Citrix Receiver for Windows 4.9 LTSR

Contents

4.9 LTSR 中的新增功能

April 4, 2019

关于 Citrix Receiver 的重要更新

Citrix Cloud TLS 版本弃用

为了提高与 Citrix Cloud 的连接的安全性，Citrix 将自 2019 年 3 月 15 日起阻止通过传输层安全性 (TLS) 1.0 和 1.1 进行的任何通信。但是，此弃用不影响进行 Citrix Receiver for Windows 4.9 LTSR 跟踪的客户的用户。有关详细信息，请参阅 Citrix Cloud TLS 版本弃用。

累积更新 6 现已可用

面向 Citrix Receiver for Windows 4.9 LTSR 的累积更新 6 (CU6) 已于 2019 年 3 月 19 日发布。CU6 中包含面向客户报告的问题的十个修复，将继续增加此 LTSR 的稳定性和易用性。在 Citrix Receiver for Windows 4.9 的基础之上构建的 CU6 中还包含来自 CU5 和 CU4 的 12 个以上的修复、来自 CU3 的超过 20 个修复、来自 CU2 的超过 18 个修复以及来自 CU1 的超过 15 个修复。CU6 可从 Citrix 下载页面下载。

减小了安装程序的大小

在本版本中，Citrix Receiver for Windows 安装程序的大小减小到 39.9 MB。与早期版本相比，大小降低了 15%。

StoreFront 帐户的新外部信标

在 StoreFront 帐户中，ping.citrix.com 用作 www.citrix.com 外部信标的替换选项。

自 Citrix Receiver for Windows 4.9 起，不需要任何用户可配置的更改。

如果使用的是早期版本的 Citrix Receiver for Windows，Citrix 建议您将 www.citrix.com 外部信标替换为 ping.citrix.com。

有关外部信标的详细信息，请参阅知识中心文章 CTX218708。

有关在 StoreFront 上配置外部信标的信息，请参阅配置信标点。

> 注意
>
> 如果未在 StoreFront 帐户上将 www.citrix.com 配置为外部信标，则请忽略。

已修复的问题

May 23, 2019

Citrix Receiver for Windows 4.9 LTSR CU6 修补程序 1 (4.9.6001)

比较对象：Citrix Receiver for Windows 4.9 LTSR CU6

安全问题

- 此修复解决了安全问题。有关详细信息，请参阅知识中心文章 CTX251986。[LD1518]

Citrix Receiver for Windows 4.9 LTSR CU6

比较对象：Citrix Receiver for Windows 4.9 LTSR CU5

HDX MediaStream Windows Media 重定向

- Windows Media 重定向客户端内容提取可能会失败。播放包含从实时 Web 流存档的脚本流的多媒体文件时会出现此问题。[LC7948]

安装、卸载、升级

- 将 Citrix Receiver for Windows 升级到版本 4.9 LTSR 后，可能不会预留自定义虚拟通道所需的注册表项。[LD0633]

键盘

- 启用了本地 **IME** 或本地键盘布局同步的情况下，按下包含右侧 Ctrl 键和右侧 Shift 键的组合键时，Shift 键可能会卡在按下的位置。[LD0585]
- 选择了是，我更喜欢使用本地键盘布局，而不是远程服务器提供的键盘布局选项的情况下，最后一个输入字符可能无法正确处理。通过单击右侧 Alt 键从韩语切换到英语时会出现此问题。请注意，应用此修复后，当您使用鼠标时，此问题可能会持续存在。[LD0825]

会话/连接

- 使用某些第三方应用程序时，主机到客户端重定向可能不起作用。这些应用程序使用包含 HTTPS 和 HTTP 地址的特殊 Web URL 时会出现此问题。[LD0484]
- 配置应用程序延迟后，已发布的应用程序可能无法在会话断开连接后重新打开现有文件。[LD0742]
- 您使用 Windows 7 基本主题，并且在用户设备上禁用了硬件加速（GDI 模式）。在本地应用程序与已发布的无缝应用程序之间切换时，可能会遇到显示问题。[LD0853]
- 在 VDA 上使用 NVIDIA GPU 并优化 GPU 中最新的 NvENC 时，h.264 DXVA 解码可能会损坏。

  要启用此修复，请设置以下注册表项：

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\GfxRender

  名称：MaxNumRefFrames

  类型：DWORD

  值：介于 2 和 8 之间 [LD0943]

用户体验

- 最大化非无缝应用程序窗口时，应用程序窗口会损坏。[LD0755]
- 启动已发布的 Windows 7 桌面时，在 Citrix Receiver for Windows 会话中拖动鼠标光标时可能会出现滞后。[LD0923]

Citrix Receiver for Windows 4.9 LTSR CU5

比较对象：Citrix Receiver for Windows 4.9 LTSR CU4

内容重定向

- 如果在首次启动启用了文件类型关联的扩展时取消默认程序窗口，可能会针对此扩展的后续启动显示以下错误消息：

  Windows 无法访问指定设备、路径或文件。您可能没有适当的权限访问该项目。 [LD0026]

键盘

- 使用条形码读卡器时，如果发送大量数据，某些数据可能会丢失。[LD0243]

会话/连接

- 将 Citrix Receiver for Windows 升级到版本 4.9.1000 后，CDViewer 可能会在注销时显示灰屏。[LC9290]
- 尝试启动应用程序可能会失败并显示以下错误消息：

  Unable to launch your application. Contact your help desk and provide them with the following information: Cannot open the Citrix Receiver.（无法启动您的应用程序。请联系技术支持人员并向其提供以下信息: 无法打开 Citrix Receiver。）

  - 要启用此修复，管理员必须设置以下注册表项：

    HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client\Engine

    名称：EngineTimeout

    类型：DWORD

    值：超过 20 秒

  - 要启用此修复，用户必须设置以下注册表项：

    HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client\Engine

    名称：EngineTimeout

    类型：DWORD

    值：超过 20 秒，例如 EngineTimeout=20 [LC9771]

- 启动托管共享桌面中的多个应用程序。如果在多个客户端之间切换，或执行断开连接或重新连接操作，则可能会显示以下错误消息：

  Citrix HDX Engine has stopped working.（Citrix HDX Engine 已停止运行。）
  Exception caused the program to stop working correctly. Please close the program.（**Citrix HDX Engine** 已停止工作异常导致该程序停止正常运行。请关闭该程序。） [LC9772]

- 使用 Citrix Receiver for Windows 启动的应用程序可能会被镜像到辅助显示器中。[LC9893]
- 当最小化无缝应用程序时，它将显示为该应用程序的微型版本。实际上，它必须看似最小化窗口或必须显示在任务栏上。[LD0034]
- 将 NVIDIA 图形卡与 GPU 结合使用时，某些第三方应用程序的已发布实例可能会作为透明应用程序打开。[LD0175]
- 从“控制面板”图标创建的本地应用程序快捷方式无法通过从 Citrix Studio 中配置的 **KEYWORDS:Prefer** 进行启动。[LD0288]
- 当您尝试使用组策略对象 (GPO) 管理模板添加第二个应用商店时，第二个应用商店中的信标和其他信息可能会丢失。[LD0413]

系统异常

- 启用双向内容重定向策略后，如果尝试在本地 Web 浏览器中打开 Web 页面，则 Redirector.exe 进程可能会意外退出。因此，双向内容重定向不起作用并显示以下错误消息：

  Citrix FTA, URL Redirector stopped working.（Citrix FTA、URL 重定向程序停止运行。）[LD0420]

- wfica32.exe 进程可能会意外退出。当配置了代理设置且尝试在 Citrix Receiver for Web 中启动新会话时会发生此问题。[LD0548]

用户界面

- 单击鼠标可能不会对远程会话做出响应。从 Desktop Viewer 工具栏打开首选项窗口并将 **MouseTimer** 设置配置为除默认值以外的任何值时，可能会发生此问题。[LD0260]
- 当您选择重置 **Receiver** 选项时，Citrix Receiver for Windows 可能会要求您在 Microsoft Windows 10 上安装.Net Framework 3.5。[LD0690]

Citrix Receiver for Windows 4.9 LTSR CU4

比较对象：Citrix Receiver for Windows 4.9 LTSR CU3

客户端设备问题

- 使用设置为“已启用”的自动显示键盘策略时，软键盘可能不会在会话中自动弹出。[LC9925]

HDX MediaStream Windows Media 重定向

- 包含嵌入式脚本的重定向多播流可能无法从客户端提取内容。视频所在位置会显示黑色屏幕。[LC9775]

键盘

- 在引入此修复之前，Bloomberg 型号 4 Starboard 键盘仅支持 PC 模式。应用此修复后，Bloomberg 型号 4 Starboard 键盘支持 PC 和 KVM 模式。[LC9984]

登录/身份验证

- 使用 Citrix Receiver for Windows 添加帐户时，键入应用商店 URL 可能会导致显示以下错误消息：无法联系身份验证服务。StoreFront URL 以文本字符串 `citrix.com` 开头时会出现此问题。[LC9631]

会话/连接

- 使用从 Citrix Studio 中配置的 KEYWORDS:Prefer 时，可能不支持命令行开关或本地用户设备上的应用程序快捷方式中提及的参数。[LD0060]
- 此修复执行以下更改：
  - 当您自定义 edtMSS 和 OutBufLength 时，edtMSS 将覆盖 OutBufLength。
  - 将 All_regions.ini 、defaulit.ica 文件和注册表中的参数名称从 udt* 更改为 edt*。

  注意：
  以管理员身份进行升级后，注册表项 HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\UDT 下的用户注册表项和条目不会从 udt* 重命名为 edt*。此外，也不会保留参数值。[LD0098]
- 即使在组策略对象 (GPO) 中更新或删除应用商店，可能也不会删除通过 GPO 添加的应用商店。[LD0147]

系统异常

- 登录应用商店时，Citrix Receiver for Windows 可能会意外退出。[LC8271]
- 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）。

  图形模块中存在陷阱时会出现此问题。[LC9466]
- 注销系统时，wfica32.exe 进程可能会意外退出。[LC9892]

TWAIN

- Citrix Receiver for Windows 4.7 或更高版本可能无法重定向扫描仪。用户设备上没有 Twain 2.0 驱动程序时会出现此问题。[LC8215]

用户体验

- 使用某些第三方应用程序建立 VPN 连接时，Citrix Receiver for Windows 可能会处于不可用状态大约 15 分钟。[LC9302]
- 从 Citrix Receiver for Windows 连接到 Linux VDA 7.17 或更高版本时，Citrix HDX Engine 的 GPU 使用率可能会很高。[LC9506]
- 在处于无缝模式的应用程序中使用日语输入法编辑器 (IME) 并输入文本时，可能无法显示文本。文本的字体大小较小时会出现该问题。

  要启用此修复，请设置以下注册表项：

- 在 *32* 位系统中：

  HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client

  名称：DisableD3DRenderWidthHeightCheck

  类型：REG_DWORD

  值：1

- 在 *64* 位系统上：

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow 6432Node\Citrix\ICA Client

  名称：DisableD3DRenderWidthHeightCheck

  类型：REG_DWORD

  值：1 [LC9882]

用户界面

- 验证 Single Sign-on 配置的配置检查器可能无法完成验证过程，并在验证 Single Sign-on 过程中卡住。[LC9625]

Citrix Receiver for Windows 4.9 LTSR CU3

比较对象：Citrix Receiver for Windows 4.9 LTSR CU2

客户端设备问题

- 某些 DVD 视频可能会在会话中通过映射的客户端驱动器播放。[LC8912]

内容重定向

- 将双向内容重定向到 VDA 时，如果浏览器已打开，第二个 URL 将在新浏览器中打开。[LC9157]
- 将 Citrix Receiver for Windows 与 Citrix XenApp Services 站点结合使用时，应用程序和图标可能会部分与文件类型相关联。[LC9402]

安装、卸载、升级

- 通过 System Center Configuration Manager (SCCM) 升级 Citrix Receiver for Windows 时，Receiver for Windows 可能会请求重新启动系统。[LC9706]

键盘

- 尝试通过从 StoreFront 下载的 APPSRV.INI 或 ICA 文件使用服务器默认值或所需的键盘布局可能会失败。

  在这种情况下的限制如下：

  - 首次配置时，必须通过控制面板在会话中手动设置键盘布局，即使以前设置了键盘布局亦如此。
  - 必须将高级首选项中的键盘布局同步设置为否。如果将布局设置为是，则将重定向本地 IME。[LC9593]

登录/身份验证

- AuthManSvr.exe 进程重新启动后，尝试从 Citrix Receiver for Windows 注销失败。[LC7981]

打印

- 尝试使用 PDF 编写器作为打印首选项打印大型文档时，打印机可能会变得无响应，或者可能会显示以下错误消息：

  “Emf viewer has stopped working.”（Emf 查看器已停止工作。）[LC8882]

会话/连接

- 启动桌面后，桌面可能会立即消失。从 Citrix Receiver for Windows 发送的重复 TLS 数据包会导致出现此问题。[LC8724]
- 尝试使用 Microsoft Internet Explorer 11 启动桌面时，可能会显示以下错误消息：

  “连接到失败，状态为 (未知客户端错误 0)”[LC8841]
- 在 StoreFront 中设置两个站点之间的聚合时，不会创建预启动会话。[LC8847]
- 在双跃点场景中，如果 VDA for Desktop OS 在第一个跃点中，应用程序在 VDA 中启动的第二个跃点中，则重新连接到运行 VDA for Desktop OS 的第一个跃点时，屏幕可能会在几秒钟内闪烁不定。[LC9071]
- 尝试使用 Citrix Receiver for Windows 启动桌面可能会在短暂的时间后超时并失败。即使通过 StoreFront 设置 **LaunchTimeoutMs** 增加启动超时值后也会出现此问题。[LC9369]
- 更改 StoreFront 中的内部信标点后，在重新启动 Citrix Receiver 之前可能无法从 Citrix Receiver for Windows 启动应用程序。[LC9442]
- 在多个已发布的应用程序之间使用 Win+Tab 或 Alt+Tab 键切换时，GDI 对象可能会在客户端上增加，直到应用程序变得无响应并显示黑色像素。[LC9655]

智能卡

- 尝试在全屏模式下使用智能卡身份验证启动已发布的桌面时，PIN 提示窗口可能不会在 Desktop Viewer 中显示。[LC8579]

系统异常

- 使用启用了触控功能的设备连接到 VDA 时，wfica32 进程可能会间歇性退出。[LC9228]
- wfica32.exe 进程可能会间歇性退出。[LC9397]

用户体验

- 即使未打开 Citrix Receiver for Windows 应用程序，其窗口也可能会自动显示。管理员在 Citrix Studio 中删除或禁用任何已发布的应用程序时会出现此问题。[LC8176]
- 刷新 Citrix receiver for Windows 内部的应用程序时，“开始” 菜单和任务栏图标可能会闪烁不定。[LC8890]
- 在 Citrix Receiver for Windows 会话中，鼠标光标丢失或显示地非常小。在 Microsoft Windows 10 中运行的端点上使用具有不同 DPI 的多个显示器时可能会出现此问题。[LC8915]
- 在 Citrix Receiver for Windows 会话中，鼠标光标可能会显示为小于常规大小。在运行 Microsoft Windows 10 版本 1607 及更高版本的端点上使用高分辨率显示器时，可能会出现此问题。

  在这种情况下的限制如下：

  - 在反向无缝模式下单击鼠标左键时，鼠标指针变小。释放单击时，鼠标指针将变得正常。
  - 在 VDA for Desktop OS 和 VDA for Server OS 上运行 Windows 10 版本 1607 和 Windows Server 2016 之前的版本时，鼠标指针将略微放大，但分辨率较低。
  - 在多显示器场景中，当显示器的 DPI 不同时，鼠标指针将无法正确缩放。窗口在多个显示器之间移动时将出现此问题，可以通过调整应用程序窗口大小进行更正。
  - 在已启动的桌面上的 Desktop Viewer 中，鼠标指针仍显示为很小。[LC9221]
- 此修复解决了 Enlightened Data Transport (EDT) 的次要性能和质量改进问题。[LC9417]

Citrix Receiver for Windows 4.9 LTSR CU2

比较对象：Citrix Receiver for Windows 4.9 LTSR CU1

客户端设备问题

- IP 语音 (VOIP) 通话过程中，如果 user1 启动了一个已发布的声音录制器应用程序并开始录制，来自 user1 的麦克风音频在通话中将不再被听到。user1 可以听到 user2 的声音。[LC8713]

HDX MediaStream Flash 重定向

- 在启用了 “HDX MediaStream Flash 重定向” 设置的情况下，断开会话连接时，PseudoContainer2.exe 进程可能会意外退出。[LC8802]

HDX MediaStream Windows Media 重定向

- 使用某些第三方应用程序发送消息时，可能会听不到通知警报。此修复改进了对播放一小段时间的声音的支持。[LC8468]

HDX 无缝本地应用程序

- 对启动过程中需要配置的任何 64 位应用程序使用本地应用程序访问功能 “**KEYWORDS:prefer=”*pattern*“**” 时，尝试启动应用程序可能会失败。[LC8580]

安装、卸载、升级

- 升级 Citrix Receiver for Windows 后，可能会删除自定义虚拟通道所需的某些注册表项。[LC8414]
- Citrix Receiver for Windows 自动更新安装后，可能不会保留自动更新安装命令行开关。因此，自动更新配置设置为默认选项。[LC9103]

会话/连接

- 尝试启动会话可能会失败并显示以下错误消息：

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

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

  注意： 修复 LC5338 适用于 StoreFront 3.0.4000、StoreFront 3.9 及更高版本。[LC5338]
- 在 VDA for Server OS 的第一个跃点上从 Citrix Receiver for Windows 中启动 selfservice.exe 进程时，断开第一个跃点的连接会导致某些第三方应用程序或 Windows 任务计划程序在断开第一个跃点的连接时运行 “SelfService.exe –disconnectapps” 以断开第二个跃点的连接。重新连接到第一个跃点时，将运行 “SelfService.exe –reconnectapps” 以在重新连接第一个跃点时重新连接到第二个跃点。在此场景中，Citrix Receiver for Windows 可能会在前台显示，而非在后台显示，并且重新连接的应用程序将在后台显示。[LC8224]

系统异常

- 使用移动 Receiver 虚拟通道时，wfica32 进程可能会间歇性退出。[LC8526]
- 使用 Bloomberg 键盘的生物特征身份验证时，用户会话可能会意外退出。[LC8766]
- 在通过 USB 重定向的会话内部使用 Bloomberg 键盘指纹扫描仪设备时，用户会话可能会意外退出。[LC8928]

用户体验

- 在输入法编辑器 (IME) 语言栏中使用自定义短语功能时，某些字符在用户会话中可能会随机被截断。[LC6155]
- 在桌面和任务栏中手动创建的流应用程序的快捷方式将被删除。[LC7500]
- 启动 Citrix Receiver for Windows 时，如果订阅的应用程序在 Receiver 自助服务窗口中包含 bpp=4 的图标，“开始” 菜单和桌面快捷方式可能会闪烁不定。[LC8480]
- 某些第三方应用程序尝试向启用了 HDX 无缝应用程序的会话发送大量字符时，可能仅会将少量字符发送到该应用程序，而非发送所有字符。[LC8560]
- 在 Windows 7 客户端计算机中在全屏模式下启动已发布的桌面时，播放重定向的 Flash 视频会导致设置为总在最前面的应用程序在 Desktop Viewer 窗口上显示。默认情况下，此修复处于禁用状态。

  要启用此修复，请设置以下注册表项：

  - 在 *32* 位系统中：

    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\XenDesktop\DesktopViewer

    名称：PreventAlwaysOnTopWindowPopover

    类型：DWORD

    值：2；要禁用该修复，请将该注册表项值设置为 0 或删除该注册表项。
  - 在 *64* 位系统上：

    HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\XenDesktop\DesktopViewer

    名称：PreventAlwaysOnTopWindowPopover

    类型：DWORD

    值：2；要禁用该修复，请将该注册表项值设置为 0 或删除该注册表项。[LC8616]
- 在 Citrix Receiver for Windows 中刷新应用程序时，手动固定到任务栏的 Microsoft Outlook 应用程序图标可能会消失。[LC8785]

用户界面

- 在 Citrix Receiver for Windows 中更改设置选项并在 StoreFront 中为应用商店配置禁用用户订阅 **(**强制性应用商店**)** 设置时，应用程序可能不会在 “开始” 菜单中显示。[LC8648]

Citrix Receiver for Windows 4.9 LTSR CU1

比较对象：Citrix Receiver for Windows 4.9 LTSR

客户端设备问题

- 无法使用连接到扩展坞或 USB 集线器的键盘、鼠标或显示器等设备。用户会话处于全屏模式或者会话窗口处于焦点中时，如果您在启动用户会话后将扩展坞或集线器连接到客户端计算机，则会出现此问题。[LC8295]

内容重定向

- 使用漫游配置文件登录到 Citrix Receiver for Windows 时，文件类型关联可能不起作用。[LC8042]

HDX RealTime

- 在 VDA 上安装了同一型号的多个网络摄像机时，只有最新的网络摄像机可能会被会话识别并映射。应用此修复后，可以在会话内部的任何视频会议应用程序中使用型号相同的多个网络摄像机。

  > 注意：
  >
  > – 安装修复 LC5008 后，您可能无法从“首选项”选项卡切换网络摄像机。
  > – 要启用此修复，必须同时安装包含修复 LC5008 的服务器和客户端修补程序。[LC5008]

会话/连接

- 尝试使用“运行方式”命令以与当前已登录的用户身份不同的用户身份启动 Microsoft Internet Explorer 时，如果 Redirector.exe 进程正在系统中运行，则浏览器可能会启动，但内容在大约 20-30 秒时间内无法加载。[LC5227]
- 尝试使用 Mozilla Firefox 启动桌面可能会失败。Desktop Viewer 无法从 Internet Explorer 的临时目录中删除以前创建的 ICA 文件时会出现此问题。这会导致出现阻止您在启动新会话时复制 ICA 文件的“访问被拒绝”错误。[LC7883]
- 从“开始”菜单或桌面快捷方式启动应用程序时，应用程序可能会启动，但会出现以下错误消息：

  “Cannot find this file, Please verify that the correct path and file name are given.”（找不到此文件，请确认是否指定了正确的路径和文件名。）[LC8253]
- 安装 Citrix Receiver for Windows 4.8 后，员工 Web 门户的某些功能可能无法正常运行。但是，在 Microsoft Internet Explorer 中禁用了 Citrix ICA 客户端 ActiveX 控件时，Web 站点将正确运行。[LC8428]

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）[LC8040]

- Citrix Receiver for Windows 4.8 可能会遇到致命异常，显示蓝屏。在系统中多次使用某些多功能键盘型号和即插即用键盘重新启动系统时会出现此问题。[LC8182]
- 播放音频文件过程中从用户设备中移除耳机后，会话可能会变得无响应，直至您断开并重新连接会话。[LC8243]
- 在已发布的无缝应用程序中使用键盘快捷方式 “Alt+Enter” 时，wfica32.exe 进程可能会意外退出。[LC8317]
- 在双跃点场景中，当您在客户端之间切换会话时，wfica32.exe 进程可能会意外退出。[LC8354]

用户体验

- 在音频质量设置为高的情况下录制声音时，声音录制件的质量可能会非常差。[LC8241]
- 在多显示器环境中将无缝窗口从全屏还原到其原始大小，然后跨显示器将其拖回以便查看整个应用程序时，窗口可能会被错误地裁剪。因此，只有一部分窗口可见。宽度超过显示器，因而部分在屏幕外部显示的无缝窗口会出现此问题。[LC8325]
- 在应用商店的 web.config 文件中配置快捷方式选项时，已发布的应用程序快捷方式可能会从 “开始” 菜单和桌面中消失。

  注意： 此修复提供面向修复 LC7577 的完整修复。[LC8391]

- 如果在使用 Epic Hyperspace 时在无缝模式下启动会话，该应用程序可能不允许在端点上本地运行的其他应用程序在前台显示。Epic Hyperspace 应用程序可能会保留前台焦点，直至您将其最小化。[LC8462]
- 连接到已发布的桌面时，空白区域可能会在调整窗口大小时发生变化的桌面上显示。使用旧图形模式时会出现此问题。[LC8518]

