适用于 Windows 的 Citrix Workspace 应用程序

Contents

关于此版本

April 6, 2023

2303 中的新增功能

WebEx 插件的客户端应用程序管理 **[**技术预览版**]**

支持 WebEx 插件的下载、安装和自动更新，其处理方式与 Zoom 插件相同。

有关如何启用此功能的详细信息，请参阅 WebEx 插件的客户端应用程序管理。

> 注意：
>
> 技术预览版可供客户在其非生产环境或有限生产环境中进行测试，并为客户提供共享反馈的机会。Citrix 不接受功能预览版的支持案例，但欢迎提供改进这些功能的反馈。Citrix 可能会根据反馈的严重性、紧迫性和重要性对反馈执行操作。建议不要在生产环境中部署 Beta 版本。

可以通过 Podio 表单提供有关此功能的反馈。

配置浏览器内容重定向叠加浏览器临时数据存储的路径

自 Citrix Workspace 应用程序 2303 版本起，要求您为基于 Chromium Embedded Framework (CEF) 的浏览器配置临时数据存储路径。

有关详细信息，请参阅配置浏览器内容重定向叠加浏览器临时数据存储的路径。

支持 **StoreFront** 应用商店的新式身份验证方法

适用于 Windows 的 Citrix Workspace 应用程序 2303 支持 StoreFront 应用商店的新式验证。可以使用下面的任何一种方式向 Citrix StoreFront 应用商店进行身份验证：

- 使用 Windows Hello 和 FIDO2 安全密钥。有关详细信息，请参阅其他身份验证方式。
- 从 Azure Active Directory (AAD) 作为身份提供程序的已加入 AAD 的计算机单点登录到 Citrix StoreFront 应用商店。有关详细信息，请参阅其他身份验证方式。
- Workspace 管理员可以为对 Citrix StoreFront 应用商店进行身份验证的用户配置和强制执行 Azure Active Directory 条件访问策略。有关详细信息，请参阅支持 Azure AD 中的条件访问。

必须使用 Microsoft Edge WebView2 作为底层浏览器进行直接 StoreFront 和网关身份验证，才能启用此功能。

> 注意：
>
> 请确保 Microsoft Edge WebView2 Runtime 版本为 102 或更高版本。

可以使用 GPO 模板为 StoreFront 应用商店启用新式验证方法。有关详细信息，请参阅支持 StoreFront 应用商店的新式验证方法部分。

改善了优化 **Microsoft Teams** 视频通话的体验

自本版本起，默认情况下，对优化的 Microsoft Teams 视频会议呼叫启用联播支持。有了这种支持，通过调整到适当的分辨率以便为所有呼叫者提供最佳通话体验，可以改善跨不同端点的视频会议通话的质量和体验。

通过这种改进的体验，每个用户都可以提供分辨率不同（例如 720p、360p 等）的多个视频流，具体取决于多种因素，包括端点能力、网络条件等。接收端点随后会请求其能够处理的最大质量分辨率，从而为所有用户提供最佳视频体验。

> 注意：
>
> 此功能仅在 Microsoft Teams 推出更新后可用。有关 ETA 的信息，请转至并搜索 Microsoft 365 路线图。Microsoft 推出此更新时，您可以查看 CTX253754 以获取文档更新和公告。

应用程序保护的增强功能：反 **DLL** 注入

作为应用程序保护的一部分，我们现在有一项安全增强功能，可帮助保护 Citrix Workspace 应用程序免受某些未经授权的动态链接库 (DLL) 或不可信模块的侵害。如果注入了此类不可信模块，Citrix Workspace 应用程序会检测到这些干预措施并停止加载这些模块。

可以为以下组件启用反 DLL 注入：

- Citrix 身份验证管理器
- Citrix Workspace 应用程序 UI
- Citrix Virtual Apps and Desktops

有关详细信息，请参阅应用程序保护文档。

> 免责声明：
>
> 此功能通过筛选对底层操作系统所需功能（加载 DLL 所需的特定 API 调用）的访问来发挥作用。这样做意味着它甚至可以提供保护，使其免受某些自定义和专门构建的黑客工具的侵害。但是，随着操作系统的发展，加载 DLL 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。

Citrix Enterprise Browser

本版本包括基于 Chromium 版本 109 的 Citrix Enterprise Browser 版本 109.1.1.29。有关 Citrix Enterprise Browser 的详细信息，请参阅 Citrix Enterprise Browser 文档。

StoreFront 支持 Secure Private Access

作为管理员，您现在可以使用 Secure Private Access 解决方案在 StoreFront 中配置 Web 和 SaaS 应用程序。管理员配置应用程序后，最终用户可以使用具有增强的安全性的 Citrix Enterprise Browser 打开 Web 和 SaaS 应用程序。

有关详细信息，请参阅 Citrix Secure Private Access 文档中的本地 Secure Private Access。

2303 中已修复的问题

- 发布的 URL 通过 Citrix Enterprise Browser 而非设备的默认浏览器打开。[CTXBR-4718]
- 在无权主动访问外部站点的环境中使用 SSON 时，枚举应用程序和启动应用程序或桌面时可能会遇到延迟。自 Citrix Workspace 应用程序版本 2210.5 以及 Citrix Workspace 应用程序版本 2203 CU2 以后，就会出现此问题。[CVADHELP-21786]
- 当您从 Citrix Workspace 打开应用程序时，wfica32.exe 进程可能会意外停止并提示错误消息。仅当您启用了自适应音频功能时才会出现此问题。[CVADHELP-20999]
- 当您使用 PowerShell 脚本在远程计算机上安装 Citrix Workspace 应用程序 2212 时，Citrix Workspace 应用程序安装程序可能会停止。此问题发生在远程计算机上开始安装之前。[CVADHELP-22278]
- 当您尝试通过组策略对象 (GPO) 或命令行配置多个应用商店时，其中一个应用商店可能未完全配置。[CVADHELP-22034]
- 屏幕可能会在左上角显示身份验证弹出窗口，而非显示在中央位置。[CVADHELP-21835]
- 在将应用商店身份验证令牌设置为 **true** 的情况下添加应用商店后，Citrix Workspace 可能会在白屏上变得无响应，并且应用商店身份验证令牌设置为 **false**。[CVADHELP-21582]
- 当 VPN 断开连接或重新连接时，尝试访问适用于 Windows 的 Citrix Workspace 应用程序可能会失败。[CVADHELP-21662]
- 当您使用 Microsoft Teams 从 HP EliteBook G6 端点共享屏幕时，可能会看到红色窗口而非红色边框。[CVADHELP-20763]
- 您可能无法在 Bloomberg 键盘 5 或 Bloomberg 键盘 2013 上使用 Bloomberg 终端应用程序。在启用了应用程序保护功能的系统中安装 Citrix Workspace 应用程序版本 2302 时会出现此问题。[CVADHELP-22221]
- 重新连接桌面时，窗口的位置和大小可能不会保持不变。当桌面处于窗口模式并使用非主显示器时会出现此问题。[HDX-44997]
- 当桌面处于正常分辨率和 DPI 时，**Desktop Viewer** 工具栏可能会覆盖屏幕。[HDX-45206]
- 在多会话场景中，当您打开第二个会话时，该会话可能会隐藏在第一个会话的后面。此外，第二个会话的 Citrix Workspace 应用程序图标可能不在任务栏上。[RFWIN-29773]

2303 中的已知问题

- 如果您在还原会话对话框中进行任何鼠标交互（鼠标操作或移动），Citrix Workspace 应用程序可能会停止响应。从 Citrix Workspace 应用程序版本 2302 升级到 2303 之后启动会话时，如果之前有断开连接的会话，则会出现此问题。[RFWIN-29663]

> 注意：
>
> 有关早期版本中的问题的完整列表，请参阅已知问题。

早期版本

本部分内容提供了有关我们根据 Citrix Workspace 应用程序的生命周期里程碑支持的早期版本中的新增功能和已修复的问题的信息。

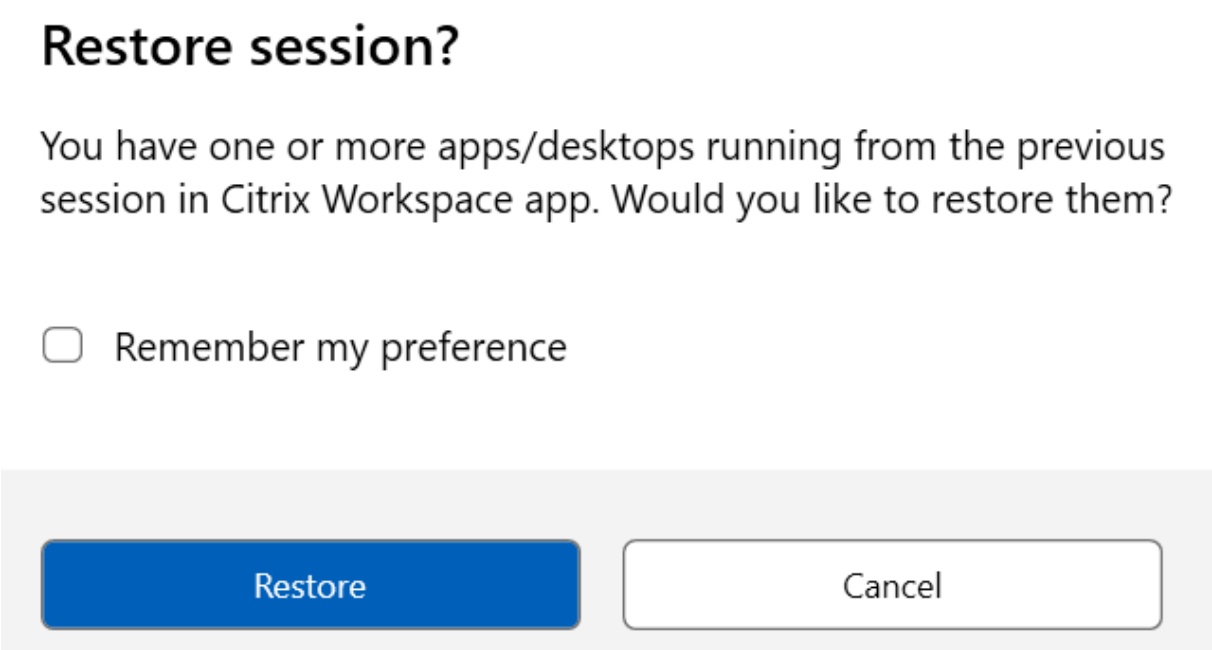
2302

新增功能

改进了虚拟应用程序和桌面的重新连接体验

此版本在重新连接到已断开连接的虚拟应用程序和桌面时提供了增强的用户体验。

当 Citrix Workspace 应用程序尝试刷新断开连接的 Citrix Workspace 应用程序或作为 Workspace 控制功能的一部分启动新虚拟应用程序或桌面时，会出现以下提示：



仅当 Global App Configuration Service 中的显示重新连接会话的重新连接提示设置为 true 时，才会出现此提示。

单击还原进行重新连接以打开新的和断开连接的虚拟应用程序和桌面。如果您只想启动新选定的应用程序和桌面，请单击取消。

也可以选择记住我的首选项，在下次登录时应用选定的首选项。

之前的新还原会话**?** 仅在以下情况下才会出现提示：

- 用户尝试启动属于工作区应用商店的应用程序，
- 没有为 Workspace 控制功能配置管理员策略或应用程序配置设置，
- Workspace 控制重新连接选项在客户端上设置为默认值。

> 注意：
>
> 重新连接选项中的重新连接设置优先于在对话框中设置的首选项。有关详细信息，请参阅使用“高级首选项”对话框配置重新连接选项。

Zoom 插件的客户端应用程序管理

现在，您可以使用客户端应用程序管理功能管理 Zoom 插件。

> 注意：
>
> 此功能仅适用于 Workspace（云）会话。

有关详细信息，请参阅 Zoom 插件的客户端应用程序管理。

支持 **StoreFront** 应用商店的新式验证方法 [技术预览版]

自本版本起，适用于 Windows 的 Citrix Workspace 应用程序支持 StoreFront 应用商店的新式验证方法。可以使用下面的任何一种方式向 Citrix StoreFront 应用商店进行身份验证：

- 使用 Windows Hello 和 FIDO2 安全密钥。有关详细信息，请参阅其他身份验证方式。
- 从 Azure Active Directory (AAD) 作为身份提供程序的已加入 AAD 的计算机单点登录到 Citrix StoreFront 应用商店。有关详细信息，请参阅其他身份验证方式。
- Workspace 管理员可以为对 Citrix StoreFront 应用商店进行身份验证的用户配置和强制执行 Azure Active Directory 条件访问策略。有关详细信息，请参阅支持 Azure AD 中的条件访问。

必须使用 Microsoft Edge WebView2 作为底层浏览器进行直接 StoreFront 和网关身份验证，才能启用此功能。

> 注意：
>
> 请确保 Microsoft Edge WebView2 Runtime 版本为 102 或更高版本。

可以使用 GPO 模板为 StoreFront 应用商店启用新式验证方法。有关详细信息，请参阅支持 StoreFront 应用商店的新式验证方法部分。

> 注意：
>
> 技术预览版可供客户在其非生产环境或有限生产环境中进行测试，并为客户提供共享反馈的机会。Citrix 不接受功能预览版的支持案例，但欢迎提供改进这些功能的反馈。Citrix 可能会根据反馈的严重性、紧迫性和重要性对反馈执行操作。建议不要在生产环境中部署 Beta 版本。

可以通过 Podio 表单提供有关此功能的反馈。

更新了优化后的 **Microsoft Teams** 的音频设备选择行为

自本版本起，当您更改端点上的声音设置中的默认音频设备时，Citrix VDI 中经过优化的 Microsoft Teams 会更改当前的音频设备选择以匹配端点默认值。

但是，如果您在 Microsoft Teams 中明确选择了设备，您的选择将优先，并且不遵循端点默认值。在清除 Microsoft Teams 缓存之前，您的选择持续不变。

应用程序保护增强功能

自本版本起，适用于 Windows 的 Citrix Workspace 应用程序允许您使用 Global App Configuration 为身份验证和自助服务插件配置应用程序保护。以前，您只能使用组策略对象配置这些组件。

如果您使用 Global App Configuration Service 启用反键盘记录和防屏幕捕获功能，这些功能将同时适用于身份验证和自助服务插件。

> 注意：
>
> Global App Configuration Service 配置不适用于虚拟应用程序、虚拟桌面、Web 应用程序和 SaaS 应用程序。这些资源将继续使用 Delivery Controller 和 Citrix Secure Private Access 进行控制。有关详细信息，请参阅 Citrix Virtual Apps and Desktops 文档中的“应用程序保护”的配置部分。

有关详细信息，请参阅应用程序保护增强功能部分。

Citrix Enterprise Browser

本版本包括基于 Chromium 版本 108 的 Citrix Enterprise Browser 版本 108.1.1.97。有关 Citrix Enterprise Browser 的详细信息，请参阅 Citrix Enterprise Browser 文档。

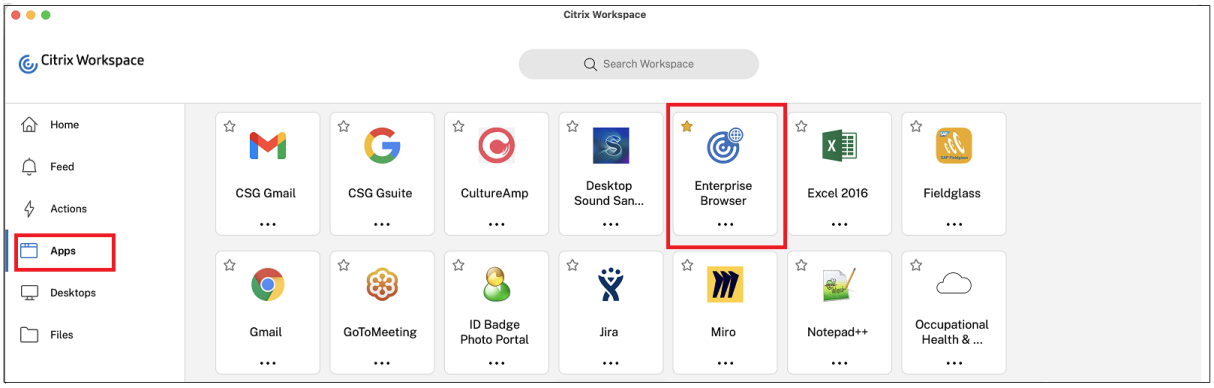
通过 **Citrix Enterprise Browser** 打开所有 **Web** 和 **SaaS** 应用程序

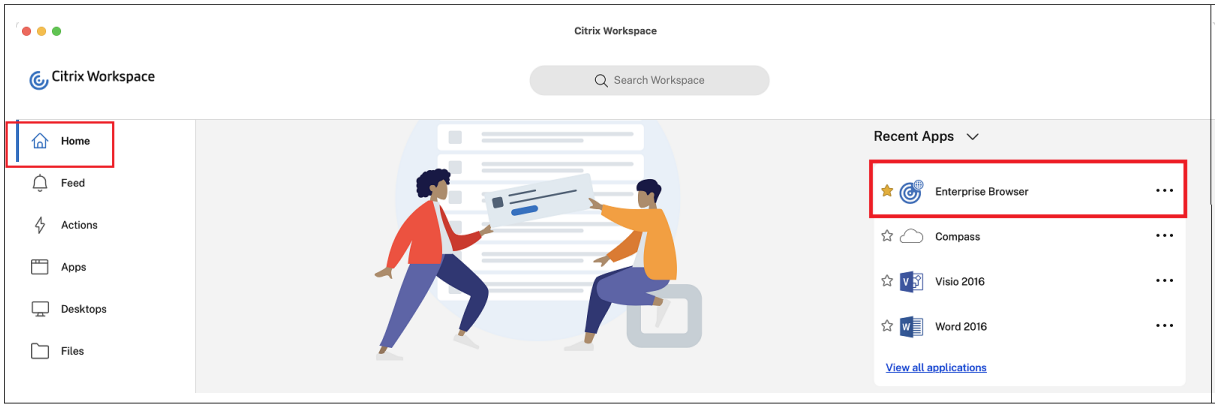
在本版本的 Enterprise Browser 中（在适用于 Windows 的 Citrix Workspace 应用程序中），Citrix Workspace 应用程序中可用的所有内部 Web 应用程序和外部 SaaS 应用程序都将在 Citrix Enterprise Browser 中打开。

可以选择从 **Citrix Workspace** 应用程序中启动 **Citrix Enterprise Browser**

以前，您可以在打开 Web 或 SaaS 应用程序后从 Citrix Workspace 应用程序打开 Citrix Enterprise Browser。

自本版本起，您可以直接从 Citrix Workspace 应用程序中打开 Citrix Enterprise Browser，无需打开 Web 或 SaaS 应用程序。通过此功能，您可以轻松访问 Citrix Enterprise Browser，而不需要管理员进行任何配置。默认情况下，此功能可用。



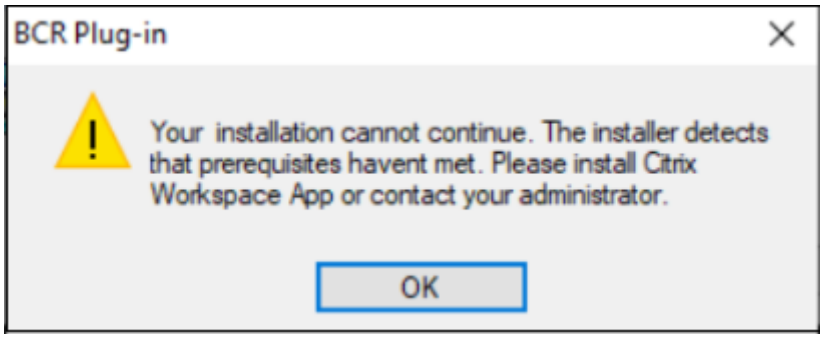


> 注意：
>
> 最终用户必须通过 Secure Private Access 获得至少一个 Web 或 SaaS 应用程序的权限。

已修复的问题

- 如果 Citrix Enterprise Browser 是默认浏览器，某些增强的安全性设置为关的 SaaS 应用程序将无法在 Citrix Enterprise Browser 中打开。[CTXBR-4106] [CTXBR-4405]
- 使用 Microsoft Edge WebView2 Runtime 版本 109 及更高版本时，尝试从自定义 Web 应用商店启动应用程序或桌面可能会失败。[RFWIN-29200].
- 您可能无法向 Citrix Workspace 应用程序中添加隐藏的应用商店。当您尝试添加需要智能卡身份验证的 Citrix Gateway FQDN 时或者 StoreFront 应用商店名称中包含空格（例如 `https://servername.company.com?Store` Service）时，就会出现此问题。[CVADHELP-21516]
- 如果您在达到设置的超时值之前退出 Citrix Workspace 应用程序，则不活动超时值可能不会过期。因此，您稍后无需输入任何凭据即可启动 Citrix Workspace 应用程序。[CVADHELP-20912]
- 安装 Citrix Workspace 应用程序后，您可能无法自动看到身份验证弹出页面。[CVADHELP-20593]
- 在多显示器设置中，每当用户断开连接并重新连接到会话时，应用程序窗口就会移动到不同的显示器。[HDX-45043]

- 在某些较旧的 AMD GPU 系列中，Citrix Workspace 应用程序 2206 或更高版本可能会看到紫色视频内容或屏幕闪烁。[HDX 46264]
- 无法修复 BCRClient.msi，并且在 Citrix Workspace 应用程序安装期间出现以下错误：



[HDX-46964]

2212

新增功能

> 注意：
>
> 自本版本起，请确保 Microsoft Edge WebView2 Runtime 版本为 102 或更高版本。有关详细信息，请参阅系统要求和兼容性。

客户端应用程序管理

适用于 Windows 的 Citrix Workspace 应用程序 2212 现在提供客户端应用程序管理功能，使 Citrix Workspace 应用程序成为端点安装和管理 Secure Access Agent 和端点分析 (EPA) 插件等代理所需的单个客户端应用程序。

借助此功能，管理员可以轻松地从单个管理控制台部署和管理所需的代理。

> 注意：
>
> 此功能仅适用于 Workspace（云）会话。

有关详细信息，请参阅客户端应用程序管理。

Zoom 插件的客户端应用程序管理 **[**技术预览版**]**

自适用于 Windows 的 Citrix Workspace 应用程序 2212 起，您现在可以使用客户端应用程序管理功能管理 Zoom 插件。

> 注意：
>
> 此功能仅适用于 Workspace（云）会话。

有关详细信息，请参阅客户端应用程序管理。

可以使用此 Podio 表单记录您对此技术预览的反馈。

> 注意：
>
> 技术预览版可供客户在其非生产环境或有限生产环境中进行测试，并为客户提供共享反馈的机会。Citrix 不接受功能预览版的支持案例，但欢迎提供改进这些功能的反馈。Citrix 可能会根据反馈的严重性、紧迫性和重要性对反馈执行操作。建议不要在生产环境中部署 Beta 版本。

自动更新版本控制

管理员现在可以管理组织中的设备的自动更新版本。

管理员可以通过在 Global App Config Service 中设置 maximumAllowedVersion 属性中的版本来控制版本。

Global App Config Service 中的示例 JSON 文件：

```
"AutoUpdate": {


"userOverride": false,

"AutoUpdatePluginsSettings": [

    {


    "pluginSettings":

{
        "upgradeToLatest": false,
        "maximumAllowedVersion": "22.9.0.3934",                }


,

    "pluginName": "WorkspaceApp",

    "pluginId": "1CDF566D-B2C7-47F-6283C862E1D6"

   }


<!--NeedCopy-->
```


设置版本后，用户设备上的 Citrix Workspace 应用程序会自动更新到在 maximumAllowedVersion 属性中指定的版本。

> 备注：
>
> - 要实现自动更新版本控制，必须将 Global App Config Service 中的 `upgradeToLatest` 设置设为 false。如果此设置为 true，则将忽略 `maximumAllowedVersion`。
> - 请勿修改 pluginId，因为此 ID 已映射到 Citrix Workspace 应用程序。
> - 如果管理员尚未在 Global App Config Service 中配置版本，则默认情况下，Citrix Workspace 应用程序将更新到最新的可用版本。

强制提示联邦身份提供商登录

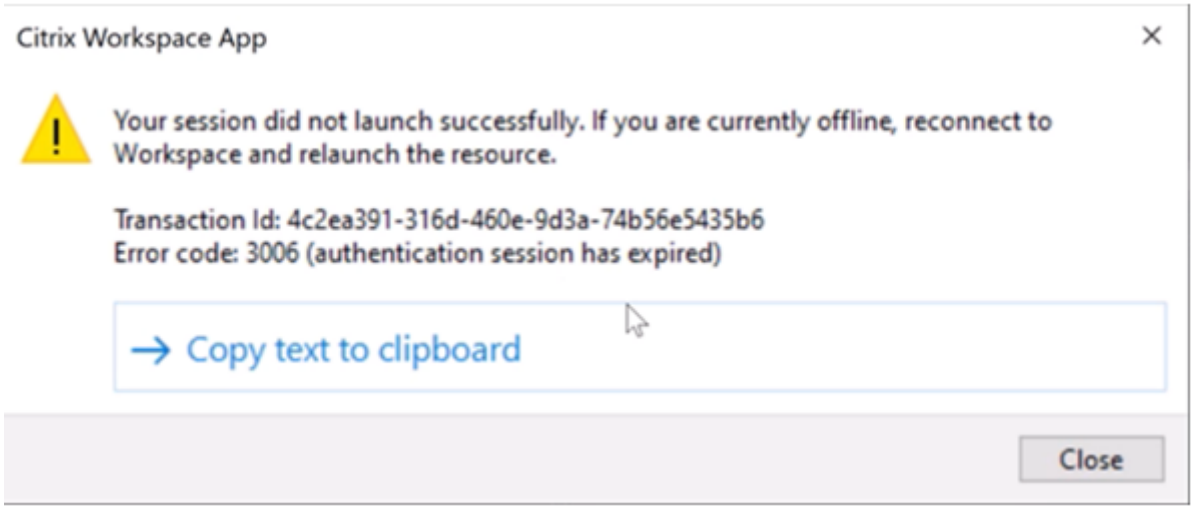
Citrix Workspace 应用程序现在支持联合身份提供商会话设置。有关详细信息，请参阅 Citrix 知识中心文章 CTX253779。

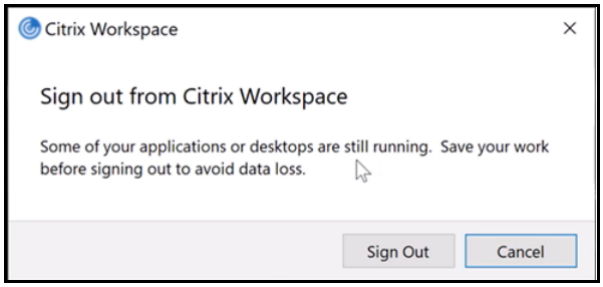
您不再需要使用应用商店身份验证令牌策略来强制执行登录提示。

改善了连接租用文件到期后的重新连接体验

以前，连接租用文件和身份验证令牌到期时不会通知最终用户。

自本版本起，系统将提示您一条错误消息和一个同意对话框。只有当您在会话中运行资源时，才会出现同意对话框。如果没有资源正在运行，则只会出现错误对话框。系统将不提示您注销同意对话框。





您可以单击注销从当前的 Citrix Workspace 应用程序会话中注销，也可以单击取消继续会话。

> 注意：
>
> 请在单击注销之前保存您的数据。

应用程序保护的增强功能：反 **DLL** 注入 **[技术预览版]**

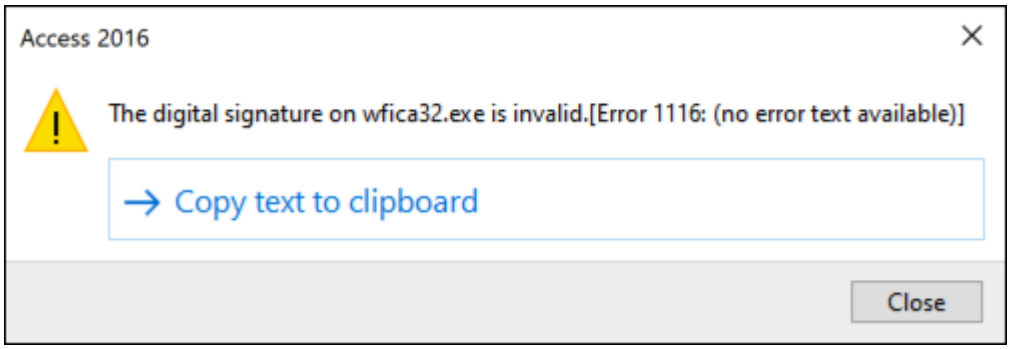
作为应用程序保护的一部分，我们现在有一项安全增强功能，可帮助保护 Citrix Workspace 应用程序免受某些未经授权的动态链接库 (DLL) 或不可信模块的侵害。如果注入了此类不可信模块，Citrix Workspace 应用程序会检测到这些干预措施并停止加载这些模块。

以前，此技术预览版功能仅适用于受保护的虚拟应用程序和桌面。在本版本中，我们扩大了其作用域，现在包括：

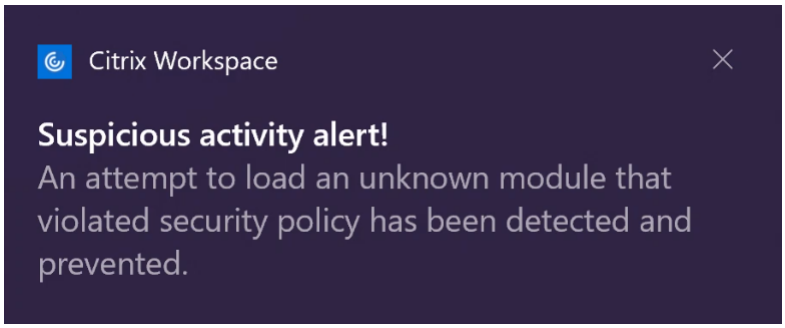
- 所有虚拟应用程序和桌面会话
- Citrix Workspace 应用程序身份验证窗口（本地部署/StoreFront）

此外，此增强功能现在：

- 当受保护组件上存在某些不可信或恶意 DLL 时，立即退出会话



- 当不可信或恶意 DLL 被阻止时显示通知。



免责声明：

此功能通过筛选对底层操作系统所需功能（加载 DLL 所需的特定 API 调用）的访问来发挥作用。这样做意味着它甚至可以提供保护，使其免受某些自定义和专门构建的黑客工具的侵害。但是，随着操作系统的发展，加载 DLL 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。

可以使用此 Podio 表单注册此技术预览版。

> 注意：
>
> 技术预览版可供客户在其非生产环境或有限生产环境中进行测试，并为客户提供共享反馈的机会。Citrix 不接受功能预览版的支持案例，但欢迎提供改进这些功能的反馈。Citrix 可能会根据反馈的严重性、紧迫性和重要性对反馈执行操作。建议不要在生产环境中部署 Beta 版本。

支持默认安装应用程序保护

现在，在 Citrix Workspace 应用程序安装期间，默认情况下会安装应用程序保护组件。

安装期间出现的 Enable app protection（启用应用程序保护）复选框将替换为 Start App Protection after installation（安装后启动应用程序保护）。

选中此复选框后，应用程序保护将在安装后立即启动。

> 注意：
>
> 如果您未启用此复选框，则对于有权使用应用程序保护的客户，应用程序保护会在首次启动受保护的资源或组件时自动启动。

您也可以使用 /`startappprotection` 命令行参数启动应用程序保护组件。但是，先前的 /`includeappprotection` 开关已弃用。

> 注意：
>
> 以前，Citrix 身份验证和 Citrix Workspace 应用程序屏幕默认强制执行反屏幕捕获和反键盘记录功能。但是，自 2212 起，这些功能默认处于禁用状态，需要使用组策略对象进行配置。有关 GPO 配置的信息，请参阅应用程序保护配置的增强功能。

应用程序保护增强功能：屏幕截图检测和通知

自本版本起，当有人可能尝试对任何受保护的资源进行屏幕捕获时，您可以查看通知。有关受应用程序保护的资源的信息，请参阅应用程序保护什么？。

出现以下情况时会显示通知：

- 尝试通过屏幕捕获工具截取屏幕截图或录制视频。
- 尝试通过 Print Screen 键截取屏幕截图。

> 注意：
>
> 屏幕捕获工具的每个运行实例仅显示一次。如果您重新启动该工具并尝试捕获屏幕截图，该通知会再次出现。

Desktop Viewer 优化

此版本通过将启动时间缩短 5 秒来优化 Desktop Viewer 体验。Desktop Viewer 工具栏可快速打开，可能会显示默认的 Windows 会话登录屏幕。管理员可以通过将以下注册表配置为引入一些以毫秒为单位的延迟来隐藏这种体验：

- 位置：HKEY_CURRENT_USER\SOFTWARE\Citrix\XenDesktop\DesktopViewer
- 名称：ExtendConnectScreenMS
- 类型：DWORD
- 值：00000000（以毫秒为单位的延迟）

> 注意：
>
> 注册表配置是可选的。

Citrix Enterprise Browser

> 注意：
>
> 在适用于 Windows 的 Citrix Workspace 应用程序版本 2210 中，通过 **Citrix Enterprise Browser** 打开所有 **Web** 和 **SaaS** 应用程序功能处于禁用状态。

本版本包括基于 Chromium 版本 107 的 Citrix Enterprise Browser 版本 107.1.1.13。有关 Citrix Enterprise Browser 的详细信息，请参阅 Citrix Enterprise Browser 文档。

- 将 **Citrix Enterprise Browser** 设置为工作浏览器

  现在，您可以将 Citrix Enterprise Browser 配置为工作浏览器以打开所有工作链接。您可以选择使用备用浏览器打开非工作链接。

工作链接是与管理员为最终用户配置的 Web 或 SaaS 应用程序关联的链接。当用户单击本机应用程序中的任何链接时，如果它是工作链接，则会通过 Enterprise Browser 将其打开。如果不是，则通过最终用户选择的备用浏览器将其打开。

有关详细信息，请参阅将 Citrix Enterprise Browser 设置为工作浏览器。

2212 中已修复的问题

- 即使只存在一个证书，Citrix Workspace 应用程序也会提示您选择证书。向 Workspace（云）应用商店进行身份验证时会出现此问题。
  可以通过添加以下注册表来禁止显示此证书提示：

  On 32-bit systems:

  - Location: HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle or HKEY_CURRENT_USER\Software\Citrix\Da
  - Name: SuppressCertSelectionPrompt
  - Type: String
  - Value: True

  On 64-bit systems

  - Location: HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle or HKEY_CURRENT_USER\So
  - Name: SuppressCertSelectionPrompt
  - Type: String
  - Value: True

  [CVADHELP-20844]
- 当 VPN 断开连接或重新连接时，尝试访问适用于 Windows 的 Citrix Workspace 应用程序可能会失败 [CVADHELP-20376]
- 对配置了 EPA 的应用商店进行身份验证时无法检测到端点分析 (EPA)。当您将 Citrix Workspace 应用程序从早期版本更新到 2210 或更高版本时会出现此问题。[CVADHELP-21387]
- 在优化的 Microsoft Teams 通话期间，端点可能会进入睡眠状态。[HDX-44438]
- Citrix Analytics 无法从最终用户处接收与网络相关的指标。即使满足以下必备条件，也会出现此问题：
  - 使用 Citrix Workspace 应用程序，应用程序或桌面会话处于运行状态的时间超过 15 分钟。
  - 使用的应用商店或帐户已启用 CAS。

  > 注意：
  >
  > 在基于浏览器启动应用程序或桌面时，不会发送与网络相关的 CAS 事件。仅当您通过 Web 打开应用程序或桌面以及通过本机 Citrix Workspace 应用程序添加的同一个应用商店时，才会发送该应用程序。

  [CVADHELP-21448]
- 在无缝模式下打开已发布的应用程序时，其他本地应用程序或无缝应用程序可能会出现在前台并覆盖已发布的应用程序。[CVADHELP-20742]

2210.5

新增功能

此版本解决了有助于改进整体性能、安全性和稳定性的问题。

客户端应用程序管理 [技术预览版]

适用于 Windows 的 Citrix Workspace 应用程序 2210.5 现在提供客户端应用程序管理功能，使 Citrix Workspace 应用程序成为端点安装和管理 Secure Access Agent 和端点分析 (EPA) 插件等代理所需的单个客户端应用程序。

