用户体验与移动应用商店的体验相似。 在自助服务模式下，您可以根据需要配置强制、自动置备的以及精选应用程序关键字设置。 当其中一个用户选择应用程序时，该应用程序的快捷方式将放置到用户设备上的应用程序文件夹中。

访问 StoreFront 3.0 站点时，您的用户将看到 Receiver 用户体验。 有关 Receiver 用户体验的详细信息，请参阅 Receiver 和 StoreFront 3.0 技术预览版。

在 XenApp 场中发布应用程序时，要增强通过 StoreFront 应用商店访问这些应用程序的用户的体验，请务必包含已发布的应用程序的有意义的说明。 这些说明通过 Citrix Receiver 向用户显示。

## 配置自助服务模式

如上文所述，通过将 StoreFront 帐户添加到 Receiver 中或将 Receiver 配置为指向 Web Interface XenApp Services 站点，可以配置自助服务模式，在此模式下，您的用户可以从 Receiver 用户界面订阅应用程序。 这种增强的用户体验与移动应用商店的体验相似。

在自助服务模式下，您可以根据需要配置强制、自动置备的以及精选应用程序关键字设置。

- 要自动为某个应用商店的所有用户订阅某个应用程序，请将字符串 KEYWORDS:Auto 附加到您在 XenApp 中发布该应用程序时提供的说明的末尾。 用户登录到该应用商店时，将自动置备相应的应用程序，无需用户手动订阅。

- 要向用户公告应用程序，或者在 Receiver 的精选列表中列出常用的应用程序，以使其更易于查找，请将字符串 KEYWORDS:Featured 附加到应用程序说明后面。

有关详细信息，请参阅 StoreFront 文档。

如果 XenApp 部署中的 Web Interface 没有 XenApp Services 站点，请创建一个站点。 站点的名称及创建方法取决于已安装的 Web Interface 的版本。 有关详细信息，请参阅 Web Interface 文档。

> **注意**
>
> 使用自助服务模式启动会话时，默认启用自动连接。

### 配置 StoreFront

使用 Storefront 后，您创建的应用商店将由可向 Citrix Receiver 提供身份验证和资源交付基础结构的各项服务组成。 应创建一些应用商店，这些应用商店将枚举 XenDesktop 站点和 XenApp 场中的桌面和应用程序，并将这些资源汇集在一起，以使其对用户可用。

1. 安装并配置 StoreFront。 有关详细信息，请参阅 StoreFront 文档。

   注意：对于需要更大控制权的管理员，Citrix 提供了一个模板，供您创建 Receiver 下载站点。

# 配置应用程序交付

Nov 02, 2016

通过 XenDesktop 或 XenApp 交付应用程序时，请考虑采用以下方案增强用户访问其应用程序时的体验：

- Web 访问模式 - 如果未执行任何配置，Receiver for Windows 4.4 将提供基于浏览器访问应用程序和桌面的功能。 用户只需要打开浏览器访问 Receiver for Web 或 Web Interface 站点，选择并使用所需的应用程序。 在此模式下，不会将任何快捷方式放置在用户的桌面上。
- 自助服务模式 - 通过简单地将 StoreFront 帐户添加到 Receiver 中或将 Receiver 配置为指向 StoreFront 站点，可以配置*自助服务模式*，在此模式下，用户可以从 Receiver 用户界面订阅应用程序。 这种增强的用户体验与移动应用商店的体验相似。 在自助服务模式下，您可以根据需要配置强制、自动置备的以及精选应用程序关键字设置。

注意：默认情况下，Receiver for Windows 4.4 允许用户选择要在其“开始”菜单中显示的应用程序。

- 仅应用程序快捷方式模式 - 作为 Receiver 管理员，您可以将 Receiver for Windows 4.4 配置为自动直接将应用程序和桌面快捷方式放置在“开始”菜单中或桌面上，方式与 Receiver for Windows 3.4 Enterprise 的方式相似。 新的*仅快捷方式*模式允许用户在熟悉的 Windows 导航架构中查找所有已发布的应用程序，该位置正是用户希望找到应用程序的位置。

有关使用 XenApp 和 XenDesktop 7 交付应用程序的信息，请参阅 Create a Delivery Group application（创建交付组应用程序）。

注意：在交付组中添加有意义的应用程序说明。 使用 Web 访问或自助服务模式时，说明将对 Receiver 用户可见。
有关如何在“开始”菜单中或桌面上配置快捷方式的详细信息，请参阅 Citrix 产品文档中的 Configure Shortcut Only Mode（配置仅快捷方式模式）。

## 配置自助服务模式

通过简单地将 StoreFront 帐户添加到 Receiver 中或将 Receiver 配置为指向 StoreFront 站点，可以配置*自助服务模式*，在此模式下，用户可以从 Receiver 用户界面订阅应用程序。 这种增强的用户体验与移动应用商店的体验相似。

注意：默认情况下，Receiver for Windows 4.4 允许用户选择要在其“开始”菜单中显示的应用程序。
在自助服务模式下，您可以根据需要配置强制、自动置备的以及精选应用程序关键字设置。

将关键字附加到为交付组应用程序提供的说明后面：

- 要将某个应用程序设为强制应用程序，以便无法将其从 Receiver for Windows 中删除，请将字符串 KEYWORDS:Mandatory 附加到应用程序描述后面。 不会向用户提供用于取消订阅强制应用程序的“删除”选项。
- 要自动为所有用户订阅某个应用程序的存储，请将字符串 KEYWORDS:Auto 附加到说明后面。 用户登录到该应用商店时，相应的应用程序将自动置备，而无需用户手动订阅。
- 要向用户公告应用程序，或者在 Receiver 的精选列表中列出常用的应用程序，以使其更易于查找，请将字符串 KEYWORDS:Featured 附加到应用程序说明后面。

## 自定义应用程序快捷方式的位置

在“开始”菜单集成和仅桌面快捷方式模式下，您可以将已发布的应用程序**快捷方式**放在 Windows 的“开始”菜单中和桌面上。 采用这种方式时，用户无需从 Receiver 用户界面订阅应用程序。 “开始”菜单集成和桌面快捷方式管理为需要一致地访问一组核心应用程序的用户组提供了无缝桌面体验。

作为 Receiver 管理员，请使用命令行安装标志、GPO、帐户服务或注册表设置来禁用常用“自助服务”Receiver 界面，并将其替换为预配置的“开始”菜单。 标志的名称为 SelfServiceMode ，默认设置为 true 。 管理员将 SelfServiceMode 标志设置为 false时，用户不再对自助服务 Receiver 用户界面具有访问权限。 相反，这些用户可以从“开始”菜单或通过桌面快捷方式（本文称为**仅快捷方式模式**）访问订阅的应用程序。

用户和管理员可以使用多个注册表设置来自定义设置快捷方式的方法。 请参阅使用注册表项自定义应用程序快捷方式的位置。

**使用快捷方式**

- 用户无法删除应用程序。 将 SelfServiceMode 标志设置为 false （仅快捷方式模式）时，所有应用程序均为强制应用程序。 如果用户从桌面删除快捷方式图标，当用户选择 Receiver 系统托盘图标上的刷新时，此图标会再次显示。
- 用户只能配置一个应用商店。 帐户和首选项选项不可用。 这是为了阻止用户配置其他应用商店。 管理员可以向用户授予特殊权限，以允许用户使用组策略对象模板或通过手动在客户端计算机上添加注册表项 (HideEditStoresDialog) 来添加多个帐户。 如果管理员向用户授予此权限，用户将可以在系统托盘图标中看到“首选项”选项，此时用户可以添加或删除帐户。
- 用户无法通过 Windows 控制面板删除应用程序。
- 可以通过可自定义的注册表设置添加桌面快捷方式。 默认情况下不添加桌面快捷方式。 更改注册表设置后，必须重新启动 Receiver。
- 在开始菜单中创建快捷方式，并采用默认类别路径 UseCategoryAsStartMenuPath。

注意：Windows 8/8.1 不允许在“开始”菜单中创建嵌入式文件夹。 “应用程序”将单独显示或在根文件夹下显示，不在通过 XenApp 定义的“类别”子文件夹中显示。

- 可以在安装过程中添加标志 [/DESKTOPDIR="Dir_name"] 以便将所有快捷方式放置到单个文件夹中。 CategoryPath 受桌面快捷方式支持。
- 自动重新安装修改后的应用程序是一项可以通过注册表项 AutoReInstallModifiedApps。 启用 AutoReInstallModifiedApps 后，在服务器上对已发布应用程序和桌面的属性所做的任何更改均反映到客户端计算机上。 禁用 AutoReInstallModifiedApps 时，应用程序和桌面属性将不会更新，并且，如果在客户端删除了快捷方式，刷新时也不会恢复快捷方式。 默认情况下，启用 AutoReInstallModifiedApps。 请参阅使用注册表项自定义应用程序快捷方式的位置。

## 使用组策略对象模板自定义应用程序快捷方式的位置

**注意：**应在配置应用商店之前更改组策略。 如果您或某个用户在任何时间想要自定义组策略，您或该用户必须重置 Receiver，配置组策略，然后重新配置应用商店。

作为管理员，您可以使用组策略配置快捷方式。

1. 打开本地组策略编辑器，方法是运行命令gpedit.msc （在将策略应用于单台计算机时在本地从开始菜单运行）或者使用组策略管理控制台（在应用域策略时）。
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 Configuration 文件夹，然后选择 receiver.admx（或 receiver.adml）。 有关 ADMX 模板的详细信息，请参阅关于 ADMX 模板的使用
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 > 自助服务。
7. 选择管理 SelfServiceMode以启用或禁用自助服务 Receiver 用户界面。
8. 选择管理应用程序快捷方式以启用或禁用：
   - 桌面上的快捷方式
   - “开始”菜单中的快捷方式
   - 桌面目录
   - “开始”菜单目录
   - 快捷方式的类别路径
   - 在注销时删除应用程序
   - 在退出时删除应用程序
9. 选择允许用户添加/删除帐户以向用户授予添加或删除多个帐户的权限。

## 使用注册表项自定义应用程序快捷方式的位置

> **注意**
>
> 默认情况下，注册表项使用字符串格式。

可以使用注册表项设置自定义快捷方式。 可以设置位于以下位置的注册表项。 在应用这些注册表项的地方，这些注册表项按照列出的首选顺序发挥作用。

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。
**注意：**应在配置应用商店之前更改注册表项。 如果您或某个用户在某一时间想要自定义注册表项，您或此用户必须重置 Receiver，配置注册表项，然后重新配置应用商店。
**32 位计算机的注册表项**

| 注册表名称 | 默认值 | 首选顺序位置 |
| --- | --- | --- |
| RemoveAppsOnLogoff | False | HKLM\SOFTWARE\Policies\Citrix\Dazzle<br>HKLM\SOFTWARE\Citrix\Dazzle<br>HKCU\Software\Citrix\Dazzle<br>HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties |
| RemoveAppsOnExit | False | HKLM\SOFTWARE\Policies\Citrix\Dazzle<br>HKLM\SOFTWARE\Citrix\Dazzle<br>HKCU\Software\Citrix\Dazzle<br>HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties |
| PutShortcutsOnDesktop | False | HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties<br>HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties<br>HKCU\Software\Citrix\Dazzle<br>HKLM\SOFTWARE\Policies\Citrix\Dazzle<br>HKLM \SOFTWARE\Citrix\Dazzle |
| PutShortcutsInStartMenu | True | HKCU\Software\Citrix\Receiver\SR\Store\+StoreID+\Properties<br>HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties |

| 注册表名称 | 默认值 | 首选顺序位置 |
| --- | --- | --- |
| | | HKCU\Software\Citrix\Dazzle<br>HKLM\SOFTWARE\Policies\Citrix\Dazzle<br>HKLM\SOFTWARE\Citrix\Dazzle |
| SelfServiceMode | True | HKLM\SOFTWARE\Policies\Citrix\Dazzle<br>HKLM\SOFTWARE\Citrix\Dazzle |
| UseCategoryAsStartMenuPath | True | HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties<br>HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties<br>HKCU\Software\Citrix\Dazzle<br>HKLM\SOFTWARE\Policies\Citrix\Dazzle<br>HKLM \SOFTWARE\Citrix\Dazzle |
| StartMenuDir | ""（空） | HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties<br>HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties<br>HKCU\Software\Citrix\Dazzle<br>HKLM\SOFTWARE\Policies\Citrix\Dazzle<br>HKLM \SOFTWARE\Citrix\Dazzle |
| DesktopDir | ""（空） | HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties<br>HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties<br>HKCU\Software\Citrix\Dazzle<br>HKLM\SOFTWARE\Policies\Citrix\Dazzle<br>HKLM\SOFTWARE\Citrix\Dazzle |
| AutoReinstallModifiedApps | True | HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties<br>HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties |

| 注册表名称 | 默认值 | 首选顺序位置 |
| --- | --- | --- |
| | | HKCU\Software\Citrix\Dazzle<br>HKLM\SOFTWARE\Policies\Citrix\Dazzle<br>HKLM\SOFTWARE\Citrix\Dazzle |
| HideEditStoresDialog | 在 SelfServiceMode 中为 True，在 NonSelfServiceMode 中为 False。 | HKLM\SOFTWARE\Policies\Citrix\Dazzle<br>HKLM\SOFTWARE\Citrix\Dazzle<br>HKCU\Software\Citrix\Dazzle<br>HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties |
| WSCSupported | True | HKCU\Software\Citrix\Dazzle<br>HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID +\Properties<br>HKLM\SOFTWARE\Policies\Citrix\Dazzle<br>HKLM\SOFTWARE\Citrix\Dazzle |
| WSCReconnectAll | True | HKCU\Software\Citrix\Dazzle<br>HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties<br>HKLM\SOFTWARE\Policies\Citrix\Dazzle<br>HKLM\SOFTWARE\Citrix\Dazzle |
| WSCReconnectMode | 3 | HKCU\Software\Citrix\Dazzle<br>HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID +\Properties<br>HKLM\SOFTWARE\Policies\Citrix\Dazzle<br>HKLM\SOFTWARE\Citrix\Dazzle |
| WSCReconnectModeUser | 在安装期间不创建注册表项。 | HKCU\Software\Citrix\Dazzle<br>HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID+\Properties<br>HKLM\SOFTWARE\Policies\Citrix\Dazzle<br>HKLM\SOFTWARE \Citrix\Dazzle |