Citrix Receiver for Windows 4.9 LTSR

比较对象：Citrix Receiver for Windows 4.8

HDX 3D Pro

- 如果在 VDA 上启用了 HDX 3D Pro，使用某些第三方应用程序会导致 VDA 断开连接。

  要启用此修复，请设置以下注册表项：

  - 在 *32* 位 *Windows* 中：

    HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA

Client\Engine\Configuration\Advanced\Modules\Thinwire3.0

名称：Tw2IgnoreValidationErrors

类型：REG_SZ

值：TRUE

HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA

Client\Engine\Configuration\Advanced\Modules\Thinwire3.0

名称：Tw2IgnoreExecutionErrors

类型：REG_SZ

值：TRUE

- 在 *64* 位 *Windows* 上

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced

  名称：Tw2IgnoreValidationErrors

  类型：REG_SZ

  值：TRUE

  HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced

  名称：Tw2IgnoreExecutionErrors

  类型：REG_SZ

  值：TRUE [LC7655]

服务器/站点管理

- 用户密码过期时，“更改密码”输入表单可能会变为非交互。新密码不满足要求时会出现此问题。[LC7943]

会话/连接

- 按照知识中心文章 CTX128232 中所述的过程将桌面组分配到外部客户端 IP 地址时，如果通过 NetScaler Gateway 访问，已发布的应用桌面可能无法启动。此时可能会显示以下错误消息：

  无法启动应用程序 [LC5932]

- 通过 Juniper SSL VPN 连接时，Citrix Receiver for Windows 可能无法连接到 StoreFront。StoreFront URL 的 DNS 解析失败时会出现此问题。[LC6711]

- 断开与使用集成网络摄像机的 VDA 的连接时，Citrix Receiver for Windows 可能会意外退出。网络摄像机运行过程中断开与 VDA 的连接时会出现此问题。[LC6815]

- 如果启用了 Desktop Lock，StoreFront 会话过期时，用户会话可能会自动断开连接。[LC6984]
- 使用 Epic Hyperspace 软件进行医疗听写时，记录过程中用户设备上的听写记录器可能会变得无响应。[LC7435]
- 使用 Citrix ICA 客户端对象 API 通过 NetScaler 启动客户端会话并在组策略对象中配置“客户端选择性信任”时，会话可能无法启动。[LC7575]
- 在注册表项 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle（在 32 位 Windows 上）和 HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle（在 64 位 Windows 上）下，将注册表值 DisableStubCreation 设置为 true 时，文件类型关联可能无法打开关联的文档。注册表项 HKEY_CURRENT_USER\SOFTWARE\Classes\Dazzle 下的相关文件名扩展缺少%1 参数时会出现此问题。<*appname*>.<*extension*>.1\shell\open\command。[LC7619]
- 如果启用了本地应用程序访问，在全屏模式下启动的 VDA for Desktop OS 会话的大小和位置可能不正确。[LC7646]
- 通过组策略设置或命令行添加应用商店并配置在 Windows 登录时重新连接时，Citrix Receiver for Windows 在 Windows 登录时可能不会自动重新连接。[LC7679]
- 从睡眠模式还原后，客户端自动重新连接功能可能不起作用，阻止了会话重新连接。[LC7705]
- 如果启用了本地应用程序访问，wfcrun32.exe 进程可能会意外退出。[LC7946]

智能卡

- 如果在用户会话中设置了位于策略“交互式登录: 智能卡删除行为”下的本地安全性设置“锁定工作站”，从该会话中删除智能卡读卡器时，会话可能不会被锁定。[LC7571]
- 在用户会话中从服务器调用 SCardListReaderGroup API 时，Citrix Receiver for Windows 可能不会执行在客户端调用的 API。[LC7699]

用户体验

- 在设备的触摸屏上轻按两次对用户会话中的某些应用程序可能不起作用。[LC6698]
- 单击任务栏图标以在无缝会话中的第三方应用程序的窗口之间切换焦点时，第三方应用程序的相应窗口可能无法在前台显示。[LC6709]
- 如果在其中一个鼠标按钮处于按下状态时更改用户设备的分辨率，无缝应用程序可能无法接收该鼠标事件的鼠标释放状态。因此，鼠标捕获将丢失。[LC7419]
- 在应用商店的 web.config 文件中配置快捷方式选项时，已发布的应用程序快捷方式可能会从“开始”菜单和桌面中消失。[LC7577]
- 如果在使用 Epic Hyperspace 时在无缝模式下启动会话，该应用程序可能不允许在端点上本地运行的其他应用程序在前台显示。Epic Hyperspace 应用程序可能会保留前台焦点，直至将该应用程序最小化。[LC7906]

注意： 本版本的 Citrix Receiver for Windows 还包括版本 4.8、4.7、4.6、4.5、4.4、4.3、4.2、4.1 和 4.0 中的所有修复。

已知问题

March 26, 2019

Citrix Receiver for Windows 4.9 LTSR CU6 中的已知问题

在此版本中没有发现新问题。

Citrix Receiver for Windows 4.9 LTSR CU5 中的已知问题

在此版本中没有发现新问题。

Citrix Receiver for Windows 4.9 LTSR CU4 中的已知问题

在此版本中没有发现新问题。

Citrix Receiver for Windows 4.9 LTSR CU3 中的已知问题

在此版本中没有发现新问题。

Citrix Receiver for Windows 4.9 LTSR CU2 中的已知问题

在此版本中没有发现新问题。

Citrix Receiver for Windows 4.9 LTSR CU1 中的已知问题

Citrix Receiver for Windows 4.9 包含版本 4.5、4.6、4.7 和 4.8 中存在的部分已知问题，还包含以下已知问题：

- 在启用了 Framehawk 的情况下，当您频繁地尝试登录并注销时，wfica32.exe 进程可能会意外退出。[LCMRFWIN-704]

Citrix Receiver for Windows 4.9 中的已知问题

- 在 Surface Pro 上，如果在窗口模式下启动了桌面会话，则在桌面模式与平板电脑模式之间切换时，“Desktop Viewer” 选项将变得无响应。[RFWIN-5837]

第三方声明

November 19, 2018

Citrix Receiver for Windows 可能包含根据以下文档中定义的条款进行许可的第三方软件：

Citrix Receiver for Windows 第三方声明（**PDF** 下载）

系统要求和兼容性

February 1, 2019

要求

- 本版本的 Citrix Receiver for Windows 至少需要 500 MB 可用磁盘空间和 1 GB RAM。
- .NET Framework 最低要求
  - 自助服务插件需要.NET 3.5 Service Pack 1，才能允许用户从 Receiver 用户界面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++ 2008 Service Pack 1 可再发行组件包。

兼容性列表

Citrix Receiver for Windows 4.9 与以下 Windows 操作系统和 Web 浏览器兼容。此外，还与当前所有受支持的 XenApp、XenDesktop 和 NetScaler Gateway 版本兼容，这些版本在 Citrix Product Lifecycle Matrix（Citrix 产品生命周期表）中列出。

> 注意
>
> NetScaler Gateway End Point Analysis Plug-in (EPA) 不支持本机 Citrix Receiver for Windows。

操作系统	浏览器
Windows 10 [1]	Internet Explorer
Windows 8.1，32 位和 64 位版本（包括 Embedded Edition）	最新的 Google Chrome（需要 StoreFront）
Windows 7，32 位和 64 位版本（包括 Embedded Edition）	最新的 Mozilla Firefox
Windows Thin PC	Microsoft Edge
Windows Server 2016	
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）	

[1] 支持 Windows 10 周年更新、创意者更新、秋季创意者更新和 2018 年 4 月更新（版本 1803）以及 2018 年 10 月更新（版本 1809）。

> 注意
>
> - 2018 年 10 月更新（版本 1809）仅在 Receiver for Windows 版本 4.9 CU5 及更高版本中受支持。
> - 2018 年 4 月更新仅在 Receiver for Windows 4.9 CU3 及更高版本中受支持。
> - 秋季创意者更新仅在 Receiver for Windows 4.9 CU1 及更高版本中受支持。Receiver for Windows 4.9 不支持该更新。

支持能力表

在启用了触控功能的设备上受支持的操作系统	在 VDA 上受支持的操作系统
Windows 10	Windows 10
Windows 8	Windows 8
Windows 7	Windows 7
	Windows 2012 R2
	Windows Server 2016
	Windows Server 2008 R2

连接、证书和身份验证

March 26, 2019

连接

1. HTTP 应用商店
2. HTTPS 应用商店
3. NetScaler Gateway 10.5 及更高版本
4. Web Interface 5.4

可以将 Citrix Receiver for Windows 连接到 VDA，或者可以在加入了 Windows 域的计算机、托管设备（本地和远程设备，启用或未启用 VPN 皆可）以及未加入域的计算机上建立 ICA 会话。

证书

1. 专用（自签名）证书
2. Root
3. 通配符证书
4. 中间证书

专用（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 Citrix Receiver for Windows 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，指出该证书不可信。如果用户选择忽略警告继续，则会显示一个应用程序列表，但应用程序无法启动。

安装根证书

对于加入了域的计算机，您可以使用组策略对象管理模板分发和信任 CA 证书。

对于未加入域的计算机，组织可以创建一个自定义安装软件包以分发和安装 CA 证书。请与系统管理员联系以获得帮助。

通配符证书

通配符证书在同一域内的某个服务器上使用。

Citrix Receiver for Windows 支持通配符证书，但是，必须在符合贵组织的安全策略时使用这些证书。实际上，可以考虑使用通配符证书的替代项，即使用者备用名称 (SAN) 扩展中包含服务器名称列表的证书。这些证书是由私有证书颁发机构和公共证书颁发机构颁发。

中间证书

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 配置中间证书。

身份验证

对 **StoreFront** 进行身份验证

	使用浏览器的 **Receiver for Web**	**StoreFront** 服务站点（本机）	**StoreFront XenApp Services** 站点（本机）	**NetScaler** 到 **Receiver for Web**（浏览器）	**NetScaler** 到 **StoreFront** 服务站点（本机）
匿名	是	是			
域	是	是	是	是 *	是 *
域直通	是	是	是		
安全令牌				是 *	是 *
双重（域 + 安全令牌）				是 *	是 *
SMS				是 *	是 *
智能卡	是	是		是	是
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 4.8 支持通过 NetScaler Gateway 到 StoreFront 本机服务的 2FA（域 + 安全令牌）。

对 **Web Interface** 进行身份验证

Citrix Receiver for Windows 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 *	
双重（域 + 安全令牌）			是 *	
SMS			是 *	
智能卡	是	是		
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 文档中配置身份验证和授权以及 StoreFront 文档中的管理权限主题。

有关 Web Interface 支持的身份验证方法的信息，请参阅 Web Interface 文档。

安装

January 7, 2019

可以按照以下方法安装 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 Citrix Receiver for Windows 的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。Citrix Receiver for Windows 确定与电子邮件地址关联的 NetScaler Gateway 或 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 Citrix Receiver for Windows 的用户。
  - 如果 Citrix Receiver for Windows 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 Citrix Receiver for Windows，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 Citrix Receiver for Windows。

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。使用可执行文件 (.exe) 安装 Citrix Receiver 时，还将安装 HDX RTME。

如果安装了 HDX RealTime Media Engine，则当您卸载并重新安装 Citrix Receiver for Windows 时，使用的模式务必与安装 HDX RTME 时使用的模式相同。

> 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 for Windows 时，请注意以下 HDX RTME 问题：

- 最新版的 Citrix ReceiverPlusRTME 包含 HDX RTME；不需要进一步安装即可安装 RTME。
- 支持从早期版本的 Citrix Receiver for Windows 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 Citrix Receiver for Windows 升级到最新的捆绑版本（例如，从 Receiver 4.7 升级到捆绑版本的带 RTME 的 Receiver 4.7）。
- 如果您已安装早期版本的 RTME，安装最新版本的 Citrix Receiver for Windows 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。

> 重要提示
>
> XenApp/XenDesktop 服务器上的 HDX RealTime Connector 的最低版本必须为 2.0.0.417，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 Citrix Receiver for Windows 后升级和打开此置备文件。
- 提供预配文件的另一个方法是，通知用户输入 NetScaler Gateway 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 Citrix Receiver for Web 站点，然后按照从 Citrix Receiver for Web 部署 Citrix Receiver for Windows 所述完成配置。通知用户如何升级 Citrix Receiver for Windows、访问 Citrix Receiver for Web 站点以及从 Citrix 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 Citrix Receiver for Windows 的 Web Interface 站点，并按照从 Web Interface 登录屏幕部署 Citrix Receiver for Windows 所述完成配置。告知用户如何升级 Citrix Receiver for Windows。例如，您可以创建一个下载站点，使用户能够获取重命名的 Citrix Receiver 安装程序。

升级注意事项

可以使用 Citrix Receiver for Windows 4.x 升级 Citrix 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 Citrix 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 Citrix Receiver for Windows 3.x，则不支持每计算机升级方式。

手动安装和卸载 **Citrix Receiver for Windows**

November 19, 2018

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 Citrix Receiver for Windows。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。

验证可用磁盘空间

Citrix Receiver for Windows 执行检查以确定是否有足够的可用磁盘空间来完成安装。该验证在全新安装及升级过程中执行。

全新安装过程中，安装将在磁盘空间不足时终止，并显示以下对话框。

升级 Citrix Receiver for Windows 时，安装将在磁盘空间不足时终止，并显示以下对话框。

下表提供了有关安装 Citrix Receiver for Windows 所需的最低磁盘空间的详细信息。

安装类型	所需磁盘空间
全新安装	320 MB
升级 Citrix Receiver	206 MB

> 注意
>
> - 安装程序仅在解压缩安装包后对磁盘空间执行检查。
> - 如果无提示安装过程中系统的磁盘空间不足，则不显示该对话框，而是在 **CTXInstall_TrolleyExpress-*.log** 中记录错误消息。

卸载 **Citrix 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 Citrix Receiver for Windows。

> 注意
>
> 您在继续安装 Citrix Receiver for Windows 之前收到卸载 Citrix HDX RTME 软件包的提示。有关详细信息，请参阅知识中心文章 CTX200340。

使用命令行界面卸载 **Citrix Receiver for Windows**

还可以通过键入以下命令从命令行卸载 Citrix Receiver for Windows：

CitrixReceiver.exe /uninstall

卸载 Citrix Receiver for Windows 后，由 receiver.adm/receiver.adml 或 receiver.admx 创建的自定义 Citrix Receiver for Windows 注册表项仍保留在 Software\Policies\Citrix\ICA Client 目录中的 HKEY_LOCAL_MACHINE 和 HKEY_LOCAL_USER 下面。

重新安装 Citrix Receiver for Window 时，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。

使用命令行参数配置和安装

March 26, 2019

可以通过指定命令行选项自定义 Citrix Receiver for Windows 安装程序。安装程序包将在启动安装程序之前自解压到用户的临时目录。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。

有关空间要求的详细信息，请参阅系统要求。

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]

自动更新

选项	/AutoUpdateCheck = auto/manual/disabled
说明	指示 Citrix Receiver for Windows 在有可用更新时进行检测；自动 – 系统将在有可用更新时向您发出通知（默认设置）；手动 – 系统在有更新可用时不向您发出通知。手动检查更新；已禁用 – 禁用自动更新
示例用法	CitrixReceiver.exe / AutoUpdateCheck = auto；CitrixReceiver.exe / AutoUpdateCheck = manual；CitrixReceiver.exe / AutoUpdateCheck = disabled

选项	/AutoUpdateStream= LTSR/Current
说明	指示 Citrix Receiver for Windows 的版本；**LTSR** – 指示版本为长期服务版本；当前 – 指示版本为最新版本的 Citrix Receiver for Windows
示例用法	CitrixReceiver.exe /AutoUpdateStream= LTSR；CitrixReceiver.exe / AutoUpdateStream= Current

选项	/DeferUpdateCount
说明	指示显示以后提醒我选项的次数。指示可以将更新推迟设置的次数；**-1** – 指示您可以将通知推迟任意次数（默认值 = -1）；**0** – 指示不显示“以后提醒我”选项；任何其他数值 – 指示显示“以后提醒我”选项该次数。例如，如果将该值设置为 10，以后提醒我选项将显示 10 次。
示例用法	CitrixReceiver.exe /DeferUpdateCount=-1；CitrixReceiver.exe /DeferUpdateCount=-0 ；CitrixReceiver.exe /DeferUpdateCount= 任何其他数值 >

选项	/AURolloutPriority
说明	指示您可以暂缓推出更新的期限；快 – 在交付期限的初期推出更新；中 – 在交付期限的中期推出更新；慢 – 在交付期限的末期推出更新。
示例用法	CitrixReceiver.exe /AURolloutPriority= 快； CitrixReceiver.exe /AURolloutPriority= 中； CitrixReceiver.exe /AURolloutPriority= 慢

启用双向内容重定向

> 注意
>
> 默认情况下，如果已在服务器上安装双向内容重定向组件，Citrix Receiver for Windows 将不安装这些组件。如果使用 XenDesktop 作为客户端计算机，则必须使用 /FORCE_LAA 开关安装双向内容重定向组件，从而安装 Citrix Receiver for Windows。但是，必须在服务器和客户端上配置该功能。

选项	ALLOW_BIDIRCONTENTREDIRECTION=1
说明	指示在客户端到主机与主机到客户端之间已启用双向内容重定向。
示例用法	CitrixReceiver.exe /ALLOW_BIDIRCONTENTREDIRECTION=1

启用本地应用程序访问

选项	FORCE_LAA=1
说明	默认情况下，如果已在服务器上安装客户端本地应用程序访问组件，Citrix Receiver for Windows 将不安装这些组件。要强制在 Citrix Receiver 上安装客户端本地应用程序访问组件，请使用 FORCE_LAA 命令行开关。需要管理员级别的权限才能执行这些步骤。有关本地应用程序访问的详细信息，请参阅 XenApp 和 XenDesktop 文档中的本地应用程序访问。
示例用法	CitrixReceiver.exe /FORCE_LAA =1

显示使用信息

选项	/? 或 /help
说明	指示用法信息
示例用法	CitrixReceiver.exe /?；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，Citrix Receiver for Windows 安装时处于暂停状态的 USB 设备在重新启动用户设备后才能被 Citrix Receiver for Windows 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	指示 Citrix Receiver for Windows 将随单点登录组件安装。相关选项 ENABLE_SSON 在命令行中包含 /includeSSON 时启用。如果要使用 ADDLOCAL= 指定各项功能，并希望安装单点登录，还必须指定值 SSON。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 Citrix Receiver for Windows。有关详细信息，请参阅 如何手动安装并配置 Citrix Receiver 以实现直通身份验证。注意：智能卡、Kerberos 以及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 **Single Sign-On**

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，在启用了单点登录身份验证的情况下安装之后，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，此功能设置为 true。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。
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；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

识别用户设备

选项	CLIENT_NAME=<ClientName>
说明	指定客户端名称，其中 ClientName 是用来识别连接到服务器的用户设备的名称。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 ENABLE_DYNAMIC_CLIENT_NAME =Yes

安装指定的组件

选项	ADDLOCAL=<feature… ,>
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。组件包括：ReceiverInside – 安装 Citrix Receiver 体验（Receiver 操作的必需组件）；ICA_Client – 安装标准 Citrix Receiver（Receiver 操作的必需组件）。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）；[可选] SSON - 安装 Single Sign On. 需要具有管理员权限。AM – 安装身份验证管理器；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；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，请参阅知识中心文章 CTX200337；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；USB – 安装 USB 支持。需要具有管理员权限；DesktopViewer – 安装 Desktop Viewer；Flash – 安装 HDX Media Stream for Flash；Vd3d – 启用 Windows Aero 体验（面向支持此功能的操作系统）。

选项	ADDLOCAL=<feature… ,>
示例用法	CitrixReceiver.exe ADDLO-CAL=ReceiverInside,ICA_Client,AM,SELFSERVICE,DesktopView

配置 **Citrix Receiver for Windows** 以手动添加应用商店

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：N – 不允许用户添加或删除自己的应用商店；S – 仅允许用户添加或删除安全应用商店（配置了 HTTPS）；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；也可以通过更新注册表项 HKLM\Software[Wow6432Node]Citrix\Dazzle\AllowAddStore 来控制此功能。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：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；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；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；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}
说明	默认值为 PNAgent 服务器在运行时指定的值。指定用户是否能够将应用商店的凭据本地保存在自己的计算机上，并且仅适用于使用 PNAgent 协议的应用商店。默认值为 S。选项包括：N – 不允许用户保存密码；S – 仅允许用户保存安全应用商店的密码（配置了 HTTPS）；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；也可以通过更新注册表项 HKLM\Software[Wow6432Node]\Citrix\Dazzle\AllowSavePwd 来控制此功能；注意：如果 AllowSavePwd 不起作用，则必须手动添加以下注册表项：32 位操作系统客户端的注册表项：HKLM\Software\Citrix\AuthManager；• 64 位操作系统客户端的注册表项：HKLM\Software\wow6432node\Citrix\AuthManager；• 类型：REG_SZ；• 值：never - 从不允许用户保存其密码。secureonly - 仅允许用户保存安全应用商店（使用 HTTPS 配置）的密码。always - 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。
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。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。还可以通过更新注册表项 HKCU 或 HKLM\Software[Wow6432Node]Citrix\AuthManager:Certificat 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“否”。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 使用 Kerberos 配置域直通身份验证。
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。有关会话预启动功能的信息，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}
说明	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。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 \RelativePath。位置：HKLM\Software[Wow6432Node]Citrix\Dazzle；HKCU\Software\Citrix\Dazzle；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。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。示例：• 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；• 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；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/IISLocatio | 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：x 和 y – 整数 0 到 9；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；servername.domain – 托管应用商店的服务器的完全限定域名；IISLocation – IIS 内的应用商店路径。应用商店 URL 必须与 StoreFront 预配文件中的 URL 一致。应用商店 URL 的格式为“/Citrix/store/discovery”。要获取 URL，请从 StoreFront 中导出一个预配文件，在记事本中打开，并复制 <Address> 元素中的 URL。•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；storedescription – 应用商店的可选描述，例如 HR App Store。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

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。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

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 for Windows 会为每个已订阅的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

November 19, 2018

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 Citrix Receiver for Windows。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 Citrix 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 for Windows 下载页面中。

- 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，set 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。

部署 Citrix Receiver for Windows 每计算机部署

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。

删除 Citrix Receiver for Windows 每计算机部署

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 Citrix Receiver for Windows 每用户部署的情况，两个 Citrix Receiver for Windows 每用户脚本将包含在 Citrix Receiver for Windows 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。

部署 **Citrix Receiver for Windows** 每用户部署

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。

删除 **Citrix Receiver for Windows** 每用户部署

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 **Citrix Receiver for Windows**

January 7, 2019

可以从 Receiver for Web 部署 Citrix Receiver for Windows，以确保您在尝试从浏览器连接到应用程序之前已安装 Receiver. 借助 Citrix Receiver for Web 站点，您可以通过 Web 页面访问 StoreFront 应用商店。如果 Citrix Receiver for Web 站点检测到用户没有 Citrix Receiver for Windows 的兼容版本，系统会提示您下载并安装 Citrix Receiver for Windows。

有关详细信息，请参阅 StoreFront 文档中的
Citrix Receiver for Web 站点。

如果已从 Citrix Receiver for Web 部署 Citrix Receiver for Windows，则基于电子邮件的帐户发现将不受支持。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 Citrix Receiver for Windows，则 Citrix Receiver for Windows 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。
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 **Citrix Receiver for Windows**

November 19, 2018

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 Citrix Receiver for Windows，以确保用户在尝试使用 Web Interface 之前安装了 Citrix Receiver for Windows。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 Citrix Receiver for Windows 的兼容版本，系统会提示用户下载并安装 Citrix Receiver for Windows。

如果已从 Web Interface 部署 Citrix Receiver for Windows，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 Citrix Receiver for Windows，则 Citrix Receiver for Windows 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。
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，Citrix Receiver for Windows 安装文件必须位于 Web Interface 服务器上。默认情况下，Web Interface 假定 Citrix Receiver for Windows 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。