借助此功能，管理员可以轻松地从单个管理控制台部署和管理所需的代理。

注意：此功能仅适用于 Workspace（云）会话。

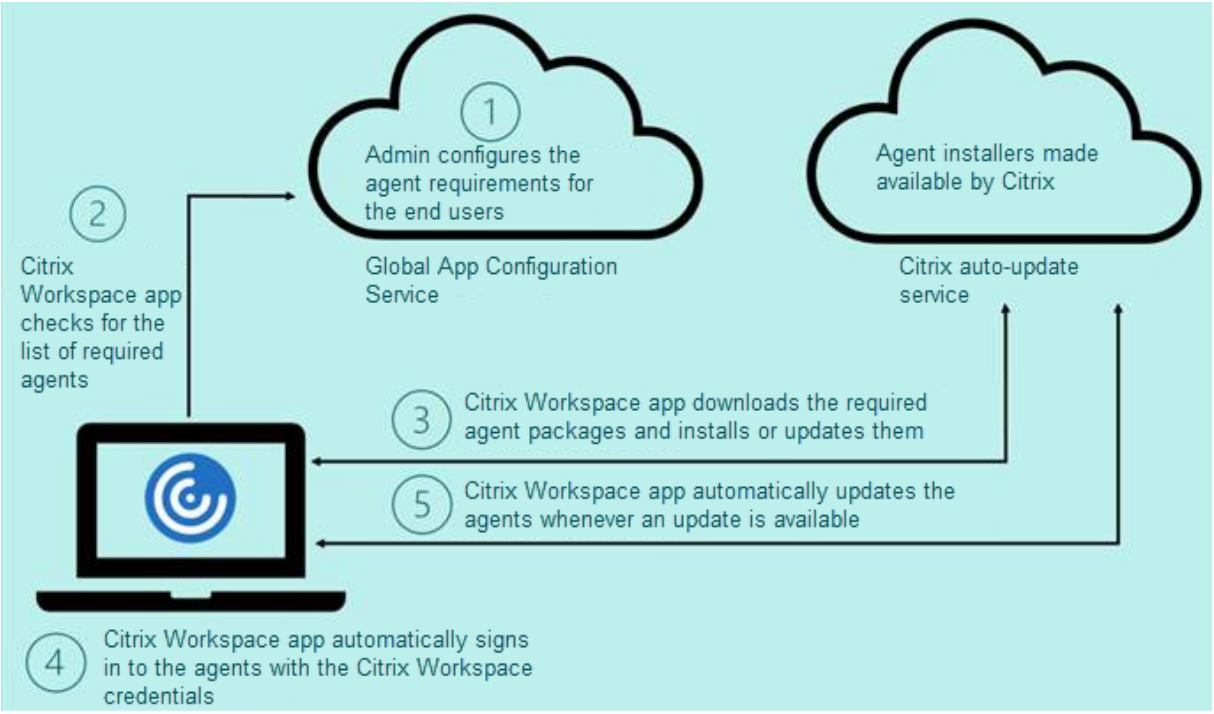
客户端应用程序管理包括以下步骤：

- 管理员必须在 Global App Configuration Service 中指定最终用户设备上所需的代理。通过此技术预览版，管理员可以指定 Secure Access Agent 和端点分析 (EPA) 代理。
- Citrix Workspace 应用程序从 Global App Configuration Service 获取代理列表。
- 根据从 Global App Configuration Service 获取的列表，Citrix Workspace 应用程序通过自动更新服务下载代理软件包。如果之前未在端点上安装代理，Citrix Workspace 应用程序将触发代理的安装。如果已安装代理，Citrix Workspace 应用程序会触发代理更新（如果下载的代理版本高于安装的版本）。

Citrix Workspace 应用程序可确保在将来有更新时自动更新代理。

Citrix Workspace 应用程序使用 Citrix Workspace 凭据自动登录代理。

下图说明了工作流程：



可以使用 Podio 表单注册此技术预览版。提交申请，我们将与您联系以获取更多详细信息。

> 注意：
>
> 技术预览版可供客户在其非生产环境或有限生产环境中进行测试，并为客户提供共享反馈的机会。Citrix 不接受功能预览版的支持案例，但欢迎提供改进这些功能的反馈。Citrix 可能会根据反馈的严重性、紧迫性和重要性对反馈执行操作。建议不要在生产环境中部署 Beta 版本。

自动更新的增强功能

Citrix Workspace 应用程序现在支持在启用了代理自动配置 (PAC) 和 Web 代理自动发现协议 (WPAD) 检测时自动更新。

Citrix Enterprise Browser

本版本包括基于 Chromium 版本 105 的 Citrix Enterprise Browser 版本 105.2.1.40。有关 Citrix Enterprise Browser 的详细信息，请参阅 Citrix Enterprise Browser 文档。

已修复的问题

此版本解决了有助于改进整体性能、安全性和稳定性的问题。

2210

新增功能

面向网络摄像机重定向的背景模糊

适用于 Windows 的 Citrix Workspace 应用程序现在支持面向网络摄像机重定向的背景模糊。您可以通过选中首选项 > 连接 > 启用背景模糊复选框来启用此功能。

适用于 **Windows 11** 上的 **Web** 和 **SaaS** 应用程序的应用程序保护增强功能

此应用程序保护增强功能优化了 Windows 11 上的 Web 和 SaaS 应用程序用户的体验和安全功能。此增强功能可以通过面向 Secure Private Access 客户的 Citrix Enterprise Browser 获得。

本地应用程序保护 **[**技术预览版**]**

应用程序保护提供增强的安全性，保护我们的客户免受键盘记录器、端点意外和恶意屏幕截图的侵害。目前，应用程序保护功能仅针对 Workspace 资源提供。借助本地应用程序保护，应用程序保护功能扩展到端点上的本地应用程序。自适用于 Windows 的 Citrix Workspace 应用程序 2210 起，应用程序保护可以应用到 Windows 设备上的本地应用程序。

可以使用此 Podio 表单注册此技术预览版。

> 注意：
>
> 技术预览版可供客户在其非生产环境或有限生产环境中进行测试，并为客户提供共享反馈的机会。Citrix 不接受功能预览版的支持案例，但欢迎提供改进这些功能的反馈。Citrix 可能会根据反馈的严重性、紧迫性和重要性对反馈执行操作。建议不要在生产环境中部署 Beta 版本。

限制视频分辨率

让用户使用性能较低的客户端端点的管理员可以选择限制传入或传出的视频分辨率，以减少编码和解码视频对这些端点产生的影响。自适用于 Windows 的 Citrix Workspace 应用程序 2010 起，您可以使用客户端配置选项限制这些分辨率。

> 注意：
>
> 以受限分辨率运行的用户会影响会议的整体视频质量，因为 Microsoft Teams 服务器会被迫对所有会议参与者使用最小公分母分辨率。

默认情况下，安装了 Citrix Workspace 应用程序 2210 的客户端上禁用呼叫限制。管理员必须在 HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream 中设置以下客户端配置，才能将其启用：

名称	类型	强制	接受的值
EnableSimulcast	整数	是	1-3（将其设置为 1）
MaxOutgoingResolution	整数	是	180、240、360、540、720、1080（Microsoft Teams 支持的分辨率）
MaxIncomingResolutio	整数	是	180、240、360、540、720、1080（Microsoft Teams 支持的分辨率）
MaxIncomingStreams	整数	是	1–8
MaxSimulcastLayers	整数	是	1-3（将其设置为 1）
MaxVideoFrameRate	整数	否	1–30
MaxScreenshareFrameI	整数	否	1–15

所有注册表项都为 DWORD。

Citrix Enterprise Browser

本版本包括基于 Chromium 版本 105 的 Citrix Enterprise Browser 版本 105.1.1.27。有关 Citrix Enterprise Browser 的详细信息，请参阅 Citrix Enterprise Browser 文档。

重命名 **Citrix Workspace Browser**

Citrix Workspace Browser 现在称为 Citrix Enterprise Browser。自定义架构现已从 citrixworkspace:// 更改为 citrixbrowser://。

在我们的产品及其文档中实现此转换是一个正在进行的过程。感谢您在此转换期间耐心等待。

- 产品 UI、产品中内置的内容以及产品文档中的图像和说明将在接下来的几周内更新。
- 某些项目（例如命令和 MSI）可能会继续保留以前的名称，以防止损坏客户的现有脚本。
- 相关产品文档以及从此产品文档链接的其他资源（例如视频和博客文章）可能仍包含以前的名称。

将 **Citrix Enterprise Browser** 设为工作浏览器 **[**技术预览版**]**

现在，您可以将 Citrix Enterprise Browser 配置为打开管理员在 Citrix Workspace 应用程序中配置的所有工作或企业链接和应用程序。此功能为您提供了一种在 Citrix Enterprise Browser 中仅打开工作链接或 Web 和 SaaS 应用程序的方法。
您可以选择使用备用浏览器打开任何其他非工作链接或应用程序。

通过 **Citrix Enterprise Browser** 打开所有 **Web** 和 **SaaS** 应用程序

自本版本起，Citrix Workspace 应用程序中可用的所有内部 Web 应用程序和外部 SaaS 应用程序都将在 Citrix Enterprise Browser 中打开。

> 注意：
>
> 在适用于 Windows 的 Citrix Workspace 应用程序版本 2210 中，通过 **Citrix Enterprise Browser** 打开所有 **Web** 和 **SaaS** 应用程序功能处于禁用状态。

支持浏览器扩展 **[**技术预览版**]**

您可以以安全的方式将管理员提供的扩展程序添加到 Citrix Enterprise Browser。管理员可以部署、管理和控制扩展程序。最终用户可以根据需要在 citrixbrowser://extensions 下查看和使用该扩展程序。有关更多设置，请参阅 Global App Configuration Service。

> 注意：
>
> 此功能是仅限请求的预览版。要在您的环境中将其启用，请填写 Podio 表单。

有关如何配置的信息，请参阅 Citrix Enterprise Browser 文档。

使用 **Global App Config Service** 管理 **Citrix Enterprise Browser [**技术预览版**]**

管理员可以使用适用于 Citrix Workspace 的 Global App Configuration Service，通过集中管理的服务提供 Citrix Enterprise Browser 设置。

Global App Configuration Service 旨在让管理员轻松配置 Citrix Workspace 和管理 Citrix Workspace 应用程序设置。此功能允许管理员使用 Global App Configuration Service 将各种设置或系统策略应用到特定应用商店中

的 Citrix Enterprise Browser。管理员现在可以使用 Global App Configuration Service 配置和管理以下 Citrix Enterprise Browser 设置：

- “Enable CWB for all apps”（为所有应用程序启用 CWB）- 将 Citrix Enterprise Browser 设为用于从 Citrix Workspace 应用程序打开 Web 和 SaaS 应用程序的默认浏览器。
- “Enable save passwords”（启用保存密码）- 允许或拒绝最终用户保存密码。
- “Enable incognito mode”（启用隐身模式）- 启用或禁用隐身模式。
- “Managed Bookmarks”（托管书签）- 允许管理员将书签推送到 Citrix Enterprise Browser。
- “Enable developer tools”（启用开发人员工具）- 在 Enterprise Browser 中启用或禁用开发人员工具。
- “Delete browsing data on exit”（退出时删除浏览数据）- 允许管理员配置 Citrix Enterprise Browser 在退出时删除哪些数据。
- “Extension Install Force list”（强制安装扩展程序列表）- 允许管理员在 Citrix Enterprise Browser 中安装扩展程序。
- “Extension Install Allow list”（扩展程序安装允许列表）- 允许管理员配置用户可以添加到 Citrix Enterprise Browser 的扩展程序的允许列表。此列表利用了 Chrome 网上应用店。

> 备注：
>
> - 此功能是仅限请求的预览版。要在您的环境中将其启用，请填写 Podio 表单。
> - 技术预览版可供客户在其非生产环境或有限生产环境中进行测试，并为客户提供共享反馈的机会。Citrix 不接受功能预览版的支持案例，但欢迎提供改进这些功能的反馈。Citrix 可能会根据反馈的严重性、紧迫性和重要性对反馈执行操作。建议不要在生产环境中部署 Beta 版本。
> - 名称和值对区分大小写。
> - Global App Configuration Service 中的所有浏览器设置都属于以下类别：

```
{

    "category": "browser",
    "userOverride": false,
    "assignedTo": [
    "AllUsersNoAuthentication"
    ]
 }


<!--NeedCopy-->
```

> - 管理员也可以将这些设置应用到非托管设备。有关详细信息，请参阅 Global App Configuration Service 文档。

已修复的问题

- 重新引入了高级首选项下的高 **DPI** 菜单。

- 默认的新值为否，使用本机分辨率，也称为 DPI 匹配。

  选择此选项时，Citrix Workspace 应用程序会尝试自动将本地 Windows 客户端的显示分辨率和 DPI 缩放设置与 HDX 会话进行匹配。建议在所有情况下都使用 DPI 匹配，尤其是在使用高分辨率显示器（1920x1080 以上）时。

- 是选项（也称为客户端扩展或兼容模式）仅推荐用于非 DPI 感知的旧版应用程序，并且只能在特殊情况下使用。此选项可能会在显示旧版应用程序时引入一些副作用，例如因 HDX 会话放大或拉伸而导致的文本模糊。

  当两台具有不同 DPI 设置（或混合 DPI）的显示器连接到本地 Windows 客户端时，这也是一个可行的选项。

  > 注意：
  >
  > 此选项与 Microsoft Teams 的 HDX 优化不兼容。

- 使用第三个选项允许操作系统缩放分辨率（也称为 “DPI 无感知”），适用于 Windows 的 Citrix Workspace 应用程序会忽略本地 Windows 客户端上的 DPI 缩放设置。在此模式下，Windows 操作系统需要管理 Workspace 应用程序和 HDX 会话的扩展，就像管理任何其他非 DPI 感知的应用程序一样。不建议在 DPI 缩放比例超过 100% 的情况下使用此模式。

[HDX-43720]

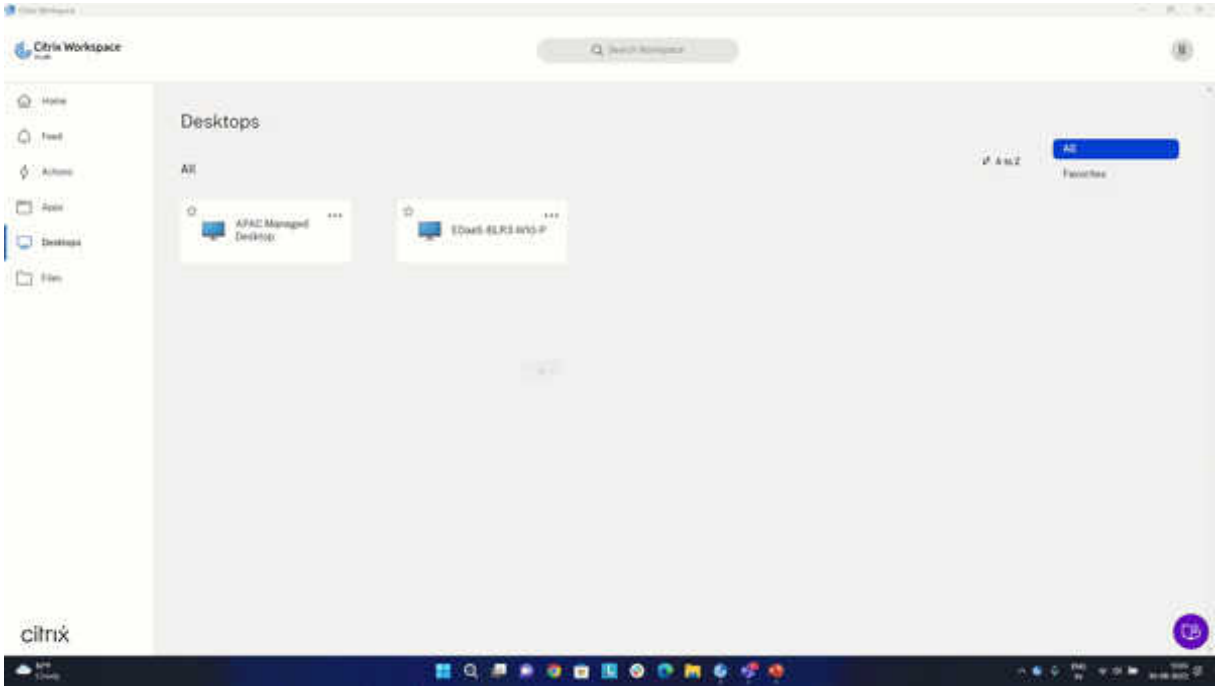
- 当您通过 GPO 添加已禁用的应用商店并通过 GUI 添加来自同一 StoreFront 服务器的其他应用商店时，可能会出现一个加载屏幕，添加帐户可能会失败。[CVADHELP-20776]
- 当您通过 GPO 从同一 StoreFront 服务器添加两个应用商店时，配置第二个应用商店可能会间歇性失败。[CVADHELP-20655]
- 即使通过 GPO 禁用了 Global App Config Service 策略，Citrix Workspace 应用程序也会尝试连接到 Global App Config 服务器。[CVADHELP-20775]
- 在 Windows 2106 或更高版本中使用 Citrix Workspace 应用程序时，出站 ICA 代理功能可能不起作用。[CVADHELP-20824]
- 对于域用户，receiver.exe 进程可能会意外失败。您可能会在适用于 Windows 的 Citrix Workspace 应用程序 2206 或更高版本上看到此问题。[CVADHELP-20986]
- 在经过优化的 Microsoft Teams 视频会议中，在开启视频的情况下加入通话，您可能会看到通话中断。此问题偶尔出现，也会在客户端上 HdxRtcEngine.exe 进程失败时出现。[CVADHELP-21095]

2209

新增功能

快速启动断开连接的桌面 **[技术预览版]**

通过启用此功能，您可以立即打开以前断开连接的桌面。启用此功能后，Citrix Workspace 应用程序将在隐藏模式下启动断开连接的会话。启动桌面后，会话将立即显示。



> 注意：
>
> 这仅适用于 Workspace（云）会话。

可以使用 Podio 表单注册此技术预览版。

> 注意：
>
> 技术预览版可供客户在其非生产环境或有限生产环境中进行测试，并为客户提供共享反馈的机会。Citrix 不接受功能预览版的支持案例，但欢迎提供改进这些功能的反馈。Citrix 可能会根据反馈的严重性、紧迫性和重要性对反馈执行操作。建议不要在生产环境中部署 Beta 版本。

自动更新版本控制 [技术预览版]

管理员现在可以管理组织中的设备的自动更新版本。

管理员可以通过在 Global App Config Service 中设置 maximumAllowedVersion 和 minimumAllowedVersion 属性中的范围来控制版本。

Global App Config Service 中的示例 JSON 文件：

```
"AutoUpdate": {

"userOverride": false,
"AutoUpdatePluginsSettings": [
    {

    "pluginSettings": {

```



```
        "upgradeToLatest": false,
        "maximumAllowedVersion": "22.9.0.3934",
        "minimumAllowedVersion": "22.9.0.3934",
            }
  ,
     "pluginName": "WorkspaceApp",
     "pluginId": "1CDF566D-B2C7-47CA-802F-6283C862E1D6"
    }


<!--NeedCopy-->
```

设置范围时，用户设备上的 Citrix Workspace 应用程序会自动更新到介于上述范围之间的最高可用版本。

如果要将 Citrix Workspace 应用程序自动更新到特定版本，请在 Global App Config Service 的 maximumAllowedVersion 和 minimumAllowedVersion 属性中输入相同的版本。

> 注意：
>
> - 要实现自动更新版本控制，必须将 Global App Config Service 中的 upgradeToLatest 设置设为 false。如果设置为 true，maximumAllowedVersion 和 minimumAllowedVersion 将被忽略。
> - 请勿修改 pluginId，因为它已映射到 Citrix Workspace 应用程序。
> - 如果管理员尚未在 Global App Config Service 中配置版本，则默认情况下，Citrix Workspace 应用程序将更新到最新的可用版本。

启用该功能：

1. 启动注册表编辑器。
2. 导航到 `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle` 注册表路径。
3. 创建具有以下属性的注册表值：
   - 注册表项名称：Test-EnableAUVersionControl
   - 类型：DWORD
   - 值：0 表示已禁用，大于 0 表示已启用
4. 重新启动 Citrix Workspace 应用程序以使所做的更改生效。

可以通过 Podio 表单提供有关此功能的反馈。

> 注意：
>
> 技术预览版可供客户在其非生产环境或有限生产环境中进行测试，并为客户提供共享反馈的机会。Citrix 不接受功能预览版的支持案例，但欢迎提供改进这些功能的反馈。Citrix 可能会根据反馈的严重性、紧迫性和重要性对反馈执行操作。建议不要在生产环境中部署 Beta 版本。

WebRTC 的升级版，适用于经过优化的 **Microsoft Teams**

用于优化的 Microsoft Teams 的 WebRTC 版本已升级到版本 M98。

支持在 **VDA** 上自动更新 **Citrix Workspace** 应用程序

现在，您可以通过创建以下注册表值在 VDA 上启用自动更新功能：

在 32 位计算机上：

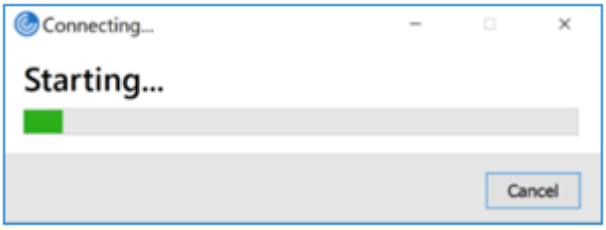
- 注册表项：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\AutoUpdate
- 注册表值：AllowAutoUpdateOnVDA
- 注册表类型：REG_SZ
- 注册表数据：True

在 64 位计算机上：

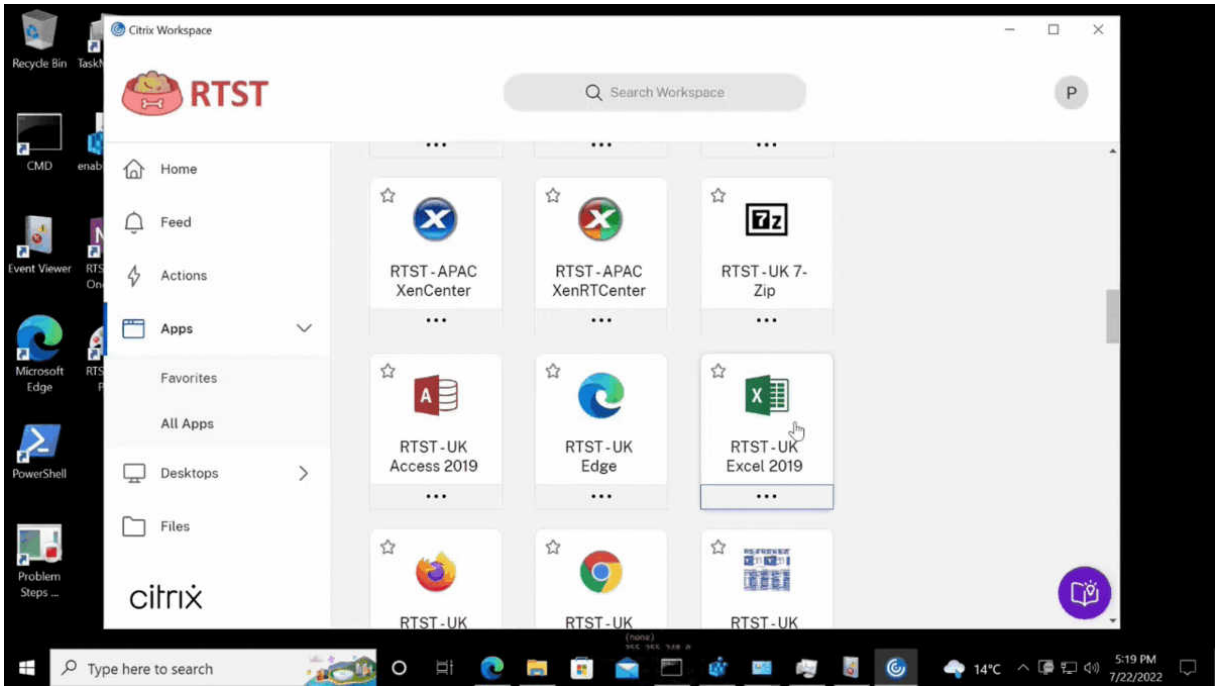
- 注册表项：HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\AutoUpdate
- 注册表值：AllowAutoUpdateOnVDA
- 注册表类型：REG_SZ
- 注册表数据：True

改善了虚拟应用程序和桌面的启动体验 [技术预览版]

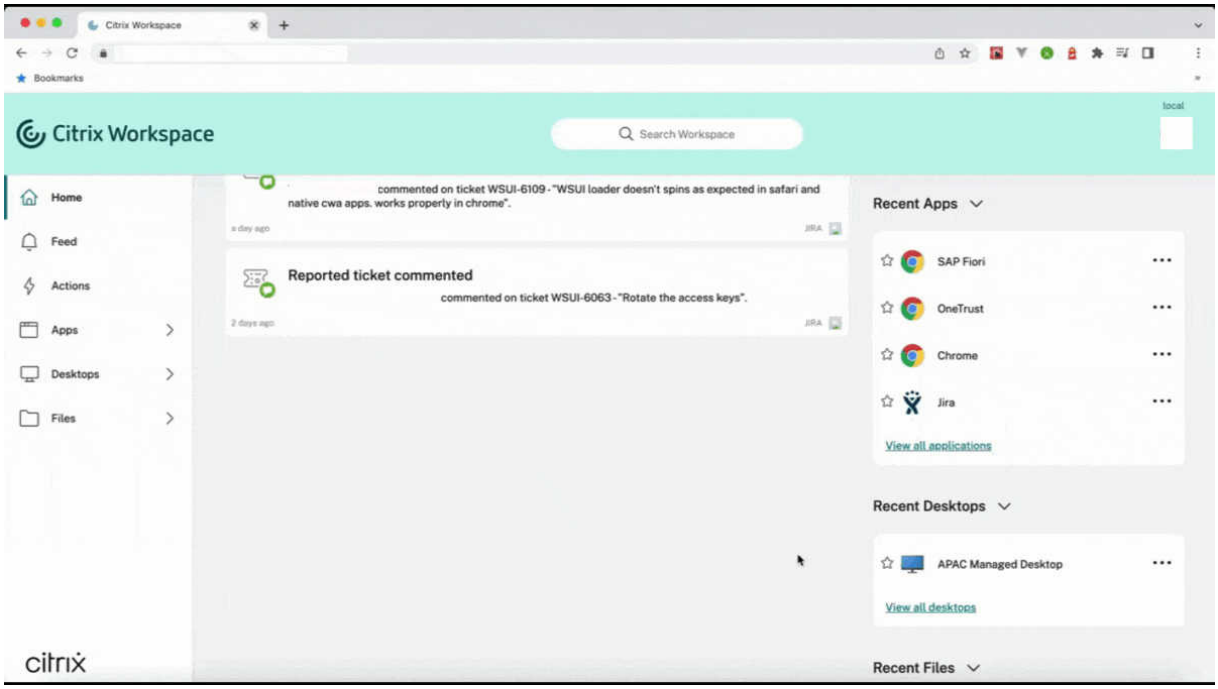
以前，启动进度对话框对用户来说不直观。它使用户假设启动过程没有响应，并且用户关闭了对话框，因为通知消息是静态的。



改进后的应用程序和桌面启动体验信息更丰富、更新式，并且在适用于 Windows 的 Citrix Workspace 应用程序上提供了用户友好的体验。这有助于让用户及时了解有关启动状态的相关信息。通知显示在屏幕的右下角。



适用于 Web 的 Workspace 也支持此功能。用户可以查看有关启动进度的有意义的通知，而不仅仅是微调器。如果正在启动并且用户尝试关闭浏览器，则会显示一条警告消息。



可以使用以下注册表启用此功能。

1. 打开注册表编辑器。
2. 导航到 `HKLM\SOFTWARE\WOW6432Node\Citrix\Dazzle`。
3. 创建并添加一个名为 NewLaunchExpSupport 的注册表字符串，然后将其值设置为 True。

4. 重新启动 Citrix Workspace 应用程序以使所做的更改生效。

> 注意：
>
> 这仅适用于 Workspace（云）会话。

已知问题：

- 在多显示器设置中，Citrix Workspace 应用程序的桌面会话中的应用程序窗口移至不同的显示器。当您断开并重新连接会话时会出现此问题。
- 基于浏览器的启动不支持此功能。

可以通过 Podio 表单提供有关此功能的反馈。

> 注意：
>
> 技术预览版可供客户在其非生产环境或有限生产环境中进行测试，并为客户提供共享反馈的机会。Citrix 不接受功能预览版的支持案例，但欢迎提供改进这些功能的反馈。Citrix 可能会根据反馈的严重性、紧迫性和重要性对反馈执行操作。建议不要在生产环境中部署 Beta 版本。

Citrix Enterprise Browser（以前称为 **Citrix Workspace Browser**）

本版本包括基于 Chromium 版本 103 的 Citrix Enterprise Browser 版本 103.2.1.10。有关 Citrix Enterprise Browser 的详细信息，请参阅 Citrix Enterprise Browser 文档。

- **Citrix Enterprise Browser** 配置文件

  配置文件可帮助您将每个 Citrix Workspace 帐户的个人信息（例如历史记录、书签、密码和其他设置）分开保存。基于您的 Workspace 应用商店创建配置文件，使您能够获得独特且个性化的浏览体验。

  > 注意：
  >
  > 升级到版本 103.2.1.10 并首次登录设备后，只有您之前保存的密码会被删除。首次使用其他应用商店登录设备时，之前保存的所有数据都将丢失。

已修复的问题

- 应用此修复后，当您从适用于 Windows 的 Citrix Workspace 应用程序中注销时，会显示一个特定于本地应用商店的登录页面。

  要启用此修复，请设置以下注册表值：

  在 32 位系统中：

  - HKEY_LOCAL_MACHINE/Software/Citrix/Dazzle
  - 名称：ShowSignInPageOnLogOff
  - 类型：REG_SZ
  - 值：True

  在 64 位系统上：

- HKEY_LOCAL_MACHINE/Software/Wow6432Node/Citrix/Dazzle
- 名称：ShowSignInPageOnLogOff
- 类型：REG_SZ
- 值：True

[CVADHELP-19967]

- 组策略对象中的 Applocker 规则阻止 Citrix Gateway 插件与 Citrix Workspace 的集成。因此，系统会在 temp 文件夹中创建多个格式为 VPNXXXX.tmp 的临时文件。即使注册表项 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client 的值为 DisableIconHide，也会创建这些文件。[CVADHELP-19709]
- 当您通过 PNAgent 站点启动已发布的应用程序时，适用于 Windows 的 Citrix Workspace 应用程序会显示以下消息：

  发生致命错误。

  [RFWIN-28208]
- Citrix Workspace 应用程序在启动后可能无法响应。{CVADHELP-20317]

2207

新增功能

使用 **HDX** 进行的 **Microsoft Teams** 优化的背景模糊和效果

适用于 Windows 的 Citrix Workspace 应用程序现在支持使用 HDX 进行的 Microsoft Teams 优化中的背景模糊和效果。

您可以模糊背景或者使用自定义图像替换背景，并通过帮助对话专注于轮廓（身体和面部）来避免意外干扰。该功能可用于 P2P 或电话会议。

> 注意：
>
> 此功能现在已与 Microsoft Teams UI/按钮集成。多窗口支持是要求 VDA 更新到 2112 或更高版本的必备条件。有关详细信息，请参阅多窗口会议和聊天。

限制：

- 不支持管理员和用户定义的背景替换。
- 背景效果不会在会话之间持续存在。当您关闭并重新启动 Microsoft Teams 或重新连接 VDA 时，背景效果将重置为关闭。
- 重新连接 ICA 会话后，效果将关闭。但是，Microsoft Teams UI 显示一个对勾，指示之前的效果仍处于启用状态。Citrix 和 Microsoft 正在共同努力解决此问题。
- 更换背景图像时，设备必须连接到 Internet。

> 注意：
>
> 此功能仅在 Microsoft Teams 推出将来的更新后可用。Microsoft 推出此更新时，请查看 CTX253754 和 Microsoft 365 Public roadmap（Microsoft 365 公开路线图）以获取文档更新和公告。

面向网络摄像机重定向的背景模糊 [技术预览版]

适用于 Windows 的 Citrix Workspace 应用程序现在支持面向网络摄像机重定向的背景模糊。可以使用以下注册表启用此功能：

- 位置：HKCU\Software\Citrix\HdxRealTime。
- 名称：EnableBackgroundEffectFilter。
- 类型：DWORD。
- 值：0 表示已禁用。任何其他值都表示已启用。如果该值不存在或者为 0，则会忽略所有背景模糊设置，并禁用处理模糊效果的首选项 > 连接 > 启用背景模糊复选框。

建议：

关闭 ICA 会话之前，请关闭 VDA 上的网络摄像机应用程序。

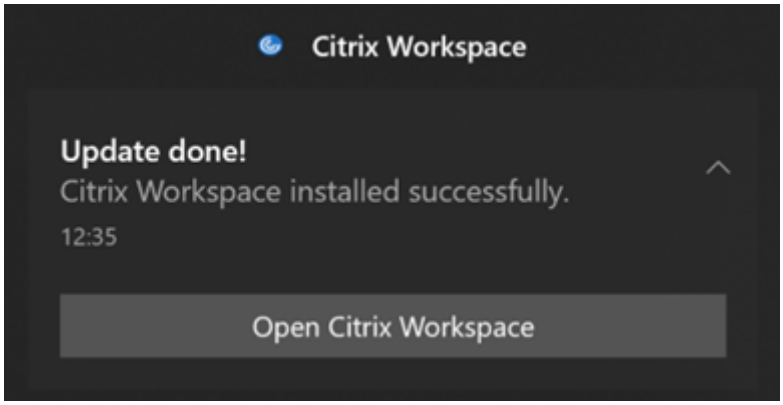
可以通过 Podio 表单提供有关此功能的反馈。

改进了自动更新体验

自动更新功能会自动将 Citrix Workspace 应用程序更新到最新版本，无需任何用户干预。

Citrix Workspace 应用程序会定期检查并下载该应用程序的最新可用版本。Citrix Workspace 应用程序根据用户活动确定最佳安装时间，以免造成任何中断。

安装完成后，将显示以下通知：



（无提示自动更新成功）

如果 Citrix Workspace 应用程序找不到在后台安装更新的正确时间，则会显示通知提示。

自动更新的增强功能 [技术预览版]

Citrix Workspace 应用程序现在支持在启用了代理自动配置 (PAC) 和 Web 代理自动发现协议 (WPAD) 检测时自动更新。

> 注意：
>
> 技术预览版可供客户在其非生产环境或有限生产环境中进行测试，并为客户提供共享反馈的机会。Citrix 不接受功能预览版的支持案例，但欢迎提供改进这些功能的反馈。Citrix 可能会根据反馈的严重性、紧迫性和重要性对反馈执行操作。建议不要在生产环境中部署 Beta 版本。

可以通过 Podio 表单提供有关此功能的反馈。

Citrix Enterprise Browser

本版本包括基于 Chromium 版本 102 的 Citrix Enterprise Browser 版本 102.1.1.14。

- 通过 **Citrix Enterprise Browser** 打开所有 **Web** 和 **SaaS** 应用程序 **[技术预览版]**

  自本版本起，Citrix Workspace 应用程序中可用的所有内部 Web 应用程序和外部 SaaS 应用程序都将在 Citrix Enterprise Browser 中打开。可以使用 Podio 表单注册此技术预览版。

  > 注意：
  >
  > 技术预览版可供客户在其非生产环境或有限生产环境中进行测试，并为客户提供共享反馈的机会。Citrix 不接受功能预览版的支持案例，但欢迎提供改进这些功能的反馈。Citrix 可能会根据反馈的严重性、紧迫性和重要性对反馈执行操作。建议不要在生产环境中部署 Beta 版本。

有关 **Citrix Workspace** 应用程序更新的注意事项

将适用于 Windows 的 Citrix Workspace 应用程序从早期版本更新到 2207 时，系统会提示用户登录。只有 Workspace 应用商店才会提示登录。

已修复的问题

会话/连接

- 优化的 Microsoft Teams 可能不会选择连接到端点的新默认音频设备。[CVADHELP-20528]

  > 注意：
  >
  > 此修复仅在 Microsoft Teams 推出将来的更新后可用。

- 如果您在 Citrix Workspace 应用程序安装期间设置了 AllowAddStore=N，则通过组策略对象或命令行使用 geo DNS URL 配置应用商店可能会失败。[CVADPHELP-19853]
- Citrix 身份验证管理器 (AuthManSvr.exe) 可能会在登录期间意外退出。[CVADHELP-18901]

用户界面

- 使用自定义 Web 应用商店时，Citrix Workspace 应用程序中的链接将在系统浏览器中打开。[RFWIN-27855]

2206

新增功能

使用 **HDX** 进行的 **Microsoft Teams** 优化的背景模糊和效果 **[技术预览版]**

在适用于 Windows 的 Citrix Workspace 应用程序 2206 中，Citrix 引入了使用 HDX 进行的 Microsoft Teams 优化中的背景模糊和效果的技术预览版。

现在，您可以模糊背景或使用自定义图像替换背景，并通过帮助对话专注于轮廓（身体和面部）来避免意外干扰。该功能可用于 P2P 或电话会议。

> 注意：
>
> - 在此技术预览版中，该功能只能通过注册表项进行控制，并且未与 Microsoft Teams 用户界面/按钮集成。
> - 新背景在所有 Microsoft Teams 会议和通话中都将保留，直到您通过注册表项再次对其进行更改为止。要使更改生效，只能重新启动 Microsoft Teams。该功能正式发布后，此限制删除，为此，它需要多窗口支持（VDA 2112 或更高版本）。
>
> 要激活或停用背景模糊和效果，管理员或用户必须在客户端/端点上配置以下注册表项：

位置：`HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream`

- 名称：VideoBackgroundEffect
- 类型：DWORD
- 值：0（已禁用）、1（已启用）、2（背景图像替换，也需要存在 **VideoBackgroundImage** 注册表项）

仅当您想要替换背景图像而非模糊背景时，才需要以下注册表项：

- 名称：VideoBackgroundImage
- 类型：REG_SZ
- 值：my_image_name.jpeg

> 注意：
>
> 文件名，例如 my_image_name.jpg（或者您为文件提供的名称）必须放置在用户设备上的 Citrix Workspace 应用程序安装目录 `C:\Program Files (x86)\Citrix\ICA Client` 中。

改善了图形性能

Citrix Workspace 应用程序 2206 为 Intel 集成 GPU 提供了显著的性能改进

- 图形 CPU 占用量已降低，提高了整体性能。

修复了以下问题：

- 在 Intel 第 10 代 GPU 或更高版本上播放视频后每秒帧数较低。
- Intel 和 AMD GPU 上的“无损构建”或“针对主动变化的区域”的亮度差异。

应用程序保护的增强功能：反代码注入 [技术预览版]

Citrix Workspace 应用程序现在可确保任何未经授权的动态链接库 (DLL) 或不受信任的模块都无法访问会话。

如果在会话期间注入了任何不受信任的模块，Citrix Workspace 应用程序都会检测到此类干预并停止加载该模块。

此外，如果在会话启动之前检测到任何不受信任或恶意的 DLL，应用程序保护会阻止会话启动并显示错误消息。关闭错误消息将退出虚拟应用程序和桌面会话。

可以使用此 Podio 表单注册此技术预览版。

> 注意：
>
> 技术预览版可供客户在其非生产环境或有限生产环境中进行测试，并为客户提供共享反馈的机会。Citrix 不接受功能预览版的支持案例，但欢迎提供改进这些功能的反馈。Citrix 可能会根据反馈的严重性、紧迫性和重要性对反馈执行操作。建议不要在生产环境中部署 Beta 版本。

