适用于 Windows 的 Citrix Workspace 应用程序 1912 LTSR

Contents

关于此版本

September 25, 2023

1912 中的新增功能

累积更新 7 (CU7) 是 1912 LTSR 的最新更新。

Microsoft Teams 增强功能

CU6 及更高版本支持以下 Microsoft Teams 增强功能：

Desktop Viewer 进入全屏模式时，用户可以从 Desktop Viewer 覆盖的所有屏幕中选择一个屏幕进行共享。在窗口模式下，用户可以共享 Desktop Viewer 窗口。在无缝模式下，用户可以从所有屏幕中选择一个屏幕进行共享。Desktop Viewer 更改窗口模式（最大化、还原或最小化）时，屏幕共享将停止。

CU5 及更高版本支持以下 Microsoft Teams 增强功能：

- 屏幕共享改进功能 - 现在，当您共享屏幕时，仅以本机位图格式捕获 Desktop Viewer 屏幕。
- 对等方现在可以在屏幕共享会话中看到演示者的鼠标指针。
- 改进了视频呈现效果。
- 提高了性能和可靠性。
- WebRTC 媒体引擎现在支持在客户端设备上配置的代理服务器。
- 回声消除、自动增益控制、噪音抑制配置的增强功能：如果 Microsoft Teams 配置了这些选项，Citrix 重定向的 Microsoft Teams 将遵循配置的值。否则，这些选项将默认设置为 True。
- 现在，您可以为媒体流量配置首选网络接口。

  导航到 `\HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream` 并创建名为 `NetworkPreference`(REG_DWORD) 的注册表项。

  根据需要选择以下值之一：

  - 1：以太网
  - 2：Wi-Fi
  - 3：手机网络
  - 5：环回
  - 6：任何

  默认情况下，如果未设置任何值，WebRTC 媒体引擎将选择最佳可用路线。

- 您现在可以禁用音频设备模块 2 (ADM2)，以便将旧版音频设备模块 (ADM) 用于四声道麦克风。这有助于解决通话中与麦克风有关的问题。

  要禁用 ADM2，请导航到 \HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream 并创建一个名为 DisableADM2 (REG_DWORD) 的注册表项，然后将值设置为 1。

- DirectWShow 现在为默认呈现器。

  要更改默认呈现器，请执行以下操作：

  - 启动注册表编辑器。
  - 导航到以下关键位置：HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream。
  - 更新以下值："UseDirectShowRendererAsPrimary"=dword:00000000

    其他可能的值：

    * 0：媒体基础
    * 1：DirectShow（默认）
  - 重新启动 Citrix Workspace 应用程序。

> 注意：
>
> - 只有 Microsoft Windows 10 Desktop 操作系统端点支持此增强功能。
> - Microsoft Windows 7 和 8 操作系统端点不支持此增强功能。
> - 此增强功能支持在安装 Citrix Workspace 应用程序软件包期间确定。我们建议您在将操作系统从 Microsoft Windows 版本 7 升级到版本 10 时卸载 Citrix Workspace 应用程序。

App Protection

> 免责声明
>
> App Protection 策略通过筛选对基础操作系统所需功能的访问（捕获屏幕或键盘按下所需的特定 API 调用）来运行。这意味着 App Protection 策略甚至可以针对自定义的专用黑客工具提供保护。但是，随着操作系统的发展，捕获屏幕和记录键盘的新方法可能会出现。虽然我们会继续识别和解决这些问题，但我们无法保证在特定配置和部署中提供充足的保护。

App Protection 是一项附加功能，可在使用 Citrix Virtual Apps and Desktops 时提供增强的安全性。该功能限制了客户端受键盘记录和屏幕捕获恶意软件影响的能力。App Protection 可防止泄露屏幕上显示的用户凭据和敏感信息等机密信息。该功能可防止用户和攻击者截取屏幕截图以及使用键盘记录器收集和利用敏感信息。

> 注意：
>
> Citrix 建议您仅使用本机 Citrix Workspace 应用程序启动受保护的会话。

使用 Controller 在 StoreFront 与 Controller 之间配置 App Protection。有关在 Controller 上配置 App Protection 的信息，请参阅 App Protection 文档。然后，通过使用以下任一方法来包含 App Protection 组件，将此配置应用于 Citrix Workspace 应用程序：

- 图形用户界面
- 命令行接口

可以在 Citrix Workspace 应用程序安装或按需安装期间包含 App Protection 组件。

> 注意：
>
> - 此功能仅在 Microsoft Windows Desktop 操作系统（例如 Windows 10、Windows 8.1 和 Windows 7）上受支持。
> - 远程桌面协议 (RDP) 不支持此功能。

有关在 Citrix Workspace 应用程序中配置 App Protection 的信息，请参阅 App Protection。

App Protection 功能的增强功能　以前，当您尝试创建受保护窗口的屏幕截图时，整个屏幕（包括后台中未受保护的应用程序）将停止运行。

现在，当您使用截图工具创建屏幕截图时，只有受保护的窗口停止运行或隐藏。可以在受保护窗口外截取该区域的屏幕截图，但在非 Aero 模式下，整个屏幕将停止显示。

但是，如果您使用 **PrtScr** 键捕获屏幕截图，则必须退出 Citrix Workspace 应用程序。

此外，此版本还解决了改进 App Protection 功能的问题。

安装程序增强功能

在早期版本中，如果管理员尝试在具有用户安装的应用程序实例的系统中安装 Citrix Workspace 应用程序，则会阻止安装。

在此版本中，管理员现在可以覆盖用户安装的 Citrix Workspace 应用程序的实例，并成功继续安装。

Citrix Workspace 更新的增强功能

在早期版本中，如果 Citrix Workspace 应用程序由管理员安装，则非管理员无法对其进行更新。

在此版本中，非管理员可以在管理员安装的实例上更新 Citrix Workspace 应用程序。您可以通过右键单击通知区域中的 Citrix Workspace 应用程序图标并选择检查更新来完成此操作。

> 注意：
>
> 检查更新选项现在可用于 Citrix Workspace 应用程序的用户安装的实例和管理员安装的实例。

支持出站代理

智能控制允许管理员定义粒度策略，以便使用 Citrix Gateway 配置和强制执行虚拟应用程序和桌面的用户环境属性。例如，您可能希望禁止用户将驱动器映射到其远程桌面。这可以使用 Citrix Gateway 上的智能控制功能来实现。

但是，当 Citrix Workspace 应用程序和 Citrix Gateway 属于单独的企业帐户时，方案会发生变化。在这种情况下，客户端域无法应用智能控制功能，因为客户端域上不存在网关。相反，您可以利用出站 ICA 代理。出站 ICA 代理允许您使用智能控制功能，即使 Citrix Workspace 应用程序和 Citrix Gateway 部署在不同的组织中亦如此。

Citrix Workspace 应用程序支持使用 Citrix ADC LAN 代理启动会话。可以配置单个静态代理，也可以使用出站代理插件在运行时选择代理服务器。

可以使用以下方法配置出站代理：

- 静态代理：通过提供代理主机名和端口号来配置代理服务器。
- 动态代理：可以使用代理插件 DLL 在一个或多个代理服务器中选择单个代理服务器。

可以使用组策略对象管理模板和注册表编辑器配置出站代理。

有关出站代理的详细信息，请参阅 Citrix Gateway 文档中的出站 ICA 代理支持。

有关在 Citrix Workspace 应用程序中配置出站代理的详细信息，请参阅出站代理。

Citrix 嵌入式浏览器二进制文件

此版本不再安装 Citrix 嵌入式浏览器。在升级到版本 1912 的情况下，Citrix 嵌入式浏览器将被删除。

在未安装 Citrix 嵌入式浏览器的情况下，以下功能会发生变化：

- 浏览器内容重定向不起作用。
- SaaS 和 Web 应用程序不会使用 Citrix 嵌入式浏览器启动。相反，这些应用程序是在 Citrix Secure Browser Service 中启动的。

增强了与 **Microsoft Teams** 的桌面共享功能

使用 Microsoft Teams 共享工作区时，Citrix Workspace 应用程序会在当前共享的监视器区域周围显示一个红色边框。您只能共享 Desktop Viewer 窗口，或者共享其顶部的任何本地窗口。最小化 Desktop Viewer 窗口时，屏幕共享将暂停。

Microsoft Teams 上的端点编码器性能估算器

启动 HdxTeams.exe 进程（嵌入在 Citrix Workspace 应用程序中负责处理 Microsoft Teams 重定向的 WebRTC 媒体引擎）时，该进程会估算端点的 CPU 可以在不过载的情况下维持的最佳编码分辨率。可能的值为 240p、360p、720p 和 1080p。

性能评估过程（也称为 `webrtcapi.EndpointPerformance`）在 HdxTeams.exe 初始化时运行。宏模块代码确定了使用特定端点可以实现的最佳分辨率。然后，在对等方之间或对等方与会议服务器之间的编解码器协商过程中包含尽可能高的分辨率。

有关配置端点编码器的信息，请参阅 Microsoft Teams 上的端点编码器性能估算器。

有关信息，请参阅 Citrix Virtual Apps and Desktops 文档中的 Microsoft Teams 优化。

Citrix Analytics 服务的增强功能

在本版本中，Citrix Workspace 应用程序可以安全地将最新网络跃点的公用 IP 地址传输到 Citrix Analytics 服务。每次会话启动都会收集此数据。它可以帮助 Citrix Analytics 服务分析性能低下问题是否与特定地理区域相关。默认情况下，IP 地址日志会发送到 Citrix Analytics 服务。但是，您可以使用注册表编辑器在 Citrix Workspace 应用程序中禁用此选项。

要禁用 IP 地址日志传输，请导航到以下注册表路径并将 `SendPublicIPAddress` 注册表项设置为 **Off**。

- 在 64 位 Windows 计算机上，导航到 `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle`。
- 在 32 位 Windows 计算机上，导航到 `HKEY_LOCAL_MACHINE\SOFTWARE \Citrix\Dazzle`。

> 注意：
>
> - 尽管 Citrix Workspace 应用程序会传输在其上启动的每个 IP 地址，但 IP 地址传输是在最佳情况下所做的努力。某些地址可能不准确。
> - 在封闭的客户环境中（端点在 Intranet 中运行），请确保在端点上将 URL `https://locus.analytics.cloud.com/api/locateip` 列入白名单。

有关 Performance Analytics 如何使用此信息的详细信息，请参阅性能自助服务。

已修复的问题

October 31, 2023

适用于 **Windows** 的 **Citrix Workspace** 应用程序 **1912 LTSR CU7**

比较对象：Citrix Workspace 应用程序 1912 LTSR CU6

内容重定向

- 当 Desktop Viewer 设置为全屏模式并且端点设备上的默认浏览器已最大化时，双向内容重定向功能可能不会将本地默认 Web 浏览器窗口带到前台。Internet Explorer 以外的本地默认 Web 浏览器会出现此问题。[CVADHELP-19041]

登录/身份验证

- 尝试添加 Citrix Gateway URL 可能会间歇性失败，并显示以下错误消息：

  无法联系身份验证服务。

  [CVADHELP-19415]

会话/连接

- 当至少有一个已配置的 Delivery Controller 无法访问时，使用 Storebrowse 实用程序枚举 Citrix Gateway URL 的资源可能会失败。[CVADHELP-15416]
- 启用 Citrix IME 后，某些第三方应用程序可能无法响应，并且应用程序在用户会话中启动可能会失败。出现此问题的原因是 CtxIme 模块出现故障。[CVADHELP-18511]
- 尝试刷新或启动应用程序会导致出现 **cannot contact store**（无法联系应用商店）错误消息。检索特定的已订阅应用程序的快捷方式描述失败时会出现此问题。

  您的应用程序当前不可用。请在几分钟后重试，或与技术支持人员联系，并提供以下信息**: cannot contact store**（无法与应用商店联系）。

  [CVADHELP-18736]
- 使用 **selfservice.exe** –**init** –**ipoll** –**exit** 命令后，尝试启动用户会话可能会失败。[CVADHELP-19095]
- 应用此修复后，您可以在 HKEY_CURRENT_USER 或 HKEY_LOCAL_MACHINE 中将 **TWITaskbar-GroupingMode** 设置为 **GroupNone**。例如，**TWITaskbarGroupingMode** 注册表项在 HKEY_LOCAL_MACHINE\SOF Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Seamless Windows 下提供。[CVADHELP-19106]

用户体验

- 在多显示器环境中启用“无损构建”图形策略时，使屏幕跨便携式计算机和外部显示器可能会导致图像失真。[CVADHELP-19065]

适用于 **Windows** 的 **Citrix Workspace** 应用程序 **1912 LTSR CU6**

比较对象：Citrix Workspace 应用程序 1912 LTSR CU5

客户端设备问题

- 在 Citrix Workspace 应用程序会话中，启动 YouTube 视频或 Microsoft Teams 通话，然后断开耳机的连接可能会使会话无响应。[CVADHELP-17629]

安装、卸载、升级

- 在未安装自助服务的情况下将适用于 Windows 的 Citrix Workspace 应用程序从版本 CU4 升级到版本 CU5 时，可能会出现以下提示：

  从不受支持的版本升级

  Citrix Workspace 将自动卸载旧版本并删除所有设置，您可以稍后还原这些设置。否则，您将必须手动删除所有内容。单击“确定”以继续。

  [CVADHELP-18790]

登录/身份验证

- 使用不正确的密码登录 Citrix Gateway 允许 Storebrowse 进行多次身份验证尝试，这可能会锁定用户帐户。[CVADHELP-17467]
- 尝试通过 Citrix Gateway 使用智能卡时，初始化后 Citrix Workspace 应用程序身份验证可能会失败。如果在 15 分钟后刷新身份验证过程，Citrix Workspace 内部的嵌入式浏览器中可能会显示 404 错误消息。这会导致应用程序卡在身份验证循环中，直到您关闭并重新打开应用程序。[CVADHELP-18305]

会话/连接

- 当文件夹重定向共享处于脱机状态时，使用文件夹重定向打开已发布的应用程序可能会失败，并显示以下错误消息。

  Unable to launch application（无法启动应用程序）

  [CVADHELP-16387]

- 尝试使用启用了限制每个用户一个实例和 **vPrefer** 选项的快捷方式打开应用程序时，Citrix Director 上可能会出现连接失败错误。[CVADHELP-17372]
- 在电话会议期间，在 HDX 优化模式下使用 Microsoft Teams 时，传入呼叫的视频部分可能会闪烁不定。[CVADHELP-17398]
- Citrix Workspace 应用程序可能会轮询内部应用商店的外部信标。应用此修复后，在没有网关的情况下使用应用商店时，不会轮询外部信标。[CVADHELP-18275]

- 如果没有适当的权限，则无法创建通过 Citrix Workspace 应用程序发布的应用程序的快捷方式。因此，每次刷新时都可能会将图标下载到用户配置文件中，从而增加端点上的缓存大小和 StoreFront 端的 CPU 占用量。[CVADHELP-18609]
- 从适用于 Mac 的 Citrix Workspace 应用程序向适用于 Windows 的 Citrix Workspace 应用程序进行的优化的 Microsoft Teams 点对点通话可能会断开连接。[CVADHELP-18696]
- 如果客户端具有多个 NIC，使用指定客户端 IP 地址的访问策略规则从交付组启动会话可能会失败。

  ```
  Rule: Set-BrokerAccessPolicyRule -Name <rulename> -includedClientIPs
   <Client ip address>
  ```

  [CVADHELP-18783]

系统异常

- Citrix 身份验证管理器 (AuthManSvr.exe) 可能会在登录期间意外退出。[CVADHELP-17233]

用户体验

- 在多显示器环境中在窗口模式下打开桌面窗口时，可能会出现以下行为。

  在显示器 1 上打开并拖动到显示器 2 的窗口可能在显示器 1 上显示为最大化，而非在显示器 2 上显示为最大化。

  [CVADHELP-17373]

用户界面

- 应用此修复后，当配置了多个帐户和当前帐户注册表时，您可以切换到所需的帐户。[CVADHELP-17718]
- 使用组策略对象同时配置已启用和已禁用的应用商店可能会导致启用的应用商店首次出现非 X1 用户界面或绿色气泡用户界面，而非 X1 用户界面。[CVADHELP-17942]
- 在 Citrix Workspace 应用程序中禁用应用商店帐户可能不会从开始菜单或桌面中删除应用程序快捷方式。[CVADHELP-18260]

适用于 **Windows** 的 **Citrix Workspace** 应用程序 **1912 LTSR CU5**

比较对象：Citrix Workspace 应用程序 1912 LTSR CU4

客户端设备问题

- 使用 Citrix Workspace 应用程序 1912 LTSR CU4 时，使用 COM 端口号大于 9 的设备可能无法在会话中映射。[CVADHELP-17734]

安装、卸载、升级

- 尝试使用 **/forceinstall** 参数升级适用于 Windows 的 Citrix Workspace 应用程序可能会失败。Receiver 清理实用程序无法启动清理过程时会出现此问题。[CVADHELP-17656]

登录/身份验证

- 如果 Citrix Gateway 会话超时，Citrix Workspace 可能无法在启动应用程序时提示进行身份验证。[CVADHELP-17187]

无缝窗口

- 某些第三方应用程序可能仍保留在前台，使其他已启动的应用程序保留在后台。[CVADHELP-16897]

安全问题

- 当 USB .cat 文件使用 SHA-1 证书签名时，尝试安装适用于 Windows 的 Citrix Workspace 应用程序 1912 LTSR 可能会失败。[CVADHELP-17679]

会话/连接

- 在某些浏览器上使用 HTML 或动画在 GPU 瘦客户端上浏览 Web 页面时，适用于 Windows 的 Citrix Workspace 应用程序可能会变得无响应。wfica32 进程占用大量内存时会出现此问题。[CVADHELP-16172]
- 将适用于 Windows 的 Citrix Workspace 应用程序升级到版本 1912 LTSR CU1 或 CU2 后，会话可靠性可能会失败。启用了 Enlightened Data Transport (EDT) 协议时，如果连接是通过 Citrix Gateway 建立的，则会出现此问题。[CVADHELP-16694]
- CGP 端口 (2598) 在端点上被阻止时通过适用于 Windows 的 Citrix Workspace 应用程序启动会话可能会失败。[CVADHELP-17632]

用户体验

- 此修复通过使用新的组策略对象设置可信应用商店帐户列表来禁止显示信任帐户弹出消息。[CVADHELP-16597]
- 在 VDA 上使用某些第三方应用程序时，鼠标移动可能会延迟。[CVADHELP-16737]

用户界面

- 使用适用于 Windows 的 Citrix Workspace 应用程序 1912 LTSR CU2 时，“开始”菜单快捷方式可能不会自动刷新。在后端上添加了新应用程序或进行了更改时会出现此问题。[CVADHELP-17122]
- 将 **CurrentAccount** 值设置为注册表 HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle 下的 **AllAccount** 可能不起作用。存在一个或多个应用商店帐户时会出现此问题。[CVADHELP-17229]
- 尝试使用适用于 Windows 的 Citrix Workspace 应用程序登录 Wyse 瘦客户端设备时，授权提示窗口可能会显示在 **Desktop Lock** 屏幕后面。因此，直到将授权提示窗口置于前台后才能登录。[CVADHELP-17880]

适用于 **Windows** 的 **Citrix Workspace** 应用程序 **1912 LTSR CU4**

比较对象：Citrix Workspace 应用程序 1912 LTSR CU3

客户端设备问题

- 启用客户端 **COM** 端口重定向策略后，尝试访问蓝牙设备的 COM 端口可能会失败。[CVADHELP-14939]

登录/身份验证

- 用户名包含变音字符时，尝试登录适用于 Windows 的 Citrix Workspace 应用程序版本 1912 LTSR CU3 可能会失败。[CVADHELP-17267]

安全问题

- 二进制文件中可能缺少控制流防护二进制文件保护。[CVADHELP-16531]

会话/连接

- 在点对点通话期间使用 Microsoft Teams 中的屏幕共享功能时，可能会出现黑屏。[CVADHELP-15605]
- 如果 **HDX** 自适应传输策略设置为首选，并且启用了 **EDT MTU** 发现，则在尝试启动应用程序或桌面时，可能会显示灰屏或黑屏以及一条警告消息。[CVADHELP-15805]
- 即使在禁用了应用程序或更改快捷方式的路径后，为应用程序创建的快捷方式也可能无法删除。[[CVADHELP-16448]
- 通过 Citrix Gateway 连接或断开 VPN 连接时，尝试通过适用于 Windows 的 Citrix Workspace 应用程序启动应用程序可能会失败。[CVADHELP-16714]
- 在双跃点场景中时，端点客户端名称可能无法传递给 Delivery Controller 或 Director。VDA 版本 2003 及更高版本会出现此问题。[CVADHELP-16783]

- 将适用于 Windows 的 Citrix Workspace 应用程序升级到版本 1912 LTSR CU1 或 CU2 后，会话可靠性可能会失败。启用了 Enlightened Data Transport (EDT) 协议时，如果连接是通过 Citrix Gateway 建立的，则会出现此问题。[CVADHELP-16694]

用户体验

- 使用适用于 Windows 的 Citrix Workspace 应用程序版本 1912 LTSR CU2 时，会话可能会显示屏幕内容模糊的图形工件。[CVADHELP-16451]
- 将适用于 Windows 的 Citrix Receiver 版本 4.9.6 升级到 Citrix Workspace 应用程序版本 1912 LTSR CU2 或 CU3 后，尝试启动应用程序快捷方式，某些桌面上的快捷方式图标可能会闪烁不定。[CVADHELP-16967]

用户界面

- 如果在会话运行时选择注销，则会显示注销提示以确认该操作。按取消将导致错误。[CVADHELP-15516]
- 将适用于 Windows 的 Citrix Receiver 4.9 LTSR CU7 升级到适用于 Windows 的 Citrix Workspace 应用程序版本 CU2 或 CU3 并尝试设置默认应用商店帐户时，可能会发生不一致的行为。例如，默认应用商店帐户始终默认为“所有帐户”。进行此更改后，即使在退出并重新启动 Citrix Workspace 应用程序后，仍然将主应用商店帐户设置为不同的应用商店名称。[CVADHELP-16903]

适用于 **Windows** 的 **Citrix Workspace** 应用程序 **1912 LTSR CU3**

比较对象：Citrix Workspace 应用程序 1912 LTSR CU2

安装、卸载、升级

- 尝试使用手动创建的快捷方式刷新 Citrix Workspace 应用程序时，该快捷方式可能会被删除，然后重新创建。[CVADHELP-15397]

键盘

- 使用日语键盘时，全角输入模式可能无法与通过本地应用程序访问启动的 Microsoft Excel 一起使用。启用了 App Protection 功能的适用于 Windows 的 Citrix Workspace 应用程序会出现此问题。[CVADHELP-15410]

登录/身份验证

- 即使启用了使我保持登录状态和 **don’t ask again for 60 days**（60 天内不再询问）策略之后，Microsoft Azure 多重身份验证仍可能会提示进行身份验证。

> 注意：
>
> 我们建议用户退出其应用商店，而非从其应用商店中注销。如果用户使用 webview 身份验证从应用商店中注销，系统可能会再次提示其进行身份验证，因为在此类情况下，Internet Explorer cookie 会被清除。默认情况下，此修复处于启用状态（存储 cookie）。可以通过启用 **Citrix** 组件 **> Citrix Workspace >** 用户身份验证下的阻止存储永久性 **cookie** GPO 策略来禁用此修复。如果禁用此修复，cookie 将不存储，并在注销过程中清除。如果禁用此修复，cookie 将不存储，并在注销过程中清除。

[CVADHELP-14814]

- 在加入了 Azure Active Directory (AD) 的设备上，当 Citrix Workspace 应用程序尝试访问应用商店，然后传递端点登录凭据时，用户可能无权登录。此外，无法使用其他用户帐户登录。[CVADHELP-14844]

打印

- 将原始数据格式的文档发送到打印队列时，可能无法打印该文档。使用 XPS 打印机驱动程序时会出现此问题。[CVADHELP-14497]

会话/连接

- 在某些情况下，Citrix Studio 中显示的 Citrix 产品许可证使用情况与 Citrix License Manager 中显示的许可证使用情况不一致。[CVADHELP-14950]
- 启用 **vPrefer** 选项后，App-V 应用程序可能会在远程服务器上启动，而非在本地服务器上启动。[CVADHELP-15356]
- 通过适用于 Windows 的本机 Citrix Workspace 应用程序启动已发布的桌面时，本机 Citrix Workspace 应用程序将自动在桌面前台运行。启用了本地应用程序访问功能时会出现此问题。[CVADHELP-15654]
- Selfservice.exe 进程可能会变得无响应，并且可能会显示 **.NET-BroadcastEventWindow.4.0.0.0.1** 提示。尝试从运行 Windows 10 版本 1909 的系统注销时会出现此问题。[CVADHELP-15700]
- 将适用于 Windows 的 Citrix Workspace 应用程序配置为在建立会话时连接到所有帐户。如果从 Citrix Workspace 应用程序注销并重新登录，应用商店帐户设置将更改为一个应用商店帐户，而非默认为所有帐户。[CVADHELP-15728]
- 启用双向内容重定向策略后，尝试将 URL 从客户端重定向到 VDA 可能会失败。[CVADHELP-15739]
- 在代理服务器不使用端口 8080 的情况下，Citrix Workspace 应用程序可能无法连接到已发布的应用程序和桌面。出现此问题的原因是适用于 Windows 的 Citrix Workspace 应用程序可能无法使用代理端口而改为使用默认端口 8080。[CVADHELP-15977]
- 适用于 Windows 的 Citrix Workspace 应用程序可能会忽略代理类型设置。在非英语版本的 Microsoft Windows 操作系统中会出现此问题。[CVADHELP-16017]

- 当 **EnableFactoryReset** 注册表设置设为 **False** 时，尝试卸载 Citrix Workspace 应用程序可能会失败并显示以下错误消息：

  此功能已禁用。

  [CVADHELP-16114]

- 使用处于优化模式的 Microsoft Teams 时，当您加入电话会议时，音频可能会失真。[CVADHELP-16232]

系统异常

- 启用 **EchoCancellation** 策略并将音频质量设置为中等后，wfica32.exe 进程可能会间歇性退出，导致会话最终断开连接。[CVADHELP-14568]
- Receiver.exe 进程可能会意外退出。[CVADHELP-15669]

适用于 **Windows** 的 **Citrix Workspace** 应用程序 **1912 LTSR CU2**

比较对象：Citrix Workspace 应用程序 1912 LTSR CU1

安装、卸载、升级

- 尝试将适用于 Windows 的 Citrix Workspace 应用程序从版本 190*x* 升级到版本 1912 可能会失败。可执行文件夹路径中的某处存在违规文件时会出现此问题。[CVADHELP-15277]
- 尝试将 Citrix Workspace 应用程序从版本 1912 更新到版本 1912 CU1 或 2006 时，Citrix Workspace 应用程序的更新功能可能无法在非英语操作系统中运行。[CVADHELP-15357]

键盘

- 使用中文输入法编辑器 (IME) Wuxiami 时，Shift 键可能会保持在向下位置。如果通用本地时间设置为开，则会出现此问题。[CVADHELP-15243]

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 CTX277662。[CVADHELP-15613]

会话/连接

- 在禁用了注册表编辑工具的情况下，执行升级后可能无法保留先前安装的注册表项。因此，尝试启动桌面失败。[CVADHELP-15104]

- Citrix Workspace 应用程序可能会在 1911 之前的版本上显示脚本错误，在 1911 及更高版本上显示一个空白页面。应用 Microsoft 安全基准 GPO 策略时，使用 Internet Explorer WebBrowser 控件显示登录页面时会出现此问题。[CVADHELP-15475]
- 在双跃点场景中，尝试使用开始菜单中的快捷方式启动应用程序可能会失败。如果启用了每个用户一个实例的应用程序限制，则会出现此问题。[CVADHELP-15576]
- 通过 Citrix Workspace 应用程序版本 1912 或更高版本登录到应用商店时，应用程序可能无法枚举。[CVADHELP-15597]

用户体验

- 如果您通过 VPN 连接到自助服务插件 (SSP)，尝试刷新 SSP 可能会失败。[CVADHELP-14418]
- 尝试使用 **SelfService.exe -init -ipoll -exit** 命令关闭 SelfService.exe 进程可能会失败。[CVADHELP-15126]
- 使用 HP Active stylus 触控笔在已发布的应用程序中写入时，写入功能可能会遇到三到四秒的延迟。[CVADHELP-15203]
- 在对适用于 Windows 的 Citrix Workspace 应用程序进行全新安装或将现有安装升级到最新安装后，尝试启动会话可能会失败。会话启动将卡在正在准备您的桌面屏幕上。使用 Citrix Gateway URL 配置 Desktop Lock 时会出现此问题。

  > 注意：
  >
  > 首次使用 Citrix Gateway URL 和 Desktop Lock 配置适用于 Windows 的 Citrix Workspace 应用程序时，在 Desktop Lock 出现之前的一段时间内会出现黑屏。如果黑屏保持很长时间，请使用 **Ctrl+Alt+Delete**（适用于物理机）和 **Ctrl+Alt+End**（适用于虚拟机）注销。

  [CVADHELP-15334]
- 将 Citrix Workspace 应用程序从版本 1912 升级到版本 1912 CU1 后，应用程序枚举可能很慢，大约需要 10 分钟才能完成。[CVADHELP-15766]

适用于 **Windows** 的 **Citrix Workspace** 应用程序 **1912 LTSR CU1** 修补程序 **1 (19.12.1001)**

比较对象：适用于 Windows 的 Citrix Workspace 应用程序 1912 LTSR CU1

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 CTX277662。[CVADHELP-15613]

适用于 **Windows** 的 **Citrix Workspace** 应用程序 **1912 LTSR CU1**

比较对象：Citrix Workspace 应用程序 1912 LTSR

内容重定向

- 尝试重定向长 URL 时，URL 可能不会重定向到 VDA，并且 Redirector.exe 进程意外退出，并出现以下异常：

  INVALID_CRUNTIME_PARAMETER

  [CVADHELP-13197]

安装、卸载、升级

- 尝试在运行 Windows 10 的 VDA 上安装或升级 Citrix Workspace 应用程序可能会失败。执行以下步骤时会出现此问题：

  1. 安装 Citrix Workspace 应用程序。
  2. 安装 VDA。
  3. 将 Citrix Workspace 应用程序升级到更高版本。

  出现该问题的原因是，升级或安装会导致删除 Citrix 显示适配器。[CVADHELP-13764]

- 尝试使用自动更新功能来自动更新 HDX RealTime Media Engine (RTME) 以及 Citrix Workspace 应用程序可能会失败。RTME 无法升级到最新版本。[CVADHELP-15047]

登录/身份验证

- 如果使用两个不同的帐户将两个应用商店添加到适用于 Windows 的 Citrix Workspace 应用程序，则删除主应用商店后，“登录”按钮可能无法用于辅助应用商店。[CVADHELP-13805]
- 启用了多重身份验证并使用“Windows 安全”对话框登录时，在向应用商店进行身份验证时，不会显示 Active Directory 联合身份验证服务 (ADFS) 对话框。[CVADHELP-14316]
- 将 Citrix Gateway 配置为通过 Citrix Workspace 应用程序支持单点登录 (SSO) 时，SSO 可能会失败。当用户名或密码包含 **%**、**=** 和 **&** 等特殊字符时，会出现此问题。[CVADHELP-14564]

SDK

- 此修复程序改进了对传统私钥句柄提供的支持。[CVADHELP-14530]

会话/连接

- 启用了本地应用程序访问和 Desktop Lock 时，当您按 Ctrl+Alt+Del 键后执行切换用户功能时，本地用户会话可能会重新连接。但是，当服务器会话尝试重新连接时，VDA 会停留在显示已连接到桌面的消息的白屏上。桌面永远不会显示。[CVADHELP-13046]
- 在多显示器环境中，尝试最大化用户会话可能会失败。重新停靠您的便携式计算机时会出现此问题。[CVADHELP-13614]
- 在双跳场景中，当您尝试启动会话时，Citrix HDX Engine 可能会意外退出。[CVADHELP-13915]
- 在 Citrix Workspace 应用程序中启用 **vPrefer** 选项后，尝试启动 App-V 应用程序可能会失败并显示以下错误消息：

  无法启动

  [CVADHELP-14039]
- 将已发布的应用程序添加到收藏夹后，只能打开一个应用程序。当这些已发布的应用程序使用相同的可执行文件名称（如 **KEYWORDS:prefer=" <application_name>** 所示）时，会出现此问题。[CVADHELP-14098]
- 升级 Citrix Workspace 应用程序后，与已弃用的功能 **HDX MediaStream for Flash**（例如，Flash 和 Flash2）相关的注册表值可能会从注册表设置 HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\ICA 3.0\VirtualDriver 中删除。此问题可能会导致连接失败。[CVADHELP-14850]

系统异常

- 当您尝试重新连接到会话时，wfica32.exe 进程可能会意外退出。适用于 Windows 的 Citrix Workspace 应用程序的 1904.1 版本会出现此问题。[CVADHELP-12807]
- 启用本地应用程序访问后，会话可能变得无响应，并显示以下错误消息：

  Citrix HDX 引擎未响应

  [CVADHELP-14058]
- 如果您尝试在未配置自助服务模式的情况下安装 Citrix Workspace 应用程序，则可能会发生异常。当您从高级首选项表中打开快捷方式和重新连接菜单时，会出现此问题。Citrix Workspace 应用程序 1907-2002 版本会出现此问题。[CVADHELP-14940]

TWAIN

- 尝试使用 TWAIN 设备执行扫描可能会失败。Windows 任务管理器的应用程序选项卡上的状态列中显示 Citrix HDX 引擎“未响应”。[CVADHELP-14782]

用户体验

- 在双跃点场景中（即适用于多会话操作系统的 VDA 在第一个跃点中运行，而已发布的应用程序则在第二个跃点中运行），Citrix Workspace 应用程序帐户菜单中的“刷新应用程序”选项可能无法正常工作。[CVADHELP-13230]
- 在适用于 Windows 的 Citrix Workspace 应用程序上使用应用商店 URL 添加帐户时，可能需要很长时间才能完成。当该 URL 包含端口号时，会出现此问题。[CVADHELP-14051]
- 您可以在系统托盘中看到两个 Citrix Workspace 应用程序图标。Citrix Workspace 应用程序 1912 版本会出现此问题。[CVADHELP-14577]
- 在 VDA 环境中使用单点登录时，可能会出现闪屏。当您将适用于 Windows 的 Citrix Workspace 应用程序升级到版本 1911 或更高版本时，会出现此问题。[CVADHELP-14590]

用户界面

- 应用程序可能会尝试间歇性地进入前台，取代当前的应用程序。它在任务栏中的图标可能会闪烁不定，通知用户应用程序尝试进入前台。[CVADHELP-13071]

适用于 **Windows** 的 **Citrix Workspace** 应用程序 **1912 LTSR**

> 注意：
>
> 如果您是当前正在使用 Citrix Workspace 应用程序 1911 的当前版本的客户，并且希望移动到 LTSR 轨道：
>
> 与 Citrix Workspace 应用程序 1911 相比，此版本包含以下修复。
>
> 如果您是当前正在使用 Citrix Receiver 4.9 for Windows 的客户，并且希望保留在 LTSR 轨道上：
>
> 此版本包含 Citrix Receiver for Windows 4.9（包括其 CU）到 4.12 中的所有修复和 Citrix Workspace 应用程序 1808 到 1911 中的所有修复，并列出了 Citrix Workspace 应用程序 2002 中的以下修复（与 Citrix Workspace 应用程序 1911 相比）：版本 1912 包含 Citrix Receiver for Windows 4.9 LTSR CU9 与 Citrix Workspace 应用程序版本 1911 之间的所有修复以及以下修复：

HDX MediaStream Windows Media 重定向

- 在多显示器环境中，当您在用户会话中使用 Windows Media Player 播放 MP4 视频时，该视频可能会在主显示器上正常播放。但是，当您将播放器移动到其他屏幕时，使用扩展坞通过 DisplayLink 连接的辅助显示器或扩展显示器上可能会出现黑屏。[CVADHELP-11848]

会话/连接

- 尝试使用快速智能卡从 HDX RealTime Media Engine 重新连接到会话时，HDX RealTime Media Engine 可能会意外退出。[CVADHELP-12605]

- 当已发布的应用程序收到许多在短时间内播放短声音的请求时，wfica32.exe 进程可能会意外退出。[CVADHELP-12855]
- 达到会话超时后，会话可能会自动注销。当您尝试再次启动会话时，会话启动所需的时间超过正常时间。出现网络中断时会出现此问题。[CVADHELP-13017]
- 无缝应用程序窗口可能会呈现为部分截断并保持截断，直到您手动调整窗口大小为止。[CVADHELP-13108]
- Citrix Workspace 应用程序现在在每次刷新或启动时都会执行快捷方式图标的存在检查。如果图标不可用，Citrix Workspace 应用程序将再次获取该图标。这样做可以确保快捷方式正确显示。[RFWIN-15501]
- 尝试启用“双向内容重定向”策略（在计算机配置 **>** 管理模板 **>** 经典管理模板 **(ADM) > Citrix** 组件 **> Citrix Workspace >** 用户体验下）时，系统会提示您键入特定于 URL 的条目，即使您未启用特定于 URL 的应用程序或桌面覆盖亦如此。[RFWIN-15867]