使用 **System Center Configuration Manager 2012 R2** 部署

November 19, 2018

可以使用 Microsoft System Center Configuration Manager (SCCM) 部署 Citrix Receiver for Windows。

注意：只有 Citrix Receiver for Windows 4.5 及更高版本支持 SCCM 部署。

使用 SCCM 完成 Citrix Receiver for Windows 的部署分为四部分：

1. 向 SCCM 部署中添加 Citrix Receiver for Windows
2. 添加分发点
3. 将 Receiver 软件部署到软件中心
4. 创建设备集合

向 **SCCM** 部署中添加 **Citrix Receiver for Windows**

1. 将下载的 Citrix Receiver 复制到 Configuration Manager 服务器上的某个文件夹并启动 Configuration Manager 控制台。

2. 选择 **Software Library**（软件库）> **Application Management**（应用程序管理）。右键单击 **Application**（应用程序）并单击 **Create Application**（创建应用程序）。
   此时将显示 “Create Application”（创建应用程序）向导。
3. 在 **General**（常规）窗格中，选择 **Manually specify the application information**（手动指定应用程序信息），然后单击 **Next**（下一步）。
4. 在 **General Information**（常规信息）窗格中，指定与应用程序有关的信息，例如名称、制造商、软件版本等。
5. 在 “Application Catalog”（应用程序目录）向导中，指定其他信息，例如，语言、应用程序名称、用户类别等，然后单击 **Next**（下一步）。

   注意：用户可以看到您在此处指定的信息。
6. 在 **Deployment Type**（部署类型）窗格中，单击 **Add**（添加）以配置 Citrix Receiver 安装程序的部署类型。
   此时将显示 “Create Deployment Type”（创建部署类型）向导。
7. 在 **General**（常规）窗格中：设置 Windows Installer（*.msi 文件）的部署类型，选择 **Manually specify the deployment type information**（手动指定部署类型信息），然后单击 **Next**（下一步）。
8. 在 **General Information**（常规信息）窗格中：指定部署类型详细信息（例如，Receiver 部署），然后单击 **Next**（下一步）。
9. 在 **Content**（内容）窗格中：
   a) 提供 Citrix Receiver 安装文件所在的路径。例如：SCCM 服务器上的 Tools。
   b) 将安装程序指定为以下项之一：
      - CitrixReceiver.exe /silent，适用于默认无提示安装。
      - CitrixReceiver.exe /silent /includeSSON，启用域直通。
      - CitrixReceiver.exe /silent SELFSERVICEMODE=false，在非自助服务模式下安装 Receiver。
   c) 将 CitrixReceiver.exe /uninstall 指定为 **Uninstall program**（卸载程序）（启用通过 SCCM 卸载）。
10. 在 **Detection Method**（检测方法）窗格中：选择 **Configure rules to detect the presence of this deployment type**（配置用于检测是否存在此部署类型的规则），然后单击 **Add Clause**（添加子句）。此时将显示 “Detection Rule”（检测规则）对话框。
11. 将 **Setting Type**（设置类型）设置为 “File System”（文件系统）。
12. 在 **Specify the file or folder to detect the application**（指定要检测应用程序的文件或文件夹）下，设置以下选项：

    - **Type**（类型）- 在下拉菜单中，选择 “File”（文件）。
    - **Path**（路径）- %ProgramFiles (x86)%\Citrix\ICA Client\Receiver
    - **File or folder name**（文件或文件夹名称）- Receiver.exe
    - **Property**（属性）- 在下拉菜单中，选择 **Version**（版本）
    - **Operator**（运算符）- 在下拉菜单中，选择 **Greater than or equal to**（大于或等于）
    - **Value**（值）- 键入 **4.3.0.65534**

    注意：此规则组合也适用于 Citrix Receiver for Windows 升级。

13. 在 **User Experience**（用户体验）窗格中，设置：

    - **Installation behavior**（安装行为）- Install for system（为系统安装）
    - **Logon requirement**（登录要求）- Whether or not a user is logged on（用户是否登录）
    - **Installation program visibility**（安装程序可见性）- Normal（正常）。

    单击下一步。

    注意：请勿为此部署类型指定任何要求和依赖项。

14. 在 **Summary**（摘要）窗格中，验证此部署类型的设置。单击下一步。

    此时将显示成功消息。

15. 在 **Completion**（完成）窗格中，新类型（Receiver 部署）将在 “Deployment types”（部署类型）下列出。

16. 单击 **Next**（下一步），然后单击 **Close**（关闭）。

添加分发点

1. 在 Configuration Manager 控制台中右键单击 Receiver for Windows，然后选择 **Distribute Content**（分发内容）。
   此时将显示 “Distribute Content”（分发内容）向导。

2. 在 “Content Distribution”（内容分发）窗格中，单击 **Add**（添加）**> Distribution Points**（分发点）。此时将显示 “Add Distribution Points”（添加分发点）对话框。

3. 浏览到提供内容的 SCCM 服务器，然后单击 **OK**（确定）。在 “Completion”（完成）窗格中，将显示成功消息。

4. 单击 **Close**（关闭）。

将 **Receiver** 软件部署到软件中心

1. 在 Configuration Manager 控制台中右键单击 Receiver for Windows，然后选择 **Deploy**（部署）。
   此时将显示 “Deploy Software”（部署软件）向导。

2. 在要部署应用程序的集合（可以是设备集合，也可以是用户集合）中选择 **Browse**（浏览），然后单击 **Next**（下一步）。

3. 在 **Deployment Settings**（部署设置）窗格中，将 **Action**（操作）设置为 “Install”（安装），将 **Purpose**（用途）设置为 “Required”（必需）（启用无人参与安装）。单击下一步。

4. 在 **Scheduling**（计划）窗格中，指定在目标设备上部署软件的计划。

5. 在 **User Experience**（用户体验）窗格中，设置 **User notifications**（用户通知）行为；选择 **Commit changes at deadline or during a maintenance window (requires restart)**（在最后期限或维护时段提交更改 (需要重新启动)），然后单击 **Next**（下一步）以完成 “Deploy Software”（部署软件）向导。在 “Completion”（完成）窗格中，将显示成功消息。

重新启动目标端点设备（仅在立即开始安装时才需要执行）。

在端点设备上，Citrix Receiver for Windows 在软件中心中的 **Available Software**（可用软件）下显示。根据您所配置的计划，安装将自动触发。或者，您也可以根据需要制定计划或者进行安装。安装开始后，安装状态将在软件中心中显示。

创建设备集合

1. 启动 Configuration Manager 控制台，单击 **Assets** and **Compliance**（资产与合规性）> **Overview**（概述）> **Devices**（设备）。
2. 右键单击 **Device Collections**（设备集合）并选择 **Create Device Collection**（创建设备集合）。此时将显示 “Create Device Collection”（创建设备集合）向导。
3. 在 **General**（常规）窗格中，键入设备的名称，然后单击用于限制集合的 **Browse**（浏览）。这决定设备的范围，可以是 SCCM 创建的默认设备集合之一。单击下一步。
4. 在 “Membership Rules”（成员身份规则）窗格中，单击用于过滤设备的 **Add Rule**（添加规则）。此时将显示 “Create Direct Membership Rule”（创建直接成员身份规则）向导。
   - 在 “Search for Resources”（搜索资源）窗格中，根据要过滤的设备选择 **Attribute name**（属性名称），并提供属性名称的值以选择设备。
5. 单击下一步。在 “Select Resources”（选择资源）窗格中，选择需要作为设备集合的一部分的设备。在 “Completion”（完成）窗格中，将显示成功消息。
6. 单击关闭。
7. 在 “Membership rules”（成员身份规则）窗格中，将列出新规则。单击下一步。
8. 在 “Completion”（完成）窗格中，将显示成功消息。单击 **Close**（关闭）以完成 “Create Device Collection”（创建设备集合）向导。新设备集合将在 **Device Collections**（设备集合）中列出。在 “Deploy Software”（部署软件）向导中浏览时，新设备集合属于设备集合的一部分。

> 注意
>
> 将 **MSIRESTARTMANAGERCONTROL** 属性设置为 **False** 时，使用 SCCM 部署 Citrix Receiver for Windows 可能会不成功。
> 根据我们的分析，Citrix Receiver for Windows 并不是导致本次失败的原因。此外，重试可能会使部署成功。

配置

January 7, 2019

使用 Citrix 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 Citrix Receiver for Windows 中添加 StoreFront 帐户配置自助服务模式。此模式允许用户从 Citrix Receiver for Windows 用户界面订阅应用程序。
- 通过组策略对象管理模板配置
- 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 文档中的身份验证和授权。

配置应用程序交付

March 26, 2019

通过 XenDesktop 或 XenApp 交付应用程序时，请考虑使用以下方案以改善用户体验：

- Web 访问模式 — 如果未执行任何配置，Citrix Receiver for Windows 将提供针对应用程序和桌面的基于浏览器的访问权限。可以打开浏览器访问 Receiver for Web 或 Web Interface 站点，以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 - 通过将 StoreFront 帐户添加到 Citrix Receiver for Windows 中或将 Citrix Receiver for Windows 配置为指向 StoreFront 站点，可以配置自助服务模式，在此模式下，您可以从 Citrix Receiver for Windows 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、自动预配的以及精选应用程序关键字设置。

注意： 默认情况下，Citrix Receiver for Windows 允许您选择要在 “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 Citrix Receiver for Windows 管理员，您可以将 Citrix Receiver for Windows 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 Citrix Receiver for Windows Enterprise 的方式相似。新的仅快捷方式模式允许您在熟悉的 Windows 导航架构中查找所有已发布的应用程序，该位置正是您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 Citrix Receiver for Windows 用户可见。

配置 **NetScaler Gateway** 应用商店

Citrix 建议使用组策略对象管理模板为网络路由、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。
可以将 receiver.admx / receiver.adml 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 for Windows 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。

要使用组策略对象管理模板添加或指定 **NetScaler Gateway**，请执行以下操作：

1. 以管理员身份通过运行 gpedit.msc 打开 Citrix Receiver 组策略对象管理模板。
    - 如果要在一台计算机上应用该策略，请从 “开始” 菜单启动。
    - 如果要对域策略应用，请使用组策略管理控制台启动。
2. 在 “计算机配置” 节点下，转至 “管理模板”>“经典管理模板 (ADM)”>“Citrix 组件”>“Citrix Receiver”>“StoreFront”，然后选择 “NetScaler Gateway URL/StoreFront 帐户列表”。
3. 编辑设置。
    - 应用商店名称 - 指示显示的应用商店名称
    - 应用商店 URL - 指示应用商店的 URL
    - #Store name - 指示 NetScaler Gateway 后面的应用商店名称
    - 应用商店启用的状态 - 指示应用商店的状态，开/关
    - 应用商店描述 - 提供应用商店的描述
4. 添加或指定 NetScaler URL。输入 URL 的名称（以分号分隔）：

> 示例：
>
> `HRStore; https://dtls.blrwinrx.com\##Store name;On; Store for HR staff`
>
> 其中，#Store name 是 NetScaler Gateway 后面的应用商店名称；dtls.blrwinrx.com 是 NetScaler URL.
>
> 在使用 GPO 添加 NetScaler Gateway 之后启动 Citrix Receiver for Windows 时，通知区域中会显示以下消息。

限制：

1. NetScaler URL 应列在最前面，后跟 StoreFront URL。
2. 不支持多个 NetScaler URL。
3. 在 NetScaler URL 中所做的所有更改都要求重置 Citrix Receiver for Windows，更改才能生效。
4. 使用这种方法配置的 NetScaler Gateway URL 不支持位于 NetScaler Gateway 后面的 PNA Services 站点。

配置自助服务模式

通过简单地将 StoreFront 帐户添加到 Citrix Receiver 中或将 Citrix 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，Citrix Receiver for Windows 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、自动预配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 Citrix 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应用商店，请将字符串 KEYWORDS:Auto 附加到说明后面。用户登录该应用商店时，相应的应用程序将自动预配，而无需用户手动订阅。
- 要向用户公告应用程序，或者在 Citrix 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。

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。如果您在任何时间想要自定义组策略，请重置 Citrix 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：在将策略应用到单个计算机时，通过从开始菜单本地运行行命令 gpedit.msc 打开，或在应用域策略时通过使用组策略管理控制台打开。
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）
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 **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 **<annotatedServices>** 部分的 **C:\inetpub\wwwroot\Citrix\Roaming** 中的 web.config 文件：

- 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 和 Windows 10 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：

<account id=… name=”Store”

此部分的结尾是 </account> 标记。

在帐户部分结束之前，在前几项属性部分中：

<properties> <clear /> </properties>

可以将属性添加到此部分的 <clear /> 标记之后，每个属性占一行，并提供名称和值。例如：

<property name=”PutShortcutsOnDesktop” value=”True” />

注意：在 <clear /> 标记之前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 <clear /> 标记属于可选操作。

以下是此部分的扩展示例：

<properties><property name=”PutShortcutsOnDesktop” value=”True” /><property name=”DesktopDir” value=”Citrix Applications” />

> 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，将配置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 Citrix 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 Citrix Receiver 版本类似，但是，版本 4.2.100 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。注意： 此设置仅适用于 Web Interface 站点。

> 注意：
>
> **PutShortcutsInStartMenu=false** 设置适用于 XenApp 6.5 和 XenDesktop 7.x。

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。

小心：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。

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：
   a) Reg add HKLM\Software\Citrix\Dazzle /v CommonStubDirectory /t REG_SZ /d “\ShareOne\ReceiverStub
   b) Reg add HKLM\Software\Citrix\Dazzle /v
   c) opyStubsFromCommonStubDirectory /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。
   d) 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：	以自助服务模式配置 Citrix Receiver。在此模式下，您还可以根据需要配置自动预配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 Citrix 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。根据需要使用自动预配的和强制应用程序。

“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应用程序快捷方式。在此类情况下，最简单的方法是浏览器访问；安装 Citrix Receiver 但不执行任何配置，然后浏览到 Citrix Receiver for Web 和 Web Interface。还可以将 Citrix 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 Citrix Receiver 自动将应用程序快捷方式放置在“开始”菜单中，请执行以下操作：	配置 Citrix Receiver，使 PutShortcutsInStartMenu=False。即使在自助服务模式下，Citrix 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 Citrix Receiver 自动将所有应用程序快捷方式都放置在“开始”菜单中，请执行以下操作：	配置 Citrix Receiver，使 SelfServiceMode = False。所有可用的应用程序将在“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：	配置 Citrix Receiver，使 PutShortcutsOnDesktop = true。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：	配置 Citrix Receiver，使 DesktopDir= 用于放置应用程序的桌面文件夹的名称。

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：	配置 Citrix Receiver，使 **PutShortcutsInStartMenu=false** 并启用每应用程序设置。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 Citrix Receiver 放置在“开始”菜单中的应用程序快捷方式显示在其关联的类别（文件夹）中，请执行以下操作：	配置 Citrix Receiver，使 **UseCategoryAsStartMenuPath=True**。注意：Windows 8/8.1 和 Windows 10 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 Citrix 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：	配置 Citrix Receiver，使 StartMenuDir=“开始”菜单文件夹名称。

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

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 Citrix Receiver 中提供的应用程序，请附加字符串 KEYWORDS:prefer=”pattern”。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，Citrix 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，Citrix Receiver 将订阅该应用程序，但不创建快捷方式。用户从 Citrix Receiver 窗口中启动该应用程序时，Citrix Receiver 将启动本地安装的（首选）应用程序。

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

> 注意： Citrix 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：

- 要指定应使用本地安装的应用程序而非 Citrix Receiver 中提供的应用程序，请附加字符串 KEYWORDS:prefer="pattern"。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，Citrix 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，Citrix Receiver 将订阅该应用程序，但不创建快捷方式。用户从 Citrix Receiver 窗口中启动该应用程序时，Citrix Receiver 将启动本地安装的（首选）应用程序。
  如果用户在 Citrix Receiver 外部卸载了某个首选应用程序，下次 Citrix Receiver 刷新时将取消订阅该应用程序。如果用户从 Citrix Receiver 窗口中卸载了某个首选应用程序，Citrix Receiver 将取消订阅该应用程序，但不卸载。

> 注意： Citrix 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 2010	否
“\Microsoft Word 2010”	\Programs\Microsoft Office\Microsoft Word 2010	否
“\Programs\Microsoft Word 2010”	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 文档的优化用户体验中的“其他建议”。

配置 XenDesktop 环境

November 19, 2018

在安装 Citrix Receiver for Windows 之后，用户利用以下配置步骤可访问其托管应用程序和桌面：

- 自适应传输 - 自适应传输通过尽可能优先于 TCP 来应用名为 Enlightened Data Transport (EDT) 的新 Citrix 协议来优化数据传输。有关配置自适应传输的详细信息，请参阅配置自适应传输。

- 自动更新 - 自动更新功能提供 Citrix Receiver for Windows 以及 HDX RealTime Optimization Pack 的自动更新，不需要手动下载更新。有关配置自动更新的详细信息，请参阅配置自动更新。
- 双向内容重定向 - 双向内容重定向允许您启用或禁用客户端到主机和主机到客户端 URL 重定向。有关配置双向内容重定向的详细信息，请参阅配置双向内容重定向。
- Bloomberg 键盘 - 可将专用 USB 设备（例如，Bloomberg 键盘和 3D 鼠标）配置为使用 USB 支持。有关配置 Bloomberg 键盘的信息，请参阅配置 Bloomberg 键盘。
- 复合 USB 设备 - 复合 USB 设备能够执行多种功能。这是通过使用不同的接口展示其中的每项功能来实现的。有关配置复合 USB 设备的详细信息，请参阅配置复合 USB 设备。
- USB 支持 - USB 支持允许用户在连接到虚拟桌面时与各种各样的 USB 设备进行交互。有关配置 USB 支持的详细信息，请参阅配置 USB 支持。

配置自适应传输

January 7, 2019

> 要求
>
> - XenApp 和 XenDesktop 7.12 及更高版本（启用使用 Citrix Studio 的功能时需要）。
> - StoreFront 3.8。
> - 仅限 IPv4 VDA。不支持 IPv6 配置以及 IPv6 和 IPv4 混合配置。
> - 添加防火墙规则以允许通过 VDA 的 UDP 端口 1494 和 2598 传送入站流量。
>
> 注意
>
> TCP 端口 1494 和 2598 也是必需端口，并在您安装 VDA 时自动打开。但是，UDP 端口 1494 和 2598 不自动打开。必须将其启用。

必须先通过应用策略在 VDA 上配置自适应传输，才能将其用于 VDA 与 Citrix Receiver 之间的通信。

默认情况下，允许在 Citrix Receiver for Windows 中启用自适应传输。但是，默认情况下，仅当 VDA 在 Citrix Studio 策略中配置为首选时以及在 VDA 上应用该设置时，客户端才尝试使用自适应传输。

可以使用 **HDX** 自适应传输策略设置启用自适应传输。将该新策略设置为首选将尽可能使用自适应传输，并回退到 TCP。

要在特定客户端上禁用自适应传输，请使用 Citrix Receiver 组策略对象管理模板相应地设置 EDT 选项。

使用 **Citrix Receiver** 组策略对象管理模板配置自适应传输（可选）

下面是用于自定义您的环境的可选配置步骤。例如，您可能出于安全原因针对特定客户端禁用该功能。

> 注意
>
> 默认情况下，自适应传输处于禁用状态（关），并始终使用 TCP。

1. 以管理员身份通过运行 gpedit.msc 打开 Citrix Receiver 组策略对象管理模板。
   - 如果要在一台计算机上应用该策略，请从“开始”菜单启动。
   - 如果要在某个域中应用该策略，请使用组策略管理控制台启动。

   有关如何将 Citrix Receiver for Windows 管理模板文件导入到组策略编辑器的信息，请参阅使用组策略对象模板配置 Citrix Receiver for Windows。
2. 在“计算机配置”节点下，转至管理模板 > **Citrix Receiver** > 网络路由。
3. 将 **Receiver** 的传输协议策略设置为已启用。
4. 根据需要选择 **Citrix Receiver** 的通信协议。
   - 关：指示使用 TCP 进行数据传输。
   - 首选：指示 Citrix Receiver 先尝试使用 UDP 连接到服务器，然后切换到 TCP 以完成回退。
   - 开：指示 Citrix Receiver 仅使用 UDP 连接到服务器。使用此选项时，不回退到 TCP。
5. 单击应用和确定。
6. 在命令行中，运行 gpupdate /force 命令。

此外，要使自适应传输配置生效，用户需要将 Citrix Receiver Windows 模板文件添加到“策略定义”文件夹中。有关将 admx/adml 模板文件添加到本地 GPO 的详细信息，请参阅使用组策略对象模板配置 Citrix Receiver for Windows。

要确认策略设置是否已生效，请执行以下操作：

导航到 HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Network\UDT 并验证是否包括注册表项 **HDXOverUDP**。

配置自动更新

March 26, 2019

从 Citrix Receiver for Windows 配置自动更新时，请遵照优先级顺序按照下面的方法进行操作：

1. 组策略对象管理模板
2. 命令行接口
3. 高级首选项（每用户）

使用组策略对象管理模板配置

1. 以管理员身份通过运行 gpedit.msc 打开 Citrix Receiver 组策略对象管理模板。
   - 要在单台计算机上应用该策略，请从“开始”菜单中启动 Citrix Receiver 组策略对象管理模板。

- 如果要在某个域中应用该策略，请使用组策略管理控制台启动 Citrix Receiver 组策略对象管理模板。

2. 在“计算机配置”节点下，转至管理模板 > **Citrix** 组件 > **Citrix Receiver** > 自动更新。
3. 选择设置检查更新的延迟策略。此策略允许您暂缓推出一段时间。
4. 选择已启用，然后从延迟组下拉菜单中，选择以下选项之一：
   - 快 - 在交付期限的初期推出更新。
   - 中 - 在交付期限的中期推出更新。
   - 慢 - 在交付期限的末期推出更新。
5. 单击应用和确定保存此策略。
6. 在“自动更新模板”部分中，选择启用或禁用自动更新策略。
7. 选择已启用并根据需要设置值：
   - 从启用自动更新策略下拉列表中，选择以下选项之一：
     - 自动 - 系统将在有可用更新时向您发出通知（默认设置）。
     - 手动 - 系统在有可用更新时不向您发出通知。手动检查更新。
   - 选择仅限 **LTSR** 以仅获取 LTSR 的更新。
   - 从 **auto-update-DeferUpdate-Count** 下拉列表中，选择一个介于 **-1** 到 **30** 之间的值，其中
     - **-1** - 指示您可以将通知推迟任意次数（默认值 = -1）。
     - **0** - 指示不显示以后提醒我选项。
     - 任何其他数值 - 指示显示以后提醒我选项该次数。例如，如果将该值设置为 10，以后提醒我选项将显示 10 次。
8. 单击应用和确定保存此策略。

使用命令行接口配置

安装 **Citrix Receiver for Windows** 时

要在 Citrix Receiver 安装过程中以管理员身份使用命令行设置配置自动更新设置，请执行以下操作：

- **/AutoUpdateCheck =** auto/manual/disabled
- **/AutoUpdateStream=** LTSR/Current。其中，LTSR 是指长期服务版本，Current 是指当前版本。
- **/DeferUpdateCount=** 介于 -1 到 30 之间的任意值
- **/AURolloutPriority=** auto/fast/medium/slow

例如：*CitrixReceiver.exe / AutoUpdateCheck=auto /AutoUpdateStream= Current /DeferUpdateCount=-1 / AURolloutPriority= fast*

- 要在 Citrix Receiver 安装过程中以用户身份使用命令行设置配置自动更新设置，请执行以下操作：
  - **/AutoUpdateCheck=**auto/manua**l**

例如：*CitrixReceiver.exe / AutoUpdateCheck=auto*

使用组策略对象管理模板编辑自动更新设置将替换在所有用户的 Citrix Receiver for Windows 安装过程中应用的设置。

完成 **Citrix Receiver for Windows** 安装后

可以在安装 Citrix Receiver for Windows 后配置自动更新。

使用命令行：

打开 Windows 命令提示窗口，并将目录更改到 **CitrixReceiverUpdater.exe** 所在位置。CitrixReceiverUpdater.exe 通常位于 *CitrixReceiverInstallLocation*\Citrix\Ica Client\Receiver 下。