适用于 **Windows 11** 上的 **Web** 和 **SaaS** 应用程序的应用程序保护增强功能 [技术预览版]

此应用程序保护增强功能优化了 Windows 11 上的 Web 和 SaaS 应用程序用户的体验和安全功能。此增强功能可以通过面向 Secure Private Access 客户的 Citrix Enterprise Browser 获得。您可以通过 Podio 表单注册技术预览版。有关详细信息，请参阅应用程序保护。

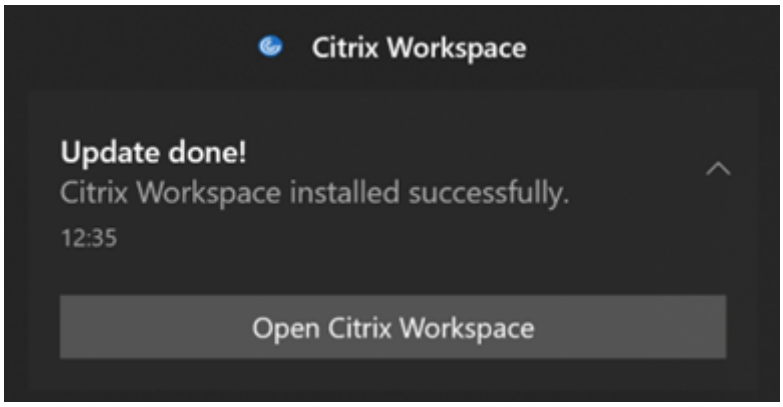
> 注意：
>
> 技术预览版可供客户在其非生产环境或有限生产环境中进行测试，并为客户提供共享反馈的机会。Citrix 不接受功能预览版的支持案例，但欢迎提供改进这些功能的反馈。Citrix 可能会根据反馈的严重性、紧迫性和重要性对反馈执行操作。建议不要在生产环境中部署 Beta 版本。

改进了自动更新体验 [技术预览版]

自动更新功能会自动将 Citrix Workspace 应用程序更新到最新版本，无需任何用户干预。

Citrix Workspace 应用程序会定期检查并下载该应用程序的最新可用版本。Citrix Workspace 应用程序根据用户活动确定最佳安装时间，以免造成任何中断。

安装完成后，将显示以下通知：



（无提示自动更新成功）

如果 Citrix Workspace 应用程序找不到在后台安装更新的正确时间，则会显示通知提示。

您可以通过 Podio 表单注册技术预览版。

> 注意：
>
> 技术预览版可供客户在其非生产环境或有限生产环境中进行测试，并为客户提供共享反馈的机会。Citrix 不接受功能预览版的支持案例，但欢迎提供改进这些功能的反馈。Citrix 可能会根据反馈的严重性、紧迫性和重要性对反馈执行操作。建议不要在生产环境中部署 Beta 版本。

启用 **DPI** 匹配

自适用于 Windows 的 Citrix Workspace 应用程序 2206 起，默认情况下会启用 DPI 匹配。这意味着 Citrix Workspace 应用程序会尝试自动将本地 Windows 客户端的显示分辨率和 DPI 缩放设置与 Citrix 会话进行匹配。作为此更改的一部分，Citrix Workspace 应用程序中的“高级首选项”下提供的“高 DPI”选项不再可用。有关详细信息，请参阅 Citrix 知识中心文章 CTX460068。

Citrix Enterprise Browser

本版本包括基于 Chromium 版本 101 的 Citrix Enterprise Browser 版本 101.1.1.12。有关 Citrix Enterprise Browser 中的功能或缺陷修复，请参阅 Citrix Enterprise Browser 文档中的新增功能。

已修复的问题

安装、卸载、升级

- Citrix Workspace Updater 服务可能无法启动，从而导致安装失败。当客户端未连接到 Internet 时会出现此问题。[CVADHELP-19613]

会话/连接

- 使用 Citrix Workspace 应用程序 2204.1 或更高版本时，会话可能会断开连接。如果存在运行未签名二进制文件（例如 wfica.ocx）的限制，则会出现此问题。[CVADHELP-20053]
- 添加应用商店 URL 后首次启动 Citrix Workspace 应用程序时，将显示以下错误消息：

  “您的 Citrix Workspace 应用程序在初始化 Microsoft Edge WebView2 时遇到错误。请重新启动您的应用程序。”

  当您通过 GPO 或命令行添加应用商店 URL 并在发现后包含“/”（例如，`https://sales.example.com/Citrix/Store/discovery/;On;Store`）时会出现此问题。

  [CVADHELP-20214]
- 在适用于 Windows 的 Citrix Workspace 应用程序中，使用组策略对象添加应用商店 URL 时，可能会显示以下错误消息：
  “无法连接到服务器”。

如果其中一个应用商店已禁用且无法访问，则会出现此问题。
[CVADHELP-19751]

- 从版本 2006 或更早版本更新 Citrix Workspace 应用程序时，可能会删除现有应用商店的网关和信标配置，并再次添加相同的配置，即使组策略对象中的应用商店配置未更改亦如此。[CVADHELP-19839]
- 尝试使用 Citrix Workspace 应用程序从平板电脑启动应用程序或桌面可能会失败。无法检索客户端 IP 地址时会出现此问题。[CVADHELP-19703]
- 在 Microsoft Teams 通话期间共享屏幕或应用程序时，您的对等方可能会看到视觉伪影。出现此问题是因为帧速率不稳定，例如视频播放不正确（冻结或瞬时黑帧）。此版本包括改进的帧速率或采样率，有助于减少视觉伪影。[HDX-38032]

用户界面

- 从自定义门户应用商店打开虚拟桌面时，**Desktop Viewer** 工具栏可能不可见。[CVADHELP-20253]
- 将适用于 Windows 的 Citrix Workspace 应用程序与浏览器内容重定向一起使用时，即使松开鼠标按钮，仍会继续调整浏览器窗口的大小。[HDX-38024]
- 在 DDC 上启用“自动显示键盘”策略后，会话期间可能不会显示电池状态通知和自动键盘弹出对话框。[HDX-39558]
- 插入 USB 设备或访问文件时，Citrix Workspace 应用程序可能会显示旧版 **Citrix Workspace -** 安全警告对话框。[LCM-10369]

服务连续性

- Citrix Workspace 应用程序启动可能会因为缺少租用文件而失败，导致出现 3002 错误。此版本包括改进功能，即仅当客户端同步服务器上存在的所有租用文件时，租用同步才会完成。[RFWIN-26540]

2205

新增功能

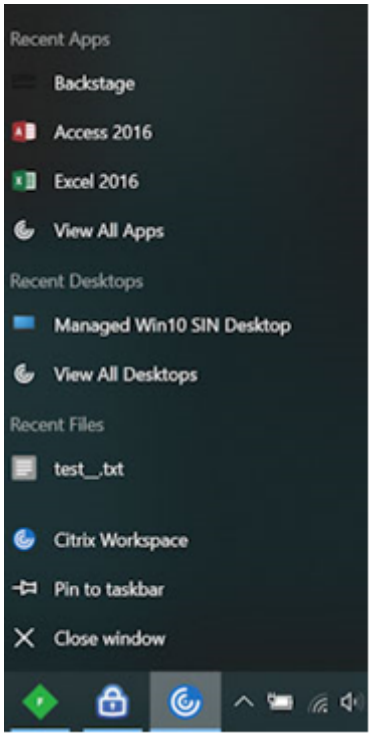
> 注意：
>
> 自本版本起，请确保 Microsoft Edge WebView2 Runtime 版本为 99 或更高版本。有关详细信息，请参阅系统要求和兼容性。

更改为 **Citrix Casting**

以前，Citrix Casting 在 Citrix Workspace 应用程序安装期间默认启用。自本版本起，仅当您在安装期间使用 `/IncludeCitrixCasting` 命令运行 Citrix Workspace 应用程序安装程序时，才会启用 Citrix Casting。
当您更新 Citrix Workspace 应用程序时，Citrix Casting 会自动更新。有关 Citrix Casting 的详细信息，请参阅 Citrix Casting。

快速访问资源

自本版本起，您可以快速访问最近使用过的应用程序、桌面和文件。右键单击任务栏中的 Citrix Workspace 应用程序图标，从弹出菜单中查看并打开最近使用过的资源。



在 **Citrix Workspace** 应用程序退出时注销自定义 **Web** 应用商店

当 `signoutCustomWebstoreOnExit` 属性设置为 True 时，关闭 Citrix Workspace 应用程序会使您退出自定义 Web 应用商店。可以在 **Global App Configuration Service** 中配置 `signoutCustomWebstoreOnExit` 属性。

有关详细信息，请参阅 Global App Configuration Service 文档。

支持在最大化模式下打开 **Workspace** 应用程序

自本版本起，您可以选择以最大化模式打开 Citrix Workspace 应用程序。可以在 Global App Configuration Service 中设置 `maximise workspace window` 属性，以使 Workspace 应用程序在默认情况下以最大化模式打开，代替每次都手动最大化 Citrix Workspace 应用程序。

有关 Global App Configuration Service 的详细信息，请参阅入门。

Workspace 支持 **Storebrowse**

适用于 Windows 的 Citrix Workspace 应用程序现在为自助服务提供 Storebrowse 支持，这使 Storebrowse 用户能够访问云和 Workspace 功能。

> 注意：
>
> - 此功能仅为单点登录提供 Storebrowse 支持。
> - 必须具备系统要求和兼容性中提到的必备条件才能使用此功能。

有关详细信息，请参阅 适用于 Workspace 的 Storebrowse。

Citrix Enterprise Browser

- 此版本包括基于 Chromium 版本 99 的 Citrix Enterprise Browser 版本 99.1.1.8,。有关 Citrix Enterprise Browser 中的功能或缺陷修复，请参阅 Citrix Enterprise Browser 文档中的新增功能。
- 现在，当您在 Citrix Workspace 应用程序中执行以下任何操作时，Citrix Workspace 应用程序会提醒您关闭活动浏览器窗口：
  - 从应用商店注销
  - 切换到其他应用商店
  - 添加新应用商店
  - 删除当前应用商店

已修复的问题

用户界面

- 在适用于 Windows 的 Citrix Workspace 应用程序中，非管理员用户可能无法通过高级首选项对话框禁用数据收集设置。[RFWIN-26795]

会话/连接

- 当您重新启动 Microsoft Teams 时，现有的 HdxRtcEngine.exe 进程可能不会关闭，并且可能会启动一个新进程。[HDX-40006]
- 在使用 Microsoft Teams HDX 优化的点对点通话期间，应用程序窗口共享可能会在大量重复开始/停止共享后无法停止，并且在重新启动 Citrix Workspace 应用程序之前，您可能无法共享桌面屏幕或应用程序窗口、呼叫或接听来电。[HDX-39549]
- 在使用 Microsoft Teams HDX 优化的“授予控制权”会话期间，远程光标的绘制与其实际位置略有偏移。[HDX-36376]
- 首次使用适用于 Windows 的 Citrix Workspace 应用程序版本 2112 或更高版本访问 VDA 时，可能会显示以下安全消息：

  联机应用程序正在尝试访问连接到您的计算机 **HDX** 文件访问的设备上存储的信息。

  在早期版本中，此消息仅在首次访问交付组中的每个已发布资源时出现，而不是每个 VDA。

  [CVADHELP-19636]

安装、卸载、升级

- 升级适用于 Windows 的 Citrix Workspace 应用程序时，可能会创建以下额外的注册表项：

  `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\WOW6432Node\Citrix`

  配置自动更新命令行策略时会出现此问题。

  `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Keyboard` 中的 TransparentKeyPassthrough 注册表值不会保留在 32 位计算机上。

  [CVADHELP-19625]

2204.1

新增功能

音频重定向增强功能

改进了对所有音频编解码器（包括自适应音频和所有传统音频编解码器）的音频回声消除支持。

支持 **Web** 和 **SaaS** 应用程序的增强的单点登录 **(SSO)** 体验 **[**技术预览版**]**

使用第三方身份提供程序 (IdP) 时，此功能简化了内部 Web 应用程序和 SaaS 应用程序的 SSO 配置。增强的 SSO 体验可将整个过程缩短为几个命令。它消除了在 IdP 链中配置 Citrix Secure Private Access 以设置 SSO 的强制性必备条件。它还可以改善用户体验，前提是使用相同的 IdP 对 Workspace 应用程序和正在启动的特定 Web 或 SaaS 应用程序进行身份验证。

可以使用此 Podio 表单注册此技术预览版。

> 注意：
>
> 技术预览版可供客户在其非生产环境或有限生产环境中进行测试，并为客户提供共享反馈的机会。Citrix 不接受功能预览版的支持案例，但欢迎提供改进这些功能的反馈。Citrix 可能会根据反馈的严重性、紧迫性和重要性对反馈执行操作。建议不要在生产环境中部署 Beta 版本。

Citrix Enterprise Browser

此版本包括基于 Chromium 版本 98 的 Citrix Enterprise Browser 版本 98.1.2.20。有关 Citrix Enterprise Browser 中的功能或缺陷修复，请参阅 Citrix Enterprise Browser 文档中的新增功能。

Microsoft Teams 优化

- 支持备用铃声：在优化 Microsoft Teams（Citrix HDX 在 “关于/版本” 中进行了优化）时，您可以使用备用铃声功能选择要在其上接收来电通知的辅助设备。例如，如果您已将扬声器设置为备用铃声，并且您的端点已连接

到耳机，则即使您的耳机是音频呼叫本身的主要外围设备，Microsoft Teams 也会向扬声器发送来电信号。如果您没有连接到多个音频设备，或者外围设备不可用（例如，蓝牙耳机），则无法设置备用铃声。

> 注意：
>
> 此功能仅在 Microsoft Teams 推出将来的更新后可用。要了解 Microsoft 何时推出此更新，请参阅 Microsoft 365 roadmap（Microsoft 365 路线图）。也可以参阅 CTX253754 了解文档更新和公告。

- 应用程序保护和 **Microsoft Teams** 增强功能：当启用了应用程序保护的适用于 Windows 的 Citrix Workspace 应用程序仅处于 Desktop Viewer 模式时，Microsoft Teams 才支持传入视频和屏幕共享。在无缝模式下发布的应用程序不会呈现传入视频和屏幕共享。

已修复的问题

会话/连接

- 从适用于 Windows 的 Citrix Workspace 应用程序触发某些条件时，Citrix ADC 设备可能会崩溃。[HDX-39683]
- 在 Citrix Workspace 应用程序中，在接听或拨打 Microsoft Teams 电话时，您可能会遇到间歇性故障。此时将显示以下错误消息：

Call could not be established.（无法建立呼叫。）

[HDX-38819]

- 当您尝试重定向到在适用于 Windows 的 Citrix Workspace 应用程序中设置的首选网络摄像机时，该设置可能无法按配置执行。

  应用此修复后，首选网络摄像机将成为用户会话中唯一可用的网络摄像机。当用户会话中有多个网络摄像机可用时，这可以提供更好的控制能力。

  [HDX-38214]

- 如果 Citrix Workspace 应用程序配置为在 **“桌面”** 和 **“开始”** 菜单快捷方式文件夹中显示应用程序，则在 Citrix Workspace 应用程序退出后从 **“桌面”** 或 **“开始”** 菜单启动应用程序和桌面会话可能会导致失败。[RFWIN-26508]
- 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]

- 应用此修复后，您可以在 `HKEY_CURRENT_USER` 或 `HKEY_LOCAL_MACHINE` 中将 **TWITaskbarGroupingMode** 设置为 **GroupNone**。例如，**TWITaskbarGroupingMode** 注册表项在 HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Client\Engine\Lockdown Profiles\All Regions\Lockdown\Virtual Channels\Seamless Windows 下提供。[CVADHELP-19106]

安装、卸载、升级

- 当客户使用应用程序个性化服务时，Workspace 安装程序可能会在验证证书时挂起。[RFWIN-21122]

2202

新增功能

Storebrowse 对 Workspace 的支持 [技术预览版]

自本版本起，适用于 Windows 的 Citrix Workspace 应用程序为自助服务提供 Storebrowse 支持。这使 Storebrowse 用户能够访问云和 Workspace 功能。

> 注意：
>
> - 此功能仅为单点登录提供 Storebrowse 支持。
> - 必须具备系统要求和兼容性中提到的必备条件才能使用此功能。

有关详细信息，请参阅 适用于 Workspace 的 Storebrowse。

> 注意：
>
> 技术预览版可供客户在其非生产环境或有限生产环境中进行测试，以及共享反馈。Citrix 不接受功能预览版的支持案例，但欢迎提供改进这些功能的反馈。Citrix 可能会根据反馈的严重性、紧迫性和重要性对反馈执行操作。建议不要将 Beta 版本部署在生产环境中。

Citrix Enterprise Browser

有关 Citrix Enterprise Browser 中的功能或缺陷修复，请参阅 Citrix Enterprise Browser 文档中的新增功能。

> 注意：
>
> 适用于 Windows 的 Citrix Workspace 2202 的系统要求已更改，如下所示：
>
> - 所需的最低.NET 版本为 4.8。
> - 所需的最低 VCRedist 版本为 14.30.30704.0。

已修复的问题

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 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]

- 尝试刷新或启动应用程序会导致 **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]

会话/连接

- 当启用了应用程序保护的适用于 Windows 的 Citrix Workspace 应用程序在后台启动时，Print Screen 键可能无法捕获屏幕截图。[RFWIN-25835]
- 使用适用于 Windows 的 Citrix Workspace 应用程序通过 StoreFront 上的 PNAgent 站点启动已发布的应用程序可能会失败，并显示以下错误消息：

  无法启动应用程序。请与技术支持人员联系。

[CVADHELP-19209]

- 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]

- 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]
- 通过组策略对象或命令配置应用商店后，刷新从通知区域或开始菜单打开的自助服务用户界面可能会失败。此时将显示无法访问服务器消息。[CVADHELP-19242]
- 尽管已配置域直通功能，但虚拟桌面仍会提示您输入凭据。从 Citrix Workspace 应用程序启动虚拟桌面时会出现此问题。[RFWIN-26111]
- 在 Citrix Workspace 应用程序 2112.1 中，在优化的 Microsoft Teams 视频通话中打开网络摄像机时，端点上的 CPU 利用率可能会很高。[HDX-37168]

2112.1

新增功能

支持 **Citrix Workspace** 应用程序中的本地应用程序发现

自本版本起，管理员可以在 Citrix Workspace 应用程序中配置本地安装的应用程序的发现和枚举。您可以使用 Global App Configuration Service 来配置此功能。有关配置此功能的信息，请参阅 Global App Configuration Service。此功能非常适用于在 Kiosk 模式下运行的设备以及在 Citrix Workspace 中无法虚拟化的应用程序。

服务连续性

在 Workspace 身份验证的身份提供程序中断期间，用户可能无法通过 Workspace 应用程序登录屏幕登录 Citrix Workspace。
Citrix Workspace 应用程序登录屏幕的顶部将显示消息登录时遇到问题**?** 脱机使用 **Workspace**。

单击脱机使用 **Workspace** 以枚举在客户端设备上存储有有效连接租约的所有应用程序和桌面。

自本版本起，该消息将在 40 秒超时后显示。有关详细信息，请参阅 Citrix Workspace 文档中的服务连续性部分。

改进了虚拟桌面体验

本版本改进了调整虚拟桌面大小时的体验。

提高了 **ICA** 文件的安全性

在早期版本中，当您启动虚拟应用程序和桌面会话时，ICA 文件会下载到本地磁盘。

在本版本中，我们以 Citrix Workspace 应用程序在虚拟应用程序和桌面会话启动期间处理 ICA 文件的方式提供了增强的安全性。

Citrix Workspace 应用程序现在允许您将 ICA 文件存储在系统内存中，而非本地磁盘中。此功能旨在消除表面攻击以及在本地存储时可能会滥用 ICA 文件的任何恶意软件。此功能也适用于在适用于 Web 的 Workspace 上启动的虚拟应用程序和桌面会话。
有关详细信息，请参阅提高了 ICA 文件安全性部分。

自适应音频更新

使用 UDP 音频传输时，自适应音频现在可用。有关详细信息，请参阅自适应音频。

Microsoft Teams 优化

> 注意：
>
> 以下功能仅在 Microsoft Teams 推出功能更新后可用。Microsoft 推出此更新时，请参阅 Microsoft 365 roadmap（Microsoft 365 路线图），另请查看 CTX253754 以获取文档更新和公告。

- **Microsoft Teams** 的多窗口聊天和会议

  在 Citrix Virtual Apps and Desktops 2112 或更高版本中通过 HDX 进行优化时，您可以在 Microsoft Teams 中使用多个窗口进行聊天和会议。可以通过各种方式弹出对话或会议。有关弹出窗口功能的详细信息，请参阅 Microsoft Office 365 站点上的 Teams Pop-Out Windows for Chats and Meetings（Teams 用于聊天和会议的弹出窗口）。

  如果您正在运行较旧版本的 Citrix Workspace 应用程序或 Virtual Delivery Agent (VDA)，请谨记，Microsoft 将来会弃用单窗口代码。但是，在此功能正式发布后，您至少有九个月的时间升级到支持多个窗口（2112 或更高版本）的 VDA 或 Citrix Workspace 应用程序版本。

- 应用程序共享

  以前，当您在 Citrix Studio 中启用了 HDX 3D Pro 策略时，将无法使用 Microsoft Teams 中的屏幕共享功能共享应用程序。

  自适用于 Windows 的 Citrix Workspace 应用程序 2112.1 和 Citrix Virtual Apps and Desktops 2112 起，启用此策略后，您可以使用 Microsoft Teams 中的屏幕共享功能共享应用程序。

- 授予控制权

  可以使用授予控制权按钮将共享屏幕的控制权限授予参加会议的其他用户。另一位参与者可以通过键盘、鼠标和剪贴板输入进行选择和修改共享的屏幕。双方现在都可以控制共享屏幕，并且可以随时收回控制权。

- 获取控制权

  在屏幕共享会话期间，任何参与者都可以通过“请求控制权”按钮请求控制权限。然后，共享屏幕的人员可以批准或拒绝该请求。拥有控制权后，您可以控制共享的屏幕上的键盘和鼠标输入，以及释放控制权以停止共享控制权。

  限制：

  在优化的用户与端点上运行的本机 Microsoft Teams 桌面客户端上的用户之间的点对点通话期间，请求控制权选项不可用。解决方法：用户可以加入会议以获取请求控制权选项。

- **Dynamic e911**

  在本版本中，Citrix Workspace 应用程序支持动态紧急呼叫。在 Microsoft 通话套餐、接线员连接和直接路由中使用时，它提供了以下功能：

  - 配置和路由紧急呼叫
  - 通知安全人员

  提供通知的依据是端点上运行的 Citrix Workspace 应用程序的当前位置，而非 VDA 上运行的 Microsoft Teams 客户端。
  Ray Baum 法律要求将 911 呼叫者的可调度位置传送到相应的公共安全应答点 (PSAP)。自适用于 Windows 的 Citrix Workspace 应用程序 2112.1 起，使用 HDX 的 Microsoft Teams 优化遵从 Ray Baum 的法律。

Citrix Enterprise Browser

本版本的 Enterprise Browser 基于 Chromium 版本 95。

已修复的问题

安装、卸载、升级

如果您以用户身份安装了版本低于 2109 的 Workspace 应用程序，而管理员安装的版本为 2109，则当您以用户身份重新登录设备时，将显示 **Entry point not found**（找不到入口点）错误消息。单击确定时，该消息将消失，并且 Workspace 应用程序将更新到版本 21.0.9。[RFWIN-25008]

登录/身份验证

- 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该应用程序。[RFWIN-25006]
- 添加使用智能卡身份验证的应用商店可能会失败，并显示以下错误消息：
  此应用商店不存在。请重试或联系技术支持。
  [CVADHELP-18647]
- 通过 **Storebrowse** 执行应用程序枚举会在枚举文件中的每个字符之间添加空字符。[CVADHELP-18773]

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]
- 在启用了 **vPrefer** 选项并且配置了每个用户一个实例应用程序限制的情况下尝试打开应用程序时，Citrix Director 上可能会出现连接失败错误。[CVADHELP-17372]
- Citrix Workspace 应用程序可能会轮询仅限内部应用商店的外部信标。应用此修复后，外部信标不会轮询仅针对内部应用商店或没有与其关联的网关的应用商店。[CVADHELP-18275]
- 在适用于 Windows 的 Citrix Workspace 应用程序 2109 及更高版本中，启用旧图形模式后，桌面会话可能会断开连接。[CVADHELP-18718]
- 在适用于 Windows 的 Citrix Workspace 应用程序 2109 或更高版本中使用应用程序保护时，图形卡的性能可能会很差。[CVADHELP-18831]
- Microsoft Edge WebView2 Runtime 自动升级后，适用于 Windows 的 Citrix Workspace 应用程序将显示空白屏幕。[RFWIN-25295]
- Citrix Workspace 应用程序停止运行。[RFWIN-25301]
- 处理应用程序保护组件中的泄漏会导致少量进程失败。[RFWIN-25358]
- 如果未配置 Desktop Lock 设置的 GPO 存储，Citrix Workspace 应用程序 Desktop Lock 可能会失败。[RFWIN-25392]
- 在 Microsoft Teams 中，当您调整会话的大小时，屏幕共享将停止。[HDX-31858]
- 在多显示器模式下，当您在 Microsoft Teams 中共享屏幕时断开显示器连接时，将显示一个空白屏幕。[HDX-34733]
- 在屏幕共享会话期间，当 Microsoft Teams 在无缝模式下和多显示器设置中运行时，指示共享屏幕的红色边框将跨越屏幕。[HDX-34978]
- 在适用于 Mac 的 Citrix Workspace 应用程序 2109 与适用于 Windows 的 Citrix Workspace 应用程序 2109 之间进行 P2P 通话时，您可能会遇到通话失败问题。[HDX-35223]
- 在 Microsoft Teams 视频通话期间，摄像机可能会闪烁。[HDX-36345]
- 通过在 default.ica 文件中将字段值设置为 **ClientName** 来自定义 StoreFront 时，尝试启动会话可能会失败。有关详细信息，请参阅 Citrix 知识中心文章 CTX335725。[CVADHELP-19033]

要了解产品中的现有问题，请参阅已知问题。

2109.1

新增功能

支持 Windows 11

Windows 11 操作系统现在支持适用于 Windows 的 Citrix Workspace 应用程序。

已修复的问题

如果您的管理员在 Google Chrome 中安装了外部扩展，则当打开时 Citrix Enterprise Browser 将崩溃。[CTXBR-2135]

要了解产品中的现有问题，请参阅已知问题。

2109

新增功能

自适应音频

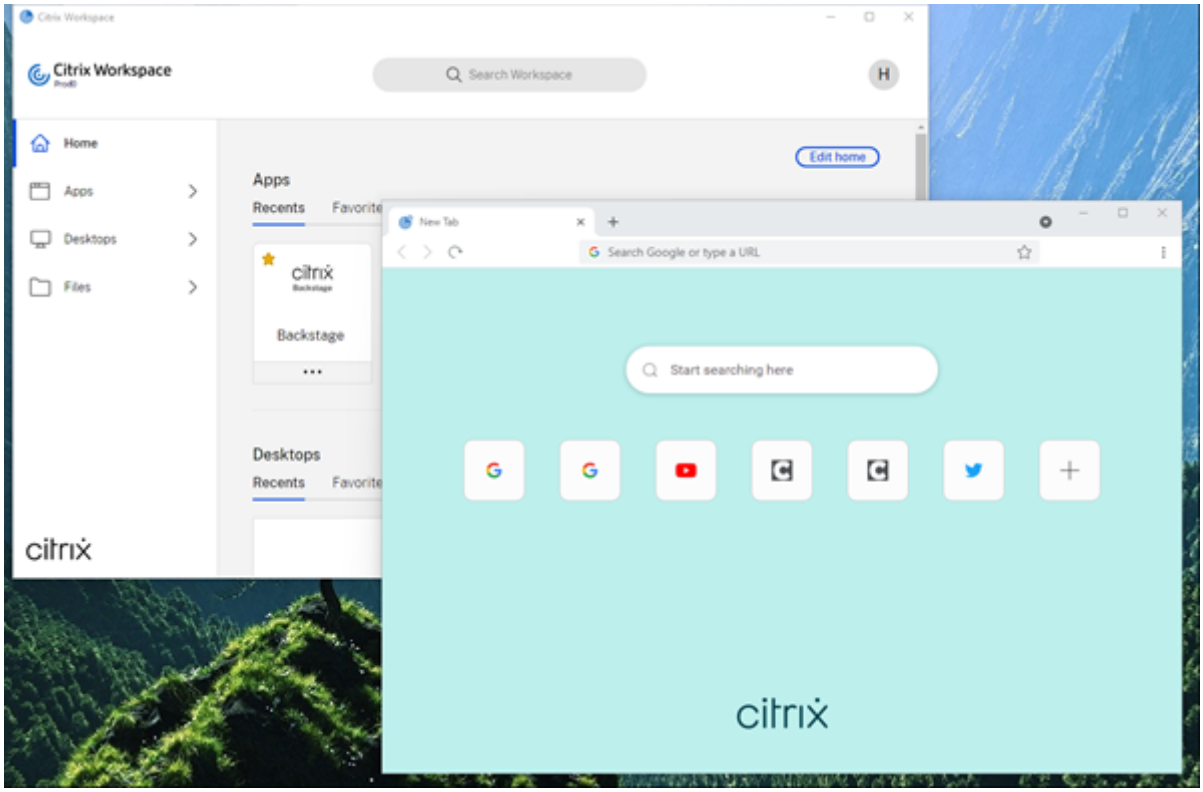
使用自适应音频时，您无需在 VDA 上配置音频质量策略。自适应音频可优化环境设置，并替换已弃用的音频压缩格式，以提供卓越的用户体验。

> 注意：
>
> 如果实时音频应用程序需要 UDP 音频交付，则必须在 VDA 上禁用自适应音频，以允许回退到 UDP 音频交付。

有关详细信息，请参阅自适应音频。

Citrix Enterprise Browser

Citrix Enterprise Browser 是客户端计算机上运行的本机浏览器。它允许用户从 Citrix Workspace 应用程序内以安全方式打开 Web 和 SaaS 应用程序。



我们一直持续致力于丰富用户体验，全新的浏览器将为您带来更加类似于本机浏览器的增强用户体验，并配备以下功能：

- 无需 VPN 即可访问内部 Web 页面
- 麦克风和网络摄像机支持
- 选项卡式浏览体验
- 多窗口视图
- 可编辑的地址栏
- 书签
- 新选项卡页面上具有快捷方式
- 可自定义的设置
- 代理身份验证支持
- 分析

管理员可以基于每个 URL 以不同的组合方式启用 Secure Workspace Access（以前称为 Secure Workspace Access）或应用程序保护策略。这些功能包括反键盘记录、防屏幕捕获、下载、打印、剪贴板限制和水印等。

有关详细信息，请参阅 Citrix Enterprise Browser。

StoreFront 到 **Workspace URL** 迁移

当贵组织从本地 StoreFront 移至 Workspace 时，最终用户必须手动将新的 Workspace URL 添加到其端点设备上的 Workspace 应用程序中。通过此功能，管理员可以将用户从 StoreFront 应用商店无缝迁移到 Workspace 应用商店，同时将用户交互降至最少。

有关此功能有关详细信息，请参阅 StoreFront 到 Workspace URL 迁移。

支持自定义 **Web** 应用商店

在此版本中，您可以通过适用于 Windows 的 Citrix Workspace 应用程序访问贵组织的自定义 Web 应用商店。

要使用此功能，管理员必须将域或自定义 Web 应用商店添加到 Global App Configuration Service 中允许访问的 URL 列表中。添加时，您可以在 Citrix Workspace 应用程序的添加帐户屏幕中提供自定义 Web 应用商店 URL。自定义 Web 应用商店将在本机 Workspace 应用程序窗口中打开。

有关配置自定义 Web 应用商店的详细信息，请参阅自定义 Web 应用商店。

支持基于 **Windows Hello** 和 **FIDO2** 安全密钥的身份验证

在此版本中，可以使用 Windows Hello 和 FIDO2 安全密钥对 Citrix Workspace 进行身份验证。

有关详细信息，请参阅对 Citrix Workspace 进行身份验证的其他方法。

从加入了 **Microsoft Azure Active Directory (AAD)** 且 **AAD** 为身份提供程序的计算机单点登录 **(SSO)** 到 **Citrix Workspace** 应用程序

在此版本中，您可以从加入了 Azure Active Directory (AAD) 且 AAD 为身份提供程序的计算机单点登录到 Citrix Workspace 应用程序。

有关详细信息，请参阅对 Citrix Workspace 进行身份验证的其他方法。

支持 **Azure Active Directory** 中的条件访问

在此版本中，Workspace 管理员可以为向 Citrix Workspace 应用程序进行身份验证的用户配置并强制执行 Azure Active Directory 条件访问策略。

有关详细信息，请参阅支持 Azure AD 中的条件访问。

支持服务连续性

此版本支持 Citrix Workspace Web 扩展中的服务连续性。可以将适用于 Google Chrome 或 Microsoft Edge 的 Workspace Web 扩展与适用于 Windows 2109 的 Workspace 应用程序结合使用。这些扩展可通过 Google 网上应用店和 Microsoft Edge 加载项 Web 站点获取。
Workspace 应用程序将使用浏览器扩展的本机消息主机协议与 Citrix Workspace Web 扩展通信。同时，Workspace 应用程序和 Workspace Web 扩展会使用 Workspace 连接租用使浏览器用户能够在中断期间访问其应用程序和桌面。
有关详细信息，请参阅服务连续性。

Microsoft Teams 增强功能

以下功能仅在 Microsoft Teams 推出功能更新后可用。

Microsoft 推出此更新时，您可以查看 CTX253754 以获取文档更新和公告。

- 支持 **WebRTC**：此版本支持 WebRTC 1.0，可提供更好的视频会议体验以及库视图。
- 屏幕共享增强功能：您可以使用 Microsoft Teams 中的屏幕共享功能来共享各个应用程序、窗口或整个屏幕。使用此功能必须安装 Citrix Virtual Delivery Agent 2109。
- 应用程序保护兼容性：启用应用程序保护后，现在可以通过具有 HDX 优化功能的 Microsoft Teams 共享内容。借助此功能，您可以共享在虚拟桌面中运行的应用程序窗口。使用此功能必须安装 Citrix Virtual Delivery Agent 2109。

  > **Note:**
  >
  > Full monitor or desktop sharing is disabled when App Protection is enabled for the delivery group.