系统异常

- 捕获 CDF 跟踪时，Receiver.exe 进程可能会意外退出。[CVADHELP-13077]

已知问题

June 14, 2023

适用于 **Windows** 的 **Citrix Workspace** 应用程序 **1912 LTSR CU7** 中的已知问题

在此版本中没有发现新问题。

适用于 **Windows** 的 **Citrix Workspace** 应用程序 **1912 LTSR CU6** 中的已知问题

- 当您在 Microsoft Teams 中以已发布的应用程序形式共享屏幕时，不会显示共享屏幕底部的红色边框。[LCMRFWIN-4194]

适用于 **Windows** 的 **Citrix Workspace** 应用程序 **1912 LTSR CU5** 中的已知问题

- 将某些第三方远程处理应用程序（例如 mRemoteNG）连接到端点，将已发布的应用程序的应用程序工具栏停靠到端点两侧时，系统可能会变得无响应，CPU 使用率为 100%。[LCMRFWIN-4164]
- 尝试在 Microsoft Teams 优化的通话过程中停止屏幕共享时，会话可能会间歇性变得无响应。[LCMRFWIN-4184]

适用于 **Windows** 的 **Citrix Workspace** 应用程序 **1912 LTSR CU4** 中的已知问题

- 在会话期间，当您单击检查更新并成功下载更新时，当前会话不会在下载成功对话框中列出。[RFWIN-23152]

适用于 **Windows** 的 **Citrix Workspace** 应用程序 **1912 LTSR CU3** 中的已知问题

在此版本中没有发现新问题。

适用于 **Windows** 的 **Citrix Workspace** 应用程序 **1912 LTSR CU2** 中的已知问题

在此版本中没有发现新问题。

适用于 **Windows** 的 **Citrix Workspace** 应用程序 **1912 LTSR CU1** 中的已知问题

- 尝试在 WebEx 会议中使用网络摄像机可能会导致 Citrix Workspace 应用程序变得无响应。将 UDP 音频设置为中时会出现此问题。

  解决方法为，在注册表编辑器中导航到以下路径，并设置以下内容：

  路径：HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced

  名称：EchoCancellation

  类型：REG_SZ

  值：FALSE

  [DOCFB-3805]

适用于 **Windows** 的 **Citrix Workspace** 应用程序 **1912 LTSR** 中的已知问题

- 尝试使用 **Print Screen** 键捕获屏幕可能会失败。最小化受保护的 Citrix Workspace 应用程序会话时会出现此问题。[RFWIN-15155]
- 当您在已发布的会话和本地设备上启动 Microsoft Word 并从帐户中删除应用商店时，在本地设备上启动应用程序时会出现以下错误消息：

  是否要查找 **Citrix Workspace** 中用于打开此文件的应用程序**?**

  [RFWIN-15884]
- 尝试在启用了 SSL 的 VDA 上启动会话可能会失败。[RFWIN-16129]
- 在受保护的桌面会话中，尝试截取非受保护会话的屏幕截图可能会失败。[RFWIN-16704]
- 您可能无法使用图形用户界面删除使用组策略对象 (GPO) 管理模板添加的应用商店详细信息。[RFWIN-16754]
- 尝试更改受保护会话中的显示内容会导致会话退出。[RFWIN-16784]

第三方声明

June 14, 2023

适用于 Windows 的 Citrix Workspace 应用程序 1912 LTSR 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：

适用于 Windows 的 Citrix Workspace 应用程序第三方声明（PDF 下载）

系统要求和兼容性

April 22, 2024

要求

- 1 GB RAM。
- .NET Framework 要求
  - 自助服务插件需要 NET 4.6.2。此插件允许您从适用于 Windows 的 Citrix Workspace 应用程序用户界面或命令行订阅和启动应用程序和桌面。有关详细信息，请参阅使用命令行参数。
- 最新版本的 Microsoft Visual C++ Redistributable。

  > 注意：
  >
  > Citrix 建议您使用最新版本的 Microsoft Visual C++ Redistributable。否则，升级过程中可能会出现重新启动提示。

  自版本 1904 起，Citrix Workspace 应用程序安装程序包不包含 Microsoft Visual C++ Redistributable 的单个二进制文件，但包含 Microsoft Visual C++ Redistributable 安装程序。Citrix Workspace 应用程序安装程序会在安装过程中检查系统中是否存在 Microsoft Visual C++ Redistributable 程序包，并在必要时进行安装。Citrix Workspace 应用程序 1912 及更高版本需要 Microsoft Visual C++ Redistributable 14.24.28127.4 或更高版本。

  > 注意：
  >
  > 尝试使用非管理员权限在没有 Microsoft Visual C++ Redistributable 软件包的系统中安装 Citrix Workspace 应用程序可能会失败。

  只有管理员能够安装 Microsoft Visual C++ Redistributable 程序包。

  有关.NET Framework 或 Microsoft Visual C++ Redistributable 安装问题的故障排除，请参阅知识中心文章 CTX250044。

兼容性列表

Citrix Workspace 应用程序与当前所有受支持的 Citrix Virtual Apps and Desktops、Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）和 Citrix Gateway 版本兼容，这些版本在 Citrix 产品生命周期列表中列出。

Citrix Workspace 应用程序与以下 Windows 操作系统兼容：

> 注意：
>
> Citrix Gateway End-Point Analysis Plug-in (EPA) 在 Citrix Workspace 上受支持。在本机 Citrix Workspace 应用程序中，仅在使用 nFactor 身份验证时才受支持。有关详细信息，请参阅 Citrix ADC 文档中的将预身份验证和后身份验证 EPA 扫描配置为 nFactor 身份验证中的一个因素。

操作系统

Windows 10 32 位和 64 位 Enterprise Edition。有关兼容的 Windows 10 操作系统的详细信息，请参阅 Windows 10 与适用于 Windows 的 Citrix Workspace 应用程序的兼容性。

Windows 10 32 位和 64 位 Pro Edition（自适用于 Windows 的 Citrix Workspace 应用程序 1912 LTSR CU5 更高版本起受支持）

Windows 8.1，32 位和 64 位版本（包括 Embedded Edition）

Windows 7，32 位和 64 位版本（扩展安全更新 - ESU）

Windows 7 Embedded Standard (Extended Security Update - ESU)

Windows Thin PC

Windows Server 2016

Windows Server 2012 R2 Standard Edition 和 Datacenter Edition

Windows Server 2019

Windows Server 2008 R2

Windows 10 Enterprise LTSC 2019

Windows 10 Enterprise 2016 LTSB 1607

Windows 10 与适用于 **Windows** 的 **Citrix Workspace** 应用程序的兼容性

> 注意：
>
> - 不建议将早期发布的 Citrix 软件版本安装到半年频道版本。选择这样做的客户将需要验证生成支持电话的任何问题是否已在较新的 Citrix 软件版本（如果可用）中得以解决，并且可能需要升级到较新的 Citrix 软件版本。

> - 一旦 Windows 10 版本到达服务终止状态，该版本将不再由 Microsoft 提供服务或支持。Citrix 支持在其制造商支持的操作系统中运行其软件。有关 Windows 10 结束服务的信息，请参阅 Microsoft 的 Windows 生命周期概况介绍。

Citrix Workspace 应用程序版本	Windows 10 Enterprise Edition 版本号	内部版本号
1912 CU7 及更高版本	LTSC 2021	19044
1912 CU6 及更高版本	21H2	19044
1912 CU6 及更高版本	21H2	19044
1912 CU5 及更高版本	21H1	19043.1165
1912 CU2 及更高版本	20H2	19042.685
1912 CU1 及更高版本	2004	19041.329
1911 及更高版本	1909	18363.418
1909 及更高版本	1903	18362.116
1812 及更高版本	1809	17763.107
1808 及更高版本	10 1803	17134.376

支持的浏览器

有关支持的浏览器列表，请参阅通过 Citrix Receiver for Web 站点访问应用商店。

操作系统列表

在启用了触控功能的设备上受支持的操作系统
Windows 10
Windows 8
Windows 7

在 **VDA** 上受支持的操作系统
Windows 10

在 **VDA** 上受支持的操作系统
Windows 8
Windows 7
Windows 2012 R2
Windows Server 2016
Windows 2008 R2

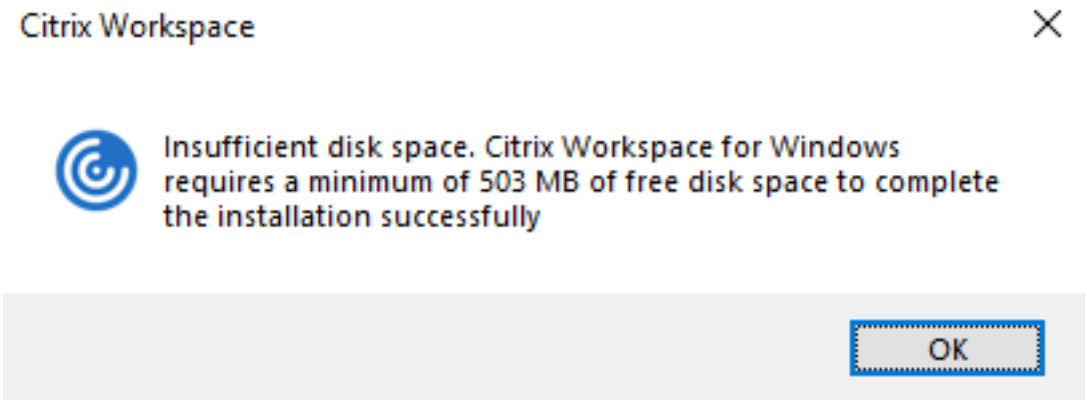
验证可用磁盘空间

下表提供了有关安装适用于 Windows 的 Citrix Workspace 应用程序所需的磁盘空间的详细信息：

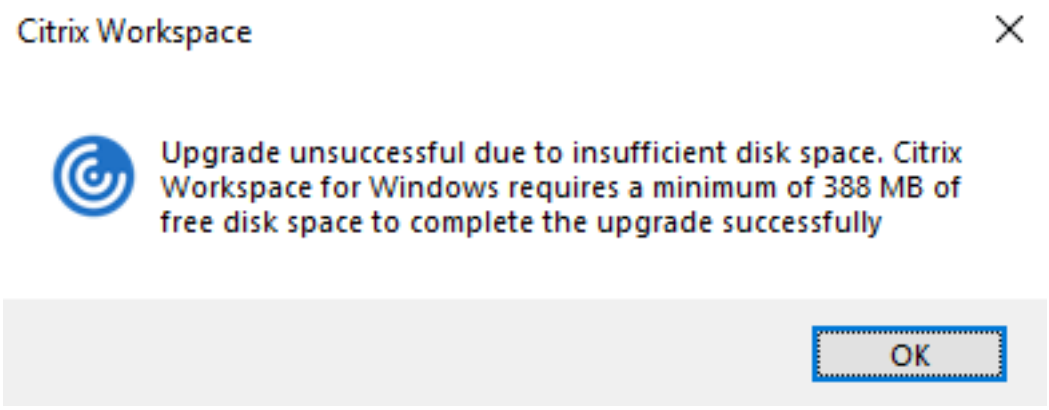
安装类型	所需磁盘空间
全新安装	572 MB
升级	350 MB

Citrix Workspace 应用程序检查完成安装所需的磁盘空间。该验证在全新安装及升级过程中执行。

执行全新安装时，安装将在磁盘空间不足时停止，并显示以下对话框。



升级过程中，安装将在磁盘空间不足时终止，并显示以下对话框。



> 注意：
>
> - 安装程序仅在解压缩安装包后检查磁盘空间。
> - 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。

连接、证书和身份验证

连接

- HTTP 应用商店
- HTTPS 应用商店
- Citrix Gateway 10.5 及更高版本
- Web Interface 5.4

Certificates（证书）

> 注意：
>
> 适用于 Windows 的 Citrix Workspace 应用程序带有数字签名。数字签名带有时间戳。因此，证书即使在过期后也有效。

- 专用（自签名）证书
- Root
- 通配符证书
- 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，要从中访问 Citrix 资源的用户设备上必须安装组织的证书颁发机构颁发的根证书。

> 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并继续，则会显示应用程序但无法启动。

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 Workspace 应用程序支持通配符证书，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，可以不使用通配符证书，而是改为使用包含采用使用者备用名称 (SAN) 扩展的服务器名称列表的证书。私有证书颁发机构和公共证书颁发机构负责颁发这些证书。

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 Citrix Gateway 服务器证书。有关信息，请参阅 Configuring Intermediate Certificates（配置中间证书）。

身份验证

StoreFront 身份验证

	适用于 **Web** 的 **Workspace**（使用浏览器）	**StoreFront** 服务站点（本机）	**StoreFront**、**Citrix Virtual Apps and Desktops**（本机）、**Citrix DaaS**	**Citrix Gateway** 到适用于 **Web** 的 **Workspace**（浏览器）	**Citrix Gateway** 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 *

	适用于 **Web** 的 **Workspace**（使用浏览器）	**StoreFront** 服务站点（本机）	**StoreFront**、**Citrix Virtual Apps and Desktops**（本机）、**Citrix DaaS**	**Citrix Gateway** 到适用于 **Web** 的 **Workspace**（浏览器）	**Citrix Gateway** 到 **StoreFront** 服务站点（本机）
双重身份验证（域 + 安全令牌）				是 *	是 *
SMS				是 *	是 *
智能卡	是	是		是	是
用户证书				是（Citrix Gateway 插件）	是（Citrix Gateway 插件）

* 在设备上安装或不安装 Citrix Gateway 插件均可。

> 注意：
>
> Citrix Workspace 应用程序支持使用 Citrix Gateway 到 StoreFront 本机服务的双重身份验证（域 + 安全令牌）。

对 **Web Interface** 进行身份验证　Citrix Workspace 应用程序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 Citrix Gateway** 站点	**Citrix Gateway** 到 **Web Interface**（浏览器）	**Citrix Gateway** 到 **Web Interface Citrix Gateway** 站点
匿名	是			
域	是	是	是 *	
域直通	是	是		
安全令牌			是 *	
双重身份验证（域 + 安全令牌）			是 *	
SMS			是 *	
智能卡	是	是		
用户证书			是（Citrix Gateway 插件）	

* 仅在包含 Citrix 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：

- Citrix Gateway 文档中的配置身份验证和授权。
- StoreFront 文档中的配置身份验证和委派。

证书吊销列表

启用证书吊销列表 (CRL) 检查功能后，Citrix Workspace 应用程序将检查服务器的证书是否已被吊销。执行此检查有助于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 连接的整体安全性。

可以在多个级别启用 CRL 检查。例如，可以将 Citrix Workspace 应用程序配置为仅检查本地证书列表，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 CRL 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。

退出 Citrix Workspace 应用程序并关闭所有 Citrix Workspace 组件，包括连接中心。

有关详细信息，请参阅 TLS 部分。

安装和卸载

May 23, 2024

管理员安装适用于 **Windows** 的 **Citrix Workspace** 应用程序 **1912 LTSR** 之前需要注意的事项

- 适用于 Windows 的 Citrix Workspace 应用程序 1912 LTSR 需要.NET Framework 4.6.2 或更高版本。Citrix Workspace 应用程序安装程序下载并安装.NET Framework（如果您的系统中不存在）。但是，我们建议您在安装或更新 Citrix Workspace 应用程序之前手动安装所需的.NET Framework。
- 如果您尝试执行无人参与安装，请参阅知识中心文章 CTX257546。
- 要了解有关受支持和不受支持的密码套件的最新信息，请参阅知识中心文章 CTX250104。

可以从下载页面或从贵公司的下载页面（如果可用）下载 `CitrixWorkspaceApp.exe` 安装包来安装 Citrix Workspace 应用程序。可以通过以下方式安装软件包：

- 运行基于 Windows 的交互式安装向导，或
- 使用命令行界面键入安装程序文件名、安装命令和安装属性。有关使用命令行界面安装 Citrix Workspace 应用程序的信息，请参阅使用命令行参数。

使用管理员和非管理员权限进行安装：

用户和管理员都可以安装 Citrix Workspace 应用程序。仅当将直通身份验证和 Citrix Ready Workspace Hub 与适用于 Windows 的 Citrix Workspace 应用程序结合使用时才需要管理员权限。

下表描述了以管理员或用户身份安装 Citrix Workspace 应用程序时的差异：

	安装文件夹	安装类型
管理员	C:\Program Files (x86)\Citrix\ICA Client	每系统安装
用户	%USERPROFILE%\AppData\Local\Citrix\ICA Client	每用户安装

> 注意：
>
> 如果系统中存在用户安装的适用于 Windows 的 Citrix Workspace 应用程序实例，并且管理员在同一系统中安装适用于 Windows 的 Citrix Workspace 应用程序，则将发生冲突。Citrix 建议您先卸载用户安装的所有适用于 Windows 的 Citrix Workspace 应用程序实例，然后再以管理员身份安装适用于 Windows 的 Citrix Workspace 应用程序。

使用基于 **Windows** 的安装程序

可以使用安装介质、网络共享、Windows 资源管理器或命令行通过手动运行 `CitrixWorkspaceApp.exe` 安装程序包安装适用于 Windows 的 Citrix Workspace 应用程序。

默认情况下，安装程序日志位于 `%temp%\CTXReceiverInstallLogs*.logs`。

1. 启动 `CitrixWorkspaceApp.exe` 文件并单击启动。
2. 阅读并接受“最终用户许可协议”，然后继续安装。
3. 如果尝试在具有管理员权限的已加入域的计算机上进行安装，则会出现一个额外的对话框来启用或禁用单点登录。有关详细信息，请参阅域直通身份验证。
4. 按照基于 Windows 的安装程序完成安装。

使用命令行参数

可以通过在命令行界面中键入安装程序文件名、安装命令和安装属性来安装 Citrix Workspace 应用程序。可以通过指定命令行选项来自定义 Citrix Workspace 应用程序安装程序。安装程序包将在启动安装程序之前自解压到系统临时文件夹。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文件夹。

要使用 Windows 命令行安装 Citrix Workspace 应用程序，请启动命令提示符，然后在单行中键入安装程序文件名、安装命令和安装属性。下面列出了可用的安装命令和属性：

```
CitrixWorkspaceApp.exe [commands] [properties]
```


命令行参数列表

参数大致分类如下：

- 常用参数
- 安装参数
- HDX 功能参数
- 首选项和用户界面参数
- 身份验证参数

常用参数

- /? 或 /help - 列出所有安装命令和属性。
- /silent - 在安装过程中禁用安装对话框和提示。
- /noreboot - 在安装过程中禁止提示重新启动对话框。禁止显示重新启动提示时，处于暂停状态的 USB 设备在重新启动用户设备之后才能被 Citrix Workspace 应用程序识别。
- /includeSSON - 要求您以管理员身份安装。指示 Citrix Workspace 应用程序随单点安装组件安装。有关详细信息，请参阅域直通身份验证。
- /rcu - 此开关仅在从不受支持的软件版本升级时才有效。指示 Citrix Workspace 应用程序将通过卸载现有版本来安装或升级。这也会清除现有设置。

  > 注意：
  >
  > /rcu 开关自版本 1909 起已弃用。有关详细信息，请参阅弃用。

- /forceinstall - 在以下情况下清理系统中安装的 Citrix Workspace 应用程序的任何现有配置或条目时，此开关非常有效：
  - 您正在从不受支持的 Citrix Workspace 应用程序版本进行升级。
  - 安装或升级不成功。

安装参数

/AutoUpdateCheck

指示 Citrix Workspace 应用程序在有可用更新时进行检测。

- 自动（默认设置）- 系统将在有可用更新时向您发出通知。例如，CitrixWorkspaceApp.exe /AutoUpdateCheck=auto。
- 手动 - 系统在有可用更新时不向您发出通知。手动检查更新。例如，CitrixWorkspaceApp.exe /AutoUpdateCheck=manual。
- 已禁用-禁用自动更新。例如，CitrixWorkspaceApp.exe /AutoUpdateCheck=disabled。

/AutoUpdateStream

如果您已启用自动更新，则可以选择要更新到的版本跟踪。有关详细信息，请参阅生命周期里程碑。

- LTSR - 仅自动更新到长期服务版本累积更新。例如，CitrixWorkspaceApp.exe /AutoUpdateStream=LTSR。
- 当前 - 自动更新到最新版本的 Citrix Workspace 应用程序。例如，CitrixWorkspaceApp.exe /AutoUpdateStream=Current。

/DeferUpdateCount

指示更新可用时可以推迟更新通知的次数。有关详细信息，请参阅 Citrix Workspace 更新。

- -1（默认值）- 允许推迟任意次通知。例如，CitrixWorkspaceApp.exe /DeferUpdateCount=-1。
- 0 - 指示针对每个可用更新您将（仅）收到一条通知。系统不会再次提醒您有关更新的信息。例如，CitrixWorkspaceApp.exe /DeferUpdateCount=0。
- 任何其他数字 “n” - 允许推迟更新通知 “n” 次。以后提醒我选项显示 “n” 次。例如，CitrixWorkspaceApp.exe /DeferUpdateCount=<n>。

/AURolloutPriority

发布新版本的应用程序后，Citrix 会在特定交付周期内推出更新。使用此参数，您可以控制在交付周期内的哪个时间可以接收更新。

- 自动（默认值）- 您将在 Citrix 配置的交付周期内收到更新。例如，CitrixWorkspaceApp.exe /AURolloutPriority=Auto。
- 快 - 您将在交付周期开始时收到更新。例如，CitrixWorkspaceApp.exe /AURolloutPriority=Fast。
- 中 - 您将在交付期间中间时段收到更新。例如，CitrixWorkspaceApp.exe /AURolloutPriority=Medium。
- 慢 - 您将在交付周期结束时收到更新。例如，CitrixWorkspaceApp.exe /AURolloutPriority=Slow。

/includeappprotection

在使用 Citrix Virtual Apps and Desktops 和 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）时通过限制客户端受键盘记录和屏幕捕获恶意软件影响的能力，提高了安全性。

- CitrixWorkspaceApp.exe /includeappprotection

有关详细信息，请参阅 App Protection。

INSTALLDIR

指定 Citrix Workspace 应用程序安装的自定义安装目录。默认路径为 C:\Program Files\Citrix。例如，CitrixWorkspaceApp.exe INSTALLDIR=C:\Program Files\Citrix。

ADDLOCAL

安装一个或多个指定的组件。例如，CitrixWorkspaceapp.exe ADDLOCAL=ReceiverInside,ICA_Client,AM,SELFSERVICE,DesktopViewer,Flash,Vd3d,WebHelper,BrowserEngine,WorkspaceHub,USB。

HDX 功能参数

ALLOW_BIDIRCONTENTREDIRECTION

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。有关详细信息，请参阅“Citrix Virtual Apps and Desktops”文档中的双向内容重定向策略设置部分。

- 0（默认值）- 指示双向内容重定向处于禁用状态。例如，CitrixWorkspaceApp.exe ALLOW_BIDIRCONTENTREDIRECTION=0。
- 1 - 指示双向内容重定向处于启用状态。例如，CitrixWorkspaceApp.exe ALLOW_BIDIRCONTENTREDIRECT=1。

FORCE_LAA

指示 Citrix Workspace 应用程序随客户端本地应用程序访问组件安装。必须使用管理员权限安装 Citrix Workspace 应用程序，此组件才能运行。有关详细信息，请参阅“Citrix Virtual Apps and Desktops”文档中的本地应用程序访问。

- 0(默认值)- 指示未安装本地应用程序访问组件。例如，CitrixWorkspaceApp.exe FORCE_LAA=0。
- 1 - 指示安装客户端本地应用程序访问组件。例如，CitrixWorkspaceApp.exe FORCE_LAA=1。

LEGACYFTAICONS

指定是否为与订购的应用程序具有文件类型关联的文档或文件显示应用程序图标。

- false（默认设置）- 指定是否为与订购的应用程序具有文件类型关联的文档或文件显示应用程序图标。设置为 false 时，操作系统将为没有为其指定特定图标的文档生成一个图标。操作系统生成的图标由较小版本的应用程序图标覆盖的通用图标组成。例如，CitrixWorkspaceApp.exe LEGACYFTAICONS=False。
- ture - 指定不为与订购的应用程序具有文件类型关联的文档或文件显示应用程序图标。例如，CitrixWorkspaceApp.exe LEGACYFTAICONS=True。

ALLOW_CLIENTHOSTEDAPPSURL

在用户设备上启用 URL 重定向功能。有关详细信息，请参阅“Citrix Virtual Apps and Desktops”文档中的本地应用程序访问。

- 0（默认值）- 在用户设备上禁用 URL 重定向功能。例如，CitrixWorkspaceApp.exe ALLOW_CLIENTHOSTEDAPPSURL=0。
- 1- 在用户设备上启用 URL 重定向功能。例如，CitrixWorkspaceApp.exe ALLOW_CLIENTHOSTEDAPPSURL=1。

首选项和用户界面参数

ALLOWADDSTORE

允许您根据指定的参数配置应用商店（http 或 https）。

- S（默认值）–仅允许您添加或删除安全应用商店（使用 HTTPS 配置）。例如，CitrixWorkspaceApp.exe ALLOWADDSTORE=S。
- A –允许您添加或删除安全应用商店 (HTTPS) 和非安全应用商店 (HTTP)。如果 Citrix Workspace 应用程序是按用户安装的，则不适用。例如，CitrixWorkspaceApp.exe ALLOWADDSTORE=A。
- N –不允许用户添加或删除自己的应用商店。例如，CitrixWorkspaceApp.exe ALLOWADDSTORE=N。

ALLOWSAVEPWD

允许您在本地保存应用商店凭据。此参数仅适用于使用 PNAgent 协议的应用商店。

- S（默认值）–仅允许保存安全应用商店的密码（已配置 HTTPS）。例如，CitrixWorkspaceApp.exe ALLOWSAVEPWD=S。
- N - 不允许保存密码。例如，CitrixWorkspaceApp.exe ALLOWSAVEPWD=N。
- A –允许保存安全应用商店 (HTTPS) 和非安全应用商店 (HTTP) 的密码。例如，CitrixWorkspaceApp.exe ALLOWSAVEPWD=A。

STARTMENUDIR

指定“开始”菜单中的快捷方式的文件夹。

- <Directory Name> - 默认情况下，应用程序显示在开始 > 所有程序下。可以在 \Programs 文件夹中指定快捷方式的相对路径。例如，要将快捷方式放置在“开始”>“所有程序”>“Workspace”下，请指定 STARTMENUDIR=\Workspace。

DESKTOPDIR

指定桌面上快捷方式的文件夹。

> 注意：
>
> 使用 DESKTOPDIR 选项时，请将 PutShortcutsOnDesktop 项设置为 True。

- <Directory Name> - 可以指定快捷方式的相对路径。例如，要将快捷方式放置在“开始”>“所有程序”>“Workspace”下，请指定 DESKTOPDIR=\Workspace。

SELFSERVICEMODE

控制对自助服务 Citrix Workspace 应用程序用户界面的访问。

- True - 指示用户有权访问自助服务用户界面。例如，CitrixWorkspaceApp.exe SELFSERVICEMODE=True。
- False - 指示用户无法访问自助服务用户界面。例如，CitrixWorkspaceApp.exe SELFSERVICEMODE=False。

ENABLEPRELAUNCH

控制会话预启动。有关详细信息，请参阅应用程序启动时间。

- True - 指示会话预启动功能处于启用状态。例如，CitrixWorkspaceApp.exe ENABLEPRELAUNCH=True。
- False - 指示会话预启动功能处于禁用状态。例如，CitrixWorkspaceApp.exe ENABLEPRELAUNCH=False。

DisableSetting

隐藏快捷方式和重新连接选项，使其不在高级首选项表中显示。有关详细信息，请参阅在“高级首选项”表中隐藏特定设置。

- 0（默认值）- 在“高级首选项”表中显示快捷方式和重新连接选项。例如，CitrixWorkspaceApp.exe DisableSetting=0。
- 1 - 仅在“高级首选项”表中显示重新连接选项。例如，CitrixWorkspaceApp.exe DisableSetting=1。
- 2 - 仅在“高级首选项”表中显示快捷方式选项。例如，CitrixWorkspaceApp.exe DisableSetting=2。
- 3 - 在“高级首选项”表中隐藏快捷方式和重新连接选项。例如，CitrixWorkspaceApp.exe DisableSetting=3。

EnableCEIP

指示您参与客户体验改善计划 (CEIP)。有关详细信息，请参阅 CEIP。

- true（默认值）- 选择加入 CEIP。例如，`CitrixWorkspaceApp.exe EnableCEIP=True`。
- false - 选择退出 CEIP。例如，`CitrixWorkspaceApp.exe EnableCEIP=False`。

EnableTracing

控制 **AlwaysOn** 跟踪功能。

- True（默认设置）- 启用 **AlwaysOn** 跟踪功能。例如，`CitrixWorkspaceApp.exe EnableTracing=true`。
- False - 禁用 **AlwaysOn** 跟踪功能。例如，`CitrixWorkspaceApp.exe EnableTracing=false`。

CLIENT_NAME

指定服务器用来识别用户设备的名称。

- <ClientName> - 指定服务器上用来识别用户设备的名称。默认名称为 %COMPUTERNAME%。例如，`CitrixReceiver.exe CLIENT_NAME=%COMPUTERNAME%`。

ENABLE_DYNAMIC_CLIENT_NAME

允许客户端名称与计算机名称相同。更改计算机名称时，客户端名称也会随之更改。

- 是（默认设置）- 允许客户端名称与计算机名称相同。例如，`CitrixWorkspaceApp.exe ENABLE_DYNAMIC_CLIENT_NAME=Yes`。
- 否 - 不允许客户端名称与计算机名称相同。必须为 CLIENT_NAME 属性指定一个值。例如，`CitrixWorkspaceApp.exe ENABLE_DYNAMIC_CLIENT_NAME=No`。

身份验证参数

ENABLE_SSON

Citrix Workspace 应用程序通过 /includeSSON 命令安装时启用单点登录。有关详细信息，请参阅域直通身份验证。

- 是（默认设置）- 指示单点登录处于启用状态。例如，`CitrixWorkspaceApp.exe /ENABLE_SSON=Yes`。
- 否 - 指示单点登录处于禁用状态。例如，`CitrixWorkspaceApp.exe /ENABLE_SSON=No`。

ENABLE_KERBEROS

指定 HDX 引擎是否必须使用 Kerberos 身份验证。仅当启用了单点登录身份验证时才适用。有关详细信息，请参阅使用 Kerberos 的域直通身份验证。

- 是 - 指示 HDX 引擎将使用 Kerberos 身份验证。例如，`CitrixWorkspaceApp.exe ENABLE_KERBEROS=Yes`。
- 否 - 指示 HDX 引擎将不使用 Kerberos 身份验证。例如，`CitrixWorkspaceApp.exe ENABLE_KERBEROS=No`。

除上述属性外，您还可以指定与 Citrix Workspace 应用程序结合使用的应用商店 URL。最多可以添加 10 个应用商店。请使用以下属性执行此操作：

```
STOREx="storename;http[s]://servername.domain/IISLocation/discovery;[On, Off]; [storedescription]"
```

值：

- x - 整数 0 到 9，用于标识应用商店。
- storename - 应用商店的名称。此值必须与在 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] - **Off** 选项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 - 应用商店的说明，例如 `HR App Store`。

命令行安装示例

要指定 **Citrix Gatewaya** 应用商店 **URL**，请执行以下操作：

```
CitrixWorkspaceApp.exe STORE0=HRStore;https://ag.mycompany.com#Storename;On;Store
```

其中，*Storename* 指示需要配置的应用商店的名称。

> 注意：
>
> - 使用此方法配置的 Citrix Gateway 应用商店 URL 不支持使用 Citrix Gateway 的 PNA Services 站点。
> - 如果配置多个应用商店，请将 Citrix Gateway 应用商店 URL 置于列表中的第一位。仅允许存在一个 Citrix Gateway 应用商店 URL 配置。

无提示安装所有组件并指定两个应用商店：


```
CitrixWorkspaceApp.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"
```

> 注意：
>
> - 请务必在应用商店 URL 中包括 `/discovery` 以成功执行直通身份验证。
> - Citrix Gateway 应用商店 URL 必须是已配置的应用商店 URL 列表中的第一个条目。

卸载

使用基于 **Windows** 的卸载程序：

您可以使用 Windows 的“程序和功能”实用程序（添加/删除程序）卸载适用于 Windows 的 Citrix Workspace 应用程序。

> 注意：
>
> 您会在继续安装适用于 Windows 的 Citrix Workspace 应用程序之前收到卸载 Citrix HDX RTME 软件包的提示。单击确定继续卸载。

使用命令行接口：

可以从命令行键入以下命令卸载适用于 Windows 的 Citrix Workspace 应用程序：

```
CitrixWorkspaceApp.exe /uninstall
```

对于无提示卸载适用于 Windows 的 Citrix Workspace 应用程序，请运行以下开关：

```
CitrixWorkspaceApp.exe /silent /uninstall
```

> 注意：
>
> - 卸载后，receiver.adm/receiver.adml 或 receiver.admx 创建的注册表项将保留。
> - 如果您在卸载后在注册表编辑器中找到任何条目，请手动将其删除。

部署

October 31, 2023

可以通过以下方法部署 Citrix Workspace 应用程序：

- 使用 Active Directory 和示例启动脚本来部署适用于 Windows 的 Citrix Workspace 应用程序。有关 Active Directory 的信息，请参阅使用 Active Directory 和示例脚本。
- 从浏览器启动应用程序之前，使用适用于 Web 的 Workspace 确保用户已安装适用于 Windows 的 Citrix Workspace 应用程序。有关详细信息，请参阅使用适用于 Web 的 Workspace。
- 使用 Microsoft System Center Configuration Manager 2012 R2 等电子软件分发 (ESD) 工具。有关详细信息，请参阅使用 System Center Configuration Manager 2012 R2。

使用 **Active Directory** 和示例脚本

可以使用 Active Directory 组策略脚本根据 Active Directory 组织结构在系统中部署适用于 Windows 的 Citrix Workspace 应用程序。Citrix 建议使用脚本而非提取.msi 文件。有关启动脚本的常规信息，请参阅 Microsoft 文档。

要对 **Active Directory** 使用脚本，请执行以下操作：

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)。

编辑脚本

使用每个文件标题部分中的以下参数来编辑脚本：

- 当前软件包版本 - 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，且不由脚本进行身份验证。必须将共享文件夹的“读取”权限设置为“所有人”。
- 脚本日志记录目录 - 此参数指定复制安装日志且不由脚本进行身份验证的网络共享。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。

脚本

Citrix Workspace 应用程序安装程序包括用于安装和卸载 Citrix Workspace 应用程序的示例每计算机和每用户脚本。这些脚本位于适用于 Windows 的 Citrix Workspace 应用程序的下载页面。

部署类型	要部署	要删除
每计算机	CheckAndDeployWorkspacePerMachineStartupScript.bat	CheckAndRemoveWorkspacePerMachineSta
每个用户	CheckAndDeployWorkspacePerUserLogonScript.bat	CheckAndRemoveWorkspacePerUserLogonS

要添加启动脚本，请执行以下操作：

1. 打开组策略管理控制台。
2. 选择计算机配置或用户配置 > 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. 选择显示文件并将相应的脚本复制到显示的文件夹。
5. 关闭对话框。
6. 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。

要部署适用于 **Windows** 的 **Citrix Workspace** 应用程序，请执行以下操作：

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登录。
3. 验证新安装的软件包是否在程序和功能中列出。

要删除适用于 **Windows** 的 **Citrix Workspace** 应用程序，请执行以下操作：

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登录。
3. 验证新安装的软件包是否未在程序和功能中列出。

使用适用于 **Web** 的 **Workspace**

可以从适用于 Web 的 Workspace 部署适用于 Windows 的 Citrix Workspace 应用程序，以确保您在尝试从浏览器连接到应用程序之前已安装适用于 Windows 的 Citrix Workspace 应用程序。借助适用于 Web 的 Workspace 站点，您可以通过 Web 页面访问 StoreFront 应用商店。如果适用于 Web 的 Workspace 站点检测到用户没有兼容版本的适用于 Windows 的 Citrix Workspace 应用程序，系统会提示您下载并安装适用于 Windows 的 Citrix Workspace 应用程序。

如果已使用适用于 Web 的 Workspace 部署适用于 Windows 的 Citrix Workspace 应用程序，则不支持基于电子邮件的帐户发现。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 安装了适用于 Windows 的 Citrix Workspace 应用程序，则适用于 Windows 的 Citrix Workspace 应用程序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 `CitrixWorkspaceApp.exe` 下载到本地计算机。
2. 将 `CitrixWorkspaceApp.exe` 重命名为 `CitrixWorkspaceAppWeb.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适用于 Web 的 Workspace 站点。

使用 **System Center Configuration Manager 2012 R2**

可以使用 Microsoft System Center Configuration Manager (SCCM) 部署 Citrix Workspace 应用程序。

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

使用 SCCM 完成适用于 Windows 的 Citrix Workspace 应用程序的部署分为四个部分：

1. 向 SCCM 部署中添加 Citrix Workspace 应用程序
2. 添加分发点
3. 将 Citrix Workspace 应用程序部署到软件中心
4. 创建设备集合

向 **SCCM** 部署中添加 **Citrix Workspace** 应用程序

1. 将下载的 Citrix Workspace 应用程序安装文件夹复制到 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 Workspace 应用程序设置的部署类型。