也可以使用此二进制文件设置自动更新命令行策略。

例如：管理员可以使用全部四个选项：

- CitrixReceiverUpdater.exe */AutoUpdateCheck=auto /AutoUpdateStream= STSR /DeferUpdateCount=-1 / AURolloutPriority= fast*

使用图形用户界面配置

个人用户可以使用高级首选项对话框覆盖自动更新设置。这是一项基于用户的配置，并且这些设置仅适用于当前用户。

1. 右键单击通知区域中的 Citrix Receiver for Windows。
2. 选择高级首选项并单击自动更新。

   此时将显示自动更新对话框。
3. 选择以下选项之一：
   - 是，通知我
   - 否，不要通知我
   - 使用管理员指定的设置
4. 单击保存。

使用 **StoreFront** 配置自动更新

1. 使用文本编辑器打开 web.config 文件，该文件通常位于 C:\inetpub\wwwroot\Citrix\Roaming 目录中。
2. 在该文件中找到用户帐户元素（您的部署的帐户名称为 Store）

   例如：<account id=… name=”Store”>

   在 *</account>* 标记之前，导航到该用户帐户的属性：


```
<properties>
 <clear />
</properties>
```

3. 在 *<clear />* 标记后面添加自动更新标记。

```
<account>
    <clear />
    <account id="d1197d2c-ac82-4f13-9346-2ee14d4b0202" name="F84Store"
     description="" published="true" updaterType="Citrix" remoteAccessType="None">
     <annotatedServices>
      <clear />
      <annotatedServiceRecord serviceRef="1__Citrix_F84Store">
       <metadata>
        <plugins>
         <clear />
        </plugins>
        <trustSettings>
         <clear />
        </trustSettings>
        <properties>
         <property name="Auto-Update-Check" value="auto" />
         <property name="Auto-Update-DeferUpdate-Count" value="1" />
              <property name="Auto-Update-LTSR-Only" value="FALSE" />
         <property name="Auto-Update-Rollout-Priority" value="fast" />
            </properties>
       </metadata>
      </annotatedServiceRecord>
     </annotatedServices>
     <metadata>
      <plugins>
       <clear />
```



```
    </plugins>
    <trustSettings>
     <clear />
    </trustSettings>
    <properties>
     <clear />
    </properties>
   </metadata>
  </account>
```

auto-update-Check

指示 Citrix Receiver for Windows 在有可用更新时进行检测。

有效值包括：

- 自动 - 系统将在有可用更新时向您发出通知（默认设置）。
- 手动 - 系统在有可用更新时不向您发出通知。手动检查更新。
- 已禁用 – 禁用自动更新

auto-update-LTSR-Only

指示 Citrix Receiver for Windows 必须仅接受 LTSR 的更新。

有效值包括：

- True – 自动更新仅检查 Citrix Receiver for Windows 的 LTSR 更新
- False – 自动更新还检查 Citrix Receiver for Windows 的非 LTSR 更新。

auto-update-DeferUpdate-Count

指示可以推迟通知的次数。以后提醒我选项在设置次数值中显示。

有效值包括：

- -1 - 指示您可以将通知推迟任意次数（默认值 = -1）。
- 0 - 指示不显示以后提醒我选项。
- 任何其他数值 - 指示显示“以后提醒我”选项该次数。例如，如果将该值设置为 10，以后提醒我选项将显示 10 次。

auto-update-Rollout-Priority:

指示可以为推出设置的时间期限。

有效值包括：

- 快 - 在交付期限的初期推出更新。
- 中 - 在交付期限的中期推出更新。
- 慢 - 在交付期限的末期推出更新。

限制：

1. 您的系统必须有权访问 Internet。
2. Receiver for Web 用户不能自动下载 StoreFront 策略。
3. 如果您配置了截获出站代理的 SSL，则必须添加 Receiver 自动更新签名服务 (https://citrixupdates.cloud.com) 和下载位置 (https://downloadplugins.citrix.com) 的例外。
4. 默认情况下，自动更新功能在 VDA 上处于禁用状态。这包括 RDS 多用户服务器计算机、VDI 和 RemotePC 计算机。
5. 自动更新功能在安装了 Desktop Lock 的计算机上处于禁用状态。

配置双向内容重定向

January 7, 2019

可以使用以下方法之一启用双向内容重定向：

1. 组策略对象管理模板
2. 注册表

> 注意
>
> - 双向内容重定向在本地应用程序访问处于启用状态的会话中不起作用。
> - 必须在服务器和客户端上启用双向内容重定向。在服务器或客户端上禁用时，该功能将禁用。

使用组策略对象管理模板启用双向内容重定向

请在首次安装 Citrix Receiver for Windows 时使用组策略对象管理模板配置。

1. 以管理员身份通过运行 gpedit.msc 打开 Citrix Receiver 组策略对象管理模板。
   - 如果要在一台计算机上应用该策略，请从“开始”菜单启动。
   - 如果要在某个域中应用该策略，请使用组策略管理控制台启动。
2. 在“用户配置”节点下，转至管理模板 **> ** 经典管理模板 **(ADM)** > **Citrix** 组件 > **Citrix Receiver** > 用户体验。

3. 选择双向内容重定向策略。
4. 编辑设置。

   注意：
   包括 URL 时，可以指定单个 URL 或以分号分隔的 URL 列表。可以使用星号 (*) 作为通配符。
5. 单击应用和确定。
6. 在命令行中，运行 gpupdate /force 命令。

使用注册表启用双向内容重定向

要启用双向内容重定向，请从 Citrix Receiver for Windows 安装文件夹 (C:\Program Files (x86)\Citrix\ICA Client) 运行 **redirector.exe /RegIE** 命令。

限制：

- 如果重定向由于会话启动问题失败，则不存在回退机制。

重要：

- 请确保重定向规则不会导致出现循环配置。例如，如果设置了 VDA 规则以便 URL `https://www.my_company.com` 配置为重定向到客户端，并且相同的 URL 配置为重定向到该 VDA 导致的循环配置。
- URL 重定向仅支持显式 URL（出现在浏览器的地址栏中或使用浏览器导航找到的 URL，具体取决于浏览器）。
- 如果显示名称相同的两个应用程序配置为使用多个 StoreFront 帐户，主 StoreFront 帐户中的显示名称将用于启动应用程序或桌面会话。
- 新浏览器窗口仅在 URL 重定向到客户端时显示。URL 重定向到 VDA 时，如果浏览器已打开，重定向的 URL 将在新选项卡中打开。
- 支持文档、电子邮件、PDF 等文件中的嵌入式链接。

配置 **Bloomberg** 键盘

November 19, 2018

Citrix Receiver for Windows 支持在 XenApp 和 XenDesktop 会话中使用 Bloomberg 键盘。所需的组件随插件安装。可以在 Citrix Receiver for Windows 安装过程中或者使用注册表启用 Bloomberg 键盘功能

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。

要启用或禁用 **Bloomberg** 键盘支持，请执行以下操作：

小心： 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。

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。

有关配置 Bloomberg 键盘的详细信息，请参阅知识中心文章 CTX122615

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。

小心： 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。

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：

   - HKEY_CURRENT_USER\Software\Citrix\XenDesktop\DesktopViewer
   - HKEY_LOCAL_MACHINE\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：

   - HKEY_CURRENT_USER\Software\Policies\Citrix\XenDesktop\DesktopViewer
   - HKEY_LOCAL_MACHINE\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：

   a) HKEY_CURRENT_USER\Software\Policies\Citrix\…
   b) HKEY_LOCAL_MACHINE\Software\Policies\Citrix\…
   c) HKEY_CURRENT_USER\Software\Citrix\…
   d) HKEY_LOCAL_MACHINE\Software\Citrix\…

配置复合 **USB** 设备重定向

November 19, 2018

使用组策略对象管理模板配置复合 **USB** 重定向

1. 以管理员身份通过运行 **gpedit.msc** 打开 Citrix Receiver 组策略对象管理模板。
   a) 要在单台计算机上应用该策略，请从“开始”菜单中启动 Citrix Receiver 组策略对象管理模板。
   b) 如果要在某个域中应用该策略，请使用组策略管理控制台启动 Citrix Receiver 组策略对象管理模板。
2. 在“用户配置”节点下，转至管理模板 > **Citrix** 组件 > **Citrix Receiver** > 远程连接客户端设备 > 通用 **USB** 远程连接。
3. 选择拆分设备策略。
4. 选择已启用。
5. 单击应用。
6. 单击确定保存该策略。

使用组策略对象管理模板允许或拒绝使用某个接口

1. 以管理员身份通过运行 gpedit.msc 打开 Citrix Receiver 组策略对象管理模板。
   a) 要在单台计算机上应用该策略，请从“开始”菜单中启动 Citrix Receiver 组策略对象管理模板。
   b) 如果要在某个域中应用该策略，请使用组策略管理控制台启动 Citrix Receiver 组策略对象管理模板。
2. 在“用户配置”节点下，转至管理模板 > **Citrix** 组件 > **Citrix Receiver** > 远程连接客户端设备 > 通用 **USB** 远程连接。
3. 选择 **USB** 设备规则策略。
4. 选择已启用。
5. 在 **USB** 设备规则文本框中，添加要允许或拒绝使用的 USB 设备。
   例如，*ALLOW: vid=047F pid= C039 split=01 intf=00,03 //*允许使用 *00* 和 *03* 接口，限制使用其他接口。
6. 单击应用和确定。

   在桌面会话中，拆分 USB 设备在 Desktop Viewer 中的设备下显示。此外，还可以从首选项 > 设备中查看拆分 USB 设备。

   在应用程序会话中，拆分 USB 设备显示在连接中心中。

下表提供了与允许或拒绝使用 USB 接口时的行为场景有关的详细信息。

要允许使用某个接口，请执行以下操作：

拆分	接口	操作
TRUE	有效编号 0 -n	允许使用指定接口
TRUE	数值无效	允许使用所有接口
FALSE	任意值	允许使用父设备的通用 USB 接口
未指定	任意值	允许使用父设备的通用 USB 接口

例如，SplitDevices- *true* 指示拆分所有设备。

要拒绝使用某个接口，请执行以下操作：

拆分	接口	操作
TRUE	有效编号 0 -n	拒绝使用指定接口
TRUE	数值无效	拒绝使用所有接口
FALSE	任意值	拒绝使用父设备的通用 USB 接口
未指定	任意值	拒绝使用父设备的通用 USB 接口

例如，SplitDevices- *false* 指示设备不通过指定接口号拆分。

例如：My_<*plantronics*> 耳机

接口号：

- 音频接口类 -0
- HID 接口类-3

用于 My_<*plantronics*> 耳机的示例规则：

- ALLOW: vid=047F pid= C039 split=01 intf=00,03 //允许使用 00 和 03 接口，限制使用其他接口。
- DENY: vid=047F pid= C039 split=01 intf=00,03 // 拒绝使用 00 和 03

限制：

Citrix 建议您不要拆分网络摄像机的接口。解决方法为，使用通用 USB 重定向作为单个设备重定向该设备。要实现更加出色的性能，请使用优化后的虚拟通道。

配置 **USB** 支持

March 26, 2019

USB 支持允许您在连接到虚拟桌面时与各种各样的 USB 设备进行交互。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。

在典型的低延迟/高速 LAN 环境中支持 USB 设备（例如网络摄像机、麦克风、扬声器和耳机）中的常时等量功能。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。

XenApp 和 XenDesktop 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
配置 Bloomberg 键盘。有关为其他专用 USB 设备配置策略规则的信息，请参阅知识中心文章
CTX122615

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 设备可远程连接，但集线器本身无法远程连接。

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

有关自动重定向特定 USB 设备的说明，请参阅知识中心文章 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
默认情况下启用	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。新式音频设备通常使用常时等量传输，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。有关详细信息，请参阅知识中心文章 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。

> 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。有关此内容的说明，请参阅知识中心文章 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。某些视频设备（例如具有运动检测功能的网络摄像机）需要进行额外配置。有关此内容的说明，请参阅知识中心文章 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，如蓝牙键盘或鼠标。

  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 Citrix Receiver for Windows 模板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 Citrix Receiver for Windows 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：
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\GenericUSB Type=String Name=”DeviceRules” Value=
** 小心 **：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。
产品默认规则的存储位置为：
HKEY_LOCAL_MACHINE\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，请参阅知识中心文章 [CTX119722](https://support.citrix.com/article/CTX119722/)。
按用户配置 USB 音频
Citrix 建议使用组策略对象 receiver.admx/receiver.adml 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 receiver.admx 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 for Windows 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。

** 注意 **：此功能仅在 XenApp 服务器上可用。

按用户配置 USB 音频设备

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 receiver 模板导入到组策略编辑器中，可以忽略步骤 2 到 5。

1. 在组策略编辑器的左窗格中，选择管理模板文件夹。

1. 在 ** 操作 ** 菜单中，选择 ** 添加/删除模板 **。

1. 选择 ** 添加 ** 并浏览到 Receiver 的 Configuration 文件夹（对于 32 位计算机，通常为 C:\Program Files\Citrix\ICA Client\Configuration；对于 64 位计算机，通常为 C:\Program Files (x86)\Citrix\ICA Client\Configuration），然后选择 receiver.admx。

1. 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。

1. 在“计算机配置”节点下，转至 ** 管理模板 > 经典管理模板 (ADM) > Citrix 组件 > Citrix Receiver > 用户体验 **，然后选择 ** 通过通用 USB 重定向实现音频 **。

1. 编辑设置。

1. 单击 ** 应用 ** 和 ** 确定 **。

1. 以管理员模式打开 cmd 提示符。

1. 运行以下命令

gpupdate /force

** 注意 **：任何策略更改均需要重新启动 XenApp 服务器，更改才能生效。

根驱动器 >

配置 **StoreFront**

March 26, 2019

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 Citrix Receiver for Windows 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，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）。

> 提示
>
> 在您选择用于显示所有应用商店的选项后，Citrix Receiver for Windows 偶尔会显示旧 StoreFront UI 而非更新的 StoreFront UI。

配置 **StoreFront**

请按照 StoreFront 文档中所述安装和配置 StoreFront。Citrix Receiver for Windows 需要 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 属性描述中设置一个注册表项。

> 注意：
>
> 对于需要更大控制权的管理员，Citrix 提供了一个模板，供您用于创建 Citrix Receiver for Windows 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 Citrix 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。

小心：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。

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。已发布桌面可以更改 Citrix Receiver for Windows 的行为。

Citrix Receiver for Windows 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 **Citrix Receiver for Windows** 的工作区控制

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

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

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

HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle（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。

通过 **CLI** 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。用户不必从 Citrix 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 Citrix 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”Citrix Receiver 界面，并将其替换为预配置的“开始”菜单。此标志称为 SelfServiceMode，且默认情况下设置为 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（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。

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 Citrix Receiver for Windows 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 Citrix Receiver for Windows。
- 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 [DESKTOPDIR=”Dir_name”] 标志，以便将所有快捷方式放置到单个文件夹中。桌面快捷方式支持类别路径。
- 自动重新安装修改后的应用程序是一项可以通过 AutoReInstallModifiedApps 注册表项启用的功能。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”。

通过注册表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。

小心：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。

> 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; HKLM\SOFTWARE\Citrix\Dazzle; HKCU\Software\Citrix\Dazzle; HKCU\Software\Citrix\Receiver\SR\Store” + primaryStoreID + \Properties

注册表名称	默认值	首选顺序位置
RemoveAppsOnExit	False	HKLM\SOFTWARE\Policies\Citrix\Dazzle; HKLM\SOFTWARE\Citrix\Dazzle; HKCU\Software\Citrix\Dazzle; HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties
PutShortcutsOnDesktop	False	HKCU\Software\Citrix\Receiver\SR\Store+Sto +\Properties; HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties; HKCU\Software\Citrix\Dazzle; HKLM\SOFTWARE\Policies\Citrix\Dazzle; HKLM \SOFTWARE\Citrix\Dazzle
PutShortcutsInStartMenu	True	HKCU\Software\Citrix\Receiver\SR\Store+Sto HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties; HKCU\Software\Citrix\Dazzle; HKLM\SOFTWARE\Policies\Citrix\Dazzle; HKLM\SOFTWARE\Citrix\Dazzle
SelfServiceMode	True	HKLM\SOFTWARE\Policies\Citrix\Dazzle; HKLM\SOFTWARE\Citrix\Dazzle
UseCategoryAsStartMenuPath	True	HKCU\Software\Citrix\Receiver\SR\Store+Sto +\Properties; HKCU\Software\Citrix\Receiver\SR\Store" + primaryStoreID + \Properties; HKCU\Software\Citrix\Dazzle; HKLM\SOFTWARE\Policies\Citrix\Dazzle; HKLM \SOFTWARE\Citrix\Dazzle

注册表名称	默认值	首选顺序位置
StartMenuDir	”“（空）	HKCU\Software\Citrix\Receiver\SR\Store+Sto +\Properties; HKCU\Software\Citrix\Receiver\SR\Store” + primaryStoreID + \Properties; HKCU\Software\Citrix\Dazzle; HKLM\SOFTWARE\Policies\Citrix\Dazzle; HKLM \SOFTWARE\Citrix\Dazzle
DesktopDir	”“（空）	HKCU\Software\Citrix\Receiver\SR\Store+Sto +\Properties; HKCU\Software\Citrix\Receiver\SR\Store” + primaryStoreID + \Properties; HKCU\Software\Citrix\Dazzle; HKLM\SOFTWARE\Policies\Citrix\Dazzle; HKLM\SOFTWARE\Citrix\Dazzle
AutoReinstallModifiedApps	True	HKCU\Software\Citrix\Receiver\SR\Store+Sto +\Properties; HKCU\Software\Citrix\Receiver\SR\Store” + primaryStoreID + \Properties; HKCU\Software\Citrix\Dazzle; HKLM\SOFTWARE\Policies\Citrix\Dazzle; HKLM\SOFTWARE\Citrix\Dazzle
HideEditStoresDialog	在 SelfServiceMode 中为 True，在 NonSelfServiceMode 中为 False	HKLM\SOFTWARE\Policies\Citrix\Dazzle; HKLM\SOFTWARE\Citrix\Dazzle; HKCU\Software\Citrix\Dazzle; HKCU\Software\Citrix\Receiver\SR\Store” + primaryStoreID + \Properties

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

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\Ci HKLM\SOFTWARE\Wow6432Node\Citrix\Dazz HKCU\Software\Citrix\Dazzle; HKCU\Software\Citrix\Receiver\SR\Store” + primaryStoreID + \Properties

注册表名称	默认值	首选顺序位置
RemoveAppsOnExit	False	HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM\SOFTWARE\Wow6432Node\Citrix\Dazz HKCU\Software\Citrix\Dazzle; HKCU\Software\Citrix\Receiver\SR\Store” + primaryStoreID + \Properties
PutShortcutsOnDesktop	False	HKCU\Software\Citrix\Receiver\SR\Store+Sto +\Properties; HKCU\Software\Citrix\Receiver\SR\Store” + primaryStoreID + \Properties; HKCU\Software\Citrix\Dazzle; HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM \SOFTWARE\Wow6432Node\Citrix\Dazzle
PutShortcutsInStartMenu	True	HKCU\Software\Citrix\Receiver\SR\Store+Sto HKCU\Software\Citrix\Receiver\SR\Store” + primaryStoreID + \Properties; HKCU\Software\Citrix\Dazzle; HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM\SOFTWARE\Wow6432Node\Citrix\Dazz
SelfServiceMode	True	HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM\SOFTWARE\Wow6432Node\Citrix\Dazz
UseCategoryAsStartMenuPath	True	HKCU\Software\Citrix\Receiver\SR\Store+Sto +\Properties; HKCU\Software\Citrix\Receiver\SR\Store” + primaryStoreID + \Properties; HKCU\Software\Citrix\Dazzle; HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM \SOFTWARE\Wow6432Node\Citrix\Dazzle

注册表名称	默认值	首选顺序位置
StartMenuDir	”“（空）	HKCU\Software\Citrix\Receiver\SR\Store+Sto +\Properties; HKCU\Software\Citrix\Receiver\SR\Store” + primaryStoreID + \Properties; HKCU\Software\Citrix\Dazzle; HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM \SOFTWARE\Wow6432Node\Citrix\Dazzle
DesktopDir	”“（空）	HKCU\Software\Citrix\Receiver\SR\Store+Sto +\Properties; HKCU\Software\Citrix\Receiver\SR\Store” + primaryStoreID + \Properties; HKCU\Software\Citrix\Dazzle; HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM\SOFTWARE\Wow6432Node\Citrix\Dazz
AutoReinstallModifiedApps	True	HKCU\Software\Citrix\Receiver\SR\Store+Sto +\Properties; HKCU\Software\Citrix\Receiver\SR\Store” + primaryStoreID + \Properties; HKCU\Software\Citrix\Dazzle; HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM\SOFTWARE\Wow6432Node\Citrix\Dazz
HideEditStoresDialog	在 SelfServiceMode 中为 True， 在 NonSelfServiceMode 中为 False	HKLM\SOFTWARE\Wow6432Node\Policies\Ci HKLM\SOFTWARE\Wow6432Node\Citrix\Dazz HKCU\Software\Citrix\Dazzle; HKCU\Software\Citrix\Receiver\SR\Store” + primaryStoreID + \Properties

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

使用图形用户界面配置应用程序显示

注意：只能设置已订阅应用程序和桌面的快捷方式。

1. 登录 Citrix Receiver for Windows。
2. 右键单击通知区域中的 Citrix Receiver for Windows 图标，然后单击高级首选项。
   此时将显示“高级首选项”窗口。
3. 单击设置选项。

   注意：默认情况下，会选中“在开始菜单中显示应用程序”选项。
4. 指定文件夹名称。这会将所有已订阅应用程序移动到“开始”菜单中的指定文件夹。应用程序可以同时添加到“开始”菜单中的新文件夹或现有文件夹。启用此功能后，现有应用程序和新添加的应用程序都会被添加到指定文件

夹。

5. 选中桌面选项窗格下的在桌面上显示应用程序复选框。
6. 指定文件夹名称。这会将所有已订阅应用程序移动到本地桌面上的指定文件夹。
7. 选中类别选项下的为开始菜单和桌面启用不同路径复选框。这会按照应用程序属性服务器中定义的方式创建应用程序的快捷方式和类别文件夹。例如，IT 应用程序、财务应用程序

   注意：默认情况下，会选择“类别为“开始”菜单路径”选项。

   a) 选择类别为 **“开始”** 菜单路径以按照应用程序属性服务器中定义的方式在 Windows“开始”菜单中显示已订阅的应用程序及其类别文件夹。
   b) 选择类别为桌面路径以按照应用程序属性服务器中定义的方式在本地桌面中显示已订阅应用程序及其类别文件夹。
8. 单击确定。

使用图形用户界面配置重新连接选项

登录到服务器后，用户可以随时重新连接到所有桌面或应用程序。默认情况下，单击“重新连接”选项将打开已断开连接的桌面或应用程序，以及当前正在另一个客户端设备上运行的任何桌面或应用程序。可以将“重新连接”选项配置为仅重新连接用户先前断开连接的桌面或应用程序。

1. 登录 Citrix Receiver for Windows。
2. 右键单击系统托盘中的 Citrix Receiver for Windows 图标，然后单击高级首选项。将显示高级首选项窗口。
3. 单击设置选项。
4. 单击重新连接选项。
5. 选择 **Enable for Workspace Control Support**（启用以实现工作区控制支持）以允许用户随时重新连接到所有桌面或应用程序。

   a) 选择重新连接到所有活动会话和断开连接的会话以允许用户重新连接到活动会话和已断开连接的会话。

   b) 选择仅重新连接到已断开的会话以允许用户仅重新连接到已断开的会话。

   注意：受支持的重新连接模式采用在 GPO 中设置的值。用户可以修改此选项，方法是导航到管理模板 **> Citrix** 组件 **> Citrix Receiver >** 自助服务 **>** 控制 **Receiver** 尝试重新连接到现有会话的时间。