- 实时辅助字幕：在 Microsoft Teams 中启用实时辅助字幕时，本版本支持实时传输讲话者所讲的内容。

Microsoft Teams 优化

适用于 Windows 的 Citrix Workspace 2109 版本支持在 VM 托管应用程序上经过优化的 Microsoft Teams 中进行点对点音频和视频通话、电话会议和屏幕共享。

支持 Bloomberg 键盘 5

本版本支持 Bloomberg 键盘 5。要使用 Bloomberg 键盘 5，必须配置注册表编辑器。有关配置键盘的详细信息，请参阅 Bloomberg 键盘中的 “配置 Bloomberg 键盘 5” 部分。

已修复的问题

无缝窗口

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

用户界面

使用适用于 Windows 的 Citrix Workspace 应用程序时，“开始” 菜单快捷方式可能不会自动刷新。添加新应用程序或在后端进行了更改时会出现此问题。[CVADHELP-17122]

客户端设备问题

使用 Citrix Workspace 应用程序时，使用大于 9 的 COM 端口号进行连接的设备可能无法在会话中映射。[CVADHELP-17734]

会话/连接

- 将适用于 Windows 的 Citrix Workspace 应用程序升级到版本 2106 时，使用代理服务器启动应用程序或桌面可能会失败，并显示以下错误消息：

  无法连接到服务器。请与系统管理员联系并陈述以下错误：在指定地址上未配置 **Citrix XenApp** 服务器。（套接字错误 **10060**） [CVADHELP-18137]

- 尝试使用 VDA 上安装的适用于 Windows 的 Citrix Workspace 应用程序重定向网络摄像机时，网络摄像机可能会出现故障。[HDX-28691]

- 如果您在多显示器设置中通过 HDX 优化在 Microsoft Teams 中共享屏幕，屏幕共享选择器将无法捕获单个显示器。虚拟桌面未使用 Desktop Viewer 工具栏或使用 Desktop Lock 时会出现此问题。所有显示器都不是单个显示器，而是压缩到一个复合映像中。您可能会在适用于 Windows 的 Citrix Workspace 应用程序 2106 或更高版本上看到此问题。
  在本版本中，禁用了多显示器屏幕共享功能：

- 如果在 StoreFront 或 ICA 文件中禁用了 Desktop Viewer，或者

- 如果 Desktop Lock 正在使用中。只能共享主显示器。[HDX-34200]

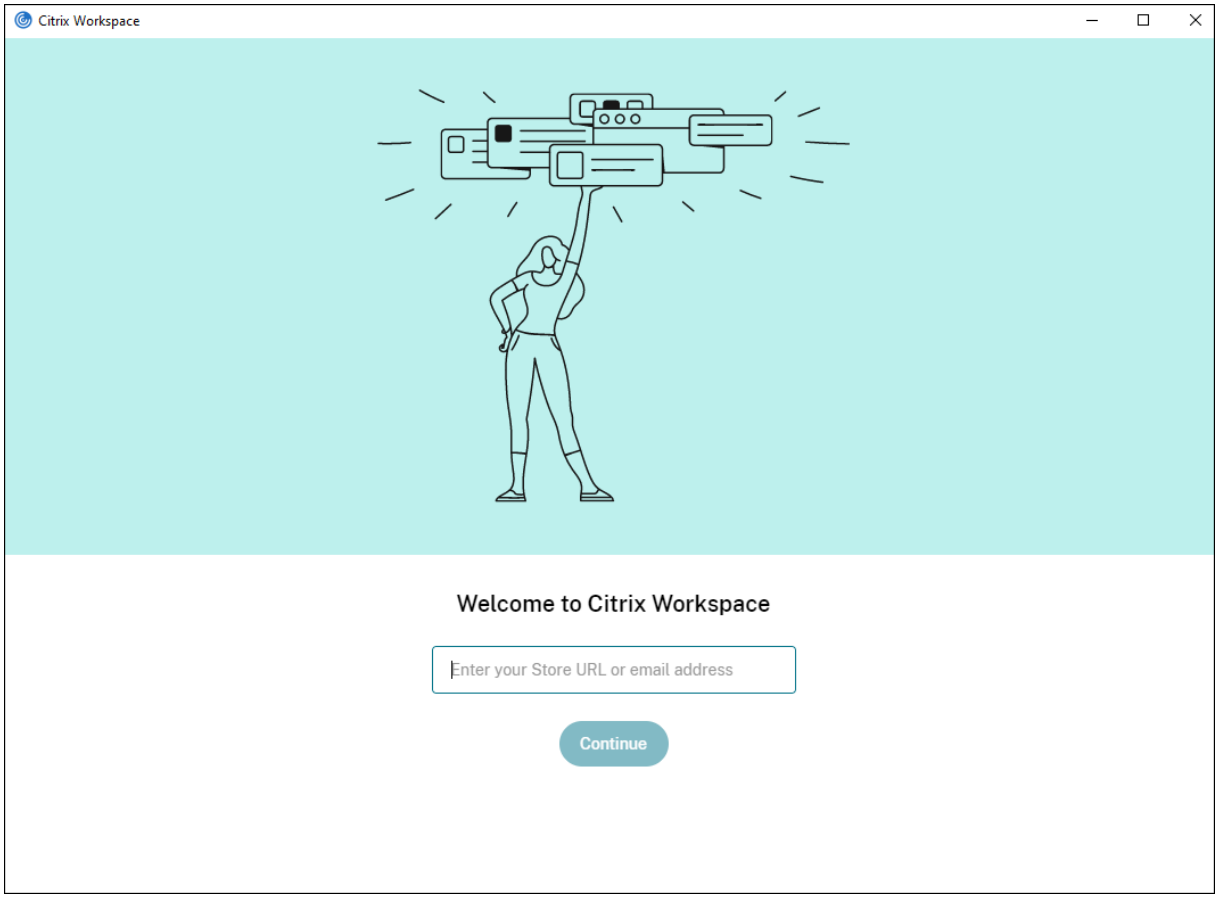
要了解产品中的现有问题，请参阅已知问题。

2108

新增功能

改进了“添加帐户”屏幕

本版本引入了改进后的“添加帐户”屏幕。



Citrix Workspace 会话的不活动超时

管理员可以配置不活动状态超时值。不活动超时值指定在用户自动从 Citrix Workspace 会话中注销之前允许的空闲时间量。如果在指定的时间间隔内没有来自鼠标、键盘或触摸的活动，Citrix Workspace 应用程序将自动注销。不活动超时不会影响已在运行的虚拟应用程序和桌面会话或 Citrix StoreFront 应用商店。

有关详细信息，请参阅 Workspace 会话的不活动超时

> 注意：
>
> 管理员只能为 Workspace（云）会话配置不活动超时。

支持自定义 **Web** 应用商店 **[技术预览版]**

在此版本中，您可以通过适用于 Windows 的 Citrix Workspace 应用程序访问贵组织的自定义 Web 应用商店。要使用此功能，管理员必须将域或自定义 Web 应用商店添加到 Global App Configuration Service 中允许使用的 URL 列表中。添加时，您可以在 Citrix Workspace 应用程序的添加帐户屏幕中提供自定义 Web 应用商店 URL。自定义 Web 应用商店将在本机 Workspace 应用程序窗口中打开。

有关配置自定义 Web 应用商店的信息，请参阅自定义 Web 应用商店

> 注意：
>
> 技术预览版可供客户在其非生产环境或有限生产环境中进行测试，以及共享反馈。Citrix 不接受功能预览版的支持案例，但欢迎提供改进这些功能的反馈。Citrix 可能会根据反馈的严重性、紧迫性和重要性对反馈执行操作。建议不要将 Beta 版本部署在生产环境中。

StoreFront 到 Workspace URL 迁移 [技术预览版]

当贵组织从本地 StoreFront 移至 Workspace 时，最终用户必须手动将新的 Workspace URL 添加到其端点设备上的 Workspace 应用程序中。通过此功能，管理员可以将用户从 StoreFront 应用商店无缝迁移到 Workspace 应用商店，同时将用户交互降至最少。

有关此功能的详细信息，请参阅 StoreFront 到 Workspace URL 迁移 [技术预览版]

> 注意：
>
> 技术预览版可供客户在其非生产环境或有限生产环境中进行测试，以及共享反馈。Citrix 不接受功能预览版的支持案例，但欢迎提供改进这些功能的反馈。Citrix 可能会根据反馈的严重性、紧迫性和重要性对反馈执行操作。建议不要将 Beta 版本部署在生产环境中。

已修复的问题

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。[RFWIN-23829]

要了解产品中的现有问题，请参阅已知问题。

2107

新增功能

EPA 增强功能

自本版本起，Citrix Workspace 应用程序可以下载并在 Workspace 部署中安装 EPA 插件。安装完成后，高级端点分析 (Advanced Endpoint Analysis, EPA) 将扫描设备以检查在 Citrix Gateway 上配置的端点安全要求。扫描完成后，将显示 Citrix Workspace 应用程序登录窗口。

> 注意：
>
> 只有在环境中配置了 nFactor 身份验证时，此功能才有效。

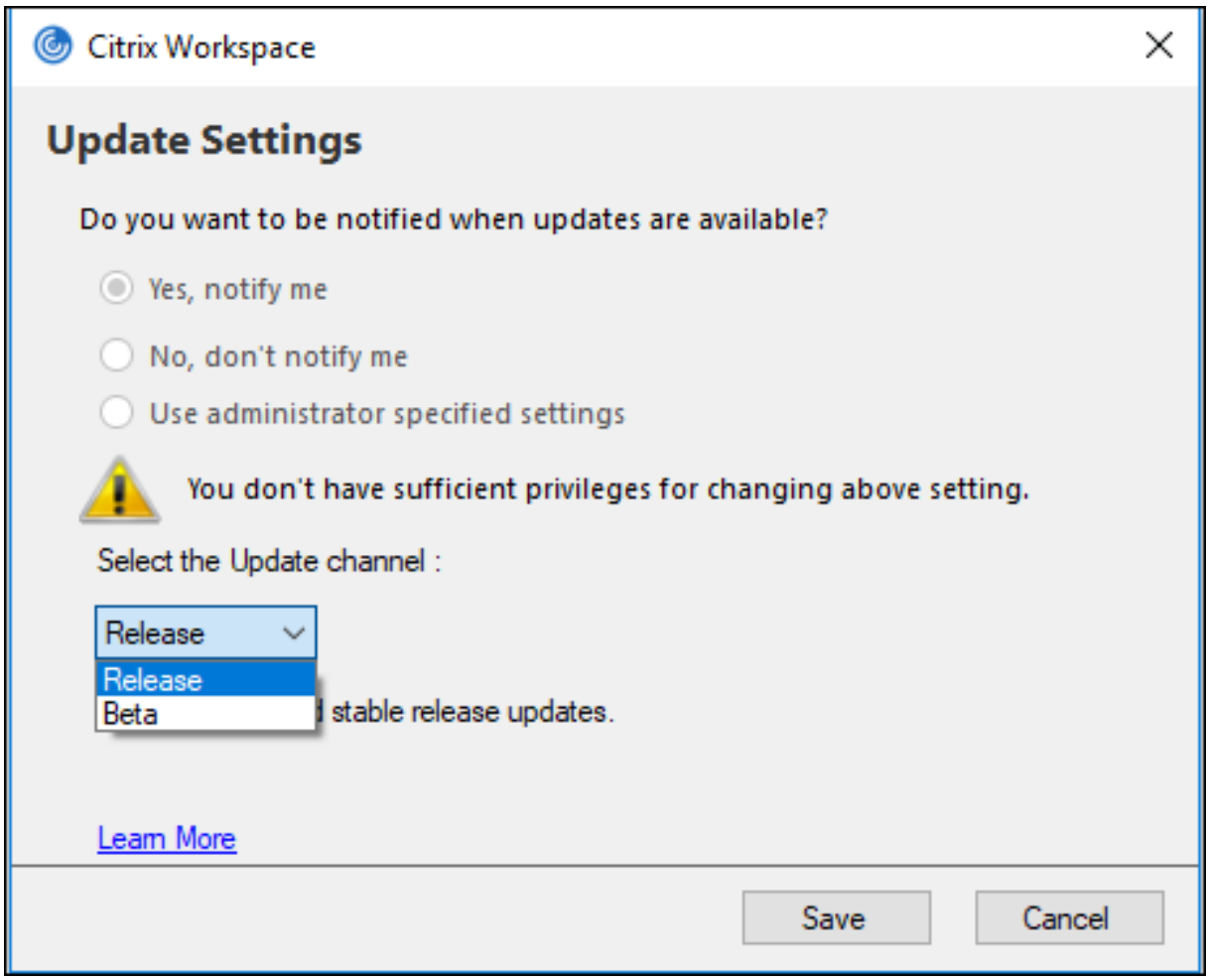
有关 EPA 扫描的详细信息，请参阅高级端点分析扫描。

Citrix Workspace 应用程序 Beta 版程序

自本版本起，您可以将 Citrix Workspace 应用程序的现有安装自动更新到最新的 Beta 版本并进行测试。Beta 版本是在提供完全受支持的稳定版本更新之前发布的早期访问版本。将 Citrix Workspace 应用程序配置为自动更新时，您将收到更新通知。

要更新到 Beta 版本，请从更新设置窗口中的下拉菜单中选择 **Beta** 通道：

- 版本 - 完全受支持的稳定版本更新
- **Beta** - 早期访问版本，以轻松测试和报告通用版本之前出现的问题



> 注意：
>
> Beta 版本可供客户在其非生产环境或有限生产环境中进行测试，以及共享反馈。Citrix 不接受 Beta 版本的支持案例，但欢迎通过提供反馈来改进这些版本。Citrix 可能会根据反馈的严重性、紧迫性和重要性对反馈执行操作。建议不要将 Beta 版本部署在生产环境中。

有关安装自动更新通道的详细信息，请参阅安装 Citrix Workspace 应用程序 Beta 计划。

支持以下身份验证机制 [技术预览版]

自本版本起，可以使用以下机制对 Citrix Workspace 应用程序进行身份验证：

- 基于 Windows Hello 和 FIDO2 安全密钥的身份验证
- 从加入了 Microsoft Azure Active Directory (AAD) 且 AAD 为身份提供程序的计算机单点登录 (SSO) 到 Citrix Workspace 应用程序

系统要求

Microsoft Edge WebView2 Runtime 版本 92 或更高版本。

> 注意：
>
> 自版本 2107 起，Microsoft Edge WebView2 Runtime 安装程序随 Citrix Workspace 应用程序安装程序打包。在 Workspace 应用程序安装期间，安装程序会检查系统中是否存在 Microsoft Edge WebView2 Runtime，如果找不到，则会进行安装。
>
> 如果您尝试以非管理员身份安装 Citrix Workspace 应用程序，但 Microsoft Edge WebView2 Runtime 不存在，安装将停止并显示以下消息：
>
> ```
> You must be logged on as an administrator to install the following
> prerequisite package(s):
> Edge Webview2 Runtime
> ```
>
> 此功能仅在 Workspace (Cloud) 部署中受支持。

启用身份验证机制

要启用身份验证机制，管理员必须执行以下步骤：

1. 启动注册表编辑器。
2. 导航到以下注册表路径：
   - 以管理员角色：
     - 对于 64 位操作系统：`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle`
     - 对于 32 位操作系统：`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle`
   - 以非管理员角色：
     - 对于 64 位或 32 位操作系统：`\HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle`
3. 创建具有以下属性的注册表值：

   注册表项名称： EdgeChromiumEnabled

   类型：字符串值

   值： True
4. 重新启动 Citrix Workspace 应用程序以使所做的更改生效。

> 注意：
>
> 技术预览版可供客户在其非生产环境或有限生产环境中使用，以及共享反馈。Citrix 不接受功能预览版的支持案例，但欢迎提供改进这些功能的反馈。Citrix 可能会根据反馈的严重性、紧迫性和重要性对反馈执行操作。

支持使用 **Azure AD** 进行条件访问 **[技术预览版]**

在本版本中，如果您的管理员配置了策略，您可以使用条件访问进行身份验证。

系统要求

Microsoft Edge WebView2 Runtime 版本 92 或更高版本。

> 注意：
>
> 自版本 2107 起，Microsoft Edge WebView2 Runtime 安装程序随 Citrix Workspace 应用程序安装程序打包。在 Workspace 应用程序安装期间，安装程序会检查系统中是否存在 Microsoft Edge WebView2 Runtime，如果找不到，则会进行安装。

使用条件访问启用身份验证

要启用通过 Azure AD 使用条件访问的身份验证，管理员必须执行以下步骤：

1. 启动注册表编辑器。
2. 导航到以下注册表路径：
   - 对于 64 位操作系统：`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle`
   - 对于 32 位操作系统：`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Dazzle`
3. 创建具有以下属性的注册表值：

   注册表项名称： EdgeChromiumEnabled

   类型：字符串值

   值： True
4. 重新启动 Citrix Workspace 应用程序以使所做的更改生效。

支持在 **Workspace** 应用程序中进行本地应用程序发现 **[技术预览版]**

自版本 2107 起，管理员可以在 Citrix Workspace 应用程序中配置本地安装的应用程序的发现和枚举。您可以使用 Global App Configuration Service 来配置此功能。有关配置此功能的信息，请参阅 Global App Configuration Service。

此功能非常适用于在 Kiosk 模式下运行的设备以及在 Citrix Workspace 中无法虚拟化的应用程序。

> 注意：
>
> 技术预览版可供客户在其非生产环境或有限生产环境中使用，以及共享反馈。Citrix 不接受功能预览版的支持案例，但欢迎提供改进这些功能的反馈。Citrix 可能会根据反馈的严重性、紧迫性和重要性对反馈执行操作。

已修复的问题

键盘

安装应用程序保护后，键盘输入可能与某些 HP G5 系列便携式计算机不兼容。[RFWIN-24103]

会话/连接

- 启用了拖放精选功能时，尝试调整已发布的应用程序的大小可能会失败。[CVADHELP-17089]
- 使用网络代理设置配置客户端和 VDA 时，浏览器内容重定向在 Chrome 浏览器上可能会失败。[CVADHELP-17430]
- 使用单点登录时，当您使用 UPN 凭据登录，然后在端点上更改密码时，尝试启动会话后可能会显示以下错误消息：

  用户名或密码不正确。重试。[CVADHELP-17620]
- 在 Microsoft Teams 会议期间启动视频通话时，Desktop Viewer 可能会变得无响应。[HDX-32435]

要了解产品中的现有问题，请参阅已知问题。

2106

新增功能

Global App Config Service

新的适用于 Citrix Workspace 的 Global App Configuration Service 使 Citrix 管理员能够通过集中管理的服务提供 Workspace 服务 URL 和 Workspace 应用程序设置。

有关详细信息，请参阅 Global App Configuration Service 文档。

用于通过 **Global App Config Service** 禁用身份验证令牌的存储的选项

Citrix Workspace 应用程序现在提供了额外的用于禁止在本地磁盘上存储身份验证令牌的选项。除了现有的组策略对象 (GPO) 配置外，还可以使用 Global App Configuration Service 禁止在本地磁盘上存储身份验证令牌。

在 Global App Configuration Service 中，将 `Store Authentication Tokens` 属性设置为 `False`。

有关详细信息，请参阅 Global App Configuration Service 文档。

服务连续性

服务连续性消除或最大限度地减少了对连接过程中涉及的组件可用性的依赖。无论云服务的运行状况如何，用户都可以启动其虚拟应用程序和桌面。

有关详细信息，请参阅 Citrix Workspace 文档中的服务连续性部分。

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。

基于 Chromium 的浏览器支持双向 URL

双向内容重定向允许您将 URL 配置为从客户端重定向到服务器以及从服务器重定向到客户端。您可以使用服务器和客户端上的策略对此进行配置。

使用组策略对象 (GPO) 管理模板，您可以在 Delivery Controller 上设置服务器策略，在 Citrix Workspace 应用程序上设置客户端策略。

在此版本中，已为 Google Chrome 和 Microsoft Edge 添加了双向 URL 重定向支持。

必备条件：

- Citrix Virtual Apps and Desktops 版本 2106 或更高版本。
- 浏览器重定向扩展程序版本 5.0。

要将 Google Chrome 浏览器注册到双向 URL 重定向，请从 Citrix Workspace 应用程序安装文件夹中运行以下命令：

```
1 %ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /regChrome /
    verbose
```

要从双向 URL 重定向中取消注册 Google Chrome 浏览器，请从 Citrix Workspace 应用程序安装文件夹中运行以下命令：

```
1 %ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe  /unregChrome /
    verbose
```

有关在 Citrix Workspace 应用程序中配置 URL 重定向的信息，请参阅双向内容重定向。

有关浏览器内容重定向的详细信息，请参阅 Citrix Virtual Apps and Desktops 文档中的浏览器内容重定向。

改进了 **ICA** 文件安全性 **[**技术预览版**]**

在早期版本中，当您启动虚拟应用程序和桌面会话时，ICA 文件会下载到本地磁盘。

在本版本中，我们以 Citrix Workspace 应用程序在虚拟应用程序和桌面会话启动期间处理 ICA 文件的方式提供了增强的安全性。

Citrix Workspace 应用程序现在允许您将 ICA 文件存储在系统内存中，而非本地磁盘中。此功能旨在消除表面攻击以及在本地存储时可能会滥用 ICA 文件的任何恶意软件。此功能也适用于在适用于 Web 的 Workspace 上启动的虚拟应用程序和桌面会话。

有关详细信息，请参阅提高了 ICA 文件安全性部分。

要提供有关此功能的反馈，请使用 Podio 表单。

已修复的问题

会话/连接

- 使用 Google Chrome、Mozilla Firefox 或 Microsoft Internet Explorer 作为默认 PDF 查看器时，尝试使用 Citrix PDF 打印机打印文件可能会失败。[CVADHELP-16662]
- 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。设置了 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]
- 连接 VPN 或断开连接 VPN 时，尝试使用适用于 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，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 `CurrentAccount` 值设置为注册表 `HKEY_LOCAL_MACHINE\Software\Citrix\Dazzle` 下的 `AllAccount` 可能无法生效。存在一个或多个应用商店帐户时会出现此问题。[CVADHELP-17229]
- 用户名包含变音字符时，尝试登录适用于 Windows 的 Citrix Workspace 应用程序可能会失败。[CVADHELP-17267]
- 尝试下载本地网络上托管的文件可能会失败。[CVADHELP-17337]
- 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]
- 尝试使用微应用下载文件可能会失败。[CVADHELP-17438]

用户界面

- 使用中文或日语输入法编辑器 (IME) 在文本框中输入文本时，文本可能会显示在屏幕左上角的文本框之外。[CVADHELP-15614]
- 当您尝试从快捷方式启动应用程序时，某些桌面上的快捷方式图标可能会闪烁不定。将 Citrix Receiver for Windows 4.9.6 升级到 Citrix Workspace 应用程序后，会出现此问题。[CVADHELP-16967]

- 尝试在 ping.citrix.com 上运行信标检查器测试可能会失败。[RFWIN-22672]
- 服务连续性可能不支持 Windows 设备上具有 Unicode 用户名但为 Citrix Workspace 帐户使用使用 ASCII 用户名的所有用户。如果 Unicode 用户名中包含西里尔文字符或东亚字符，Workspace 连接租用将无法为这些用户启动。[RFWIN-23040、RFWIN-23046]

要了解产品中的现有问题，请参阅已知问题。

2105

新增功能

通过 **301** 重定向支持自定义 **URL**

Citrix Workspace 应用程序现在允许您添加通过 HTTP 301 重定向从 StoreFront 或 Citrix Gateway 重定向到 Citrix Workspace 的 URL。

如果要从 StoreFront 迁移到 Citrix Workspace，则可以通过 HTTP 301 重定向将 StoreFront URL 重定向到 Citrix Workspace URL。因此，添加旧的 StoreFront URL 时，系统会自动将您重定向到 Citrix Workspace。

重定向示例：

StoreFront URL https://< Citrix Storefront url>/Citrix/Roaming/Accounts 可以重定向到 Citrix Workspace URL https://<Citrix Workspace url>/Citrix/Roaming/Accounts。

Microsoft Teams 增强功能

- 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。禁用 ADM2 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。

要了解产品中的现有问题，请参阅已知问题。

已修复的问题

会话/连接

- 使用适用于 Windows 的 Citrix Workspace 应用程序时，应用程序保护的资源可能无法启动并保持卡在正在连接屏幕上。服务器操作系统（例如 Windows Server 2019）上安装的 Citrix Workspace 应用程序会出现此问题。[RFWIN-22120]
- 尝试在 Git bash 上运行命令可能会失败。启用了应用程序保护功能的 Citrix Workspace 应用程序会出现此问题。[RFWIN-22187]
- 安装最新版本的 Citrix Workspace 应用程序后，登录 StoreFront 时可能会收到升级提示。[RFWIN-22419]
- 尝试退出 Citrix Workspace 应用程序可能会失败。当用户凭据提示反复出现时会出现此问题。[RFWIN-22491]
- 为应用程序创建桌面快捷方式并重新启动客户端设备后，首次尝试从快捷方式启动应用程序可能会失败。使用命令行界面安装 Citrix Workspace 应用程序时，如果未指定 `storedescription`，则会出现此问题。[RFWIN-22510]
- 从 Citrix Files 下载文件时，某些非英语文件名可能会出现乱码。[RFWIN-22516]
- 在启用了硬件强制的堆栈保护并且支持 HSP 或 CET 功能的情况下，第 11 代 Intel Core 处理器和 AMD Ryzen 5000 系列处理器上的应用程序可能会意外退出。[RFWIN-22592]
- 如果“HDX 自适应传输”策略设置为“首选”，并且启用了“EDT MTU 发现”，则当您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。[RFWIN-22697]
- 适用于 Windows 的 Citrix Workspace 应用程序可能无法枚举应用程序，并卡在灰色屏幕上。该问题特定于 Intel Iris Xe 图形卡。[RFWIN-22952]
- 在 Microsoft Teams 点对点视频通话期间，HdxRtcEngine.exe 进程可能会变得无响应。屏幕分辨率不同的多显示器设置中会出现此问题。[HDX-28616]
- 从 Outlook 加入 Microsoft Teams 会议时，传入的视频可能无法正常运行。在未启动 Microsoft Teams 的情况下加入会议时会出现此问题。[HDX-29558]
- 在 Microsoft Teams 会议期间，将鼠标指针悬停在视频上时，视频可能会闪烁不定。[HDX-29668]

系统异常

- 由于故障模块 gfxrender.dll，`Wfica32.exe` 进程可能会意外退出。[RFWIN-22446]

安全问题

- 在 Citrix Workspace 应用程序的管理员安装的实例上，具有非管理员权限的用户可能能够升级权限级别。有关详细信息，请参阅 Citrix 知识中心文章 CTX307794。

要了解产品中的现有问题，请参阅已知问题。

2103.1

新增功能

键盘布局配置的增强功能

键盘布局配置现在包括不同步选项。该选项可用于组策略对象 (GPO) 策略和 GUI 配置。

选择不同步选项时，将在会话中使用服务器键盘布局，并且不将客户端键盘布局与服务器键盘布局同步。

有关详细信息，请参阅键盘布局和语言栏。

用于禁用存储身份验证令牌的选项

身份验证令牌会加密并存储在本地磁盘上，这样您就不需要在系统或会话重新启动时重新输入凭据。

Citrix Workspace 应用程序引入了用于禁止在本地磁盘上存储身份验证令牌的选项。为了增强安全性，我们现在提供了组策略对象 (GPO) 策略来配置身份验证令牌存储。

> 注意：
>
> 此配置仅在云部署中适用。

有关详细信息，请参阅身份验证令牌。

Microsoft Teams 增强功能

- 默认情况下，VP9 视频编解码器现在处于禁用状态。
- 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**。
- `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。

已修复的问题

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）。可以使用 GPO 选项禁用此修复。如果禁用此修复，cookie 将不存储，并在注销过程中清除。

[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，您可能无法授权登录。此外，无法使用其他用户帐户登录。[CVADHELP-14844]

安全问题

- 此修复提高了底层组件的安全性。[RFWIN-20912]

会话/连接

- 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]
- 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。适用于 Windows 的 Citrix Workspace 应用程序无法使用代理端口而改为使用默认端口 8080 时会出现此问题。[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]
- 在用户会话中按下 **ALT** + **Tab** 键时，可能会打开适用于 Windows 的 Citrix Workspace 应用程序的新空白窗口。[CVADHELP-16379]
- 即使受保护的窗口已最小化，**Print Screen** 键也可能无法捕获屏幕截图。[RFWIN-16777]
- 如果您在 Microsoft Teams 通话中使用网络摄像机或视频，`HDXrtcengine.exe` 可能会变得无响应。解决方法：请参阅知识中心文章 CTX296639。[HDX-29122]
- 尝试使用 IME 撰写 DBCS 文本时，可能缺少下划线。Windows 10 2004 操作系统会出现此问题。[RFWIN-20006]
- 错误地设置 `C:\ProgramData\Citrix` 文件夹的权限可能会导致 Citrix Workspace 应用程序意外退出。[RFWIN-22753]
- 在 Microsoft Teams 视频通话过程中，摄像机上的 LED 可能会闪烁，预览视频可能会停止。[CVADHELP-16383]

用户界面

- 单击“退出”选项一次时，适用于 Windows 的 Citrix Workspace 应用程序可能无法关闭。解决方法为，选择两次“退出”选项以关闭 Workspace 应用程序。[RFWIN-21518]

要了解产品中的现有问题，请参阅已知问题。

2102

新增功能

代理身份验证支持

以前，在配置了代理身份验证的客户端计算机上，如果 **Windows** 凭据管理器中不存在代理凭据，则不允许您向 Citrix Workspace 应用程序进行身份验证。

现在，在配置了代理身份验证的客户端计算机上，如果代理凭据未存储在 **Windows** 凭据管理器中，则会显示身份验证提示，要求您输入代理凭据。然后，Citrix Workspace 应用程序将代理服务器凭据保存在 **Windows** 凭据管理器中。这样可以打造无缝登录体验，因为您无需在访问 Citrix Workspace 应用程序之前在 Windows 凭据管理器中手动保存凭据。

Microsoft Teams 增强功能

- 改进了视频呈现效果。
- 提高了性能和可靠性。

已修复的问题

会话/连接

- 当您尝试使用启用了 vPrefer 选项的 Citrix Workspace 应用程序从已发布桌面上的收藏夹中打开某个应用程序时，该应用程序在打开时可能会显示一个旋转圆圈。如果这个旋转圆圈一直存在，则无法再次打开该应用程序。[CVADHELP-13237]
- 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]
- 以繁体中文或日语提供应用程序名称时，`StoreBrowse.exe` 命令可能无法显示已发布应用程序的完整列表。[CVADHELP-15952]
- 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]
- 日志收集功能可能无法收集 CDF 跟踪。[CVADHELP-16587]

系统异常

- `Receiver.exe` 进程可能会意外退出。[CVADHELP-15669]

用户界面

- 使用中文或日语输入法编辑器 (IME) 在文本框中输入文本时，文本可能会显示在屏幕左上角的文本框之外。[CVADHELP-15614]

要了解产品中的现有问题，请参阅已知问题。

2012.1

新增功能

此版本解决了有助于改进整体性能和稳定性的问题。

已修复的问题

- 将 Citrix Workspace 应用程序从版本 2012 自动更新到更高版本失败，并显示以下错误消息：

  “Could not load file or assemble Newtonsoft.Json”（无法加载文件或程序集 Newtonsoft.Json）

  仅当在 Citrix Workspace 应用程序的管理员安装的实例上启用了自动更新时才会出现此问题。

  解决方法为，从 Citrix 下载页面下载 Citrix Workspace 应用程序版本 2012.1 或更高版本并手动安装。

  [RFWIN-21715]

要了解产品中的现有问题，请参阅已知问题。

2012

新增功能

支持意大利语

适用于 Windows 的 Citrix Workspace 应用程序现在提供意大利语版本。

日志收集

日志收集简化了 Citrix Workspace 应用程序收集日志的过程。这些日志可帮助 Citrix 进行故障排除，并在出现复杂问题的情况下辅助提供支持。

现在，您可以使用 GUI 收集日志。

有关详细信息，请参阅日志收集。

支持对 **Citrix Workspace** 进行域直通身份验证

本版本引入了对 Citrix Workspace 进行域直通身份验证的支持以及对 StoreFront 的现有支持。

面向 **Citrix Workspace** 的无提示身份验证

Citrix Workspace 应用程序引入了组策略对象 (GPO) 策略以启用面向 Citrix Workspace 的无提示身份验证。此策略使 Citrix Workspace 应用程序能够在系统启动时自动登录 Citrix Workspace。仅当为加入了域的设备上的 Citrix Workspace 配置了域直通（单点登录）时，才使用此策略。

有关详细信息，请参阅无提示身份验证。

应用程序保护配置的增强功能

以前，默认情况下，身份验证管理器和自助服务插件对话框受到保护。

本版本引入了组策略对象 (GPO) 策略，该策略允许您同时为身份验证管理器和自助服务插件界面分别配置反键盘记录和反屏幕捕获功能。

> 注意：
>
> 此 GPO 策略不适用于 ICA 和 SaaS 会话。ICA 和 SaaS 会话继续使用 Delivery Controller 和 Citrix Secure Private Access 进行控制。

有关详细信息，请参阅应用程序保护配置的增强功能。

Microsoft Teams 增强功能

- 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。
- WebRTC 媒体引擎现在支持在客户端设备上配置的代理服务器。

已修复的问题

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]

会话/连接

- 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]
- 执行以下操作之一时，可能会出现安全警告对话框：
  - 使用 **Storebrowse** 命令从 StoreFront 检索 ICA 文件。
  - 使用 ICA 文件启动应用程序，而非从浏览器启动。

  [CVADHELP-15221]
- 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]

- 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]
- 尝试在 Microsoft Teams 通话中共享您的屏幕可能会导致黑屏。[HDX-27041]
- 在 Microsoft Teams 通话中，音频可能会断断续续。禁用 UDP 流量端口时会出现此问题。[HDX-27914]

用户体验

- 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]
- 如果 “高 DPI” 设置为 “是” 或 “否”，则在启动桌面会话时，**CD Viewer** 工具栏中的某些元素可能无法向上扩展以匹配设备的当前 DPI 设置。用户设备的 DPI 设置大于 100% 时会出现此问题。[CVADHELP-15418]
- 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]

要了解产品中的现有问题，请参阅已知问题。

已知问题

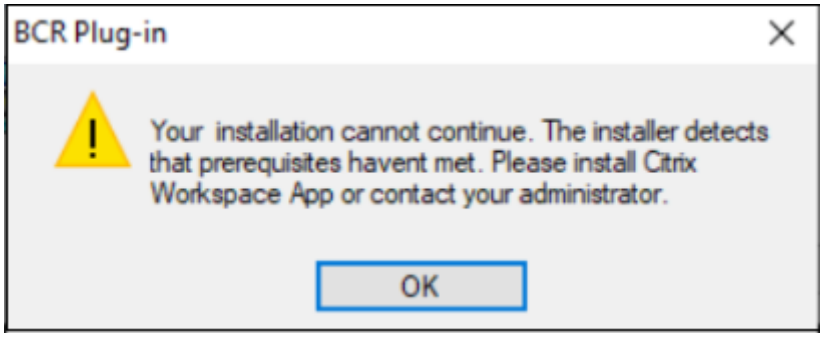
2302 中的已知问题

- 您可能无法在 Bloomberg 键盘 5 或 Bloomberg 键盘 2013 上使用 Bloomberg 终端应用程序。在启用了应用程序保护功能的系统中安装 Citrix Workspace 应用程序版本 2302 时会出现此问题。解决方法是，升级到 Citrix Workspace 应用程序版本 2303 或者创建以下注册表项并重新启动计算机：
  - 注册表项：HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\epusbfilter
  - 值：[DWORD]
  - DisableUSBFiltering= 1

  [CVADHELP-22221]

2212 中的已知问题

- 当无法修复 BCRClient.msi 时，在 Citrix Workspace 应用程序安装期间会出现以下错误：



[HDX-46964]

- 如果 Citrix Enterprise Browser 是默认浏览器，某些已关闭增强的安全性的 SaaS 应用程序无法在 Citrix Enterprise Browser 中打开。[CTXBR-4106]

2210.5 中的已知问题

- 在无缝模式下打开已发布的应用程序时，其他本地应用程序或无缝应用程序可能会出现在前台并覆盖已发布的应用程序。[CVADHELP-20742]
- 在某些较旧的 AMD GPU 系列中，Citrix Workspace 应用程序 2206 或更高版本可能会看到紫色视频内容或屏幕闪烁。
  解决方法是修改以下注册表：
  - Key: HKLM\SOFTWARE\WOW6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Gf
  - Value: [DWORD]
  - ForceVP= 1

  [HDX-46264]

2210 中的已知问题

- 当桌面处于正常分辨率和 DPI 时，**Desktop Viewer** 工具栏可能会覆盖屏幕。[HDX-45206]
- **Desktop Viewer** 工具栏在全屏模式下可能无法正确显示，并且显示选项的顺序不正确。[HDX-45189]
- 重新连接桌面时，窗口的位置和大小可能不会保持不变。[HDX-44997]

2209 中的已知问题

在此版本中没有发现新问题。

2207 中的已知问题

在此版本中没有发现新问题。

2206 中的已知问题

在此版本中没有发现新问题。

2205 中的已知问题

- 在适用于 Windows 的 Citrix Workspace 应用程序中，高级音频编码 (AAC) 最多只能支持 6 个通道。[CTXBR-2941]
- 插入 USB 设备或访问文件时，Citrix Workspace 应用程序可能会显示旧版 **Citrix Workspace -** 安全警告对话框。[LCM-10369]
- 在 DDC 上启用自动显示键盘策略后，会话期间可能不会显示电池状态通知和自动键盘弹出对话框。[HDX-39558]

2204.1 中的已知问题

- 安装程序在您的系统中找不到 Microsoft Edge WebView2 时，在脱机模式下安装适用于 Windows 的 Citrix Workspace 应用程序可能会失败。

  解决方法：以管理员身份安装 **MicrosoftEdgeWebView2RuntimeInstallerX86.exe**，然后尝试安装适用于 Windows 的 Citrix Workspace 应用程序。

  [RFWIN-26329]

2202 中的已知问题

- Citrix Workspace 应用程序的全新安装或更新操作可能会导致延迟约 10-30 分钟。有关详细信息，请参阅 Citrix 知识中心文章 CTX335639。[RFWIN-25752]

2112.1 中的已知问题

- 当启用了应用程序保护的适用于 Windows 的 Citrix Workspace 应用程序在后台启动时，Print Screen 键可能无法捕获屏幕截图。[RFWIN-25835]
- Citrix Workspace 应用程序的全新安装或更新操作可能会导致延迟约 10-30 分钟。有关详细信息，请参阅 Citrix 知识中心文章 CTX335639。[RFWIN-25752]
- 启用代理身份验证后，从适用于 Windows 的 Citrix Workspace 应用程序注销可能不会成功。[RFWIN-24813]
- 如果您在 Microsoft Windows 11 计算机上使用 Citrix Workspace 应用程序，活动源和操作选项卡可能会丢失。[WSP-13311]
- 使用 Citrix Enterprise Browser 时，即使受保护的窗口已最小化，也无法截取不受保护的 URL 窗口的屏幕截图。[CTXBR-1925]
- 如果您启用了“浏览器内容重定向”功能，则无法登录 Google Meet。[HDX-34649]
  解决方法：

1. 确保 https://www.youtube.com/* 在访问控制列表中。
2. 确保 https://accounts.google.com/* 在身份验证站点列表中。
3. 在任何 Google 中介站点（例如 YouTube）上登录您的 Google 帐户。
4. 在 Google Chrome 的同一实例中启动 Google Meet。

- 在 Citrix Workspace 应用程序 2112.1 中，在优化的 Microsoft Teams 视频通话中打开网络摄像机时，端点上的 CPU 利用率可能会很高。
  解决方法：在端点上创建以下注册表值：

  Computer\HKEY_CURRENT_USER\SOFTWARE\Citrix\HDXMediaStream
  名称：UseDefaultCameraConfig
  类型：REG_DWORD
  值：0

  [HDX-37168]

- 在 Citrix Workspace 应用程序中，在接听或拨打 Microsoft Teams 电话时，您可能会遇到间歇性故障。此时将显示以下错误消息：

  Call could not be established.（无法建立呼叫。）

  解决方法：尝试重新建立 Microsoft Teams 通话。

  [HDX-38819]

2109.1 中的已知问题

在此版本中没有发现新问题。

2109 中的已知问题

如果您以用户身份安装了版本低于 2109 的 Workspace 应用程序，而管理员安装的版本为 21.0.9，则当您以用户身份重新登录设备时，将显示 **Entry point not found**（找不到入口点）错误消息。单击确定时，该消息将消失，并且 Workspace 应用程序将更新到版本 21.0.9。[RFWIN-25008]

如果您的管理员在 Google Chrome 中安装了外部扩展，则当打开时 Citrix Enterprise Browser 将崩溃。[CTXBR-2135]

2108 中的已知问题

用户名包含西里尔字符或东亚字符时，会话在客户端计算机上在脱机模式（服务连续性）下无法启动。[RFWIN-23906]