| 注册表名称 | 默认值 | 首选顺序位置 |
| --- | --- | --- |

64 位计算机的注册表项

| 注册表名称 | 默认值 | 首选顺序位置 |
| --- | --- | --- |
| RemoveAppsOnLogoff | False | HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle<br>HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle<br>HKCU\Software\Citrix\Dazzle<br>HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties |
| RemoveAppsOnExit | False | HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle<br>HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle<br>HKCU\Software\Citrix\Dazzle<br>HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties |
| PutShortcutsOnDesktop | False | HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties<br>HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties<br>HKCU\Software\Citrix\Dazzle<br>HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle<br>HKLM \SOFTWARE\Wow6432Node\Citrix\Dazzle |
| PutShortcutsInStartMenu | True | HKCU\Software\Citrix\Receiver\SR\Store\+StoreID+\Properties<br>HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties<br>HKCU\Software\Citrix\Dazzle<br>HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle<br>HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle |
| SelfServiceMode | True | HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle<br>HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle |
| UseCategoryAsStartMenuPath | True | HKCU\Software\Citrix\Receiver\SR\Store\+StoreID |

| 注册表名称 | 默认值 | +\Properties<br>首选顺序位置 |
| --- | --- | --- |
| | | HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties<br><br>HKCU\Software\Citrix\Dazzle<br><br>HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle<br><br>HKLM \SOFTWARE\Wow6432Node\Citrix\Dazzle |
| StartMenuDir | ""（空） | HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties<br><br>HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties<br><br>HKCU\Software\Citrix\Dazzle<br><br>HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle<br><br>HKLM \SOFTWARE\Wow6432Node\Citrix\Dazzle |
| DesktopDir | ""（空） | HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties<br><br>HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties<br><br>HKCU\Software\Citrix\Dazzle<br><br>HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle<br><br>HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle |
| AutoReinstallModifiedApps | True | HKCU\Software\Citrix\Receiver\SR\Store\+StoreID +\Properties<br><br>HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties<br><br>HKCU\Software\Citrix\Dazzle<br><br>HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle<br><br>HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle |
| HideEditStoresDialog | 在 SelfServiceMode 中为 True，在 NonSelfServiceMode 中为 False。 | HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle<br><br>HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle<br><br>HKCU\Software\Citrix\Dazzle |

| 注册表名称 | 默认值 | 首选顺序位置 |
| --- | --- | --- |
| | | HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties |
| WSCSupported | True | HKCU\Software\Citrix\Dazzle<br>HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID +\Properties<br>HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle<br>HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle |
| WSCReconnectAll | True | HKCU\Software\Citrix\Dazzle<br>HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID + \Properties<br>HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle<br>HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle |
| WSCReconnectMode | 3 | HKCU\Software\Citrix\Dazzle<br>HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID +\Properties<br>HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle<br>HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle |
| WSCReconnectModeUser | 在安装期间不创建注册表项。 | HKCU\Software\Citrix\Dazzle<br>HKCU\Software\Citrix\Receiver\SR\Store\" + primaryStoreID+\Properties<br>HKLM\SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle<br>HKLM\SOFTWARE\Wow6432Node\Citrix\Dazzle |

### 使用 StoreFront 帐户设置自定义应用程序快捷方式的位置

您可以从 StoreFront 站点在“开始”菜单和桌面上设置快捷方式。 可以将下列设置添加到 C:\inetpub\wwwroot\Citrix\Roaming 中的 web.config 文件的 部分：

- 要将快捷方式放在桌面上，请使用 PutShortcutsOnDesktop。 设置：true 或 false（默认为 false）。
- 要将快捷方式放在“开始”菜单中，请使用 PutShortcutsInStartMenu。 设置：true 或 false（默认为 true）。
- 要在“开始”菜单中使用类别路径，请使用 UseCategoryAsStartMenuPath。 设置：true 或 false（默认为 true）。

注意：Windows 8/8.1 不允许在“开始”菜单中创建嵌入式文件夹。 “应用程序”将单独显示或在根文件夹下显示，不在通过 XenApp 定义的“类别”子文件夹中显示。

- 要在“开始”菜单中为所有快捷方式设置单个目录，请使用 StartMenuDir。 设置：字符串值，指示快捷方式写入到的文件夹的名

称。

- 要重新安装修改后的应用程序，请使用 AutoReinstallModifiedApps。 设置：true 或 false（默认为 true）。
- 要在桌面上为所有快捷方式显示单个目录，请使用 DesktopDir。 设置：字符串值，指示快捷方式写入到的文件夹的名称。
- 要不在客户端“add/remove programs”上创建条目，请使用 DontCreateAddRemoveEntry。 设置：true 或 false（默认为 false）。
- 要删除应用商店中以前提供但现在不再提供的应用程序对应的快捷方式和 Receiver 图标，请使用 SilentlyUninstallRemovedResources。 设置：true 或 false（默认为 false）。

在 web.config 文件中，更改应添加到帐户的 XML 部分。 请通过查找以下开头标记查找此部分：

此部分以 标记结尾。
在帐户部分结束之前，在前几项属性部分中：

可以将属性添加到此部分中 标记的后面，一个属性占据一行，同时提供名称和值。 例如：

注意：在 标记前面添加的属性元素可能会使其失效。 添加属性名称和值时删除 标记属于可选操作。
以下是此部分的扩展示例：

重要：在多服务器部署中，请一次仅使用一台服务器以更改服务器组的配置。 确保 Citrix StoreFront 管理控制台未在部署中的任何其他服务器上运行。 完成后，请将对配置所做的更改传播到服务器组，以便更新部署中的其他服务器。

### 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

可以将 Receiver 配置为自动直接在“开始”菜单中或桌面上放置应用程序和桌面快捷方式。 此功能与以前发布的 Receiver 版本类似，但是，版本 4.4 中引入了使用 XenApp 每应用程序设置控制应用程序快捷方式放置的功能。 如果环境中有一些应用程序需要在一致的位置显示，此功能将非常有用。

如果要设置快捷方式的位置以便每个用户都能在相同的位置找到这些快捷方式，请使用 XenApp 每应用程序设置：

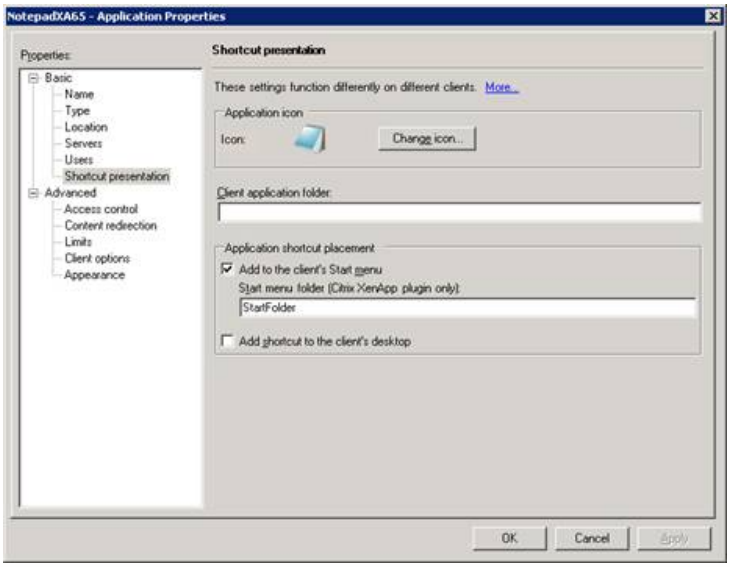
| | |
|---|---|
| 如果要通过每应用程序设置来确定应用程序的放置位置，而无论处于自助服务模式还是“开始”菜单模式，请执行以下操作： | 通过 **PutShortcutsInStartMenu=false** 配置 Receiver 并启用每应用程序设置。<br>注意：此设置仅适用于 Web Interface 站点。 |

注意：**PutShortcutsInStartMenu=false** 设置同时适用于 XenApp 6.5 和 XenDesktop 7.x。

**在 XenApp 6.5 中配置每应用程序设置**

在 XenApp 6.5 中配置每应用程序发布快捷方式：

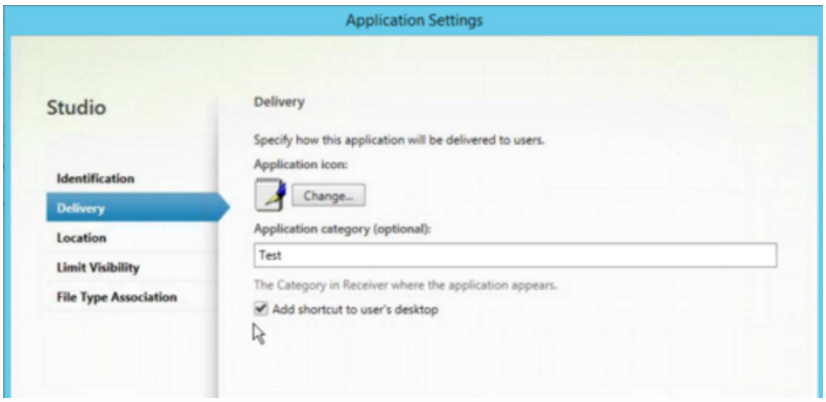
1. 在 XenApp 应用程序属性屏幕中，展开基本属性。
2. 选择快捷方式显示选项。
3. 在“快捷方式显示”屏幕的应用程序快捷方式放置部分中，选中添加到客户端“开始”菜单复选框。 选中该复选框后，输入要用于放置快捷方式的文件夹的名称。 如果未指定文件夹名称，XenApp 会将快捷方式放置在“开始”菜单中，而不是放置在文件夹中。
4. 选择添加到客户端“开始”菜单以包括客户端计算机的桌面上的快捷方式。
5. 单击应用。
6. 单击 OK（确定）。




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

在 XenApp 7.6 中配置每应用程序发布快捷方式：

1. 在 Citrix Studio 中，找到应用程序设置屏幕。
2. 在“应用程序设置”屏幕中，选择交付。 在此屏幕中，可以指定如何向用户交付应用程序。
3. 为应用程序选择恰当的图标。 单击更改浏览到所需图标所在的位置。
4. 在应用程序类别字段中，选择性指定 Receiver 中应用程序显示时所属的类别。 例如，如果要添加 Microsoft Office 应用程序的快捷方式，请输入 Microsoft Office。
5. 选中将快捷方式添加到用户桌面复选框。
6. 单击确定。




缩短枚举延迟或对应用程序存根进行数字签名

如果用户在每次登录时都遇到应用程序枚举延迟，或者如果需要对应用程序存根进行数字签名，Receiver 将提供从网络共享复制 .EXE 存根的功能。

此功能涉及以下几个步骤：

1. 在客户端计算机上创建应用程序存根。
2. 将应用程序存根复制到可从网络共享访问的一个通用位置。
3. 如有需要，请准备一份白名单（或者，通过企业证书对存根进行签名）。
4. 添加注册表项以使 Receiver 能够通过从网络共享复制存根来创建这些存根。

如果启用了 RemoveappsOnLogoff 和 RemoveAppsonExit，并且用户在每次登录时都遇到应用程序枚举延迟，请使用以下解决方法来缩短延迟：

1. 使用 regedit 添加 HKCU\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d "true"。
2. 使用 regedit 添加 HKLM\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d "true"。 HKCU 的优先级高于 HKLM。

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。
允许计算机使用存储在网络共享上的预创建的存根可执行文件：

1. 在客户端计算机上，为所有应用程序创建存根可执行文件。 为此，请将所有应用程序添加到使用 Receiver 的计算机；Receiver 将生成可执行文件。
2. 从 %APPDATA%\Citrix\SelfService 获取存根可执行文件。 您只需要 .exe 文件。
3. 将这些可执行文件复制到网络共享。
4. 为要锁定的各个客户端计算机设置以下注册表项：
    1. Reg add HKLM\Software\Citrix\Dazzle /v CommonStubDirectory /t REG_SZ /d "\\ShareOne\ReceiverStubs"
    2. Reg add HKLM\Software\Citrix\Dazzle /v
    3. CopyStubsFromCommonStubDirectory /t REG_SZ /d "true"。 如果愿意，还可以在 HKCU 上配置以下设置。 HKCU 的优先级高于 HKLM。
    4. 退出并重新启动 Receiver 以测试设置。

## 示例用例

本主题介绍了应用程序快捷方式的用例。

**允许用户选择希望放置在“开始”菜单中的应用程序（自助服务）**

如果您有几十个（甚至上百个）应用程序，最好允许用户选择自己要收藏并添加到“开始”菜单中的应用程序：

| | |
|---|---|
| 如果希望用户选择要放置在“开始”菜单中的应用程序，请执行以下操作： | 在自助服务模式下配置 Receiver。 在此模式下，您还可以根据需要配置*自动置备的*和*强制*应用程序关键字设置。 |
| 如果希望用户选择要放置在“开始”菜单中的应用程序，同时还希望将特定的应用程序快捷方式放置在桌面上，请执行以下操作： | 不为 Receiver 配置任何选项，然后对要放置在桌面上的几个应用程序使用每应用程序设置。 根据需要使用*自动置备的*和*强制*应用程序。 |

**“开始”菜单中不放置任何应用程序快捷方式**

如果用户有一台家用计算机，您可能完全不需要或不希望放置快捷方式。 在此类情况下，最简单的方法是浏览器访问；安装 Receiver 但不执行任何配置，然后浏览到 Receiver for Web 和 Web Interface。 还可以将 Receiver 配置为进行自助访问而不将快捷方式放置在任何位置。

| | |
|---|---|
| 如果希望阻止 Receiver 自动将应用程序快捷方式放置在“开始”菜单中的任何位置，请执行以下操作： | 通过 PutShortcutsInStartMenu=False 配置 Receiver。 即使在自助服务模式下，Receiver 也不会将应用程序放置在“开始”菜单中，除非使用每应用程序设置将其放置在该位置。 |