   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，Workspace 部署），然后单击 **Next**（下一步）。
9. 在 **Content**（内容）窗格中：

   a) 提供 Citrix Workspace 应用程序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：

- `CitrixWorkspaceApp.exe /silent` 用于默认静默安装。
- `CitrixWorkspaceApp.exe /silent /includeSSON` 用于启用域直通。
- `CitrixWorkspaceApp.exe /silent SELFSERVICEMODE=false` 用于以非自助服务模式安装 Citrix Workspace 应用程序。

c) 为 **Uninstall program**（卸载程序）指定 `CitrixWorkspaceApp.exe /uninstall`（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。

- 将 **Setting Type**（设置类型）设置为“File System”（文件系统）。
- 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\`
  - 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）
  - 值 - 输入要部署的 Citrix Workspace 应用程序的版本号。

> 注意：
>
> 适用于 Windows 的 Citrix Workspace 应用程序升级也适用此规则组合。

11. 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“Next”（下一步）。

> 注意：
>
> 请勿为此部署类型指定任何要求和依赖项。

12. 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。

13. 在 **Completion**（完成）窗格中，新部署类型（Workspace 部署）将在“Deployment types”（部署类型）下列出。

14. 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 Citrix Workspace 应用程序，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. 单击关闭。

将 **Citrix Workspace** 应用程序部署到软件中心

1. 在 Configuration Manager 控制台中右键单击 Citrix Workspace 应用程序，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 Workspace 应用程序在软件中心中的 **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 **Name**（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“Next”（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 部署适用于 Windows 的 Citrix Workspace 应用程序可能会不成功。
> 根据我们的分析，适用于 Windows 的 Citrix Workspace 应用程序并不是导致此失败的原因。此外，重试可能会使部署成功。

更新

April 22, 2024

手动更新

如果您已安装适用于 Windows 的 Citrix Workspace 应用程序，请从 Citrix 下载页面下载并安装该应用程序的最新版本。

自动更新

自版本 1912 累积更新 4 (CU4) 起，将修改 Citrix Workspace 更新日志路径。Workspace 更新日志存在于 C:\Program Files(x86)\Citrix\Logs 中，用于计算机范围的更新。日志存在于用户的临时文件夹中，用于用户范围内的更新，

发布新版本的 Citrix Workspace 应用程序后，Citrix 会在安装了 Citrix Workspace 应用程序的系统中推送更新。

> 注意：
>
> - 如果您配置了截获出站代理的 SSL，请添加 Workspace 自动更新服务 `https://downloadplugins.citrix.com/` 以从 Citrix 接收更新。
> - 自动更新不适用于 Citrix Workspace 应用程序 2104 和 Citrix Workspace 应用程序 1912 LTSR CU4 之前的版本。
> - 如果您配置了截获出站代理的 SSL，请添加 Workspace 自动更新签名服务 (`https://citrixupdates.cloud.com/`) 和下载位置 (`https://downloadplugins.citrix.com/`) 的例外，以从 Citrix 接收更新。
> - 您的系统必须具有 Internet 连接才能接收更新。
> - 默认情况下，Citrix Workspace 更新在 VDA 上处于禁用状态。这包括 RDS 多用户服务器计算机、VDI 和 Remote PC Access 计算机。
> - Citrix Workspace 更新在安装了 Desktop Lock 的计算机上处于禁用状态。
> - 适用于 Web 的 Workspace 用户不能自动下载 StoreFront 策略。
> - Citrix Workspace 更新仅限于 LTSR 更新。
> - Citrix HDX RTME for Windows 随附在 Citrix Workspace 更新中。系统将向您通知同时在 Citrix Workspace 应用程序的 LTSR 和当前版本中可用的 HDX RTME 更新。

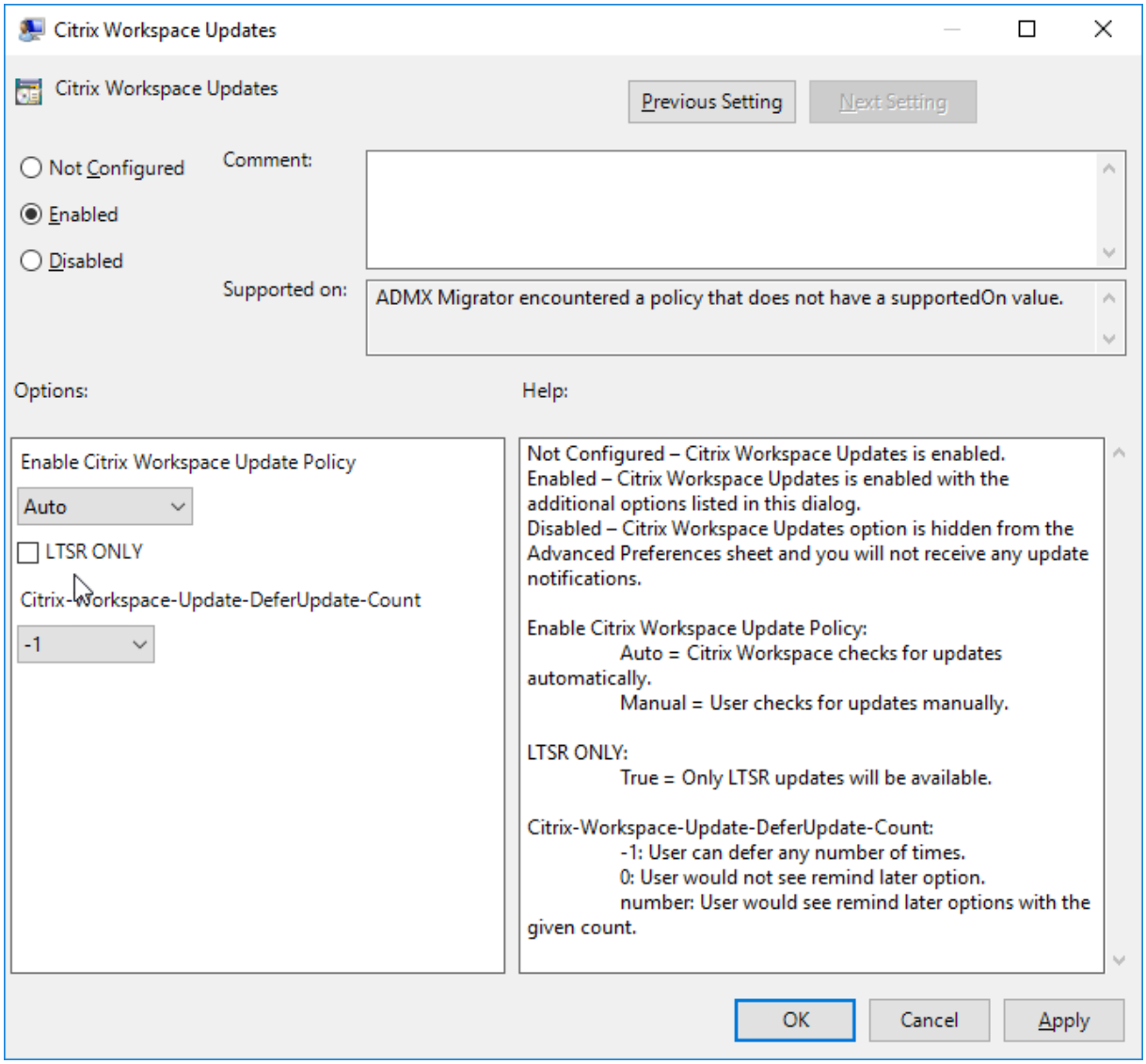
自动更新的高级配置（**Citrix Workspace** 更新）

可以使用以下方法配置 Citrix Workspace 更新：

1. 组策略对象 (GPO) 管理模板
2. 命令行接口
3. 图形用户界面
4. StoreFront

使用组策略对象管理模板配置 **Citrix Workspace** 更新

通过运行 gpedit.msc 打开 Citrix Workspace 应用程序组策略对象管理模板，然后导航到“计算机配置”节点，转到管理模板 > **Citrix** 组件 > **Citrix Workspace** > **Workspace** 更新。



1. 启用或禁用更新 - 选择已启用或已禁用以启用或禁用 Workspace 更新。

   > 注意：
   >
   > 选择已禁用时，系统不会通知您新更新。这样还将在高级首选项表中隐藏 Workspace 更新选项。

2. 更新通知 - 当有更新可用时，您可以选择自动接收通知或手动检查更新。启用 Workspace 更新后，请从启用 **Citrix Workspace** 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。

3. 选择仅限 **LTSR** 以仅获取 LTSR 的更新。

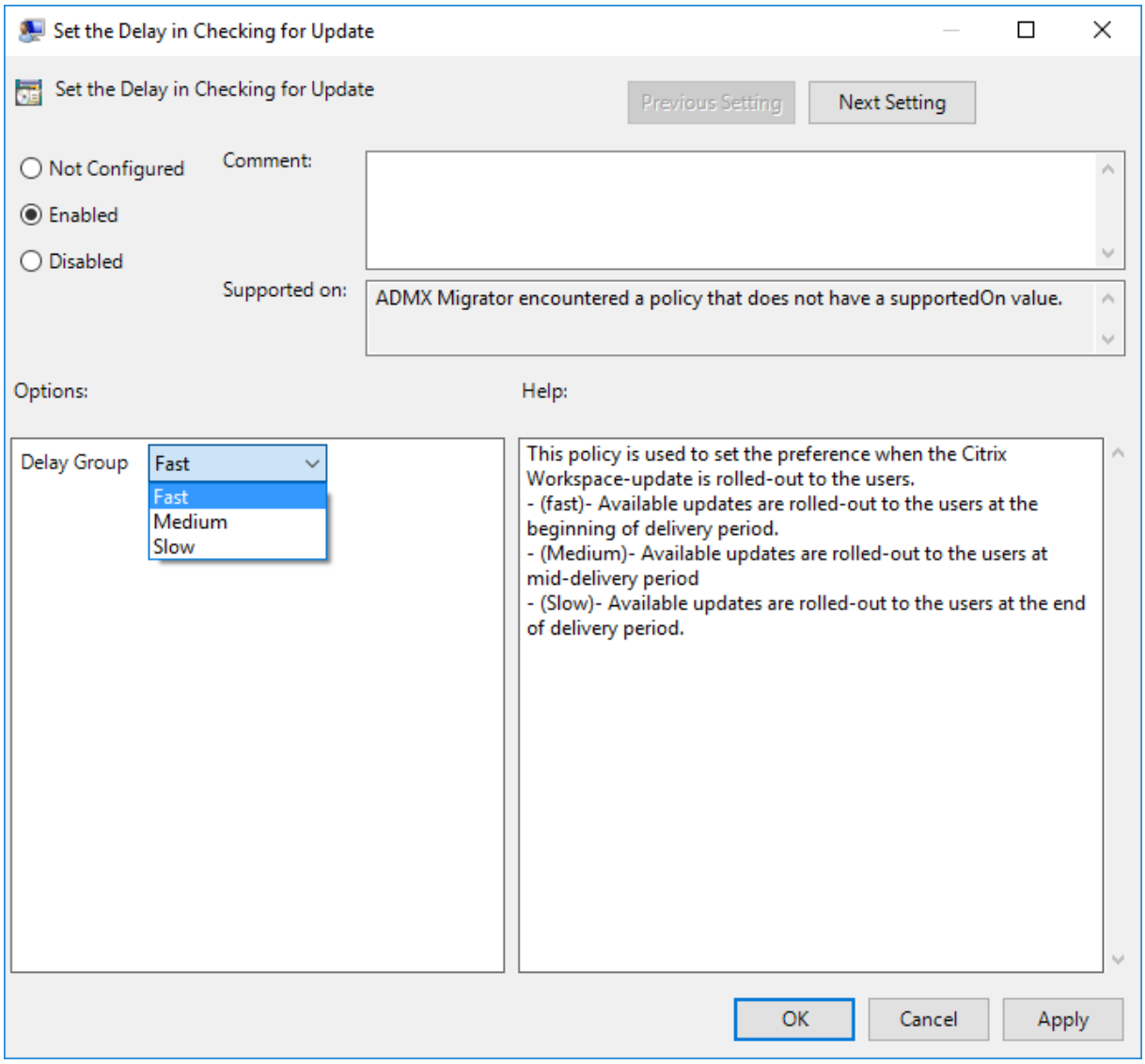
4. 从 **Citrix-Workspace-Update-DeferUpdate-Count** 下拉列表中，选择一个介于 -1 到 30 之间的值：

   - -1 - 允许推迟任意次通知（默认值）。

- 0 - 您将仅收到一个更新通知。

配置检查更新的延迟　新版本的 Citrix Workspace 应用程序可用时，Citrix 会在特定交付期间滚动更新。使用此参数，您可以控制在交付期间内的哪个阶段可以接收更新。

要配置交付期间，请运行 `gpedit.msc` 以启动组策略对象管理模板。在“计算机配置”节点下，转至管理模板 > **Citrix** 组件 > **Citrix Workspace** > 设置检查更新的延迟。



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。

> 注意：
>
> 选择已禁用时，系统不会通知您可用的更新。这样还将在高级首选项表中隐藏 Workspace 更新选项。

使用命令行界面配置 **Citrix Workspace** 更新

通过在安装 **Citrix Workspace** 应用程序时指定命令行参数：

可以通过在 Citrix Workspace 应用程序安装期间指定命令行参数来配置 Workspace 更新。有关详细信息，请参阅安装参数。

通过在安装 **Citrix Workspace** 应用程序后使用命令行参数：

也可以在安装适用于 Windows 的 Citrix Workspace 应用程序后配置 Citrix Workspace 更新。使用 Windows 命令行导航到 CitrixReceiverUpdater.exe 所在的位置。

通常情况下，CitrixWorkspaceUpdater.exe 位于 `CitrixWorkspaceInstallLocation\Citrix\Ica Client\Receiver`。可以运行此二进制文件以及安装参数部分中列出的命令行参数。

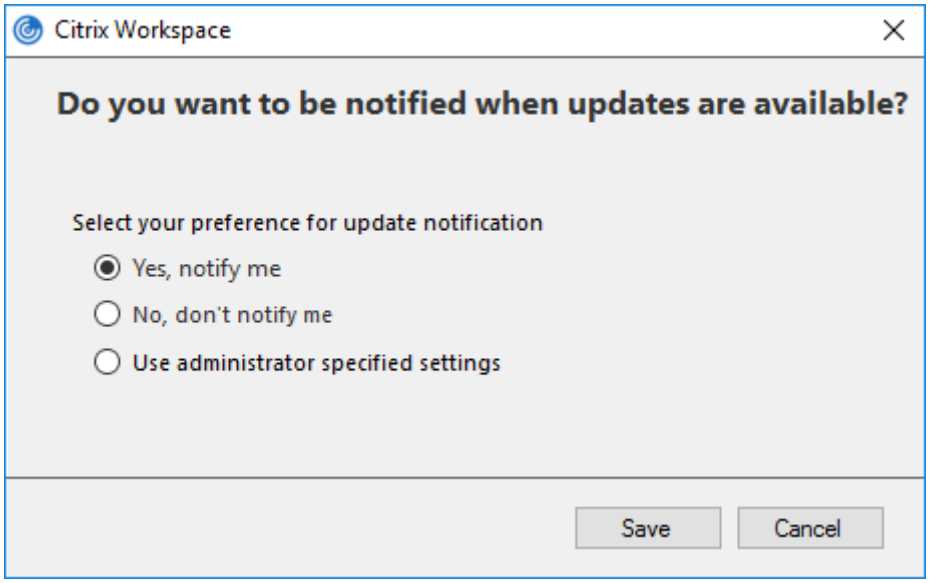
例如，

```
CitrixReceiverUpdater.exe /AutoUpdateCheck=auto /AutoUpdateStream=Current /DeferUpdateCount=-1 /AURolloutPriority=fast
```

> 注意：
>
> `/AutoUpdateCheck`这是必需的参数，必须设置才能配置 `/AutoUpdateStream`、`/DeferUpdateCount`、`/AURolloutPriority` 等其他参数。

使用图形用户界面配置 **Citrix Workspace** 更新

个人用户可以使用高级首选项对话框覆盖 Citrix Workspace 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。右键单击通知区域中的 Citrix Workspace 应用程序图标。选择高级首选项 > **Workspace** 更新。选择通知首选项，然后单击保存。



> 注意：
>
> 可以隐藏通知区域中的 Citrix Workspace 应用程序图标中提供的全部或部分“高级首选项”表。有关详细信息，请参阅高级首选项表部分。

使用 **StoreFront** 配置 **Citrix Workspace** 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 directory` 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>
 <!--NeedCopy-->
```

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 />

```



```
59          </trustSettings>
60
61          <properties>
62
63            <clear />
64
65          </properties>
66
67        </metadata>
68
69      </account>
70
71  <!--NeedCopy-->
```

属性的含义及其可能值的详细信息如下：

- **Auto-update-Check**：指示 Citrix Workspace 应用程序在有可用更新时自动进行检测。
- **Auto-update-LTSR-Only**：指示发布更新仅针对 LTSR。
- **Auto-update-Rollout-Priority**：指示可以在其间接收更新的交付期间。
- **Auto-update-DeferUpdate-Count**：指示可以延迟发布更新通知的次数。

入门

April 22, 2024

这是帮助您在安装 Citrix Workspace 应用程序后设置环境的参考文档。

必备条件：

请按照系统要求部分中所述，验证是否满足所有系统要求。

在开始使用 Citrix Workspace 应用程序之前，必须配置以下内容：

- 组策略对象管理模板
- StoreFront
- Citrix Gateway 应用商店
- 将应用商店 URL 添加到 Citrix Workspace 应用程序中
- 客户端驱动器映射
- 域名服务名称解析

组策略对象管理模板

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 Workspace 应用程序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。

Citrix 建议使用 Windows 组策略对象 (GPO) 管理模板配置 Citrix Workspace 应用程序。

自 Citrix Receiver for Windows 4.6 起，安装目录中包括 `CitrixBase.admx`、`CitrixBase.adml` 和管理模板文件（receiver.adm 或 receiver.admx\receiver.adml，具体取决于操作系统）。

> 注意：
>
> .adm 文件仅供 Windows XP Embedded 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 Workspace 应用程序是随 VDA 安装的，则 admx/adml 文件位于 Citrix Workspace 应用程序安装目录中。例如：\< 安装目录\>\\Online Plugin\\Configuration.

如果安装 Citrix Workspace 应用程序时未安装 VDA，则 admx/adml 文件通常位于 `C:\Program Files\Citrix\ICA Client\Configuration` 目录中。

请参见以下表格获取有关 Citrix Workspace 应用程序模板文件及其各自位置的信息。

> 注意：
>
> Citrix 建议您使用随最新版本的 Citrix Workspace 应用程序提供的 GPO 模板文件。

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

> 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 Workspace 应用程序时，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：

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。

可以使用.adm 模板文件配置本地 GPO 和/或基于域的 GPO。

1. 通过运行 gpedit.msc 打开 Citrix Workspace 应用程序组策略对象管理模板。
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 Workspace 应用程序模板文件将在本地 GPO 目录管理模板 **>** 经典管理模板 **(ADM) > Citrix** 组件 **> Citrix Workspace** 中提供。

向本地 GPO 添加.adm 模板文件后，将显示以下消息：

“下列在 [strings] 节中的项目太长，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：

可以使用.adm 模板文件配置本地 GPO 和/或基于域的 GPO。请参阅此处有关管理 ADMX 文件的 Microsoft MSDN 文章。

安装 Citrix Workspace 应用程序后，按下表中所示复制模板文件：

文件类型	复制来源	复制目标位置
receiver.admx	安装目录\ICA Client\Configuration\receiver.admx	%systemroot%\policyDefinitions
CitrixBase.admx	安装目录\ICA Client\Configuration\CitrixBase.admx	%systemroot%\policyDefinitions
receiver.adml	安装目录\ICA Client\Configuration[MUIculture]receiver.adml	%systemroot%\policyDefinitions[MUIculture
CitrixBase.adml	安装目录\ICA Client\Configuration[MUIculture]\CitrixBase.adml	%systemroot%\policyDefinitions[MUIculture

> 注意：
>
> 仅当将 CitrixBase.admx/CitrixBase.adml 添加到 \PolicyDefinitions 文件夹时，才会在管理模板 > **Citrix** 组件 > **Citrix Workspace** 文件夹中的本地 GPO 中提供 Citrix Workspace 应用程序模板文件。

StoreFront

Citrix StoreFront 对与 Citrix Virtual Apps and Desktops、Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）和 VDI-in-a-Box 的连接进行身份验证，枚举可用桌面和应用程序并将其聚合到能够使用 Citrix

Workspace 应用程序进行访问的应用商店中。

除了本节概述的配置外，您还必须配置 Citrix Gateway，以支持用户从内部网络之外进行连接（例如，从 Internet 或远程位置连接）。

> 注意：
>
> 选择用于显示所有应用商店的选项时，可能会看到旧的 StoreFront 用户界面。

配置 **StoreFront**：

请按照 StoreFront 文档中所述安装和配置 StoreFront。Citrix Workspace 应用程序需要 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中所述在用户设备上的 **ALLOWADDSTORE** 属性描述下设置一个注册表项。

> 注意：
>
> 对于需要更大控制权的管理员，Citrix 提供了一个模板，供您用于创建适用于 Windows 的 Citrix Workspace 应用程序下载站点。

Citrix Gateway 应用商店

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

1. 通过运行 gpedit.msc 打开 Citrix Workspace 应用程序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 Workspace** > **StoreFront**。
3. 选择 **Citrix Gateway URL/StoreFront** 帐户列表。
4. 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 Citrix 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
5. 添加或指定 Citrix Gateway URL。输入 URL 的名称（以分号分隔）：

示　例：`CitrixWorkspaceApp.exe STORE0= HRStore;https://ag.mycompany.com#Storename;On;Store`
其中 #Store 名称是 Citrix Gateway 后面的应用商店名称。

在早期版本中，如果在 GPO 中使用 **Citrix Gateway URL/StoreFront** 帐户列表策略添加或删除帐户，必须重置 Citrix Receiver，所做的更改才能生效。

自版本 1808 起，在重新启动 Citrix Workspace 应用程序时，即会在会话中应用对 **Citrix Gateway URL/StoreFront** 帐户列表策略所做的任何更改。不需要重置。

> 注意：
>
> 在全新安装 Citrix Workspace 应用程序 1808 及更高版本时，不需要重置 Citrix Workspace 应用程序。如果升级到版本 1808 及更高版本，则应重置 Citrix Workspace 应用程序以使所做的更改生效。

限制：

- Citrix Gateway URL 应列在最前面，后跟 StoreFront URL。
- 不支持多个 Citrix Gateway URL。
- 使用这种方法配置的 Citrix Gateway URL 不支持位于 Citrix Gateway 后面的 PNA Services 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 Workspace 应用程序，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 Citrix Virtual Apps 服务器中创建 **WSCReconnectModeUser** 并修改现有注册表项 **WSCReconnectMode**。已发布的桌面可以更改 Citrix Workspace 应用程序的行为。

Citrix Workspace 应用程序的 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 = Citrix Workspace 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 Workspace** 应用程序的工作区控制　要禁用工作区控制，请创建以下注册表项：

`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle`（64 位）

`HKEY_LOCAL_MACHINE\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_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\\Dazzle`（64 位）

`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\\Dazzle`（32 位）

名称：**WSCReconnectMode**

类型：REG_SZ

值数据：0

> 注意：
>
> 此外，如果不创建注册表项，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 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。

使用命令行自定义应用程序快捷方式的位置

使用“开始”菜单集成和仅桌面快捷方式模式，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 Workspace 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 Workspace 应用程序管理员，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 Workspace 应用程序界面，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 Workspace 应用程序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 Workspace 应用程序系统托盘图标上的“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。

- 用户无法使用 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，重新启动 Citrix Workspace 应用程序。
- 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 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，而不在通过 Citrix Virtual Apps 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，对服务器上已发布的应用程序和桌面的属性所做的任何更改均会反映到客户端计算机上。禁用 AutoReInstallModifiedApps 后，应用程序和桌面属性将不会更新，并且如果在客户端上删除了快捷方式，则刷新时也不会恢复快捷方式。默认情况下，启用 AutoReInstallModifiedApps。请参阅“使用注册表项自定义应用程序快捷方式的位置”。

使用注册表编辑器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。
> - 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 Citrix Workspace 应用程序，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：

Registry key	Value	Key path
WSCSupported	True	• HKEY_CURRENT_USER \ SOFTWARE \Citrix\Dazzle • HKEY_CURRENT_USER \ SOFTWARE \Citrix\Receiver\ SR\Store\" + primaryStoreID +\Properties • HKEY_LOCAL_MACHINE \SOFTWARE\Policies\Citrix \Dazzle • HKEY_LOCAL_MACHINE \SOFTWARE\Citrix\Dazzle
WSCReconnectAll	True	• HKEY_CURRENT_USER \ SOFTWARE \Citrix\Dazzle • HKEY_CURRENT_USER \ SOFTWARE \Citrix\Receiver \SR\Store\" + primaryStoreID + \Properties • HKEY_LOCAL_MACHINE \SOFTWARE\Policies \Citrix\Dazzle • HKEY_LOCAL_MACHINE \SOFTWARE\Citrix\Dazzle
WSCReconnectMode	3	• HKEY_CURRENT_USER \ SOFTWARE \Citrix\Dazzle • HKEY_CURRENT_USER \ SOFTWARE \Citrix\Receiver \SR\Store\" + primaryStoreID +\Properties • HKLM\SOFTWARE\Policies\Citrix \Dazzle • HKLM\SOFTWARE\Citrix\Dazzle
WSCReconnectModeUser	Registry is not created during installation	• HKEY_CURRENT_USER \ SOFTWARE \Citrix\Dazzle • HKEY_CURRENT_USER \ SOFTWARE \Citrix\Receiver \SR\Store\" + primaryStoreID+\Properties • HKEY_LOCAL_MACHINE \SOFTWARE\Policies \Citrix\Dazzle • HKEY_LOCAL_MACHINE \SOFTWARE \Citrix\Dazzle

64 位计算机的注册表项：

Registry key	Value	Key path
WSCSupported	True	• HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle • HKEY_CURRENT_USER\SOFTWARE\Citrix\Receiver\SR\Store • HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Dazzle • HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\D
WSCReconnectAll	True	• HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle • HKEY_CURRENT_USER\SOFTWARE\Citrix\Receiver\SR\Store • HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Policies\Dazzle • HKEY_LOCAL_MACHINE \SOFTWARE\Wow6432Node\Citrix\D
WSCreconnectMode	3	• HKEY_CURRENT_USER \ SOFTWARE \Citrix\Dazzle • HKEY_CURRENT_USER \ SOFTWARE \Citrix\Receiver\SR \Store\"+ primaryStoreID +"\Properties • HKEY_LOCAL_MACHINE \SOFTWARE\Wow6432Node \Policies\Citrix\Dazzle • HKEY_LOCAL_MACHINE \SOFTWARE\Wow6432Node \Citrix\Dazzle
WSCReconnectModeUser	Registry is not created during installation.	• HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle • HKEY_CURRENT_USER \ SOFTWARE \Citrix\Receiver\SR \Store\"+ primaryStoreID+\Properties • HKEY_LOCAL_MACHINE \SOFTWARE\Wow6432Node\Policies\Citrix\Dazzle • HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node \Citrix\Dazzle

用户帐户

您可以使用以下方法向用户提供访问虚拟桌面和应用程序所需的帐户信息：

- 配置基于电子邮件的帐户发现
- 预配文件
- 向用户提供需手动输入的帐户信息

> 重要提示
>
> Citrix 建议您在安装后重新启动 Citrix Workspace 应用程序。这样可确保用户能够添加帐户，并且 Citrix Workspace 应用程序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 Workspace 应用程序，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。

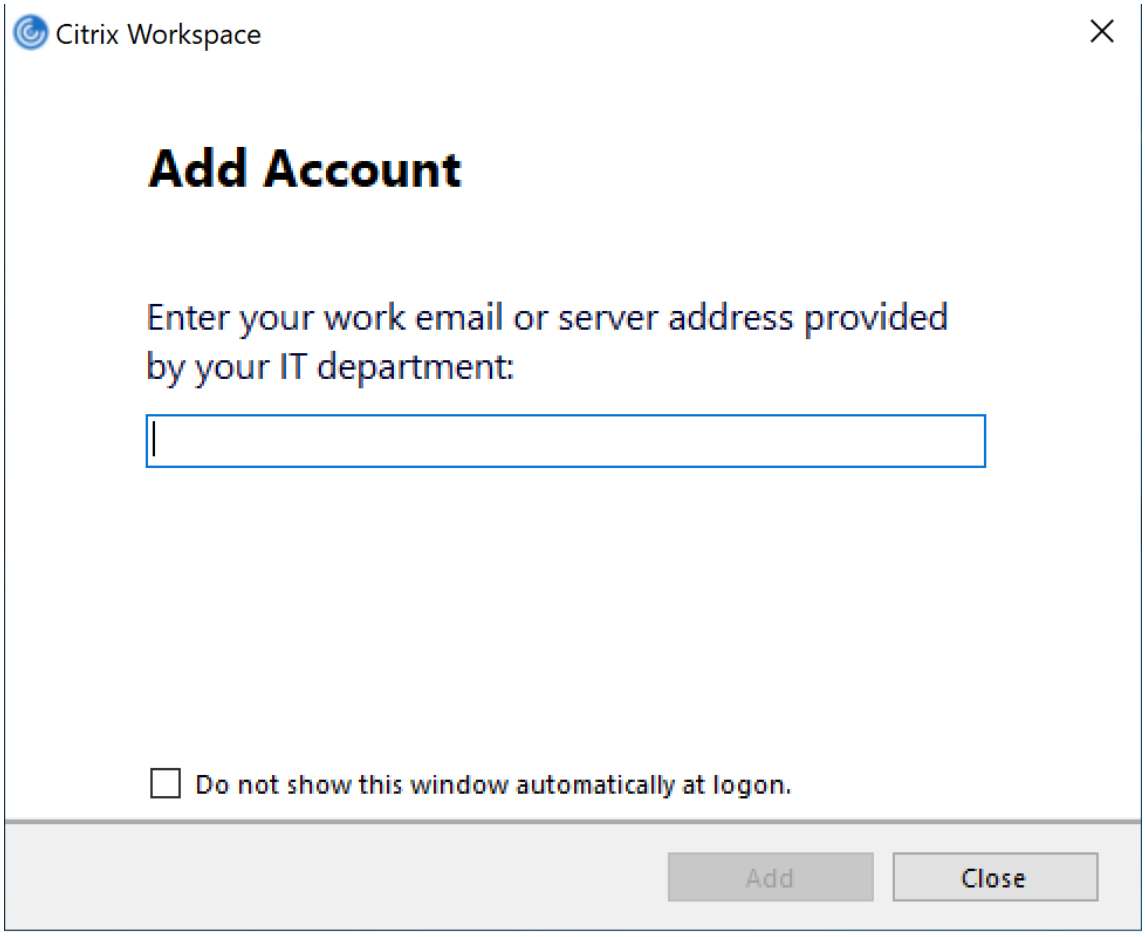
隐藏“添加帐户”对话框

添加帐户对话框在应用商店未配置时会显示出来。使用添加帐户对话框，您可以输入电子邮件地址或服务器 URL 来设置 Citrix Workspace 应用程序帐户。

Citrix Workspace 应用程序会确定与该电子邮件地址关联的是 Citrix Gateway、StoreFront 服务器还是 App Controller 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。
这是按用户进行的设置，并在适用于 Windows 的 Citrix Workspace 应用程序重置期间重置。

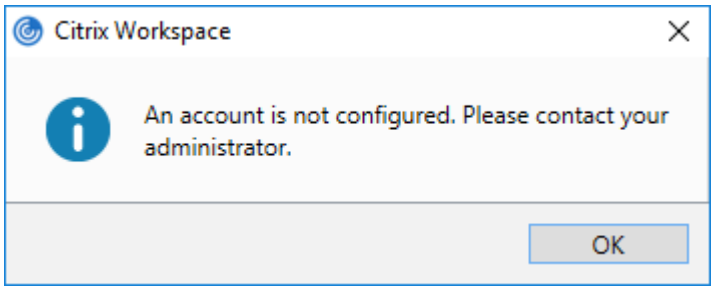
2. 命令行安装

   以管理员身份使用命令行接口，通过以下开关安装适用于 Windows 的 Citrix Workspace 应用程序。

   ```
   CitrixWorkspaceApp.exe /ALLOWADDSTORE=N
   ```

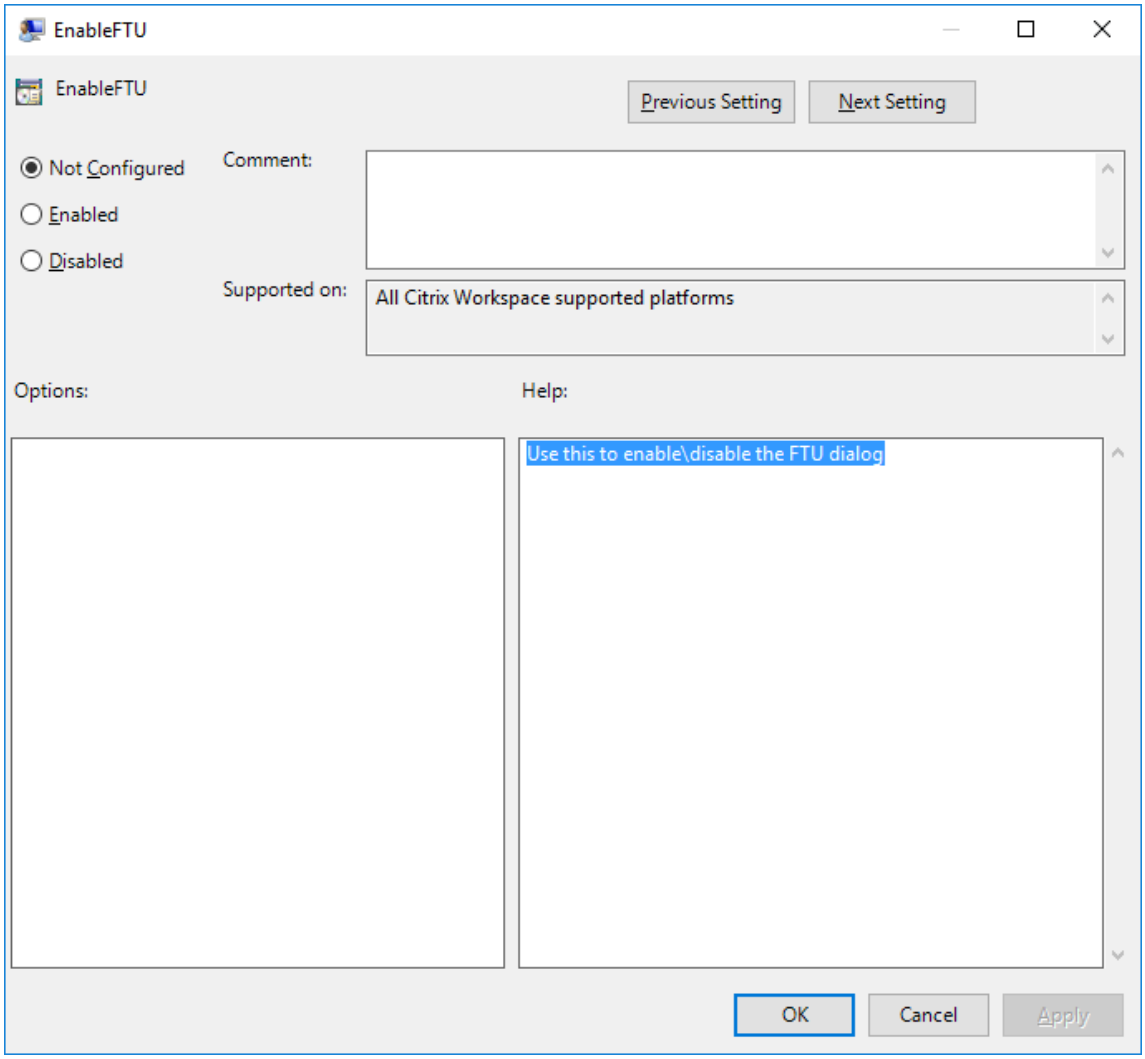
   这是按计算机进行的设置；因此该行为应当适用于所有用户。

   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。

- 重命名 **Citrix** 执行文件：
  将 **CitrixWorkspaceApp.exe** 重命名为 **CitrixWorkspaceAppWeb.exe** 以更改添加帐户对话框的行为。
  重命名该文件后，“开始”菜单中将不显示添加帐户对话框。
- 组策略对象管理模板：
  要在 Citrix Workspace 应用程序安装向导中隐藏添加帐户选项，请按如下所示，在本地组策略对象管理模板中的 Self-Service 节点下禁用 **EnableFTUpolicy**。
  这是按计算机进行的设置，因此该行为适用于所有用户。



配置基于电子邮件的帐户发现

配置 Citrix Workspace 应用程序以实现基于电子邮件的帐户发现时，首次安装并配置 Citrix Workspace 应用程序过程中，用户需要输入自己的电子邮件地址（而非服务器 URL）。Citrix Workspace 应用程序将根据域名系统 (DNS) 服务 (SRV) 记录确定与电子邮件地址关联的是 Citrix 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。