2107 中的已知问题

在此版本中没有发现新问题。

2106 中的已知问题

- 在启用了服务连续性功能的应用商店中，您可能无法启动资源。Unicode 用户会遇到此问题。[RFWIN-23439]
- 尝试使用 VDA 上安装的适用于 Windows 的 Citrix Workspace 应用程序重定向网络摄像机时，网络摄像机可能会出现故障。[HDX-28691]

2105 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]

2103.1 中的已知问题

- 自助服务插件窗口为空，会话启动时不显示任何应用程序。由于第三方的限制，使用 Intel Xe 图形卡时会出现此问题。[CVADHELP-17005]
- 尝试使用日语、中文或韩语 IME 撰写字符可能无法正常工作。撰写窗口看上去放错位置，不是无缝的。使用虚拟应用程序和桌面会话和 SaaS 应用程序时不会出现此问题。[RFWIN-21158]
- 尝试退出 Citrix Workspace 应用程序可能会失败。当用户凭据提示反复出现时会出现此问题。[RFWIN-22491]
- 为应用程序创建桌面快捷方式并重新启动客户端设备后，首次尝试从快捷方式启动应用程序可能会失败。使用命令行界面安装 Citrix Workspace 应用程序时，如果未指定 `storedescription`，则会出现此问题。[RFWIN-22510]
- 从 Citrix Files 下载.txt 文件时，日语文件名可能会出现乱码。[RFWIN-22516]
- 当您尝试使用 Microsoft Teams HDX 优化进行点对点通话时，通话可能会失败。如果 VDA 版本为 2103 或更低版本，适用于 Windows 的 Workspace 应用程序为 2103 或更高版本，则会出现此问题。此问题在 Virtual Delivery Agent (VDA) 2106 中已修复。

2102 中的已知问题

- 尝试启动 ICA 会话可能会失败。当代理服务器使用端口 8080 而不是自定义端口时，会出现此问题。[CVADHELP-15977]
- 在应用程序会话中，当您在 Microsoft Paint 中打开要扫描的图像时，Microsoft Paint 应用程序和扫描过程可能都变得无响应。在窗口化模式下启动会话时会出现此问题。[RFWIN-21413]
- 在配置了 Azure Active Directory 多重身份验证 (MFA) 的计算机上，即使已选择使我保持登录状态和 **60** 天内不再询问选项，系统也会显示登录提示。[RFWIN-21623]
- 在已加入 Azure Active Directory 的计算机上尝试登录 Citrix Workspace 应用程序可能会失败。未显示身份验证提示时会出现此问题。[RFWIN-21624]
- 启动已发布的桌面会话时，自助服务插件对话框将显示在前台。在 Delivery Controller 上启用本地应用程序访问策略时，会出现此问题。[RFWIN-21629]
- 使用 **ALT** + **Tab** 键尝试切换窗口可能会导致 Citrix Workspace 应用程序出现空白屏幕。在窗口化模式下启动会话时会出现此问题。[RFWIN-21828]
- 如果您在 Microsoft Teams 通话中使用网络摄像机或视频，`HDXrtcengine.exe` 可能会变得无响应。解决方法：请参阅知识中心文章 CTX296639。[HDX-29122]

2012.1 中的已知问题

在此版本中没有发现新问题。

2012 中的已知问题

- 如果您尝试将受保护的应用程序添加到收藏夹，则可能会显示以下消息：“您的应用程序当前不可用...”然后单击确定时，将显示以下消息：“无法添加应用程序。”切换到收藏夹屏幕后，受保护的应用程序将在此处列出，但无法将其从收藏夹中删除。[WSP-5497]
- 在启用了浏览器内容重定向的 Chrome 浏览器中，当您单击打开新选项卡的链接时，该选项卡可能无法打开。解决方法为，在 **Pop-ups blocked**（阻止了弹出窗口）消息中选择 **Always allow pop-ups and redirects**（始终允许弹出窗口和重定向）。[HDX-23950]
- 将 Citrix Workspace 应用程序从版本 2012 自动更新到更高版本失败，并显示以下错误消息：

  Could not load file or assemble Newtonsoft.Json（无法加载文件或程序集 Newtonsoft.Json）

  仅当在 Citrix Workspace 应用程序的管理员安装的实例上启用了自动更新时才会出现此问题。

  解决方法为，从 Citrix 下载页面下载 Citrix Workspace 应用程序版本 2012.1 或更高版本并手动安装。

  [RFWIN-21715]
- 如果启动应用程序栏，然后在适用于 Windows 的 Citrix Workspace 应用程序中打开连接中心菜单，应用程序栏不会显示在对其进行托管的服务器下。[HDX-27504]
- 如果使用适用于 Windows 的 Citrix Workspace 应用程序并在垂直位置启动应用程序栏，该应用程序栏将覆盖“开始”菜单或系统时钟托盘。[HDX-27505]

旧版文档

有关生命周期已结束 (EOL) 的产品版本，请参阅旧版文档。

第三方声明

适用于 Windows 的 Citrix Workspace 应用程序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

February 16, 2023

要求

- 最低 1 GB RAM。
- 下表提供了有关安装 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

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

- Microsoft Edge WebView2 Runtime 版本 102 或更高版本。

> 注意：
>
> 从 Citrix Workspace 应用程序版本 2107 开始，Microsoft Edge WebView2 Evergreen Bootstrapper 与 Citrix Workspace 应用程序安装程序打包在一起。Evergreen Bootstrapper 是一款小型安装程序，可下载与设备体系结构匹配的 WebView2 Runtime 版本并在本地进行安装。
>
> 在 Workspace 应用程序安装期间，安装程序会检查系统中是否存在 Microsoft Edge WebView2 Runtime，如果找不到，则会进行安装。
>
> 您必须连接到 **Internet** 才能下载和安装 **Microsoft Edge WebView2 Runtime**。
>
> 如果您尝试以非管理员权限安装或升级 Citrix Workspace 应用程序，但 Microsoft Edge WebView2 Runtime 不存在，安装将停止并显示以下消息：
>
> 必须以管理员身份登录才能安装以下必备软件包:
>
> Edge Webview2 Runtime”

- 自助服务插件需要 NET 4.8。此插件允许您从 Workspace 用户界面或命令行订阅和启动应用程序和桌面。

  当您尝试安装或升级到 Citrix Workspace 应用程序 1904 或更高版本，但必备的.NET Framework 版本在 Windows 系统中不可用时，Citrix Workspace 应用程序安装程序将下载并安装所需的.NET Framework 版本。

  > 注意：
  >
  > 当您尝试使用非管理员权限安装或升级 Citrix Workspace 应用程序，但系统中没有.NET Framework 4.8 或更高版本时，安装将失败。

- 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，Microsoft Visual C++ Redistributable 安装程序随 Citrix Workspace 应用程序安装程序打包。Workspace 应用程序安装过程中，安装程序会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。

> 注意：
>
> 如果您的系统中不存在 Microsoft Visual C++ 可再发行组件包，使用非管理员权限安装 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 Citrix 知识中心文章 CTX250044。

> 注意：
>
> 您必须连接到 **Internet** 才能下载和安装**.NET Framework** 和 **Microsoft Visual C++ Redistributable**。否则，管理员可以使用部署方法（例如 **SCCM**）安装这些要求。

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。

> 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。
> - 仅当客户获得了 Microsoft 的主流支持或扩展支持时，才支持在 Windows 上安装 Citrix Workspace 应用程序。
> - Windows ARM64 操作系统仅在仿真器模式下支持适用于 Windows 的 Citrix Workspace 应用程序。
> - 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。

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

操作系统
Windows 11
Windows 10 Enterprise（32 位和 64 位版本）。有关兼容的 Windows 10 版本的详细信息，请参阅 Windows 10 与适用于 Windows 的 Citrix Workspace 应用程序的兼容性。
Windows 10 Enterprise（2016 LTSB 1607、LTSC 2019）
Windows 10（Home Edition*、Pro）
Windows Server 2022
Windows Server 2019
Windows Server 2016

* 不支持域直通身份验证、Desktop Lock、FastConnect API 以及需要加入域的 Windows 计算机的配置。

Windows 10 或 **11** 与适用于 **Windows** 的 **Citrix Workspace** 应用程序的兼容性

下表列出了 Windows 10 版本号以及适用于 Windows 的 Citrix Workspace 应用程序的相应兼容版本。

Windows 10 版本号	内部版本号	Citrix Workspace 应用程序版本
22H2	19045	2206 及更高版本
21H2	19044	2112.1 及更高版本
21H1	19043.928	2106 及更高版本
20H2	19042.508	2012 及更高版本
2004	19041.113	2006.1 及更高版本
1909	18363.418	1911 及更高版本
1903	18362.116	1909 及更高版本
1809	17763.107	1812 及更高版本
1803	17134.376	1808 及更高版本

> 注意：
>
> Windows 10 版本仅与提及的 Citrix Workspace 应用程序版本兼容。例如，Windows 10 版本 21H1 与 2106 之前的版本不兼容。

下表列出了 Windows 11 版本号以及适用于 Windows 的 Citrix Workspace 应用程序的相应兼容版本。

Windows 11 版本号	内部版本号	Citrix Workspace 应用程序版本
22H2	22621	2209 及更高版本
21H2	22000	2109.1 及更高版本

安装和卸载

March 29, 2023

可以通过以下方式安装 Citrix Workspace 应用程序：

- 从下载页面下载 `CitrixWorkspaceApp.exe` 安装包，或者
- 从贵公司的下载页面（如果可用）。

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：
>
> 管理员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。

使用基于 **Windows** 的安装程序

可以通过使用以下方法手动运行 `CitrixWorkspaceApp.exe` 安装程序包来安装适用于 Windows 的 Citrix Workspace 应用程序：

- 安装介质
- 网络共享
- Windows 资源管理器
- 命令行接口

默认情况下，安装程序日志位于以下位置：

- 在 32 位 Windows 操作系统中 - `C:\Program Files\Citrix\Logs`
- 在 64 位 Windows 操作系统中 - `C:\Program Files (x86)\Citrix\Logs` 或 `C:\Users\<Install Username>\AppData\Local\Temp`

1. 启动 `CitrixWorkspaceApp.exe` 文件并单击启动。
2. 阅读并接受 EULA，然后继续安装。
3. 在具有管理员权限的已加入域的计算机上进行安装时，会出现一个单点登对话框录。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。

安装完成后，Citrix Workspace 应用程序会请求您添加一个帐户。有关如何添加帐户的信息，请参阅添加帐户或切换服务器。

使用命令行参数

可以通过指定不同的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目录。空间要求包括程序文件、用户数据以及启动多个应用程序后使用的临时目录。

要使用 Windows 命令行安装 Citrix Workspace 应用程序，请启动命令提示符并在一行中键入以下内容：

- 安装程序文件名，
- 安装命令，以及
- 安装属性

可用的安装命令和属性如下：

```
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 - 在安装过程中禁止显示重新启动提示。禁止显示重新启动提示时，处于暂停状态的 USB 设备无法识别。只有在重新启动设备后才会激活 USB 设备。
- /includeSSON - 要求您以管理员身份安装。指示 Citrix Workspace 应用程序随 Single Sign-On 组件安装。有关详细信息，请参阅域直通身份验证。
- /forceinstall - 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：请在以下情况下使用此开关：
  - 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。

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

安装参数

/AutoUpdateCheck

指示 Citrix Workspace 应用程序在有可用更新时进行检测。

> 注意：
>
> /AutoUpdateCheck 为必需参数，必须设置才能配置 /AutoUpdateStream、/DeferUpdateCount、/AURolloutPriority 等其他参数。

- 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，则可以选择要更新的版本。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。不再提醒您有关此更新的信息。例如，CitrixWorkspaceApp.exe /DeferUpdateCount=0。
- 任何其他数字 “n”- 允许推迟通知 “n” 次。以后提醒我选项显示 “n” 次。例如，CitrixWorkspaceApp.exe /DeferUpdateCount=<n>。

/AURolloutPriority

新版本的应用程序可用时，Citrix 会在特定交付期间推出更新。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。

/startAppProtection

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，启动应用程序保护组件并提供增强的安全性。

- CitrixWorkspaceApp.exe /startAppProtection

有关详细信息，请参阅应用程序保护。

> 注意：
>
> /startAppProtection 开关是 /includeAppProtection 开关的替换。/includeAppProtection 开关自版本 2212 起已弃用。有关详细信息，请参阅弃用。

/InstallEmbeddedBrowser

排除 Citrix 嵌入式浏览器二进制文件。运行 /InstallEmbeddedBrowser=N 开关以排除嵌入式浏览器功能。

仅在以下情况下才能排除 Citrix 嵌入式浏览器二进制文件：

- 全新安装
- 从不包含 Citrix 嵌入式浏览器二进制文件的版本进行升级。

如果您的 Citrix Workspace 应用程序版本包含 Citrix 嵌入式浏览器二进制文件，并且您正在升级到版本 2002，则嵌入式浏览器二进制文件会在升级期间自动更新。

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`。

/IncludeCitrixCasting

在安装过程中安装 Citrix Casting。

> 注意：
>
> 当您更新 Citrix Workspace 应用程序时，Citrix Casting 会自动更新。有关 Citrix Casting 的详细信息，请参阅 Citrix Casting。

ADDLOCAL

使用 `ADDLOCAL` 键安装 Citrix Workspace 应用程序的一个或多个特定组件。使用此键时，如果安装任何特定组件，Citrix Workspace 应用程序将默认安装所有必需组件。

> 注意：
>
> 我们建议您仅在想要安装 Citrix Workspace 应用程序的任何特定组件时才使用 `ADDLOCAL` 键。默认情况下，如果未指定任何 `ADDLOCAL` 参数，则在安装 Citrix Workspace 应用程序时将安装支持的所有组件。

下表列出了 `ADDLOCAL` 键支持的组件：

`ADDLOCAL` 键	组件名称	说明
`ReceiverInside`	Receiver	为自助服务插件提供工作区 SDK 服务。
`ICA_Client`	HDX 引擎	此组件负责处理 ICA 文件或会话启动过程。
`BCR_Client`	BCR 客户端	用于处理浏览内容重定向的插件。
`USB`	USB 客户端	用于处理 USB 重定向的插件。
`DesktopViewer`	Desktop Viewer 客户端	虚拟桌面的用户界面框架。
`AM`	AuthManager	身份验证管理器 - 授权用户访问 Citrix Workspace 应用程序。
`SSON`	SSON	单点登录组件 - 支持单点登录。

ADDLOCAL 键	组件名称	说明
SELFSERVICE	自助服务	适用于 Citrix Workspace 的插件，用于本机启动。
WebHelper	Web 帮助程序	用于将浏览器与本机 Workspace 应用程序连接的帮助程序。
WorkspaceHub	Win Docker	提供一种扩展用户的工作区、以无线方式进行镜像或扩展本地显示的方法。
CitrixEnterpriseBrowser	浏览器	允许用户在 Citrix Workspace 应用程序中以安全的方式打开 Web 或 SaaS 应用程序的本机浏览器。

例如，使用以下命令，您可以安装命令中提到的组件：

```
CitrixWorkspaceapp.exe ADDLOCAL=ReceiverInside,ICA_Client,BCR_Client,
    USB,DesktopViewer,AM,SSON,SelfService,WebHelper,WorkspaceHub,
    CitrixEnterpriseBrowser
<!--NeedCopy-->
```

> 注意：
>
> 自版本 2212 起，默认安装应用程序保护功能。因此，AppProtection 不再是 ADDLOCAL 的有效选项。

HDX 功能参数

ALLOW_BIDIRCONTENTREDIRECTION

指示是否在客户端与主机之间启用了双向内容重定向。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_BIDIRCONTENTREDIRECTION =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。请使用管理员权限安装 Workspace 应用程序，以便此组件能够运行。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

指定您是否希望显示与订购的应用程序具有文件类型关联的文档或文件的图标。

- False（默认设置）- 显示与订购的应用程序具有文件类型关联的文档或文件的图标。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`。
- True - 不显示与订阅的应用程序具有文件类型关联的文档或文件的图标。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 Citrix Workspace 应用程序协议的应用商店。

- 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目录。

- <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

指定桌面快捷方式的目录。

> 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 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。有关详细信息，请参阅 CEIP。

- True（默认设置）- 选择加入 Citrix 客户体验改善计划 (CEIP)。例如，CitrixWorkspaceApp.exe EnableCEIP=True。
- False - 选择退出 Citrix 客户体验改善计划 (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。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

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 Single Sign-on 处于启用状态。例如，CitrixWorkspaceApp.exe ENABLE_SSON=Yes。
- 否 - 指示 Single Sign-on 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，并且仅在启用单点登录身份验证时才需要。有关详细信息，请参阅使用 Kerberos 的域直通身份验证。

- 是 - 指示 HDX 引擎必须使用 Kerberos 身份验证。例如，CitrixWorkspaceApp.exe ENABLE_KERBEROS=Yes。
- 否 - 指示 HDX 引擎不使用 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 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，在记事本中将其打开，然后复制 **Address** 元素中的 URL。
- [On, Off] - **Off** 选项允许您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。如果未指定应用商店状态，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：
>
> - Citrix Gateway 应用商店 URL 必须是列表中的第一个 URL（参数 STORE0）。
> - 在多应用商店设置中，只允许使用一种 Citrix Gateway 应用商店 URL 配置。
> - 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。
> - 指定 Citrix Gateway 应用商店 URL 时，不需要 “/Discovery” 参数。

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。

重置 **Citrix Workspace** 应用程序

重置 Citrix Workspace 应用程序将还原默认设置。

重置 Citrix Workspace 应用程序时，以下项目将重置：

- 所有已配置的帐户和应用商店。
- 自助服务插件提供的应用程序、其图标和注册表项。
- 自助服务插件创建的文件类型关联。
- 缓存的文件和保存的密码。
- 每用户注册表设置。
- 每计算机安装及其注册表设置。
- 适用于 Citrix Workspace 应用程序的 Citrix Gateway 注册表设置。

从命令行界面运行以下命令以重置 Citrix Workspace 应用程序：

```
C:\Program Files (x86)\Citrix\ICA Client\SelfServicePlugin\CleanUp.exe"-
cleanUser
```

要进行无提示重置，请使用以下命令：

```
C:\Program Files (x86)\Citrix\ICA Client\SelfServicePlugin\CleanUp.exe"/
silent -cleanUser
```

> 注意：
>
> 请在参数中使用大写 U。

重置 Citrix Workspace 应用程序不影响以下内容：

- Citrix Workspace 应用程序或插件安装。
- 每计算机 ICA 锁定设置。
- Citrix Workspace 应用程序的组策略对象 (GPO) 管理模板配置。

卸载

使用基于 **Windows** 的卸载程序：

可以从控制面板中卸载适用于 Windows 的 Citrix Workspace 应用程序。有关详细信息，请参阅卸载适用于 Windows 的 Citrix Workspace 应用程序部分。

> 注意：
>
> 在 Citrix Workspace 应用程序安装期间，您会收到一条卸载 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 Citrix Workspace 应用程序：

```
CitrixWorkspaceApp.exe /uninstall
```

对于无提示卸载 Citrix Workspace 应用程序，请运行以下开关：

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

> 注意：
>
> Citrix Workspace 应用程序安装程序不控制与 GPO 相关的注册表项，因此在卸载后会保留这些注册表项。如果发现任何条目，请使用 `gpedit` 更新或者手动将其删除。

部署

March 8, 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。
- 在启动适用于 Web 的 Workspace 之前，请安装适用于 Windows 的 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 Microsoft Endpoint Manager (Intune)。有关详细信息，请参阅在 Microsoft Endpoint Manager (Intune) 中部署 Citrix Workspace 应用程序。

使用 **Active Directory** 和示例脚本

可以使用 Active Directory 组策略脚本根据组织结构部署 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)。

有关在 Azure Active Directory 中创建 OU 的信息，请参阅在 Azure Active Directory 域服务托管域中创建组织单位 (OU)。

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，设置 `DesiredVersion = 3.3.0.XXXX` 以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 Citrix Workspace 应用程序安装程序软件包的网络共享，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 - 复制安装日志的网络共享以及脚本不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 应用程序的每计算机和每用户脚本示例。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	`CheckAndDeployWorkspaceP.bat`	`CheckAndRemoveWorkspacePerMachineS.bat`
每个用户	`CheckAndDeployWorkspacePerUserLogon.bat`	`CheckAndRemoveWorkspacePerUserLogo.bat`

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，将相应的脚本复制到显示的文件夹，然后关闭对话框。
5. 在属性菜单中，单击添加，然后使用浏览查找并添加新创建的脚本。

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

1. 将分配的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. 将选定要删除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**

借助适用于 Web 的 Workspace，您可以使用 Web 页面通过浏览器访问 StoreFront 应用商店。

在从浏览器连接到应用程序之前，请执行以下操作：

1. 安装适用于 Windows 的 Citrix Workspace 应用程序。
2. 从适用于 Web 的 Workspace 部署 Citrix Workspace 应用程序

如果适用于 Web 的 Workspace 检测到不存在兼容版本的 Citrix Workspace 应用程序，系统会显示一条提示。提示显示您必须下载并安装适用于 Windows 的 Citrix Workspace 应用程序。

> 注意：
>
> 适用于 Web 的 Workspace 不支持基于电子邮件的帐户发现。

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 StoreFront。

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。

可以使用以下四个部分通过 SCCM 部署 Citrix Workspace 应用程序：

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，指定应用程序信息，例如名称、制造商、软件版本。
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 /silent /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 - 键入当前 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）- 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。根据所配置的计划，安装将自动触发。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，然后单击 **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 **Browse**（浏览）选择限制集合。

   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：
>
> 当 **MSIRESTARTMANAGERCONTROL** 属性设置为 **False** 时，使用 SCCM 配置 Citrix Workspace 应用程序可能会失败。
> 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。

在 **Microsoft Endpoint Manager (Intune)** 中部署 **Citrix Workspace** 应用程序

要在 Microsoft Endpoint Manager (Intune) 中部署 Citrix Workspace 应用程序 - 本机 Win 32 应用程序，请执行以下操作：

1. 创建以下文件夹：
   - 用于存储安装所需的所有源文件的文件夹，例如 `C:\CitrixWorkspace_Executable`。
   - 输出文件所在的文件夹。输出文件位于 `.intunewin` 文件中，例如 `C:\Intune_CitrixWorkspaceApp`。
   - Microsoft Win32 Content Prep Tool 所在的文件夹，例如 `C:\Intune_WinAppTool`。此工具有助于将安装文件转换为 `.intunewin` 格式。您可以从 Microsoft-Win32-Content-Prep-Tool 下载打包工具。
2. 将安装所需的所有源文件转换为 `.intunewin` 文件：
   a) 启动命令提示符，然后转到存在 Microsoft Win32 Content Prep Tool 的文件夹，例如 `C:\Intune_WinAppTool`。
   b) 运行 `IntuneWinAppUtil.exe` 命令。
   c) 在提示符下，输入以下信息：
      - 源文件夹：`C:\CitrixWorkspace_Executable`
      - 安装文件：`CitrixWorkspaceApp.exe`
      - 输出文件夹：`C:\Intune_CitrixWorkspaceApp`
        `.intunewin` 文件已创建。
3. 将软件包添加到 Microsoft Endpoint Manager (Intune)：
   a) 打开 Microsoft Endpoint Manager (Intune) 控制台：`https://endpoint.microsoft.com/##home`。

> 注意：
>
> 以下指令只能在 https://endpoint.microsoft.com/##home 上执行。您也可以通过 https://portal.azure.com 添加软件包。

b) 单击 **Apps**（应用程序）> **Windows app**（Windows 应用程序），然后单击 **+Add**（+ 添加）。

c) 从 **App type**（应用程序类型）下拉列表中选择 **Windows app (Win 32)**（Windows 应用程序 (Win 32)）。

d) 单击 **App package file**（应用程序包文件），找到 CitrixWorkspaceApp.intunewin 文件，然后单击 **OK**（确定）。

e) 单击 **App information**（应用程序信息）并填写必填信息、名称、说明和发布者，然后单击 **OK**（确定）。

f) 单击 **Program**（程序），输入以下信息，然后单击 **OK**（确定）：

- 安装命令：`CitrixWorkspaceApp.exe /silent`
- 卸载命令：`CitrixWorkspaceApp.exe /uninstall`
- 安装行为：系统

g) 单击 **Requirement**（要求），输入所需的信息，然后单击 **OK**（确定）。

> 注意：
>
> 从 “Operating System Architecture”（操作系统体系结构）列表中同时选择 x64 和 x32。操作系统版本可以是 Win 1607 及更高版本中的任何版本。

h) 单击 **Detection rules**（检测规则），选择 **Manually configure detection rules**（手动配置检测规则）作为 **Rules format**（规则格式），然后单击 **OK**（确定）。

i) 单击 **Add**（添加），选择所需的 **Rule type**（规则类型），然后单击 **OK**（确定）。

- 如果 **Rule type**（规则类型）为 **File**（文件），则路径可以是 `C:\Program Files (x86)\Citrix\ICA Client\wfica32.exe`（示例）。
- 如果 **Rule type**（规则类型）为 **Registry**（注册表），请输入 `HKEY_CURRENT_USER\Software\Citrix` 作为 **Path**（路径），输入 **Key exists**（注册表项存在）作为 **Detection method**（检测方法）。

j) 单击 **Return codes**（返回代码），检查默认返回代码是否有效，然后单击 **OK**（确定）。

k) 单击 **Add**（添加）将应用程序添加到 Intune 中。

4. 验证部署是否成功：

a) 单击 **Home**（主页）> **Apps**（应用程序）> **Windows**。

b) 单击 **Device install status**（设备安装状态）。

设备状态显示安装了 Citrix Workspace 应用程序的设备数量。

更新

January 30, 2023

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。有关安装的信息，请参阅安装和卸载。

自动更新

新版本的 Citrix Workspace 应用程序可用时，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。当 LTSR 和当前版本的 Citrix Workspace 应用程序上的 HDX RTME 更新可用时，将显示一条通知。
> - 自版本 2105 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。有关日志记录的信息，请参阅日志收集部分。
> - 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。检查更新选项可用于 Citrix Workspace 应用程序的用户安装的实例和管理员安装的实例。
> - 您还可以在启用了代理自动配置 (PAC) 和 Web 代理自动发现协议 (WPAD) 检测时执行自动更新。当代理需要凭据进行身份验证时，不支持此功能。
> - 如果添加了非 EDCHE 密码套件，Citrix Workspace 将无法访问 Citrix 自动更新服务器，并且在自动更新期间会出现以下错误：
>
>   无法连接到服务器

手动或自动更新后，重新启动适用于 Windows 的 Citrix Workspace 应用程序。

可以通过高级首选项查看设备上安装的 Citrix Workspace 应用程序的当前版本，也可以从 HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\CitrixOnlinePluginPac 位置查询 **DisplayVersion** 注册表。

要在高级首选项中查看版本，请执行以下操作：

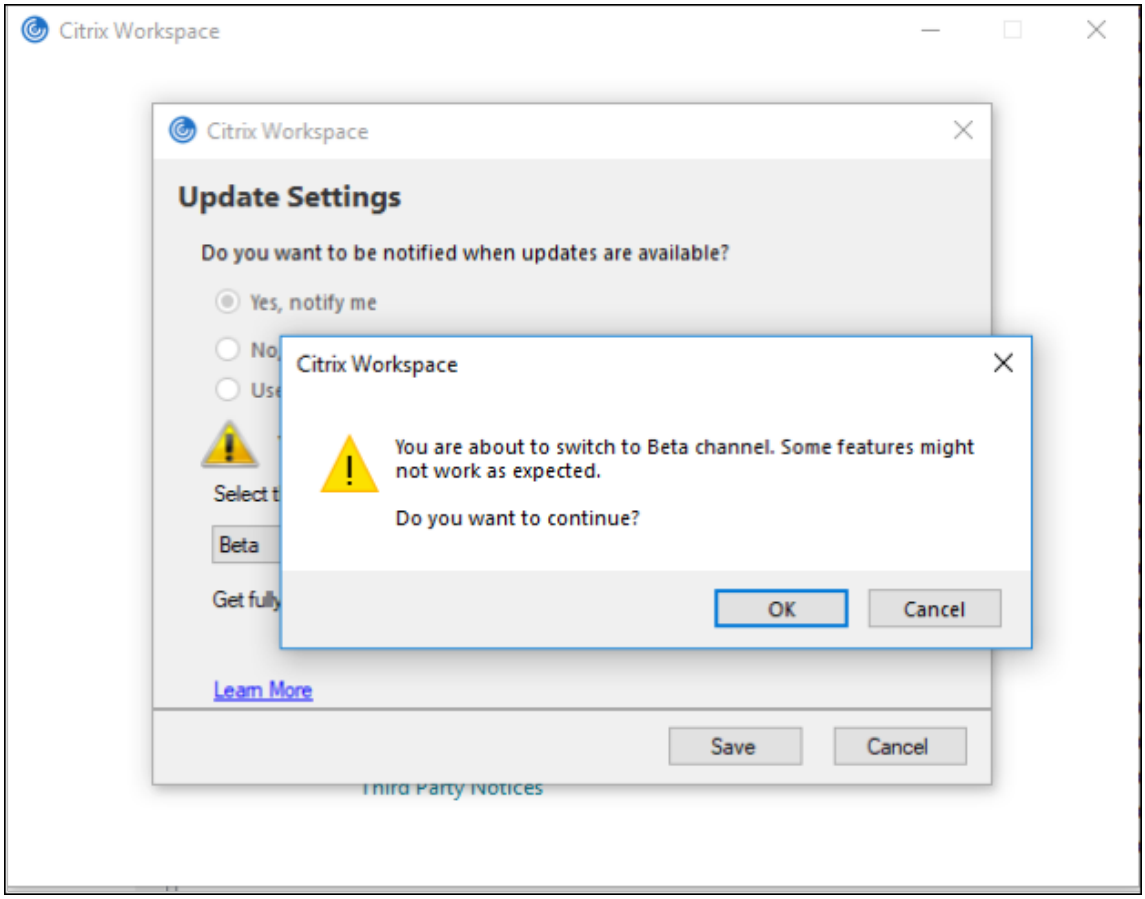
1. 右键单击通知区域中的 Citrix Workspace 应用程序图标。
2. 选择高级首选项。

   Citrix Workspace 应用程序版本显示在关于部分中。

安装 **Citrix Workspace** 应用程序 **Beta** 版程序

将 Citrix Workspace 应用程序配置为自动更新时，您将收到更新通知。要在您的系统中安装 Beta 版本，请执行以下步骤：

1. 从系统托盘打开 Citrix Workspace 应用程序。
2. 导航到高级首选项 > **Citrix Workspace** 更新。
3. Beta 版本可用时，从下拉列表中选择 **Beta**，单击保存。
   此时将显示通知窗口。



4. 单击确定更新到 Beta 版本。

要从 Beta 版本切换到发布版本，请执行以下步骤：

1. 从系统托盘打开 Citrix Workspace 应用程序。
2. 导航到高级首选项 > **Citrix Workspace** 更新。
3. 在更新设置屏幕中，从“更新通道”下拉列表中选择版本，然后单击保存。

> 注意：
>
> - 如果有任何新更新可用，则会显示自动更新通知。
> - Beta 版本可供客户在其非生产环境或有限生产环境中进行测试，并共享反馈。Citrix 不接受 Beta 版本的支持案例，但欢迎通过提供反馈来改进这些版本。Citrix 可能会根据反馈的严重性、紧迫性和重要性对反馈执行操作。建议不要在生产环境中部署 Beta 版本。

支持在 **VDA** 上自动更新 **Citrix Workspace** 应用程序

自适用于 Windows 的 Citrix Workspace 应用程序版本 2209 起，可以通过创建以下注册表值在 VDA 上启用自动更新功能：

在 32 位计算机上：

- 注册表项：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\AutoUpdate

- 注册表值：AllowAutoUpdateOnVDA
- 注册表类型：REG_SZ
- 注册表数据：True

在 64 位计算机上：

- 注册表项：HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\AutoUpdate
- 注册表值：AllowAutoUpdateOnVDA
- 注册表类型：REG_SZ
- 注册表数据：True

自动更新版本控制

管理员现在可以管理组织中的设备的自动更新版本。

管理员可以通过在 Global App Config Service 中设置 maximumAllowedVersion 属性中的版本来控制版本。

Global App Config Service 中的示例 JSON 文件：

```
"AutoUpdate": {


"userOverride": false,

"AutoUpdatePluginsSettings": [

    {


    "pluginSettings":

{
        "upgradeToLatest": false,
        "maximumAllowedVersion": "22.9.0.3934",                }


,

    "pluginName": "WorkspaceApp",

    "pluginId": "1CDF566D-B2C7-47F-6283C862E1D6"