   要通过注册表修改此选项，请参阅知识中心文章 CTX136339。
6. 单击确定。

使用命令行接口隐藏 **“**设置选项**”**

选项	/DisableSetting
说明	禁止“设置选项”显示在“高级首选项”对话框中。
示例用法	CitrixReceiver.exe /DisableSetting=3

如果想在“设置选项”中同时显示“应用程序显示”和“重新连接选项”。	输入 CitrixReceiver.exe /DisableSetting=0
如果想在“高级首选项”对话框中隐藏“设置选项”	输入 CitrixReceiver.exe /DisableSetting=3
如果希望“设置选项”仅显示“应用程序显示”	输入 CitrixReceiver.exe /DisableSetting=2
如果希望“设置选项”仅显示“重新连接选项”	输入 CitrixReceiver.exe /DisableSetting=1

配置组策略对象管理模板

March 26, 2019

Citrix 建议使用 Windows 组策略对象编辑器配置 Citrix Receiver for Windows。Citrix Receiver for Windows 在安装目录中包括管理模板文件（receiver.adm 或 receiver.admx\receiver.adml，具体取决于操作系统）。

注意：

- 自 Citrix Receiver for Windows 4.6 起，安装目录包括 CitrixBase.admx 和 CitrixBase.adml 文件。Citrix 建议您使用 CitrixBase.admx 和 CitrixBase.adml 文件以确保选项在组策略对象编辑器中正确组织并显示。
- .adm 文件仅供 Windows XP 嵌入式平台使用。.admx/.adml 文件供 Windows Vista/Windows Server 2008 以及所有更高版本的 Windows 使用。
- 如果 Citrix Receiver for Windows 是随 VDA 安装的，则会在 Citrix Receiver for Windows 安装目录中找到 admx/adml 文件。例如：\Online Plugin\Configuration。安装目录 >
- 如果安装 Citrix Receiver for Windows 时未安装 VDA，则通常可在 C:\Program Files\Citrix\ICA Client\Configuration 目录中找到 admx/adml 文件。

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。

注意：

Citrix 建议您使用随最新的 Citrix Receiver for Windows 提供的 GPO 模板文件。

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

注意：

- 如果未将 CitrixBase.admx\adml 添加到本地 GPO，启用 ICA 文件签名策略可能会丢失。
- 升级 Citrix Receiver for Windows 时，必须如下文的过程中所述将最新的模板文件添加到本地 GPO 中。导入最新的文件时，将保留之前的设置。

要向本地 **GPO** 中添加 **receiver.adm** 模板文件（仅限 **Windows XP** 嵌入式操作系统），请执行以下操作：

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 Citrix Receiver for Windows 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”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**。

将.adm 模板文件添加到本地 GPO 后，将显示以下消息：
“[strings] 部分中的以下条目太长，已被截断:”
单击确定可忽略该消息。

要向本地 **GPO** 中添加 **receiver.admx/adml** 模板文件（更高版本的 **Windows** 操作系统），请执行以下操作：

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。

1. 安装 Citrix Receiver for Windows 之后，复制模板文件。

   admx:

   从：\ICA Client\Configuration\receiver.admx 安装目录 >

   到：%systemroot%\policyDefinitions

   从：\ICA Client\Configuration\CitrixBase.admx 安装目录 >

   到：%systemroot%\policyDefinitions

   adml:

   从：\ICA Client\Configuration\\[MUIculture]receiver.adml 安装目录 >

   到：%systemroot%\policyDefinitions\[MUIculture]

   从：\ICA Client\Configuration\\[MUIculture]\CitrixBase.adml 安装目录 >

   到：%systemroot%\policyDefinitions\[MUIculture]

   注意：
   仅当用户将 CitrixBase.admx/CitrixBase.adml 添加到 \ policyDefinitions 文件夹时，Citrix Receiver for Window 模板文件才可以在 “管理模板”>“Citrix 组件”>“Citrix Receiver” 文件夹中的本地 GPO 中找到。

向用户提供帐户信息

March 26, 2019

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
- 向用户提供预配文件
- 向用户提供需手动输入的帐户信息。

> 重要
>
> Citrix 建议您在安装后重新启动 Citrix Receiver for Windows。这样可确保用户能够添加帐户，并且 Citrix Receiver for Windows 能够发现在安装过程中处于暂停状态的 USB 设备。

此时将显示一个指示安装成功的对话框，然后显示添加帐户对话框。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。

隐藏 “添加帐户” 对话框

添加帐户对话框在应用商店未配置时会显示出来。用户可以使用此窗口通过输入电子邮件地址或服务器 URL 设置一个 Citrix Receiver 帐户。

Citrix Receiver for Windows 会确定与该电子邮件地址相关联的是 NetScaler Gateway、StoreFront 服务器还是 AppController 虚拟设备，然后提示用户登录以获取枚举。

可以按以下方法隐藏“添加帐户”对话框：

1. 在系统登录处

   选择登录时不自动显示此窗口以防止“添加帐户”窗口在进行后续登录时弹出。

   此设置特定于每个用户，并且会在 Citrix Receiver for Windows 重置操作过程中重置。

2. 命令行安装

   以管理员身份使用命令行接口，通过以下开关安装 Citrix Receiver for Windows：
   CitrixReceiver.exe /ALLOWADDSTORE=N。
   这是按计算机进行的设置；因此该行为应当适用于所有用户。

   未配置应用商店时会显示以下消息。

   此外，可以按以下方法隐藏“添加帐户”对话框。

注意： Citrix 建议用户使用系统登录或命令行接口方法隐藏“添加帐户”对话框。

- 重命名 **Citrix** 执行文件：
  将 **CitrixReceiver.exe** 重命名为 **CitrixReceiverWeb.exe** 以更改“添加帐户”对话框的行为。通过重命名文件，“添加帐户”对话框将无法通过“开始”菜单进行显示。
  有关 Citrix Receiver for Web 的详细信息，请参阅从 Receiver for Web 部署 Receiver for Windows
- 组策略对象：
  要在 Citrix Receiver for Windows 安装向导中隐藏“添加帐户”按钮，请按如下所示，在本地组策略编辑器中的“自助服务”节点下禁用 **EnableFTUpolicy**。
  这是按计算机进行的设置；因此该行为应当适用于所有用户。
  要加载模板文件，请参阅使用组策略对象模板配置 Receiver。

配置基于电子邮件的帐户发现

配置 Citrix Receiver for Windows 以实现基于电子邮件的帐户发现时，首次安装并配置 Citrix Receiver for Windows 过程中，用户需要输入自己的电子邮件地址（而非服务器 URL）。Citrix Receiver for Windows 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 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。

向用户提供预配文件

StoreFront 提供预配文件，用户可以打开这些预配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预配文件。将这些文件提供给用户，以便用户能够自动配置 Citrix Receiver for Windows。安装 Citrix Receiver for Windows 之后，用户只需打开文件即可配置 Citrix Receiver for Windows。如果您配置了 Citrix Receiver for Web 站点，用户还可以从这些站点获取 Citrix Receiver for Windows 预配文件。

- 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 才能访问 SalesApps，或者输入 server2.com?HRApps 才能访问 HRApps。此功能需要首次使用的用户通过输入 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，Citrix Receiver for Windows 将尝试验证连接。如果验证成功，Citrix Receiver for Windows 将提示用户登录到该帐户。

要管理帐户，Citrix Receiver 用户可以打开 Citrix Receiver for Windows 主页，单击，然后单击帐户。

自动共享多个应用商店帐户

> 警告
>
> 注册表编辑器使用不当可能导致严重问题，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 Citrix Receiver for Windows 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

配置自动更新

March 26, 2019

从 Citrix Receiver for Windows 配置自动更新时，请遵照优先级顺序按照下面的方法进行操作：

1. 组策略对象管理模板
2. 命令行接口
3. 高级首选项（每用户）

使用组策略对象管理模板配置

1. 以管理员身份通过运行 gpedit.msc 打开 Citrix Receiver 组策略对象管理模板。
    - 要在单台计算机上应用该策略，请从“开始”菜单中启动 Citrix Receiver 组策略对象管理模板。
    - 如果要在某个域中应用该策略，请使用组策略管理控制台启动 Citrix Receiver 组策略对象管理模板。
2. 在“计算机配置”节点下，转至管理模板 > **Citrix** 组件 > **Citrix Receiver** > 自动更新。
3. 选择设置检查更新的延迟策略。此策略允许您暂缓推出一段时间。
4. 选择已启用，然后从延迟组下拉菜单中，选择以下选项之一：
    - 快 - 在交付期限的初期推出更新。
    - 中 - 在交付期限的中期推出更新。
    - 慢 - 在交付期限的末期推出更新。
5. 单击应用和确定保存此策略。

6. 在“自动更新模板”部分中，选择启用或禁用自动更新策略。
7. 选择已启用并根据需要设置值：
   - 从启用自动更新策略下拉列表中，选择以下选项之一：
     - 自动 - 系统将在有可用更新时向您发出通知（默认设置）。
     - 手动 - 系统在有可用更新时不向您发出通知。手动检查更新。
   - 选择仅限 **LTSR** 以仅获取 LTSR 的更新。
   - 从 **auto-update-DeferUpdate-Count** 下拉列表中，选择一个介于 **-1** 到 **30** 之间的值，其中
     - **-1** - 指示您可以将通知推迟任意次数（默认值 = -1）。
     - **0** - 指示不显示以后提醒我选项。
     - 任何其他数值 - 指示显示以后提醒我选项该次数。例如，如果将该值设置为 10，以后提醒我选项将显示 10 次。
8. 单击应用和确定保存此策略。

使用命令行接口配置

安装 **Citrix Receiver for Windows** 时

要在 Citrix Receiver 安装过程中以管理员身份使用命令行设置配置自动更新设置，请执行以下操作：

- **/AutoUpdateCheck=** auto/manual/disabled
- **/AutoUpdateStream=** LTSR/Current。其中，LTSR 是指长期服务版本，Current 是指当前版本。
- **/DeferUpdateCount=** 介于 -1 到 30 之间的任意值
- **/AURolloutPriority=** auto/fast/medium/slow

例如：*CitrixReceiver.exe / AutoUpdateCheck=auto /AutoUpdateStream= Current /DeferUpdateCount=-1 / AURolloutPriority= fast*

- 要在 Citrix Receiver 安装过程中以用户身份使用命令行设置配置自动更新设置，请执行以下操作：
  - **/AutoUpdateCheck=auto/manual**

例如：*CitrixReceiver.exe / AutoUpdateCheck=auto*

使用组策略对象管理模板编辑自动更新设置将替换在所有用户的 Citrix Receiver for Windows 安装过程中应用的设置。

完成 **Citrix Receiver for Windows** 安装后

可以在安装 Citrix Receiver for Windows 后配置自动更新。

使用命令行：

打开 Windows 命令提示窗口，并将目录更改到 **CitrixReceiverUpdater.exe** 所在位置。CitrixReceiverUpdater.exe 通常位于 *CitrixReceiverInstallLocation*\Citrix\Ica Client\Receiver 下。

也可以使用此二进制文件设置自动更新命令行策略。

例如：管理员可以使用全部四个选项：

- CitrixReceiverUpdater.exe */AutoUpdateCheck=auto /AutoUpdateStream= STSR /DeferUpdateCount=-1 / AURolloutPriority= fast*

使用图形用户界面配置

个人用户可以使用高级首选项对话框覆盖自动更新设置。这是一项基于用户的配置，并且这些设置仅适用于当前用户。

1. 右键单击通知区域中的 Citrix Receiver for Windows。
2. 选择高级首选项并单击自动更新。

   此时将显示自动更新对话框。
3. 选择以下选项之一：
   - 是，通知我
   - 否，不要通知我
   - 使用管理员指定的设置
4. 单击保存。

使用 **StoreFront** 配置自动更新

1. 使用文本编辑器打开 web.config 文件，该文件通常位于 C:\inetpub\wwwroot\Citrix\Roaming 目录中。
2. 在该文件中找到用户帐户元素（您的部署的帐户名称为 Store）

   例如：<account id=… name=”Store”>

   在 *</account>* 标记之前，导航到该用户帐户的属性：

   <properties>
   <clear />
   </properties>
3. 在 *<clear />* 标记后面添加自动更新标记。

```
<account>

    <clear />

    <account id=”d1197d2c-ac82-4f13-9346-2ee14d4b0202” name=”F84Store”

      description=”” published=”true” updaterType=”Citrix”
         remoteAccessType=”None”>
```



```
8
9         <annotatedServices>
10
11           <clear />
12
13           <annotatedServiceRecord serviceRef="1__Citrix_F84Store">
14
15             <metadata>
16
17               <plugins>
18
19                 <clear />
20
21               </plugins>
22
23               <trustSettings>
24
25                 <clear />
26
27               </trustSettings>
28
29               <properties>
30
31                 <property name="Auto-Update-Check" value="auto" />
32
33                 <property name="Auto-Update-DeferUpdate-Count" value="1"
                       />
34
35                       <property name="Auto-Update-LTSR-Only" value="
                          FALSE" />
36
37                 <property name="Auto-Update-Rollout-Priority" value="fast
                       " />
38
39                    </properties>
40
41             </metadata>
42
43           </annotatedServiceRecord>
44
45         </annotatedServices>
46
47         <metadata>
48
49           <plugins>
```

```
50
51            <clear />
52
53          </plugins>
54
55          <trustSettings>
56
57            <clear />
58
59          </trustSettings>
60
61          <properties>
62
63            <clear />
64
65          </properties>
66
67        </metadata>
68
69      </account>
```

auto-update-Check

指示 Citrix Receiver for Windows 在有可用更新时进行检测。

有效值包括：

- 自动 - 系统将在有可用更新时向您发出通知（默认设置）。
- 手动 - 系统在有可用更新时不向您发出通知。手动检查更新。
- 已禁用 – 禁用自动更新

auto-update-LTSR-Only

指示 Citrix Receiver for Windows 必须仅接受 LTSR 的更新。

有效值包括：

- True – 自动更新仅检查 Citrix Receiver for Windows 的 LTSR 更新
- False – 自动更新还检查 Citrix Receiver for Windows 的非 LTSR 更新。

auto-update-DeferUpdate-Count

指示可以推迟通知的次数。以后提醒我选项在设置次数值中显示。

有效值包括：

- -1 - 指示您可以将通知推迟任意次数（默认值 = -1）。
- 0 - 指示不显示以后提醒我选项。
- 任何其他数值 - 指示显示“以后提醒我”选项该次数。例如，如果将该值设置为 10，以后提醒我选项将显示 10 次。

auto-update-Rollout-Priority：

指示可以为推出设置的时间期限。

有效值包括：

- 快 - 在交付期限的初期推出更新。
- 中 - 在交付期限的中期推出更新。
- 慢 - 在交付期限的末期推出更新。

限制：

1. 您的系统必须有权访问 Internet。
2. Receiver for Web 用户不能自动下载 StoreFront 策略。
3. 如果您配置了截获出站代理的 SSL，则必须添加 Receiver 自动更新签名服务 `https://citrixupdates.cloud.com` 和下载位置 `https://downloadplugins.citrix.com` 的例外。
4. 默认情况下，自动更新功能在 VDA 上处于禁用状态。这包括 RDS 多用户服务器计算机、VDI 和 RemotePC 计算机。
5. 自动更新功能在安装了 Desktop Lock 的计算机上处于禁用状态。

优化环境

November 19, 2018

您可以优化环境：

- 缩短应用程序启动时间
- 简化设备与已发布的资源的连接
- 支持 DNS 名称解析
- 将代理服务器与 XenDesktop 连接结合使用
- 启用对匿名应用程序的访问
- 检查单点登录配置

缩短应用程序启动时间

November 19, 2018

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 Citrix Receiver for Windows 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 Citrix Receiver for Windows 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。

小心：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。

注册表位置为：

HKEY_LOCAL_MACHINE\Software[Wow6432Node]Citrix\Dazzle

HKEY_CURRENT_USER\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 Citrix Receiver for Windows 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 receiver.admx 文件自定义预启动功能。但是，可以通过在安装 Citrix Receiver for Windows 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。

HKEY_LOCAL_MACHINE 注册表值

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

对于所有其他受支持的 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 到下午 1:45 之间启动。

HKEY_CURRENT_USER 注册表值

HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Prelaunch

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

映射客户端设备

January 7, 2019

Citrix Receiver for Windows 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，Citrix Receiver for Windows 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 Server Manager 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 Citrix Receiver for Windows 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
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 Citrix 产品文档中的 XenDesktop 或 XenApp 文档。

HDX Plug and Play USB 设备重定向

更新时间：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 Citrix Receiver for Windows 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。

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 Citrix Receiver for Windows。
3. 在命令提示窗口中，键入：

   net use comx:\\client\comz:。

   其中，x 为服务器上的 COM 端口号（端口 1 到 9 可用于映射），z 为要映射的客户端 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，请将您的用户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，就如同在使用用户设备上的 COM 端口一样。

支持 **DNS** 名称解析

November 19, 2018

对于使用 Citrix XML Service 的 Citrix Receiver for Windows，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 Citrix Receiver for Windows 也使用 Citrix XML Service。对于通过 Web Interface 连接的 Citrix Receiver for Windows，由 Web 服务器代表 Citrix Receiver for Windows 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 Citrix Receiver for Windows 上处于启用状态。如果在服务器场中禁用了 DNS 名称解析，则 Citrix Receiver for Windows 的任何 DNS 名称请求都将返回一个 IP 地址。在 Citrix Receiver for Windows 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。

小心：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\I
   Client\Engine\Lockdown Profiles\All Regions\Lockdown\Application Browsing 中。
2. 将值设置为 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** 结合使用

February 21, 2019

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。更多信息，请参阅 Web Interface 文档。

使用配置检查器验证 **Single Sign-On** 配置

November 19, 2018

从 Citrix Receiver for Windows 4.5 开始，用户可使用配置检查器运行测试，以确保正确配置 Single Sign-On。该测试在 Single Sign-On 的不同检查点运行，并显示配置结果。

1. 登录 Citrix Receiver for Windows。
2. 右键单击通知区域中的 Citrix Receiver for Windows 并选择高级首选项。此时将显示“高级首选项”窗口。
3. 选择配置检查器。此时将显示 Citrix 配置检查器窗口。
4. 从选择窗格中选择 **SSONChecker**。
5. 单击运行。将显示一个进度条，显示测试的状态。

配置检查器窗口包含以下列：

1. 状态：显示特定检查点的测试结果。
    - 绿色复选标记表明该特定检查点配置正确。
    - 蓝色的 “I” 指示有关检查点的信息。
    - • 红色的 “X” 指示该特定检查点配置不正确。
2. 提供程序：显示在其上运行测试的模块的名称。在本案例中，为 Single Sign-On。
3. 套件：指示测试的类别。例如，安装。
4. 测试：指示运行的具体测试的名称。
5. 详细信息：提供有关测试的其他信息，无论通过还是未通过。用户获得有关每个检查点和相应结果的详细信息。

需要执行以下测试：

1. 已随 Single Sign-On 安装
2. 登录凭据捕获
3. 网络提供程序注册：只有将 “Citrix Single Sign-On” 设置为网络提供程序列表中的第一个时，针对网络提供程序注册的测试结果才会显示一个绿色复选标记。如果 Citrix Single Sign-On 显示在列表中的任何其他位置，则针对网络提供程序注册的测试结果会显示一个蓝色的 “I”，并包含其他信息。
4. Single Sign-On 进程正在运行
5. 组策略：默认情况下，此策略配置在客户端上。
6. Internet 的安全区域设置：确保将 Store/XenApp Service URL 添加到 “Internet 选项” 中的安全区域列表中。如果通过组策略配置安全区域，策略中出现任何更改时，都需要重新打开高级首选项窗口才能使更改生效，同时显示测试的正确状态。
7. 适用于 Web Interface/StoreFront 的身份验证方法。

注意：如果用户正访问 Receiver for Web，则测试结果不适用。
如果 Citrix Receiver for Windows 配置有多个应用商店，则会在所有已配置的应用商店上运行身份验证方法测试。

注意：测试结果可以另存为报告，且默认的报告格式是.txt。

隐藏 **“高级首选项”** 窗口中的 **“配置检查器”** 选项：

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。
2. 在组策略编辑器中，转至 **Citrix** 组件 > **Citrix Receiver** > 自助服务 > **DisableConfigChecker**。
3. 选择已启用。
   这会隐藏高级首选项窗口中的 “配置检查器” 选项。
4. 单击应用和确定。
5. 打开命令提示窗口。
6. 运行 gpupdate /force 命令。

要使所做的更改生效，请关闭并重新打开“高级首选项”对话框。

限制：

配置检查器不包括 XenApp/XenDesktop 服务器上“信任发送到 XML Service 的请求”配置的检查点。

改善用户体验

March 26, 2019

可以通过以下功能改善用户体验：

配置通用客户端输入法编辑器 (IME)

使用命令行接口配置通用客户端 IME

要启用通用客户端 IME，请从 Citrix Receiver for Windows 安装文件夹 (C:\Program Files (x86)\Citrix\ICA Client) 运行 **wfica32.exe /localime:on** 命令。

> 注意
>
> 可以使用命令行开关 **wfica32.exe /localime:on** 启用通用客户端 IME 和键盘布局同步。

要禁用通用客户端 IME，请从 Citrix Receiver for Windows 安装文件夹 (C:\Program Files (x86)\Citrix\ICA Client) 运行 **wfica32.exe /localgenericime:off** 命令。此命令不影响键盘布局同步设置。

如果使用命令行接口禁用了通用客户端 IME，则可以通过运行 **wfica32.exe /localgenericime:on** 命令再次启用该功能。

切换：

Citrix Receiver for Windows 在此版本中支持切换功能。可以运行 **wfica32.exe /localgenericime:on** 命令来启用或禁用该功能。但是，键盘布局同步设置的优先级高于切换开关。如果键盘布局同步设置为关，切换将不启用通用客户端 IME。

使用图形用户界面配置通用客户端 IME

通用客户端 IME 需要 VDA 7.13 或更高版本。

可以通过启用键盘布局同步来启用通用客户端 IME 功能。有关详细信息，请参阅 键盘布局同步。

Citrix Receiver for Windows 允许您配置不同的选项来启用通用客户端 IME。可以根据您的要求和使用情况从这些选项中进行选择。

1. 在活动的应用程序会话中，右键单击通知区域中的 Citrix Receiver 图标并选择连接中心。

2. 选择首选项并单击本地 **IME**。

下面的选项可用来支持不同的 IME 模式：

1. 启用服务器 **IME** - 选择此选项将禁用本地 IME。此选项意味着只能使用在服务器上设置的语言。
2. 将本地 **IME** 设置为高性能模式 – 选择此选项将在带宽有限的情况下使用本地 IME。此选项将显示候选窗口功能。
3. 将本地 **IME** 设置为最佳体验模式 – 选择此选项将在实现最佳用户体验的情况下使用本地 IME。此选项占用高带宽。默认情况下，在启用了通用客户端 IME 时选择此选项。

设置中的更改仅在当前会话中应用。

使用注册表编辑器启用热键配置

启用了通用客户端 IME 时，可以使用 **Shift+F4** 热键选择不同的 IME 模式。IME 模式的不同选项在会话的右上角显示。

默认情况下，通用客户端 IME 的热键处于禁用状态。

在注册表编辑器中，导航到 HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Keys。

选择 **AllowHotKey** 并将默认值更改为 1。

> 注意
>
> 热键功能在桌面和应用程序会话中受支持。

限制：

1. 通用客户端 IME 不支持 Search UI 等 UWP（通用 Windows 平台）应用程序以及 Windows 10 操作系统的 Edge 浏览器。解决方法：改为使用服务器 IME。
2. 通用客户端 IME 在处于保护模式的 Internet Explorer 11 中不受支持。解决方法：可以使用 **Internet** 选项禁用保护模式。为此，请单击安全并取消选中启用保护模式。

键盘布局

键盘布局同步允许用户在客户端设备上的首选键盘布局之间切换。默认情况下，此功能处于禁用状态。

要启用键盘布局同步，请执行以下操作：

1. 在 Citrix Receiver for Windows 通知区域图标中，选择高级首选项 > 本地键盘布局设置 > 是。
2. 单击保存。

可以通过选择否禁用该功能。

还可以通过命令行启用和禁用键盘布局同步，方法是从 Citrix Receiver for Windows 安装文件夹 (C:\program files (x86)\Citrix\ICA Client) 运行 **wfica32:exe /localime:on** 或 **wfica32:exe /localime:off**。