有关配置基于电子邮件的帐户发现的详细信息，请参阅 Global App Configuration Service。

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 Workspace 应用程序。安装 Citrix Workspace 应用程序后，用户只需打开该文件即可配置 Citrix Workspace 应用程序。如果您配置适用于 Web 的 Workspace 站点，用户还可以从这些站点获取 Citrix Workspace 应用程序预配文件。

有关详细信息，请参阅 StoreFront 文档中的为用户导出应用商店预配文件。

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 Citrix DaaS 站点的 URL。

- 要通过 Citrix 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 Citrix Gateway 启用了远程访问的应用商店。

  - 要显示所有已配置的应用商店：向用户提供 Citrix Gateway 完全限定域名。
  - 要限制对特定应用商店的访问：按以下格式向用户提供 Citrix Gateway 完全限定域名以及应用商店名称：

CitrixGatewayFQDN?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 Workspace 应用程序将尝试验证连接。如果验证成功，Citrix Workspace 应用程序将提示用户登录该帐户。

要管理帐户，请打开 Citrix Workspace 应用程序主页，然后单击，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。在编辑注册表之前，请务必进行备份。

如果您有多个应用商店帐户，则可以将适用于 Windows 的 Citrix Workspace 应用程序配置为在建立会话时自动连接到所有帐户。要在打开 Citrix Workspace 应用程序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：HKEY_LOCAL_MACHINE\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：HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle

注册表项名称：CurrentAccount

值：AllAccount

类型：REG_SZ

客户端驱动器映射

适用于 Windows 的 Citrix Workspace 应用程序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 Workspace 应用程序将向服务器告知可用的客户端驱动器、COM 端口和 LPT 端口。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 Citrix Virtual Apps and Desktops 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 Citrix Virtual Apps and Desktops 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 H 驱动器映射到运行适用于 Windows 的 Citrix Workspace 应用程序的用户设备上的 C 驱动器。

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 Virtual Apps and Desktops 文档。

HDX Plug and Play USB 设备重定向

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 Citrix Virtual Apps and Desktops 文档中的 USB 和客户端驱动器注意事项。

> 重要提示
>
> 如果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 Workspace 应用程序中将权限设置为始终允许或拒绝设备重定向或者在每次连接设备时都进行提示。此设置只影响在用户更改此设置之后插入的设备。

要将客户端 **COM** 端口映射到服务器 **COM** 端口，请执行以下操作：

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 Citrix Virtual Apps and Desktops 文档。

> 重要提示
>
> COM 端口映射与 TAPI 不兼容。

1. 对于 Citrix Virtual Apps and Desktops 部署，请启用客户端 COM 端口重定向策略设置。
2. 登录 Citrix Workspace 应用程序。
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。

DNS 名称解析

对于使用 Citrix XML Service 的适用于 Windows 的 Citrix Workspace 应用程序，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此功能，否则，Citrix 建议不要在服务器场中启用 DNS 名称解析。

通过 Web Interface 与已发布的应用程序连接的 Citrix Workspace 应用程序也使用 Citrix XML Service。对于通过 Web Interface 连接的 Citrix Workspace 应用程序，Web 服务器将代表 Citrix Workspace 应用程序对 DNS 名称进行解析。

DNS 名称解析在服务器上默认处于禁用状态，而在 Citrix Workspace 应用程序上处于启用状态。当 DNS 名称解析在服务器上处于禁用状态时，请求获取 DNS 名称的任何 Citrix Workspace 应用程序将返回 IP 地址。在 Citrix Workspace 应用程序中不需要禁用 DNS 名称解析。

要对特定用户设备禁用 **DNS** 名称解析，请执行以下操作：

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。在编辑注册表之前，请务必进行备份。

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

配置

May 23, 2024

App Protection

> 免责声明
>
> App Protection 策略通过筛选对基础操作系统所需功能的访问（捕获屏幕或键盘按下所需的特定 API 调用）来运行。这意味着 App Protection 策略甚至可以针对自定义的专用黑客工具提供保护。但是，随着操作系统的发

> 展，捕获屏幕和记录键盘的新方法可能会出现。虽然我们会继续识别和解决这些问题，但我们无法保证在特定配置和部署中提供充足的保护。

App Protection 是一项附加功能，可在使用 Citrix Virtual Apps and Desktops 和 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）时提供增强的安全性。该功能限制了客户端受键盘记录和屏幕捕获恶意软件影响的能力。App Protection 可防止泄露屏幕上显示的用户凭据和敏感信息等机密信息。该功能可防止用户和攻击者截取屏幕截图以及使用键盘记录器收集和利用敏感信息。

App Protection 功能要求您在许可证服务器上安装附加许可证。还必须存在 Citrix Virtual Desktops 许可证。有关许可的信息，请参阅“App Protection”文档中的配置部分。

要求：

- Citrix Virtual Apps and Desktops 版本 1912 或更高版本。
- StoreFront 版本 1912。
- Citrix Workspace 应用程序 1912 或更高版本。

必备条件：

- 必须在 Controller 上启用 App Protection 功能。有关详细信息，请参阅 App Protection 文档。

可以使用以下方法之一将 App Protection 组件包括在 Citrix Workspace 应用程序中：

- 在使用命令行界面或图形用户界面安装 Citrix Workspace 应用程序期间。或
- 应用程序启动期间（按需安装）。

> 注意：
>
> - 此功能仅在 Microsoft Windows Desktop 操作系统（例如 Windows 10、Windows 8.1 和 Windows 7）上受支持。
> - 远程桌面协议 (RDP) 不支持此功能。

本地 **HDX** 会话保护：

两个策略在会话中提供了反键盘记录和反屏幕截图功能。这些策略必须通过 PowerShell 进行配置。没有图形用户界面可用于实现此目的。

> 注意：
>
> Citrix DaaS 不支持 App Protection 功能。

有关 Citrix Virtual Apps and Desktops 上的 App Protection 配置的信息，请参阅 App Protection 文档。

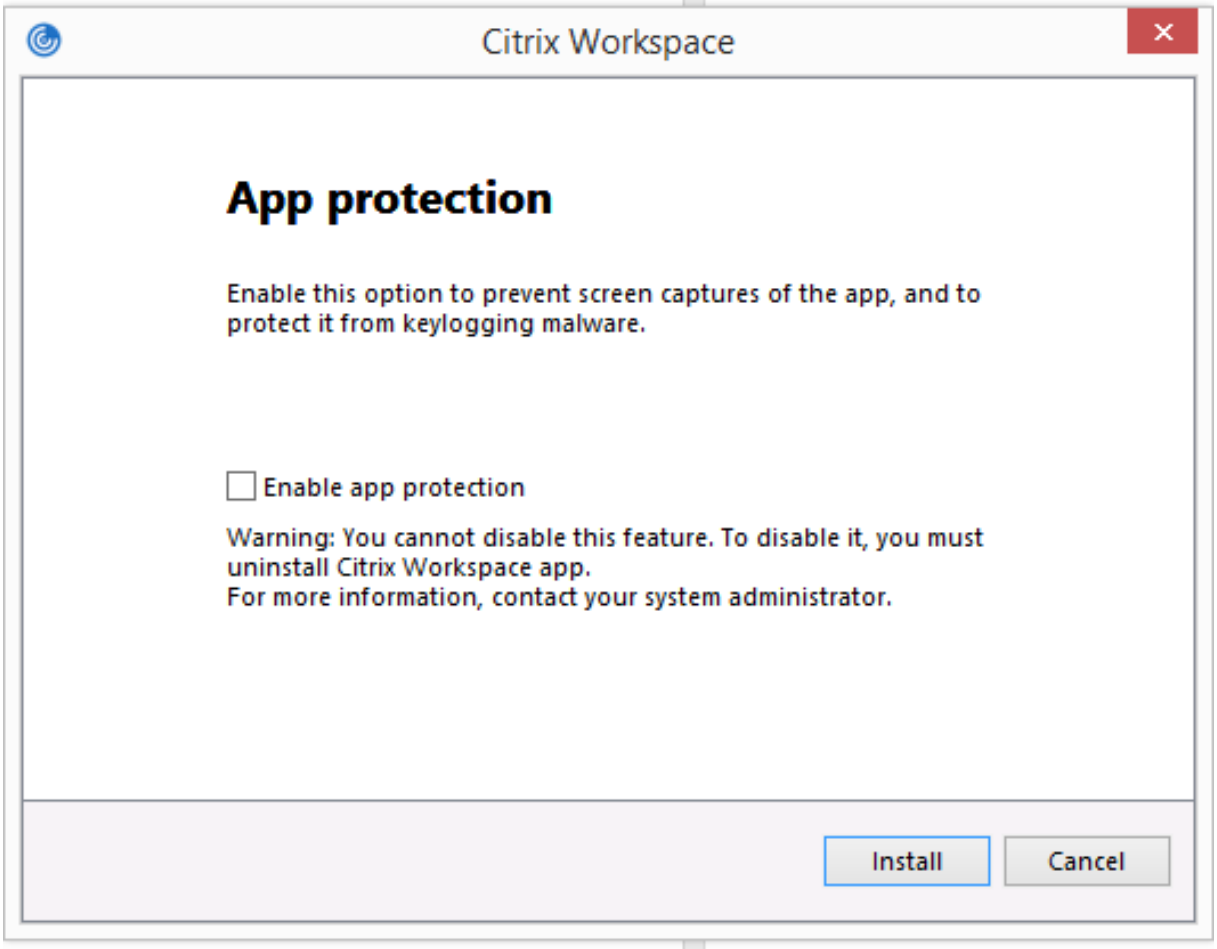
App Protection - Citrix Workspace 应用程序中的配置

> 注意：
>
> - 仅当您的管理员已指示您这样做时，才能将 App Protection 组件包含在 Citrix Workspace 应用程序中。
> - App Protection 组件可能会影响设备上的屏幕捕获功能。

在 Citrix Workspace 应用程序安装过程中，可以使用以下方法之一包括 App Protection：

- 图形用户界面
- 命令行接口

图形用户界面　在 Citrix Workspace 应用程序安装过程中，请使用以下对话框来包括 App Protection 组件。选择启用 **App Protection**，然后单击安装以继续安装。



> 注意：
>
> 在安装过程中未启用 App Protection 会导致在启动受保护的应用程序时出现提示。请按照提示安装 App Protection 组件。

命令行接口　请在 Citrix Workspace 应用程序安装过程中，使用命令行开关 /`includeappprotection` 添加 App Protection 组件。

下表提供了有关受保护的屏幕的信息，具体取决于部署：

App Protection 部署	受保护的屏幕	不受保护的屏幕
包含在 Citrix Workspace 应用程序中	自助服务插件和身份验证管理器/用户证书对话框	连接中心、设备、任何 Citrix Workspace 应用程序错误消息、客户端自动重新连接、添加帐户
在 Controller 上配置	ICA 会话屏幕（应用程序和桌面）	连接中心、设备、任何 Citrix Workspace 应用程序错误消息、客户端自动重新连接、添加帐户

预期行为：

预期行为取决于用户访问包含受保护的资源的 StoreFront 应用商店的方法。

> 注意：
>
> - Citrix 建议您仅使用本机 Citrix Workspace 应用程序启动受保护的会话。

- 适用于 **Web** 的 **Workspace** 上的行为：

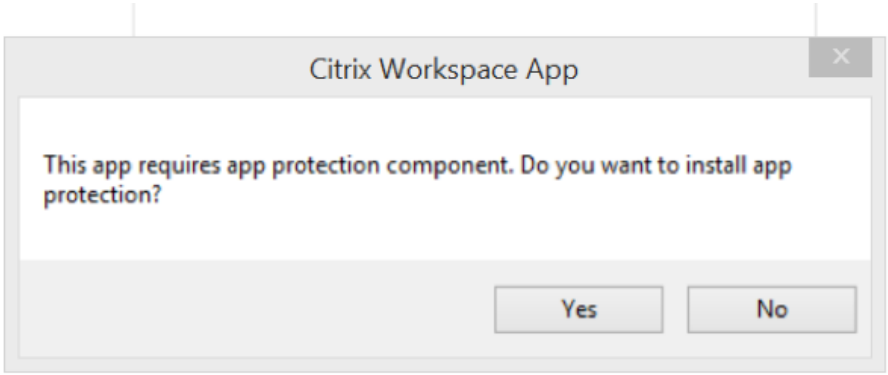
  适用于 Web 的 Workspace 配置不支持 App Protection 组件。不枚举受 App Protection 策略保护的应用程序。有关所分配的资源的详细信息，请与系统管理员联系。

- 不支持 **App Protection** 的 **Citrix Workspace** 应用程序版本中的行为：

  在 Citrix Workspace 应用程序版本 1911 及更早版本中，在 StoreFront 中不枚举受 App Protection 策略保护的应用程序。

- 在 **Controller** 上配置了 **App Protection** 功能的应用程序的行为：

  如果在 Controller 上配置了 App Protection，并且您尝试启动受保护的应用程序，App Protection 将按需安装。此时将显示以下对话框：



单击是后，将安装 App Protection 组件，用户可以启动受保护的应用程序。

- 使用远程桌面协议 **(RDP)** 时受保护会话的行为
  - 如果启动远程桌面协议 (RDP) 会话，则活动的受保护会话将断开连接。
  - 无法在远程桌面协议 (RDP) 会话中启动受保护的会话。

App Protection 错误日志：

App Protection 组件日志注册到调试输出。要收集这些日志，请执行以下操作：

1. 从 Microsoft Web 站点下载并安装 DebugView 应用程序。
2. 启动命令提示符并运行以下命令：

   ```
   Dbgview.exe /t /k /v /l C:\logs.txt
   ```

   从上面的示例中，您可以查看 log.txt 文件中的日志。

该命令指示以下内容：

- /t - DebugView 应用程序在通知区域中以最小化方式启动。
- /k - 启用内核捕获。
- /v - 启用详细内核捕获。
- /l - 将输出记录到特定文件。

卸载 **App Protection** 组件：

要卸载 App Protection 组件，必须从系统中卸载 Citrix Workspace 应用程序。重新启动系统以使更改生效。

> 注意：
>
> App Protection 仅在从版本 1912 开始升级时受支持。

已知问题或限制：

- Microsoft Server 操作系统（例如 Windows Server 2012 R2 和 Windows Server 2016）中不支持任何功能。
- 要创建本地设备的屏幕截图，必须最小化与 Citrix Workspace 应用程序相关的窗口。否则，您将无法创建本地设备的屏幕截图。
- 双跳场景中不支持任何功能。
- 要使此功能正常运行，请在 VDA 上禁用客户端剪贴板重定向策略。

Microsoft Teams 上的端点编码器性能估算器

启动 HdxTeams.exe 进程（嵌入在 Citrix Workspace 应用程序中负责处理 Microsoft Teams 重定向的 WebRTC 媒体引擎）时，该进程会估算端点的 CPU 可以在不过载的情况下维持的最佳编码分辨率。可能的值为 240p、360p、720p 和 1080p。

性能评估过程（也称为 `webrtcapi.EndpointPerformance`）在 HdxTeams.exe 初始化时运行。宏模块代码确定了使用特定端点可以实现的最佳分辨率。然后，在对等方之间或对等方与会议服务器之间的编解码器协商过程中包含尽可能高的分辨率。

对于具有自己的最大可用分辨率的端点，有四种性能类别：

端点性能	最大分辨率	注册表项值
快	1080p	3
中	720p	2
慢	360p	1
非常慢	240p	0

可以通过配置标志禁用 VP9 或 H264 编解码器。
H264 在 CPU 上较轻，但占用的带宽更多。相反，VP9 占用的 CPU 功率较多，但占用的带宽较少。

Citrix Workspace 应用程序中的注册表路径：

导航到注册表路径 HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream 并创建以下项：\

名称	类型	值	说明
DisableVP9	DWORD	1; 0	1 - 禁用 VP9 编解码器；0 - 启用
DisableH264	DWORD	1;0	1 - 禁用 H.264 编解码器；0 - 启用

名称	类型	值	说明
OverridePerformance	DWORD	0;1;2;3	强制实现所需的性能。值必须介于 0 到 3 之间，其中 0 表示非常慢，3 表示非常快。

有关 Microsoft Teams 优化的详细信息，请参阅 Microsoft Teams 优化。

自适应传输

自适应传输是 Citrix Virtual Apps and Desktops 和 Citrix DaaS 的数据传输机制。此传输速度更快，能够扩展，改进了应用程序的交互性，并且在具有挑战性的远距离 WAN 和 Internet 连接中互动性更强。自适应传输维持高服务器可扩展性，并有效利用带宽。借助自适应传输，ICA 虚拟通道可以自动响应不断变化的网络条件。它们可以在 Citrix 协议（名为 Enlightened Data Transport (EDT)）与 TCP 之间智能地切换基本协议，以实现最佳性能。这提高了所有 ICA 虚拟通道（包括 Thinwire 显示远程处理、文件传输（客户端驱动器映射）、打印和多媒体重定向）的数据吞吐量。相同的设置适用于 LAN 和 WAN 条件。

在早期版本中，当 **HDXoverUDP** 设置为首选后，将尽可能使用基于 EDT 的数据传输，并启用回退到 TCP。

启用了会话可靠性时，EDT 和 TCP 会尝试并行连接、会话可靠性重新连接和客户端自动重新连接。此增强功能缩短了 EDT 设置为“首选”时的连接时间，但所需的基础 UDP 传输不可用，并且必须使用 TCP。

默认情况下，回退到 TCP 后，自适应传输将继续每隔 5 分钟搜寻一次 EDT。

要求：

- Citrix Virtual Apps and Desktops 7.12 或更高版本。
- StoreFront 3.8。
- 仅限 IPv4 VDA。IPv6 配置以及 IPv6 和 IPv4 混合配置不受支持。
- 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 为必需端口，在您安装 VDA 时自动打开。但是，UDP 端口 1494 和 2598 不自动打开。请将其设置为已启用。

默认情况下，Citrix Workspace 应用程序允许自适应传输。此外，默认情况下，仅当在 Delivery Controller 上将 VDA 配置为首选时以及在 VDA 上应用了该设置时，客户端才会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。

使用组策略对象 (GPO) 管理模板禁用客户端上的自适应传输。

使用 **Citrix Workspace** 应用程序组策略对象 **(GPO)** 管理模板配置自适应传输

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），并且 TCP 始终处于使用状态。

1. 通过运行 gpedit.msc 打开 Citrix Workspace 应用程序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 Workspace** > 网络路由。
3. 将 **Citrix Workspace** 的传输协议策略设置为已启用。
4. 根据需要选择 **Citrix Workspace** 的通信协议。
    - 关 - 指示使用 TCP 进行数据传输。
    - 首选 - 指示客户端尝试首先使用 UDP 连接到服务器。如果 UDP 不可用，连接将切换到 TCP 作为回退。
    - 开 - 指示适用于 Windows 的 Citrix Workspace 应用程序仅使用 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。

要使用自适应传输，请将 Citrix Workspace 应用程序模板文件添加到策略定义文件夹。有关向本地 GPO 中添加模板文件的信息，请参阅组策略对象模板部分。

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 **HDX-OverUDP** 注册表项。

有关详细信息，请参阅 Citrix Virtual Apps and Desktops 文档中的自适应传输部分。

“高级首选项”表

您可以自定义通知区域中的 Citrix Workspace 应用程序图标的右键菜单中存在的高级首选项表的可用性及其内容。自定义可以确保用户能够仅在其系统中应用管理员指定的设置。具体而言，用户能够执行以下操作：

- 一起隐藏“高级首选项”表
- 在表中隐藏以下特定设置：
    - 数据收集
    - 连接中心
    - 配置检查器
    - 键盘和语言栏

- 高 DPI
- 支持信息
- 快捷方式和重新连接
- Citrix Casting

在右键菜单中隐藏“高级首选项”选项

可以使用 Citrix Workspace 应用程序组策略对象 (GPO) 管理模板隐藏“高级首选项”表：

1. 通过运行 gpedit.msc 打开 Citrix Workspace 应用程序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 Workspace** > 自助服务 > 高级首选项选项。
3. 选择禁用高级首选项策略。
4. 选择已启用在通知区域中的 Citrix Workspace 应用程序图标的右键菜单中隐藏“高级首选项”选项。

> 注意：
>
> 默认情况下，选择未配置选项。

使用组策略对象 **(GPO)** 管理模板隐藏“高级首选项”表中的特定设置

1. 通过运行 gpedit.msc 打开 Citrix Workspace 应用程序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 Workspace** > 自助服务 > 高级首选项选项。
3. 选择适用于要隐藏的设置的策略。

下表列出了可以选择的选项以及每个选项的影响：

选项	操作
未配置	显示设置
已启用	隐藏设置
已禁用	显示设置

可以在“高级首选项”表中隐藏以下特定设置：

- 配置检查器
- 连接中心
- 高 DPI
- 数据收集
- 删除保存的密码
- 键盘和语言栏
- 快捷方式和重新连接

- 支持信息
- Citrix Casting

使用注册表编辑器在“高级首选项”表中隐藏“重置 **Workspace**”选项

可以使用注册表编辑器在“高级首选项”表中隐藏重置 **Workspace** 选项。

1. 启动注册表编辑器
2. 导航到 `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle`。
3. 创建一个字符串值注册表项 **EnableFactoryReset** 并将其设置为以下任意选项：
    - True - 在“高级首选项”表中显示“重置 Workspace”选项。
    - False - 在“高级首选项”表中隐藏“重置 Workspace”选项。

在“高级首选项”表中隐藏“**Citrix Workspace** 更新”选项

> 注意：
>
> “Citrix Workspace 更新”选项的策略路径与“高级首选项”表中存在的其他选项的策略路径不同。

1. 通过运行 gpedit.msc 打开 Citrix Workspace 应用程序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 Workspace** > **Workspace** 更新。
3. 选择 **Workspace** 更新策略。
4. 选择已禁用在高级首选项表中隐藏“Workspace 更新”设置。

应用程序交付

通过 Citrix Virtual Apps and Desktops 和 Citrix DaaS 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 Workspace 应用程序将提供基于浏览器访问应用程序和桌面的功能。可以使用适用于 Web 的 Workspace 或 Web Interface 站点来选择和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 Workspace 应用程序中或将 Citrix Workspace 应用程序配置为指向 StoreFront Web 站点，可以配置自助服务模式，在此模式下，您可以从 Citrix Workspace 应用程序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 Workspace 应用程序允许您选择要在“开始”菜单中显示的应用程序。

- 仅快捷方式模式 - 可以将 Citrix Workspace 应用程序配置为自动直接在“开始”菜单中或桌面上放置应用程序和桌面快捷方式。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。

有关详细信息，请参阅 Citrix Virtual Apps and Desktops 文档中的创建交付组部分。

配置自助服务模式

将 StoreFront 帐户添加到 Citrix Workspace 应用程序，或者将 Citrix Workspace 应用程序配置为指向 StoreFront 站点以使用自助服务模式。自助服务允许用户从 Citrix Workspace 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 Workspace 应用程序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 Workspace 应用程序中删除，请将字符串 KEYWORDS: Mandatory 附加到应用程序说明后面。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。
- 要向用户宣传应用程序，或者要通过在 Citrix Workspace 的“精选”列表中列出常用的应用程序以使其更易于找到，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

1. 通过运行 gpedit.msc 打开 Citrix Workspace 应用程序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 Workspace** > 自助服务。
3. 选择管理 **SelfServiceMode** 策略。
    a) 选择已启用以查看自助服务用户界面。
    b) 选择已禁用以手动订阅应用程序。此选项将隐藏自助服务用户界面。
4. 选择管理应用程序快捷方式策略。
5. 根据需要选择选项。
6. 单击应用和确定。
7. 重新启动 Citrix Workspace 应用程序以使所做的更改生效。

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，而不在通过 Citrix Virtual Apps and Desktops 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 Citrix Workspace 图标，请使用 SilentlyUninstallRemovedResources。设置：true 或 false（默认为 false）。

在 web.config 文件中，将更改添加到帐户的 **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，请将对配置所做的更改传播到服务器组，以便更新部署中的其他服务器。有关详细信息，请参阅 StoreFront 文档。

使用 **Citrix Virtual Apps and Desktops 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 Workspace 应用程序配置为自动直接在“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适用于 Windows 的 Workspace 版本类似，但是，版本 4.2.100 中引入了使用 Citrix Virtual Apps 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。

如果您希望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 Citrix Virtual Apps 每应用程序设置：

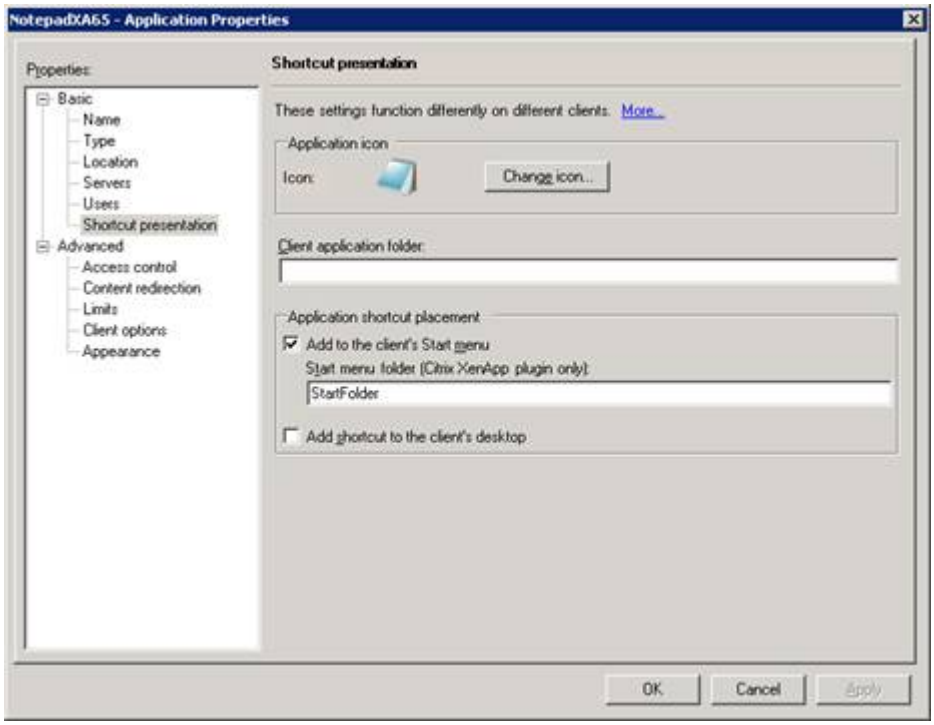
如果您希望通过每应用程序设置来确定应用程序的放置位置，而无论处于自助服务模式还是“开始”菜单模式。	为适用于 Windows 的 Citrix Workspace 应用程序配置 **PutShortcutsInStartMenu=false** 并启用每应用程序设置。注意：此设置仅适用于 Web Interface 站点。

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

在 **XenApp 6.5** 中配置每应用程序设置

在 XenApp 6.5 中配置每应用程序发布快捷方式：

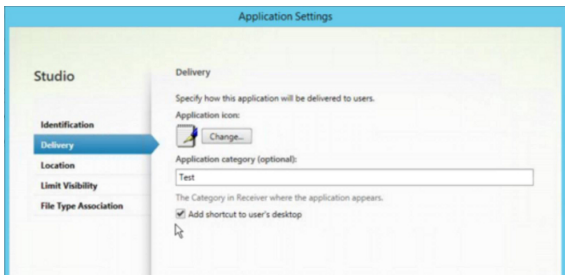
1. 在 **XenApp** 应用程序属性屏幕中，展开基本属性。
2. 选择快捷方式显示选项。
3. 在快捷方式显示屏幕的“应用程序快捷方式放置”部分中，选中添加到客户端“开始”菜单复选框。选中该复选框后，输入要用于放置快捷方式的文件夹的名称。如果未指定文件夹名称，XenApp 会将快捷方式放置在“开始”菜单中，而不是放置在文件夹中。
4. 选择添加到客户端“开始”菜单以包括客户端计算机的桌面上的快捷方式。
5. 单击应用。
6. 单击确定。



使用 **XenApp 7.6** 中的每应用程序设置自定义应用程序快捷方式的位置

在 XenApp 7.6 中配置每应用程序发布快捷方式：

1. 在 Citrix Studio 中，找到应用程序设置屏幕。
2. 在应用程序设置屏幕中，选择交付。在此屏幕中，可以指定如何向用户交付应用程序。
3. 为应用程序选择恰当的图标。单击更改浏览到所需图标所在的位置。
4. 在应用程序类别字段中，可以选择指定要在 Citrix Workspace 应用程序中显示的应用程序的类别。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，Citrix Workspace 应用程序将提供从网络共享复制.EXE 存根的功能。

此功能涉及多个步骤：

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. 添加注册表项以使适用于 Windows 的 Workspace 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 HKEY_CURRENT_USER\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d “true”。
2. 使用 regedit 添加 HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle /v ReuseStubs /t REG_SZ /d “true”。HKEY_CURRENT_USER 的优先级高于 HKEY_LOCAL_MACHINE。

> 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 Citrix Workspace 应用程序的计算机；Citrix Workspace 应用程序将生成可执行文件。
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. 对于已锁定的各个客户端计算机，请设置以下注册表项：
    a) Reg add HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle /v CommonStubDirectory /t REG_SZ /d “\\ShareOne\WorkspaceStubs”
    b) Reg add HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle /v
    c) CopyStubsFromCommonStubDirectory /t REG_SZ /d “true”. 如果愿意，还可以在 HKEY_CURRENT_USER 上配置以下设置。HKEY_CURRENT_USER 的优先级高于 HKEY_LOCAL_MACHINE。
    d) 退出并重新启动 Citrix Workspace 应用程序以测试设置。

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：

如果您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 Workspace 应用程序。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。
如果您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。	不为 Citrix Workspace 应用程序配置任何选项，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 Workspace 应用程序但不执行任何配置，然后浏览到适用于 Web 的 Workspace 和 Web Interface。还可以将 Citrix Workspace 应用程序配置为进行自助访问而不将快捷方式放置在任何位置。

如果您希望阻止 Citrix Workspace 应用程序自动将应用程序快捷方式放置在“开始”菜单中的任何位置。	为 Citrix Workspace 应用程序配置 PutShortcutsInStartMenu=False。即使在自助服务模式下，Citrix Workspace 应用程序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。

如果您希望 Citrix Workspace 应用程序自动将所有应用程序快捷方式都放置在“开始”菜单中。	为 Citrix Workspace 应用程序配置 SelfServiceMode=False。所有可用的应用程序都将显示在“开始”菜单中。
如果您希望将所有应用程序快捷方式都放置在桌面上。	为 Citrix Workspace 应用程序配置 PutShortcutsOnDesktop=true。所有可用的应用程序都将显示在桌面上。

如果您希望将所有快捷方式都放置在桌面上的文件夹中。	为 Citrix Workspace 应用程序配置 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

如果您希望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：

如果您希望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。	为 Citrix Workspace 应用程序配置 PutShortcutsInStartMenu=false 并启用每应用程序设置。

应用程序放置在类别文件夹或特定文件夹中

如果您希望应用程序在特定文件夹中显示，请使用以下选项：

如果您希望 Citrix Workspace 应用程序放置在“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。	为 Citrix Workspace 应用程序配置 UseCategoryAsStartMenuPath=True。
如果希望 Citrix Workspace 应用程序放置在“开始”菜单中的应用程序位于特定文件夹中。	为 Citrix Workspace 应用程序配置 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：

如果您希望 Citrix Workspace 应用程序在注销时删除所有应用程序。	为 Citrix Workspace 应用程序配置 RemoveAppsOnLogoff=True。
如果您希望 Citrix Workspace 应用程序在退出时删除应用程序。	配置 Citrix Workspace 应用程序，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：

- 要指定必须使用本地安装的应用程序而非 Citrix Workspace 应用程序中提供的应用程序，请附加文本字符串 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 Workspace 应用程序将搜索指定的模式，以确定是否已在本地安装该应用程序。如果已在本地安装，Citrix Workspace 应用程序将订阅该应用程序，但不创建快捷方式。用户从 Citrix Workspace 应用程序窗口中启动该应用程序时，Citrix Workspace 应用程序将启动本地安装的（首选）应用程序。

  如果用户在 Citrix Workspace 应用程序外部卸载了某个首选应用程序，则下次 Citrix Workspace 应用程序刷新时将取消订阅该应用程序。如果用户从 Citrix Workspace 应用程序对话框中卸载了某个首选应用程序，Citrix Workspace 应用程序将取消订阅该应用程序，但不卸载。

> 注意：
>
> Citrix Workspace 应用程序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 Workspace 应用程序中提供的应用程序，请附加文本字符串 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 Workspace 应用程序将搜索指定的模式，以确定是否已在本地安装该应用程序。如果已在本地安装，Citrix Workspace 应用程序将订阅该应用程序，但不创建快捷方式。用户从 Citrix Workspace 应用程序对话框中启动该应用程序时，Citrix Workspace 应用程序将启动本地安装的（首选）应用程序。

  如果用户在 Citrix Workspace 应用程序外部卸载了某个首选应用程序，则下次 Citrix Workspace 应用程序刷新时将取消订阅该应用程序。如果用户从 Citrix Workspace 应用程序中卸载了某个首选应用程序，Citrix Workspace 应用程序将取消订阅该应用程序，但不卸载。

自 1912 起，您可以使用注册表编辑器在 Citrix Workspace 应用程序中配置自动刷新行为。

在早期版本中，当您重新启动 Citrix Workspace 应用程序时，即使缓存数据可用，也会执行自动刷新。

> 注意：
>
> 不能在非 X1 应用商店帐户中配置此选项。

使用注册表编辑器配置自动刷新：

1. 启动注册表编辑器，导航到 HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle 路径。

2. 创建以下字符串值注册表项：

注册表项	值
InitialRefreshMinMs	10000（10 秒）
InitialRefreshMaxMs	15000（15 秒）
SuppressRefreshMs	1000（1 秒）

3. 保存并关闭编辑器。

> 注意：
>
> Citrix Workspace 应用程序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
控制台	McAfee\VirusScan Console	是

- 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 Citrix Virtual Apps and Desktops 中以程序方式实施的覆盖很有用。

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	\Programs\Microsoft Word 2010	是

- prefer=”\Folder1\Folder2\…\ApplicationName”

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

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

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

应用程序启动时间

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 Workspace 应用程序时或在计划的时间（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。用户向适用于 Windows 的 Citrix Workspace 应用程序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，但对您不可见。

StoreFront 部署支持会话预启动功能。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。Citrix Virtual Apps and Desktops 部署不支持会话预启动。

有关详细信息，请参阅 Citrix Virtual Apps and Desktops 文档中的交付组中的会话预启动和会话延迟。

默认禁用会话预启动功能。要启用会话预启动功能，请在 Workspace 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，则将自动启用预启动。如果您希望使用域直通 (SSON) 而不启用预启动，请将 **EnablePreLaunch** 注册表项的值设置为 false。

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 Workspace 应用程序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 Citrix Virtual Apps 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。

不能使用 receiver.admx 文件自定义预启动功能。但是，可以通过在安装适用于 Windows 的 Citrix Workspace 应用程序的过程中或安装完成后修改注册表值来更改预启动配置。

- HKEY_LOCAL_MACHINE 值在客户端安装过程中写入。
- 您可以通过 HKEY_CURRENT_USER 值在同一计算机上向不同的用户提供不同的设置。用户无需管理权限即可更改 HKEY_CURRENT_USER 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 64 位 Windows 操作系统：HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Prelaunch

对于 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 表示小时和分钟；M:T:W:TH:F:S:SU 表示星期几。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。

双向内容重定向

双向内容重定向策略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。服务器策略在 Studio 中设置，客户端策略则在 Citrix Workspace 应用程序组策略对象管理模板中设置。

尽管 Citrix 还提供主机到客户端重定向以及适用于客户端到 URL 重定向的本地应用程序访问，但我们建议您对加入域的 Windows 客户端使用双向内容重定向。