   }


<!--NeedCopy-->
```


设置版本后，用户设备上的 Citrix Workspace 应用程序会自动更新到在 maximumAllowedVersion 属性中指定的版本。

> 备注：
>
> - 要实现自动更新版本控制，必须将 Global App Config Service 中的 upgradeToLatest 设置设为 false。如果设置为 true，则将忽略 maximumAllowedVersion。
> - 请勿修改 pluginId，因为它已映射到 Citrix Workspace 应用程序。
> - 如果管理员尚未在 Global App Config Service 中配置版本，则默认情况下，Citrix Workspace 应用程序将更新到最新的可用版本。

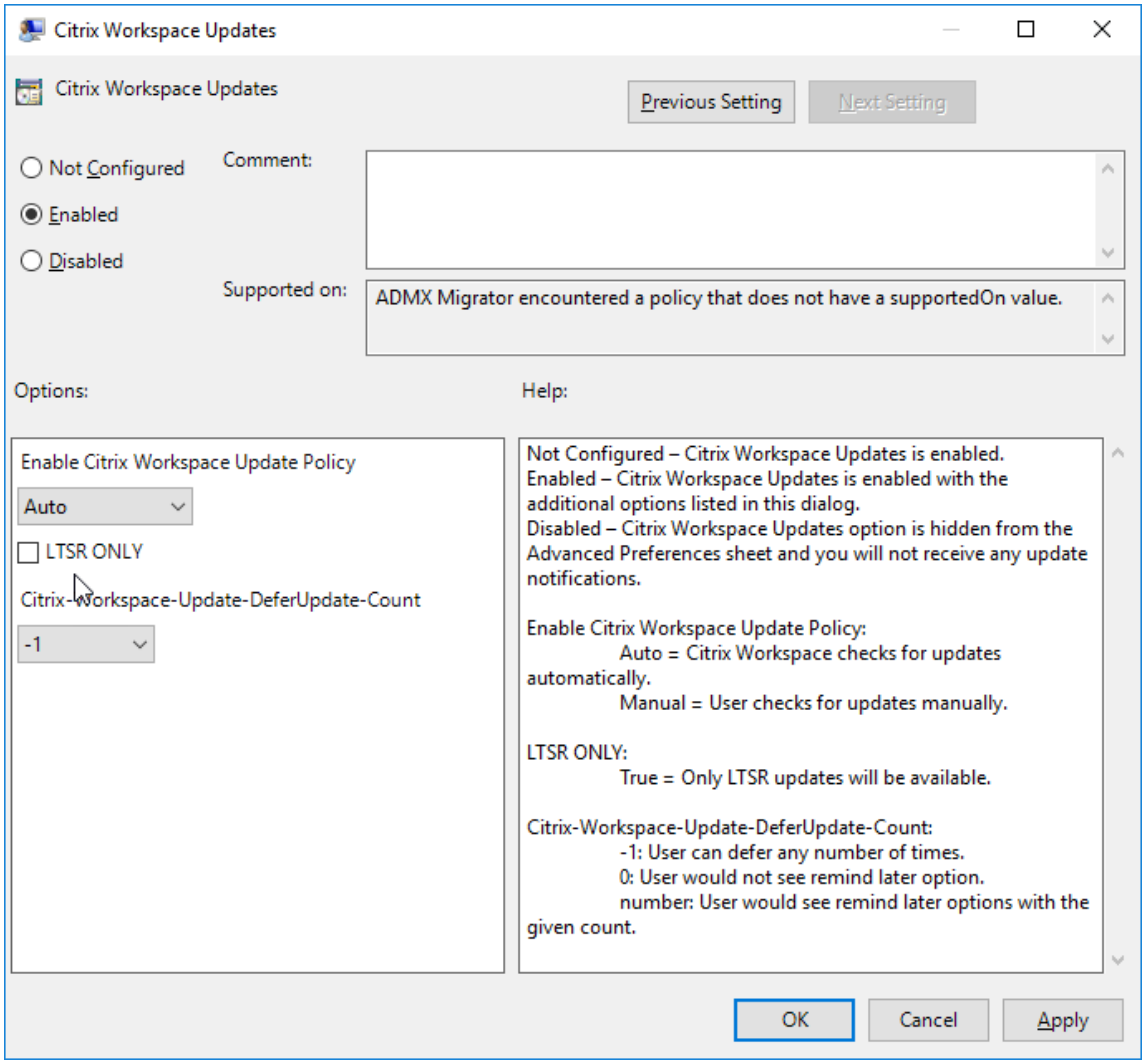
自动更新的高级配置（**Citrix Workspace** 更新）

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. GUI
4. StoreFront

使用组策略对象管理模板配置 **Citrix Workspace** 更新

1. 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。
2. 转到管理模板 > **Citrix** 组件 > **Citrix Workspace** > **Workspace** 更新。



3. 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。已禁用选项还将在高级首选项表中隐藏 Workspace 更新选项。

4. 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。

5. 选择仅限 **LTSR** 以仅获取 LTSR 的更新。

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

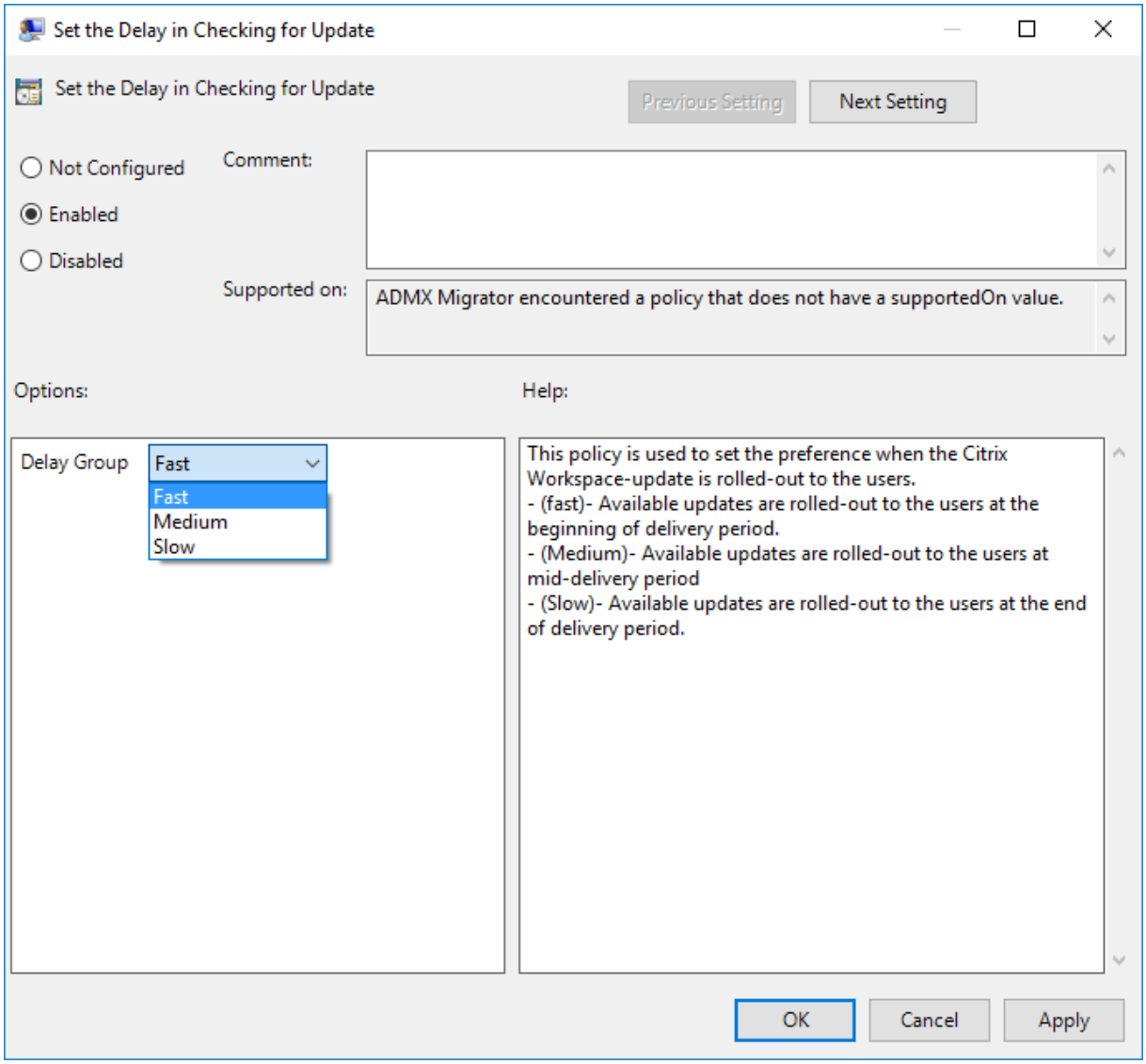
   - 如果值为 0，则不会出现以后提醒我选项。每次定期自动检查更新时都会显示 **Update available**（更新可用）提示。

- 如果值为 -1，则会显示以后提醒我选项，并显示 **Update available**（更新可用）提示。您可以将更新通知推迟任意次数。
- 介于 1-30 之间的值定义了带有 **Update available**（更新可用）提示的以后提醒我选项必须出现的次数。您可以根据在此字段中定义的值推迟更新通知。但是，**Update available**（更新可用）提示会继续出现，但不会出现以后提醒我选项。

配置检查更新的延迟

新版本的 Workspace 应用程序可用时，Citrix 会在特定交付期间推出更新。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。已即你用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 **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` 的位置。

通常，CitrixReceiverUpdater.exe 位于 `CitrixWorkspaceInstallLocation\Citrix\Ica Client\Receiver`。可以运行二进制文件 `CitrixReceiverUpdater.exe` 以及安装参数部分中列出的命令行参数。

例如，

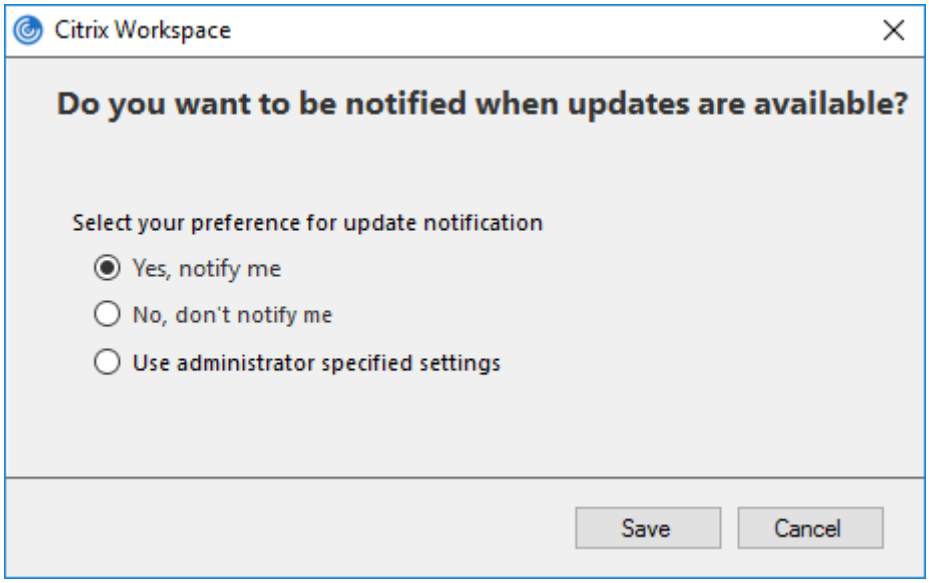
```
CitrixReceiverUpdater.exe /AutoUpdateCheck=auto /AutoUpdateStream=Current /DeferUpdateCount=-1 /AURolloutPriority=fast
```

> 注意：
>
> `/AutoUpdateCheck` 为必需参数，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。

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 > **Citrix Workspace** 更新。
3. 选择通知首选项，然后单击保存。



> 注意：
>
> 您可以隐藏 Citrix Workspace 应用程序图标中提供的“高级首选项”表的全部或部分内容。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`。
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"

```



```
7       description="" published="true" updaterType="Citrix"
            remoteAccessType="None">
8
9       <annotatedServices>
10
11        <clear />
12
13        <annotatedServiceRecord serviceRef="1__Citrix_F84Store">
14
15          <metadata>
16
17            <plugins>
18
19              <clear />
20
21            </plugins>
22
23            <trustSettings>
24
25              <clear />
26
27            </trustSettings>
28
29            <properties>
30
31              <property name="Auto-Update-Check" value="auto" />
32
33              <property name="Auto-Update-DeferUpdate-Count" value
                    ="1" />
34
35                    <property name="Auto-Update-LTSR-Only" value
                        ="FALSE" />
36
37              <property name="Auto-Update-Rollout-Priority" value=
                    "fast" />
38
39                  </properties>
40
41          </metadata>
42
43        </annotatedServiceRecord>
44
45      </annotatedServices>
46
47      <metadata>
```



```
48
49          <plugins>
50
51            <clear />
52
53          </plugins>
54
55          <trustSettings>
56
57            <clear />
58
59          </trustSettings>
60
61          <properties>
62
63            <clear />
64
65          </properties>
66
67        </metadata>
68
69      </account>
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。
  - 自动（默认）- 自动检查和执行更新
  - 手动 - 仅当用户从 Citrix Workspace 应用程序系统托盘菜单发出检查请求时才会获取更新
  - 已禁用 - 不执行更新检查。
- **Auto-update-LTSR-Only**：指示更新仅针对 LTSR。
  - True - 更新程序将忽略任何未标记为 LTSR 有效的更新。仅考虑 LTSR 更新。
  - False（默认）- 更新程序仅考虑当前的流更新。
- **Auto-update-Rollout-Priority**：指示可以在其间接收更新的交付期间。
  - 快 - 在交付期限即将开始时向用户推出更新。
  - 中 - 在交付期限的中期推出更新。
  - 慢 - 在交付期限结束时推出更新。
- **Auto-update-DeferUpdate-Count**：指示可以延迟更新通知的次数。

> 注意：
>
> 此配置仅适用于交互式更新，在启用了无提示自动更新功能时不适用，因为用户没有任何用于延迟更新的选项。

- -1：用户可以任意次推迟自动更新。
- 0：用户无法查看以后提醒我选项。
- 数值：用户可以查看以后提醒选项指定的次数。

入门

February 16, 2023

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

应用商店

应用商店将用户可用的应用程序和桌面聚合到一个位置。一个用户可以拥有多个应用商店并根据需要在应用商店之间切换。管理员提供包含预配置的资源和设置的应用商店 URL。可以通过 Citrix Workspace 应用程序访问这些应用商店。

应用商店的类型

可以在 Citrix Workspace 应用程序中添加以下应用商店类型：Workspace、StoreFront、Citrix Gateway 应用商店和自定义 Web 应用商店。

Workspace

Citrix Workspace 是一个基于云的企业应用商店，可通过任何设备随时随地安全统一地访问应用程序、桌面和内容（资源）。这些资源可以是 Citrix DaaS、内容应用程序、本地和移动应用程序、SaaS 和 Web 应用程序以及浏览器应用程序。有关详细信息，请参阅 Citrix Workspace 概述。

StoreFront

StoreFront 是本地企业应用商店应用程序，将来自 Citrix Virtual Apps and Desktops 站点的应用程序和桌面聚合到一个易于用户使用的应用商店中。

有关详细信息，请参阅 StoreFront 文档。

Citrix Gateway 应用商店

将 Citrix Gateway 配置为允许用户从内部网络外部进行连接。例如，从 Internet 或远程位置进行连接的用户。

自定义 **Web** 应用商店

此功能提供从适用于 Windows 的 Citrix Workspace 应用程序访问贵组织的自定义 Web 应用商店的权限。要使用此功能，管理员必须将域或自定义 Web 应用商店添加到 Global App Configuration Service 允许使用的 URL 列表中。

有关为最终用户配置 Web 应用商店 URL 的详细信息，请参阅 Global App Configuration Service。

您可以在 Citrix Workspace 应用程序的添加帐户屏幕中提供自定义 Web 应用商店 URL。自定义 Web 应用商店将在本机 Workspace 应用程序窗口中打开。

要删除自定义 Web 应用商店，请转至帐户 > 添加或删除帐户，选择自定义 Web 应用商店 URL，然后单击删除。

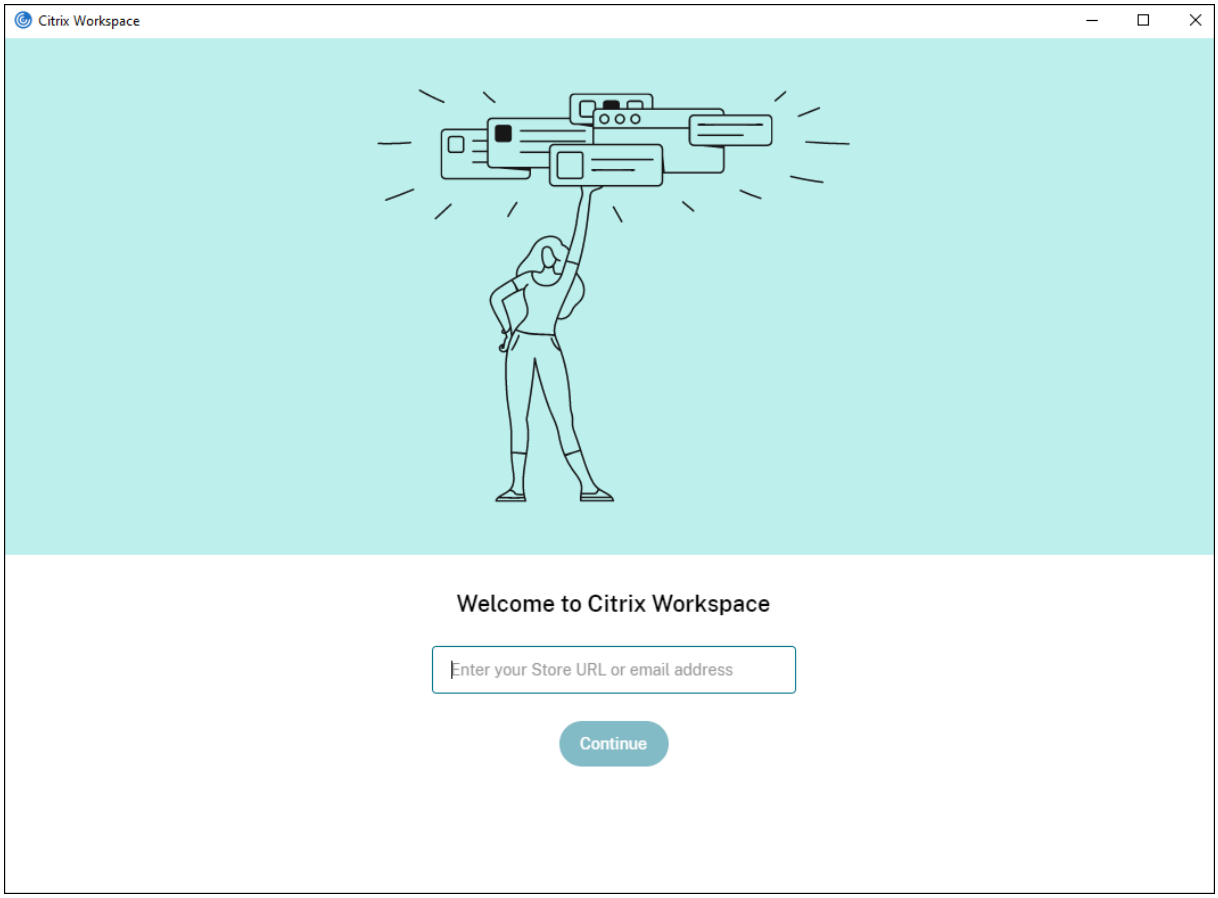
将应用商店 **URL** 添加到 **Citrix Workspace** 应用程序中

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：

- 向用户提供需手动输入的帐户信息
- 配置基于电子邮件的帐户发现
- 通过 CLI 添加应用商店
- 预配文件
- 使用组策略对象管理模板

向用户提供需手动输入的帐户信息

成功安装 Citrix Workspace 应用程序后，将显示以下屏幕。用户需要输入电子邮件地址或服务器地址才能访问应用程序和桌面。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 Workspace 应用商店，请提供 Workspace URL。
- 要连接到 StoreFront 应用商店，请提供该服务器的 URL。例如：`https://servername.company.com`。
- 要通过 Citrix Gateway 进行连接，请先确定用户需要看到所有已配置的应用商店，还是仅需要看到对特定 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：

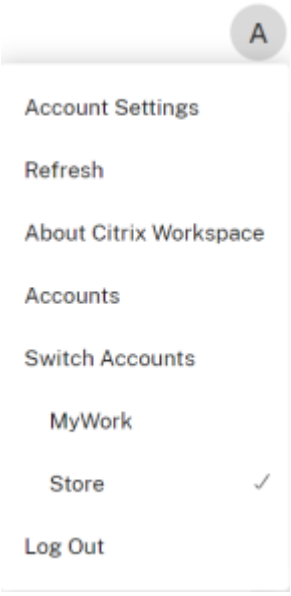
    CitrixGatewayFQDN?MyStoreName：

    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 以访问 SalesApps，或者输入
    * server2.com?HRApps 以访问 **HRApps**。

    CitrixGatewayFQDN?MyStoreName 功能要求新用户通过输入 URL 创建一个帐户，并且不适用于基于电子邮件的发现。

使用应用商店 URL 配置 Workspace 应用程序后，即可通过配置文件菜单中的帐户选项管理该帐户。



在配置了代理身份验证的客户端计算机上，如果代理凭据未存储在 **Windows** 凭据管理器中，则会显示身份验证提示，要求您输入代理凭据。然后，Citrix Workspace 应用程序将代理服务器凭据保存在 **Windows** 凭据管理器中。这样可以打造无缝登录体验，因为您无需在访问 Citrix Workspace 应用程序之前在 **Windows** 凭据管理器中手动保存凭据。

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 Citrix Gateway 或 StoreFront 服务器。该应用程序随后将提示用户登录以访问虚拟桌面和应用程序。

要为 Citrix Workspace 应用商店配置基于电子邮件的帐户发现，请参阅 Global App Configuration Service 文档中的 Getting started（入门）。
要为 Citrix StoreFront 或 Citrix Gateway 应用商店配置基于电子邮件的帐户发现，请参阅 Configuring email-based account discovery（配置基于电子邮件的帐户发现）。

通过 **CLI** 添加应用商店

以管理员身份使用命令行接口安装适用于 Windows 的 Citrix Workspace 应用程序。

有关详细信息，请参阅命令行参数列表。

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，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。

使用组策略对象管理模板

要使用组策略对象管理模板添加或指定 Citrix StoreFront 或 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. 选择已启用选项，然后单击显示。如果启用此策略设置，则可以输入 StoreFront 帐户和 NetScaler Gateway URL 的列表。
5. 在值字段中输入 URL。
6. 指定与 Workspace 应用程序一起使用的应用商店 URL：

   ```
   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 的格式如下：/Citrix/store/discovery。要获取 URL，请从 StoreFront 中导出一个预配文件，在记事本中将其打开，然后复制 Address 元素中的 URL。
   - [On, Off] - Off 选项允许您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。如果未指定应用商店状态，则默认设置为 On。
   - storedescription - 应用商店的说明，例如 HR App Store。

7. 添加或指定 Citrix Gateway URL。输入 URL 的名称（以分号分隔）：

   示例：`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。

> 注意：
>
> - Citrix Gateway 应用商店 URL 必须是列表中的第一个 URL（参数 STORE0）。
> - 在多应用商店设置中，只允许使用一种 Citrix Gateway 应用商店 URL 配置。

- 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。
- 指定 Citrix Gateway 应用商店 URL 时，不需要 /Discovery 参数。

自版本 1808 起，对 Citrix Gateway URL/StoreFront 帐户列表策略所做的更改将在应用程序重新启动后在会话中应用。不需要重置。

注意：

Citrix Workspace 应用程序版本 1808 及更高版本不需要在全新安装中进行重置。如果升级到 1808 或更高版本，则必须重置 Citrix Workspace 应用程序以使所做的更改生效。

限制：

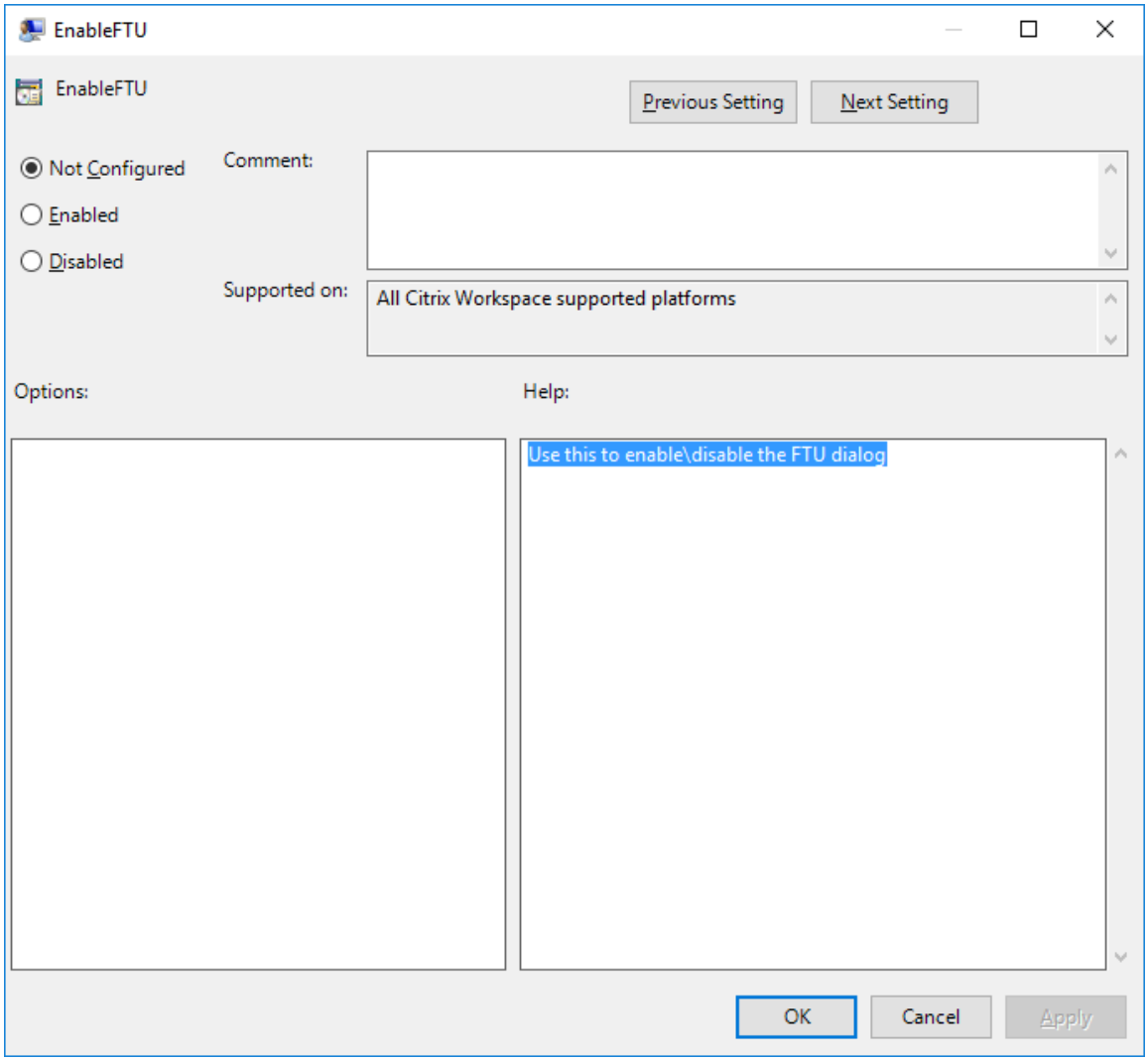
- Citrix Gateway URL 应列在最前面，后跟 StoreFront URL。
- 不支持多个 Citrix Gateway URL。

注意：

用户还可以通过 Web 浏览器访问应用商店。用户可以从 Web 浏览器登录 Citrix Store，然后从 Web 启动虚拟应用程序或桌面。虚拟应用程序或桌面启动利用本机安装的 Citrix Workspace 应用程序的功能。

在这种情况下，可能需要对用户隐藏添加帐户提示。这可以通过以下设置来实现：

- 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。



域名服务名称解析

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 建议不要在服务器上启用 DNS 名称解析。

默认情况下，DNS 名称解析在服务器上处于禁用状态，在 Citrix Workspace 应用程序中处于启用状态。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，需要您重新安装操作系统。我们不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。

连接

通过 Citrix Workspace 应用程序，用户可以安全地自助访问虚拟桌面和应用程序，以及根据需要访问 Windows、Web 和软件即服务 (SaaS) 应用程序。可以通过 Citrix StoreFront 或通过 Web Interface 创建的旧 Web 页面管理用户的访问。

使用 **Citrix Workspace UI** 连接到资源

Citrix Workspace 应用程序主页根据用户的帐户设置（即，用户连接到的服务器）以及 Citrix Virtual Apps and Desktops 或 Citrix DaaS 管理员配置的设置显示用户可用的虚拟桌面和应用程序。可以使用首选项 > 帐户页面配置 StoreFront 服务器的 URL，或者如果配置了基于电子邮件的帐户发现，则通过输入电子邮件地址进行配置。

连接到某个应用商店后，自助服务将显示以下选项卡：收藏夹、桌面和应用程序。要启动会话，请单击相应的图标。要向收藏夹中添加某个图标，请单击 **...** 图标并选择添加到收藏夹。

配置

April 6, 2023

使用适用于 Windows 的 Citrix Workspace 应用程序时，使用以下配置可访问其托管应用程序和桌面。

管理员任务和注意事项

本文讨论了与适用于 Windows 的 Citrix Workspace 应用程序的管理员相关的任务和注意事项。

功能标志管理

如果生产环境中的 Citrix Workspace 应用程序出现问题，我们可以在 Citrix Workspace 应用程序中动态禁用受影响的功能，即使该功能已发布亦如此。

为此，我们将使用功能标志以及名为 LaunchDarkly 的第三方服务。不需要做任何配置即可启用传输到 LaunchDarkly 的流量，但当您配置了阻止出站流量的防火墙或代理时除外。在这种情况下，您根据策略要求通过特定 URL 或 IP 地址启用传输到 LaunchDarkly 的流量。

可以通过以下方式启用传输到 LaunchDarkly 的流量和通信：

启用传输到以下 **URL** 的流量

- events.launchdarkly.com
- stream.launchdarkly.com
- clientstream.launchdarkly.com
- Firehose.launchdarkly.com
- mobile.launchdarkly.com

在允许列表中列出 **IP** 地址

如果必须在允许列表中列出 IP 地址，请参阅 LaunchDarkly public IP list（LaunchDarkly 公用 IP 列表），获取当前所有 IP 地址范围的列表。可以使用此列表来了解您的防火墙配置是否自动更新，以便与基础结构更新保持一致。有关基础结构变更的状态的详细信息，请参阅 LaunchDarkly Status 页面。

LaunchDarkly 系统要求

如果您在 Citrix ADC 上将以下服务的拆分通道设置为关，请验证应用程序是否能够与以下服务通信：

- LaunchDarkly 服务。
- APNs 侦听器服务

禁用 **LaunchDarkly** 服务

可以使用组策略对象 (GPO) 策略禁用 LaunchDarkly 服务。

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** > 合规性。
3. 选择禁止向第三方发送数据策略并将其设置为“已启用”。
4. 单击应用和确定。

组策略对象管理模板

我们建议您使用组策略对象管理模板配置以下对象的规则：

- 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
- 用户体验。

您可以将 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。将 Citrix Workspace 应用程序设置应用到整个企业内多个不同的用户设备时，导入非常有用。要在单个用户设备上进行修改，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。

安装目录包括 CitrixBase.admx 和 CitrixBase.adml 以及管理模板文件（receiver.adml 或 receiver.admx‘receiver.adml‘）。

> 注意：
>
> .admx 和.adml 文件用于兼容性列表中提到的 Windows 版本。

如果随 VDA 安装了 Citrix Workspace 应用程序，则 ADMX/ADML 文件通常位于 \<installation directory>\Online Plugin\Configuration 目录中。

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。

请参见下表获取有关 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	<Installation Directory>\ICA Client\Configuration
receiver.admx	<Installation Directory>\ICA Client\Configuration
receiver.adml	<Installation Directory>\ICA Client\Configuration\[MUIculture]
CitrixBase.admx	<Installation Directory>\ICA Client\Configuration
CitrixBase.adml	<Installation Directory>\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，请将最新的模板文件添加到本地 GPO 中。导入后保留先前的设置。有关详细信息，请参阅以下过程：

要向本地 **GPO** 中添加 **receiver.admx/adml** 模板文件，请执行以下操作：

可以使用.adm 模板文件配置本地 GPO 和基于域的 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，复制以下模板文件：

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

> 注意：
>
> 将 CitrixBase.admx/CitrixBase.adml 添加到 `\PolicyDefinitions` 文件夹中，以查看管理模板 > **Citrix** 组件 > **Citrix Workspace** 中的模板文件。

应用程序保护

> 免责声明
>
> 应用程序保护策略将筛选对基础操作系统所需功能的访问权限（捕获屏幕或键盘按下所需的特定 API 调用）。应用程序保护策略甚至能够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。

应用程序保护功能是一项附加功能，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。应用程序保护可防止泄露屏幕上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。

应用程序保护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 Citrix Virtual Apps and Desktops 文档中的配置部分。

要求：

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

必备条件：

- 必须在 Controller 上启用应用程序保护功能。有关详细信息，请参阅 Citrix Virtual Apps and Desktops 文档中的应用程序保护部分。

> 注意：
>
> - 此功能仅在桌面操作系统（例如 Windows 11、Windows 10、Windows 8.1）上受支持。
> - 自版本 2006.1 起，Windows 7 不支持 Citrix Workspace 应用程序。因此，应用程序保护在 Windows 7 中不起作用。有关详细信息，请参阅弃用。
> - 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。没有可用于实现此目的的 GUI。

> 注意：
>
> 自版本 2103 起，Citrix DaaS 支持对 StoreFront 和 Workspace 使用应用程序保护。

有关 Citrix Virtual Apps and Desktops 和 Citrix DaaS 上的应用程序保护配置的信息，请参阅应用程序保护。

应用程序保护 - **Citrix Workspace** 应用程序中的配置

现在，在 Citrix Workspace 应用程序安装期间，默认情况下会安装应用程序保护组件。

安装期间出现的 **Enable app protection**（启用应用程序保护）复选框将替换为 **Start App Protection after installation**（安装后启动应用程序保护）。

选中此复选框后，应用程序保护将在安装后立即启动。

> 注意：
>
> 如果您未启用此复选框，则对于有权使用应用程序保护的客户，应用程序保护会在首次启动受保护的资源或组件时自动启动。

命令行接口

您也可以使用 /`startappprotection` 命令行参数启动应用程序保护组件。但是，先前的 /`includeappprotection` 开关已弃用。

下表提供了有关受保护的屏幕的信息，具体取决于部署：

应用程序保护部署	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

当您创建屏幕截图时，只有受保护的窗口停止运行。您可以创建受保护窗口外部的区域的屏幕截图。但是，如果使用 PrtScr 键捕获 Windows 10 设备上的屏幕截图，则必须最小化受保护的窗口。

以前，Citrix 身份验证和 Citrix Workspace 应用程序屏幕默认强制执行反屏幕捕获和反键盘记录功能。但是，自 2212 起，这些功能默认处于禁用状态，需要使用组策略对象进行配置。

> 注意：
>
> 此 GPO 策略不适用于 ICA 和 SaaS 会话。ICA 和 SaaS 会话继续使用 Delivery Controller 和 Citrix Secure Private Access 进行控制。

为自助服务插件界面配置应用程序保护

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**。
3. 要为自助服务插件对话框配置反键盘记录和反屏幕捕获，请选择自助服务 > 管理应用程序保护策略。
4. 选择以下选项之一或同时选中二者：
    - 反键盘记录：防止键盘记录器捕获按键。
    - 反屏幕捕获：防止用户创建屏幕截图和共享其屏幕。
5. 单击应用和确定。

为身份验证管理器配置应用程序保护

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**。
3. 要为身份验证管理器配置反键盘记录和反屏幕捕获，请选择用户身份验证 > 管理应用程序保护策略。
4. 选择以下选项之一或同时选中二者：
    - 反键盘记录：防止键盘记录器捕获按键。
    - 反屏幕捕获：防止用户创建屏幕截图和共享其屏幕。
5. 单击应用和确定。

预期行为：

预期行为取决于用户访问具有受保护的资源的 StoreFront 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。

应用程序保护增强功能：屏幕截图检测和通知

自适用于 Windows 的 Citrix Workspace 应用程序 2212 起，当有人可能尝试对任何受保护的资源进行屏幕捕获时，您可以查看通知。有关受应用程序保护的资源的信息，请参阅应用程序保护什么？。

出现以下情况时会显示通知：

- 尝试通过屏幕捕获工具截取屏幕截图或录制视频。
- 尝试通过 Print Screen 键截取屏幕截图。

> 注意：
>
> 屏幕捕获工具的每个运行实例仅显示一次。如果您重新启动该工具并尝试捕获屏幕截图，该通知会再次出现。

应用程序保护增强功能：使用 **Global App Configuration** 为身份验证和自助服务插件配置应用程序保护

自 2302 版起，适用于 Windows 的 Citrix Workspace 应用程序允许您使用 Global App Configuration 为身份验证和自助服务插件配置应用程序保护。以前，您只能使用组策略对象配置这些组件。

如果您使用 Global App Configuration Service 启用反键盘记录和防屏幕捕获功能，这些功能将同时适用于身份验证和自助服务插件。

> 注意：
>
> Global App Configuration Service 配置不适用于虚拟应用程序、虚拟桌面、Web 应用程序和 SaaS 应用程序。这些资源将继续使用 Delivery Controller 和 Citrix Secure Private Access 进行控制。有关详细信息，请参阅 Citrix Virtual Apps and Desktops 文档中的“应用程序保护”的配置部分。

使用 **Global App Configuration Service API** 为身份验证和自助服务插件配置应用程序保护

管理员可以使用 API 配置这些应用程序保护功能。设置如下所示：

- 用于启用或禁用反屏幕捕获的设置：

  “name”: “enable anti screen capture for auth and ssp”
  “value”: “true” or “false”

- 用于启用或禁用反键盘记录的设置：

  “name”: “enable anti key-logging for auth and ssp”
  “value”: “true” or “false”

要进行配置，请参阅下面在 Global App Configuration Service 中为适用于 Windows 的 Citrix Workspace 应用程序启用防屏幕捕获和反键盘记录功能的 JSON 文件示例：

```
{

        "category": "App Protection",

        "userOverride": true,

        "assignedTo": [

          "AllUsersNoAuthentication"
```



```
11
12            ],
13
14            "settings": [
15
16              {
17
18
19                "name": "enable anti screen capture for auth and ssp",
20
21                "value": true
22
23               }
24  ,
25
26              {
27
28
29                "name": "enable anti key-logging for auth and ssp",
30
31                "value": true
32
33               }
34
35
36            ] }
```

附加说明

- 适用于 **Web** 的 **Workspace** 上的行为：

  适用于 Web 的 Workspace 配置不支持应用程序保护组件。不枚举受应用程序保护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。

- 不支持应用程序保护的 **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 中不枚举受应用程序保护策略保护的应用程序。

- 在 **Controller** 上配置了应用程序保护功能的应用程序的行为：

  在配置了应用程序保护的控制器上，如果您尝试启动受保护的应用程序，应用程序保护会自动启动并保护该应用程序。

- 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。

应用程序保护错误日志

自版本 2103 起，应用程序保护日志将作为 Citrix Workspace 应用程序日志的一部分进行收集。有关日志收集的详细信息，请参阅日志收集。

卸载应用程序保护组件

要卸载应用程序保护组件，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：
>
> 应用程序保护仅在从版本 1912 开始升级时受支持。

已知问题或限制

- 启动受保护的桌面后，已经运行的桌面会话和后续启动的桌面会话也将受到保护。这是一个已知限制，因为名为 `CDViewer.exe` 的客户端进程对所有桌面会话都相同。但是，对于应用程序会话，预计不会出现这种限制。
- 此功能在 Microsoft Server 操作系统（例如 Windows Server 2012 R2 和 Windows Server 2016）中不受支持。
- 双跃点场景不支持此功能。
- 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。

应用程序类别

应用程序类别允许用户管理 Citrix Workspace 应用程序中的应用程序的集合。您可以为在不同交付组之间共享，或由交付组中一个用户子集使用的应用程序创建应用程序组。

有关详细信息，请参阅 Citrix Virtual Apps and Desktops 文档中的创建应用程序组。

提高了 **ICA** 文件的安全性

此功能可在虚拟应用程序和桌面会话启动期间处理 ICA 文件时提供增强的安全性。

Citrix Workspace 应用程序允许您在启动虚拟应用程序和桌面会话时将 ICA 文件存储在系统内存中，而非本地磁盘中。

此功能旨在消除表面攻击以及在本地存储时可能会滥用 ICA 文件的任何恶意软件。此功能也适用于在适用于 Web 的 Workspace 上启动的虚拟应用程序和桌面会话

配置

通过 Web 访问 Citrix Workspace 或 StoreFront 时，也支持 ICA 文件安全性。如果可以通过 Web 访问客户端，则客户端检测是此功能运行的必备条件。如果您使用浏览器访问 StoreFront，请在 StoreFront 部署的 web.config 文件中启用以下属性：

StoreFront 版本	属性
2.x	pluginassistant
3.x	protocolHandler

通过浏览器登录应用商店时，请单击检测 **Workspace** 应用程序。如果未显示该提示，请清除浏览器 cookie 并重试。

如果是 Workspace 部署，则可以通过导航到帐户设置 > 高级 > 应用程序和桌面启动首选项来查找客户端检测设置。

您可以采取额外的措施以便仅使用存储在系统内存中的 ICA 文件启动会话。使用以下任意方法：

- 客户端上的组策略对象 (GPO) 管理模板。
- Global App Config Service。
- 适用于 Web 的 Workspace。

使用 **GPO**：

要阻止从存储在本地磁盘上的 ICA 文件启动会话，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** 组件 > **Citrix Workspace** > **Client Engine**。
3. 选择安全 **ICA** 文件会话启动策略并将其设置为已启用。
4. 单击应用和确定。