**将所有应用程序快捷方式都放置在“开始”菜单中或桌面上**

如果用户只有极少数应用程序，您可以将所有应用程序都放置在“开始”菜单中或桌面上，或者放置在桌面上的某个文件夹中。

| | |
|---|---|
| 如果希望 Receiver 自动将所有应用程序快捷方式都放置 | 通过 SelfServiceMode =False 配置 Receiver。 所有可用的应 |

| | |
|---|---|
| 在“开始”菜单中，请执行以下操作： | 用程序将在“开始”菜单中显示。 |
| 如果希望将所有应用程序快捷方式都放置在桌面上，请执行以下操作： | 通过 PutShortcutsOnDesktop = true 配置 Receiver。 所有可用的应用程序将在桌面上显示。 |
| 如果希望将所有快捷方式都放置在桌面上的文件夹中，请执行以下操作： | 通过要将应用程序放置到的桌面文件夹的 DesktopDir=Name 配置 Receiver。 |

**使用 XenApp 6.5 或 7.x 中的每应用程序设置**

如果要设置快捷方式的位置以便每个用户都能在相同的位置找到这些快捷方式，请使用 XenApp 每应用程序设置：

| | |
|---|---|
| 如果要通过每应用程序设置来确定应用程序的放置位置，而无论处于自助服务模式还是“开始”菜单模式，请执行以下操作： | 通过 **PutShortcutsInStartMenu=false** 配置 Receiver 并启用每应用程序设置。<br>注意：此设置仅适用于 Web Interface 站点。 |

**应用程序放置在类别文件夹或特定文件夹中**

如果希望应用程序在特定文件夹中显示，请使用以下选项：

| | |
|---|---|
| 如果希望 Receiver 放置在“开始”菜单中的应用程序快捷方式在其关联的类别（文件夹）中显示，请执行以下操作： | 通过 UseCategoryAsStartMenuPath=True 配置 Receiver。<br>注意：Windows 8/8.1 不允许在“开始”菜单中创建嵌入式文件夹。 “应用程序”将单独显示或在根文件夹下显示，不在通过 XenApp 定义的“类别”子文件夹中显示。 |
| 如果希望 Receiver 放置在“开始”菜单中的应用程序在特定文件夹中显示，请执行以下操作： | 通过“开始”菜单文件夹名称的 StartMenuDir= 配置 Receiver。 |

**注销或退出时删除应用程序**

如果在另一个用户要共享端点时不希望用户看到应用程序，可以确保在用户注销和退出时删除应用程序：


| | |
|---|---|
| 如果希望 Receiver 在注销时删除所有应用程序，请执行以下操作： | 通过 RemoveAppsOnLogoff=True 配置 Receiver。 |
| 如果希望 Receiver 在退出时删除应用程序，请执行以下操作： | 通过 RemoveAppsOnExit=True 配置 Receiver。 |

配置本地应用程序访问应用程序

配置本地应用程序访问应用程序时：

- 要指定应使用本地安装的应用程序而非 Receiver 中提供的应用程序，请附加字符串 KEYWORDS:prefer="模式"。 此功能称为“本地应用程序访问”。
  在用户的计算机上安装应用程序之前，Receiver 将搜索指定的模式，以确定应用程序是否已在本地安装。 如果已在本地安装，Receiver 将订阅该应用程序，但不创建快捷方式。 用户从 Receiver 窗口中启动该应用程序时，Receiver 将启动本地安装的（首选）应用程序。

  如果用户在 Receiver 外部卸载了某个首选应用程序，下次 Receiver 刷新时将取消订阅该应用程序。 如果用户从 Receiver 窗口中卸载了某个首选应用程序，Receiver 将取消订阅该应用程序，但不卸载。

  注意：Receiver 订阅某个应用程序时，将应用关键字 prefer。 在订阅应用程序后再添加关键字将不起作用。
  可以为某个应用程序多次指定关键字 prefer。 只需一个匹配项即可将此关键字应用到某个应用程序。 可以在任何组合中使用以下模式：

  - prefer="ApplicationName"
    此应用程序名称模式与具有在快捷方式文件名称中指定的应用程序名称的任何应用程序相匹配。 此应用程序名称可以是一个单词，也可以是一个短语。 如果是短语，则需要使用引号。 不允许对部分词语或文件路径应用匹配，且匹配不区分大小写。 应用程序名称匹配模式对管理员手动执行的覆盖非常有用。

    | **KEYWORDS:prefer=** | **“Programs”下的快捷方式** | **是否匹配** |
    |---|---|---|
    | Word | \Microsoft Office\Microsoft **Word** 2010 | 是 |
    | "Microsoft Word" | \Microsoft Office**Microsoft Word** 2010 | 是 |
    | 控制台 | \McAfee\VirusScan **Console** | 是 |
    | Virus | \McAfee\VirusScan Console | 否 |
    | McAfee | \McAfee\VirusScan Console | 否 |

  - prefer="\\Folder1\Folder2\...\ApplicationName"
    绝对路径模式与完整的快捷方式文件路径以及“开始”菜单下的完整应用程序名称相匹配。 “Programs”文件夹是“开始”菜单目录下的子文件夹，因此必须将其包含在绝对路径中以确定该文件夹中的目标应用程序。 如果路径中有空格，则需要使用引号。 匹配区分大小写。 绝对路径匹配模式对在 XenDesktop 中以程序方式执行的替代非常有用。

    | **KEYWORDS:prefer=** | **“Programs”下的快捷方式** | **是否匹配** |
    |---|---|---|
    | "\\Programs\Microsoft Office\Microsoft Word 2010" | **\Programs\Microsoft Office\Microsoft Word 2010** | 是 |
    | "\\Microsoft Office\" | \Programs\Microsoft Office\Microsoft Word | 否 |

| KEYWORDS:prefer= | “Programs”下的快捷方式 | 是否匹配 |
| --- | --- | --- |
| "\\Microsoft Word 2010" | \Programs\Microsoft Office\Microsoft Word 2010 | 否 |
| "\\Programs\Microsoft Word 2010" | **\Programs\Microsoft Word 2010** | 是 |

- prefer=”\Folder1\Folder2\...\ApplicationName”
  相对路径模式与“开始”菜单下的相对快捷方式文件路径相匹配。 提供的相对路径中必须包含应用程序名称，并且可以选择性包含快捷方式所在的文件夹。 如果快捷方式文件路径以提供的相对路径结束，匹配将非常有用。 如果路径中有空格，则需要使用引号。 匹配区分大小写。 相对路径匹配模式对以程序方式执行的替代非常有用。

| KEYWORDS:prefer= | “Programs”下的快捷方式 | 是否匹配 |
| --- | --- | --- |
| "\Microsoft Office\Microsoft Word 2010" | **\Microsoft Office\Microsoft Word 2010** | 是 |
| "\Microsoft Office\" | \Microsoft Office\Microsoft Word 2010 | 否 |
| "\Microsoft Word 2010" | \Microsoft Office**\Microsoft Word 2010** | 是 |
| "\Microsoft Word" | \Microsoft Word 2010 | 否 |

有关其他关键字的信息，请参阅 StoreFront 文档优化用户体验中的“其他建议”部分。

# 配置 XenDesktop 环境

Jul 07, 2016

本文中的主题介绍如何配置 USB 支持、防止 Desktop Viewer 窗口变暗以及配置多用户和设备的设置。

### 为 XenDesktop 和 XenApp 连接配置 USB 支持

USB 支持允许用户在连接到虚拟桌面时与大量的 USB 设备进行交互。 用户可以将 USB 设备插入其计算机，然后该设备将会远程连接至其虚拟桌面。 可用于远程连接的 USB 设备包括闪存驱动器、智能电话、PDA、打印机、扫描仪、MP3 播放器、安全设备和平板计算机。 Desktop Viewer 用户可以使用工具栏中的首选项控制 USB 设备在虚拟桌面上的可用性。

此外还支持典型低延迟/高速 LAN 环境中的 USB 同步设备，例如网络摄像头、麦克风、扬声器和耳机。 这样一来，这些设备可使用诸如 Microsoft Office Communicator 和 Skype 软件包进行交互。

XenDesktop 和 XenApp 会话直接支持下列类型的设备，因此不使用 USB 支持：

- 键盘
- 鼠标
- 智能卡

注意：可将专用 USB 设备（例如，Bloomberg 键盘和 3-D 鼠标）配置为使用 USB 支持。 有关配置 Bloomberg 键盘的信息，请参阅 Configure Bloomberg keyboards（配置 Bloomberg 键盘）。 有关为其他专用 USB 设备配置策略规则的信息，请参阅 CTX 119722。

默认情况下，不支持通过 XenDesktop 和 XenApp 对特定类型的 USB 设备进行远程处理。 例如，用户可能有通过内部 USB 连接到系统板的网络接口卡。 不适合对这种设备进行远程连接。 默认情况下，不支持将下列类型的 USB 设备用于 XenDesktop 会话：

- 蓝牙适配器
- 集成的网络接口卡
- USB 集线器
- USB 图形适配器

连接到集线器的 USB 设备可远程处理，但集线器本身无法远程处理。

默认情况下，不支持将下列类型的 USB 设备用于 XenApp 会话：

- 蓝牙适配器
- 集成的网络接口卡
- USB 集线器
- USB 图形适配器
- 音频设备
- 大容量存储设备

有关修改用户可用的 USB 设备范围的说明，请参阅更新可进行远程连接的 USB 设备的列表。

有关自动重定向特定 USB 设备的说明，请参阅 CTX123015。

## USB 支持的工作原理

用户插入 USB 设备后，系统将根据 USB 策略对该设备进行检查，如果允许，则会将其远程连接到虚拟桌面。 如果默认策略拒

绝连接此设备，则只能在本地桌面中使用。

用户插入 USB 设备时，会向用户显示通知，告知用户发现新设备。 用户通过每次在连接后从列表中选择设备，可以决定将哪些 USB 设备远程连接到虚拟桌面。 或者，用户可以配置 USB 支持，以便在会话之前和/或会话期间插入的所有 USB 设备都会自动远程连接到虚拟桌面。

### 大容量存储设备

除 USB 支持外，远程访问可以通过客户端驱动器映射来实现，您可以通过 Citrix Receiver 策略远程连接客户端设备 > 客户端驱动器映射来配置驱动器映射，这仅适用于大容量存储设备。 应用此策略后，用户登录时，用户设备上的驱动器将自动映射至虚拟桌面上的驱动器盘符。 这些驱动器显示为具有映射驱动器盘符的共享文件夹。

两种类型的远程连接策略之间的主要区别如下：

| 功能 | 客户端驱动器映射 | USB 支持 |
| --- | --- | --- |
| 默认情况下处于启用状态 | 是 | 否 |
| 可配置只读访问权限 | 是 | 否 |
| 可在会话期间安全删除设备 | 否 | 如果用户单击通知区域中的安全删除硬件，则为“是” |

如果同时启用通用 USB 和客户端驱动器映射策略，并在会话开始之前插入大容量存储设备，将首先使用客户端驱动器映射进行重定向，然后才考虑通过 USB 支持进行重定向。 如果在会话开始之后插入该设备，则将首先使用 USB 支持进行重定向，然后才考虑使用客户端驱动器映射。

### 默认情况下允许连接的 USB 设备类

默认 USB 策略规则允许连接多种 USB 设备类。

虽然此列表中列出了这些 USB 设备类，但其中某些类只能在进行额外配置后才能在 XenDesktop 和 XenApp 会话中用于远程连接。 这些类如下所示。

- 音频（类 01）。 包括音频输入设备（麦克风）、音频输出设备和 MIDI 控制器。 现今的音频设备通常使用等量传输，但是 XenDesktop 4 或更高版本不支持此功能。 音频（类 01）不适用于 XenApp，因为这些设备在 XenApp 中不可以使用 USB 支持进行远程连接。
  注意：某些专业设备（例如 VOIP 电话），需要进行额外配置。 有关此操作的相关说明，请参阅 CTX123015。
- 物理接口设备（类 05）。 这些设备类似于人体学接口设备 (HID)，但是通常提供“实时”输入或反馈，包括力量反馈式操纵杆、运动平台和力量反馈式外骨骼。
- 静止图像处理（类 06）。 包括数码相机和扫描仪。 数码相机通常支持静止图像处理类，该类使用图片传输协议 (PTP) 或媒体传输协议 (MTP) 将图像传输到计算机或其他外设。 相机还可能显示为大容量存储设备，并可能通过相机自身提供的安装菜单配置相机以使用其中任一类。
  请注意，如果相机显示为大容量存储设备，则应使用客户端驱动器映射，而不需要 USB 支持。
- 打印机（类 07）。 虽然某些打印机使用供应商特定协议（类 ff），但是大多数打印机通常仍包含在此类中。 多功能打印机可能具有内部集线器或是复合设备。 在这两种情况下，打印元素通常使用打印机类，扫描或传真元素使用其他类，例如，静止图像处理。
  打印机通常在没有 USB 支持的情况下也可以正常工作。

注意：此类设备（特别是具有扫描功能的打印机）需要进行额外配置。 有关此操作的相关说明，请参阅 CTX123015。

- 大容量存储（类 08）。 最常见的大容量存储设备是 USB 闪存驱动器；其他大容量存储设备包括 USB 外置硬盘驱动器、CD/DVD 驱动器和 SD/MMC 卡读卡器。 许多有内部存储功能的设备也提供大容量存储接口，包括媒体播放器、数码相机和手机。 大容量存储（类 08）不适用于 XenApp，因为这些设备在 XenApp 中不可以使用 USB 支持进行远程连接。 已知的子类包括：
  - 01 受限的闪存设备
  - 02 典型的 CD/DVD 设备 (ATAPI/MMC-2)
  - 03 典型的磁带设备 (QIC-157)
  - 04 典型的软盘驱动器 (UFI)
  - 05 典型的软盘驱动器 (SFF-8070i)
  - 06 大部分使用 SCSI 的此变体的大容量存储设备