可以使用以下方法之一启用双向内容重定向：

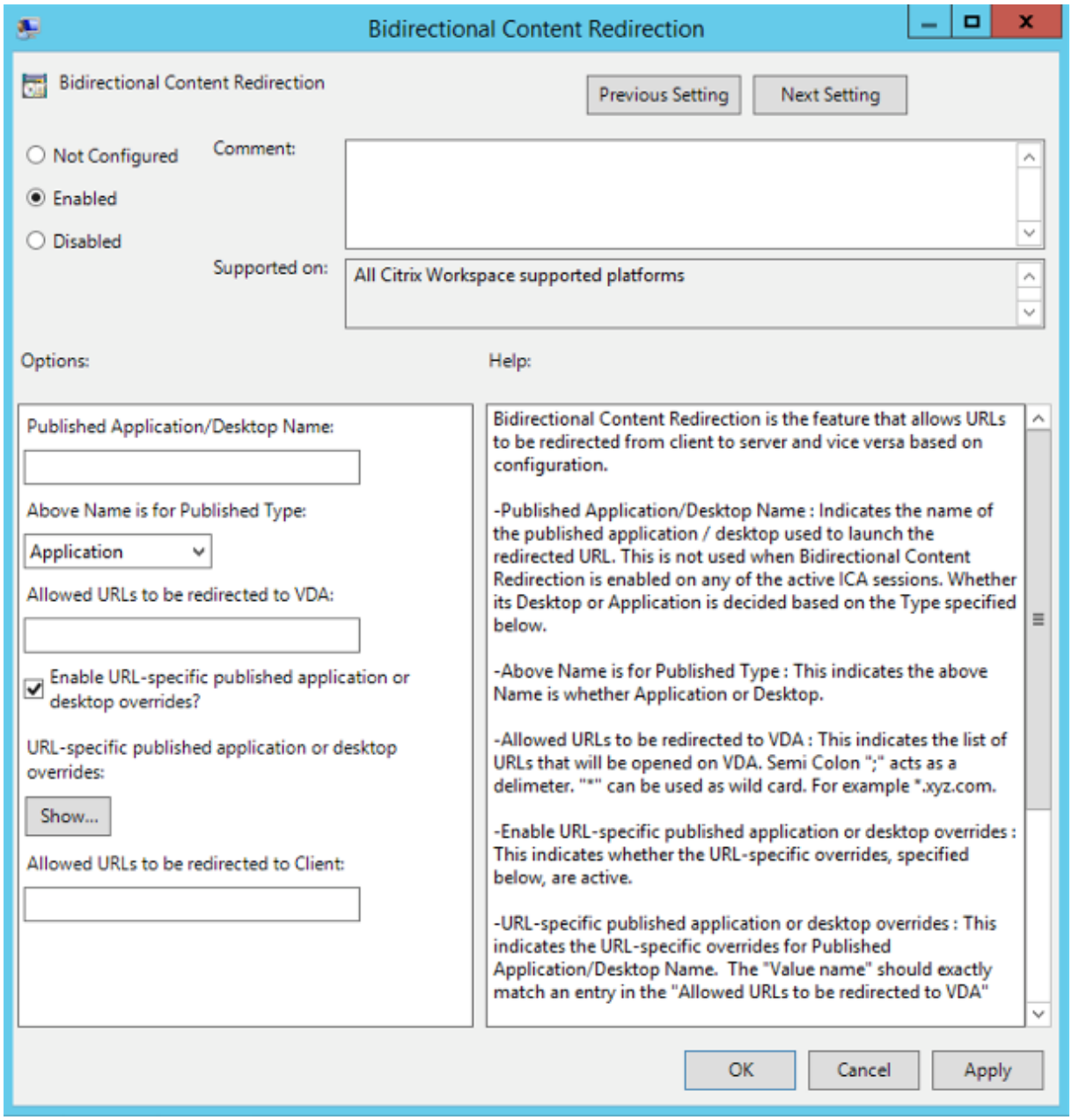
1. 组策略对象 (GPO) 管理模板
2. 注册表编辑器

> 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。
> - 包括 URL 时，可以指定一个 URL 或以分号分隔的 URL 列表。可以使用星号 (*) 作为通配符。

要使用 **GPO** 管理模板启用双向内容重定向，请执行以下操作：

请仅在首次安装适用于 Windows 的 Citrix Workspace 应用程序时使用组策略对象管理模板配置。

1. 通过运行 gpedit.msc 打开 Citrix Workspace 应用程序组策略对象管理模板。
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 Workspace** > 用户体验。
3. 选择双向内容重定向策略。

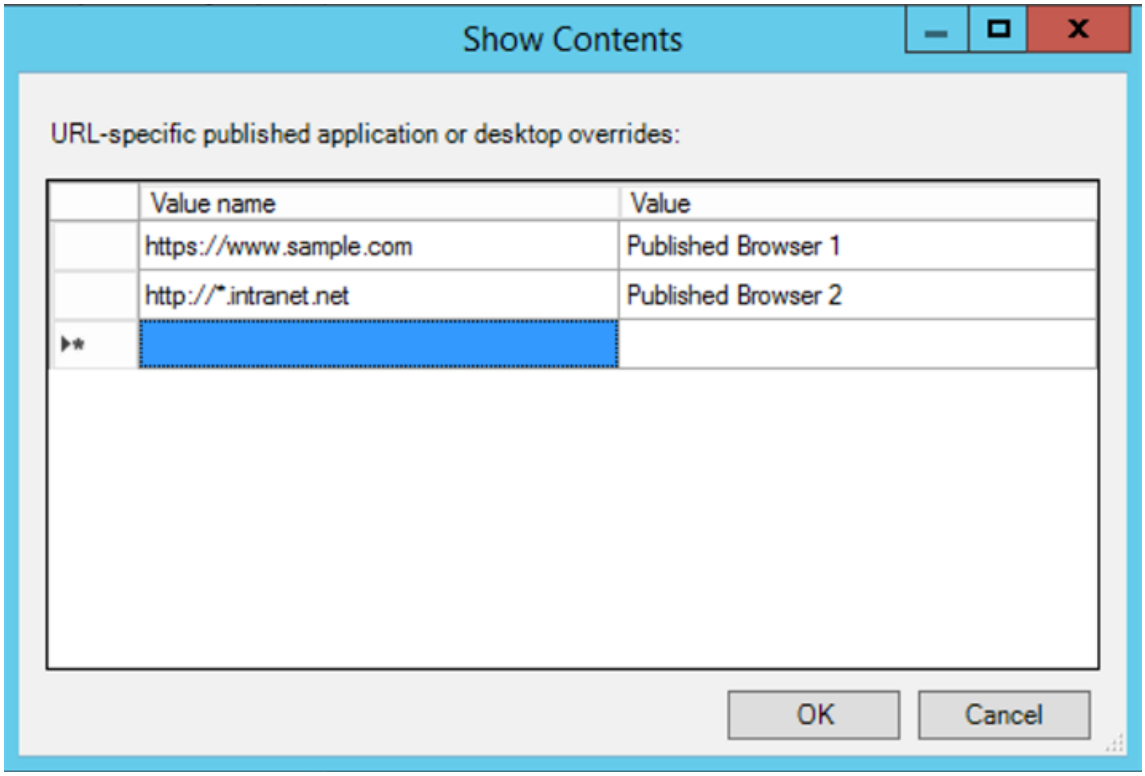


1. 在已发布的应用程序/桌面名称字段中，提供用于启动重定向的 URL 的资源名称。

   > 注意：
   >
   > 包括 URL 时，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。

2. 从上面的名称适用的已发布类型中，根据需要选择资源应用程序或桌面。
3. 在允许重定向到 **VDA** 的 **URL** 字段中，输入必须重定向的 URL。用分号分隔列表。

4. 选择是否启用 **URL** 特定的已发布应用程序或桌面替代**?** 选项以替代 URL。
5. 单击显示以显示一个列表，其中值名称必须与允许重定向到 **VDA** 的 **URL** 字段中列出的任何 URL 匹配。该值必须与已发布的应用程序名称匹配。



6. 在允许重定向到客户端的 **URL:** 字段中，输入必须从服务器重定向到客户端的 URL。用分号分隔列表。

> 注意：
>
> 包括 URL 时，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。

7. 单击应用和确定。
8. 在命令行中，运行 `gpupdate /force` 命令。

要使用注册表启用双向内容重定向，请执行以下操作：

要启用双向内容重定向，请从 Citrix Workspace 应用程序安装文件夹 `C:\Program Files (x86)\Citrix\ICA Client`) 运行 `redirector.exe /RegIE` 命令。

> 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和 VDA，则会发生循环配置。
> - 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。
> - 确保只有一种服务器文件类型关联和主机内容重定向策略在同一台计算机上设置为“已启用”。Citrix 建议您禁用服务器文件类型关联功能或主机内容 (URL) 重定向功能，以确保 URL 重定向正常运行。

限制：

如果重定向由于会话启动问题而失败，则不存在回退机制。

Bloomberg 键盘

Citrix Workspace 应用程序支持在虚拟应用程序和桌面会话中使用 Bloomberg 键盘。所需的组件随插件安装。可以在安装适用于 Windows 的 Citrix Workspace 应用程序时或者使用注册表编辑器启用 Bloomberg 键盘功能。

不建议使用 Bloomberg 键盘进行多个会话。该键盘仅在单会话环境中才能使用。

配置 **Bloomberg** 键盘：

> 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：

   - 要启用此功能，对于类型为 DWORD、名称为 **EnableBloombergHID** 的条目，请将值设置为 1。
   - 要禁用此功能，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。

要防止 **Desktop Viewer** 窗口变暗，请执行以下操作：

如果使用了多个 Desktop Viewer 窗口，则默认情况下，处于非活动状态的桌面将变暗。如果用户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。通过编辑注册表编辑器，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

- 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

使用这些注册表项之前，请核实您的 Citrix Virtual Apps and Desktops 和 Citrix DaaS 管理员是否已为此功能设置了策略。

将该条目设置为任意非零值，例如 1 或 true。

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

1. HKEY_CURRENT_USER\Software\Policies\Citrix\…
2. HKEY_LOCAL_MACHINE\Software\Policies\Citrix\…
3. HKEY_CURRENT_USER\Software\Citrix\…
4. HKEY_LOCAL_MACHINE\Software\Citrix\…

Citrix Casting

Citrix Ready Workspace Hub 将数字环境和物理环境结合在一起，在安全的智能空间中交付应用程序和数据。完整的系统连接了设备（或一些对象），例如移动应用程序和传感器，以创建智能化的响应环境。

Citrix Ready Workspace Hub 在 Raspberry Pi 3 平台上构建而成。运行 Citrix Workspace 应用程序的设备将连接到 Citrix Ready Workspace Hub，并将应用程序或桌面投射到较大的显示器上。Citrix Casting 仅在 Microsoft Windows 10 版本 1607 及更高版本或 Windows Server 2016 上受支持。

Citrix Casting 是一种允许您从移动设备安全地即时访问任何应用程序并在大屏幕上显示的功能。

> 注意：
>
> - 适用于 Windows 的 Citrix Casting 支持 Citrix Ready Workspace Hub 版本 2.40.3839 及更高版本。早期版本的 Workspace Hub 可能无法被系统检测到或导致出现投射错误。
> - 适用于 Windows 的 Citrix Workspace 应用程序（应用商店版本）不支持 Citrix Casting 功能。

必备条件：

- 在设备上启用了蓝牙以便发现 Hub。
- Citrix Ready Workspace Hub 和 Citrix Workspace 应用程序都必须位于同一网络中。
- 在运行 Citrix Workspace 应用程序的设备与 Citrix Ready Workspace Hub 之间不得阻止端口 55555。

- 对于 Citrix Casting，不得阻止端口 1494。
- 端口 55556 为移动设备与 Citrix Ready Workspace Hub 之间的 SSL 连接的默认端口。可以在 Raspberry Pi 的设置页面上配置不同的 SSL 端口。如果阻止了 SSL 端口，用户将无法与 Workspace Hub 之间建立 SSL 连接。
- Citrix Casting 仅在 Microsoft Windows 10 版本 1607 及更高版本或 Windows Server 2016 上受支持。

配置 **Citrix Casting** 启动

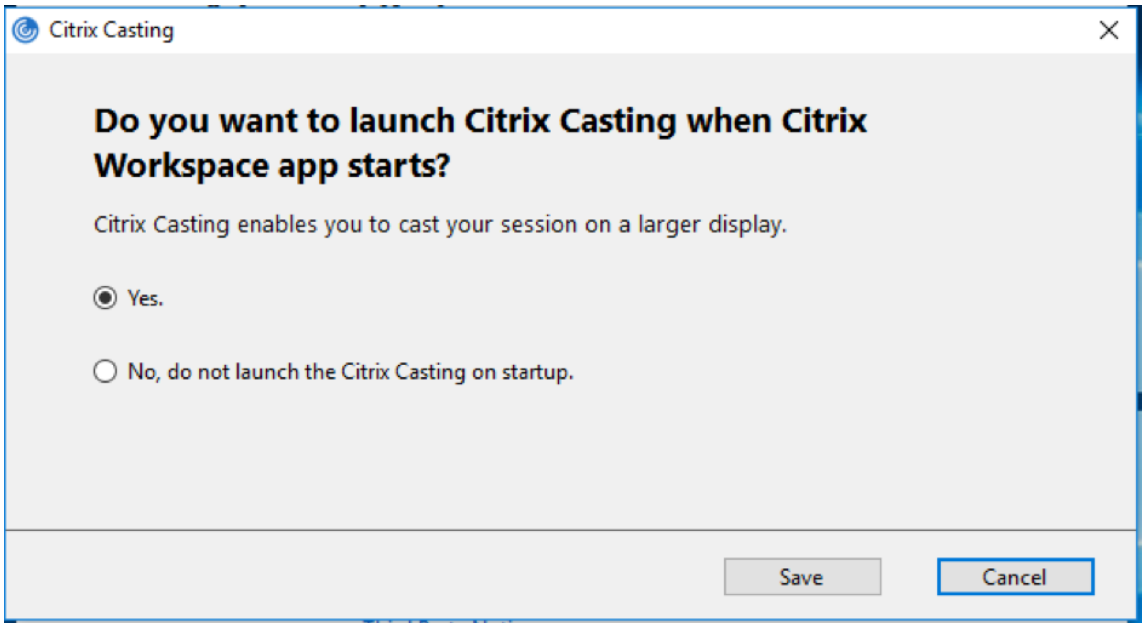
> 注意：
>
> 可以隐藏通知区域中的 Citrix Workspace 应用程序图标中提供的全部或部分“高级首选项”表。有关详细信息，请参阅“高级首选项”表。

1. 右键单击通知区域中的 Citrix Workspace 应用程序图标并选择高级首选项。

   此时将显示高级首选项对话框。

2. 选择 **Citrix Casting**。

   此时将显示 **Citrix Casting** 对话框。



3. 选择以下选项之一：

   - 是 - 指示在 Citrix Workspace 应用程序启动时启动 Citrix Casting。
   - No, do not launch the Citrix Casting on startup（否，不在启动时启动 Citrix Casting）- 指示不在 Citrix Workspace 应用程序启动时启动 Citrix Casting。

> 注意：
>
> 选择 **No**（否）选项不会终止当前屏幕投射会话。该设置仅在下一次启动 Citrix Workspace 应用程序时应用。

4. 单击保存以应用所做的更改。

如何将 **Citrix Casting** 与 **Citrix Workspace** 应用程序结合使用

1. 登录 Citrix Workspace 应用程序，并在您的设备上启用蓝牙。

   此时将显示可用 Hub 列表。该列表按 Workspace Hub 信标软件包的 RSSI 值排序。

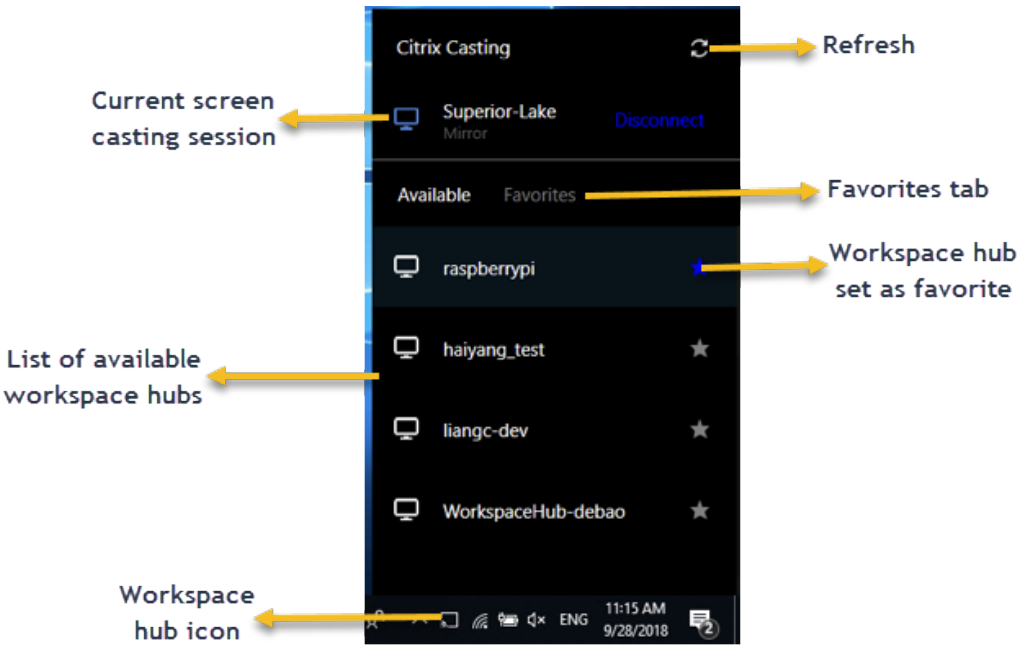
2. 选择要投射屏幕的 Workspace Hub，然后选择以下选项之一：

   - 镜像用于复制主屏幕并将显示内容投射到已连接的 Workspace Hub 设备。
   - 扩展用于将 Workspace Hub 设备屏幕用作辅助屏幕。

> 注意：
>
> 退出 Citrix Workspace 应用程序不会退出 Citrix Casting。

在 **Citrix Casting** 通知对话框中，提供了以下选项：

1. 当前屏幕投射会话显示在顶部。
2. 刷新图标。
3. 断开连接，用于停止当前屏幕投射会话。
4. 星型图标，用于将 Workspace Hub 添加到收藏夹。
5. 右键单击通知区域中的 Workspace Hub 图标并选择退出可断开屏幕投射会话连接，并退出 Citrix Ready Workspace Hub。



自检列表

如果 Citrix Workspace 应用程序无法检测到范围内的任何可用 Workspace Hub 并与之进行通信，请确保在自检中完成以下各项：

1. Citrix Workspace 应用程序和 Citrix Ready Workspace Hub 连接到同一网络。
2. 在启动 Citrix Workspace 应用程序的设备上启用了蓝牙并且蓝牙正常运行。
3. 启动 Citrix Workspace 应用程序的设备在 Citrix Ready Workspace Hub 的范围内（小于 10 米且没有墙之类的任何阻挡物）。
4. 在 Citrix Workspace 应用程序中启动浏览器，然后键入 `http://<hub_ip>:55555/device-details.xml` 以检查是否显示了 Workspace Hub 设备的详细信息。
5. 在 Citrix Ready Workspace Hub 中单击刷新，并尝试重新连接到 Workspace Hub。

已知问题及限制

1. 在设备与 Citrix Ready Workspace Hub 连接到同一网络之前，Citrix Casting 不起作用。
2. 如果出现网络问题，Workspace Hub 设备上可能存在延迟显示。
3. 选择扩展后，启动 Citrix Ready Workspace 应用程序的主屏幕会闪烁多次。
4. 在扩展模式下，不能将辅助显示器设置为主显示器。
5. 设备上的显示设置发生任何变化时，屏幕投射会话都会自动断开连接。例如，屏幕分辨率发生变化、屏幕方向发生变化。
6. 在屏幕投射会话期间，如果运行 Citrix Workspace 应用程序的设备处于锁定、睡眠或休眠状态，则在登录时会显示错误。

7. 不支持多个屏幕投射会话。
8. Citrix Casting 支持的最大屏幕分辨率为 1920 x 1440。
9. Citrix Casting 支持 Citrix Ready Workspace Hub 版本 2.40.3839 及更高版本。早期版本的 Workspace Hub 可能无法被系统检测到或导致出现投射错误。
10. 适用于 Windows 的 Citrix Workspace 应用程序（应用商店版本）不支持此功能。
11. 在 Windows 10 Build 1607 中，可能无法正确定位处于扩展模式的 Citrix Casting。

复合 **USB** 设备重定向

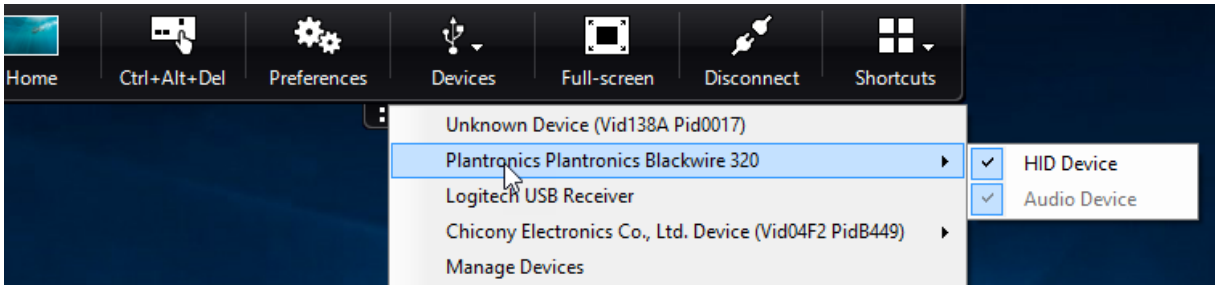
配置复合 **USB** 重定向：

1. 通过运行 gpedit.msc 打开 Citrix Workspace 应用程序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 Workspace** > 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. 单击应用和确定保存此策略。

要允许或拒绝使用某个接口，请执行以下操作：

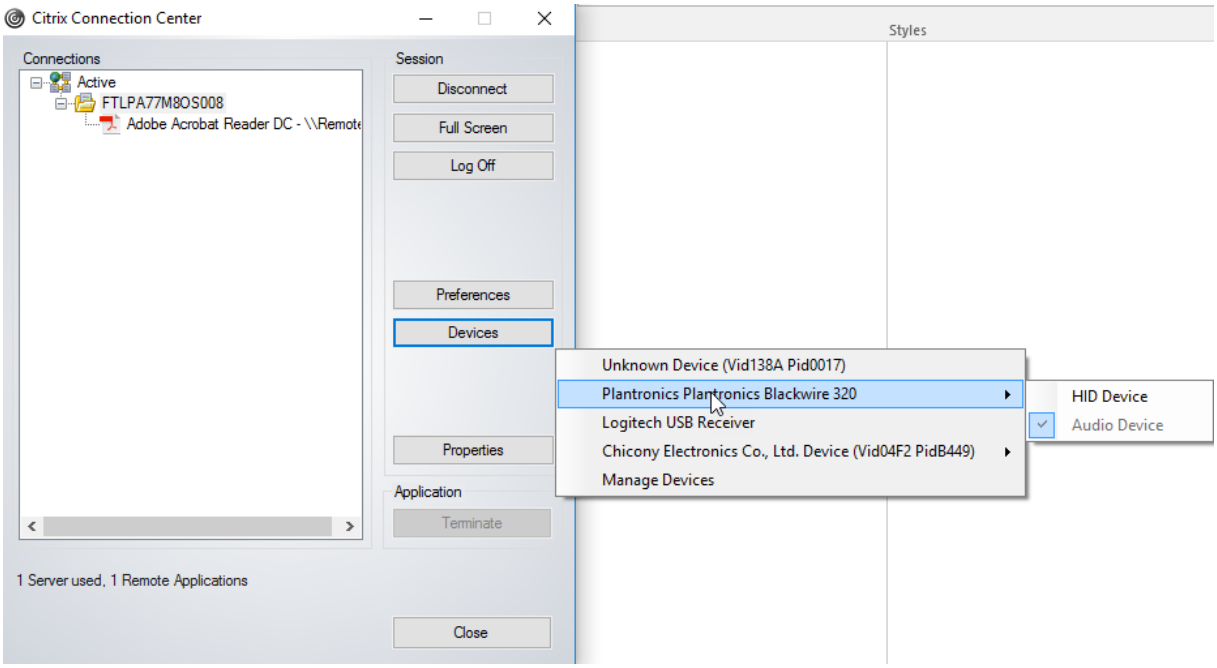
1. 通过运行 gpedit.msc 打开 Citrix Workspace 应用程序组策略对象管理模板。
2. 在用户配置节点下，转至管理模板 > **Citrix** 组件 > **Citrix Workspace** > 远程连接客户端设备 > 通用 **USB** 远程连接。
3. 选择 **USB** 设备规则策略。
4. 选择已启用。
5. 在 **USB** 设备规则文本框中，添加要允许或拒绝使用的 USB 设备。
   例如，`ALLOW: vid=047F pid= C039 split=01 intf=00,03` - 允许 00 和 03 接口，限制其他接口。
6. 单击应用和确定。

在桌面会话中，拆分的 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。



> 注意：
>
> 拆分复合 USB 设备以进行通用 USB 重定向时，必须从 Desktop Viewer 或连接中心选择该设备以重定向设备。

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

拆分	接口	操作
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：*MyPlantronics* 耳机

接口号：

- 音频接口类 -0
- HID 接口类-3

用于 *MyPlantronics* 耳机的示例规则：

- 允　　许：`vid=047F pid= C039 split=01 intf=00,03 /Allowed 00 and 03 interface, restrict others`
- DENY: `vid=047F pid= C039 split=01 intf=00,03 / deny 00 and 03`

限制：

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

DPI 缩放

Citrix Workspace 应用程序允许操作系统控制会话分辨率。

可以在会话中应用高 DPI，但此功能默认处于禁用状态。这表示会话缩放将遵从操作系统的分辨率。

可以使用以下选项配置 DPI 缩放：

1. 组策略对象 (GPO) 管理模板（每计算机配置）
2. 高级首选项（每用户配置）

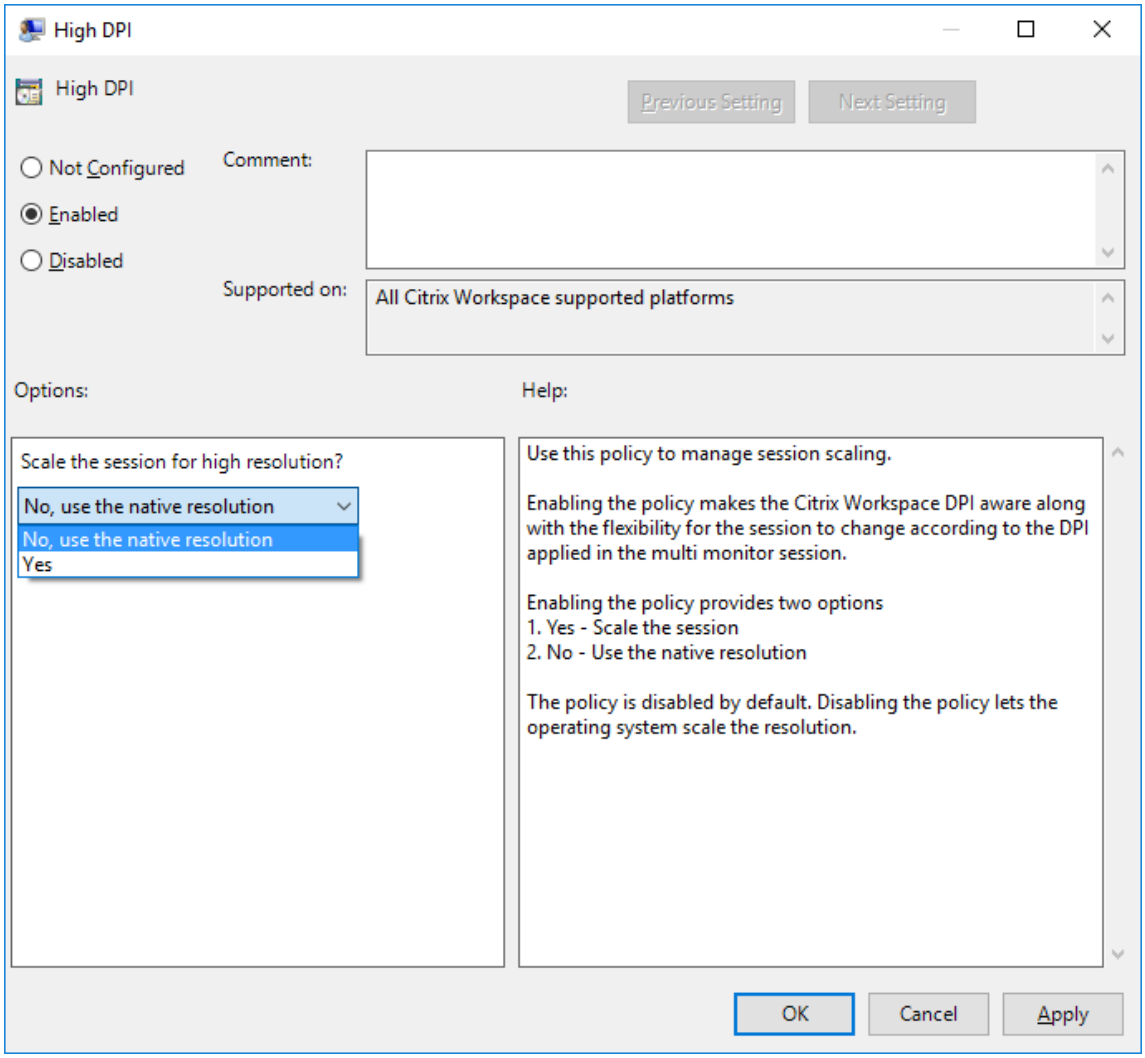
限制：

- 即使启用了此功能，也会在 Desktop Viewer 中观察到轻微模糊的情况。
- 在会话中，当您更改 DPI 设置并重新启动时，会话窗口的大小可能会不恰当。解决方法：调整会话窗口的大小。

要使用 **GPO** 管理模板配置 **DPI** 缩放，请执行以下缩放：

1. 通过运行 gpedit.msc 打开 Citrix Workspace 应用程序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 Workspace** > **DPI**

3. 选择高 **DPI** 策略。



4. 选择以下选项之一：

   a) 是 - 指示在会话中应用高 DPI。
   b) 否，使用本机分辨率 - 表示由操作系统设置分辨率。

5. 单击应用和确定。
6. 在命令行中，运行 `gpupdate /force` 命令以应用所做的更改。

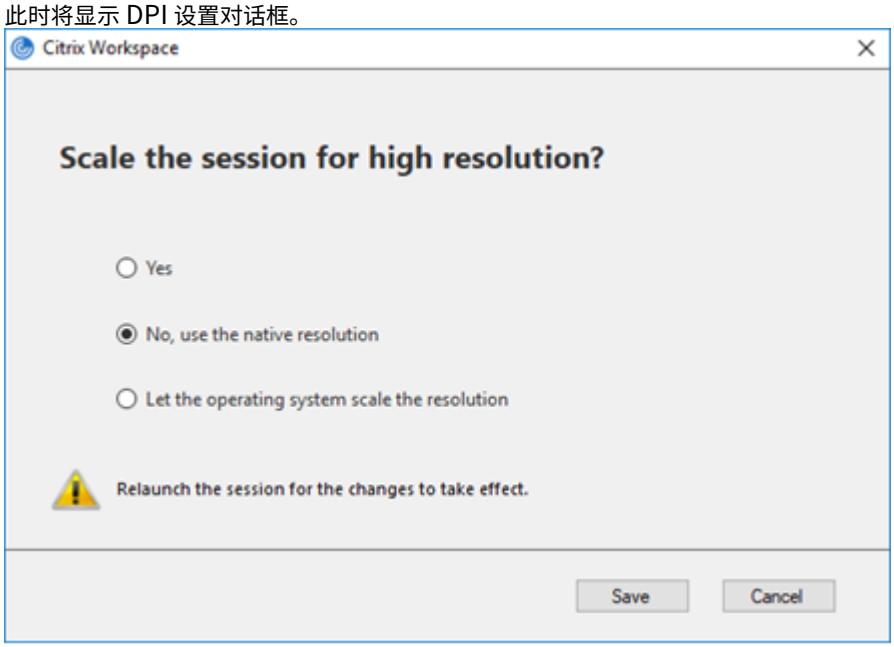
使用图形用户界面配置 **DPI** 缩放：

> 注意：
>
> 可以隐藏通知区域中的适用于 Windows 的 Citrix Workspace 应用程序图标中提供的全部或部分“高级首选项”表。有关详细信息，请参阅“高级首选项”表。

1. 右键单击通知区域中的 Citrix Workspace 应用程序图标。

2. 选择高级首选项并单击 **DPI** 设置。

   此时将显示 DPI 设置对话框。



3. 选择以下选项之一：

   a) 是 - 指示在会话中应用高 DPI。
   b) 否，使用本机分辨率 - 指示 Citrix Workspace 应用程序检测 VDA 上的 DPI 并进行应用。
   c) 允许操作系统缩放分辨率 - 默认情况下，此选项处于选中状态。这样，由 Windows 处理 DPI 缩放。此选项还意味着“将高 DPI”策略设置为“禁用”。

4. 单击保存。
5. 重新启动 Citrix Workspace 应用程序会话以使所做的更改生效。

DPI 缩放选项

Citrix Workspace 应用程序中存在三个可能的 DPI 缩放设置 - 缩放、不缩放和操作系统缩放。不同设置的用例如下所示。

缩放：

缩放设置在 VDA 上缩放分辨率的方式与操作系统缩放类似，但是此设置支持混合 DPI 场景。此设置对应于 UI 设置“Yes”（是）或 GPO 策略中设置为“已启用”的“高 DPI”策略。当连接到新式 VDA 时，此设置也适用于混合 DPI 场景。这是缩放无缝会话的唯一方式。缩放可能会导致图像模糊，尤其是文本。连接到旧版 VDA（6.5，或配置为使用旧版图形）时，性能可能较差。本地应用程序访问、RTOP 以及使用屏幕定位的其他插件不支持缩放。根据设计，无缝应用程序将在此模式下在显示器之间跳转，以保持正确的缩放。
建议连接到新式 VDA 的 Windows 10 上的用户使用此设置。该设置支持混合 DPI，且不会对服务器资源产生任何其他影响。

不缩放：

不缩放设置将在会话中发送所有显示器的完整分辨率。这些分辨率未经过缩放，可能会导致应用程序和桌面中的文本和图标看起来较小。此设置对应于 UI 设置“No”（否）和 GPO 中设置为“已启用”的“高 DPI”策略。此设置不会导致由于缩放而出现模糊的情况，但可能会导致文本和图标看起来较小。连接到桌面会话时，可以在 VDA 中设置 DPI，以实现所需的缩放。此操作在 RDS 桌面或无缝应用程序上无法执行。启用此设置会导致会话具有更高的分辨率，从而可能影响服务器性能和可扩展性。
对于需要最佳图像质量且接受其他服务器资源的桌面会话，建议使用此设置。也可以在用户不介意文本和图标较小的情况下使用。

操作系统缩放：

操作系统缩放是默认设置，并且对应于 UI 设置“Let the operating system scale the resolution”（允许操作系统缩放分辨率）。在这种情况下，“高 DPI”策略将设置为“已禁用”。这样，Windows 操作系统就可以处理会话的 DPI 缩放。VDA 的分辨率是基于 DPI 进行缩放的，因此会导致分辨率比客户端设备的分辨率更小。此设置非常适用于单显示器会话，并且在连接到 6.5 VDA 或配置为使用旧版图形的 VDA 时很有效。此方法不支持混合 DPI - 所有显示器都必须具有相同的 DPI，否则会话不起作用。缩放可能会导致图像模糊，尤其是文本。在 Windows 10 操作系统中，光标大小也可能出现问题。
对于 Windows 7 端点上的用户或连接到旧版 VDA 的用户，建议使用此设置。如果没有混合 DPI，也可以在 Windows 10 上使用此设置。

虚拟显示布局

此功能允许您定义适用于远程桌面的虚拟显示器布局，并在远程桌面上将单个客户端显示器几乎拆分为多达八个显示器。可以在 Desktop Viewer 中的显示器布局选项卡中配置虚拟显示器。在虚拟显示器中，您可以绘制水平线或垂直线以将屏幕分隔为多个虚拟显示器。根据客户端显示器分辨率的指定百分比来分隔屏幕。

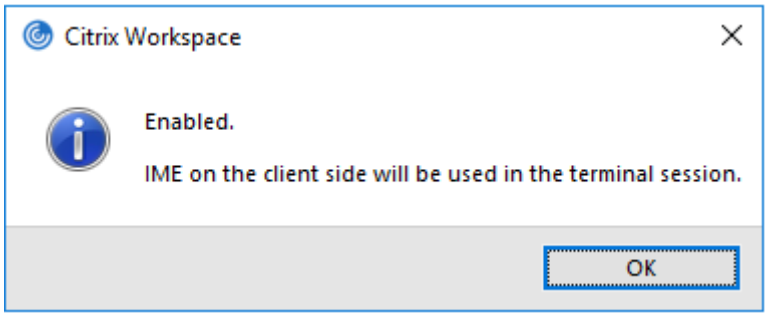
您可以为将用于 DPI 缩放或 DPI 匹配的虚拟显示器设置 DPI。应用虚拟显示器布局后，请调整其大小或重新连接会话。

此配置仅适用于全屏会话、单显示器桌面会话，并且不影响任何已发布的应用程序。此配置适用于与此客户端进行的所有后续连接。

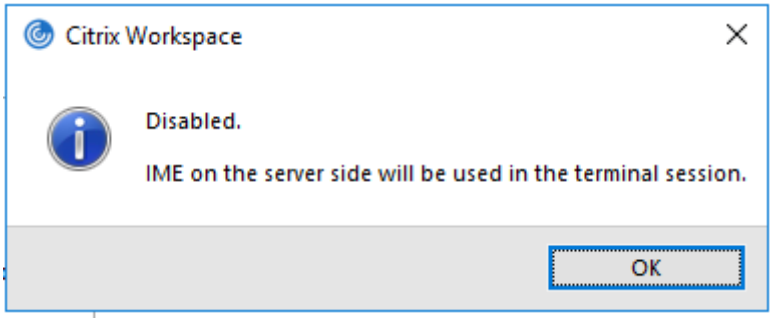
通用客户端输入法编辑器 (IME)

使用命令行界面配置通用客户端 **IME**：

- 要启用通用客户端 IME，请从 Citrix Workspace 应用程序安装文件夹 `C:\Program Files (x86)\Citrix\ICA Client` 运行 `wfica32.exe /localime:on` 命令。