使用 **Global App Config Service**：

可以使用 Citrix Workspace 应用程序 2106 中的 Global App Config Service。

要阻止从存储在本地磁盘上的 ICA 文件启动会话，请执行以下操作：

将阻止直接 **ICA** 文件启动属性设置为 **True**。

有关 Global App Config Service 的详细信息，请参阅 Global App Config Service 文档。

使用适用于 **Web** 的 **Workspace**：

要在使用适用于 Web 的 Workspace 时禁止在本地磁盘上下载 ICA 文件，请执行以下操作：

运行 PowerShell 模块。请参阅配置 DisallowICADownload。

> 注意：
>
> **DisallowICADownload** 策略不适用于 StoreFront 部署。

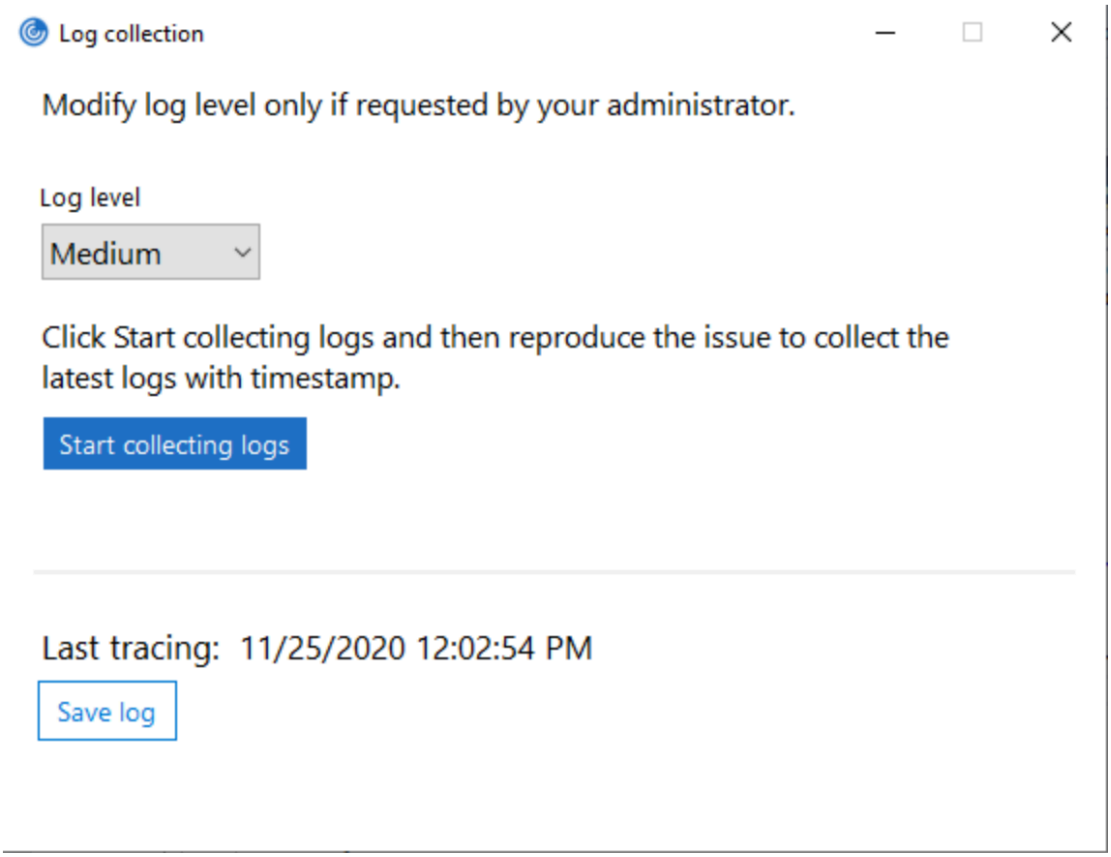
日志收集

日志收集简化了 Citrix Workspace 应用程序收集日志的过程。这些日志可帮助 Citrix 进行故障排除，并在出现复杂问题的情况下提供支持。

您可以使用 GUI 收集日志。

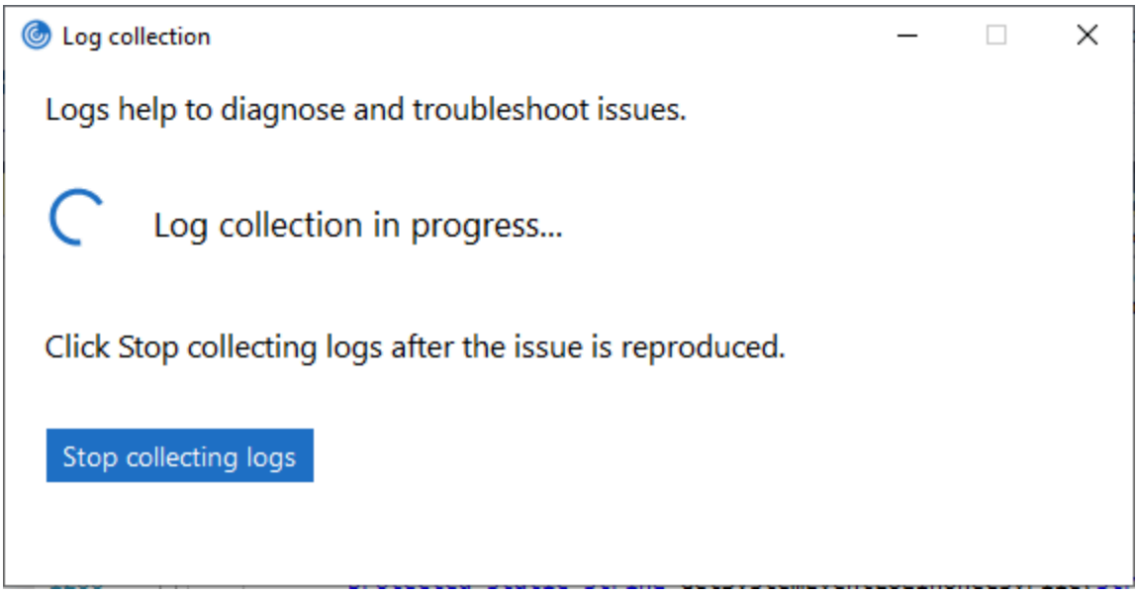
收集日志：

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. 选择日志收集。
   此时将显示“日志收集”对话框。



3. 选择以下日志级别之一：
   - 低
   - 中
   - 详细
4. 单击开始收集日志以重现问题并收集最新的日志。

   日志收集过程将开始。



5. 重现该问题后，单击停止收集日志。
6. 单击保存日志将日志保存到所需位置。

HDX 自适应吞吐量

HDX 自适应吞吐量可通过调整输出区缓冲智能地调整 ICA 会话的高峰吞吐量。输出缓冲区的数量最初设置为较高的值。这一较高的值允许更快更高效地将数据传输到客户端，尤其是在高延迟网络中。

提供更好的交互性、更快的文件传输、更流畅的视频播放、更高的帧速率和分辨率，可提升用户体验。

将持续测量会话交互性以确定 ICA 会话中的数据流是否会对交互性产生不利影响。如果出现这种情况，吞吐量将减少，以降低大量数据流对会话产生的影响并允许恢复交互性。

只有适用于 Windows 的 Citrix Workspace 应用程序 1811 及更高版本才支持此功能。

> 重要：
>
> HDX 自适应吞吐量通过将此机制从客户端移到 VDA 改变了输出缓冲区。因此，按照 CTX125027 中所述在客户端上调整输出缓冲区数量将不起作用。

自适应传输

自适应传输是 Citrix Virtual Apps and Desktops 和 Citrix DaaS 中的一种机制，允许您使用 Enlightened Data Transport (EDT) 作为 ICA 连接的传输协议的功能。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

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。这样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，您可以：

- 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 Files
  - 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。

在“高级首选项”表中隐藏特定设置

可以使用 Citrix Workspace 应用程序组策略对象管理模板在高级首选项表中隐藏用户可配置的特定设置。要隐藏设置，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** > 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。

下表列出了您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

选项	操作
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 Files
- 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。

StoreFront 到 Workspace URL 迁移

通过 StoreFront 到 Workspace URL 迁移，您可以在用户交互最少的情况下将最终用户从 StoreFront 应用商店无缝迁移到 Workspace 应用商店。

请注意，您的所有最终用户都向其 Workspace 应用程序中添加了一个 StoreFront 应用商店 `storefront.com`。作为管理员，您可以在 Global App Configuration Service 中配置 Workspace URL 映射 {'storefront.com':'xyz.cloud.com'} 的 StoreFront URL。Global App Config Service 将此设置推送到添加了 StoreFront URL `storefront.com` 的托管和未托管设备上的所有 Citrix Workspace 应用程序实例。

检测到此设置后，Citrix Workspace 应用程序将映射的 Workspace URL `xyz.cloud.com` 添加为另一个应用商店。最终用户启动新 Citrix Workspace 应用程序时，将打开 Citrix Workspace 应用商店。以前添加的 StoreFront 应用商店 `storefront.com` 仍添加到 Workspace 应用程序中。用户始终可以使用 Workspace 应用程序中的切换帐户选项切换回 StoreFront 应用商店 `storefront.com`。管理员可以控制何时从用户的端点设备上的 Workspace 应用程序中删除 StoreFront 应用商店 `storefront.com`。删除可以通过 Global App Config Service 完成。

要启用该功能，请执行以下步骤：

1. 使用 Global App Config Service 将 StoreFront 配置为 Workspace 映射。有关 Global App Config Service 的信息，请参阅 Global App Configuration Service。
2. 编辑 App Config Service 中的负载：

```
{

 "serviceURL": {

"url": "https://storefront.acme.com:443",
"migrationUrl": [
  {

    "url": "https://sampleworkspace.cloud.com:443",
    "storeFrontValidUntil": "2023-05-01"
   }

 ]
 }
 ,
"settings": {

"name": "Productivity Apps",
"description": "Provides access StoreFront to Workspace Migration"
   ,
"useForAppConfig": true,
"appSettings": {

  "windows": [
```



```
    {

      "category": "root",
      "userOverride": false,
      "assignmentPriority": 0,
      "assignedTo": [
        "AllUsersNoAuthentication"
      ],
      "settings": [
      {

       "name": "Hide advanced preferences",
        "value": false
       }

      ]
      }

    ]
    }

  }

}


<!--NeedCopy-->
```

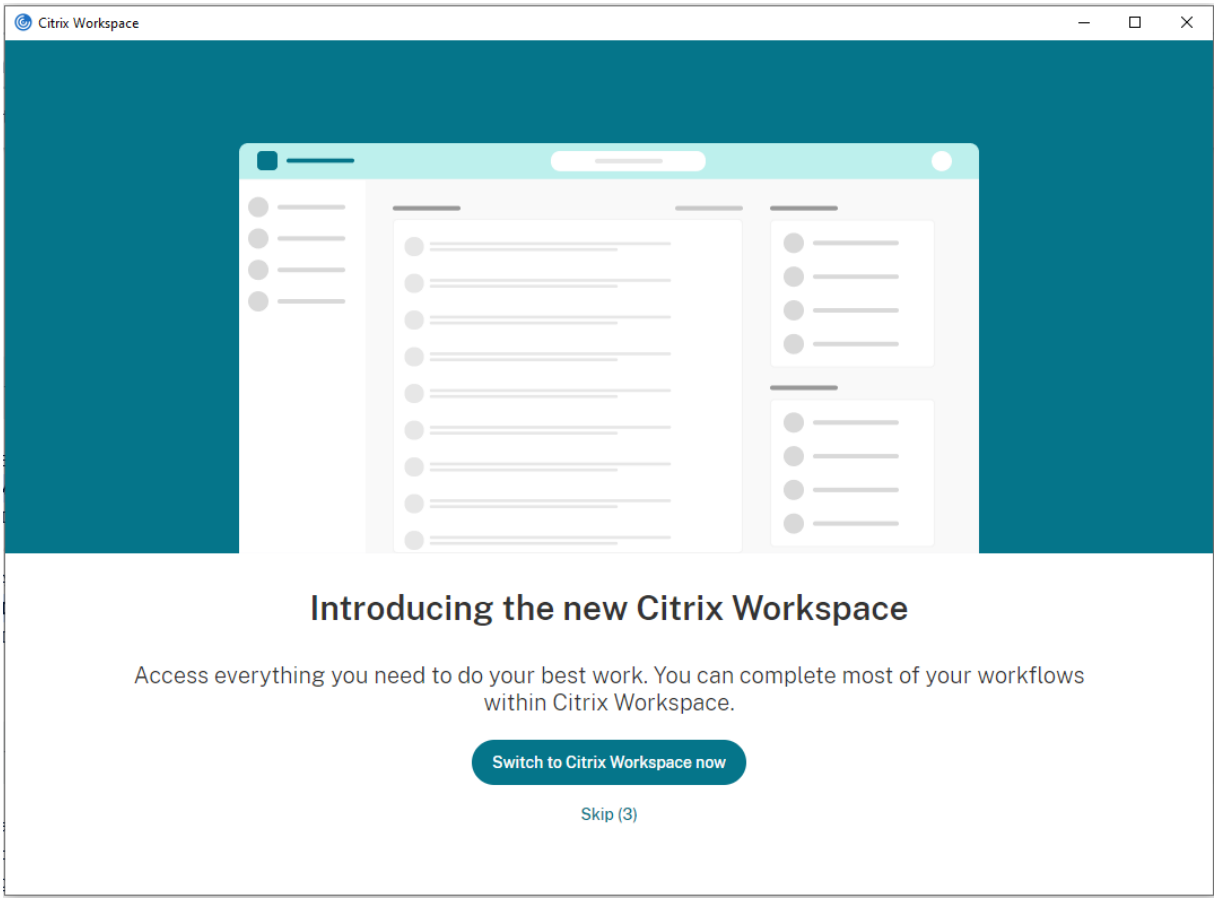
> 注意：
>
> 如果您是首次配置有效负载，请使用 POST。
> 如果您正在编辑现有的有效负载配置，请使用 PUT 并检查您的有效负载包含所有受支持的设置。

3. 在 **serviceURL** 部分中指定 StoreFront URL `storefront.com` 作为 **URL** 的值。
4. 在 **migrationUrl** 部分内部配置 Workspace URL `xyz.cloud.com`。
5. 使用 **storeFrontValidUntil** 可设置从 Workspace 应用程序中删除 StoreFront 应用商店的时间表。此字段为可选字段。可以根据您的要求设置以下值：

   - 格式为 (YYYY-MM-DD) 的有效日期

     > 注意：
     >
     > 如果您提供了过去的日期，则迁移 URL 时将立即删除 StoreFront 应用商店。如果您提供了将来的日期，StoreFront 应用商店将在设置的日期删除。

推送 App Config Service 设置后，将显示以下屏幕：



用户单击立即切换到 **Citrix Workspace** 时，Workspace URL 将添加到 Citrix Workspace 应用程序中，并且将显示身份验证提示。用户可以使用有限的选项将转换延迟多达三次。

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。可以打开浏览器访问适用于 Web 的 Workspace，以选择并使用所需的应用程序。在此模式下，不会将任何快捷方式放置在用户的桌面上。
- 自助服务模式 - 通过将 StoreFront 帐户添加到 Citrix 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。自助服务模式允许您从 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 - 管理员可以将 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。放置与 Citrix Workspace 应用程序企业版类似。新的仅快捷方式模式允许您在熟悉的

Windows 导航架构中查找所有已发布的应用程序，该位置正是您希望找到应用程序的位置。

有关详细信息，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

通过直接将 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 站点，可以配置自助服务模式。此配置允许用户从 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。而是单独显示应用程序或在根文件夹下显示应用程序。“应用程序”不在通过 Citrix Virtual Apps and Desktops 和 Citrix DaaS 定义的“类别”子文件夹中。

- 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来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。

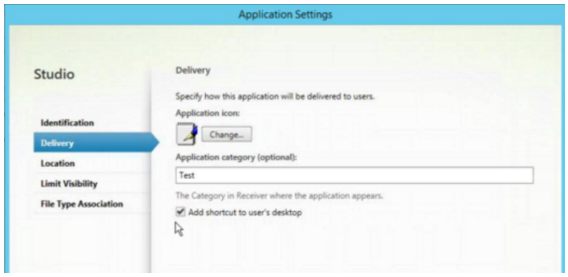
使用 **Citrix Virtual Apps and Desktops 7.x** 中的每应用程序设置自定义应用程序快捷方式的位置

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。但是，此配置与之前的适用于 Windows 的 Workspace 版本相似。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。

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

在以下情况下，Citrix Workspace 应用程序提供从网络共享复制.EXE 存根的功能：

- 每次登录时，应用程序枚举都会出现延迟，或者
- 需要对应用程序存根进行数字签名。

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，请准备一份允许列表（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。要完成创建存根可执行文件，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 中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 应用程序以使所做的更改生效。

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）

如果您有数十个甚至数百个应用程序，请允许用户选择要添加到收藏夹和开始菜单中的应用程序：

如果希望用户选择要放置在 “开始” 菜单中的应用程序。	以自助服务模式配置 Citrix 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。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进行放置。

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，请将所有应用程序都放置在“开始”菜单中或桌面上，或者放置在桌面上的某个文件夹中。

如果希望 Citrix 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

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

如果要通过每应用程序设置来确定应用程序的放置位置，而无论处于自助服务模式还是“开始”菜单模式，请执行以下操作。	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

如果您不希望用户在其他用户共享端点时看到应用程序，则可以在用户注销并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。

> 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 和 Citrix DaaS 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”。

虚拟显示布局

此功能允许您定义应用到远程桌面的虚拟监视器布局。还可以在远程桌面上将一台客户端显示器拆分为最多八台显示器。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、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。

自适用于 Windows 的 Citrix Workspace 应用程序 2106 起，全屏、多显示器桌面会话也支持虚拟显示布局。默认情况下，虚拟显示布局处于启用状态。在多显示器场景中，如果虚拟显示器的总数不超过八个虚拟显示器，相同的虚拟显示布局将应用到所有会话显示器。如果超过此限制，虚拟显示布局将被忽略，不应用到任何会话显示器。

可以通过设置以下注册表项禁用多显示器增强功能：

- HKEY_CURRENT_USER\Software\Citrix\XenDesktop\DesktopViewer

名称：**SplitAllMonitors**
类型：DWORD

值：

1 - 已启用

0 - 已禁用

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。预启动功能允许创建预启动会话。预启动会话是在用户登录到 Citrix Workspace 应用程序时或者在计划的时间（如果用户已登录）创建的。

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。

有关详细信息，请参阅标题为管理交付组的 “Citrix Virtual Apps and Desktops” 一文中的会话预启动和会话延迟指南。

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。为共享网络和服务器负载，该会话将在计划的时段内启动。例如，如果计划的预启动计划在 13:45 进行，会话实际上将在 13:15 到 13:45 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包括：

- 创建、修改或删除预启动应用程序，以及
- 更新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，您可以通过修改注册表值来更改预启动配置。可以在安装适用于 Windows 的 Citrix Workspace 应用程序期间或之后修改注册表值。

- 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。您可以为用户提供用于更改值的脚本。

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**
类型：REG_DWORD

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**
类型：REG_DWORD

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**
类型：REG_DWORD

值：

“计划的预启动”的时间（24 小时制）和具体日期按以下格式输入：

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

Citrix 为客户端到 URL 重定向提供主机到客户端重定向和本地应用程序访问。但是，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：

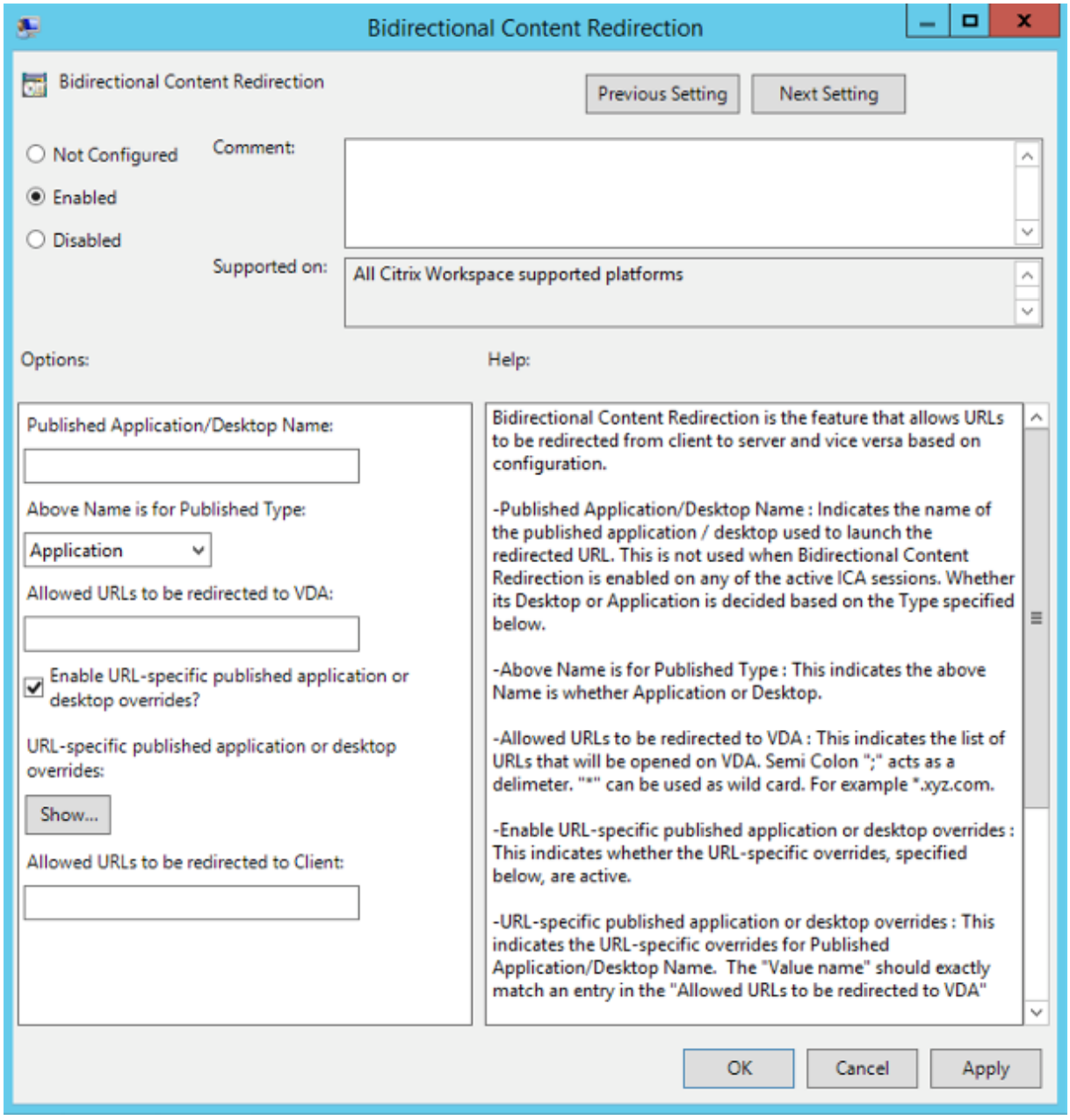
1. 组策略对象 (GPO) 管理模板
2. 注册表编辑器

> 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。

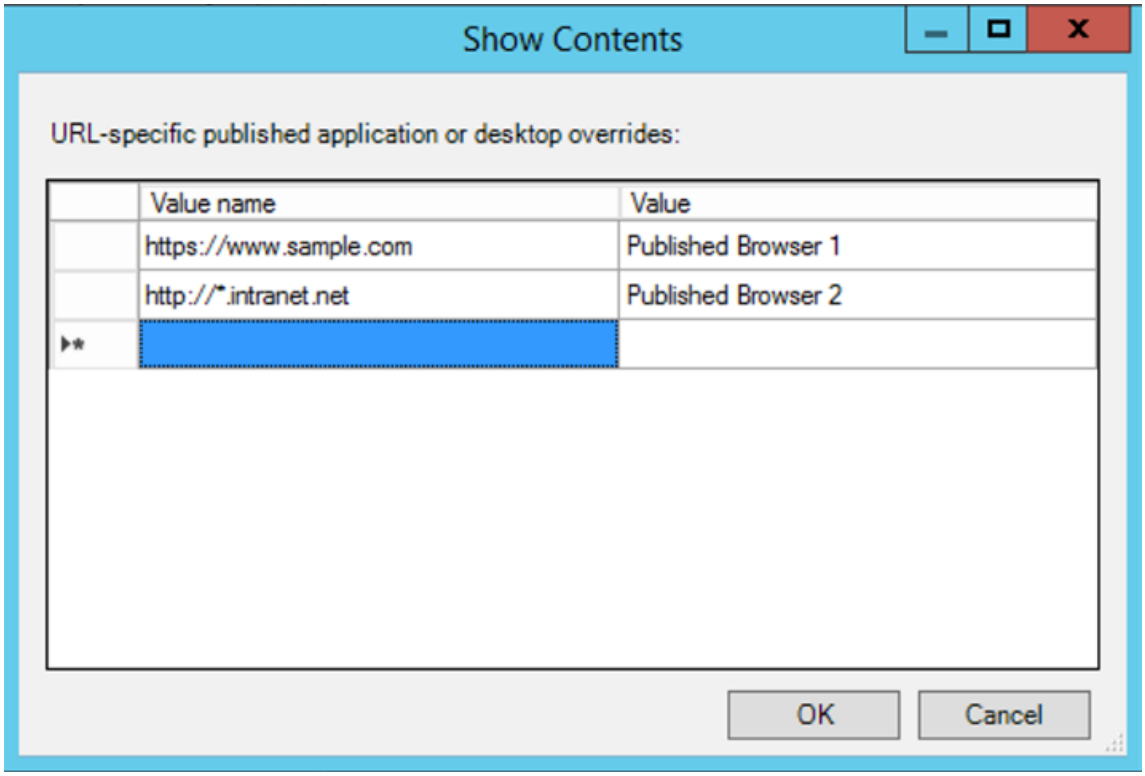
1. 通过运行 gpedit.msc 打开 Citrix Workspace 应用程序组策略对象管理模板。
2. 在用户配置节点下，转至管理模板 > 经典管理模板 **(ADM)** > **Citrix** 组件 > **Citrix Workspace** > 用户体验。
3. 选择双向内容重定向策略。



1. 在已发布的应用程序或桌面名称字段中，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，请在 Citrix Workspace 应用程序客户端上以及从 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。

> - 确保仅存在一种服务器文件类型关联，并且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或主机内容 (URL) 重定向功能，以确认 URL 重定向正常运行。
> - 在 Internet Explorer 中，单击设置 > **Internet** 选项 > 高级，然后选择浏览部分下的启用第三方浏览器扩展复选框

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。

基于 **Chromium** 的浏览器支持双向 **URL**

双向内容重定向允许您使用服务器和客户端上的策略将 URL 配置为从客户端重定向到服务器以及从服务器重定向到客户端。

服务器策略在 Delivery Controller 上设置，客户端策略在 Citrix Workspace 应用程序上设置。这些策略使用组策略对象 (GPO) 管理模板进行设置。

自版本 2106 起，已为 Google Chrome 和 Microsoft Edge 添加了双向 URL 重定向支持。

必备条件：

- Citrix Virtual Apps and Desktops 版本 2106 或更高版本。
- 浏览器重定向扩展程序版本 5.0。

要将 Google Chrome 浏览器注册到双向 URL 重定向，请从 Citrix Workspace 应用程序安装文件夹中运行以下命令：

```
%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /regChrome /verbose
```

> 注意：
>
> 在 Chrome 浏览器上使用这些命令时，将自动从 Chrome 网上应用店安装双向内容重定向扩展。

要从双向 URL 重定向中取消注册 Google Chrome 浏览器，请从 Citrix Workspace 应用程序安装文件夹中运行以下命令：

```
%ProgramFiles(x86)%\Citrix\ICA Client\redirector.exe /unregChrome /verbose
```

> 注意：
>
> 如果在访问“浏览器扩展”页面时出现以下错误，请忽略该消息：
>
> ```
> Websocket connection to wss://... failed.
> ```

有关在 Citrix Workspace 应用程序中配置 URL 重定向的信息，请参阅双向内容重定向。

有关浏览器内容重定向的详细信息，请参阅 Citrix Virtual Apps and Desktops 文档中的浏览器内容重定向。

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。如果用户想要同时查看多个桌面，有关这些桌面的信息可能无法读取。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 功能允许从移动设备即时安全地访问任何应用程序，并在大屏幕上显示。

> 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。
- 允许在运行 Citrix Workspace 应用程序的设备与 Citrix Ready Workspace Hub 之间使用端口 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。
- 在安装期间运行 `/IncludeCitrixCasting` 命令以启用 Citrix Casting。

配置 **Citrix Casting** 启动

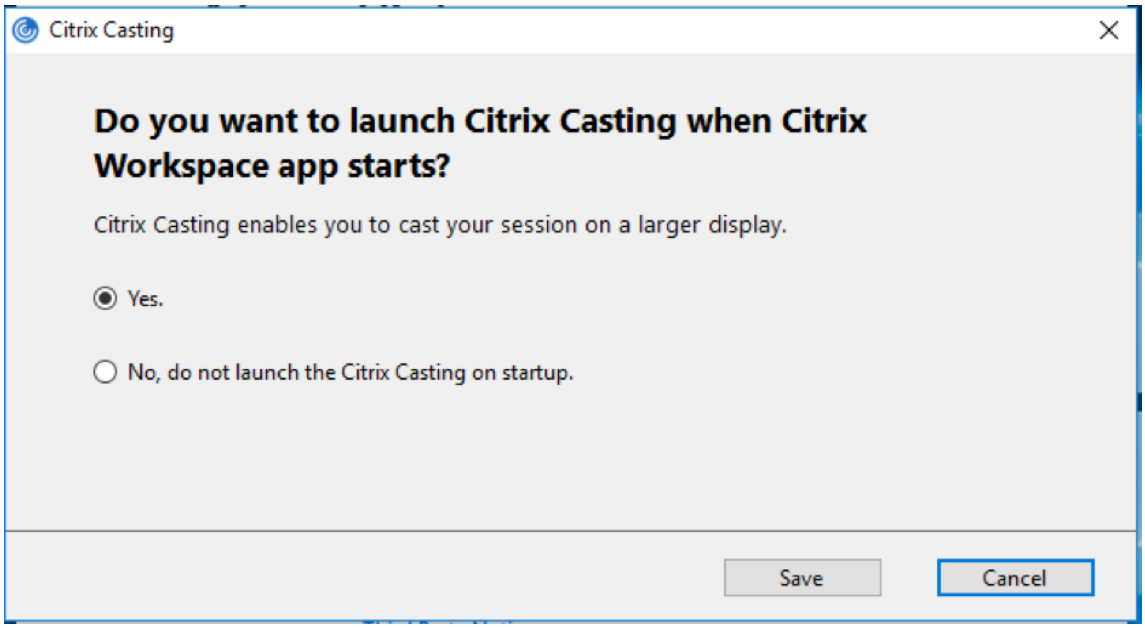
> 注意：
>
> 可以隐藏“高级首选项”表的全部或部分内容。有关详细信息，请参阅“高级首选项”表。

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。

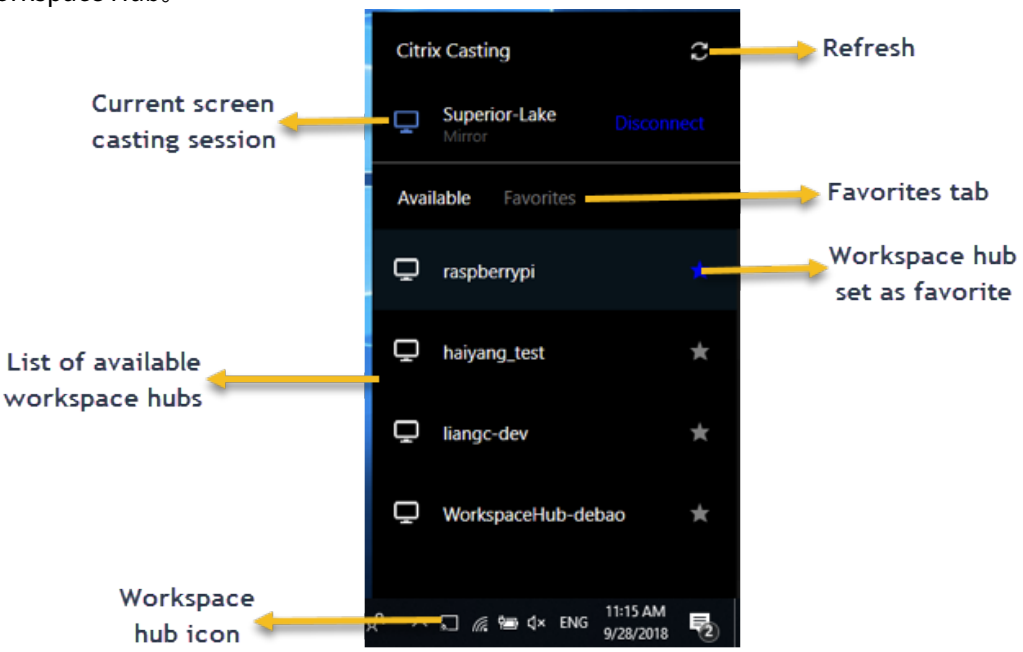
2. 选择要投射屏幕的 Workspace Hub，然后选择以下选项之一：

   - 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` 以检查其是否显示 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。

有关 Citrix Ready Workspace Hub 的详细信息，请参阅 Citrix Virtual Apps and Desktops 文档中的 Citrix Ready Workspace Hub 部分。

DPI 缩放

Citrix Workspace 应用程序具有 DPI 感知功能，支持将 Windows 客户端上的显示分辨率和 DPI 缩放比例设置与虚拟应用程序和桌面会话进行匹配。

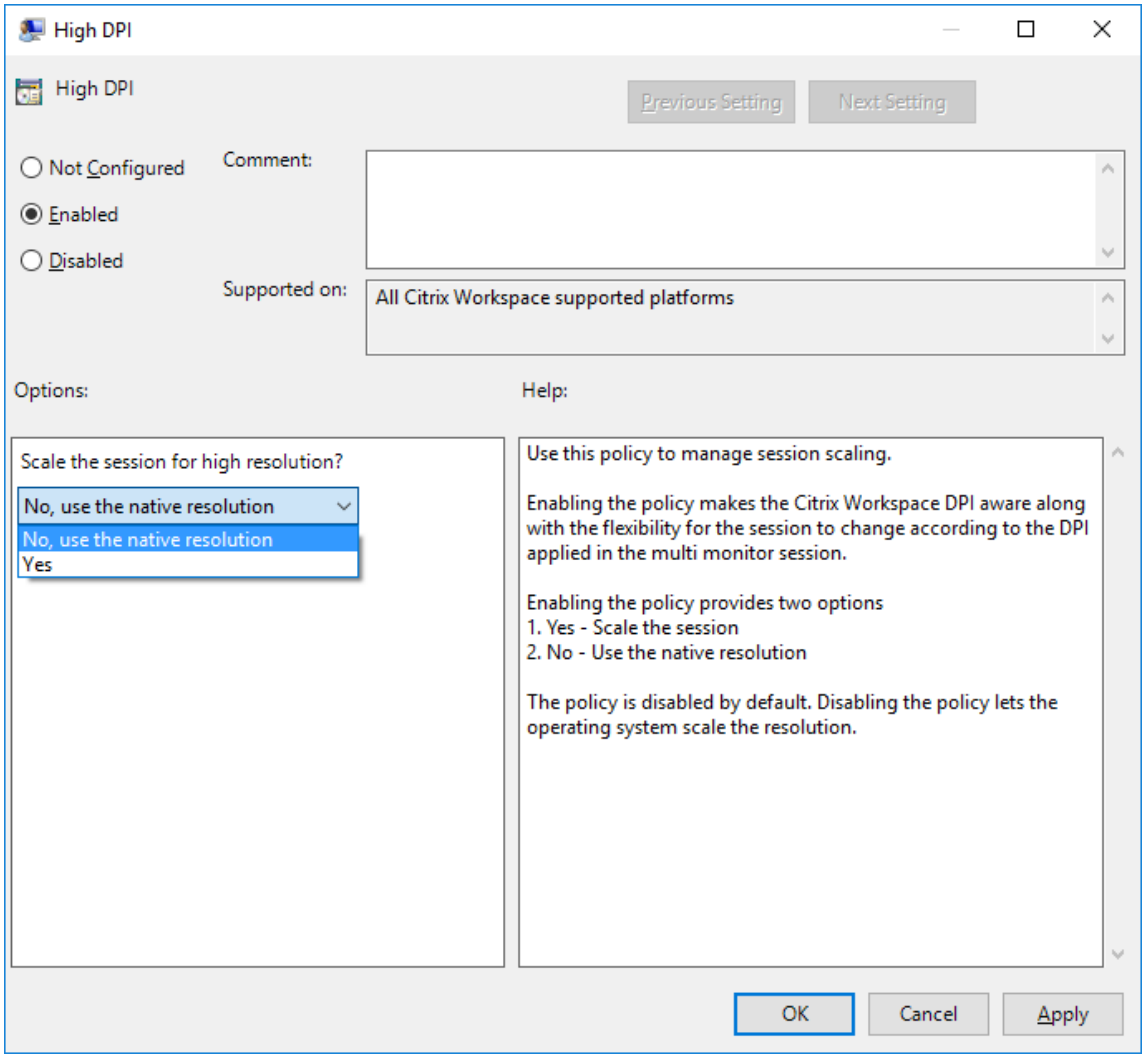
DPI 缩放比例主要用于大尺寸、高分辨率显示器，以能够舒适地查看的尺寸显示应用程序、文本、图像和其他图形元素。

默认情况下，此功能处于启用状态，它是所有用例的推荐设置。但是，如有必要，管理员仍然可以使用组策略对象 (GPO) 管理模板（每计算机配置）配置 DPI 缩放。

要使用 GPO 管理模板配置 DPI 缩放，请执行以下缩放：

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。

要使用图形用户界面配置 **DPI** 缩放，请执行以下操作：

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高 **DPI** 设置。

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 Workspace 应用程序检测 VDA 上的 DPI 并进行应用。
   c) **Let the operating system scale the resolution**（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。

注意：

> 其他注意事项：
>
> - DPI 匹配需要 Citrix Virtual Apps and Desktops 版本 1912 LTSR 或更高版本。
> - 在大多数情况下，建议使用否，使用本机分辨率（DPI 匹配）设置。
> - 默认设置允许操作系统缩放分辨率会禁用 Citrix Workspace 应用程序上的 DPI 感知。当 Windows 客户端 DPI 缩放比例设置为 100% 以外的任何值时，此模式都可能会导致图形模糊。此模式不支持具有不同 DPI 缩放比例的多台显示器。
> - 是选项会导致 Citrix Workspace 应用程序向上缩放会话窗口以匹配在 Windows 客户端上配置的 DPI 缩放比例。这是旧版功能，建议仅在客户端需要将 DPI 缩放到 100% 以上时连接到旧版 XenApp 和 XenDesktop 环境时使用。此模式可能会导致图形模糊。