  通常情况下，可以通过客户端驱动器映射来访问大容量存储设备，因此 USB 支持并不是必需的。

  重要：众所周知，有些病毒会使用所有类型的大容量存储实时传播。 因此，请慎重考虑是否存在允许使用大容量存储设备（通过客户端驱动器映射或 USB 支持）的业务需求。
- 内容安全性（类 0d）。 内容安全性设备可以加强内容保护，通常用于保护许可或数字版权管理。 此类包含硬件保护装置。
- 视频（类 0e）。 视频类包括用于处理视频或视频相关材料的设备，例如网络摄像机、数码摄相机、模拟视频变频器、某些电视调谐器，以及一些支持视频流的数码相机。

  注意：大多数音频设备使用等量传输，但是 XenDesktop 4 或更高版本不支持此功能。 某些音频设备（例如具有运动检测功能的网络摄像机）需要进行额外配置。 有关此操作的相关说明，请参阅 CTX123015。
- 个人医疗保健（类 0f）。 这些设备包括血压传感器、心率监测器、步程计、药片监测器和肺活量计等个人医疗保健设备。
- 应用程序特定和供应商特定（类 fe 和类 ff）。 许多设备使用供应商特定协议或未由 USB 联合会标准化的协议，这些协议通常显示为供应商特定（类 ff）。

### 默认情况下拒绝连接的 USB 设备类

默认 USB 策略规则拒绝连接以下 USB 设备类：

- 通信和 CDC 控制（类 02 和 0a）。 默认 USB 策略不允许连接这些设备，因为其中的一个设备可能提供与虚拟桌面自身的连接。
- 人体学接口设备（类 03）。 包含各种输入和输出设备。 典型的人体学接口设备 (HID) 包括：键盘、鼠标、指针设备、图形板、传感器、游戏控制器、按钮和控制功能。

  子类 01 又称为“引导接口”类，可供键盘和鼠标使用。

  默认的 USB 策略不允许使用 USB 键盘（类 03，子类 01，协议 1）或 USB 鼠标（类 03，子类 01，协议 2）。 这是因为即使没有 USB 支持，大部分键盘和鼠标也能够进行相应的处理，并且连接到虚拟桌面之后，通常需要本地使用和远程使用这些设备。

- USB 集线器（类 09）。 USB 集线器允许将附加设备连接到本地计算机。 无需远程访问这些设备。
- 智能卡（类 0b）。 智能卡读卡器包括非接触式智能卡读卡器和接触式智能卡读卡器，以及具有嵌入式智能卡等效芯片的 USB 令牌。

  可以使用智能卡远程连接功能访问智能卡读卡器，而不需要 USB 支持。

- 无线控制器（类 e0）。 其中一些设备可能提供关键的网络访问，或者连接关键的外设，如 Bluetooth 键盘或鼠标。

  默认 USB 策略不允许连接这些设备。 但是，有些特殊设备可能适合使用 USB 支持提供访问权限。

- **各种网络设备（类 ef，子类 04）**。 其中的一些设备可以提供关键网络访问。 默认 USB 策略不允许连接这些设备。 但是，有些特殊设备可能适合使用 USB 支持提供访问权限。

### 更新可进行远程连接的 USB 设备列表

可以通过编辑 icaclient_usb.adm 文件来更新可远程连接到桌面的 USB 设备的范围。 这允许您使用组策略对 Receiver 进行更改。 该文件位于以下已安装的文件夹中：

:\Program Files\Citrix\ICA Client\Configuration\en

或者，您可以编辑每个用户设备上的注册表，从而添加以下注册表项：

HKLM\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB Type=String Name="DeviceRules" Value=

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。
产品默认规则的存储位置为：

HKLM\SOFTWARE\Citrix\ICA Client\GenericUSB Type=MultiSz Name=“DeviceRules” Value=

请勿编辑产品默认规则。

有关这些规则及其语法的详细信息，请参阅 http://support.citrix.com/article/ctx119722/。

### 配置 Bloomberg 键盘

XenDesktop 和 XenApp 会话支持 Bloomberg 键盘（但不支持其他 USB 键盘）。 安装插件时，系统会自动安装所需的组件，但您必须在安装过程中或之后通过更改注册表项来启用此功能。

在任何一个用户设备上，均不建议与 Bloomberg 键盘进行多个会话。 该键盘只在单会话环境中才能正常使用。

**打开或关闭 Bloomberg 键盘支持**

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. 在注册表中找到以下注册表项：
   HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB
2. 执行以下操作之一：
   - 要打开此功能，对于“类型”为 DWORD 且“名称”为 EnableBloombergHID 的条目，请将“值”设置为 1。
   - 要关闭此功能，请将“值”设置为 0。

### 防止 Desktop Viewer 窗口变暗

如果用户使用了多个 Desktop Viewer 窗口，则默认情况下，处于非活动状态的桌面将变暗。 如果需要同时查看多个桌面，这可能会使这些桌面上的信息无法阅读。 通过编辑注册表，您可以禁用默认行为并防止 Desktop Viewer 窗口变暗。

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. 在用户设备上，根据是要防止设备的当前用户变暗还是防止设备本身变暗，在以下注册表项之一中创建一个名为 DisableDimming 的 REG_DWORD 条目。 如果已在设备上使用 Desktop Viewer，则已存在某个条目：

   - HKCU\Software\Citrix\XenDesktop\DesktopViewer
   - HKLM\Software\Citrix\XenDesktop\DesktopViewer

   或者，可以通过在以下注册表项之一中创建相同的 REG_WORD 条目来定义本地策略，而无需通过上述用户或设备设置控制变暗：

   - HKCU\Software\Policies\Citrix\XenDesktop\DesktopViewer

- HKLM\Software\Policies\Citrix\XenDesktop\DesktopViewer

使用这些注册表项是可选的，因为 XenDesktop 管理员（而非插件管理员或用户）通常使用组策略来控制策略设置。 因此，使用这些注册表项之前，请检查您的 XenDesktop 管理员是否已为此功能设置了策略。

2. 将该条目设置为任意非零值，例如 1 或 true。

   如果未指定条目或将条目设置为 0，则 Desktop Viewer 窗口将变暗。 如果指定了多个条目，则将使用以下优先级。 此列表中的第一个条目及其值确定窗口是否变暗：

   1. HKCU\Software\Policies\Citrix\...
   2. HKLM\Software\Policies\Citrix\...
   3. HKCU\Software\Citrix\...
   4. HKLM\Software\Citrix\...

## 配置面向多个用户和设备的设置

除了 Receiver 用户界面所提供的配置选项外，还可以使用“组策略编辑器”和 icaclient.adm 模板文件来配置设置。 使用“组策略编辑器”可以执行以下操作：

- 通过编辑 icaclient.adm 文件来扩展 icaclient 模板，使之涵盖任何 Receiver 设置。 有关编辑 .adm 文件以及对特定计算机应用设置的详细信息，请参阅“Microsoft 组策略”文档。
- 执行仅面向某客户端设备特定用户或者所有用户的更改。
- 配置面向多个用户设备的设置

Citrix 建议使用“组策略”来远程配置用户设备，但您也可以使用任何其他方法，包括使用可更新相关注册表项的“注册表编辑器”。

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. 在用户配置节点或计算机配置节点下，根据需要编辑相关设置。

# 配置 StoreFront

Jul 19, 2016

Citrix StoreFront 向 XenDesktop、XenApp 和 VDI-in-a-Box 对用户进行身份验证，枚举可用桌面和应用程序并将其聚合到用户可以通过 Receiver 访问的应用商店中。

除了本部分概述的配置，您还必须配置 NetScaler Gateway 或 Access Gateway，以支持用户从内部网络之外进行连接（例如，从 Internet 或远程位置连接）。

> **注意**
>
> 在您选择用于显示所有帐户的选项后，Citrix Receiver for Windows 始终显示较旧的 StoreFront 用户界面（绿色气泡主题），而非显示更新后的 StoreFront 用户界面。

## 配置 StoreFront

1. 请按照 StoreFront 文档中所述安装和配置 StoreFront。 Receiver for Windows 要求 HTTPS 连接。 如果为 StoreFront 服务器配置了 HTTP，则必须按使用命令行参数配置和安装 Receiver for Windows 中所述在用户设备上的 ALLOWADDSTORE 属性描述下设置一个注册表项。
   注意：对于需要更大控制权的管理员，Citrix 提供了一个模板，供您创建 Receiver 下载站点。

## 管理工作区控制重新连接

工作区控制功能使应用程序能够随用户在设备之间移动。 例如，可以使医院的临床医生在不同的工作站之间移动，而无需在每个设备上重新启动自己的应用程序。 对于 Receiver for Windows，请通过修改注册表在客户端设备上管理工作区控制。 也可以使用组策略为加入域的客户端设备管理工作区控制。

**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。

在主桌面映像中或 XenApp 服务器托管中创建 WSCReconnectModeUser 并修改现有注册表项 WSCReconnectMode。 已发布的桌面可以更改 Receiver 的行为。

Windows Receiver 的 WSCReconnectMode 注册表项设置：

- 0 = 不重新连接到任何现有会话
- 1 = 应用程序启动时重新连接
- 2 = 应用程序刷新时重新连接
- 3 = 应用程序启动或刷新时重新连接
- 4 = Receiver 界面打开时重新连接
- 8 = Windows 登录时重新连接
- 11 = 3 和 8 的组合

**禁用 Windows Receiver 的工作区控制**

要禁用 Windows Receiver 的工作区控制，请创建以下注册表项：

HKEY_CURRENT_USER\SOFTWARE\Wow6432Node\Citrix\Dazzle（面向 64 位）

HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle（面向 32 位）

名称：**WSCReconnectModeUser**

类型：REG_SZ

值数据：0

将以下注册表项的默认值从 3 修改为 0

HKEY_CURRENT_USER\SOFTWARE\Wow6432Node\Citrix\Dazzle（面向 64 位）

HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle（面向 32 位）

名称：**WSCReconnectMode**

类型：REG_SZ

值数据：0

**注意**：如果不创建新注册表项，也可以将 REG_SZ 值 WSCReconnectAll 设置为 false。

**更改状态指示器超时**

您可以更改用户启动会话时状态指示器显示的时间长度。 要更改超时期限，请在 HKLM\SOFTWARE\Citrix\ICA CLIENT\Engine\ 中创建 REG_DWORD 值 SI INACTIVE MS。 如果希望状态指示器尽快消失，可以将 REG_DWORD 值设置为 4。

> ### 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。

# 使用组策略对象模板配置 Receiver

Jan 20, 2017

## 通过 GPO 添加或指定应用商店

Citrix 建议使用组策略对象，并提供模板文件 receiver.adm 或 receiver.admx\receiver.adml（具体取决于操作系统）来配置与 Citrix Receiver for Windows 相关的设置。

> ### 注意
>
> receiver.admx/receiver.adml 适用于 Windows Vista / Windows Server 2008 或更高版本。 ADM 文件仅可用于 Windows XP 嵌入版平台。

> ### 注意
>
> 如果 Citrix Receiver for Windows 是通过 VDA 安装配置的，则会在 Citrix Receiver for Windows 安装目录中找到 admx/adml 文件。 例如：<安装目录>\online plugin\Configuration。

请参见以下表格获取有关 Citrix Receiver for Windows 模板文件及其各自位置的信息。

| 文件类型 | 文件位置 |
| --- | --- |
| receiver.adm | <安装目录>\ICA Client\Configuration |
| receiver.admx | <安装目录>\ICA Client\Configuration |
| receiver.adml | <安装目录>\ICA Client\Configuration\[MUIculture] |

> ### 注意
>
> Citrix 建议您使用随最新的 Citrix Receiver for Windows 提供的模板文件。 导入最新的文件时，将保留之前的设置。

将 adm 模板文件添加到本地 GPO

注意：可以使用 adm 模板文件配置本地 GPO 和/或基于域的 GPO。

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侧窗格中，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”并浏览到模板文件位置 <Installation Directory>\ICA Client\Configuration\receiver.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。
Citrix Receiver for Window 模板文件将在本地 GPO 中提供，路径为“管理模板”>“经典管理模板(ADM)”>“Citrix 组件”>“Citrix Receiver”。
向本地 GPO 添加 adm 模板文件后，会显示以下消息：
“下列在 [strings] 节中的项目太长，被截断：
单击“确定”忽略此消息。

将 admx/adml 模板文件添加到本地 GPO

注意：可以使用 admx/adml 模板文件配置本地 GPO 和/或基于域的 GPO。 请参阅有关管理 ADMX 文件的 Microsoft MSDN 文章（此处）
1. 安装 Citrix Receiver for Windows 之后，复制模板文件。

admx：
从：<安装目录>\ICA Client\Configuration\receiver.admx
到：%systemroot%\policyDefinitions

adml:
从：<Installation Directory>\ICA Client\Configuration\[MUIculture]receiver.adml
到：%systemroot%\policyDefinitions\[MUIculture]

Citrix Receiver for Window 模板文件在本地 GPO 中提供，路径为“管理模板”>“Citrix 组件”>“Citrix Receiver”目录。

Citrix 建议使用组策略对象 icaclient.adm 模板文件为网络路由、代理服务器、可信服务器配置、用户路由、远程用户设备和用户体验配置规则。

您可以将 icaclient.adm 模板文件用于域策略和本地计算机策略。 对于域策略，请使用组策略管理控制台导入此模板文件。 如果要将 Citrix Receiver 设置应用到整个企业内许多不同的用户设备，这一点非常有用。 如果只希望影响单个用户设备，请使用设备上的本地组策略编辑器导入此模板文件。

### 使用组策略对象模板的 Receiver 配置

> **注意**
>
> Citrix 建议您使用随最新的 Citrix Receiver 提供的 GPO 模板文件。 导入最新的文件时，将保留之前的设置。

### 关于 TLS 和组策略

使用此策略可配置用于确保 Citrix Receiver 能够安全地标识其连接到的服务器的 TLS 选项以及加密与服务器的所有通信。
Citrix 建议通过不可信网络建立的连接使用 TLS。 Citrix 支持在 Receiver 与 XenApp 或 XenDesktop 之间使用 TLS 1.0、TLS 1.1 和 TLS 1.2 协议。