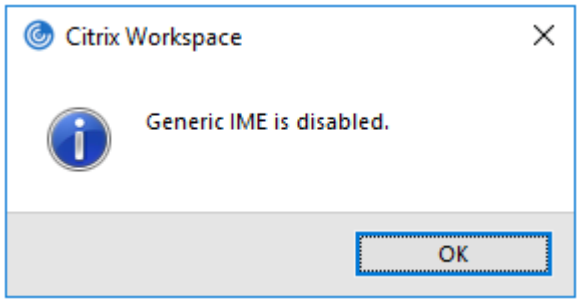


- 要禁用通用客户端 IME，请从 Citrix Workspace 应用程序安装文件夹 `C:\Program Files (x86)\Citrix\ICA Client` 运行 `wfica32.exe /localime:off` 命令。

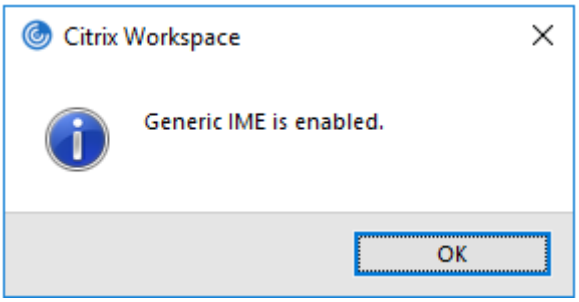


> 注意：
>
> 可以使用命令行开关 `wfica32.exe /localime:on` 启用通用客户端 IME 和键盘布局同步。

- 要禁用通用客户端 IME，请从 Citrix Workspace 应用程序安装文件夹 `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 Workspace 应用程序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。

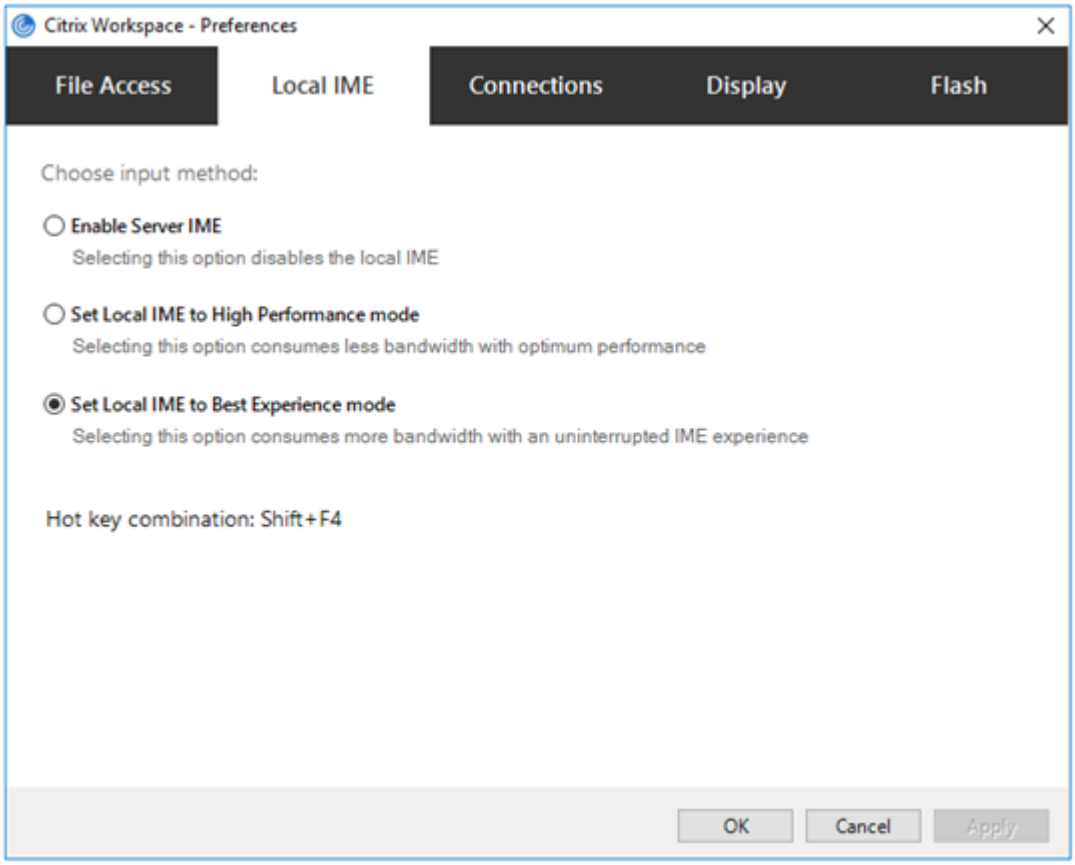
使用图形用户界面配置通用客户端 **IME**：

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 Workspace 应用程序允许您配置不同的选项以使用通用客户端 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 Workspace 应用程序图标并选择连接中心。
2. 选择首选项和本地 **IME**。



下面的选项可用来支持不同的 IME 模式：

1. 启用服务器 **IME** - 禁用本地 IME 且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 - 在带宽受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 - 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。

对设置进行的更改仅应用于当前会话。

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。

限制：

- 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。
- 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。

H.265 视频编码

Citrix Workspace 应用程序支持使用 H.265 视频编解码器进行远程图形和视频的硬件加速。要从此功能受益，必须在 VDA 和 Citrix Workspace 应用程序上支持并启用此功能。如果端点上的 GPU 不支持使用 DXVA 接口进行 H.265 解码，“图形的 H265 解码”策略设置将被忽略，会话将回退到使用 H.264 视频编解码器。

必备条件：

1. VDA 7.16 及更高版本。
2. 在 VDA 上启用针对 **3D** 图形工作负载优化策略。
3. 在 VDA 上启用使用视频编解码器的硬件编码策略。

> 注意：
>
> 仅 NVIDIA GPU 支持 H.265 编码。

在适用于 Windows 的 Citrix Workspace 应用程序中，此功能默认设置为已禁用。

使用 **Citrix** 组策略对象 **(GPO)** 管理模板将 **Citrix Workspace** 应用程序配置为使用 **H.265** 视频编码：

1. 通过运行 gpedit.msc 打开 Citrix Workspace 应用程序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 Workspace** > 用户体验。
3. 选择图形的 **H265** 解码策略。
4. 选择已启用。
5. 单击应用和确定。

使用注册表编辑器配置 **H.265** 视频编码：

在 **32** 位操作系统上未加入域的网络中启用 **H.265** 视频编码：

1. 在“运行”命令中使用 regedit 启动注册表编辑器。
2. 导 航 到 HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Graphics Engine。
3. 创建一个名为 **EnableH265** 的 DWORD 项并将该项的值设置为 1。

在 **64** 位操作系统上未加入域的网络中启用 **H.265** 视频编码：

1. 在“运行”命令中使用 regedit 启动注册表编辑器。
2. 导 航 到 HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Policies\Citrix\ICA Client\Graphics Engine。
3. 创建一个名为 EnableH265 的 DWORD 项并将该项的值设置为 1。

重新启动会话以使更改生效。

> 注意：
>
> - 如果在适用于 Windows 的 Citrix Workspace 应用程序组策略对象管理模板中禁用了图形硬件加速策略，图形的 **H265** 解码策略设置将被忽略，并且该功能不起作用。
> - 运行 HDX Monitor 3.x 工具以确定是否在会话中启用了 H.265 视频编码器。有关 HDX Monitor 3.x 工具的详细信息，请参阅知识中心文章 CTX135817。

键盘布局和语言栏

键盘布局

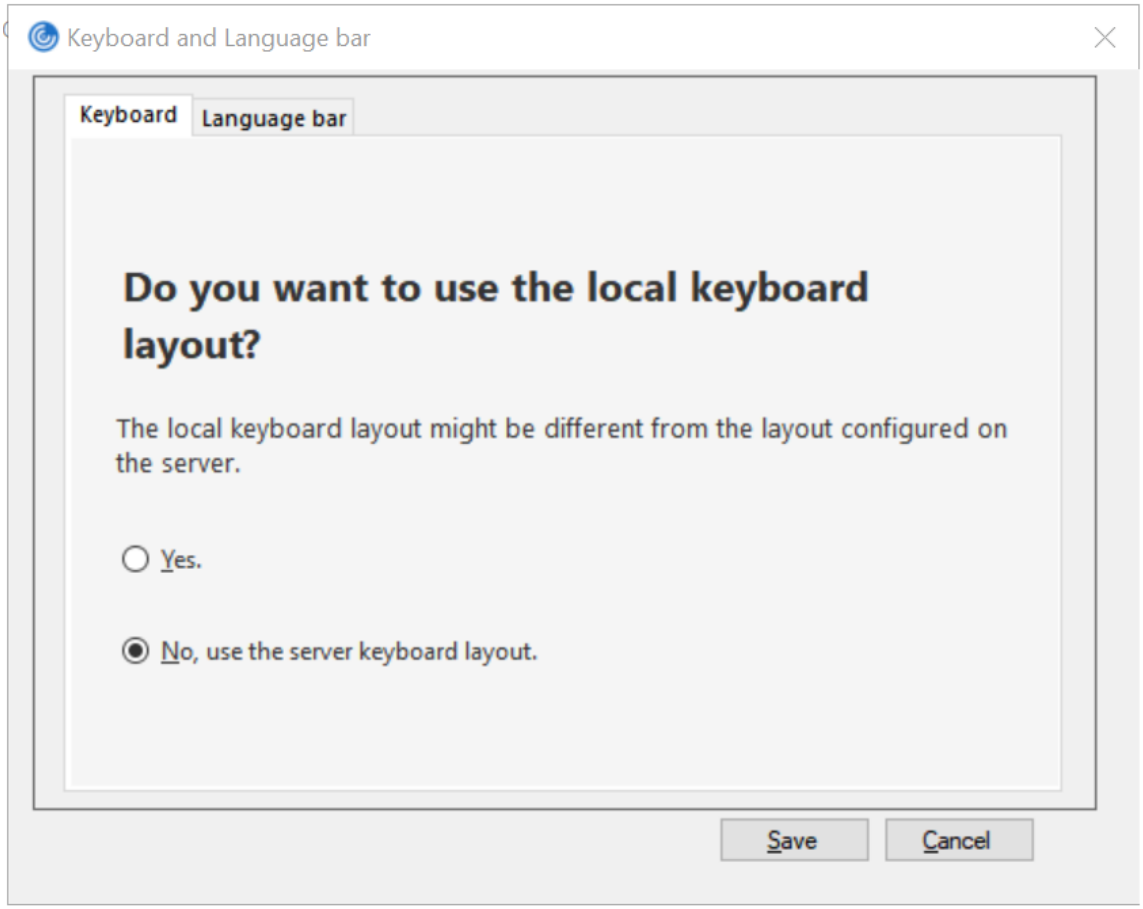
> 注意：
>
> 可以隐藏通知区域中的 Citrix Workspace 应用程序图标中提供的全部或部分“高级首选项”表。有关详细信息，请参阅“高级首选项”表。

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. 从通知区域图标中的 Citrix Workspace 应用程序图标，选择高级首选项 > 键盘和语言栏。

   此时将显示键盘和语言栏对话框。



2. 选择以下选项之一：
   - 是 - 指示在会话中使用本地键盘布局。
   - 否，使用服务器键盘 - 指示在会话中应用在 VDA 上使用的键盘布局。此选项可将本地键盘布局功能设置为禁用。
3. 单击保存。

您还可以启用和禁用键盘布局同步，方法是使用命令行从适用于 Windows 的 Citrix Workspace 应用程序安装文件夹 `C:\Program files (x86)\Citrix\ICA Client` 运行 `wfica32:exe /localime:on` 或 `wfica32:exe /localime:off`。

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` 来禁用本地键盘布局选项。用户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 Workspace 应用程序注销并重新登录。

隐藏键盘布局切换通知对话框：

通过键盘布局更改通知对话框，您可以了解会话是否正在切换键盘布局。键盘布局切换大约需要两秒钟才能完成。隐藏

通知对话框后，需要等待一段时间才能开始键入内容以避免出现不正确的字符输入。

> 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。

使用注册表编辑器隐藏键盘布局切换通知对话框：

1. 启动注册表编辑器并导航到 `HKEY_LOCAL_MACHINE\Software\Citrix\IcaIme`。
2. 按名称 **HideNotificationWindow** 创建一个字符串值注册表项。
3. 将 DWORD 值设置为 **1**。
4. 单击确定。
5. 重新启动会话以使更改生效。

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。解决方法：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，请注销并重新登录会话。
- 在 RDP 会话中，无法使用 Alt + Shift 快捷方式更改键盘布局。解决方法：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 `HKEY_LOCAL_MACHINE\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。

语言栏

语言栏显示会话中的首选输入语言。在早期版本中，只能使用 VDA 上的注册表项更改此设置。自 Citrix Receiver for Windows 4.11 起，可以使用高级首选项对话框更改设置。默认情况下，语言栏在会话中显示。

> 注意：
>
> 此功能在 VDA 7.17 及更高版本上运行的会话中可用。

配置显示或隐藏远程语言栏：

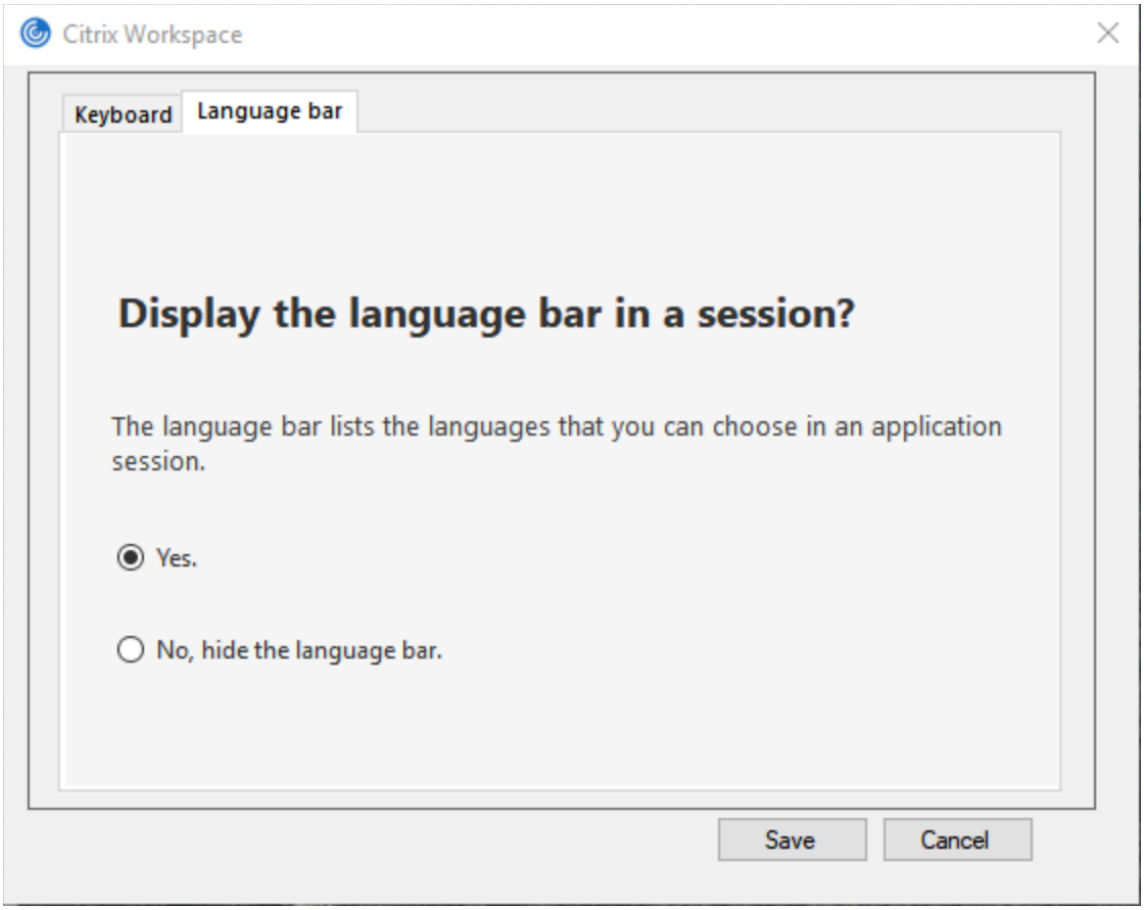
1. 右键单击通知区域中的 Citrix Workspace 应用程序图标并选择高级首选项。
2. 选择键盘和语言栏。
3. 选择语言栏选项卡。
4. 选择以下选项之一：

    a) 是 - 指示在会话中显示语言栏。

b) 否，隐藏语言栏 - 指示在会话中隐藏语言栏。

5. 单击保存。

设置更改将立即生效。



> 注意：
>
> - 可以在活动会话中更改设置。
> - 如果仅存在一种输入语言，远程语言栏将不在会话中显示。

在“高级首选项”表中隐藏语言栏选项卡：

可以使用注册表项在高级首选项表中隐藏语言栏选项卡。

1. 启动注册表编辑器。
2. 导航到`HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\LocalIME`。
3. 创建一个 DWORD 值键 **ToggleOffLanguageBarFeature**，并将其设置为 **1** 以在“高级首选项”表中隐藏“语言栏”选项。

USB 支持

USB 支持允许您在连接到 Citrix Virtual Apps and Desktops 和 Citrix DaaS 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是否可以在 Citrix Virtual Apps and Desktops 和 Citrix DaaS 上使用 USB 设备。

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。

虚拟应用程序和桌面会话直接支持以下类型的设备，因此不使用 USB 支持：

- 键盘
- 鼠标
- 智能卡

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，不支持某些类型的 USB 设备通过 Citrix Virtual Apps and Desktops 和 Citrix DaaS 进行远程连接。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，不支持在虚拟应用程序和桌面会话中使用以下类型的 USB 设备：

- 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 Citrix Virtual Apps 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

USB 支持的工作方式：

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聚焦的虚拟桌面。

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，您可以通过适用于 Windows 的 Citrix Workspace 应用程序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
默认已启用	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** 设备类别：

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，但其中某些类只有在进行额外配置后才能在虚拟应用程序和桌面会话中用于进行远程连接。这些类如下所示。

- 音频（类别 **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受 XenDesktop 4 或更高版本支持的常时等量传输。音频（类 01）不适用于 Citrix Virtual Apps，因为这些设备在 Citrix Virtual Apps 中不可使用 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（类别 **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，并且包括力量反馈式操纵杆、运动平台和力量反馈式内骨骼。
- 静态图像（类别 **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（类别 **07**）- 虽然某些打印机使用供应商特定协议（类别 ff），但是大多数打印机通常仍包含在此类别中。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（类别 **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 Citrix Virtual Apps，因为这些设备在 Citrix Virtual Apps 中不可使用 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。

- 内容安全性（类别 **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（类别 **0e**）- 视频类别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。

> 重要
>
> 大多数视频流设备使用受 XenDesktop 4 或更高版本支持的常时等量传输。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（类别 **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。

- 应用程序和供应商特定（类别 **fe** 和 **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（类别 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。
- 其他网络设备（类别 **ef**，子类 **04**）- 其中一些设备可能提供关键网络访问。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

可以通过编辑适用于 Windows 的 Citrix Workspace 应用程序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适用于 Windows 的 Citrix Workspace 进行更改。该文件位于以下已安装的文件夹中：

```
\C:\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=
```

> 重要
>
> 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 USB 设备策略设置的详细信息，请参阅 Citrix Virtual Apps and Desktops 文档中的 USB 设备策略设置。

配置 **USB** 音频

> 注意：
>
> - 首次升级或安装适用于 Windows 的 Citrix Workspace 应用程序时，必须向本地 GPO 中添加最新的模板文件。有关向本地 GPO 中添加模板文件的详细信息，请参阅组策略对象管理模板。如果进行升级，导出最新文件的过程中将保留现有设置。
> - 此功能仅在 Citrix Virtual Apps 服务器上可用。

要配置 **USB** 音频设备，请执行以下操作：

1. 通过运行 gpedit.msc 打开 Citrix Workspace 应用程序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 Workspace >** 用户体验，然后选择通过通用 **USB** 重定向传输音频。
3. 编辑设置。
4. 单击应用和确定。
5. 以管理员模式打开 cmd 提示符。
6. 运行以下命令
   `gpupdate /force`。

vPrefer 启动

在早期版本中，可以通过在 **Citrix Studio** 中设置 KEYWORDS:prefer=" application"属性来指定 VDA 上安装的应用程序的实例（在本文档中称为"本地实例"）必须优先于已发布的应用程序启动。

自版本 4.11 起，在双跃点场景中（Citrix Workspace 应用程序在托管您的会话的 VDA 中运行），您现在可以控制 Citrix Workspace 应用程序是否先启动 VDA 上安装的应用程序的本地实例（如果作为本地应用程序提供），然后再启动该应用程序的托管实例。

vPrefer 在 StoreFront 3.14 和 Citrix Virtual Desktops 7.17 及更高版本中可用。

启动应用程序时，Citrix Workspace 应用程序将读取 StoreFront 服务器上存在的资源数据并在枚举时根据 **vprefer** 标志应用设置。Citrix Workspace 应用程序在 VDA 上的 Windows 注册表中搜索应用程序的安装路径，如果存在，则启动该应用程序的本地实例。否则，将启动该应用程序的托管实例。
如果您启动的应用程序未安装在 VDA 上，则会启动托管应用程序。有关本地启动在 StoreFront 上的处理方式的详细信息，请参阅 Citrix Virtual Apps and Desktops 文档中的控制已发布的桌面上的本地应用程序启动。

如果不希望在 VDA 上启动应用程序的本地实例，请在 Delivery Controller 上使用 PowerShell 将 **LocalLaunchDisabled** 设置为 **True**。有关详细信息，请参阅 Citrix Virtual Apps and Desktops 文档。

此功能有助于更加快速地启动应用程序，从而提供更加优异的用户体验。可以使用组策略对象 (GPO) 管理模板对其进行配置。默认情况下，vPrefer 仅在双跃点场景中处于启用状态。

> 注意：
>
> 首次升级或安装 Citrix Workspace 应用程序时，必须向本地 GPO 中添加最新的模板文件。有关向本地 GPO 中添加模板文件的详细信息，请参阅组策略对象管理模板。如果进行升级，导出最新文件的过程中将保留现有设置。

1. 通过运行 gpedit.msc 打开 Citrix Workspace 应用程序 GPO 管理模板。
2. 在计算机配置节点下，转至管理模板 > **Citrix** 组件 > **Citrix Workspace** > 自助服务。
3. 选择 **vPrefer** 策略。
4. 选择已启用，然后从允许应用程序下拉菜单中，选择以下选项之一：
    - 允许所有应用程序：此选项将启动 VDA 上的所有应用程序的本地实例。Citrix Workspace 应用程序将搜索已安装的应用程序（包括记事本、计算器、写字板、命令提示窗口等本机 Windows 应用程序），并启动 VDA 上的应用程序，而非启动托管应用程序。
    - 允许已安装的应用程序：此选项将启动 VDA 上已安装的应用程序的本地实例。如果应用程序未安装在 VDA 上，则将启动托管应用程序。默认情况下，当 **vPrefer** 策略设置为已启用时，允许已安装的应用程序将处于选中状态。此选项将记事本、计算器等本机 Windows 操作系统应用程序排除在外。
    - 允许网络应用程序：此选项将启动在共享网络中发布的应用程序的实例。
5. 单击应用和确定。
6. 重新启动会话以使更改生效。

限制：

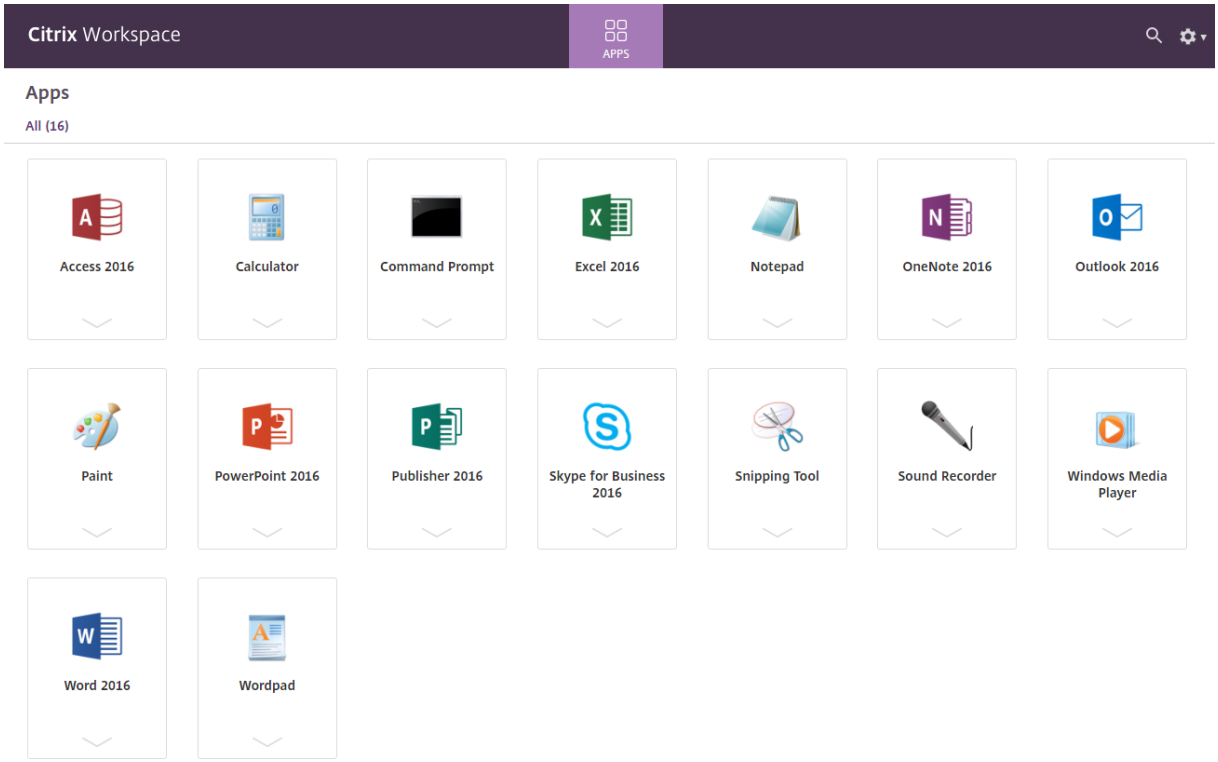
- 适用于 Web 的 Workspace 不支持此功能。

Workspace 配置

适用于 Windows 的 Citrix Workspace 应用程序支持为可能使用 Citrix Cloud 中提供的一项或多项服务的订阅者配置 Workspace。

Citrix Workspace 应用程序将智能地仅显示用户获得授权的特定工作区资源。您在 Citrix Workspace 应用程序中的所有数字工作区资源均由 Citrix Cloud Workspace 体验服务提供技术支持。

工作区属于数字工作区解决方案的一部分，通过该解决方案，IT 能够安全地提供从任何设备访问应用程序的功能。
此屏幕截图是工作区体验在您的订阅者看来是什么样子的一个示例。此界面不断变化，并且对现今的订阅者而言，所使用的界面看上去会有所差别。例如，此界面可能会在页面顶部显示“StoreFront”来代替“Workspace”。



SaaS 应用程序

对 SaaS 应用程序的安全访问提供了向用户交付已发布的 SaaS 应用程序的统一用户体验。SaaS 应用程序与单点登录一起提供。管理员现在可以通过过滤对特定 Web 站点和 Web 站点类别的访问，保护组织的网络和最终用户设备以防御恶意软件和数据泄漏。

适用于 Windows 的 Citrix Workspace 应用程序支持通过访问控制服务使用 SaaS 应用程序。通过该服务，管理员可以提供有凝聚力的支持体验、集成单点登录以及内容检查。

从云交付 SaaS 应用程序具有以下优势：

- 配置简单 - 易于操作、更新和使用。
- 单点登录–使用单点登录轻松登录。
- 适用于不同应用程序的标准模板 - 可对常用应用程序进行基于模板的配置。

必备条件：

- SaaS 应用程序必须支持 SAML 2.0 身份验证，才能应用单点登录功能。
- 必须在访问控制服务中启用 **Enable enhanced security**（启用增强安全）选项，才能在呈现 SaaS 应用程序时使用 Citrix Enterprise Browser（以前称为 Citrix Workspace Browser）。如果未启用此选项，则在启动 SaaS 应用程序时使用客户端上设置的默认浏览器。

> 注意：
>
> Citrix Workspace 应用程序汇总了从本地环境和云环境发布的应用程序和桌面以提供一致的用户体验。

Citrix Workspace 应用程序包含嵌入式 Citrix Secure Browser 以用于启动 SaaS 应用程序。据其构建 Citrix Secure Browser 的 Chromium 嵌入式框架为版本 70。这将导致在访问安全的 SaaS 应用程序时拥有很好的用户体验。

> 注意：
>
> - 对于适用于 Web 的 Workspace，仅在客户端上设置的默认浏览器而不是 Citrix Secure Browser 中启动 SaaS 应用程序。
> - ICA 会话应用程序与安全 SaaS 应用程序之间的用户体验可能有所不同。

Citrix Secure Browser 支持工具栏、剪贴板、打印、下载及水印等操作。这些操作按访问控制服务中的策略配置中定义应用于 Citrix Workspace 应用程序中。

使用 **Citrix Secure Browser** 时可以执行的操作：

工具栏 - 在应用程序上启用了工具栏选项时，可以在启动的应用程序中查看“后退”、“前进”和“刷新”选项。此外，工具栏还显示包括剪贴板操作的省略号。

剪贴板 - 在应用程序上启用了剪贴板访问时，可以在启动的应用程序中使用工具栏中显示的“剪切”、“复制”和“粘贴”选项。禁用了该选项时，“剪切”、“复制”和“粘贴”选项将灰显。

打印 - 如果启用了打印选项，则可以在启动的应用程序中运行打印命令。禁用后，打印选项将不显示在启动的应用程序中。

导航 - 如果启用了导航选项，下一步图标和上一步图标将显示在启动的应用程序中的工具栏中。

下载 - 如果启用了下载选项，您可以从启动的应用程序下载文件。右键单击启动的应用程序并选择另存为。浏览到所需位置，然后单击下载。

> 注意：
>
> 下载文件时，不会显示进度条以指示下载状态。但下载会成功。

水印 - 启用了水印选项时，包含客户端计算机的用户名和 IP 地址的水印将显示在启动的应用程序中。水印是半透明的，无法编辑以显示任何其他信息。

使用 **GPO** 配置缓存：

当多个用户使用同一设备登录以访问安全 SaaS 应用程序时，缓存将传递给下一个用户，从而在用户之间共享浏览信息。

要解决此问题，Citrix Workspace 应用程序引入了新的组策略对象 (GPO) 管理策略。此策略将不允许在本地设备上存储浏览器缓存。

1. 通过运行 gpedit.msc 打开 Citrix Workspace 应用程序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 Workspace** > **Citrix Secure Browser**。
3. 选择缓存策略。

   注意：默认情况下，此策略设置为已启用。
4. 要将其禁用，请选择已禁用，然后单击应用和确定。
5. 重新启动 Citrix Workspace 应用程序以使所做的更改生效。

限制：

1. 如果启动启用了打印选项并禁用了下载的已发布应用程序，然后在启动的应用程序中执行打印命令，即使下载功能受到限制，您仍可能能够保存 PDF。解决方法：要严格禁用下载功能，请禁用打印选项。
2. 应用程序中嵌入的视频可能不起作用。

有关 Workspace 配置的详细信息，请参阅 Citrix Cloud 中的 Workspace 配置。

PDF 打印

必备条件：

- Citrix Workspace 应用程序 1808 或更高版本。
- Citrix Virtual Apps and Desktops 7 1808 或更高版本。
- 必须在您的计算机上至少安装一个 PDF 查看器。

要启用 **PDF** 打印，请执行以下操作：

1. 在 Delivery Controller 上，使用 Citrix Studio，在左侧窗格中选择策略节点。可以创建新策略，也可以编辑现有策略。
2. 将自动创建 **PDF** 通用打印机策略设置为已启用。

重新启动 Citrix Workspace 应用程序会话以使所做的更改生效。

限制：

- Microsoft Edge 浏览器不支持 PDF 查看和打印功能。

使用 **Windows Continuum** 的 **Windows 10** 中的扩展平板电脑模式

Windows Continuum 是 Windows 10 的一项功能，可以满足客户端设备的使用需要。适用于 Windows 的 Citrix Workspace 应用程序 4.10 及更高版本支持 Windows Continuum，包括动态更改模式。

对于启用了触控功能的设备，如果未连接键盘或鼠标，Windows 10 VDA 将以平板电脑模式启动。连接了键盘或/和鼠标时，它以桌面模式启动。在任何客户端设备上或在 Surface Pro 等二合一设备的屏幕上拆卸或连接键盘，即在平板电脑模式与桌面模式之间切换。有关详细信息，请参阅 Citrix Virtual Apps and Desktops 文档中的适用于触屏设备的平板电脑模式。

当您连接或重新连接到会话时，Windows 10 VDA 将检测启用了触控功能的客户端设备上是否存在键盘或鼠标。当您在会话过程中连接或分离键盘或鼠标时，也会进行检测。此功能在 VDA 上默认处于启用状态。要禁用此功能，请使用 Citrix Studio 修改平板电脑模式切换策略。

平板电脑模式提供了更适于触屏的用户界面：

- 稍大的按钮。
- 开始屏幕和您启动的所有应用程序都以全屏模式打开。
- 任务栏包含“返回”按钮。
- 从任务栏中删除了图标。

桌面模式提供传统的用户界面，您可以像在 PC 中使用键盘和鼠标一样进行交互。

> 注意：
>
> 适用于 Web 的 Workspace 不支持 Windows Continuum 功能。

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
>
> 此功能仅在已发布的桌面会话中使用。

如果使用注册表编辑器或 default.ica 文件配置该功能，则即使会话终止后，该设置仍可持久。

您可以使用注册表在每用户和每计算机基础上控制该功能的可用性，如下所示：

使用注册表编辑器配置相对鼠标

要配置该功能，请将以下注册表项设置为适用，然后重新启动会话，以使更改生效：

要使该功能在每会话基础上可用，请执行以下操作：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Lockdown
 Profiles\All Regions\Lockdown\Virtual Channels\RelativeMouse
```

要使该功能在每用户基础上可用，请执行以下操作：

```
HKEY_CURRENT_USER\Software\Policies\Citrix\ICA Client\Engine\Lockdown
 Profiles\All Regions\Lockdown\Virtual Channels\RelativeMouse
```