注意：使用本地键盘布局选项将激活客户端 IME（输入法编辑器）。如果使用日语、中文或韩语工作的用户偏向于使用服务器 IME，则必须通过选择否或运行 **wfica32:exe /localime:off** 禁用本地键盘布局选项。连接到下一个会话时，会话将还原为远程服务器提供的键盘布局。

有时，切换客户端键盘布局在活动会话中不起作用。要解决此问题，请从 Citrix Receiver for Windows 中注销并重新登录。

限制：

- 使用提升的权限（例如，右键单击某个应用程序图标 > 以管理员身份运行）运行的远程应用程序无法与客户端键盘布局同步。要解决此问题，请手动更改服务器端 (VDA) 上的键盘布局或者禁用 UAC。
- 如果用户将客户端上的键盘布局更改为服务器上不支持的布局，由于安全原因，将禁用键盘布局同步功能 - 无法识别的键盘布局将被视为潜在的安全威胁。要恢复键盘布局同步功能，用户应注销并重新登录到会话。
- RDP 作为应用程序部署时，如果用户在 RDP 会话中工作，则无法使用 Alt + Shift 快捷方式更改键盘布局。要解决此问题，用户可以使用 RDP 会话中的语言栏切换键盘布局。
- 由于存在可能会引入性能风险的第三方问题，此功能在 Windows Server 2016 中处于禁用状态。可以通过 VDA 上的注册表设置启用此功能：在 HKLM\Software\Citrix\ICA\IcaIme 中，添加一个名为 DisableKeyboardSync 的新注册表项并将值设置为 0。

> 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。

相对鼠标

相对鼠标支持提供了用于以相对方式而非绝对方式来解释鼠标位置的选项。需要相对鼠标输入而非绝对鼠标输入的应用程序需要启用此功能。

注意： 此功能仅在已发布桌面会话中使用。

启用相对鼠标支持

1. 登录 Citrix Receiver for Windows
2. 启动已发布桌面会话
3. 从 Desktop Viewer 工具栏中，选择首选项。
   将显示 “Citrix Receiver - 首选项” 窗口。
4. 选择 “连接”。
5. 在 “相对鼠标设置” 下，启用使用相对鼠标。
6. 单击应用和确定。

注意：这是一个“按会话”实现的功能。在重新连接到已断开连接的会话后，该功能将不再可用。用户必须在每次连接或重新连接到已发布桌面时重新启用该功能。

硬件解码

使用 Citrix Receiver for Windows（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 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，未针对嵌入式 GPU 启用此功能。

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 >

> 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，并且其中一个显示器在第二个 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。

客户端麦克风输入

Citrix Receiver for Windows 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。

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

多显示器支持

最多可以将八个显示器与 Citrix Receiver for Windows 结合使用。

多显示器配置中的每个显示器各自具有制造商所设计的分辨率。在会话期间，显示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显示器进行：

- 全屏模式，会话中显示多个显示器，应用程序如同在本地一样显示到这些显示器中。

  XenDesktop：要跨任何一部分矩形排列的显示器显示 Desktop Viewer 窗口，请跨这些显示器的任意部分调整窗口的大小，然后按最大化。

- 窗口模式，会话中显示单个显示器图像，应用程序不会显示到各个显示器中。

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，该桌面会跨相同的显示器显示。如果显示器按矩形排列，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显示器，该显示器将成为会话中的主显示器。否则，会话中编号最小的显示器将成为主显示器。

要启用多显示器支持，请确保满足以下各项：

- 用户设备配置为支持多个显示器。
- 用户设备的操作系统必须能够检测到每个显示器。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设置对话框中的设置选项卡，确认每个显示器都单独显示出来。
- 检测到显示器之后：
  - **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”来配置图形内存限制。
    * 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，适合指定大小的已发布应用程序会限制在一部分显示器内。

有关为 XenApp 和 XenDesktop 计算会话图形内存要求的信息，请参阅知识中心文章 CTX115637。

设备上的打印机设置替代

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。

屏幕键盘控制

Citrix Receiver for Windows 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，Citrix Receiver for Windows 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时禁止显示屏幕键盘，请在 HKEY_CURRENT_USER\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 HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver 中创建该值。

可以将这些注册表项设置为 3 种不同的模式，如下所示：

- **Automatic**（自动）：AlwaysKeyboardPopup = 0，DisableKeyboardPopup = 0
- **Always popup**（总是弹出）（屏幕键盘）：AlwaysKeyboardPopup = 1，DisableKeyboardPopup = 0
- **Never popup**（从不弹出）（屏幕键盘）：AlwaysKeyboardPopup = 0，DisableKeyboardPopup = 1

键盘快捷方式

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 Citrix Receiver for Windows 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 Citrix Receiver for Windows 模板文件。
   注意：根据 Windows 操作系统的版本，选择 Citrix Receiver for Windows 模板文件（receiver.adm 或 receiver.admx/receiver.adml）。
5. 选择打开以添加模板，然后选择“关闭”以返回到组策略编辑器。
6. 在组策略编辑器中，依次展开“管理模板”>“经典管理模板 (ADM)”>“Citrix 组件”>“Citrix Receiver”>“用户体验”>“键盘快捷方式”。

7. 在操作菜单中，依次选择属性、已启用，然后选择所需的选项。

Citrix Receiver for Windows 对 32 位色图标的支持

Citrix Receiver for Windows 支持 32 位增强色图标，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。

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

要设置首选的颜色深度，可以将名为 TWIDesiredIconColor 的字符串注册表项添加到 HKEY_LOCAL_MACHINE\SOFTWARE\Wo
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。

启用 Desktop Viewer

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 Citrix 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。在此访问方案中，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 for Windows 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。

Desktop Viewer 会话中的键盘输入

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

Ctrl+Alt+Delete 指向本地计算机。

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

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

Ctrl+Esc 发送到远程虚拟桌面。

注意：默认情况下，如果将 Desktop Viewer 最大化，Alt+Tab 将在会话内部的窗口之间切换焦点窗口。如果 Desktop Viewer 显示在某个窗口中，Alt+Tab 将在会话外部的窗口之间切换焦点窗口。

热键序列是由 Citrix 设计的键组合。例如，Ctrl+F1 序列将重现 Ctrl+Alt+Delete，Shift+F2 将在全屏模式和窗口模式之间切换应用程序。不能对 Desktop Viewer 中显示的虚拟桌面（即，对 XenDesktop 会话）使用热键序列，但可以对已发布的应用程序（即，对 XenApp 会话）使用热键序列。

连接到虚拟桌面

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。

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 HKEY_LOCAL_MACHINE\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。

> 小心：
>
> 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。

安全连接

August 7, 2018

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

March 26, 2019

有关配置域直通身份验证的信息，请参阅知识中心文章 CTX133982。

带有 **Single Sign-on** 的 **Citrix Receiver for Windows** 安装

安装 Citrix Receiver for Windows 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

要使用命令行界面启用域直通 (SSON) 身份验证，请执行以下操作：

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 应用商店的语法的信息，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 for Windows 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 for Windows；这等同于使用命令行开关 **/includeSSON** 安装 Citrix Receiver for Windows。

下图说明了如何启用 Single Sign-On：

> 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。

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

SSON 的组策略设置

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。

使用组策略对象管理模板配置 **SSON**

1. 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。
2. 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。
3. 重新启动端点设备（其上安装了 Citrix Receiver for Windows）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）。

启用 **Delivery Controller** 以信任 **XML**

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-PSSnapin 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。

在 **StoreFront** 和 **Web Interface** 上配置 **SSON**

StoreFront 配置

要在 StoreFront 和 Web Interface 上配置 SSON，请在 StoreFront 服务器上打开 Citrix 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 **>** 身份验证方法并启用直通。

使用 **Kerberos** 配置域直通身份验证

January 7, 2019

本主题仅适用于 Citrix Receiver for Windows 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 for Windows 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 for Windows、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 for Windows 的 Single Sign-On 服务捕获智能卡 PIN。
2. Citrix Receiver for Windows 使用 IWA (Kerberos) 向 StoreFront 验证用户身份。然后，StoreFront 向 Citrix Receiver for Windows 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，无需使用 Kerberos 身份验证。在 Citrix Receiver for Windows 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，Citrix Receiver for Windows 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 for Windows，请确保您的 Kerberos 配置符合以下条件。

- Kerberos 登录只在 Citrix Receiver for Windows 与属于相同或可信 Windows Server 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可能导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因注册表编辑器使用不当导致出现的问题能够得以解决。使用注册表编辑器需自担风险。请确保在编辑注册表之前进行备份。

配置域直通身份验证以结合使用 **Kerberos** 和智能卡

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

安装 Citrix Receiver for Windows 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 Citrix Receiver for Windows 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 Citrix Receiver for Windows：

  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 Citrix Receiver for Windows。

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 Citrix 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。

关于 **FastConnect API** 和 **HTTP Basic** 身份验证

FastConnect API 使用 HTTP Basic 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

March 26, 2019

Citrix 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 Citrix Receiver for Windows 配置。

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

  直通身份验证需要使用 StoreFront 和 Citrix Receiver for Windows 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）。必须为每个站点设置专用存储才允许使用此功能，并将 DisableCtrlAltDel 方法设置为 False 以允许智能卡。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 Citrix Receiver for Windows。要更改证书的选择方式，请配置 Citrix Receiver for Windows。
- 客户端证书身份验证 – 客户端证书身份验证需要使用 NetScaler Gateway 和 StoreFront 配置。
  - 要通过 NetScaler 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 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。
- Citrix Receiver for Windows 不保存用户证书选项，但是可以在配置时存储 PIN。PIN 仅在用户会话持续时间内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，Citrix 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，Citrix 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。
- Citrix 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可能导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因注册表编辑器使用不当导致出现的问题能够得以解决。使用注册表编辑器需自担风险。请确保在编辑注册表之前进行备份。