启用此策略时，可以通过选中“Require SSL for all connections”（要求为所有连接使用 SSL）复选框，强制 Receiver 为与已发

布的应用程序和桌面建立的所有连接使用 TLS。

Citrix Receiver 按服务器出示的安全证书上的名称标识服务器。 其格式为 DNS 名称（例如 www.citrix.com）。 可以将 Receiver 限制为仅连接到“Allowed SSL servers”（允许连接的 SSL 服务器）设置中逗号分隔的列表指定的特定服务器。 可以在此处指定通配符和端口号；例如，*.citrix.com:4433 允许在端口 4433 上连接到通用名以 .citrix.com 结尾的任何服务器。 安全证书中的信息准确度由证书的颁发者声明。 如果 Receiver 无法识别和信任证书的颁发者，连接将被拒绝。

通过 TLS 连接时，服务器可能会配置为要求 Receiver 提供用于标识自身的安全证书。 使用“Client Authentication”（客户端身份验证）设置可配置是否自动提供标识，以及是否通知用户。 选项包括：

- never supply identification（从不提供标识）
- only use the certificate configured here（仅使用在此处配置的证书）
- to always prompt the user to select a certificate（始终提示用户选择证书）
- to prompt the user only if there a choice of certificate to supply（仅当需要选择提供的证书时才提示用户）

> **提示**
>
> 使用“Client Certificate”（客户端证书）设置可指定标识证书的缩略图以避免不必要地提示用户。

验证服务器的安全证书时，可以将插件配置为与证书的颁发者联系以获取证书吊销列表 (CRL)，从而确保服务器的证书尚未被吊销。 这样可以在系统受到影响时允许颁发者使证书失效。 使用“CRL verification setting”（CRL 验证设置）可将插件配置为：

- not check CRLs at all（根本不检查 CRL）
- only check CRLs that have been previously obtained from the issuer（仅检查以前从颁发者处获取的 CRL）
- actively retrieve an up-to-date CRL（主动获取最新的 CRL）
- to refuse to connect unless it can obtain an up-to-date CRL（除非能够获取最新的 CRL，否则拒绝连接）

为多种产品配置 TLS 的组织可以通过指定证书策略 OID 作为安全证书的一部分来选择标识用于 Citrix 插件的服务器。 如果在此处配置了策略 OID，Receiver 将仅接受声明了兼容策略的证书。

某些安全策略对用于连接的加密算法有一定的要求。 可以将插件限制为仅对“TLS version”（TLS 版本）设置使用 TLS v1.0、TLS 1.1 和 TLS 1.2。 同样，可以将插件限制为仅使用某些加密密码集。 这些密码集包括：

政府密码集：

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384

商用密码集：

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_AES_128_GCM_SHA256

### FIPS 安全标准合规性

Citrix Receiver for Windows 4.4 引入了 TLS 和合规模式配置选项以配置 FIPS（联邦信息处理标准）。 使用此功能可确保只能

对所有 ICA 连接使用 FIPS (Publication 140-2) 批准的加密。

新安全合规模式支持 NIST SP 800-52。 默认情况下，此模式处于禁用状态（设置为“NONE”（无））。

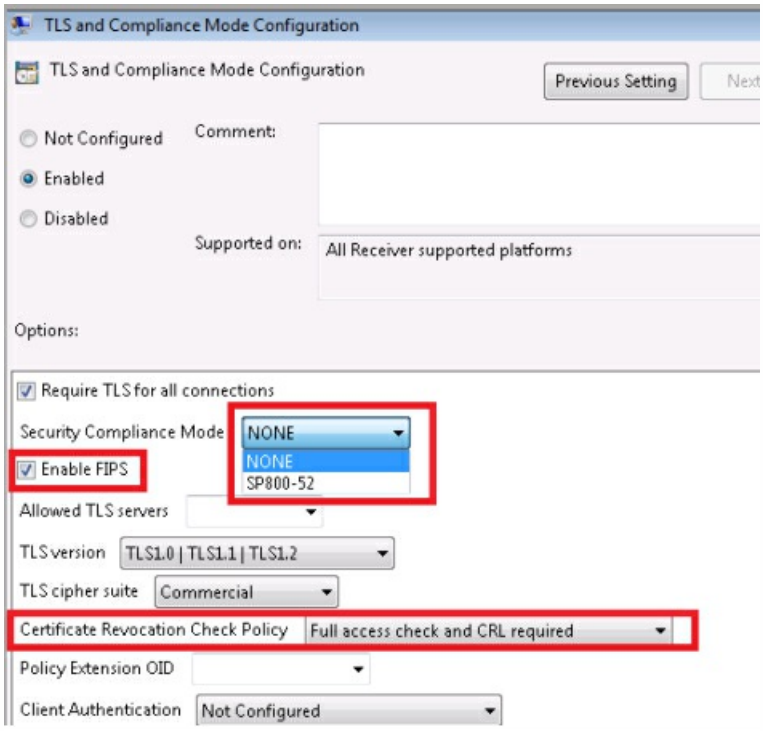
> **注意**
>
> 有关 NIST SP 800-52 要求的合规性的其他信息，请参阅 NIST page describing guidelines for TLS implementations（用于说明 TLS 实现的准则的 NIST 页）。

本版本的 Citirx Receiver 还允许您定义 TLS 版本，这将确定适用于 ICA 连接的 TLS 协议。 应选择同时适用于客户端和服务器的最高版本。

使用这些功能时，请在“TLS and Compliance Mode Configuration”（TLS 和合规模式配置）屏幕中执行以下操作：

- 选中“Enable FIPS”（启用 FIPS）复选框以使用批准的适用于所有 ICA 会话的加密。
- 将“Security Compliance Mode”（安全合规模式）设置为“SP 800-52”。
- 选择 TLS 版本。

下图说明了 FIPS 选项。




> **注意**
>
> 默认情况下，FIPS 处于禁用状态（未选中）。

## 配置 FIPS

要在所有 ICA 客户端之间配置 FIPS 加密，请执行以下操作：

1. 选择“计算机配置”>“管理模板”>“Citrix 组件”>“网络路由”> **TLS and Compliance Mode Configuration**（TLS 和合规模式配置）。
2. 在“TLS and Compliance Mode Configuration”（TLS 和合规模式配置）屏幕中，选择 **Enable FIPS**（启用 FIPS）。
3. 在“Security Compliance Mode”（安全合规模式）部分中，使用下拉菜单选择 **SP 800-52**。 配置此选项时请注意：
   - SP 800-52 合规模式要求 FIPS 合规；启用了 SP 800-52 时，无论 FIPS 设置为何，都会启用 FIPS 模式。
   - “Certificate Revocation Check Policy”（证书吊销检查策略）设置为 *Full access check and CRL required*（需要执行完全访问权限检查和 CRL）或 *Full access check and CRL required all*（全部需要执行完全访问权限检查和 CRL）。
4. 选择适用于 ICA 连接的恰当 TLS 协议版本；应选择同时适用于客户端和服务器的最高 TLS 版本，选项包括：
   - TLS 1.0 | TLS 1.1 | TLS 1.2（默认）
   - TLS 1.1 | TLS 1.2
   - TLS 1.2

### 关于 ADMX 模板的使用

安装 StoreFront 3.0 和 Citrix Receiver 4.3 后，Citrix XenApp 和 XenDesktop 支持 Microsoft 用于显示基于注册表的策略设置的新格式（使用基于标准 XML 文件格式），称为 ADMX 文件。

在 Windows Vista/ Windows Server 2008 及更高版本中，这些新文件替代了 ADM 文件，后者使用自己的标记语言。 ADM 文件仍可用于 Windows XP 嵌入版平台。 您使用的管理工具（组策略对象编辑器和组策略管理控制台）大致保持不变。 在大多数情况下，您在执行日常组策略管理任务过程中不会注意到 ADMX 文件的存在。

中央应用商店是使用新 ADMX 文件的主要优势之一。 虽然默认情况下不适用中央应用商店，但您仍可以在管理基于域的 GPO 时使用此选项。 与使用早期版本的 ADM 文件的情况不同，组策略对象编辑器不会将 ADMX 文件复制到每个已编辑的 GPO，但是能够从域控制器 sysvol（用户不可配置）上的一个域级别位置或在中央应用商店不可用时从本地管理工作站读取。 可以通过将自定义 ADMX 文件复制到中央应用商店来共享该文件，使其自动对域中的所有组策略管理员可用。 此功能简化了策略管理，改进了 GPO 文件的存储优化。

ADMX 文件分为中心语言 (ADMX) 和特定语言 (ADML) 资源，对所有组策略管理员可用。 这些因素允许组策略工具根据管理员已配置的语言调整其 UI。

> **注意**
>
> 更多详细信息，请查找与管理 ADMX 文件有关的 Microsoft MSDN 文章。

## ADMX 和 ADML 的文件名和位置

ADM 文件的命名约定（在早期版本的 Receiver 中提供）已得以改进。 下表提供了 ADM 文件到新 ADMX 文件名的映射：

| Citrix Receiver 版本（4.3 之前的版本） | Citrix Receiver 版本（4.3 及更高版本） |
| --- | --- |
| Icaclient.adm | receiver.admx\receiver.adm |
| Icaclient_usb.adm | receiver_usb.admx\receiver_usb.adm |

| | |
|---|---|
| ica-file-signing.adm | ica-file-signing.admx\ica-file-signing.admx |
| HdxFlash-Client.adm | HdxFlash-Client.admx\HdxFlash-Client.admx |

> **注意**
>
> 请在 Windows Vista/Windows Server 2008 及更高版本上使用 .admx 文件，对其他平台使用 .adm 文件。

可以将通过 Citrix Receiver 安装程序分发的自定义 ADMX 和 ADML 文件复制到中央应用商店，使其自动对域中的所有组策略管理员可用。 下表提供了需要复制 ADMX 和 ADML 文件的位置：

| 文件类型 | 文件位置 |
|---|---|
| receiver.admx | <安装目录>\ICA Client\Configuration |
| ica-file-signing.admx | <安装目录>\ICA Client\Configuration |
| receiver_usb.admx | <安装目录>\ICA Client\Configuration\en |
| HdxFlash-Client.admx | <安装目录>\ICA Client\Configuration |
| receiver.adml | <安装目录>\ICA Client\Configuration |
| ica-file-signing.adml | <安装目录>\ICA Client\Configuration |
| receiver_usb.adml | <安装目录>\ICA Client\Configuration\en |
| HdxFlash-Client.adml | <安装目录>\ICA Client\Configuration\[MUIculture] |

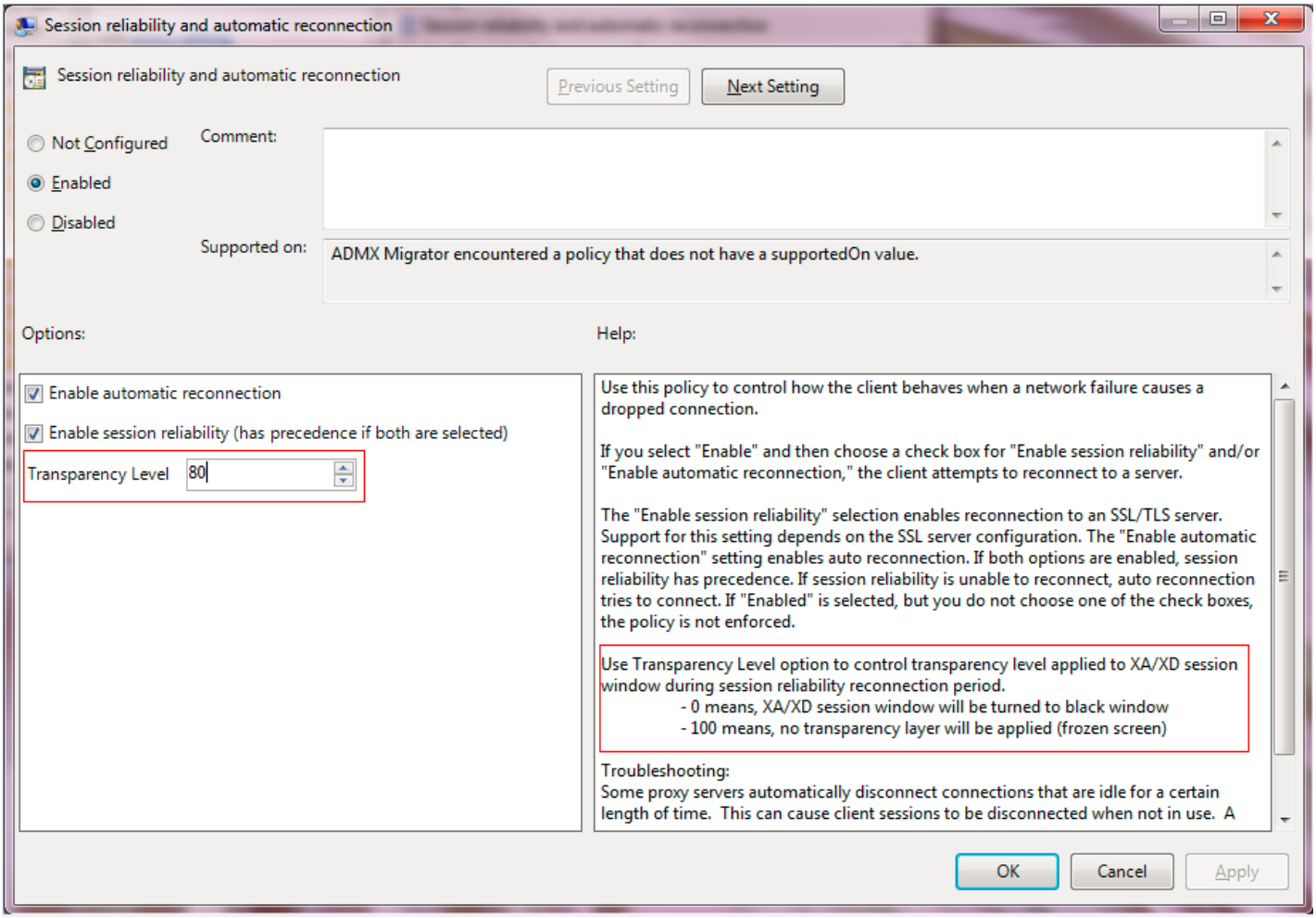
> **注意**
>
> 如果 Citrix Receiver 是通过 VDA 安装配置的，可以在安装目录中找到 ADMX/ADML 文件。 例如：<安装目录>\online plugin\Configuration。