```
1 - Name: Mouse
2 - Type: REG_SZ
3 - Value: True
```


> 注意：
>
> - 在注册表编辑器中设置的值优先级高于 ICA 文件设置。
> - 在 HKEY_LOCAL_MACHINE and HKEY_CURRENT_USER 中设置的值必须相同。其中不同的值可能会导致出现冲突。

使用 **default.ica** 文件配置相对鼠标

1. 打开 default.ica 文件，该文件通常位于 `C:\inetpub\wwwroot\Citrix\<site name>\conf\default.ica`，其中 sitename 为在创建站点时为其指定的名称。对于 StoreFront 客户，default.ica 文件通常位于 `C:\inetpub\wwwroot\Citrix\<Storename>\App_Data\default.ica`，其中 storename 为创建应用商店时为其指定的名称。
2. 在 WFClient 部分中添加一个名为 RelativeMouse 的新注册表项，其值设置为与 JSON 对象相同的配置。
3. 根据需要设置值：
   - true —启用相对鼠标
   - false —禁用相对鼠标
4. 重新启动会话以使更改生效。

> 注意：
>
> 在注册表编辑器中设置的值优先级高于 ICA 文件设置。

从 **Desktop Viewer** 启用相对鼠标

1. 登录 Citrix Workspace 应用程序。
2. 启动已发布的桌面会话。
3. 从 Desktop Viewer 工具栏中，选择首选项。

   此时将显示“Citrix Workspace - 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。

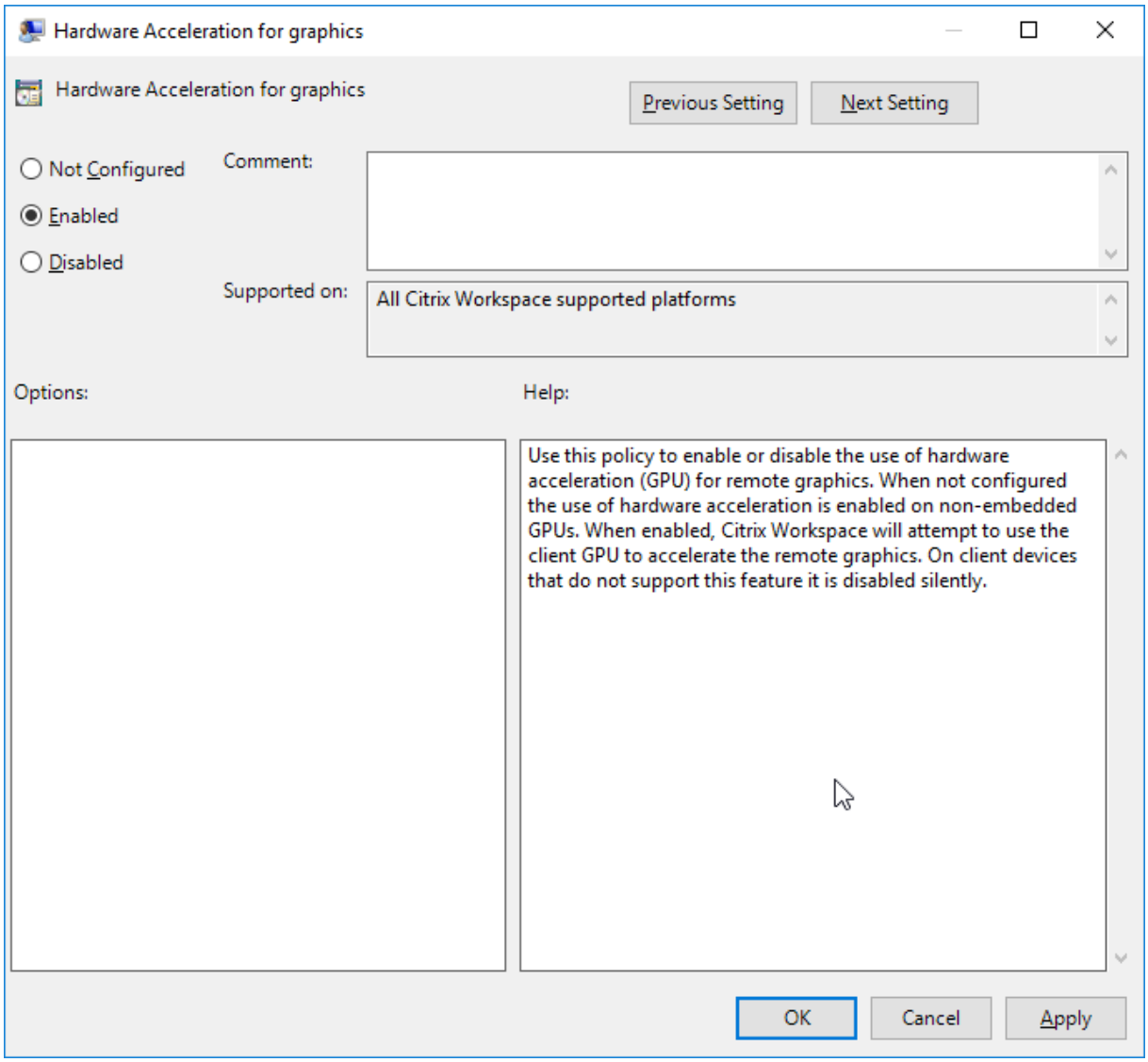
> 注意：
>
> 从 Desktop Viewer 配置相对鼠标仅将该功能应用于每会话。

硬件解码

使用 Citrix Workspace 应用程序（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 DirectX 视频加速。

要使用 **Citrix Workspace** 应用程序组策略对象管理模板启用硬件解码，请执行以下操作：

1. 通过运行 gpedit.msc 打开 Citrix Workspace 应用程序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 Workspace** > 用户体验。
3. 选择图形硬件加速。
4. 选择已启用，然后单击应用和确定。



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：HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\CEIP\Data\GfxRender。

> 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 Citrix Virtual Apps 服务器时，Citrix 建议您不要在用户的 Windows 设备上使用硬件解码。如果启用此功能，则会出现在突出显示文本时性能低下等问题以及屏幕闪烁问题。

麦克风输入

Citrix Workspace 应用程序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 Workspace 应用程序用户可以选择是否要通过使用连接中心来使用连接到其设备的麦克风。Citrix Virtual Apps and Desktops 和 Citrix DaaS 用户还可以使用 Citrix Virtual Apps and Desktops 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适用于 Windows 的 Citrix Workspace 应用程序结合使用。

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。

  Citrix Virtual Apps and Desktops 和 **Citrix DaaS**：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，然后单击最大化。

- 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。

Citrix Virtual Apps and Desktops 和 **Citrix DaaS**：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。如果虚拟应用程序和桌面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。
- 操作系统必须能够检测到每个显示器。在 Windows 平台上，要验证是否发生了此检测，请转到设置 > 系统并单击显示，然后确认每个显示器是否单独显示。
- 检测到显示器之后：
  - **Citrix Virtual Desktops**：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。
  - **Citrix Virtual Apps**：根据您安装的 Citrix Virtual Apps 服务器版本：
    - 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 Citrix Virtual Apps 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。

在双监视器上使用 **Citrix Virtual Desktops**：

1. 选择 Desktop Viewer 并单击下箭头。
2. 选择窗口。
3. 在两个显示器之间拖动 Citrix Virtual Desktops 屏幕。确保每个显示器中大约显示一半屏幕。
4. 在 Citrix Virtual Desktop 工具栏中，选择全屏。

   屏幕现在将扩展到两个监视器。

有关为 Citrix Virtual Apps and Desktops 和 Citrix DaaS 计算会话图形内存要求的信息，请参阅知识中心文章 CTX115637。

打印机

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 Workspace 应用程序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 Workspace 应用程序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 x64 计算机上，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 Citrix Workspace 应用程序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. 通过运行 gpedit.msc 打开 Citrix Workspace 应用程序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 Workspace** > 用户体验。
3. 选择键盘快捷方式策略。
4. 选择已启用以及所需的选项。
5. 重新启动 Citrix Workspace 应用程序会话以使所做的更改生效。

支持 **32** 位彩色图标：

Citrix Workspace 应用程序支持 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。

要设置首选深度，可以在 HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Preferences 中添加一个名为 TWIDesiredIconColor 的字符串注册表项并将其设置为所需值。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。

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适用于 Windows 的 Citrix Workspace 应用程序。

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 Citrix Virtual Apps and Desktops 和 Citrix DaaS 连接来设置首选项和使用多个桌面。

> 注意：
>
> 使用 Citrix Workspace 应用程序可更改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 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，对虚拟应用程序和桌面会话）使用热键序列，但可以对已发布的应用程序（即，对 Citrix Virtual Apps 会话）使用热键序列。

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 Citrix Virtual Apps 发布的虚拟应用程序，并且您的组织具有单独的 Citrix Virtual Apps 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 Citrix Virtual Apps 管理员必须更改驱动器映射策略，以包含网络驱动器。

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。如果您希望状态指示器尽快消失，可以将 REG_DWORD 值设置为 4。

客户体验改善计划 (CEIP)

收集的数据	说明	我们用它来实现什么目的
配置和使用数据	Citrix 客户体验改善计划 (CEIP) 从适用于 Windows 的 Citrix Workspace 应用程序收集配置和使用数据，并自动将数据发送到 Citrix 和 Google Analytics。	此数据可帮助 Citrix 提高 Citrix Workspace 应用程序的质量、可靠性和性能。

其他信息

Citrix 将根据与 Citrix 签订的合同条款处理您的数据，并按照 Citrix Trust Center 提供的 Citrix Services Security Exhibit 中所指定的方式对其进行保护。

Citrix 还使用 Google Analytics 从 Citrix Workspace 应用程序收集某些数据作为 CEIP 的一部分。请查看 Google 如何处理为 Google Analytics 收集的数据。

可以通过以下方式关闭将 CEIP 数据发送到 Citrix 和 Google Analytics 的功能（下面第二个表中 * 指示的为 Google Analytics 收集的两个数据元素除外）：

1. 右键单击通知区域中的 Citrix Workspace 应用程序图标。
2. 选择高级首选项。
   此时将显示高级首选项对话框。
3. 选择数据收集。
4. 选择不，谢谢以禁用 CEIP 或者放弃参与。
5. 单击保存。

或者，您可以导航到以下注册表项并按建议设置值：

路径：`HKEY_LOCAL_MACHINE\ SOFTWARE\Citrix\ICA Client\CEIP`

注册表项：`Enable_CEIP`

值：`False`

> 注意：
>
> 一旦您在数据收集对话框中选择不，谢谢或将 `Enable_CEIP` 注册表项设置为 `False`，如果您希望禁用发送 Google Analytics 收集的最后两个 CEIP 数据元素（即操作系统版本和 Citrix Workspace 应用程序版本），请导航到以下注册表项并按建议设置值：

路径：`HKEY_LOCAL_MACHINE\ SOFTWARE\Citrix\ICA Client\CEIP`

注册表项：`DisableHeartbeat`

值：`True`

Citrix 收集的特定 CEIP 数据元素包括：

操作系统版本	Citrix Workspace 应用程序版本	已连接的外部设备	屏幕分辨率
Flash 版本	Desktop Lock 配置	已启用触控功能	身份验证配置
会话启动方法	图形配置	Desktop Viewer 配置	打印
连接错误	启动时间	Citrix Workspace 应用程序语言	VDA 信息
SSON 状态	安装程序状态	安装时间	连接协议
Internet Explorer 版本			

Google Analytics 收集的特定 CEIP 数据元素包括：

操作系统版本 *	Citrix Workspace 应用程序版本 *	身份验证配置	Citrix Workspace 应用程序语言
会话启动方法	连接错误	连接协议	VDA 信息
安装程序配置	安装程序状态	客户端键盘布局	应用商店配置
自动更新首选项	连接中心使用情况	App Protection 配置	

身份验证

October 31, 2023

确保 Citrix Workspace 应用程序与已发布的资源之间的连接安全，以最大限度地提高安全性。您可以配置以下类型的身份验证：

- 域直通
- 智能卡
- Kerberos 直通

域直通身份验证

单点登录功能允许您进行身份验证并使用虚拟应用程序和桌面，而不需要重新进行身份验证。

登录 Citrix Workspace 应用程序允许您的凭据和枚举的资源传递到 StoreFront。

在早期版本中，使用 Google Chrome、Microsoft Edge 或 Mozilla FireFox 时，即使未启用该功能，也可以启动单点登录会话。

自版本 1905 起，所有 Web 浏览器都要求您使用组策略对象管理模板配置单点登录。有关使用组策略对象管理模板配置单点登录的详细信息，请参阅使用 Citrix Gateway 配置单点登录。

您可以使用以下任意选项在进行全新安装或升级安装时配置单点登录：

- 命令行接口
- 图形用户界面 (GUI)

在全新安装过程中配置单点登录

在全新安装过程中配置单点登录：

1. 在 StoreFront 或 Web Interface 上进行配置。
2. 在 Delivery Controller 上配置 XML 信任服务。
3. 修改 Internet Explorer 设置。
4. 安装具有单点登录功能的 Citrix Workspace 应用程序。

在 **StoreFront** 或 **Web Interface** 上配置单点登录

可以使用管理控制台在 StoreFront 或 Web Interface 上配置单点登录，具体取决于 Citrix Virtual Apps and Desktops 部署的类型。

通过下表了解不同的用例及其各自的配置：

用例	配置详细信息	其他信息
在 StoreFront 或 Web Interface 上配置的 SSON	启动 Citrix Studio，然后转至应用商店 > 管理身份验证方法 > 启用域直通。	如果未配置单点登录，Citrix Workspace 应用程序会自动将身份验证方法从域直通切换为用户名和密码（如果可用）。
需要适用于 Web 的 Workspace 时	启动应用商店 > 适用于 **Web** 的 **Workspace** 站点 > 管理身份验证方法 > 启用域直通。	如果未配置单点登录，Citrix Workspace 应用程序会自动将身份验证方法从域直通切换为用户名和密码（如果可用）。
未配置 StoreFront 时	如果在 VDA 上配置了 Web Interface，请启动 XenApp Services 站点 > 身份验证方法 > 启用直通。	如果未配置单点登录，Citrix Workspace 应用程序会自动将身份验证方法从直通切换为显式（如果可用）。

通过 **Citrix Gateway** 配置单点登录

使用组策略对象管理模板对 Citrix Gateway 启用单点登录。

1. 通过运行 gpedit.msc 打开 Citrix Workspace 应用程序 GPO 管理模板。
2. 在计算机配置节点下，转至管理模板 > **Citrix** 组件 > **Citrix Workspace** > 用户身份验证。
3. 选择适用于 **Citrix Gateway** 的单点登录策略。
4. 选择已启用。
5. 单击应用和确定。
6. 重新启动 Citrix Workspace 应用程序以使所做的更改生效。

在 **Delivery Controller** 上配置 **XML** 信任服务

在 Citrix Virtual Apps and Desktops 和 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）上，以管理员身份在 Delivery Controller 上运行以下 PowerShell 命令：

```
asnp Citrix* Set-BrokerSite -TrustRequestsSentToTheXmlServicePort
$True
```

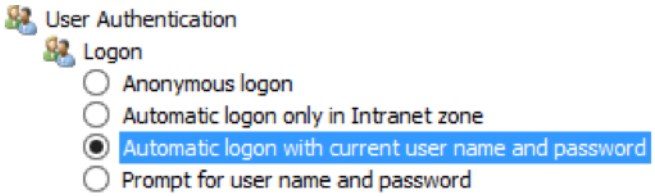
修改 **Internet Explorer** 设置

1. 使用 Internet Explorer 将 StoreFront 服务器添加到可信站点列表。为此，您需要：
    a) 从控制面板启动 **Internet** 选项。
    b) 单击安全 > 本地 **Internet**，然后单击站点。此时将显示本地 **Intranet** 窗口。

c) 选择高级。
d) 添加使用恰当的 HTTP 或 HTTPS 协议的 StoreFront 或 Web Interface FQDN 的 URL。
e) 单击应用和确定。

2. 在 **Internet Explorer** 中修改用户身份验证设置。为此，您需要：

a) 从控制面板启动 **Internet** 选项。
b) 单击安全选项卡 > 受信任的站点。
c) 单击自定义级别。此时将显示安全设置–受信任的站点区域窗口。
d) 在用户身份验证窗格中，选择使用当前用户名和密码自动登录。



a) 单击应用和确定。

使用命令行接口配置单点登录

使用 `/includeSSON` 开关安装适用于 Windows 的 Citrix Workspace 应用程序并重新启动 Citrix Workspace 应用程序以使所做的更改生效。

> 注意：
>
> 如果安装适用于 Windows 的 Citrix Workspace 应用程序时未安装单点登录组件，则不支持使用 `/includeSSON` 开关升级到最新版本的 Citrix Workspace 应用程序。

使用图形用户界面配置单点登录

1. 找到 Citrix Workspace 应用程序安装文件 (`CitrixWorkspaceApp.exe`)。
2. 双击 `CitrixWorkspaceApp.exe` 以启动安装程序。
3. 在启用单点登录安装向导中，选择启用单点登录选项。
4. 单击下一步，然后按照提示完成安装。

您现在无需提供用户凭据即可使用 Citrix Workspace 应用程序。

在适用于 **Web** 的 **Citrix Workspace** 中配置单点登录

可以使用组策略对象管理模板在适用于 Web 的 Workspace 上配置单点登录。

1. 通过运行 gpedit.msc 打开适用于 Web 的 Workspace GPO 管理模板。
2. 在计算机配置节点下，转至管理模板 > **Citrix** 组件 > **Citrix Workspace** > 用户身份验证。
3. 选择本地用户名密码策略并将其设置为已启用。
4. 单击启用直通身份验证。此选项允许适用于 Web 的 Workspace 使用您的登录凭据在远程服务器上进行身份验证。
5. 单击允许对所有 **ICA** 连接执行直通身份验证。此选项将跳过任何身份验证限制，并允许在所有连接上传递凭据。
6. 单击应用和确定。
7. 重新启动适用于 Web 的 Workspace 以使所做的更改生效。

通过启动任务管理器来验证是否已启用单点登录，并检查 `ssonsvr.exe` 进程是否正在运行。

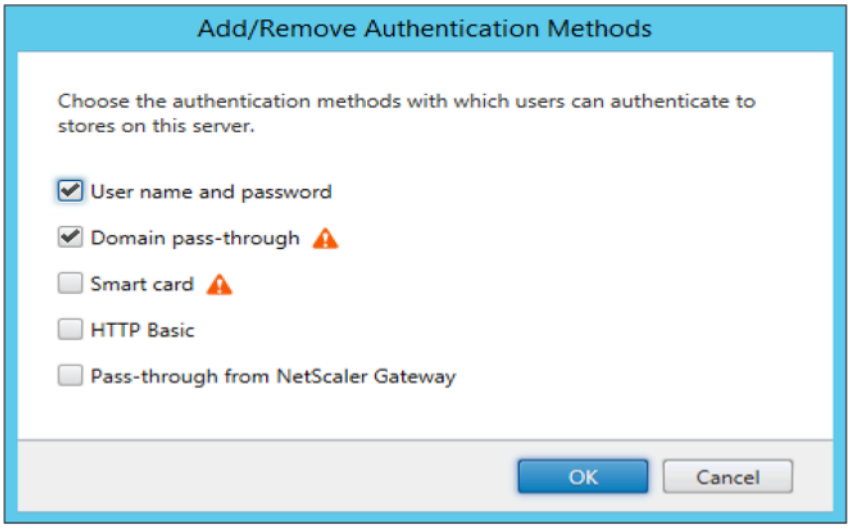
使用 **Active Directory** 配置单点登录

可以使用 Active Directory 配置单点登录身份验证。您不需要使用部署工具，例如此示例中的 Microsoft System Center Configuration Manager。

1. 下载 Citrix Workspace 应用程序安装文件 (CitrixWorkspaceApp.exe) 并将其放在合适的网络共享上。在其上安装了 Citrix Workspace 应用程序的目标计算机必须能够访问该安装文件。
2. 从适用于 Windows 的 Citrix Workspace 应用程序下载页面获取 `CheckAndDeployWorkspacePerMachineSt` `.bat` 模板。
3. 编辑 `CitrixWorkspaceApp.exe` 的位置和版本。
4. 在 **Active Directory** 组策略管理控制台中，键入 `CheckAndDeployWorkspacePerMachineStartupScrip` `.bat` 作为启动脚本。有关部署启动脚本的详细信息，请参阅 Active Directory 部分。
5. 在计算机配置节点中，转至管理模板 **>** 添加/删除模板以添加 `icaclient.adm` 文件。
6. 添加 `icaclient.adm` 模板后，转至计算机配置 > 管理模板 > **Citrix** 组件 > **Citrix Workspace** > 用户身份验证。
7. 选择本地用户名密码策略并将其设置为已启用。
8. 选择启用直通身份验证，然后单击应用。
9. 重新启动计算机以使更改生效。

在 **StoreFront** 和 **Web Interface** 上配置单点登录

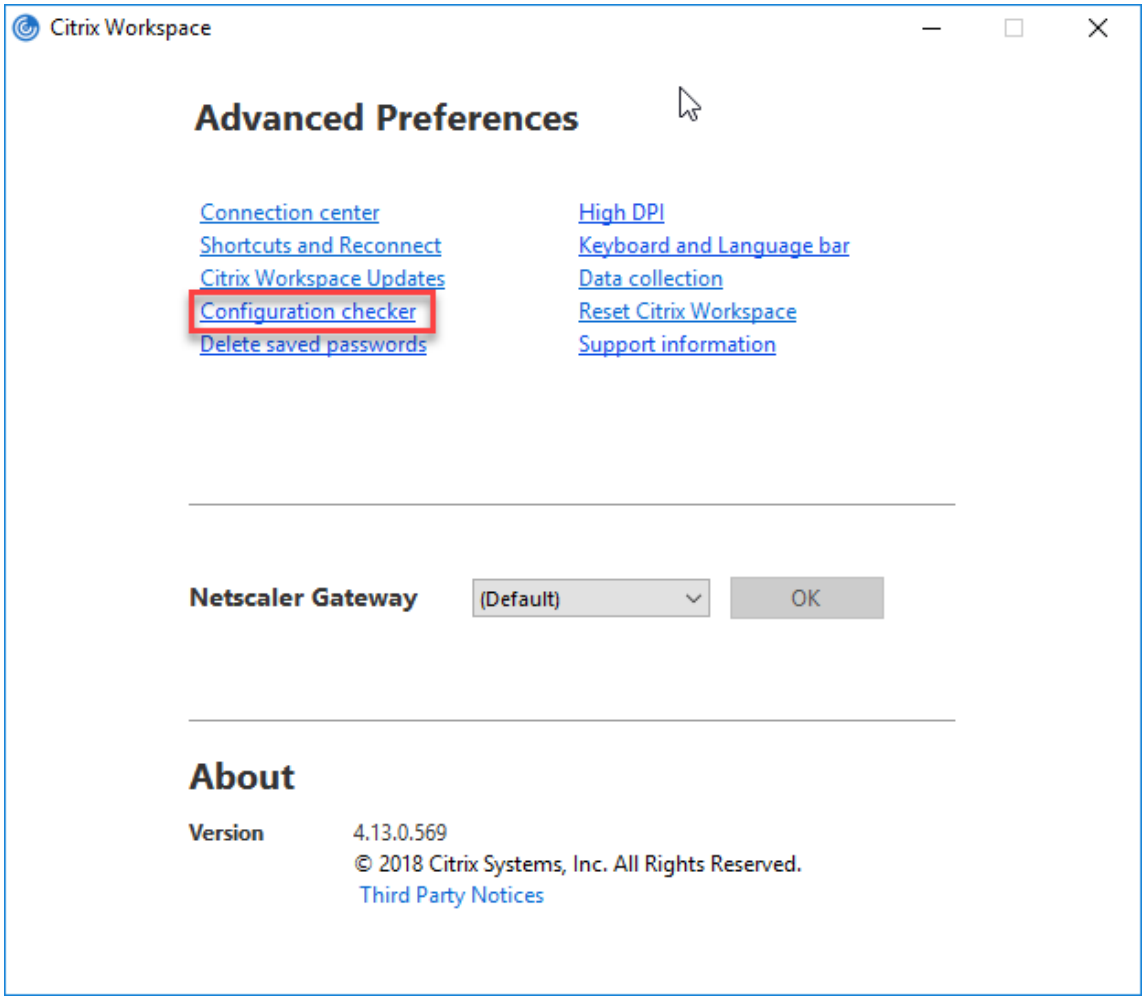
StoreFront 配置　在 StoreFront 服务器上打开 **Citrix Studio**，然后选择身份验证 **->** 添加/删除身份验证方法。选择域直通。



配置检查器

可以使用配置检查器运行测试，以确保单点登录正确配置。该测试在单点登录的不同检查点运行，并显示配置结果。

1. 右键单击通知区域中的 Citrix Workspace 应用程序图标，然后单击高级首选项。
   此时将显示高级首选项对话框。
2. 单击配置检查器。
   此时将显示 **Citrix** 配置检查器窗口。



3. 从选择窗格中选择 **SSONChecker**。
4. 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，为单点登录。
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。

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. 已随单点登录安装。
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. 单点登录进程正在运行。
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所做的更改生效，以及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：
>
> - 在适用于 Web 的 Workspace 配置中，这些测试结果不适用。
> - 在多应用商店设置中，身份验证方法测试在所有已配置的应用商店上运行。
> - 可以将测试结果保存为报告。默认报告格式为.txt。

隐藏“高级首选项”窗口中的“配置检查器”选项

1. 通过运行 gpedit.msc 打开 Citrix Workspace 应用程序组策略对象管理模板。
2. 转至 **Citrix** 组件 > **Citrix Workspace** > 自助服务 > **DisableConfigChecker**。
3. 单击已启用将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. 运行 `gpupdate /force` 命令。

限制：

配置检查器不包括 VDA 上“信任发送到 XML Service 的请求”配置的检查点。

信标测试　信标检查器是配置检查实用程序的一部分。它允许您执行信标测试，以帮助确认信标 (ping.citrix.com) 是否可访问。此测试可帮助消除资源枚举较慢（即信标不可用）的多个可能原因之一。要运行测试，请右键单击通知区域中的 Citrix Workspace 应用程序并选择高级首选项 > 配置检查器。从测试列表中选择 **Beacon checke**（信标检查器）并单击运行。

测试结果可能为以下任一情况：

- 可访问 - Citrix Workspace 应用程序能够成功联系信标。
- 不可访问 - Citrix Workspace 应用程序无法联系信标。
- 部分可访问 - Citrix Workspace 应用程序能够间歇性地联系信标。

通过 **Kerberos** 实现的域直通身份验证

本主题仅适用于在适用于 Windows 的 Citrix Workspace 应用程序与 StoreFront、Citrix Virtual Apps and Desktops 和 Citrix DaaS 之间建立的连接。

Citrix Workspace 应用程序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。

无需 Citrix Workspace 应用程序的密码即可进行 Kerberos 身份验证。因此，可以防止在用户设备上发生尝试获取密码访问权限的特洛伊木马攻击。用户可以使用任何身份验证方法登录并访问已发布的资源。例如，指纹读取器之类的生物特征身份验证器。

使用智能卡登录到配置了智能卡身份验证的 Citrix Workspace 应用程序、StoreFront、Citrix Virtual Apps and Desktops 和 Citrix DaaS 时，Citrix Workspace 应用程序将：

1. 在单点登录期间捕获智能卡 PIN。
2. 使用 IWA (Kerberos) 向 StoreFront 验证用户身份。然后，StoreFront 向您的 Citrix Workspace 应用程序提供有关可用 Citrix Virtual Apps and Desktops 和 Citrix DaaS 的信息。

   > 注意
   >
   > 应启用 Kerberos 以避免额外的 PIN 提示。如果未使用 Kerberos 身份验证，Citrix Workspace 应用程序将使用智能卡凭据向 StoreFront 进行身份验证。

3. HDX Engine 将智能卡 PIN 传递给 VDA，从而使用户登录到 Citrix Workspace 应用程序会话。Citrix Virtual Apps and Desktops 和 Citrix DaaS 随后提供请求的资源。

要将 Kerberos 身份验证用于 Citrix Workspace 应用程序，请确保您的 Kerberos 配置符合以下条件。

- Kerberos 只在 Citrix Workspace 应用程序与属于相同或可信 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。
- 必须在域和 Citrix Virtual Apps and Desktops 和 Citrix DaaS 上启用 Kerberos。为了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。

> 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。在编辑注册表之前，请务必进行备份。

通过 **Kerberos** 实现的域直通身份验证与智能卡结合使用

在继续操作之前，请参阅 Citrix Virtual Apps and Desktops 文档的保护部署部分中的智能卡信息。

安装适用于 Windows 的 Citrix Workspace 应用程序时，请包含以下命令行选项：

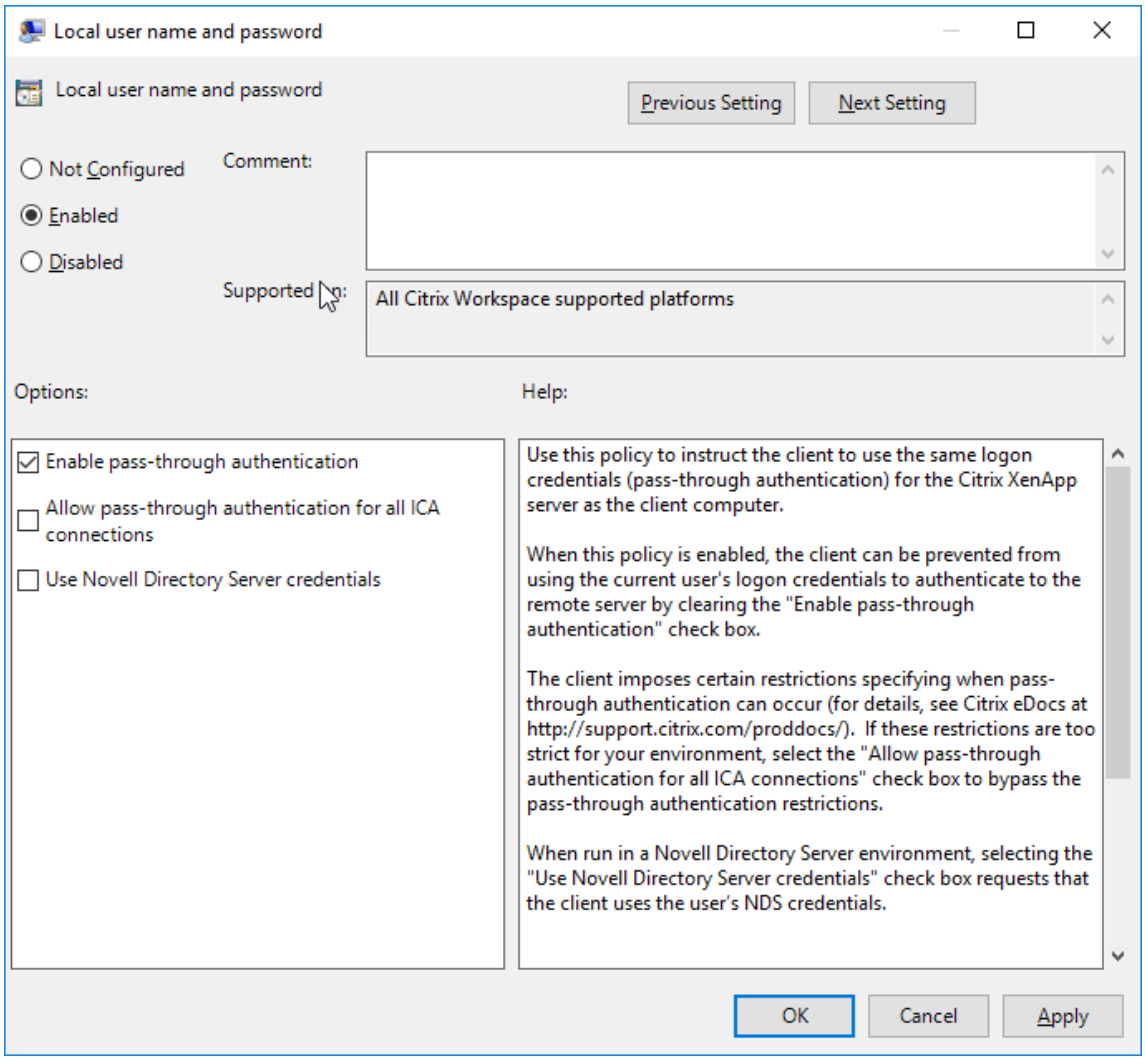
- /includeSSON

  此选项在加入域的计算机上安装 Single Sign-On 组件，从而使您的工作区能够使用 IWA (Kerberos) 向 StoreFront 进行身份验证。单点登录组件存储智能卡 PIN 码，HDX Engine 在将智能卡硬件和凭据远程传递到 Citrix Virtual Apps and Desktops 和 Citrix DaaS 时会使用此 PIN 码。Citrix Virtual Apps and Desktops 和 Citrix DaaS 自动从智能卡选择一个证书并从 HDX Engine 获得此 PIN。

  默认情况下启用一个相关选项 ENABLE_SSON。

如果安全策略阻止在设备上启用 Single Sign-On，请使用组策略对象管理模板配置 Citrix Workspace 应用程序。

1. 通过运行 gpedit.msc 打开 Citrix Workspace 应用程序组策略对象管理模板。
2. 选择管理模板 > **Citrix** 组件 > **Citrix Workspace** > 用户身份验证 > 本地用户名和密码
3. 选择启用直通身份验证。
4. 重新启动 Citrix Workspace 应用程序以使所做的更改生效。



配置 **StoreFront**：

在 StoreFront 服务器上配置身份验证服务时，选择域直通选项。该设置将启用集成 Windows 身份验证。无需选择智能卡选项，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。

智能卡

适用于 Windows 的 Citrix Workspace 应用程序支持以下智能卡身份验证：

- 直通身份验证 **(**单点登录**)** - 当用户登录 Citrix Workspace 应用程序时，直通身份验证可捕获智能卡凭据。Citrix Workspace 应用程序按以下方式使用捕获的凭据：
  - 使用智能卡凭据登录 Citrix Workspace 应用程序的已加入域的设备用户无需重新进行身份验证即可启动虚拟桌面和应用程序。
  - 在使用智能卡凭据的情况下，对于在未加入域的设备上运行的 Citrix Workspace 应用程序，用户必须再次键入其凭据才能启动桌面或应用程序。

  直通身份验证需要使用 StoreFront 和 Citrix Workspace 应用程序上的配置。
- 双模式身份验证 - 双模式身份验证允许用户在使用智能卡与键入用户名和密码之间进行选择。无法使用智能卡时，可使用此功能。例如，登录证书已过期。必须为每个站点设置专用应用商店才允许使用双模式身份验证，并将 **DisableCtrlAltDel** 方法设置为 **False** 以允许使用智能卡。双模式身份验证需要 StoreFront 配置。

  通过使用双模式身份验证，StoreFront 管理员可以允许用户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，方法是在 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。
- 客户端证书身份验证–客户端证书身份验证需要使用 Citrix Gateway 和 StoreFront 配置。
  - 要通过 Citrix Gateway 访问 StoreFront，在移除智能卡后您可能必须重新进行身份验证。
  - 当 Citrix 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 Citrix Workspace 应用程序和用户的虚拟桌面之间建立连接。支持双跳的部署在 Citrix Virtual Apps and Desktops 文档中进行了介绍。
- 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）允许用户对虚拟应用程序和桌面会话中的文档进行数字签名或加密。

限制：

- 证书必须存储在智能卡上，而非存储在用户设备上。
- Citrix Workspace 应用程序不保存用户证书选择信息，但在配置时存储 PIN。PIN 仅在非分页内存中缓存，不存储在磁盘中。
- 插入智能卡后，Citrix Workspace 应用程序不会重新连接会话。

- 针对智能卡身份验证进行配置后，Citrix Workspace 应用程序不支持虚拟专用网络 (VPN) 单点登录或会话预启动。要结合使用 VPN 与智能卡身份验证，请安装 Citrix Gateway 插件并通过 Web 页面登录，在每一步都使用智能卡和 PIN 进行身份验证。使用 Citrix Gateway 插件通过直通身份验证访问 StoreFront 不适用于智能卡用户。
- Citrix Workspace 应用程序 Updater 与 citrix.com 通信，且 Merchandising Server 与 Citrix Gateway 上的智能卡身份验证不兼容。

> 警告
>
> 某些配置需要编辑注册表。注册表编辑器使用不当可能导致问题，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。在编辑注册表之前，请务必进行备份。

要为智能卡身份验证启用单点登录，请执行以下操作：

要配置适用于 Windows 的 Citrix Workspace 应用程序，请在安装期间包含以下命令行选项：

- `ENABLE\\_SSON=Yes`

  单点登录是另一个用于直通身份验证的术语。启用此设置可阻止 Citrix Workspace 应用程序第二次显示 PIN 提示。

- 如果未安装 Single Sign-On 组件，请将 **SSONCheckEnabled** 设置为 false。此注册表项可阻止 Citrix Workspace 应用程序身份验证管理器查找 Single Sign-On 组件，因此允许 Citrix Workspace 应用程序向 StoreFront 进行身份验证。

  ```
  HKEY\\_CURRENT\\_USER\Software\Citrix\AuthManager\protocols\
  integratedwindows\
  ```

  ```
  HKEY\\_LOCAL\\_MACHINE\Software\Citrix\AuthManager\protocols\
  integratedwindows\
  ```

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适用于 Windows 的 Citrix Workspace 应用程序：

- `/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适用于 Windows 的 Citrix Workspace 应用程序身份验证方法（如用户名和密码）登录端点，则命令行如下：