为智能卡身份验证启用 **Single Sign-On**

要配置 Citrix Receiver for Windows，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 Citrix Receiver for Windows 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 Citrix Receiver for Windows 身份验证管理器查找 Single Sign-On 组件，因此允许 Citrix Receiver for Windows 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 Citrix Receiver for Windows。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：

```
1  /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 Citrix Receiver for Windows 时允许 Citrix Receiver for Windows 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。

使用户设备支持使用智能卡

1. 将证书颁发机构根证书导入设备的密钥库。
2. eware。
3. 安装和配置 Citrix Receiver for Windows。

更改证书的选择方式

默认情况下，如果多个证书有效，则 Citrix Receiver for Windows 将提示用户从列表中选择证书。或者，可以将 Citrix Receiver for Windows 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 Citrix Receiver for Windows 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 Citrix Receiver for Windows 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。

使用 **CSP PIN** 提示

默认情况下，向用户显示的 PIN 提示由 Citrix Receiver for Windows 而不是智能卡加密服务提供程序 (CSP) 提供。Citrix Receiver for Windows 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 Citrix Receiver for Windows 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 Citrix Receiver for Windows 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：SmartCard-PINEntry=CSP。

启用证书吊销列表检查以提高安全性

November 19, 2018

启用证书吊销列表 (CRL) 检查功能后，Citrix 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 Citrix 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 Citrix Receiver for Windows 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 Citrix Receiver for Windows 模板文件。
   注意：根据 Windows 操作系统的版本，选择 Citrix Receiver for Windows 模板文件（receiver.adm 或 receiver.admx/receiver.adml）。
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。
     如果未设置 CRL 验证，则默认值为“仅检查本地存储的 CRL”。

安全通信

August 7, 2018

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

- Citrix NetScaler 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 Citrix Receiver for Windows 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。

Citrix Receiver for Windows 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 Microsoft 文档 上的 Windows 安全指南。

配置并启用 **TLS**

March 26, 2019

本主题适用于 XenApp 和 XenDesktop 7.6 及更高版本。

要对所有 Citrix Receiver for Windows 通信使用 TLS 加密，请配置用户设备、Citrix Receiver for Windows 以及运行 Web Interface 的服务器（如果使用 Web Interface）。有关确保 StoreFront 通信安全的信息，请参阅 StoreFront 文档中安全部分。有关详细信息，请参阅 Web Interface 文档。

必备条件：

用户设备必须满足在系统要求中指定的要求。

使用此策略可配置用于确保 Citrix Receiver for Windows 能够安全地标识其所连接到的服务器的 TLS 选项以及加密与服务器的所有通信。

可以使用以下选项执行相应操作：

- 强制使用 TLS。Citrix 建议通过不受信任的网络（包括 Internet）建立的所有连接使用 TLS。
- 强制使用 FIPS（Federal Information Processing Standards，联邦信息处理标准）批准的加密以及帮助遵从 NIST SP 800-52 中的建议。这些选项默认处于禁用状态。
- 强制使用特定版本的 TLS 以及特定的 TLS 密码套件；Citrix 支持在 Citrix Receiver for Windows 与 XenApp 或 XenDesktop 之间使用 TLS 1.0、TLS 1.1 和 TLS 1.2 协议。
- 仅连接到特定服务器。
- 检查是否已吊销服务器证书。
- 检查特定服务器证书颁发策略。
- 选择特定的客户端证书（如果服务器未配置为请求客户端证书）。

使用组策略对象管理模板配置 **TLS** 支持

1. 以管理员身份通过运行 gpedit.msc 打开 Citrix Receiver 组策略对象管理模板。
    - 要在单台计算机上应用该策略，请从“开始”菜单中启动 Citrix Receiver 组策略对象管理模板。
    - 要在域中应用该策略，请使用组策略管理控制台启动 Citrix Receiver 组策略对象管理模板。
2. 在“计算机配置”节点下，转至管理模板 > **Citrix Receiver** > 网络路由，然后选择 **TLS** 和合规模式配置策略。
3. 选择已启用启用安全连接以及加密服务器上的通信。设置以下选项：

> 注意：Citrix 建议使用 TLS 建立安全连接。

4. 选择要求对所有连接使用 **TLS** 复选框，强制 Citrix Receiver for Windows 为与已发布的应用程序和桌面建立的所有连接使用 TLS。
5. 从安全性合规模式下拉列表中，选择恰当的选项：
   - 无 - 不强制执行合规模式
   - **SP800-52** - 选择 **SP800-52** 以遵从 NIST SP 800-52。仅当服务器或网关遵从 NIST SP 800-52 建议时才应选择此选项。

     注意：

     如果选择 SP800-52，则将自动使用 FIPS 批准的加密，即使未选择启用 **FIPS** 也是如此。还必须启用 Windows 安全选项系统加密**:** 将 **FIPS** 兼容算法用于加密、哈希和签名。否则，Citrix Receiver for Windows 可能会无法连接到已发布的应用程序和桌面。

     如果选择 SP800-52，则必须选择设置为完全访问检查或需要完全访问检查和 **CRL** 的证书吊销检查策略设置。

     如果选择 SP800-52，Citrix Receiver for Windows 将验证服务器证书是否遵从 NIST SP 800-52 中的建议。如果服务器证书不遵从，Citrix Receiver for Windows 将无法连接。
6. 启用 **FIPS** - 选择此选项将强制使用 FIPS 批准的加密。还必须启用操作系统组策略中的 Windows 安全选项 系统加密**:** 将 **FIPS** 兼容算法用于加密、哈希和签名。否则，Citrix Receiver for Windows 可能会无法连接到已发布的应用程序和桌面。
7. 从允许 **TLS** 服务器下拉列表中，选择端口号。可以确保 Citrix Receiver 仅连接到逗号分隔的列表指定的服务器。可以指定通配符和端口号。例如，*.citrix.com:4433 允许在端口 4433 上连接到公用名以.citrix.com 结尾的任何服务器。证书的颁发者断言安全证书中的信息的准确性。如果 Citrix Receiver 无法识别和信任颁发者，连接将被拒绝。
8. 从 **TLS** 版本下拉列表中，选择以下任意选项：
   - **TLS 1.0**、**TLS 1.1** 或 **TLS 1.2** - 这是默认设置。仅当对 TLS 1.0 有兼容性方面的业务要求时才建议使用此选项。
   - **TLS 1.1** 或 **TLS 1.2** - 使用此选项可确保 ICA 连接使用 TLS 1.1 或 TLS 1.2
   - **TLS 1.2** - 如果 TLS 1.2 属于业务要求，则建议使用此选项。
9. **TLS** 密码套件 - 要强制使用特定的 TLS 密码套件，请选择 “政府”(GOV)、“商务”(COM) 或 “全部”(ALL)。在某些 NetScaler Gateway 配置情况下，您可能需要选择 COM。

   Citrix Receiver for Windows 支持 1024、2048 和 3072 位长度的 RSA 密钥。此外，还支持 RSA 密钥长度为 4096 位的根证书。

   > 注意：Citrix 建议不要使用 1024 位长度的 RSA 密钥。

   请参见下面列出了所有受支持的密码套件的表格。

- 任意：设置为“任意”时，将不配置策略并允许使用以下任意密码套件。
  - TLS_RSA_WITH_RC4_128_MD5
  - TLS_RSA_WITH_RC4_128_SHA
  - TLS_RSA_WITH_3DES_EDE_CBC_SHA
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_RSA_WITH_AES_128_GCM_SHA256
  - TLS_RSA_WITH_AES_256_GCM_SHA384
- 商用：设置为“商用”时，仅允许使用以下密码套件：
  - TLS_RSA_WITH_RC4_128_MD5
  - TLS_RSA_WITH_RC4_128_SHA
  - TLS_RSA_WITH_AES_128_CBC_SHA
  - TLS_RSA_WITH_AES_128_GCM_SHA256
- 政府：设置为“政府”时，仅允许使用以下密码套件:
  - TLS_RSA_WITH_AES_256_CBC_SHA
  - TLS_RSA_WITH_3DES_EDE_CBC_SHA
  - TLS_RSA_WITH_AES_128_GCM_SHA256
  - TLS_RSA_WITH_AES_256_GCM_SHA384

10. 从证书吊销检查策略下拉列表中，选择以下任意选项：
    - 在不访问网络的情况下检查 - 执行证书吊销列表检查。仅使用本地证书吊销列表存储。所有分发点都被忽略。对于目标 SSL Relay/Secure Gateway 服务器出示的服务器证书验证来说，查找证书吊销列表并非强制性操作。
    - 完全访问检查 - 执行证书吊销列表检查。使用本地证书吊销列表存储和所有分发点。如果找到证书的吊销信息，连接将被拒绝。查找证书吊销列表并非验证目标服务器提供的服务器证书的关键。
    - 需要完全访问检查和 **CRL** - 执行证书吊销列表检查，但根 CA 除外。使用本地证书吊销列表存储和所有分发点。如果找到证书的吊销信息，连接将被拒绝。查找所有必要的证书吊销列表对验证非常重要。
    - 全部需要完全访问检查和 **CRL** - 执行证书吊销列表检查，包括根 CA。使用本地证书吊销列表存储和所有分发点。如果找到证书的吊销信息，连接将被拒绝。查找所有必要的证书吊销列表对验证非常重要。
    - 不检查 - 不执行任何证书吊销列表检查。
11. 使用策略扩展 **OID** 可以将 Citrix Receiver for Windows 限制为仅连接到配置了特定证书颁发策略的服务器。如果选择策略扩展 **OID**，Citrix Receiver for Windows 将仅接受包含策略扩展 OID 的服务器证书。

12. 从客户端身份验证下拉列表中，选择以下任意选项：
    - 已禁用 - 禁用客户端身份验证。
    - 显示证书选择器 - 始终提示用户选择证书。
    - 如果可能，则自动选择 - 仅可以选择要识别的证书时提示用户。
    - 未配置 - 指示未配置客户端身份验证。
    - 使用指定的证书 - 使用在“客户端证书”选项中所设置的客户端证书。
13. 使用客户端证书设置可指定标识证书的指纹，以避免不必要地提示用户。
14. 单击应用和确定保存此策略。

下表列出了每组中的密码套件：

TLS 密码套件	**GOV**	**COM**	**ALL**	**GOV**	**COM**	**ALL**	**GOV**	**COM**	**ALL**
启用 **FIPS**	关	关	关	开	开	开	开	开	开
安全性合规模式 **SP800-52**	关	关	关	关	关	关	开	开	开
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384						X			
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	X		X	X		X			
TLS_RSA_WITH_AES_256_GCM_SHA384						X	X		X
TLS_RSA_WITH_AES_256_CBC_SHA256	X	X	X	X	X	X	X	X	X
TLS_RSA_WITH_AES_128_CBC_SHA256	X		X	X		X	X		X
TLS_RSA_WITH_AES_128_CBC_SHA		X	X		X	X		X	X
TLS_RSA_WITH_RC4_128_MD5		X	X						
TLS_RSA_WITH_3DES_EDE_CBC_SHA	X		X	X		X	X		X

为 **Web Interface 5.4** 配置智能卡身份验证

November 19, 2018

如果 Citrix Receiver for Windows 安装了 SSON 组件，即使未在 XenApp PNAgent 站点上启用智能卡的 PIN 直通，默认情况下也会启用直通身份验证；身份验证方法的直通设置将不再有效。下面的屏幕说明了当 Citrix Receiver for Windows 正确配置了 SSON 时，如何将智能卡用作身份验证方法。

有关详细信息，请参阅如何手动安装和配置 Citrix Receiver 以实现直通身份验证。

使用智能卡移除策略控制用户向 Citrix Web Interface 5.4 PNAgent 站点进行身份验证时的智能卡移除行为。

启用此策略之后，如果从客户端设备移除智能卡，用户会从 XenApp 会话中注销。但是，用户仍然在 Citrix Receiver for Windows 中保持登录状态。

要使此策略生效，必须在 Web Interface XenApp Services 站点中设置智能卡移除策略。可以从 Web Interface 5.4 **XenApp Services** 站点 **>** 使用智能卡进行直通身份验证 **>** 启用漫游 **>** 拔出智能卡时注销会话中找到该设置。
禁用智能卡移除策略之后，如果从客户端设备移除智能卡，用户的 XenApp 会话会断开连接；Web Interface XenApp Services 站点上的智能卡移除策略没有任何效果。
注意：32 位客户端所使用的策略不同于 64 位客户端的策略。对于 32 位设备，策略名称为智能卡移除策略 **(32** 位计算机**)**；对于 64 位计算机，策略名称为智能卡移除策略 **(64** 位计算机**)**。

智能卡支持和移除更改

连接到 XenApp 6.5 PNAgent 站点时请注意以下几个方面：

- 从 Citrix Receiver for Windows 4.5 开始，PNAgent 站点登录支持智能卡登录。
- 智能卡删除策略在 PNAgent 站点上已更改：
  删除智能卡时注销 XenApp 会话 – 如果 PNAgent 站点已将智能卡配置为身份验证方法，则必须在 Receiver for Windows 上配置相应的策略以强制注销 XenApp 会话。在 XenApp PNAgent 站点上为智能卡身份验证启用漫游，同时启用智能卡删除策略，这会从 Receiver 会话中注销 XenApp；而用户在 Receiver 会话中仍然保持登录状态。

已知问题

当用户使用智能卡身份验证登录 PNAgent 站点时，用户名显示为已登录。

通过 **Secure Gateway** 进行连接

November 19, 2018

本主题仅适用于使用 Web Interface 的部署。

可以在 Normal（普通）模式或 Relay（中继）模式下使用 Secure Gateway，来为 Citrix Receiver for Windows 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 Citrix Receiver for Windows 进行任何配置。

Citrix Receiver for Windows 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 Citrix Receiver for Windows 配置代理服务器设置的信息，请参阅与 Web Interface 有关的主题。

有关配置代理服务器设置的详细信息，请参阅 Web Interface 文档。

如果安全网络中的服务器上安装了 Secure Gateway 代理，则可以在中继模式下使用 Secure Gateway 代理。

如果使用中继模式，Secure Gateway 服务器将相当于一个代理，并且必须对 Citrix Receiver for Windows 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
- 操作级别域

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

March 26, 2019

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，Citrix Receiver for Windows 必须能够经由防火墙与 Web 服务器和 Citrix 服务器通信。

常用 **Citrix** 通信端口

源	类型	端口	详细信息
Citrix Receiver	TCP	80/443	与 StoreFront 通信
ICA/HDX	TCP	1494	访问应用程序和虚拟桌面
ICA/HDX（启用了会话可靠性）	TCP	2598	访问应用程序和虚拟桌面

源	类型	端口	详细信息
ICA/HDX（通过 SSL）	TCP	443	访问应用程序和虚拟桌面
ICA/HDX（从 HTML5 Receiver）	TCP	8008	访问应用程序和虚拟桌面
ICA/HDX 音频（通过 UDP）	TCP	16500-16509	ICA/HDX 音频的端口范围
IMA	TCP	2512	Independent Management Architecture (IMA)
管理控制台	TCP	2513	Citrix 管理控制台和 *WCF 服务注意：对于基于 FMA 的平台 7.5 及更高版本，不使用端口 2513。
Application/Desktop Request	TCP	80/8080/443	XML Service
STA	TCP	80/8080/443	Secure Ticketing Authority（嵌入在 XML Service 中）

> 注意
>
> 在 XenApp 6.5 中，XenApp Command Remoting Services 通过 WCF 使用端口 2513。

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，Citrix Receiver for Windows 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。

通过代理服务器进行连接

August 7, 2018

代理服务器用于限制网络的入站和出站访问，并处理 Citrix Receiver for Windows 与服务器之间的连接。Citrix Receiver for Windows 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。

使用注册表编辑器配置代理设置，以强制 Citrix Receiver for Windows 在连接过程中遵从或放弃代理服务器的设置。

> 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。

1. 导航到 HKLM\Software\Citrix\AuthManager\
2. 设置 **ProxyEnabled**(REG_SZ)。
   a) True - 指示 Citrix Receiver for Windows 在连接过程中遵从代理服务器的设置。
   b) False - 指示 Citrix Receiver for Windows 在连接过程中放弃代理服务器的设置。
3. 关闭注册表编辑器。
4. 重新启动 Citrix Receiver for Windows 会话以使所做的更改生效。

强制执行信任关系

November 19, 2018

可信服务器配置标识 Citrix Receiver for Windows 连接中的信任关系并强制执行该信任关系。

启用了可信服务器功能时，Citrix Receiver for Windows 将指定要求并确定与服务器建立的连接是否可信。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 Citrix Receiver for Windows 将被定向到服务器上的某个可信区域

启用了此功能时，已连接的服务器驻留在 Windows 的“可信站点”区域中。有关将服务器添加到 Windows 的“可信站点”区域的说明，请参阅 Internet Explorer 联机帮助。

使用组策略对象管理模板启用可信服务器配置

必备条件：

从 Citrix Receiver for Windows 组件（包括连接中心）退出。

1. 以管理员身份通过运行 gpedit.msc 打开 Citrix Receiver 组策略对象管理模板。
   a) 要在单台计算机上应用该策略，请从“开始”菜单中启动 Citrix Receiver 组策略对象管理模板。
   b) 要在域中应用该策略，请使用组策略管理控制台启动 Citrix Receiver 组策略对象管理模板。
2. 在“计算机配置”节点下，转至管理模板 > 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。
3. 选择已启用强制 Citrix Receiver for Windows 执行区域识别。
4. 选择强制使用可信服务器配置。这将强制客户端使用可信服务器执行识别。
5. 在 **Windows Internet** 区域下拉列表中，选择客户端服务器地址。此设置仅适用于 Windows 的“可信站点”区域。

6. 在地址字段中，设置除 Windows 以外的可信站点区域的客户端服务器地址。可以使用逗号分隔的列表。
7. 单击确定和应用。

提升级别与 **wfcrun32.exe**

August 7, 2018

在运行 Windows 10、Windows 8 或 Windows 7 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.exe 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。

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

November 19, 2018

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 for Windows 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 Citrix Receiver for Windows 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 Citrix Receiver for Windows 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 Citrix Receiver for Windows 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 Citrix Receiver for Windows 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)。

选择并分发数字签名证书

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。

Citrix Receiver for Windows 帮助

August 7, 2018

Citrix Receiver 的功能

January 7, 2019

利用 Citrix Receiver，用户可以从任意设备访问虚拟桌面和应用程序，轻松实现随地工作。Receiver 安全易用，并且可以在设备之间保持一致。

注意： 管理员可能未授权您访问这些主题中介绍的所有功能。

添加帐户或切换服务器

November 19, 2018

如果技术支持人员要求您添加帐户或使用其他 NetScaler Gateway，请按以下步骤进行操作：

添加 Citrix Receiver for Windows 帐户

1. 在 Citrix Receiver for Windows 主页中，单击下箭头图标，然后单击帐户。
2. 在“添加帐户”窗口中，单击添加并填写技术支持人员提供的信息。

使用其他 NetScaler Gateway

贵公司可能会使用 NetScaler Gateway 验证您的身份。

1. 右键单击 Citrix Receiver for Windows 图标，然后单击关于。
2. 从 **NetScaler Gateway** 菜单中选择一个服务器。

更改桌面的外观和工作方式

November 19, 2018

虚拟桌面在窗口中显示。可以使用窗口工具栏中的按钮移动桌面和调整桌面大小，以及控制文件和设备的访问方式。小型工具栏底框按钮在窗口或屏幕（如果已最大化）顶部显示。单击该底框可显示工具栏。

将工具栏移动到屏幕上的其他位置

可以将工具栏移动到不遮挡其他窗口内容和控件的便利位置。

- 单击窗口或屏幕顶部的工具栏底框，然后向左或向右移动。

控制如何访问本地文件

虚拟桌面可能需要访问本地计算机上存储的文件。可以控制虚拟桌面对这些文件的访问程度。

- 在工具栏上，依次单击首选项 > 文件访问，并选择以下选项之一，然后单击“确定”：

选项	说明
读取和写入	允许虚拟桌面读取和写入本地文件。
只读	允许虚拟桌面读取但不能写入本地文件。
无访问权限	不允许虚拟桌面访问本地文件。
每次都询问	虚拟桌面每次需要访问本地文件时，系统都显示一条提示。

设置麦克风或网络摄像机

如果要更改虚拟桌面访问本地麦克风或网络摄像机的方式，请按下述步骤进行操作。

- 在工具栏上，依次单击首选项 > 连接，并选择以下选项之一：

选项	说明
自动连接	允许在虚拟桌面上使用麦克风或网络摄像机。
不连接	不允许在虚拟桌面上使用麦克风或网络摄像机。
询问我	虚拟桌面需要访问麦克风或网络摄像机时都向我发出提示。

1. 在全局设置中，选择首选网络摄像机。
2. 单击确定。

限制：

- “首选网络摄像机”对话框显示在 Citrix 连接中心中，即使 Desktop Delivery Controller 中的“Windows Media 重定向”策略设置为已禁用时也是如此。

在 **Desktop Viewer** 中显示设备

November 19, 2018

Citrix Receiver for Windows 检测已连接到您的计算机的设备，并允许您选择要与托管桌面和应用程序一起使用的设备。

可以使用首选项 **>** 连接中的设置来自定义是否希望您的设备（例如麦克风和网络摄像机）连接到虚拟会话。

- 连接到本地计算机的设备在首选项 > 设备下的“设备”列表中显示。
- 如果您已连接某个设备，但在“设备”列表中看不到该设备，请单击刷新。
- 连接后，设备将显示为已优化、受策略限制或通用。

设备	说明
已优化	设备具有 Citrix 虚拟通道，同时在远程会话和本地计算机中自动可用。已优化设备的“当前连接”列显示设备已在本地计算机和远程会话中连接。重定向对话框处于选中状态，无法编辑。可以使用“虚拟通道”列中的切换到按钮在已优化和通用之间切换。例如，如果虚拟通道不支持设备的完整功能，请选择切换到通用。
通用	设备没有 Citrix 虚拟通道，不能同时在本地计算机和远程会话中使用。选中重定向对话框可切换远程会话与本地计算机之间的设备可用性。可以在“当前连接”列中看到当前连接状态。
受策略限制	管理员已设置一个策略来限制此类设备。例如，默认情况下，USB 鼠标和键盘通常受策略限制，因为其行为在不支持 USB 的远程会话中自动处理。其他设备（例如网络设备）因安全原因可能会受到限制。受策略限制的设备的“当前连接”列仅显示本地计算机。您不能对受策略限制的设备选择重定向复选框。

管理我的密码

August 7, 2018

Citrix Single Sign-On 负责管理登录受密码保护的程序和 Web 站点时需要使用的信息。您的用户信息存储在服务器上，您可以从公司运行 Single Sign-On 的任何计算机访问该服务器。这意味您可以在携带设备外出时访问自己的程序、设置以及所做的工作。

除将登录过程自动化外，Single Sign-On 还使您无需致电公司的计算机技术支持人员即可重置 Windows 密码或解锁帐户，为您节约了时间。Single Sign-On 甚至可以为您生成高度安全的新密码。

Single Sign-On 可在您登录自己的计算机或打开首个受密码保护的程序或 Web 站点时启动，具体取决于贵公司如何

设置 Single Sign-On。目前，Single Sign-On 与您存储用户信息的服务器相连接，并可确认您的身份。因此，您将登录到存储了其登录信息的任何程序或 Web 站点。启动当前未存储任何信息的程序或 Web 站点时，系统可能还会提示您添加登录信息。

您或许能够从开始菜单启动 Single Sign-On，具体取决于贵公司的设置方式：

- 从开始菜单中，依次单击所有程序 **> Citrix > Citrix Single Sign-On**。

Single Sign-On 仅在您退出 Citrix Receiver for Windows 时关闭，但您可以暂停 Single Sign-On 而无需将其关闭。

重要：Single Sign-On 是一款非常灵活的程序，允许公司以最能满足自己要求的方式对其进行设置。此处介绍的所有功能并非对所有用户都可用。功能的可用性由贵公司决定。在某些情况下，整个任务（例如显示密码）可能都不可用。在其他情况下，所描述的适用于某项任务的步骤可能会有所差别。我们已尽力确定这些差别，但您可能会发现其他差别。如果出现这些情况，请随时在 Citrix 文档站点联系 Citrix。

使用帐户自助服务

August 7, 2018

如果贵公司启用了 Single Sign-On 的帐户自助服务功能，您可以借助该功能实现以下操作：

- 解锁 Windows 帐户（如果您收到消息，指出 Windows 帐户处于锁定状态）
- 重置 Windows 帐户密码（如果您忘记了该密码，无法登录您的计算机）。

可以在以下位置处找到“帐户自助服务”按钮：切换用户屏幕（对于 Windows Vista、Windows 7、Windows Server 2008 或 Windows Server 2008 R2）上，或者登录到 **Windows** 以及解锁计算机对话框（对于其他受支持的 Windows 操作系统）中。单击此按钮可启动帐户自助服务向导。

通过帐户自助服务功能，您现在可以自己解决这些问题，而无需致电贵公司的计算机技术支持人员。

重要：使用帐户自助服务功能时，系统会请求您提供 Single Sign-On 安全问题的答案，以确认您的身份。如果您不知道安全问题的答案，请致电贵公司的计算机技术支持人员，请其解锁您的 Windows 帐户或重置您的 Windows 密码。

解锁帐户 **(Windows Vista/Windows 7/Windows Server 2008/Windows Server 2008 R2)**

1. 出现提示时，按 Ctrl+Alt+Delete。
2. 执行以下操作之一：
   - 在欢迎屏幕上，单击切换用户。
     系统将显示“切换用户”屏幕。
   - 在欢迎屏幕上，单击其他凭据。
     系统将显示“切换用户”屏幕。
3. 单击帐户自助服务。系统将显示“帐户自助服务”屏幕。

4. 单击位于“帐户自助服务”标题下的单击此处可重置密码或解锁帐户，启动帐户自助服务向导。
5. 在欢迎使用帐户自助服务向导页面上，单击解锁我的帐户，然后单击下一步。
6. 在标识您的帐户页面上，确保显示正确的用户名和密码，然后单击下一步。系统将显示解锁我的帐户页面。
7. 在解锁我的帐户页面上，单击下一步查看第一个安全问题。
8. 在答案框中，键入第一个安全问题的答案，然后单击下一步。如果有其他安全问题，系统将显示下一个问题。
9. 重复步骤 8，直至显示解锁帐户页面。
10. 在解锁帐户页面上，单击下一步。
11. 在帐户解锁成功页面上，单击完成。

重置 **Windows** 帐户密码 **(Windows Vista/Windows 7/Windows Server 2008/Windows Server 2008 R2)**

1. 出现提示时，按 Ctrl+Alt+Delete。
2. 执行以下操作之一：
   - 在欢迎屏幕上，单击切换用户。
     系统将显示“切换用户”屏幕。
   - 在欢迎屏幕上，单击其他凭据。
     系统将显示“切换用户”屏幕。
3. 单击帐户自助服务。系统将显示“帐户自助服务”屏幕。
4. 单击位于“帐户自助服务”标题下的单击此处可重置密码或解锁帐户，启动帐户自助服务向导。
5. 在欢迎使用帐户自助服务向导页面上，单击重置我的密码，然后单击下一步。
6. 在标识您的帐户页面上，确保显示正确的用户名和密码，然后单击下一步。系统将显示重置我的密码页面。
7. 在重置我的密码页面上，单击下一步查看第一个安全问题。
8. 在答案框中，键入第一个安全问题的答案，然后单击下一步。
9. 重复步骤 8，直至显示输入新密码页面。
10. 在输入新密码页面上，键入并确认新密码，然后单击下一步。
11. 在密码更改成功页面上，单击完成返回到“帐户自助服务”屏幕，在该屏幕中，可以选择并登录您的帐户。

解锁帐户（除 **Windows Vista/Windows 7/Windows Server 2008/Windows Server 2008 R2** 以外的 **Windows** 系统）

1. 执行以下操作之一：
   - 在欢迎使用 **Windows** 对话框中，按 Ctrl+Alt+Delete，然后单击选项（如有必要）。
   - 在计算机已锁定对话框中，按 Ctrl+Alt+Delete，然后单击选项。
2. 单击帐户自助服务启动帐户自助服务向导。
3. 在欢迎使用帐户自助服务向导页面上，单击解锁我的帐户，然后单击下一步。
4. 在标识您的帐户页面上，确保显示正确的用户名和密码，然后单击下一步。系统将显示解锁我的帐户页面。
5. 在解锁我的帐户页面上，单击下一步查看第一个安全问题。
6. 在答案框中，键入第一个安全问题的答案，然后单击下一步。如果有其他安全问题，系统将显示下一个问题。

7. 重复步骤 6，直至显示解锁帐户页面。
8. 在解锁帐户页面上，单击下一步。
9. 在帐户解锁成功页面上，单击完成。

重置 **Windows** 帐户密码（除 **Windows Vista/Windows 7/Windows Server 2008/Windows Server 2008 R2** 以外的 **Windows** 系统）

1. 执行以下操作之一：
   - 在欢迎使用 **Windows** 对话框中，按 Ctrl+Alt+Delete，然后单击选项（如有必要）。
   - 在计算机已锁定对话框中，按 Ctrl+Alt+Delete，然后单击选项。
2. 单击帐户自助服务启动帐户自助服务向导。
3. 在欢迎使用帐户自助服务向导页面上，单击重置我的密码，然后单击下一步。