### 会话可靠性组策略

配置会话可靠性组策略时，请设置透明度级别。 使用此选项可以在会话可靠性重新连接期间控制适用于已发布的应用程序（或桌面）的透明度级别。

要配置透明度级别，请选择**计算机配置 - > 管理模板 -> Citrix 组件 - > 网络路由 -> 会话可靠性和自动重新连接 - > 透明度级别**。

> ## 注意
>
> 默认情况下，“透明度级别”设置为 80。



# 向用户提供帐户信息

Feb 02, 2016

请向用户提供访问虚拟桌面和应用程序所需的帐户信息。 您可以使用以下方法之一提供此信息：

- 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

> **Important**
>
> 建议首次使用 Citrix Receiver 的用户在安装后重新启动 Receiver。 重新启动 Receiver 可确保用户能够添加帐户，并且 Receiver 能够发现在安装 Receiver 处于暂停状态的 USB 设备。

## 配置基于电子邮件的帐户发现

配置 Receiver 以实现基于电子邮件的帐户发现时，首次安装并配置 Receiver 过程中，用户需要输入自己的电子邮件地址（而非服务器 URL）。 Receiver 将根据域名系统 (DNS) 服务 (SRV) 记录确定与电子邮件地址相关联的是 NetScaler Gateway、Access Gateway 还是 StoreFront 服务器，然后提示用户登录以访问虚拟桌面和应用程序。

> **注意**
>
> 配置有 Web Interface 的部署不支持基于电子邮件的帐户发现。

要将 DNS 服务器配置为支持基于电子邮件的发现，请参阅 StoreFront 文档中的配置基于电子邮件的帐户发现。

要配置 NetScaler Gateway，请参阅 NetScaler Gateway 文档中的使用基于电子邮件的发现连接到 StoreFront。

## 向用户提供置备文件

StoreFront 提供置备文件，用户可以打开这些置备文件以连接到应用商店。

- 您可以使用 StoreFront 来创建包含帐户的连接详细信息的置备文件。 将这些文件提供给用户，以便用户能够自动配置 Receiver。 安装 Receiver 后，用户只需打开此文件即可配置 Receiver。 如果您配置了 Receiver for Web 站点，用户还可以从这些站点获取 Receiver 置备文件。
  有关详细信息，请参阅 StoreFront 文档中的为用户导出应用商店置备文件。

## 向用户提供需手动输入的帐户信息

要使用户能够手动设置帐户，请务必分发连接到其虚拟桌面和应用程序所需的信息。

- 要连接到 StoreFront 应用商店，请提供该服务器的 URL。 例如：https://servername.company.com
  对于 Web Interface 部署，请提供 XenApp Services 站点的 URL。
- 要通过 NetScaler Gateway 连接，请先确定用户应看到所有已配置的应用商店，还是仅应看到对特定 NetScaler Gateway 启用了远程访问的应用商店。
  - 显示所有已配置的应用商店：向用户提供 NetScaler Gateway 完全限定的域名。

- 限制对特定应用商店的访问：按以下格式向用户提供 NetScaler Gateway 完全限定的域名以及应用商店名称：**NetScalerGatewayFQDN?MyStoreName**

  例如，如果名为 SalesApps 的应用商店对 server1.com 启用了远程访问，名为 HRApps 的应用商店对 server2.com 启用了远程访问，则用户必须输入 server1.com?SalesApps 以访问 SalesApps，或者输入 server2.com?HRApps 以访问 HRApps。 此功能需要首次登录的用户通过输入 URL 创建一个帐户，对基于电子邮件的发现不可用。

用户输入新帐户的详细信息时，Receiver 将尝试验证连接。 如果验证成功，Receiver 将提示用户登录到该帐户。

要管理帐户，Receiver 用户可以打开 Receiver 主页，单击 ，然后单击**帐户**。

### 自动共享多个应用商店帐户

如果您有多个应用商店帐户，则可以将 Citrix Receiver for Windows 配置为在建立会话时自动连接到所有帐户。 要在打开 Receiver 时自动查看所有帐户，请执行以下操作：

**对于 32 位系统，请创建注册表项 CurrentAccount：**

位置：HKLM\Software\Citrix\Dazzle

注册表项名称：CurrentAccount

值：AllAccount

类型：REG_SZ

**对于 64 位系统，请创建注册表项 CurrentAccount：**

位置：HKLM\Software\Wow6432Node\Citrix\Dazzle

注册表项名称：CurrentAccount

值：AllAccount

类型：REG_SZ

> **警告**
>
> “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。

# 优化 Citrix Receiver 环境

Nov 02, 2016

可以为用户优化 Receiver 的运行环境。

- 缩短应用程序启动时间
- 映射客户端设备
- 支持 DNS 名称解析
- 将代理服务器与 XenDesktop 连接结合使用
- 为 NDS 用户提供支持
- 将 Receiver 与 XenApp for UNIX 结合使用
- 启用对匿名应用程序的访问

有关其他优化选项的信息，请参阅 XenDesktop 文档中与维护会话活动和优化用户 HDX 体验有关的主题。

# 缩短应用程序启动时间

Feb 02, 2016

使用会话预启动功能可以缩短应用程序在常规流量时段或高流量时段的启动时间，从而向用户提供更加优异的体验。 预启动功能允许在用户登录 Receiver 时或在计划的时间（如果用户已登录）创建预启动会话。

此预启动会话可缩短首个应用程序的启动时间。 用户向 Receiver 中添加新帐户连接时，在启动下一个会话之前，会话预启动功能将不起作用。 默认应用程序 ctxprelaunch.exe 在会话中运行，但对用户不可见。

从 StoreFront 2.0 版开始，StoreFront 部署支持会话预启动。 对于 Web Interface 部署，请务必使用 Web Interface 的“保存密码”选项以避免出现登录提示。 XenDesktop 7 部署不支持会话预启动。

默认禁用会话预启动功能。 要启用会话预启动功能，请在 Receiver 命令行中指定参数 ENABLEPRELAUNCH=true，或者将注册表项 EnablePreLaunch 设置为 true。 默认设置 null 表示预启动功能处于禁用状态。

注意：如果已将客户端计算机配置为支持域直通 (SSON) 身份验证，将自动启用预启动。 如果希望使用域直通 (SSON) 而不启用预启动，请将 EnablePreLaunch 注册表项的值设置为 false。
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。
注册表位置为：

HKLM\Software\[Wow6432Node\]Citrix\Dazzle

HKCU\Software\Citrix\Dazzle

有两种类型的预启动：

- **准时预启动**。 预启动功能在用户的凭据通过身份验证之后启动，而无论该时段是否为高流量时段。 通常在正常流量时段使用。 用户可以通过重新启动 Receiver 触发准时预启动功能。
- **计划的预启动**。 预启动功能在计划的时间启动。 计划的预启动仅在用户设备已开始运行且通过身份验证后启动。 如果到达计划的预启动时间时未满足这两个条件，会话将不启动。 为分散网络和服务器负载，该会话将在计划的时段内启动。 例如，如果计划的预启动安排在下午 1:45，该会话实际将在下午 1:15 到 1:45 之间启动。 通常在高流量时段使用。

在 XenApp 服务器上配置预启动功能的步骤包括：创建、修改或删除预启动应用程序，以及更新用于控制预启动应用程序的用户策略设置。 有关在 XenApp 服务器上配置会话预启动的信息，请参阅 XenApp 文档中的“将应用程序预启动到用户设备”。

不支持使用 icaclient.adm 文件自定义预启动功能。 但是，可以通过在安装 Receiver 的过程中或安装完成后修改注册表值来更改预启动配置。 有三个 HKLM 值、两个 HKCU 值：

- HKLM 值在客户端安装过程中写入。
- HKCU 值使您能够在同一计算机上向不同的用户提供不同的设置。 用户无需具有管理权限即可更改 HKCU 值。 可以向用户提供完成此操作所需的脚本。

## HKLM 注册表值

对于 Windows 7 和 8（64 位）：HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Prelaunch

对于支持的所有其他 32 位 Windows 操作系统：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Prelaunch

名称：UserOverride

值：

0 - 使用 HKEY_LOCAL_MACHINE 值，即使同时存在 HKEY_CURRENT_USER 值也是如此。

1 - 使用 HKEY_CURRENT_USER 值（如果这些值存在）；否则使用 HKEY_LOCAL_MACHINE 值。

名称：State

值：

0 - 禁用预启动功能。

1 - 启用“准时预启动”。 （预启动功能将在用户的凭据通过身份验证后启动。）

2 - 启用“计划的预启动”。 （预启动功能将在为 Schedule 配置的时间启动。）

名称：Schedule

值：

“计划的预启动”的时间（24 小时制）和具体日期按以下格式输入：

HH:MM|M:T:W:TH:F:S:SU，其中 HH 和 MM 为小时数和分钟数。 M:T:W:TH:F:S:SU 为一周内的具体日期。 例如，要在星期一、星期三和星期五下午 1:45 启用“计划的预启动”，请将 Schedule 设置为 Schedule=13:45|1:0:1:0:1:0:0。 该会话实际将于下午 1:15 到 1:45 之间启动。

### HKCU 注册表值

HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Prelaunch

这些 State 和 Schedule 注册表项与 HKLM 具有相同的值。

# 映射客户端设备

Feb 02, 2016

Receiver 支持在用户设备上映射设备，以使这些设备可以在会话中使用。 用户可以执行以下操作：

- 透明地访问本地驱动器、打印机和 COM 端口
- 在会话与本地 Windows 剪贴板之间进行剪切和粘贴
- 收听从会话播放的音频（系统声音和 .wav 文件）

在登录过程中，Receiver 将可用的客户端驱动器、COM 端口和 LPT 端口通知给服务器。 默认情况下，系统将客户端驱动器映射到服务器驱动器盘符，并为客户端打印机创建服务器打印队列，以使客户端打印机看起来像是直接连接到会话。 这些映射仅在当前会话期间对当前用户可用。 它们会在用户注销时被删除，并在用户下一次登录时重新创建。

可以使用重定向策略设置映射用户设备，无需在登录时自动映射。 有关详细信息，请参阅 XenDesktop 或 XenApp 文档。

## 关闭用户设备映射

可以使用 Windows 服务器管理器工具来配置用户设备映射，其中包括驱动器、打印机和端口等选项。 有关可用选项的详细信息，请参阅远程桌面服务的相关文档。

## 重定向客户端文件夹

客户端文件夹重定向改变了在主机端会话中访问客户端文件的方式。 当仅在服务器上启用客户端驱动器映射时，客户端满载的卷会作为通用命名约定 (UNC) 链接自动映射到会话中。 如果您在服务器上启用客户端文件夹重定向，同时用户也在用户设备上配置客户端文件夹重定向，将重定向用户指定的部分本地卷。

只有用户指定的文件夹会作为 UNC 链接显示在会话内，而不是显示用户设备上的完整文件系统。 如果通过注册表禁用 UNC 链接，客户端文件夹将在会话内显示为映射的驱动器。 有关详细信息，包括如何为用户设备配置客户端文件夹重定向，请参阅 XenDesktop 7 文档。

## 将客户端驱动器映射到主机端驱动器盘符

通过客户端驱动器映射，可以将主机端的驱动器盘符重定向到用户设备上的驱动器。 例如，可以将 Citrix 用户会话中的驱动器 H 映射到运行 Receiver 的用户设备上的驱动器 C。

客户端驱动器映射透明地内置到标准 Citrix 设备重定向程序中。 对于“文件管理器”、Windows 资源管理器和您的应用程序而言，这些映射看起来与任何其他网络映射都是一样的。

在安装过程中，可以将托管虚拟桌面和应用程序的服务器配置为将客户端驱动器自动映射到一组给定的驱动器盘符。 默认安装映射过程会从 V 开始按倒序映射分配给客户端驱动器的驱动器盘符，从而为每个固定驱动器和 CD-ROM 驱动器分配一个驱动器盘符。 （向软盘驱动器分配了其现有的驱动器盘符。）此方法在会话中采用以下驱动器映射：

| **客户端驱动器盘符** | **服务器在访问时使用的盘符：** |
|---|---|
| A | A |
| B | B |
| C | V |

| 客户端驱动器盘符 | 服务器在访问时使用的盘符： |
| --- | --- |
| D | U |

可以对服务器进行配置，使服务器驱动器盘符与客户端驱动器盘符不发生冲突；在这种情况下，服务器驱动器盘符会改为更高的驱动器盘符。 例如，将服务器的驱动器 C 改为 M，驱动器 D 改为 N，这样，客户端设备就可以直接访问其 C 和 D 驱动器。 这种方法将在会话中建立以下驱动器映射：

| 客户端驱动器盘符 | 服务器在访问时使用的盘符： |
| --- | --- |
| A | A |
| B | B |
| C | C |
| D | D |

用于替换服务器驱动器 C 的驱动器盘符在安装过程中定义。 所有其他固定驱动器和 CD-ROM 驱动器盘符均按顺序进行替换（例如，C > M、D > N、E > O）。 这些驱动器盘符不能与任何现有的网络驱动器映射发生冲突。 如果某一网络驱动器映射到与服务器驱动器盘符相同的驱动器盘符，则该网络驱动器映射将是无效的。

用户设备连接到服务器后，会重新建立客户端映射，除非禁用了自动客户端设备映射。 默认禁用客户端驱动器映射。 要更改设置，请使远程桌面服务（终端服务）配置工具。 也可以使用策略来更好地控制客户端设备映射的应用。 有关策略的详细信息，请参阅 eDocs 中的 XenDesktop 或 XenApp 文档。