  ```
  /includeSSON LOGON_CREDENTIAL_CAPTURE_ENABLE=No
  ```

这样可阻止在登录时捕获凭据，并允许在登录 Citrix Workspace 应用程序时 Citrix Workspace 应用程序存储 PIN。

1. 通过运行 gpedit.msc 打开 Citrix Workspace 应用程序组策略对象管理模板。
2. 转至管理模板 > **Citrix** 组件 > **Citrix Workspace** > 用户身份验证 > 本地用户名和密码。
3. 选择启用直通身份验证。根据配置和安全设置，选择允许对所有 **ICA** 执行直通身份验证选项以便能够使用直通身份验证。

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。

要使用户设备支持使用智能卡，请执行以下操作：

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

要更改证书的选择方式，请执行以下操作：

默认情况下，如果多个证书有效，则 Citrix Workspace 应用程序将提示用户从列表中选择证书。或者，可以将 Citrix Workspace 应用程序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 位、2048 位或 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 Workspace 应用程序命令行中，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 Workspace 应用程序将提示用户从中选择一个证书。

将以下注册表项值添加到注册表项 SmartCardDefault LatestExpiry }。
HKEY_CURRENT_USER 或
HKEY_LOCAL_MACHINE\Software[Wow6432Node]Citrix\AuthManager:
CertificateSelectionMode={
Prompt

-

在 HKEY_CURRENT_USER 中定义的值优先级高于 HKEY_LOCAL_MACHINE 中的值，可更好地帮助用户选择证书。

要使用 **CSP PIN** 提示，请执行以下操作：

默认情况下，向用户显示的 PIN 提示由适用于 Windows 的 Citrix Workspace 应用程序而不是智能卡加密服务提供程序 (CSP) 提供。Citrix Workspace 应用程序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（如不允许在每进程或每会话缓存 PIN），则可将 Citrix Workspace 应用程序配置为使用 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 Workspace 应用程序命令行中，指定选项 `AM\_SMARTCARDPINENTRY=CSP`。
- 将以下注册表项值添加到注册表项 HKEY_LOCAL_MACHINE\Software\[Wow6432Node\]Citrix\AuthManager: SmartCardPINEntry=CSP。

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：

- PNAgent 站点登录支持智能卡登录。
- PNAgent 站点上的智能卡移除策略已发生变化：

移除智能卡时注销 Citrix Virtual Apps 会话 - 如果在 PNAgent 站点上已将智能卡配置为身份验证方法，则必须在适用于 Windows 的 Citrix Workspace 应用程序上配置相应的策略以强制注销 Citrix Virtual Apps 会话。在 XenApp PNAgent 站点上为智能卡身份验证启用漫游，同时启用智能卡移除策略，这会从 Citrix Workspace 应用程序会话中注销 Citrix Virtual Apps。而用户在 Citrix Workspace 应用程序会话中仍然保持登录状态。

限制：

当使用智能卡身份验证登录 PNAgent 站点时，用户名显示为已登录。

安全通信

April 22, 2024

要确保 Citrix Virtual Apps and Desktops 服务器与 Citrix Workspace 应用程序之间的通信安全，可以使用以下安全技术集成 Citrix Workspace 应用程序连接：

- Citrix Gateway：有关信息，请参阅本节中的主题以及 Citrix Gateway 和 StoreFront 文档。

  > 注意：
  >
  > Citrix 建议在 StoreFront 服务器与用户设备之间使用 Citrix Gateway。

- 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 Workspace 应用程序时，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。

- 可信的服务器。
- 仅适用于 Citrix Virtual Apps 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 Citrix Workspace 应用程序与服务器之间的连接。Citrix Workspace 应用程序支持 SOCKS 和安全代理协议。
- 仅适用于 Citrix Virtual Apps 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 Citrix Virtual Apps and Desktops 7.6，可以在用户和 VDA 之间直接启用 SSL 连接。

出站代理支持

智能控制允许管理员定义粒度策略，以便使用 Citrix Gateway 配置和强制执行 Citrix Virtual Apps and Desktops 和 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）的用户环境属性。例如，您可能希望禁止用户将驱动器映射到其远程桌面。这可以使用 Citrix Gateway 上的智能控制功能来实现。

但是，当 Citrix Workspace 应用程序和 Citrix Gateway 属于单独的企业帐户时，方案会发生变化。在这种情况下，客户端域无法应用智能控制功能，因为客户端域上不存在网关。相反，您可以利用出站 ICA 代理。出站 ICA 代理允许您使用智能控制功能，即使 Citrix Workspace 应用程序和 Citrix Gateway 部署在不同的组织中亦如此。

Citrix Workspace 应用程序支持使用 NetScaler LAN 代理启动会话。可以配置单个静态代理，也可以使用出站代理插件在运行时选择代理服务器。

可以使用以下方法配置出站代理：

- 静态代理：通过提供代理主机名和端口号来配置代理服务器。
- 动态代理：可以使用代理插件 DLL 在一个或多个代理服务器中选择单个代理服务器。

可以使用组策略对象管理模板和注册表编辑器配置出站代理。

有关出站代理的详细信息，请参阅 Citrix Gateway 文档中的出站 ICA 代理支持。

出站代理支持 - 配置

> 注意：
>
> 如果同时配置了静态代理和动态代理，则动态代理配置优先。

使用 **GPO** 管理模板配置出站代理：

1. 通过运行 gpedit.msc 打开 Citrix Workspace 应用程序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 Workspace** > 网络路由。
3. 选择以下选项之一：
    - 对于静态代理：选择手动配置 **NetScaler LAN** 代理策略。选择已启用，然后提供主机名和端口号。

- 对于动态代理：选择使用 **DLL** 配置 **NetScaler LAN** 代理策略。选择已启用，然后提供 DLL 文件的完整路径。例如，`C:\Workspace\Proxy\ProxyChooser.dll`。

4. 单击应用和确定。

使用注册表编辑器配置出站代理：

- 对于静态代理：
  - 启动注册表编辑器并导航到 `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Network Routing\Proxy\NetScaler`。
  - 创建 DWORD 值项，如下所示：

```
"StaticProxyEnabled"=dword:00000001
"ProxyHost"="testproxy1.testdomain.com
"ProxyPort"=dword:000001bb
```

- 对于动态代理：
  - 启动注册表编辑器并导航到 `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\ICA Client\Engine\Network Routing\Proxy\NetScaler LAN Proxy`。
  - 创建 DWORD 值项，如下所示：

```
"DynamicProxyEnabled"=dword:00000001
"ProxyChooserDLL"="c:\\Workspace\\Proxy\\ProxyChooser.dll"
```

TLS

本主题适用于 Citrix Virtual Apps and Desktops 7.6 及更高版本。

要对 Citrix Workspace 应用程序与服务器的所有通信使用 TLS 加密，请配置用户设备、Citrix Workspace 应用程序以及运行 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。

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 Workspace 应用程序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。

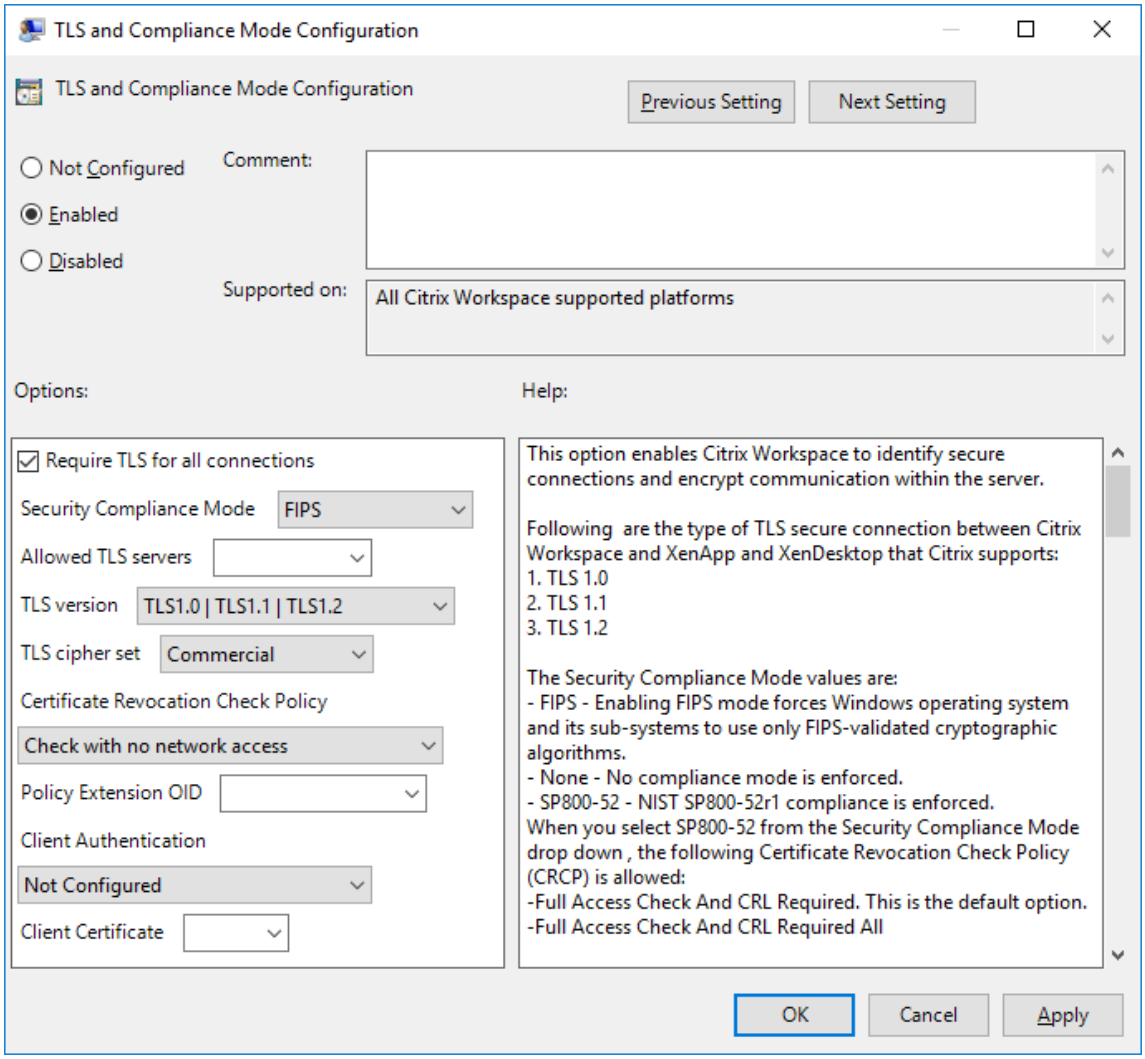
可以使用以下选项执行相应操作：

- 强制使用 TLS：Citrix 建议通过不可信网络（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）：使用 FIPS 批准的加密，有利于遵从 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 支持在适用于 Windows 的 Citrix Workspace 应用程序与 Citrix Virtual Apps and Desktops 和 Citrix DaaS 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（如果将服务器配置为请求客户端证书）。

TLS 支持

1. 通过运行 gpedit.msc 打开 Citrix Workspace 应用程序 GPO 管理模板。
2. 在计算机配置节点下，转至管理模板 > **Citrix Workspace** > 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 以实现安全连接。

a) 选择要求对所有连接使用 **TLS** 以强制 Citrix Workspace 应用程序对与已发布的应用程序和桌面的所有连接使用 TLS。

b) 从安全性合规模式下拉列表中，选择相应的选项：

   i. 无 - 不强制执行合规模式
   ii. **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 Workspace 应用程序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。

   选择 **SP800-52** 后，Citrix Workspace 应用程序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 Workspace 应用程序可能无法连接。

   i. 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 Workspace 应用程序可能会无法连接到已发布的应用程序和桌面。

c) 从允许的 **TLS** 服务器下拉列表中，选择端口号。可以确保适用于 Windows 的 Citrix Workspace 应用程序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 Workspace 无法识别和信任颁发者，连接将被拒绝。

d) 从 **TLS** 版本菜单中，选择以下选项之一：

- **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。

a) **TLS** 密码集 - 要强制使用特定的 TLS 密码集，请选择“政府”(GOV)、“商务”(COM) 或“全部”(ALL)。在某些 Citrix Gateway 配置情况下，您可能需要选择 **COM**。Citrix Workspace 应用程序支持 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 不建议使用 1024 位长度的 RSA 密钥。

- 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：
  a) TLS_RSA_WITH_RC4_128_MD5
  b) TLS_RSA_WITH_RC4_128_SHA
  c) TLS_RSA_WITH_3DES_EDE_CBC_SHA
  d) TLS_RSA_WITH_AES_128_CBC_SHA
  e) TLS_RSA_WITH_AES_256_CBC_SHA
  f) TLS_RSA_WITH_AES_128_GCM_SHA256
  g) 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：
  a) TLS_RSA_WITH_RC4_128_MD5
  b) TLS_RSA_WITH_RC4_128_SHA
  c) TLS_RSA_WITH_AES_128_CBC_SHA
  d) 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：
  a) TLS_RSA_WITH_AES_256_CBC_SHA
  b) TLS_RSA_WITH_3DES_EDE_CBC_SHA
  c) TLS_RSA_WITH_AES_128_GCM_SHA256
  d) TLS_RSA_WITH_AES_256_GCM_SHA384

a) 从证书吊销检查策略菜单中，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/Citrix Secure Web 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。

a) 使用策略扩展 **OID** 可以将 Citrix Workspace 应用程序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 Workspace 应用程序将仅接受包含策略扩展 OID 的服务器证书。

b) 从客户端身份验证菜单中，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。

a) 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。

b) 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：

Ciphersuite	Native Cyrpto Kit mode and cipher set								
	Open			FIPS			SP800-52		
	OPEN ALL	OPEN COM	OPEN GOV	FIPS ALL	FIPS COM	FIPS GOV	SP800-52 ALL	SP800-52 COM	SP800-52 GOV
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (1)	Y		Y	Y		Y	Y		Y
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384(1)	Y		Y	Y		Y	Y		Y
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Y	Y		Y	Y		Y	Y	
TLS_RSA_WITH_AES_256_GCM_SHA384 (1) (2)	X								
TLS_RSA_WITH_AES_128_GCM_SHA256 (1) (2)	X	X							
TLS_RSA_WITH_AES_256_CBC_SHA256 (1) (2)	X								
TLS_RSA_WITH_AES_256_CBC_SHA (2)	X								
TLS_RSA_WITH_AES_128_CBC_SHA (2)	X	X							
TLS_RSA_WITH_RC4_128_SHA (2) (3)	X	X							
TLS_RSA_WITH_RC4_128_MD5 (2) (3)	X	X							
TLS_RSA_WITH_3DES_EDE_CBC_SHA (2)	X								
TLS_EMPTY_RENEGOTIATION_INFO_SCSV	Y	Y	Y	Y	Y	Y	Y	Y	Y
Notes									
(1) Ciphersuites that require TLS1.2/DTLS 1.2									
(2) Ciphersuites disabled by default									
(3) Ciphersuites not available for DTLS protocol									
Y - Supported ciphersuites									
X-Deprecated ciphersuites									

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。如果在部署中使用防火墙，适用于 Windows 的 Citrix Workspace 应用程序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 Workspace 应用程序	TCP	80/443	与 StoreFront 通信
ICA/HDX	TCP	1494	访问应用程序和虚拟桌面

源	类型	端口	详细信息
ICA/HDX（启用了会话可靠性）	TCP	2598	访问应用程序和虚拟桌面
ICA/HDX（通过 SSL）	TCP	443	访问应用程序和虚拟桌面

有关端口的详细信息，请参阅知识中心文章 CTX101810。

如果为防火墙配置了网络地址转换 (NAT)，则使用 Web Interface 定义从内部地址到外部地址的映射和端口。例如，如果没有为 Citrix Virtual Apps and Desktops 服务器配置备选地址，则您可以将 Web Interface 配置为向 Citrix Workspace 应用程序提供备选地址。之后，Citrix Workspace 应用程序使用外部地址和端口号连接到服务器。

代理服务器

代理服务器用于限制网络的入站和出站访问，并处理适用于 Windows 的 Citrix Workspace 应用程序与服务器之间的连接。Citrix Workspace 应用程序支持 SOCKS 和安全代理协议。

与服务器进行通信时，Citrix Workspace 应用程序使用在运行适用于 Web 的 Workspace 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，Citrix Workspace 应用程序使用通过用户设备上默认 Web 浏览器的 **Internet** 设置进行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 Workspace 应用程序在连接过程中采用或弃用代理服务器。

> 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 `\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\AuthManager`
2. 设置 **ProxyEnabled**(REG_SZ)。
    - True - 指示 Citrix Workspace 应用程序在连接过程中遵从代理服务器的设置。
    - False - 指示 Citrix Workspace 应用程序在连接过程中放弃使用代理服务器。
3. 重新启动 Citrix Workspace 应用程序以使所做的更改生效。

可信服务器

可信服务器配置标识 Citrix Workspace 应用程序连接中的信任关系并强制执行该信任关系。

启用了可信服务器时，Citrix Workspace 应用程序将指定要求并确定与服务器的连接是否可信。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 Workspace 应用程序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 Workspace 应用程序组件（包括连接中心）退出。

1. 通过运行 gpedit.msc 打开 Citrix Workspace 应用程序 GPO 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 Workspace** > 网络路由 > 配置可信服务器配置。
3. 选择已启用强制 Citrix Workspace 应用程序执行区域识别。
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。

ICA 文件签名服务

ICA 文件签名可帮助保护您免于启动未经授权的应用程序或桌面。Citrix Workspace 应用程序根据管理策略确认由可信源生成应用程序或桌面启动，并防止从不可信服务器进行启动。您可以使用组策略对象管理模板或 StoreFront 来配置 ICA 文件签名。默认情况下，不启用 ICA 文件签名。

有关为 StoreFront 启用 ICA 文件签名服务的信息，请参阅 StoreFront 文档中的启用 ICA 文件签名服务。

对于 Web Interface 部署，Web Interface 可在启动过程中使用 Citrix ICA 文件签名服务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对 ICA 文件进行签名。

配置 **ICA** 文件签名

> 注意：
>
> 如果未将 CitrixBase.admx\adml 添加到本地 GPO，则启用 **ICA** 文件签名策略可能不存在。

1. 通过运行 gpedit.msc 打开 Citrix Workspace 应用程序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。
3. 选择启用 **ICA** 文件签名策略并根据需要选择其中一个选项：
    a) 已启用 - 指示您可以将签名证书指纹添加到可信证书指纹的白名单中。
    b) 信任证书 - 单击显示可从白名单中删除现有的签名证书指纹。可以从签名证书属性中复制并粘贴签名证书指纹。
    c) 安全策略 - 从菜单中选择以下选项之一。

i. 仅允许签名的启动 (更安全)：仅允许来自可信服务器且已签名的应用程序或桌面启动。如果签名无效，则将显示安全警告。由于未授权，您无法启动会话。
ii. 在进行未签名的启动时提示用户 (不安全) - 启动未签名或无效签名的会话时将显示一条消息提示。可以选择继续启动或取消启动（默认设置）。

4. 单击应用和确定保存此策略。
5. 重新启动 Citrix Workspace 应用程序会话以使所做的更改生效。

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. 创建一个根 CA 证书，并使用 GPO 或通过手动安装将其分发给用户设备。

Storebrowse

April 22, 2024

Storebrowse 是一款轻型命令行实用程序，用于在客户端与服务器之间进行交互。它用于对 StoreFront 中的所有操作以及向 Citrix Gateway 进行身份验证。

有关早期版本的适用于 Citrix Receiver for Windows 的 Storebrowse 实用程序的文档，请参阅 Storebrowse for Citrix Receiver for Windows（适用于 Citrix Receiver for Windows 的 Storebrowse）文档。

通过使用 Storebrowse 实用程序，管理员可以自动执行以下日常操作：

- 添加应用商店。
- 枚举已配置的应用商店中已发布的 Citrix Virtual Apps and Desktops 和 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）。
- 通过手动选择任何已发布的 Citrix Virtual Apps and Desktops 和 Citrix DaaS 生成 ICA 文件。
- 使用 Storebrowse 命令行生成 ICA 文件。
- 启动已发布的应用程序。

Storebrowse 实用程序现在属于 Authmanager 组件。安装 Citrix Workspace 应用程序后，Storebrowse 实用程序位于 `AuthManager` 安装文件夹中。

可以按以下方式检查注册表路径来确认是否与 `Authmanager` 组件一起安装了 Storebrowse 实用程序：

由管理员安装 **Citrix Workspace** 应用程序时：

在 32 位计算机上	[HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\AuthManager\Inst
在 64 位计算机上	[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\A

由用户（非管理员）安装 **Citrix Workspace** 应用程序时：

在 32 位计算机上	[HKEY_CURRENT_USER\SOFTWARE\Citrix\AuthManager\Insta
在 64 位计算机上	[HKEY_CURRENT_USER\SOFTWARE\WOW6432Node\Citrix\Au

要求

安装适用于 Windows 的 Citrix Workspace 应用程序版本 1808 或更高版本，才能在 StoreFront 和 Citrix Gateway 之间无缝地使用 Storebrowse 实用程序。要安装 Citrix Workspace 应用程序版本 1809，至少需要 530 MB 可用磁盘空间和 2 GB RAM。

兼容性列表

Storebrowse 实用程序与以下操作系统兼容：

操作系统
Windows 10（32 位和 64 位版本）
Windows 8.1（32 位和 64 位版本）
Windows 7 SP1（32 位和 64 位版本）
Windows Thin PC
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）
Windows Server 2008 R2（64 位版本）

连接

Storebrowse 实用程序支持以下类型的连接：

- HTTP 应用商店
- HTTPS 应用商店
- Citrix Gateway 11.0 及更高版本

> 注意：
>
> 在 HTTP 应用商店上使用命令行时，Storebrowse 实用程序不接受凭据。

身份验证方法

StoreFront 服务器　StoreFront 支持使用不同的身份验证方法访问应用商店，但有些方法并不建议使用。出于安全考虑，在创建应用商店时，某些身份验证方法默认情况下处于禁用状态。

- 用户名和密码：用户在访问其应用商店时可以输入其凭据并进行身份验证。在创建第一个应用商店时，显式身份验证默认情况下处于启用状态。所有用户访问方法都支持显式身份验证。
- 域直通：用户向其加入域的 Windows 计算机验证身份后，即可在访问自己的应用商店时自动登录。要使用此选项，必须在用户设备上安装 Citrix Workspace 应用程序时启用直通身份验证。有关配置域直通的详细信息，请参阅配置直通身份验证。
- **HTTP Basic**：Storebrowse 实用程序需要启用 HTTP Basic 身份验证才能与 StoreFront 服务器进行通信。默认情况下，此选项在 StoreFront 服务器上处于禁用状态。必须启用 HTTP Basic 身份验证方法。

Storebrowse 实用程序支持通过以下任一方法进行身份验证：

- 使用随 Storebrowse 实用程序内置的 `AuthManager`。注意：使用 Storebrowse 实用程序时，必须在 StoreFront 上启用 HTTP Basic 身份验证方法。当用户使用 Storebrowse 命令提供凭据时，此方法适用。
- 可以随适用于 Windows 的 Citrix Workspace 应用程序提供的外部 `Authmanager`。

Citrix Gateway 支持

使用最新版本的 Storebrowse 实用程序时，现在可以添加 Citrix Gateway URL。不需要在 Storebrowse 实用程序中进行任何额外的配置即可与 Citrix Gateway 进行通信。

通过 **Citrix Gateway** 实现单点登录

除了新添加的 Citrix Gateway 支持之外，现在还可以通过其使用单点登录。您可以添加新应用商店以及枚举已发布的资源，而无需提供您的用户凭据。

有关通过 Citrix Gateway 支持单点登录的详细信息，请参阅支持通过 Citrix Gateway 实现单点登录。

> 注意：
>
> 仅在为 Citrix Gateway 配置了单点登录身份验证的已加入域的计算机上支持此功能。

启动已发布的桌面或应用程序

现在可以直接从应用商店启动资源，而不需要使用 ICA 文件。

命令用法

以下部分提供了有关可以从 Storebrowse 实用程序使用的命令的详细信息。

-a、-addstore

说明：

添加新应用商店。返回应用商店的完整 URL。如果失败，则会报告一条错误。

> 注意：
>
> 可以使用 Storebrowse 实用程序添加多个应用商店。

StoreFront 上的命令示例：

命令：

```
storebrowse.exe -U *username* -P *password* -D *domain* -a *URL of Storefront*
```

示例：

‘.\storebrowse.exe -U {Username} -P {Password} -D {Domain} -a https://my.firstexamplestore.net‘

Citrix Gateway 上的命令示例：

命令：

```
storebrowse.exe -U *username* -P *password* -D *domain* -a *URL of CitrixGateway*
```

示例：

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -a <https://mysecondexample.com>
```


/?

说明：

提供有关 Storebrowse 实用程序用法的详细信息

(-l)、-liststore

说明：

列出用户添加的应用商店。

StoreFront 上的命令示例：

```
.\storebrowse.exe -l
```

Citrix Gateway 上的命令示例：

```
.\storebrowse.exe -l
```

(-M 0x2000 -E)

说明：

枚举可用资源

StoreFront 上的命令示例：

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -M 0
x2000 -E <https://my.firstexamplestore.net/Citrix/Store/discovery>
```

Citrix Gateway 上的命令示例：

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -M 0
x2000 -E <https://my.secondexample.net>
```

-q、-quicklaunch

说明：

使用 Storebrowse 实用程序生成访问已发布的应用程序和桌面所需的 ICA 文件。quicklaunch 选项要求提供一个启动 URL 作为输入以及应用商店 URL（可以是 StoreFront 服务器或 Citrix Gateway URL）。ICA 文件在 %LocalAppData%\Citrix\Storebrowse\cache 目录中生成。

可以执行以下命令来获取任何已发布的应用程序和桌面的启动 URL：

```
.\storebrowse -M 0X2000 -E https://myfirstexamplestore.net/Citrix/
Second/discovery
```


典型的启动 URL 类似如下所示：

```
'Controller.Calculator''Calculator''\' ''http://abc-sf.xyz.com/Citrix
/Stress/resources/v2/Q29udHJvbGxlci5DYWxjdWxhdG9y/launch/ica
```

StoreFront 上的命令示例：

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -q {
Launch_URL_of_published_ apps and desktops } <https://my.firstexamplestore
.net/Citrix/Store/resources/v2/Q2hJkOlmNoPQrSTV9y/launch/ica> <https
://my.firstexamplestore.net/Citrix/Store/discovery>
```

Citrix Gateway 上的命令示例：

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -q {
Launch_URL_of_published_ apps and desktops } <https://my.secondexmaplestore
.com>
```

-L、-launch

说明：

使用 Storebrowse 实用程序生成访问已发布的应用程序和桌面所需的 ICA 文件。launch 选项要求提供资源的名称以及应用商店 URL（可以是 StoreFront 服务器或 Citrix Gateway URL）。ICA 文件在 %LocalAppData%\Citrix\Storebrowse\cache 目录中生成。

可以执行以下命令获取已发布的应用程序和桌面的显示名称：

```
.\storebrowse -M 0X2000 -E https://myfirstexamplestore.net/Citrix/
Second/discovery
```

此命令的输出如下：

```
'Controller.Calculator''Calculator''\' ''http://abc-sf.xyz.com/Citrix
/Stress/resources/v2/Q29udHJvbGxlci5DYWxjdWxhdG9y/launch/ica
```

上面的输出中以粗体显示的名称用作 launch 选项的输入参数。

StoreFront 上的命令示例：

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -L
“{ Resource_Name } <https://my.firstexamplestore.net/Citrix/Store/
discovery>
```

Citrix Gateway 上的命令示例：

```
<.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -L {
Resource_Name } https://my.secondexamplestore.com>
```


-S、-sessionlaunch

说明：

您可以使用一个命令来添加应用商店、枚举已发布的资源（应用程序和桌面）以及启动资源。此选项接受以下各项作为参数 - 用户名、密码、域、要启动的资源的友好名称以及应用商店 URL。但是，如果用户未提供凭据，系统将发出输入凭据的 AuthManager 提示，然后将启动资源。

可以执行以下命令获取已发布的应用程序和桌面的资源的名称：

```
.\storebrowse -M 0X2000 -E https://myfirstexamplestore.net/Citrix/
Second/discovery
```

此命令的输出如下：

```
'Controller.Calculator''Calculator''\' ''http://abc-sf.xyz.com/Citrix
/Stress/resources/v2/Q29udHJvbGxlci5DYWxjdWxhdG9y/launch/ica
```

上面的输出中以粗体显示的名称将用作 –S 选项的输入参数。

StoreFront 上的命令示例：

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -S “
{ Friendly_Resource_Name } <https://my.firstexamplestore.net/Citrix/
Store/discovery >
```

Citrix Gateway 上的命令示例：

```
.\storebrowse.exe -U { Username } -P { Password } -D { Domain } -S {
Friendly_Resource_Name } <https://my.secondexamplestore.com>
```

-f、-filefolder

说明：

使用 Storebrowse 实用程序，在 -f 选项中定义的自定义路径中生成访问任何已发布的应用程序和桌面所需的 ICA 文件。

launch 选项要求提供文件夹名称和资源的名称作为输入以及应用商店 URL（这是 StoreFront 服务器或 Citrix Gateway URL）。

StoreFront 上的命令示例：

```
.\storebrowse.exe -f “C:\Temp\Launch.ica” -L “Resource_Name” { Store
 }
```

Citrix Gateway 上的命令示例：

```
.\storebrowse.exe -f “C:\Temp\Launch.ica” -L “Resource_Name” {
NSG_URL }
```


-t、-traceauthentication

说明：

生成 Storebrowse 实用程序内置 AuthManager 组件的日志。仅当 Storebrowse 实用程序使用内置 AuthManager 的情况下，才会生成日志。日志在 localappdata%\Citrix\Storebrowse\logs 目录中生成。

注意：此选项不能是用户的命令行中列出的最后一个参数。

StoreFront 上的命令示例：

```
.\storebrowse.exe -t -U { UserName } -P { Password } -D { Domain } -a
{ StoreURL }
```

Citrix Gateway 上的命令示例：

```
.\storebrowse.exe -t -U { UserName } -P { Password } -D { Domain } -a
{ NSG_URL }
```

-d、-deletestore

说明：

删除现有的 StoreFront 或 Citrix Gateway 应用商店。

StoreFront 上的命令示例：

```
.\storebrowse.exe -d https://my.firstexamplestore.net/Citrix/Store/
discovery
```

Citrix Gateway 上的命令示例：

```
.\storebrowse.exe -d https://my.secondexmaplestore.com
```

通过 **Citrix Gateway** 实现单点登录支持

单点登录允许您对域进行身份验证，并使用该域提供的 Citrix Virtual Apps and Desktops 和 Citrix DaaS，而不需要重新对每个应用程序或桌面进行身份验证。使用 Storebrowse 实用程序添加应用商店时，您的凭据将随为您枚举的虚拟应用程序和桌面一起传递到 Citrix Gateway 服务器，包括“开始”菜单设置。配置单点登录后，可以添加应用商店、枚举虚拟应用程序和桌面以及启动所需的资源，而无需多次键入您的凭据。

Citrix Gateway 版本 11 及更高版本支持此功能。

必备条件：

有关如何为 Citrix Gateway 配置单点登录的必备条件，请参阅配置域直通身份验证。

可以使用组策略对象 (GPO) 管理模板启用通过 Citrix Gateway 实现的单点登录功能。

> 注意：
>
> 从 Citrix Receiver 升级到 Citrix Workspace 应用程序或首次全新安装 Citrix Workspace 应用程序时，必须向本地 GPO 中添加最新的模板文件。有关向本地 GPO 中添加模板文件的详细信息，请参阅配置组策略对象管理模板。如果进行升级，导出最新文件时将保留现有设置。

1. 通过运行 gpedit.msc 打开 Citrix Workspace 应用程序 GPO 管理模板
2. 在计算机配置节点下，转至管理模板 > **Citrix** 组件 > **Citrix Workspace** > 用户身份验证 > 通过 **Citrix Gateway** 实现 **Single Sign-On**。
3. 使用切换选项以启用或禁用“Single Sign-On”选项。
4. 单击应用和确定。
5. 重新启动 Citrix Workspace 应用程序会话以使所做的更改生效。

限制：

- 必须在 StoreFront 服务器上启用 HTTP Basic 身份验证方法，才能通过 Storebrowse 实用程序执行凭据注入操作。
- 如果您有 HTTP 应用商店，并尝试使用该实用程序连接到该应用商店以枚举或启动已发布的虚拟应用程序和桌面时，将不支持使用命令行选项执行凭据注入操作。解决方法：使用外部 `AuthManager` 模块，该模块在您使用命令行的情况下不提供凭据时触发。
- Storebrowse 实用程序当前仅支持单个应用商店（在 StoreFront 服务器上配置了 Citrix Gateway）。
- 仅当为 Citrix Gateway 配置了单重身份验证时，才可使用 Storebrowse 实用程序中的凭据注入功能。
- Storebrowse 实用程序的命令行选项 `Username` (`-U`)、`Password` (`-P`) 和 `Domain` (`-D`) 区分大小写，并且必须采用大写形式。

Citrix Workspace 应用程序 Desktop Lock

January 17, 2024

不需要与本地桌面进行交互时，可以使用 Citrix Workspace 应用程序 Desktop Lock。可以使用 Desktop Viewer（如果已启用），但是，工具栏上仅具有必需的一组选项：

- Ctrl+Alt+Del
- 首选项
- 设备
- 断开连接。

具有 Desktop Lock 功能的适用于 Windows 的 Citrix Workspace 应用程序在加入了域的计算机上运行，这些计算机启用了 SSON (Single Sign-On) 并配置了应用商店。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。

使用命令行界面安装 **Desktop Lock**

必备条件：

- 您必须是已加入域的计算机上的管理员。
- 必须启用单点登录。
- 必须配置应用商店。

1. 通过运行以下命令安装 Citrix Workspace 应用程序：

```
`CitrixWorkspaceApp.exe /includeSSON /Silent STORE0= "AppStore; https://testserver.net/Citrix/MyStore/discover;on;Desktop App Store" `
```

2. 从 Citrix 下载页面下载可用的 `CitrixWorkspaceDesktopLock.msi`。
3. 通过运行以下命令安装 Desktop Lock：

```
installationSilent : msiexec /i CitrixWorkspaceDesktopLock.msi /qn
```

以用户身份登录后，已发布的桌面将自动启动。

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。
- 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 Citrix Virtual Apps and Desktops 文档中的配置本地应用程序访问和 URL 重定向部分。

使用 **Citrix Workspace** 应用程序 **Desktop Lock**

- 可以将 Citrix Workspace 应用程序 Desktop Lock 与以下 Citrix Workspace 应用程序功能结合使用：
  - 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 Workspace 应用程序 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 Workspace 应用程序 Desktop Lock 进行了优化，没有“主页”、“还原”、“最大化”和“显示”属性。
- Ctrl+Alt+Del 在 Desktop 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。
- 禁用连接或 Desktop Viewer 进行桌面连接时，Ctrl+F1 会触发 Ctrl+Alt+Del。

> 注意：
>
> 安装了 Desktop Lock，并且注册表路径 `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle` 或 `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\Dazzle` 中的 `LiveInDesktopDisconnectOnLock` 设置为 **False**，当端点从休眠或待机模式唤醒时，活动会话将断开连接。

安装 **Citrix Workspace** 应用程序 **Desktop Lock**

此过程将安装适用于 Windows 的 Citrix Workspace 应用程序，以便使用 Citrix Workspace 应用程序 Desktop Lock 显示虚拟桌面。有关使用智能卡的部署，请参阅智能卡。

1. 使用本地管理员帐户登录。
2. 在命令提示窗口中，运行以下命令（位于安装介质上的 Citrix Workspace app and Plug-ins > Windows > Citrix Workspace app 文件夹中）。

   例如：

```
CitrixWorkspaceApp.exe /includeSSON STORE0="DesktopStore;https://my.storefront.server/Citrix/MyStore/discovery;on;Desktop Store"
```

有关命令的详细信息，请参阅安装。

1. 在安装介质上的同一文件夹中，双击 `CitrixWorkspaceDesktopLock.msi`。此时将显示 Desktop Lock 向导。按照提示进行操作。
2. 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，则使用 Citrix Workspace 应用程序 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 中排除安装 `CitrixWorkspaceDesktopLock.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 Citrix Workspace Desktop Lock 的静默安装，请使用以下命令行：

```
msiexec /i CitrixWorkspaceDesktopLock.msi /qn
```


配置 **Citrix Workspace** 应用程序 **Desktop Lock**

授予仅访问一个运行 Citrix Workspace 应用程序 Desktop Lock 的虚拟桌面的权限。

使用 Active Directory 策略可防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 Workspace 应用程序 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 Workspace 应用程序”>“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 设备和新的 USB 设备策略。
- 驱动器映射 - 在“Citrix Workspace 应用程序”>“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 Workspace 应用程序”>“远程连接客户端设备”中，启用并配置客户端麦克风策略。

配置智能卡以便与 **Windows Desktop Lock** 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身份验证（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 Workspace”>“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 Workspace 应用程序 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://delivery-group-name 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 Workspace 应用程序 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 Workspace 应用程序 Desktop Lock 的用户设备。

删除 **Desktop Lock**

确保删除下面列出的两个组件。

1. 使用安装和配置 Citrix Workspace 应用程序 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 Workspace 应用程序 Desktop Lock。
   - 删除适用于 Windows 的 Citrix Workspace 应用程序。

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**

October 31, 2023

证书标识声明 **SDK**

通过证书标识声明 (CID) SDK，开发人员可以创建一个插件，该插件允许 Citrix Workspace 应用程序使用客户端计算机上安装的证书对 StoreFront 服务器进行身份验证。CID 将用户的智能卡标识声明给 StoreFront 服务器，而无需执

行基于智能卡的身份验证。

有关详细信息，请参阅 Certificate Identity Declaration SDK for Citrix Workspace app for Windows（适用于 Windows 的 Citrix Workspace 应用程序适用的证书标识声明 SDK）文档。

Citrix Common Connection Manager SDK

Common Connection Manager (CCM) SDK 提供一组本机 API，这些 API 允许您以编程方式交互和执行基本操作。此 SDK 不需要单独下载，因为它属于适用于 Windows 的 Citrix Workspace 应用程序安装包的一部分。

> 注意：
>
> 与启动相关的某些 API 需要 ICA 文件来发起虚拟应用程序和桌面会话的启动过程。

CCM SDK 功能包括：

- 会话启动
  - 允许使用生成的 ICA 文件启动应用程序和桌面。
- 会话断开连接
  - 与使用连接中心执行断开连接操作类似。可以对所有会话或某个特定用户执行断开连接操作。
- 会话注销
  - 与使用连接中心执行注销操作类似。可以对所有会话或某个特定用户执行注销操作。
- 会话信息
  - 提供不同的方法来获取已启动会话的连接相关信息。这包括桌面会话、应用程序会话和反向无缝应用程序会话

有关 SDK 文档的详细信息，请参阅 Programmers guide to Citrix CCM SDK（《Citrix CCM SDK 程序员指南》）。

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 Citrix Virtual Apps and Desktops 服务器上。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。

有关详细信息，请参阅 Citrix Virtual Channel SDK for Citrix Workspace app for Windows（适用于 Windows 的 Citrix Workspace 应用程序适用的 Citrix 虚拟通道 SDK）文档。

Fast Connect 3 凭据插入 API

Fast Connect 3 凭据插入 API 提供用于向单点登录 (SSON) 功能提供用户凭据的接口。此功能在适用于 Windows 的 Citrix Workspace 应用程序 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。

有关详细信息，请参阅 Fast Connect 3 Credential Insertion API for Citrix Workspace app for Windows（适用于 Windows 的 Citrix Workspace 应用程序适用的 Fast Connect 3 凭据插入 API）。

ICA 设置参考

June 14, 2023

ICA 设置参考文件提供注册表设置和 ICA 文件设置列表，允许管理员自定义 Citrix Workspace 应用程序的行为。您还可以使用 ICA 设置参考对 Citrix Workspace 应用程序的异常行为进行故障排除。

ICA 设置参考（PDF 下载）