4. 在标识您的帐户页面上，确保显示正确的用户名和密码，然后单击下一步。系统将显示重置我的密码页面。
5. 在重置我的密码页面上，单击下一步查看第一个安全问题。
6. 在答案框中，键入第一个安全问题的答案，然后单击下一步。
7. 重复步骤 6，直至显示输入新密码页面。
8. 在输入新密码页面上，键入并确认新密码，然后单击下一步。
9. 在密码更改成功页面上，单击完成。

手动更改密码

August 7, 2018

1. 按照 Web 站点或程序的说明进行操作，更改您的密码。
2. 在 Microsoft Windows 通知区域中（通常在任务栏的最右侧），右键单击 Citrix Receiver 图标，然后依次选择密码 **>** 管理密码。
3. 在“管理密码”窗口中，选择所需的程序或 Web 站点，然后单击编辑。

   注意：此时贵公司可能已激活身份验证过程。如果已激活，则请在出现提示时输入您的 Windows 用户名和密码。（如果您使用智能卡或其他不需要输入用户名和密码的身份验证方法进行登录，则请在出现提示时使用这些方法验证您的身份。）
4. 在密码框中，选择当前的内容，并键入在步骤 1 中使用的同一个密码。
5. 单击确定。这样既可在 Single Sign-On 中保存新密码。

常见疑问和问题

January 7, 2019

下表列出了使用 Single Sign-On 时可能会遇到的疑问和问题。

我收到一条错误消息，指出我的密码将过期

定期更改密码是保护信息安全的最佳方式之一。如果您的密码太长时间没有更改，Single Sign-On 会向您发出提醒通知，具体取决于贵公司所做的设置。

在更改密码之前，您将持续收到这些消息。

我不希望立即运行 **Single Sign-On**

有时您可能不希望运行 Single Sign-On。例如，您可能需要在登录页面上执行操作，但不希望 Single Sign-On 将您登录到该程序。

在这些情况下，请使用 “Single Sign-On 暂停” 功能。使用暂停功能会停止自动登录活动，但可使 Single Sign-On 保持在打开状态，供您使用。

程序拒绝接受我的新密码

您使用密码更改向导更改了某个特定程序的密码，但当您尝试登录该程序时，该程认为您的新密码无效而拒绝接受该密码。

可能的原因为：新密码存储在 Single Sign-On 中，但未被您的程序所接受。因此，Single Sign-On 将提交一个错误的密码。

如果贵公司启用了 “还原以前的密码” 功能，则请使用该功能修复此问题。

注意：如果该功能不可用，则请致电贵公司的技术支持人员。

还原程序以前的密码

1. 在 Microsoft Windows 通知区域中（通常在任务栏的最右侧），右键单击 Citrix Receiver 图标，然后依次选择密码 **>** 管理密码。
2. 在 “管理密码” 窗口中，选择所需的程序或 Web 站点，然后单击编辑。

   注意：此时贵公司可能已激活身份验证过程。如果已激活，则请在出现提示时输入您的 Windows 用户名和密码。（如果您使用智能卡或其他不需要输入用户名和密码的身份验证方法进行登录，则请在出现提示时使用这些方法验证您的身份。）

系统将显示一个对话框，其中包含所选程序的属性。

3. 单击还原以前的密码，然后单击是确认您的操作。

无法访问我的用户数据

登录您的计算机时，Single Sign-On 将连接到贵公司存储 Single Sign-On 用户信息的服务器。如果成功连接且您的身份得以确认，Single Sign-On 将启动。

如果由于某些原因导致连接或身份验证失败，Single Sign-On 将不启动，您可能会收到一条错误消息，指出无法访问您的用户数据。如果出现此问题，请联系贵公司的计算机技术支持人员。

我的 **Web** 浏览器无法与 **Single Sign-On** 结合使用

Single Sign-On 仅支持与 Microsoft Internet Explorer 结合使用。使用其他 Web 浏览器可能无法实现想要的结果。

Single Sign-On 在我注销之后将我重新登录

在某些情况下，在您从受密码保护的程序或 Web 站点注销后，该程序可能会返回到登录屏幕。如果发生上述情况，Single Sign-On 可能会对登录页面做出反应，将您重新登录到该程序，具体取决于贵公司如何设置 Single Sign-On。

如果发生上述情况，请执行以下操作之一：

- 如果贵公司启用了单点登录的暂停功能，请先使用该功能，然后再注销
- 如果暂停功能不可用，请在单点登录将您重新登录之前，从该程序中注销并快速关闭该程序的窗口

注意：请考虑致电贵公司的计算机技术支持人员说明您遇到的情况，并建议单点登录管理员激活高级检测应用程序定义设置仅在首次登录此程序时进行处理。

我在脱机工作之前是否应执行某些特殊操作

如果贵公司在您的计算机上安装了 Single Sign-On，则应在脱机工作之前刷新您的许可证，而不是通过贵公司的网络从某台服务器运行 Single Sign-On。这样可确保您在连接到贵公司的网络之前，完全占用该许可证。

刷新 **Single Sign-On** 许可证

1. 在 Microsoft Windows 通知区域中（通常在任务栏的最右侧），右键单击 Citrix Receiver 图标，然后依次选择密码 **>** 管理密码。

   注意：此时贵公司可能已激活身份验证过程。如果已激活，则请在出现提示时输入您的 Windows 用户名和密码。（如果您使用智能卡或其他不需要输入用户名和密码的身份验证方法进行登录，则请在出现提示时使用这些方法验证您的身份。）

2. 单击关于。

   此时将显示关于 **Citrix Single Sign-On** 窗口。

3. 单击刷新许可证。

4. 单击确定。

   系统将关闭关于 **Citrix Single Sign-On** 窗口。

Single Sign-On 锁定我的工作站的原因

每当您请求执行需要额外安全级别的任务时，Single Sign-On 都会锁定您的工作站。这些任务可能包括更改或显示密码。

工作站被锁定之后，您需要向 Single Sign-On 提供帐户密码，以验证您的身份。在某些情况下，系统甚至可能会要求您提供安全问题的答案。通过执行此类验证，Single Sign-On 可阻止他人访问您的敏感信息。

虽然这样可能令人烦恼，但这是为了保护贵公司、您本人以及您的数据。

自动更改密码

August 7, 2018

Single Sign-On 密码更改向导可自动执行在已通过身份验证的程序上更改密码的过程。您可以创建自己的密码，也可以允许 Single Sign-On 为您创建一个密码，具体取决于贵公司如何设置 Single Sign-On。

注意：由于密码更改向导生成的密码是由字母、数字及其他字符随机组合而成，因此这些密码的安全级别非常高。由于 Single Sign-On 负责管理密码，而您无需记住这些密码，因此请考虑使用此功能。

密码更改向导可通过以下两种方式之一启动，具体取决于贵公司如何设置该向导：

- 程序指示必须更改您的密码时
- 您启动程序的密码更改过程时

在某些情况下，Single Sign-On 可能不会检测密码更改过程，也不会启动密码更改向导。在这些情况下，您必须同时手动在 Web 站点或程序中以及 Single Sign-On 中更改您的密码，以确保密码相匹配。

选择如何创建新密码

如果贵公司启用了该选择功能，密码更改向导的请选择如何创建您的新密码页面将允许您选择如何创建新密码。选项包括：

- 选择系统生成的密码

  选择此选项并单击下一步后，密码更改向导将创建一个高度安全的密码。在此过程中此密码不会向您显示，因为其存储在 Single Sign-On 中，您无需知晓。但如果贵公司将 Single Sign-On 设置为显示此密码，您可以在退出向导后查看该密码（如有需要）。

  注意：由于密码更改向导生成的密码是由字母、数字及其他字符随机组合而成，因此这些密码的安全级别非常高。由于 Single Sign-On 负责管理密码，而您无需记住这些密码，因此请考虑使用此功能。

- 创建自己的密码

  选择此选项并单击下一步后，密码更改向导将允许您创建并提交您自己的密码。此密码必须遵循贵公司设置的任何密码策略，这些策略涉及长度、复杂度以及其他可能会影响安全性的因素。

等待确认

密码更改向导确定密码更改成功还是失败的过程中，系统将显示该向导的等待确认页面。

如果在密码更改向导关闭等待确认页面之前您确定密码更改成功，请单击跳过前往确认密码更改页面。

确认密码已更改

如果贵公司已激活密码更改向导的确认密码更改页面，则可能会显示该页面。如果显示该页面，则系统会要求您确定是否已成功更改密码。有三个选项可用。

是：

如果未显示程序的密码重置窗口或成功消息，则表示密码更改成功。

如果选择是并单击下一步，则向密码更改向导发出指示，指出密码更改操作已成功完成。密码更改向导将结束自己的进程。

否：

如果持续显示程序的密码重置窗口或失败消息，则表示密码更改失败。

如果选择否并单击下一步，则向密码更改向导发出指示，指出您的程序未接受新密码。密码更改向导将结束自己的进程，但不更改您的密码。

我不知道：

如果选择我不知道并单击下一步，则将显示一个页面，介绍如何确定密码更改操作是否已成功完成。

确定向导成功完成的另一种方法是（如果您已创建自己的密码）：暂停单点登录，并使用新密码登录该程序。

注意：您可能需要移动密码更改向导窗口，确定该程序的密码重置窗口是否仍然处于打开状态，或者该程序是否提供了任何与密码相关的反馈。

确认密码尚未更改

如果密码更改向导检测到密码未成功更改，或者您在确认密码更改页面上选择了否，则将显示密码未更改页面。

密码未更改页面提供了两个选项：

- 尝试另一个密码。

  仅当程序的密码更改表单仍处于打开状态时，才能使用此选项。如果在表单关闭后使用此选项，则程序和 Single Sign-On 中保存的密码可能不匹配。

  如果选择尝试另一个密码并单击下一步，则可以尝试向程序提交其他密码。可能会显示以下页面之一，具体取决于贵公司如何设置密码更改向导：

  - 显示请选择如何创建您的新密码页面。您可以选择使用系统生成的密码，也可以使用自己创建的密码。
  - 显示创建您自己的密码页面。
  - 将创建并提交一个系统生成的密码。密码更改向导随后会搜索密码更改成功的确认消息。

- 不再执行其他操作，退出向导。

  如果选择不再执行其他操作，退出向导，则会终止进一步尝试更改程序的密码。但您可以重新启动密码更改向导，并在其他时间再次尝试更改密码。

不再执行其他操作，退出向导

如果密码更改过程失败，或者您在确认密码更改页面上选择了否，则将显示密码未更改页面。

如果密码更改向导失败，请尝试执行以下操作更改您的密码：

- 在密码未更改页面上单击完成，退出密码更改向导并重新启动该向导，以再次尝试更改密码
- 在程序和 Single Sign-On 中手动更改密码
- 致电贵公司的计算机技术支持人员

成功更改密码后退出向导

如果密码更改向导检测到密码已成功更改，或者您在确认密码更改页面上选择了是，则将显示密码更改成功页面。

此时，程序将接受您的新密码，并将其存储在 Single Sign-On 中。

确定程序是否已接受新密码

如果您在确认密码更改页面上选择了我不知道并单击下一步，则将显示一个页面，介绍如何确定密码更改是否成功。

确定向导成功完成的另一种方法是：暂停 Single Sign-On，并使用新密码登录该程序。

如果在此页面上单击下一步，则将导致重新显示确认密码更改页面。

创建自己的密码

如果您在请选择如何创建您的新密码页面上选择了创建您自己的密码，则将显示密码更改向导的创建您自己的密码页面。如果贵公司未授予您创建自己的密码所需的权限，则可能不显示此页面。

为防止提交键入错误的密码，您必须在新密码和确认新密码框中键入您的密码。如果密码不配置，密码更改向导会向您发出通知。如果密码匹配，下一步按钮将变为可用。

密码更改向导要求您遵循贵公司制定的所有密码策略。贵公司可能会制定的策略示例包括：

- 不得使用之前的密码
- 密码必须同时包含数字和字母
- 密码不得包含某些字符
- 密码必须具有一定的长度

暂停和恢复 **Single Sign-On**

August 7, 2018

有时在工作过程中，您可能希望临时暂停 Single Sign-On。暂停的原因包括：

- 需要在登录页面上执行操作，但不希望登录该程序或 Web 页面
- 需要在 Internet 上执行操作，但不希望每次 Single Sign-On 检测到登录表单时都询问是否存储登录信息

在 Single Sign-On 中，暂停与退出不同，暂停后，Single Sign-On 的功能仍将继续运行并可用。但您不会自动登录到受密码保护的程序或 Web 站点，并且系统不会提示您存储新的登录信息。只是在您需要使用 Single Sign-On 时，可以随时快速进行恢复。

暂停 Single Sign-On：

- 在 Microsoft Windows 通知区域中（通常在任务栏的最右侧），右键单击 Citrix Receiver 图标，然后依次选择密码 **>** 暂停 **Single Sign-On**。

确定 Single Sign-On 是否已暂停:

- 在 Microsoft Windows 通知区域中（通常在任务栏的最右侧），右键单击 Citrix Receiver 图标，然后选择首选项，在 Citrix Receiver“首选项” 窗口中查看 Citrix Single Sign-On 插件的状态。

恢复 Single Sign-On：

- 在 Microsoft Windows 通知区域中（通常在任务栏的最右侧），右键单击 Citrix Receiver 图标，然后依次选择密码 **>** 恢复 **Single Sign-On**。

在密码共享组中编组程序

August 7, 2018

密码共享组由管理员创建。如果某个密码属于某个密码共享组，则该程序的密码与该共享组内所有其他程序的密码相匹配。这使您能够同时更新密码共享组中所有程序的密码。

例如，如果您的管理员创建的密码共享组中包含您的电子邮件应用程序、会计应用程序、字处理应用程序、数据输入应用程序以及人力资源应用程序，则可以只更改一次密码，该密码即会在整个共享组中进行更新。

如果您使用两个不同的用户名登录密码共享组中的某个应用程序，可能同样需要两个不同的密码。可以使用不同的密码从密码共享组中删除登录信息，删除完成后，对该登录信息所做的任何更新都将不再对该共享组内存储的其他应用程序密码产生影响。

更改共享密码

1. 在 Microsoft Windows 通知区域中（通常在任务栏的最右侧），右键单击 Citrix Receiver 图标，然后依次选择密码 **>** 管理密码。
2. 在“管理密码”窗口中，选择所需的程序或 Web 站点，然后单击编辑。

   注意：此时贵公司可能已激活身份验证过程。如果已激活，则请在出现提示时输入您的 Windows 用户名和密码。（如果您使用智能卡或其他不需要输入用户名和密码的身份验证方法进行登录，则请在出现提示时使用这些方法验证您的身份。）

   如果该程序属于某个密码共享组，则显示的对话框中将包含更改该密码共享组的密码链接。
3. 单击更改该密码共享组的密码，并按照向导中的说明进行操作。

取消程序与密码共享组的关联

1. 在 Microsoft Windows 通知区域中（通常在任务栏的最右侧），右键单击 Citrix Receiver 图标，然后依次选择密码 **>** 管理密码。
2. 在“管理密码”窗口中，选择所需的程序或 Web 站点，然后单击编辑。

   注意：此时贵公司可能已激活身份验证过程。如果已激活，则请在出现提示时输入您的 Windows 用户名和密码。（如果您使用智能卡或其他不需要输入用户名和密码的身份验证方法进行登录，则请在出现提示时使用这些方法验证您的身份。）

   如果该程序属于某个密码共享组，则显示的对话框中将包含取消该登录与密码共享组的关联链接。
3. 单击取消该登录与密码共享组的关联，并按照向导中的说明进行操作。

存储用户名和密码

November 19, 2018

如果贵公司启用了此功能，则 Single Sign-On 会在您打开受密码保护的 Web 站点或启动受密码保护的程序时自动执行检测。如果您之前在 Single Sign-On 中存储过该 Web 站点或程序的用户名、密码或其他登录信息，Single Sign-On 会自动将您登录。

打开受密码保护的 Web 站点或启动受密码保护的程序时，如果尚未存储登录信息，则可以通过以下方法在 Single Sign-On 中存储您的登录信息，具体取决于贵公司启用的 Single Sign-On 功能：

- 如果 Single Sign-On 检测到您打开了一个受密码保护的 Web 站点或启动了一个受密码保护的程序，则将自动显示一个对话框，询问您是否希望存储此信息
- 如果 Single Sign-On 未检测到程序，您可以手动添加登录信息

Single Sign-On 将存储以下各项的相关登录信息：

- 基于 **Windows** 的程序。这些程序通常从“开始”菜单或桌面进行启动。例如 Lotus Notes。
- 基于 **Web** 的程序或站点。这些程序或站点通常通过 Web 浏览器进行查看以及与之交互。例如网上商店或基于 Web 的培训程序。

  重要：Microsoft Internet Explorer（32 位版本）是 Single Sign-On 唯一支持的 Web 浏览器。
- 基于终端仿真器的程序。这些程序基于文本，通常与终端仿真器相关联。这些程序的窗口通常以深色（例如绿色）作为背景色，以稍浅的相同颜色作为文本色。

注意：请求的登录信息可能因程序而异。在大多数情况下，您需要提供自己的用户名或 ID 以及密码。如果您不知道系统要求您输入的信息，请联系贵公司的计算机技术支持人员。

自动存储登录信息

1. 打开一个受密码保护的 Web 站点或启动一个受密码保护的程序。系统将显示该 Web 站点的登录页面或程序的登录对话框。
2. 在所显示的询问您是否希望 Single Sign-On 记住此 Web 站点或程序的密码的对话框中，单击记住。
3. 如果您要存储某个 Web 站点或基于 Web 的程序的登录信息，Web 站点登录窗口中用于提交登录信息的对话框和按钮周围可能会显示多个矩形。在所显示的询问您是否选择了正确的框和按钮的对话框中，单击是。
4. 在新建登录对话框中，键入您的登录信息并单击完成。新建登录对话框将关闭，您的登录信息将存储到 Single Sign-On 中，Single Sign-On 将您登录到相应的程序。

手动存储登录信息

1. 打开一个受密码保护的 Web 站点或启动一个受密码保护的程序。系统将显示该 Web 站点的登录页面或程序的登录对话框。

2. 如果系统未显示任何对话框，询问您是否希望 Single Sign-on 记住此 Web 站点或程序的密码，请提示 Single Sign-on 允许您手动存储自己的登录信息：在 Microsoft Windows 通知区域中（通常在任务栏的最右侧），右键单击 Citrix Receiver 图标，然后依次选择密码 **>** 提交密码。

   注意：此时贵公司可能已激活身份验证过程。如果已激活，则请在出现提示时输入您的 Windows 用户名和密码。（如果您使用智能卡或其他不需要输入用户名和密码的身份验证方法进行登录，则请在出现提示时使用这些方法验证您的身份。）

3. 在所显示的询问您是否希望 Single Sign-On 记住此 Web 站点或程序的密码的对话框中，单击记住。
4. 如果您要存储某个 Web 站点或基于 Web 的程序的登录信息，Web 站点登录窗口中用于提交登录信息的对话框和按钮周围将显示多个矩形。在所显示的询问您是否选择了正确的框和按钮的对话框中，单击是。
5. 在新建登录对话框中，键入您的登录信息并单击完成。新建登录对话框将关闭，您的登录信息将存储到 Single Sign-On 中，Single Sign-On 将您登录到相应的程序。

存储一个程序的多个用户名和密码

有时您可能拥有某个程序或 Web 站点的多个帐户。例如：

- 您有权访问您部门的普通电子邮件帐户（称为访问请求）以及您自己的电子邮件帐户
- 您负责为两个项目购买材料，在供应商 Web 站点下，每个项目都有一个独立的帐户

如果贵公司启用了 Single Sign-On 的多个帐户功能，您可以为同一个程序或 Web 站点存储两组或多组帐户信息。存储多组帐户信息后，Single Sign-On 将使用登录选择器，允许您挑选登录时要使用的一组登录信息。

添加 **Single Sign-On** 中已存储的多个程序和 **Web** 站点的其他密码

1. 在 Microsoft Windows 通知区域中（通常在任务栏的最右侧），右键单击 Citrix Receiver 图标，然后依次选择密码 **>** 管理密码。
2. 在“管理密码”窗口中，选择要向其中添加其他登录帐户的程序或 Web 站点。
3. 单击复制。

   注意：此时贵公司可能已激活身份验证过程。如果已激活，则请在出现提示时输入您的 Windows 用户名和密码。（如果您使用智能卡或其他不需要输入用户名和密码的身份验证方法进行登录，则请在出现提示时使用这些方法验证您的身份。）

   列表中将额外列出该程序或 Web 页面。

4. 选择新列出的程序或 Web 页面，然后单击编辑。系统将显示一个对话框，其中包含该程序或 Web 站点的登录信息。
5. 更改登录信息（如有必要）。
6. 在应用程序名称框中，修改程序名称或 Web 站点名称，以帮助您将其与该程序的其他实例区分开来。
7. 单击确定。

在有多个帐户的情况下进行登录

如果某个程序或 Web 站点有多个帐户，Single Sign-On 将启动登录选择器，允许您选择登录时要使用的帐户。

登录具有多个帐户（存储在 Single Sign-On 中）的程序或 Web 站点：

1. 启动该程序或 Web 站点。系统将显示登录选择器对话框以及程序的登录页面。
2. 在登录选择器对话框中，单击相应的登录帐户，然后单击确定。登录选择器对话框将关闭，Single Sign-On 将您登录到该程序或 Web 站点。

注册安全问题的答案

August 7, 2018

1. 在欢迎使用安全问题注册向导页面上，单击下一步查看第一个安全问题。
2. 在答案框中，键入第一个安全问题的答案。您的答案在键入过程中可能会显示为圆点，具体取决于贵公司所做的设置。如果显示为圆点，则必须在确认答案框中重新键入您的答案。

   注意： 问题的答案区分大小写。如果您使用大写字母注册答案，在验证身份时也必须使用相同的大写字母。同样，如果在注册过程中使用句号，例如确定 Ms. Shestack 为您最喜欢的老师时，请在验证您的身份时使用相同的句号。
3. 单击下一步。如果有其他安全问题，系统将显示下一个问题。
4. 重复步骤 2 和 3，直至系统显示提交您的答案页面。
5. 在提交您的答案页面上，单击下一步。
6. 在安全问题注册成功页面上，单击完成。系统将存储安全问题的答案。

删除用户名和密码

January 7, 2019

本主题介绍如何删除 Single Sign-on 保存的密码。如果在登录时选择记住我的密码，则 Receiver 也可保存密码。要将密码从 Receiver 中删除，请右键单击 Receiver 图标，单击关于，展开高级，然后单击 删除密码。

有时您可能希望从 Single Sign-On 中删除您的登录帐户信息。例如：

- 您存储了某个程序或 Web 站点的多个帐户，但不需要再使用所有帐户
- 您存储了多个程序或 Web 站点的相关信息，但不再使用

重要：如果您删除了仍在使用的登录信息，Single Sign-On 则无法自动将您登录到该程序或 Web 站点，系统会在您下次启动该程序时再次询问您是否要存储相关信息。

1. 在 Microsoft Windows 通知区域中（通常在任务栏的最右侧），右键单击 Citrix Receiver 图标，然后依次选择密码 **>** 管理密码。
2. 在“管理密码”窗口中，选择所需的程序或 Web 站点，然后单击删除。

   注意：此时贵公司可能已激活身份验证过程。如果已激活，则请在出现提示时输入您的 Windows 用户名和密码。（如果您使用智能卡或其他不需要输入用户名和密码的身份验证方法进行登录，则请在出现提示时使用这些方法验证您的身份。）

   系统将显示一个对话框，请求您确认是否要删除所选程序的登录信息。
3. 单击是。登录信息将从 Single Sign-On 中删除，不再在“管理密码”窗口中列出。

   注意：如果您返回到该程序或 Web 站点，系统会询问您是否要存储登录信息。

显示密码

August 7, 2018

如果贵公司启用了此功能，Single Sign-On 将允许您查看自己的密码。

注意：贵公司可能已经标识了某些不得显示的密码。

警告：请勿允许他人获知您的密码。这样会给您的帐户和公司系统带来危险。

1. 在 Microsoft Windows 通知区域中（通常在任务栏的最右侧），右键单击 Citrix Receiver 图标，然后依次选择密码 **>** 管理密码。
2. 在“管理密码”窗口中，选择所需的程序或 Web 站点，然后单击显示密码。

   注意：此时贵公司可能已激活身份验证过程。如果已激活，则请在出现提示时输入您的 Windows 用户名和密码。（如果您使用智能卡或其他不需要输入用户名和密码的身份验证方法进行登录，则请在出现提示时使用这些方法验证您的身份。）

   系统将显示一个新对话框，其中包含所选程序的密码。
3. 单击确定关闭程序的密码对话框。

首次设置 **Citrix Single Sign-On**

August 7, 2018

Citrix Single Sign-On 可在您登录自己的计算机或启动首个受密码保护的程序或 Web 站点时自动启动，具体取决于贵公司如何对其进行设置。

如果贵公司对 Single Sign-On 进行了配置，使其在首次运行时收集您提供的信息，系统可能会请求您回答安全问题，例如“您最喜欢的老师是谁?”您提供的这些问题的答案可帮助验证您的身份（如有必要）。

在未连接到 **Internet** 时使用应用程序

August 7, 2018

首次打开应用程序时必须连接到 Internet。Citrix Receiver for Windows 将在设备中安装一些应用程序，以便您能够在未连接到 Internet 时运行这些程序。此安装过程可能需要几分钟时间。

注意： 脱机访问功能并不适用于所有用户或应用程序。管理员可以决定在要求您连接到 Internet 之前能够脱机使用应用程序的时间长度。

查找桌面和应用程序

August 7, 2018

在任意设备上都可以通过 Citrix Receiver for Windows 主页访问您的虚拟桌面和应用程序。

要开始操作，请在 Citrix Receiver for Windows 图标上单击鼠标右键，然后单击打开。

桌面和应用程序也可位于以下一个或多个位置：

- Windows“开始”菜单 – 从 Citrix Receiver for Windows 添加的应用程序和桌面也将添加到 Windows“开始”菜单中“所有程序”下的某个文件夹中。
- 桌面 – 管理员可能会在计算机桌面上提供快捷方式。快捷方式可以位于桌面上的某个文件夹中。
- Web 页面 – 管理员可能会在 Web 页面上提供指向桌面和应用程序的链接。打开 Internet Explorer、Firefox 或 Google Chrome，然后输入管理员提供的 URL。

管理会话

August 7, 2018

Citrix 连接中心显示通过 Receiver 建立的所有活动连接。

打开连接中心：

- 在 Receiver 图标上单击鼠标右键，然后单击连接中心。

退出冻结的虚拟应用程序

在连接中心中选择相应的应用程序，然后单击终止。

一次性关闭所有活动的虚拟应用程序

在连接中心中选择相应的服务器，然后单击注销。

更改桌面和应用程序的显示方式

可以在“无缝”和“全屏”模式之间切换。

- 无缝模式。桌面和应用程序不包含在会话窗口中。每个桌面和应用程序都将显示在各自大小可调的窗口中，如同实际安装在用户设备上一样。可以在应用程序和本地桌面之间进行切换。
- 全屏模式。应用程序位于桌面窗口中。

切换到全屏模式：在连接中心中选择相应的服务器，然后依次单击全屏 > 确定。

返回无缝模式：按 Shift + F2。

刷新或删除应用程序

August 7, 2018

注销或退出 Citrix Receiver for Windows 时，应用程序将断开连接。请通过从下拉菜单中选择刷新应用程序或单击应用程序图标来重新连接到会话。

禁用了自助服务模式时，要在通过“开始”菜单或桌面快捷方式以独占方式访问应用程序时对其进行刷新，请右键单击通知区域中的 Citrix Receiver for Windows，然后选择刷新。

选择刷新应用程序选项可获取 StoreFront 中最新的已发布应用程序和桌面。

要从“应用程序”视图中删除某个应用程序，请右键单击该应用程序，然后选择删除应用程序。

Citrix Receiver for Windows Desktop Lock

March 26, 2019

不需要与本地桌面进行交互时，可以使用 Citrix Receiver for Windows Desktop Lock。您仍可使用 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 for Windows 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 Citrix Receiver for Windows 4.2 或更高版本后不再支持以前的 Desktop Lock 版本。

不许使用 /includeSSON 标记安装 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 下载页面上提供的 CitrixReceiverDesktopLock.MSI 安装 Citrix Receiver for Windows Desktop Lock。

Citrix Receiver Desktop Lock 的系统要求

- Microsoft Visual C++ 2005 Service Pack 1 可再发行组件包。有关详细信息，请参阅 Microsoft 下载页面。
- 在 Windows 7（包括 Embedded Edition）、Windows 7 Thin PC、Windows 8、Windows 8.1 和 Windows 10（包括周年纪念日更新）上受支持。
- 仅限通过本机协议连接到 StoreFront。
- 已加入域和未加入域的端点。
- 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

> 重要
>
> 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 Citrix Receiver for Windows Desktop Lock

- 可以将 Citrix Receiver for Windows Desktop Lock 与以下 Citrix 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、双重或智能卡身份验证
- 断开 Citrix Receiver for Windows 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 重定向在 Windows 7 上处于启用状态。
- Desktop Viewer 针对 Citrix Receiver for Windows 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 **Citrix Receiver for Windows Desktop Lock**

此过程将安装 Citrix Receiver for Windows，以便使用 Citrix Receiver for Windows 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 > Citrix Receiver for Windows 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 Citrix Receiver for Windows 安装文档，网址为 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 **Citrix Receiver for Windows Desktop Lock**

仅应向每位用户授予一个运行 Citrix Receiver for Windows 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 Citrix Receiver for Windows 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 **Citrix Receiver for Windows Desktop Lock** 的设备结合使用

1. 配置 StoreFront。
   a) 将 XML Service 配置为使用 DNS 地址解析，以获取 Kerberos 支持。
   b) 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。
   c) 确保启用通过智能卡直通（默认启用）。
   d) 启用 Kerberos。
   e) 启用 Kerberos 和使用智能卡进行直通身份验证。
   f) 在 IIS 默认 Web 站点上启用匿名访问并使用集成 Windows 身份验证。
   g) 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。
   a) 从%Program Files%\Citrix\ICA Client\Configuration 导入 Receiver.admx 模板。
   b) 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”。
   c) 启用智能卡身份验证。
   d) 启用本地用户名和密码。
3. 安装 Citrix Receiver for Windows Desktop Lock 之前，配置用户设备。
   a) 将 Delivery Controller 的 URL 添加到 Windows Internet Explorer 的可信站点列表中。
   b) 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。
   c) 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 Citrix Receiver for Windows 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 Citrix Receiver for Windows Desktop Lock 的用户设备。

删除 **Citrix Receiver for Windows Desktop Lock**

确保删除下面列出的两个组件。

1. 使用安装和配置 Citrix Receiver for Windows 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 for Windows Desktop Lock。
   - 删除 Citrix Receiver for Windows。

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。本节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 - 预览任务栏中打开的窗口。

SDK 和 API

August 7, 2018

Citrix 虚拟通道 SDK

Citrix 虚拟通道软件开发工具包 (SDK) 支持为使用 ICA 协议的其他虚拟通道编写服务器端应用程序和客户端驱动程序。服务器端虚拟通道应用程序位于 XenApp 或 XenDesktop 服务器上。本版本的 SDK 支持为 Receiver for Windows 编写新虚拟通道。如果要为其他客户端平台编写虚拟驱动程序，请联系 Citrix 技术支持。

虚拟通道 SDK 提供：

- 在 Citrix 服务器 API SDK (WFAPI SDK) 中与虚拟通道功能结合使用以创建新虚拟通道的 Citrix 虚拟驱动程序应用程序编程接口 (Virtual Driver Application Programming Interface, VDAPI)。VDAPI 提供的虚拟通道支持简化了编写虚拟通道的过程。
- Windows 监视 API，用于增强视觉体验以及对与 ICA 集成的第三方应用程序的支持。
- 用来演示编程技术的虚拟通道示例程序的有效源代码。
- 虚拟通道 SDK 需要 WFAPI SDK 才能编写虚拟通道的服务器端。

有关 SDK 文档的详细信息，请参阅 Citrix Virtual Channel SDK for Citrix Receiver for Windows（适用于 Citrix Receiver for Windows 的 Citrix 虚拟通道 SDK）。

Fast Connect 3 凭据插入 API

Fast Connect 3 凭据插入 API 提供用于向 Single Sign-On (SSON) 功能提供用户凭据的接口。此功能在 Citrix Receiver for Windows 4.2 及更高版本中提供。通过此 API，Citrix 合作伙伴可以提供身份验证以及使用 StoreFront 或 Web Interface 将用户登录到虚拟应用程序或桌面，然后断开用户与这些会话的连接的 SSO 产品。

有关 Fast Connect API 文档的详细信息，请参阅 Fast Connect 3 Credential Insertion API for Citrix Receiver for Windows（适用于 Citrix Receiver for Windows 的 Fast Connect 3 凭据插入 API）。

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States