### HDX Plug and Play USB 设备重定向

更新日期：2015/01/27

HDX Plug and Play USB 设备重定向实现了媒体设备（包括照相机、扫描仪、媒体播放器和 POS 设备）动态重定向到服务器。 您或用户可以限制所有设备或一些设备进行重定向。 在服务器上编辑策略或在用户设备上应用组策略，来配置重定向设置。 有关详细信息，请参阅 XenApp 和 XenDesktop 文档中的 USB 和客户端驱动器注意事项。

重要：如果您在服务器策略中禁用了 Plug and Play USB 设备重定向，用户将无法覆盖该策略设置。
用户可以在 Receiver 中将权限设置为始终允许或拒绝设备重定向或者在每次设备连接时都进行提示。 此设置只影响在用户更改此设置之后插入的设备。

### 将客户端 COM 端口映射到服务器 COM 端口

通过客户端 COM 端口映射，在会话期间将可以使用与用户设备 COM 端口连接的设备。 可以像使用任何其他网络映射那样使用这些映射。

可以在命令提示窗口中映射客户端 COM 端口。 也可以利用远程桌面（终端服务）配置工具或使用策略来控制客户端 COM 端口映射。 有关策略的信息，请参阅 XenDesktop 或 XenApp 文档。

重要：COM 端口映射与 TAPI 不兼容。 TAPI 设备不能映射到客户端 COM 端口。
1. 对于 XenDesktop 7 部署，请启用客户端 COM 端口重定向策略设置。

2. 登录 Receiver。
3. 在命令提示符处，键入：

   net use comx:\\client\comz:。

   其中，x 是服务器上的 COM 端口号（端口 1 到 9 可用于映射），z 是要映射的客户端 COM 端口号。

4. 要确认该操作，请在命令提示窗口中键入：

   net use

   。 显示的列表中将包含映射的驱动器、LPT 端口和映射的 COM 端口。

   要在虚拟桌面或应用程序中使用此 COM 端口，请将您的设备安装到映射的端口。 例如，如果将客户端上的 COM1 映射到服务器上的 COM5，请在会话期间将您的 COM 端口设备安装到 COM5。 使用此映射 COM 端口时，就如同在使用客户端设备上的 COM 端口一样。

# 支持 DNS 名称解析

Feb 02, 2016

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

Feb 02, 2016

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

Feb 02, 2016

可以通过以下功能提升用户的体验：

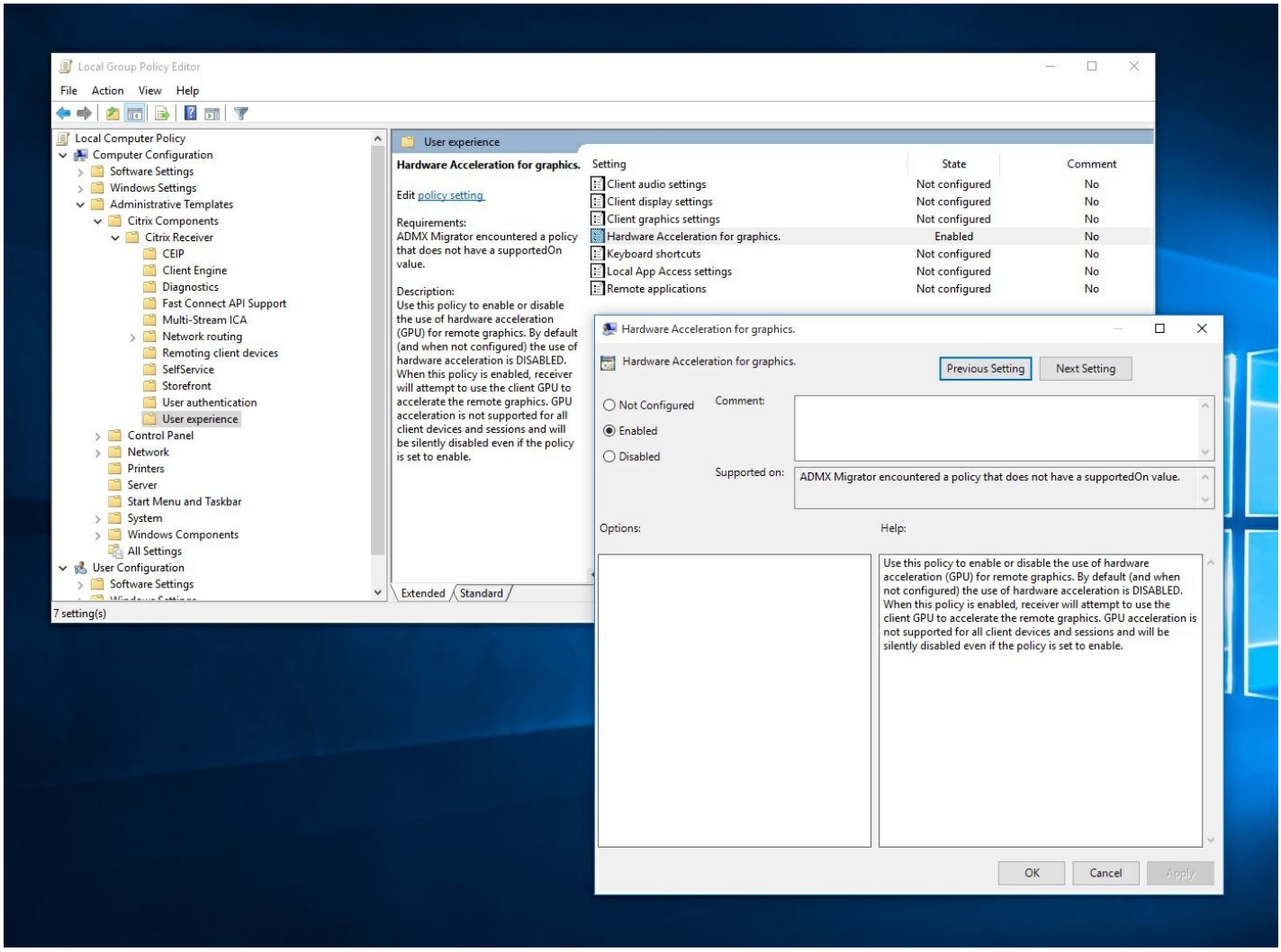
使用 Citrix Receiver for Windows 4.4（以及 HDX Engine 14.4）时，只要在客户端可用，即可使用 GPU 进行 H.264 解码。 用于 GPU 解码的 API 层为 DXVA（DirectX 视频加速）。

有关详细信息，请参阅博客 Improved User Experience: Hardware Decoding for Citrix Windows Receiver（改进的用户体验：适用于 Citrix Windows Receiver 的硬件解码）。

> **注意**
>
> 默认情况下，硬件解码功能处于关闭状态；可以通过客户端策略启用。

要启用硬件解码，请执行以下操作：

1. 将 receiver.adml 从 root\Citrix\ICA Client\Configuration\en 复制到 C:\Windows\PolicyDefinitions\en-US。
2. 将 receiver.admx 从 root\Citrix\ICA Client\Configuration 复制到 C:\Windows\PolicyDefinitions\。
3. 导航到**本地组策略编辑器**。
4. 在“计算机配置”->“管理模板”->“Citrix Receiver”->“用户体验”下，打开 **Hardware Acceleration for graphics**（图形硬件加速）。
5. 选择**已启用**，然后单击**确定**。




要验证是否已应用该策略以及是否正在对活动 ICA 会话使用硬件加速，请查找以下注册表项：

注册表路径：HKCU\Software\Citrix\ICA Client\CEIP\Data\GfxRender\<会话 ID>

> ## 提示
>
> **Graphics_GfxRender_Decoder** 和 **Graphics_GfxRender_Renderer** 的值应为 2。 如果值为 1，则表示正在使用基于 CPU 的解码。

使用硬件解码功能时，请注意以下限制：

- 如果客户端配备了两个 GPU，并且其中一个监视器在第二个 GPU 上处于活动状态，则将使用 CPU 解码。
- 连接到 Windows Server 2008 R2 上运行的 XenApp 7.x 服务器时，Citrix 建议您不要在用户的 Windows 设备上使用硬件解码。 如果启用了此功能，则会出现突出显示文本过程中性能缓慢等问题以及闪烁不定问题。

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。

更新日期：2014/11/28

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。

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。

您可以更改用户启动会话时状态指示器显示的时间长度。 要更改超时期限，请在 HKLM\SOFTWARE\Citrix\ICA CLIENT\Engine\ 中创建 REG_DWORD 值 SI INACTIVE MS。 如果希望状态指示器尽快消失，可以将 REG_DWORD 值设置为 4。

**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。**

# 确保连接安全

Feb 02, 2016

为了最大限度地提高环境的安全性，必须保障 Citrix Receiver 与您所发布的资源之间的连接安全。 可以为 Citrix 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

Feb 02, 2016

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 Citrix 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 Citrix Receiver 的任何域客户端计算机。

安装 Citrix Receiver 时，可以通过两种方式启用域直通 (SSON) 身份验证：

- 使用命令行安装
- 使用图形用户界面

## 使用命令行界面启用域直通身份验证

使用命令行界面启用域直通 (SSON) 身份验证

1. 使用 **/includeSSON** 开关安装 Citrix Receiver 4.x。
   - 安装一个或多个 StoreFront 应用商店（可以在以后的阶段完成此步骤）；安装 StoreFront 应用商店不是设置域直通身份验证的必备条件。
   - 通过启动 Citrix Receiver 确认已启用直通身份验证，然后在重新启动安装了 Citrix Receiver 的端点设备后确认 ssonsvr.exe 进程正在任务管理器中运行。

> **注意**
>
> 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。

## 使用图形用户界面启用域直通身份验证

要使用图形用户界面启用域直通身份验证，请执行以下操作：

1. 找到 Citrix Receiver 安装文件 (CitrixReceiver.exe)。
2. 双击 **CitrixReceiver.exe** 启动安装程序。
3. 在“启用单点登录”安装向导中，选中“启用单点登录”复选框以安装启用了 SSON 功能的 Citrix Receiver；这等同于使用命令行开关 **/includeSSON** 安装 Citrix Receiver。

下图说明了如何启用单点登录：


> ## 注意
>
> “启用单点登录”安装向导仅适用于在加入域的计算机上执行的全新安装。

通过启动 Citrix Receiver 确认已启用直通身份验证，然后在重新启动安装了 Citrix Receiver 的端点设备后确认 **ssonsvr.exe** 进程正在任务管理器中运行。

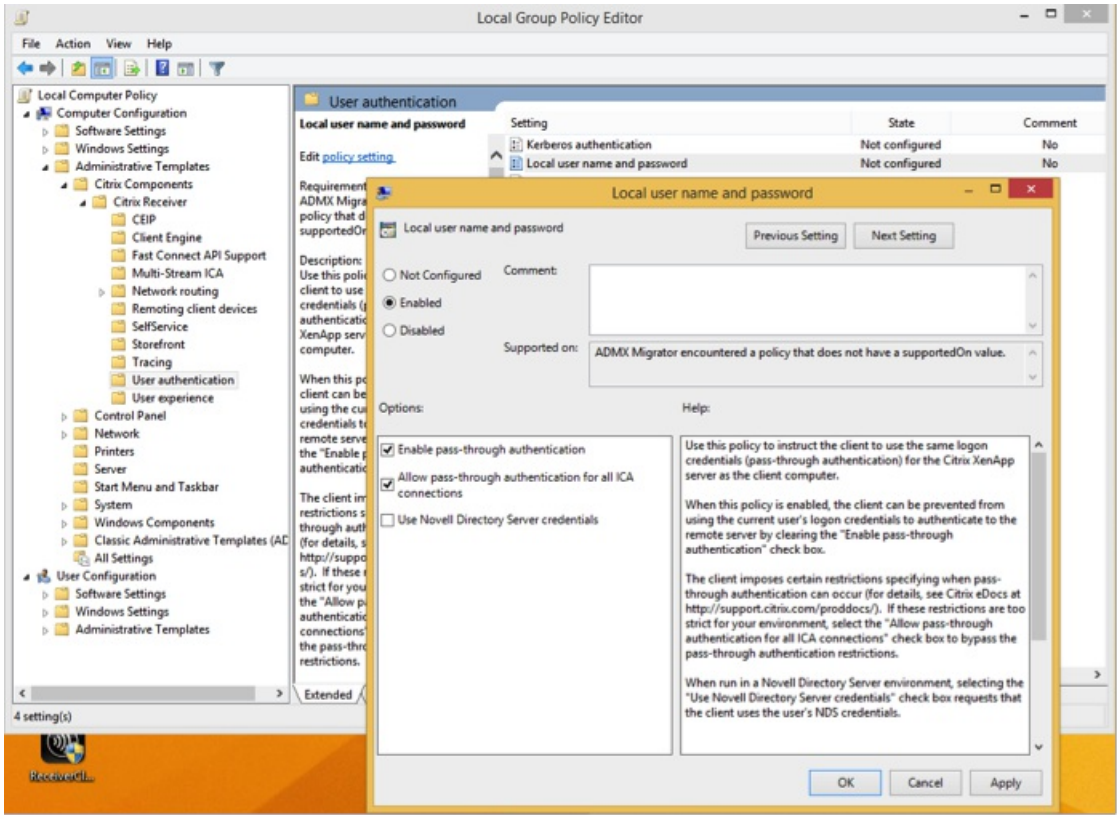
请根据本部分中的信息配置 SSON 身份验证的组策略设置。

> ## 注意
>
> 与 SSON 有关的 GPO 策略设置的默认值为**启用直通身份验证**，并且此默认值足以使 SSON 正常运行。 请按照下面的过程修改此设置。

## 为 SSON 组策略使用 ADMX 文件

请按照以下过程使用 ADMX 文件配置组策略设置：

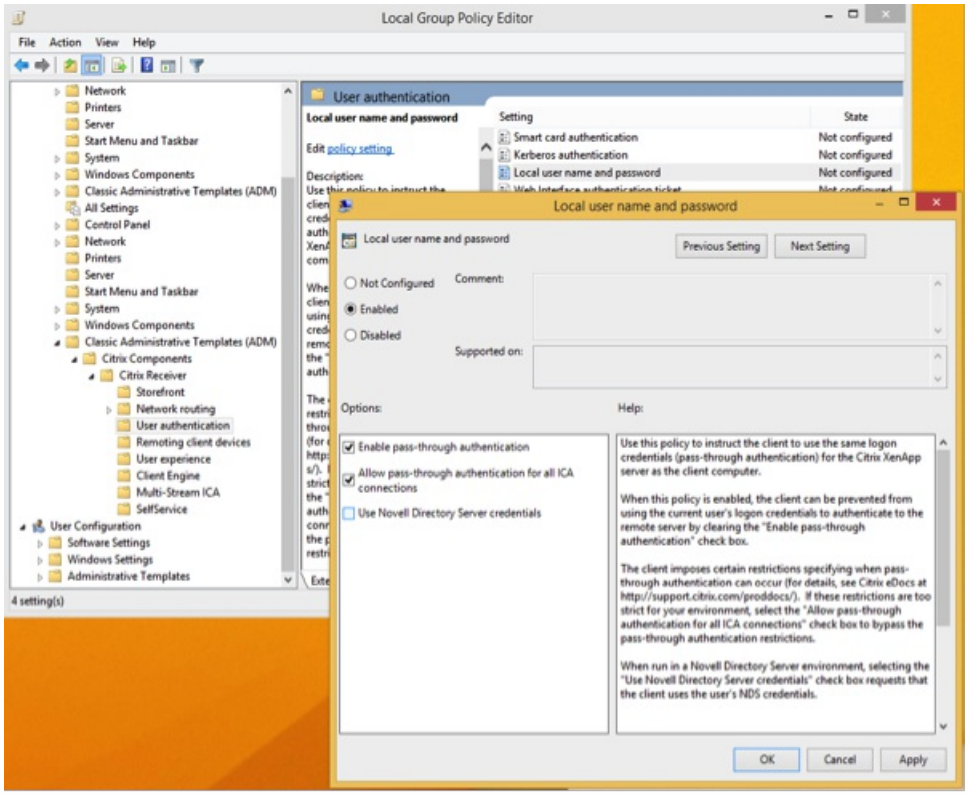
1. 加载组策略文件。 对于使用 Citrix Receiver 4.3 及更高版本的安装，请使用 %SystemDrive%\Program Files (x86)\Citrix\ICA Client\Configuration 文件夹中的 **Receiver.ADMX** 或 **Receiver.ADML** 文件。
2. 打开 **gpedit.msc**，右键单击**计算机配置 > 管理模板 - > Citrix 组件 -> Citrix Receiver -> 用户身份验证**。
3. 启用以下本地计算机 GPO 设置（在用户的本地计算机上和/或 VDA 桌面黄金映像中）：
   - 选择本地用户名和密码。
   - 选择**已启用**。
   - 选择**启用直通身份验证**。
4. 重新启动端点设备（其上安装了 Citrix Receiver）或 VDA 桌面黄金映像。




# 为 SSON 组策略使用 ADM 文件

请按照以下过程使用 ADM 文件配置组策略设置：

1. 通过选择**计算机配置 > 右键单击“管理模板”> 选择“添加/删除模板”**打开本地组策略编辑器。
2. 单击**添加**添加 ADM 模板。
3. 成功添加 **receiver.adm** 模板后，依次展开**计算机配置 > 管理模板 > 经典管理模板(ADM) > Citrix 组件 > Citrix Receiver > 用户身份验证**。




4. 在本地计算机上和/或 VDA 桌面黄金映像中打开 Internet Explorer。

5. 在 **Internet 设置 > 安全 > 可信站点**中，将 StoreFront 服务器的完全限定域名 (FQDN)（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**中找到此列表。

6. 注销并重新登录 Citrix Receiver 端点。

Citrix Receiver 打开时，如果当前用户已登录到域，用户的凭据以及枚举的 Citrix Receiver 内部的应用程序和桌面（包括用户的“开始”菜单设置）将传递到 StoreFront。 用户单击某个图标时，Citrix Receiver 会将用户的域凭据传递到 Delivery Controller，此时将打开应用程序（或桌面）。

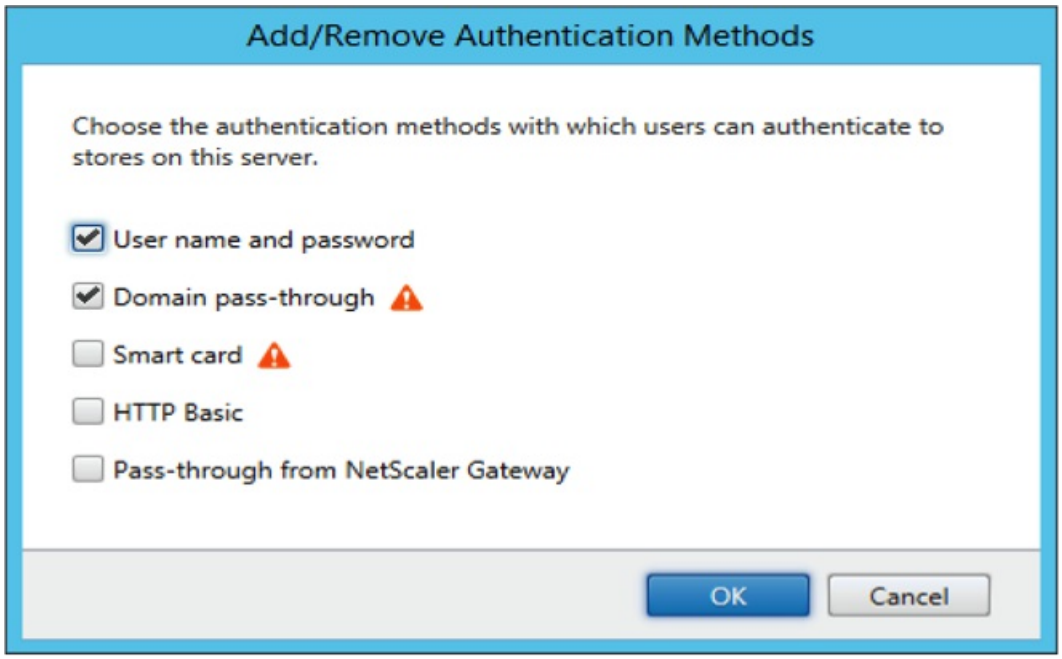
按照以下过程在 StoreFront 和 Web Interface 上配置 SSON

1. 以管理员身份登录 Delivery Controller。
2. 打开 Windows PowerShell（通过管理员权限）。 通过 PowerShell，您可以发出允许 Delivery Controller 信任发自 StoreFront 的 XML 请求的命令。
3. 如果尚未加载，请通过键入 **Add-PSSapin Citrix*** 加载 Citrix cmdlet 并按 **Enter** 键。
4. 按 Enter 键。

5. 键入 Add-PSSnapin citrix.broker.admin.v2 并按 Enter 键。
6. 键入 Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $True 并按 Enter 键。
7. 关闭 PowerShell。

## StoreFront 配置

要在 StoreFront 和 Web Ingterface 上配置 SSON，请在 StoreFront 服务器上打开 Studio，然后选择**身份验证 -> 添加/删除方法**。 选择**域直通**。




## Web Interface 配置

要在 Web Interface 上配置 SSON，请选择 **Citrix Web Interface 管理 -> XenApp Sevices 站点 -> 管理方法**并启用**直通**。

FastConnect API 使用 HTTP 基本身份验证方法，该方法经常与域直通、Kerberos 和 IWA 的关联身份验证方法混淆。 Citrix 建议您在 StoreFront 上以及 ICA 组策略中禁用 IWA。

# 使用 Kerberos 配置域直通身份验证

Feb 02, 2016

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

Citrix 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 Citrix 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 Citrix 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，Citrix Receiver 按如下方式使用 Kerberos 处理直通身份验证：

1. Citrix Receiver Single Sign-On Service 捕获智能卡 PIN。
2. Citrix 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 Citrix 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 Citrix 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。

FastConnect API 使用 HTTP 基本身份验证方法，该方法经常与域直通、Kerberos 和 IWA 的关联身份验证方法混淆。 Citrix 建议您在 StoreFront 上以及 ICA 组策略中禁用 IWA。

# 配置智能卡身份验证

Feb 02, 2016

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

Feb 02, 2016

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 Citrix 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 Citrix 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 Citrix 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

Feb 02, 2016

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

- Citrix NetScaler Gateway (Access Gateway)。 有关信息，请参阅本部分中的主题以及 NetScaler 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。）

Citrix 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。 这些模板在各种 Windows 平台上受支持。 有关这些模板和相关设置的详细信息，请参阅 https://technet.microsoft.com/zh-cn/ 上的 Windows 安全指南。

# 使用 NetScaler Gateway 进行连接

Feb 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。

> **注意**
>
> NetScaler Gateway End Point Analysis Plugin (EPA) 不支持本机 Windows Receiver。

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 NetScaler Gateway Enterprise Edition 进行连接

Aug 23, 2016

要使远程用户能够通过 NetScaler Gateway 进行连接，请将 NetScaler 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 NetScaler Gateway 插件连接。

有关配置上述连接的信息，请参阅 Citrix 产品文档站点上的 Integrating NetScaler Gateway with CloudGateway（将 NetScaler Gateway 与 CloudGateway 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 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

Feb 02, 2016

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

Feb 02, 2016

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

Feb 02, 2016

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

Feb 02, 2016

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

Feb 02, 2016

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 02, 2016

本主题仅适用于 XenDesktop 7.6 或更高版本或者 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。

本主题仅适用于 XenDesktop 7.6 或更高版本或者 XenApp 7.5。

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。

**用户设备要求**

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。

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，选择属性，选择已启用，然后在允许的 SSL 服务器文本框中按以下格式键入新端口号：server:SSL Relay 端口号，其中 SSL Relay 端口号是侦听端口的端口号。 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，选择属性，选择已启用，然后在允许的 SSL 服务器文本框中按以下格式键入以逗号分隔的可信服务器和新端口列表：servername:SSL Relay 端口号，servername:SSL Relay 端口号，其中 SSL Relay 端口号是侦听端口的端口号。 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：
   SSLProxyHost=csghq.Test.com:443

   [Excel]
   SSLProxyHost=csghq.Test.com:444

   [Notepad]
   SSLProxyHost=fred.Test.com:443

# 为 TLS 配置并启用 Receiver

Nov 02, 2016

本主题仅适用于 XenDesktop 7.6 或更高版本或者 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 Citrix 产品文档中的 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

Feb 02, 2016

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

Feb 02, 2016

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

Mar 08, 2016

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**
>
> 由于近期 Citrix 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。

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 |

Citrix Receiver 枚举应用程序并与 StoreFront 通信过程中，将使用 Windows 平台加密。

对于 Citrix Receiver 与 XenApp/XenDesktop 之间的 TCP 连接，Citrix Receiver 支持 TLS 1.0、1.1 和 1.2 以及以下密码集：

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256

对于基于 UDP 的连接，Citrix Receiver 支持 DTLS 1.0 以及以下密码集：

- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

## 启用 SP 800-52 合规模式

“计算机配置”- >“管理模板”->“Citrix 组件”- >“网络路由”->“TLS and Compliance Mode Configuration”（TLS 和合规模式配置）下引入了一个新复选框，称为 **Enable FIPS**（启用 FIPS）。 此选项可确保只能对所有 ICA 连接使用 FIPS 批准的加密。 默认情况下，此选项处于禁用状态或未选中。

引入了新的安全合规模式，称为 SP 800-52。 默认情况下，此选项设置为“NONE”（无），并且未启用。 请按照描述 NIST SP 800-52 要求的合规性的链接进行操作：http://www.nist.gov/manuscript-publication-search.cfm?pub_id=915295。

> ### 注意
>
> SP800-52 合规模式要求 FIPS 合规。 启用了 SP800-52 时，无论 FIPS 设置为何，都会启用 FIPS 模式。 允许的“Certificate Revocation Check policy”（证书吊销检查策略）值为“Full access check and CRL required”（需要执行完全访问权限检查和 CRL）或“Full access check and CRL required all”（全部需要执行完全访问权限检查和 CRL）。

## 限制 TLS 版本和密码集

可以将 Citrix Receiver 配置为限制 TLS 版本和密码集。 提供了一个选择允许使用的 TLS 协议版本的选项，这样可确定适用于 ICA 连接的 TLS 协议。 应选择同时适用于客户端和服务器的最高 TLS 版本。 选项包括：

- TLS 1.0 | TLS 1.1 | TLS 1.2（默认）。
- TLS 1.1 | TLS 1.2
- TLS 1.2

提供了一个用于选择 TLS 密码集的选项。 Citrix Receiver 可以选择以下选项：

- 任意
- 商用
- 政府

**商用密码集**

- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5

**政府密码集**

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

> ### 注意
>
> 如果启用了 **Require TLS for all connections**（要求对所有连接使用 TLS），发送至 StoreFront 的连接请求还必须使用 HTTPS；以 HTTP 格式添加应用商店失败，并且无法启动非 SSL VDA（XenDesktop 和 XenApp）。

# Receiver Desktop Lock

Aug 25, 2016

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。

Citrix Receiver Desktop Lock 在加入了域的计算机上运行，该计算机启用了 SSON (Single Sign-On) 并配置了应用商店；还可以在未加入域并且未启用 SSON 的计算机上使用 Citrix Receiver Desktop Lock。 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/admx 文件或 cmdline 选项配置应用商店和 Single Sign-On。 有关详细信息，请参阅使用命令行安装和配置 Citrix Receiver。

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 7（包括 Embedded Edition）、Windows 7 Thin PC、Windows 8 和 Windows 8.1 上受支持。
- 用户设备必须连接到局域网 (LAN) 或广域网 (WAN)。

**本地应用程序访问**

> **Important**
>
> 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。 有关详细信息，请参阅 XenApp 和 XenDesktop 中的配置本地应用程序访问和 URL 重定向。

**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）。
   例如：
   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 Receiver.admx（或 Receiver.adml）和 Receiver_usb.admx (.adml) 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(ADMX)”>“Citrix 组件”中）。 .admx 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 Receiver.admx 模板。
   2. 依次展开“管理模板”>“经典管理模板(ADMX)”>“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。