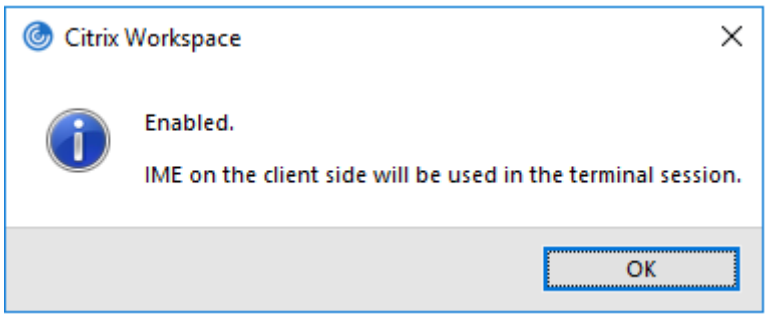
有关对 DPI 缩放问题进行故障排除的信息，请参阅知识中心文章 CTX230017。

通用客户端输入法编辑器 (IME)

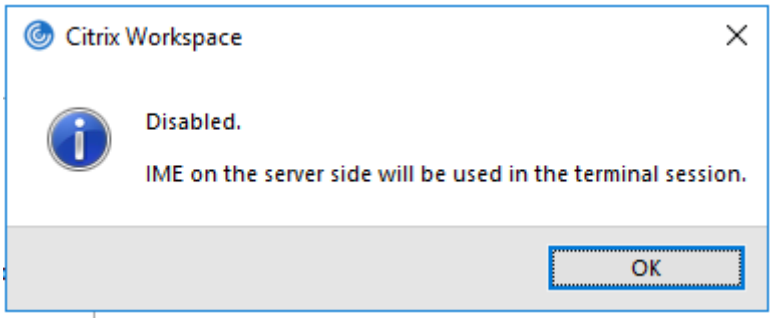
> 注意：
>
> 如果您使用的是 Windows 10 2004 版操作系统，则在会话中使用 IME 功能时可能会遇到某些技术问题。这些问题是第三方限制造成的。有关详细信息，请参阅 Microsoft 支持文章。

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。

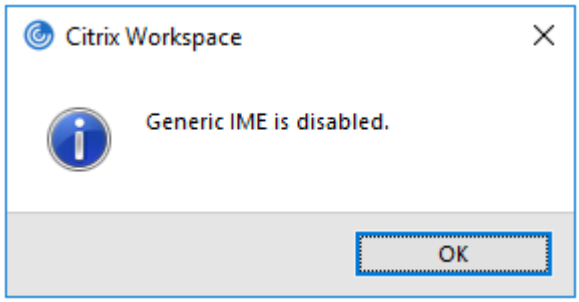


- 要禁用通用客户端 IME，请从 Citrix Workspace 应用程序安装文件夹 `C:\Program Files (x86)\Citrix\ICA Client` 运行 `wfica32.exe /localime:off` 命令。

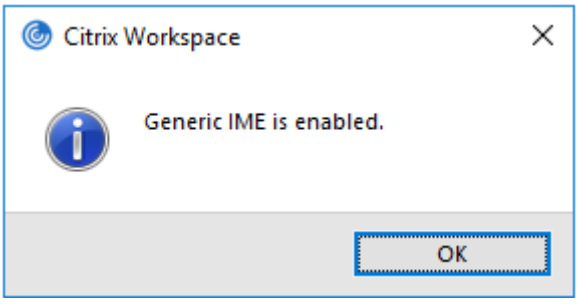


> 注意：
>
> 可以使用命令行开关 `wfica32.exe /localime:on` 启用通用客户端 IME 和键盘布局同步。

- 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。

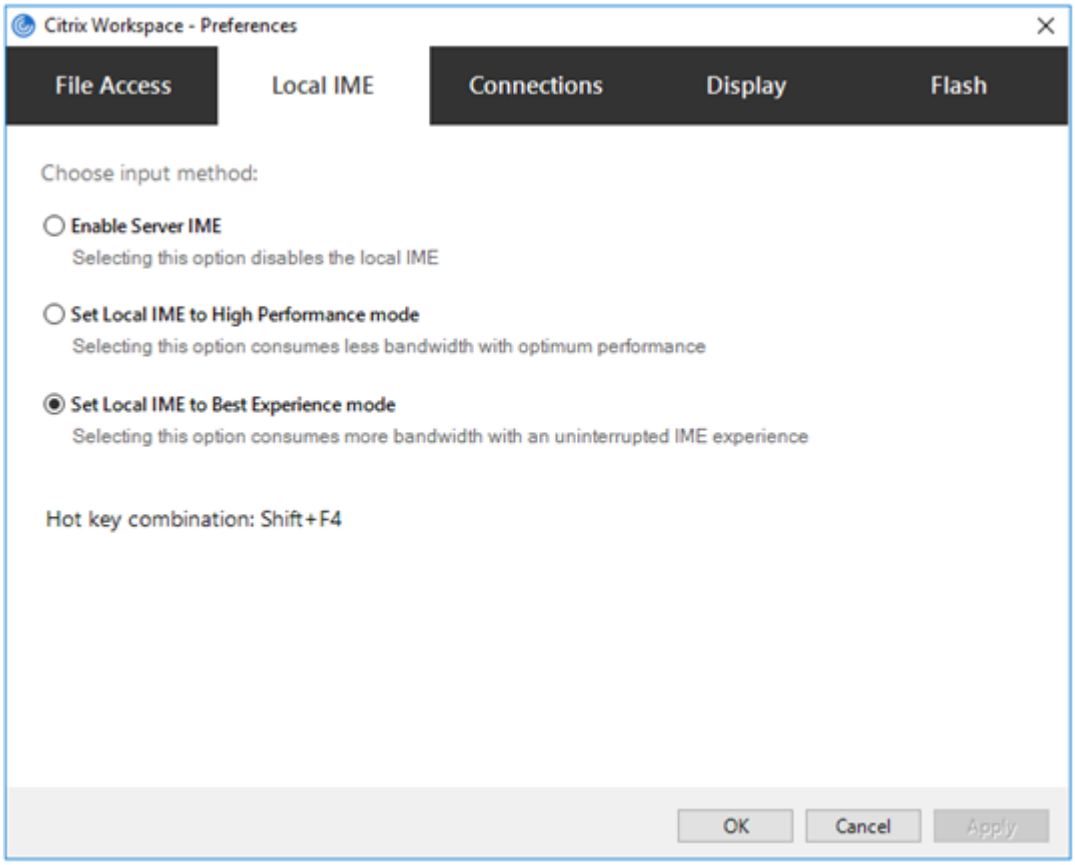
使用图形用户界面配置通用客户端 **IME**：

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. 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。

所做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_CURRENT_USER\SOFTWARE\Citrix\ICA Client\Engine\Lockdown Profiles\All Regions\Lockdown\Client Engine\Hot Key`。

选择 **AllowHotKey** 并将默认值更改为 1。

可以使用 **Shift+F4** 热键在会话中选择不同的 IME 模式。

使用这些热键组合进行切换时，IME 模式的不同选项会出现在会话的右上角。

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。要禁用，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。必须在 VDA 和 Citrix Workspace 应用程序中支持并启用 H.265 视频编解码器。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 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

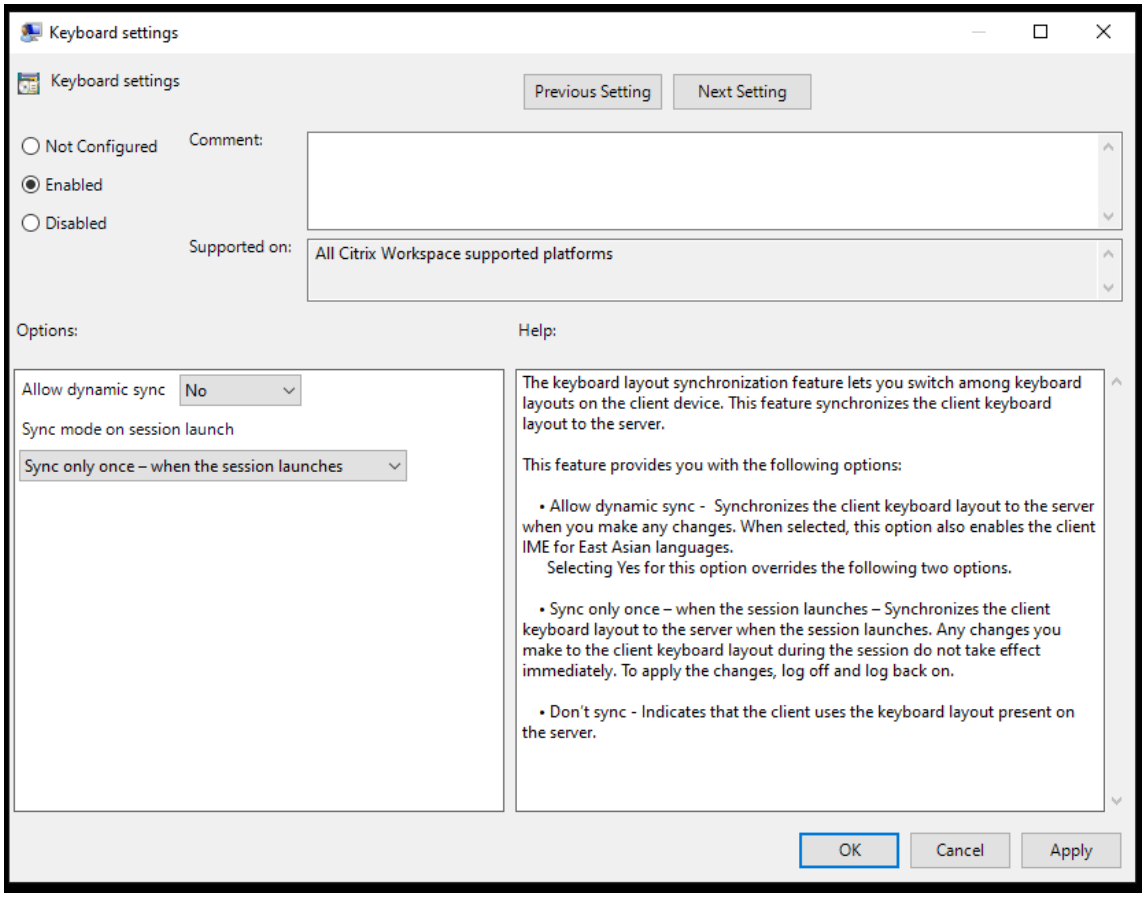
> 注意：
>
> 可以隐藏通知区域中的 Citrix Workspace 应用程序图标中提供的全部或部分“高级首选项”表。有关详细信息，请参阅“高级首选项”表。

键盘布局同步允许您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。键盘布局同步功能允许客户端键盘布局自动同步到虚拟应用程序和桌面会话。

要使用 **GPO** 管理模板配置键盘布局同步，请执行以下操作：

> 注意：
>
> GPO 配置的优先级高于 StoreFront 和 GUI 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. 在计算机配置或用户配置节点下，转至管理模板 > 经典管理模板 **(ADM)** > **Citrix** 组件 > **Citrix Workspace** > 用户体验。
3. 选择键盘设置策略。



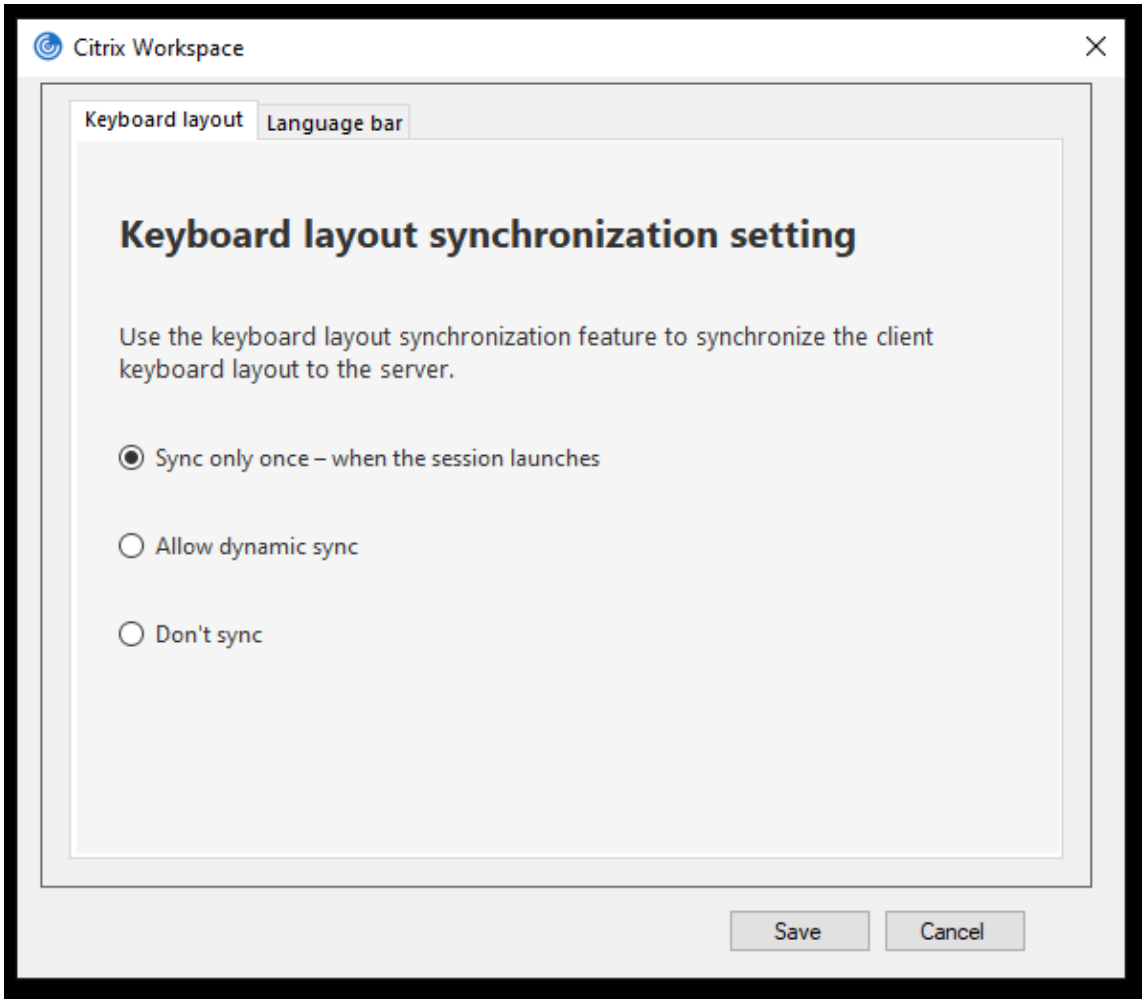
4. 选择已启用，然后选择以下选项之一：
   - 允许动态同步 - 从下拉菜单中，选择是或否。更改客户端键盘布局时，此选项会将客户端键盘布局同步到服务器。选中后，此选项还会为东亚语言启用客户端 IME。

     为此选项选择是将覆盖下面两个选项。
   - 会话启动时同步模式 - 从下拉菜单中选择以下选项之一：
     - 仅同步一次 - 会话启动时 - 在会话启动时将客户端键盘布局同步到服务器。在会话期间对客户端键盘布局所做的任何更改都不会立即生效。要应用更改，请注销并重新登录。
     - 不同步 - 指示客户端使用服务器上存在的键盘布局。
5. 选择应用和确定。

要使用图形用户界面配置键盘布局同步，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：
   - 仅同步一次 - 会话启动时 - 指示仅在会话启动时从 VDA 同步键盘布局一次。
   - 允许动态同步 - 指示在会话中更改了客户端键盘时将键盘布局动态同步到 VDA。
   - 不同步 - 指示客户端使用服务器上存在的键盘布局。
3. 单击保存。

要使用 **CLI** 配置键盘布局同步，请执行以下操作：

从适用于 Windows 的 Citrix Workspace 应用程序安装文件夹中运行以下命令。

通常情况下，Citrix Workspace 应用程序安装文件夹位于 `C:\Program files (x86)\Citrix\ICA Client`。

- 要启用：`wfica32:exe /localime:on`
- 要禁用：`wfica32:exe /localime:off`

使用客户端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` 来禁用客户端键盘布局选项。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。

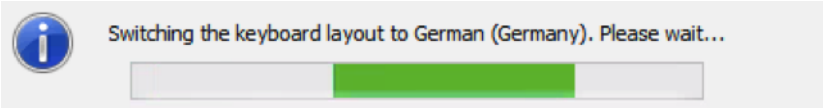
有时，切换客户端键盘布局在活动会话中不起作用。要解决此问题，请从 Citrix Workspace 应用程序注销并重新登录。

在 **Windows VDA** 上配置键盘同步

> 注意：
>
> 以下过程仅适用于 Windows Server 2016 及更高版本。在 Windows Server 2012 R2 及更早版本中，默认情况下启用键盘同步功能。

1. 启动注册表编辑器并导航到 `HKEY_LOCAL_MACHINE\Software\Citrix\IcaIme`。
2. 创建 DWORD 条目 `DisableKeyboardSync` 并将其值设置为 `0`。
   1 禁用键盘布局同步功能。
3. 重新启动会话以使更改生效。

在 VDA 和 Citrix Workspace 应用程序上启用键盘布局后，切换键盘布局时将出现以下窗口。



此窗口表示会话键盘布局正在切换到客户端键盘布局。

在 **Linux VDA** 上配置键盘同步

启动命令提示符并运行以下命令：

```
/opt/Citrix/VDA/bin/ctxreg update -k "HKEY_LOCAL_MACHINE\System\CurrentControlSet
\Control\Citrix\LanguageBar"-v "SyncKeyboardLayout"-d "0x00000001"
```

重新启动 VDA 以使更改生效。

有关 Linux VDA 上的键盘布局同步功能的详细信息，请参阅动态键盘布局同步。

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不支持的布局，出于安全原因，将禁用键盘布局的同步功能。无法识别的键盘布局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。

语言栏

语言栏显示会话中的首选输入语言。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。

使用 **GPO** 管理模板配置语言栏：

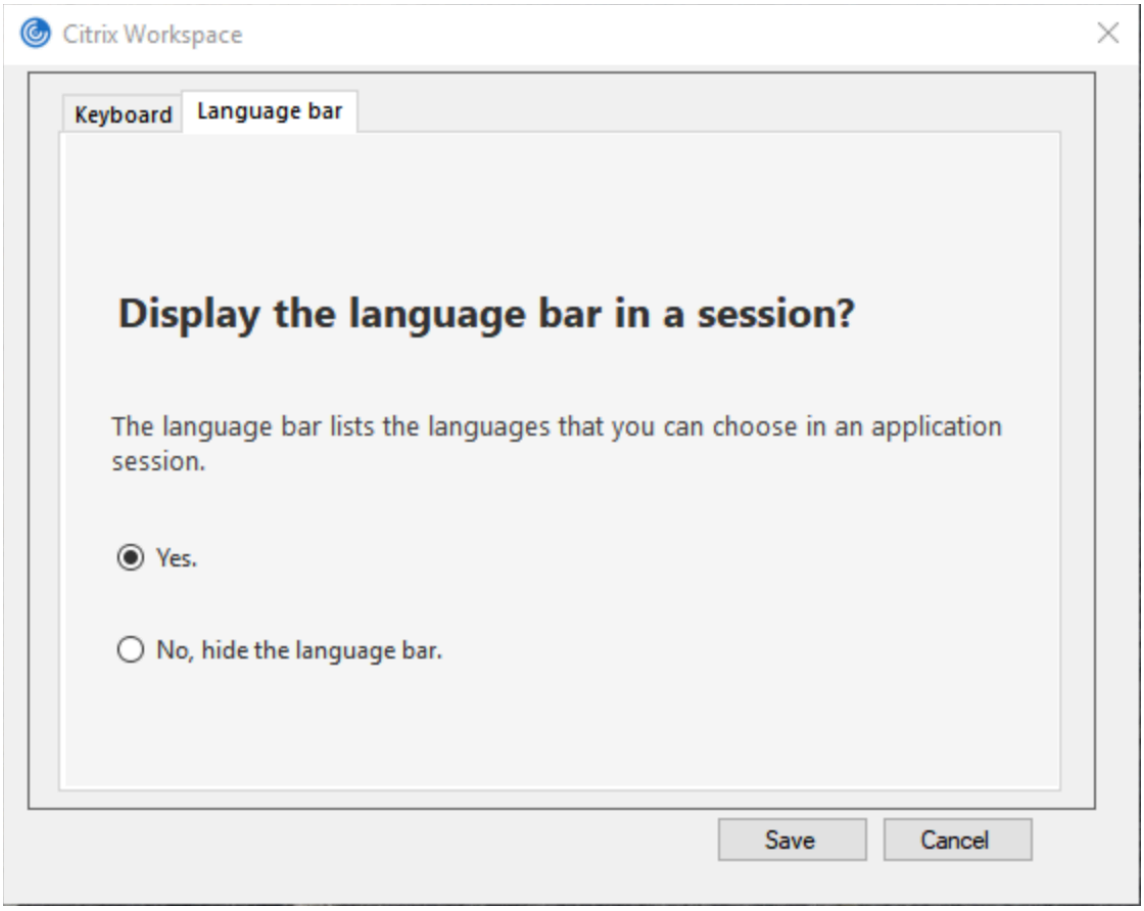
语言栏显示应用程序会话中的首选输入语言。

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. 在计算机配置或用户配置节点下，转至管理模板 > 经典管理模板 **(ADM)** > **Citrix** 组件 > **Citrix Workspace** > 用户体验。
3. 选择语言栏策略。
4. 选择已启用，然后选择以下选项之一：
   - 是 - 指示在应用程序会话中显示语言栏。
   - 否，隐藏语言栏 - 指示在应用程序会话中隐藏语言栏。
5. 单击应用和确定。

使用图形用户界面配置语言栏：

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。

此外在典型的低延迟或高速 LAN 环境中还支持 USB 同步设备（例如网络摄像机、麦克风、扬声器和耳机）中的常时等量功能。此类环境允许这些设备使用诸如 Microsoft Office Communicator 和 Skype 等软件包进行交互。

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 NIC。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 NIC
- 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 设备用于虚拟应用程序会话：

- 蓝牙适配器
- 集成 NIC
- 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。用户可以选择每次连接时必须将哪些 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。

默认情况下允许连接的 **USB** 设备类

默认的 USB 策略规则允许使用不同类别的 USB 设备。

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。此类 USB 设备类别如下所示。

- 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 XenDesktop 4 或更高版本支持的常时等量传输。音频（类 01）不适用于虚拟应用程序，因为这些设备在虚拟应用程序中不可使用 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。可能还可以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）不适用于虚拟应用程序，因为这些设备在虚拟应用程序中不可使用 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**） - 视频类涵盖用于操作视频或视频相关材料的设备。网络摄像机、数码摄相机、模拟视频变频器、某些电视调谐器等设备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 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，此类设备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

默认的 USB 策略规则不允许使用以下不同类别的 USB 设备：

- 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恰当的处理。此外，连接到虚拟桌面时，通常需要在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，或者连接关键的外围设备（例如蓝牙键盘或蓝牙鼠标）。

  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

编辑适用于 Windows 的 Citrix Workspace 应用程序模板文件以更新可远程连接到桌面的 USB 设备的范围。此更新允许您使用组策略对适用于 Windows 的 Citrix Workspace 进行更改。该文件位于已安装的以下文件夹中：

```
\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。

复合 **USB** 设备重定向

USB 2.1 及更高版本支持 USB 复合设备的概念，即多个子设备通过同一 USB 总线共享单个连接。此类设备采用单个配置控制和共享总线连接，其中唯一接口号 00-ff 用于标识每个子设备。此类设备也与为其他独立解决的 USB 设备提供新的 USB 总线源以用于连接的 USB 集线器不同。

可以将在客户端端点上发现的复合设备转发给虚拟主机作为以下设备：

- 单个复合 USB 设备，或
- 一组独立的子设备（拆分设备）

转发复合 USB 设备时，整个设备将对端点不可用。转发还将阻止对端点上的所有应用程序在本地使用设备，包括优化的 HDX 远程体验所需的 Citrix Workspace 客户端。

对于静音和音量控制，请考虑使用带音频设备和 HID 按钮的 USB 耳机设备。如果整个设备使用通用 USB 通道进行转发，该设备将不能通过优化的 HDX 音频通道进行重定向。但是，通过优化的 HDX 音频通道发送音频时，可以实现最佳体验，这与使用主机端音频驱动程序通过通用 USB 远程连接发送的音频不同。此行为是因为 USB 音频协议的噪音特性。

系统键盘或指针设备属于具有远程会话支持所需的其他集成功能的复合设备的一部分时，您也会注意到这些问题。转发完整的复合设备时，在端点上系统键盘或鼠标将变得无法工作，在远程桌面会话或应用程序中除外。

要解决这些问题，Citrix 建议您拆分复合设备，并且仅转发使用通用 USB 通道的子接口。此类机制可确保其他子设备可供客户端端点上的应用程序使用，包括提供优化的 HDX 体验的 Citrix Workspace 应用程序，同时仅允许将所需的设备转发到远程会话并供远程会话使用。

设备规则：

与常规 USB 设备一样，在策略中设置的设备规则或端点上的客户端 Citrix Workspace 应用程序配置将选择用于转发的复合设备。Citrix Workspace 应用程序使用这些规则决定允许或阻止哪些 USB 设备转发到远程会话。

每个规则都由操作关键字（允许、连接或拒绝）、冒号 (**:**) 以及与端点 USB 子系统中的实际设备匹配的零个或多个过滤参数组成。这些过滤参数对应于每个 USB 设备用来标识自身的 USB 设备描述符元数据。

设备规则是每条规则在一行中的明文，在 **#** 字符之后是可选注释。规则自上而下进行匹配（按优先级降序降序）。应用与设备或子接口匹配的第一条规则。选择相同设备或接口的后续规则将被忽略。

示例设备规则：

- ALLOW: vid=046D pid=0102 # 通过 vid/pid 允许特定设备
- ALLOW: vid=0505 class=03 subclass=01 # 当 subclass=01 时允许供应商 0505 的任何 pid
- DENY: vid=0850 pid=040C # 拒绝特定设备（包括所有子设备）
- DENY: class=03 subclass=01 prot=01 # 拒绝任所有过滤器匹配的所有设备
- CONNECT: vid=0911 pid=0C1C # 允许并自动连接特定设备
- ALLOW: vid=0286 pid=0101 split=01 # 拆分此设备并允许所有接口
- ALLOW: vid=1050 pid=0407 split=01 intf=00,01 # 拆分并且只允许 2 个接口
- CONNECT: vid=1050 pid=0407 split=01 intf=02 # 拆分和自动连接接口 2
- DENY: vid=1050 pid=0407 split=1 intf=03 # 防止接口 03 被远程访问

可以使用以下任何过滤参数将规则应用到遇到的设备：

过滤参数	说明
vid=xxxx	USB 设备供应商 ID（四位十六进制代码）
pid=xxxx	USB 设备产品 ID（四位十六进制代码）
rel=xxxx	USB 设备版本 ID（四位十六进制代码）
class=xx	USB 设备类别代码（两位十六进制代码）
subclass=xx	USB 设备子类代码（两位十六进制代码）
prot=xx	USB 设备协议代码（两位十六进制代码）
split=1（或 split=0）	选择要拆分（或不拆分）的复合设备
intf=xx [、xx、xx、…]	选择复合设备的特定子接口集（以逗号分隔的两位十六进制代码列表）

前六个参数选择必须应用规则的 USB 设备。如果未指定任何参数，规则将匹配具有该参数的任何值的设备。

USB Implementors Forum 维护已定义的类、子类和已定义类代码中的协议值列表。USB-IF 还维护注册的供应商 ID 的列表。可以直接在 Windows 设备管理器中或者使用 UsbTreeView 等免费工具检查特定设备的供应商、产品、版本和接口 ID。

当存在时，最后两个参数仅适用于 USB 复合设备。拆分参数决定复合设备必须作为拆分设备转发还是作为单个复合设备转发。

- *Split=1* 表示必须将复合设备的所选子接口作为拆分设备转发。

- *Split=0* 表示不得拆分复合设备。

> 注意：
>
> 如果忽略 split 参数，则假定使用 *Split=0*。

intf 参数选择必须将操作应用到的复合设备的特定子接口。如果忽略，该操作将应用到复合设备的所有接口。

考虑使用具有三个接口的复合 USB 耳机设备：

- 接口 0 - 音频类设备端点
- 接口 3 - HID 类设备端点（音量和静音按钮）
- 接口 5 - 管理/更新接口

建议的适用于此类型的设备的规则包括：

- CONNECT: vid=047F pid=C039 split=1 intf=03 # 允许并自动连接 HID 设备
- DENY: vid=047F pid=C039 split=1 intf=00 # 拒绝音频端点
- ALLOW: vid=047F pid=C039 split=1 intf=05 # 允许 mgmt intf 但不自动连接

启用设备规则策略：

适用于 Windows 的 Citrix Workspace 应用程序包括一组默认设备规则，这些规则可过滤某些不需要的设备类，并允许使用客户经常遇到的设备类别。

可以在以下系统注册表中检查以下默认设备规则：

- `HKEY_LOCAL_MACHINE\Software\Citrix\ICA Client\GenericUSB`（32 位 Windows）或
- `HKEY_LOCAL_MACHINE\Software\WOW6432Node\Citrix\ICA Client\GenericUSB`（64 位 Windows），在名为 **DeviceRules** 的多字符串值中。

但是，在适用于 Windows 的 Citrix Workspace 应用程序中，可以应用 **USB** 设备规则策略来覆盖这些默认规则。

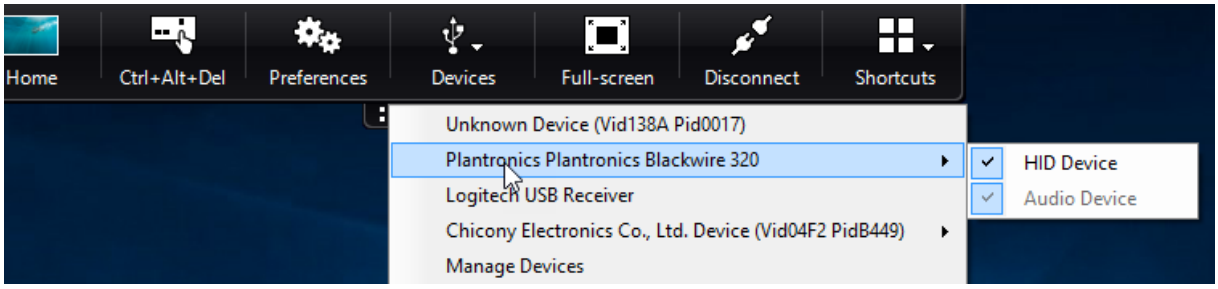
要为适用于 Windows 的 Citrix Workspace 应用程序启用设备规则策略，请执行以下操作：

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，粘贴（或直接编辑）要部署的 USB 设备规则。
6. 单击应用和确定。

Citrix 建议您在创建此策略时保留客户端附带的默认规则，方法为复制原始规则并插入新规则以根据徐需要更改行为。

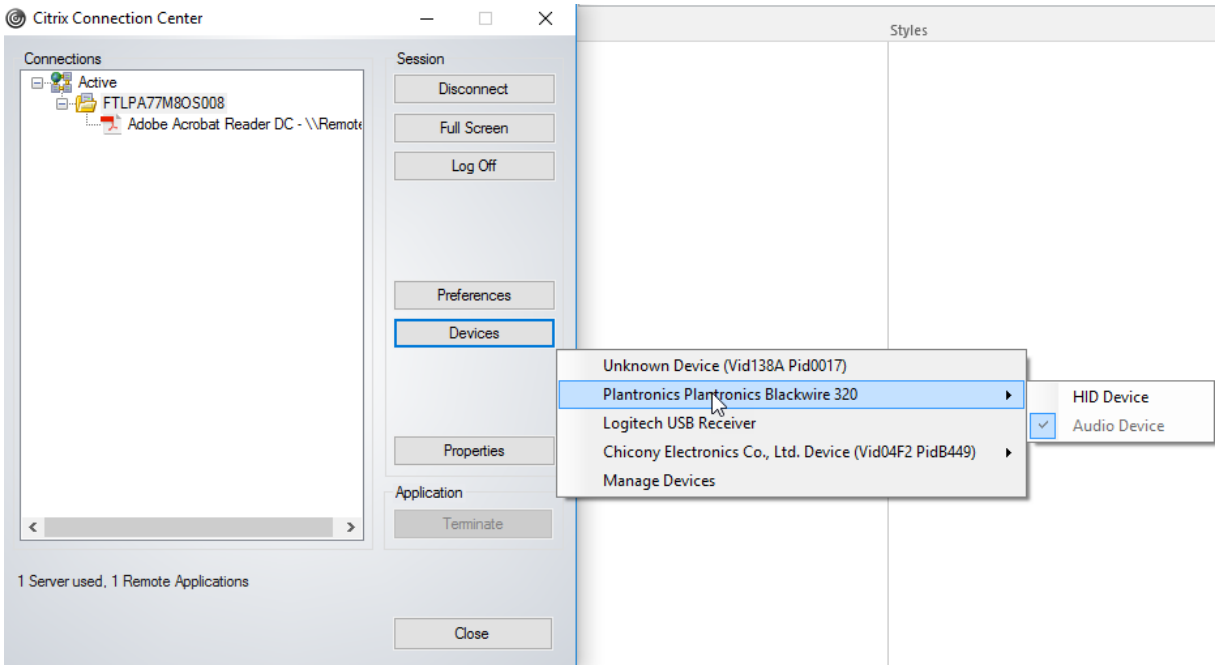
连接 **USB** 设备：

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



> 注意：
>
> CONNECT 关键字允许自动连接 USB 设备。但是，如果拆分复合 USB 设备以用于通用 USB 重定向时未使用 CONNECT 关键字，则必须从 Desktop Viewer 或连接中心手动选择该设备以连接允许的设备。

在应用程序会话中，拆分 USB 设备显示在连接中心中。



要自动连接接口，请执行以下操作：

适用于 Windows 的 Citrix Workspace 应用程序 2109 中引入的 CONNECT 关键字允许自动重定向 USB 设备。如果管理员允许设备或选定的接口在会话中自动连接，CONNECT 规则可以替换 ALLOW 规则。

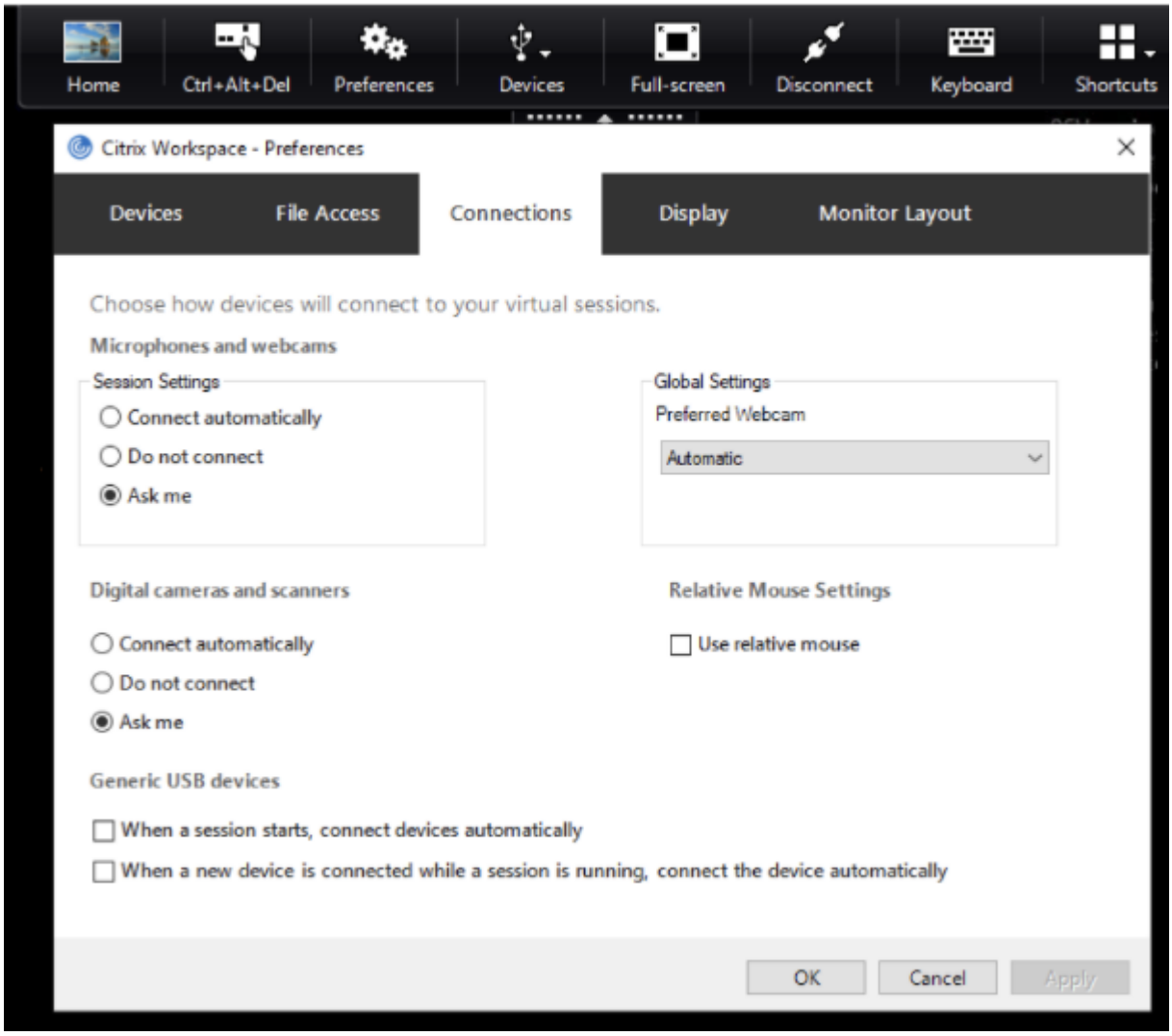
1. 通过运行 gpedit.msc 打开 Citrix Workspace 应用程序组策略对象管理模板。
2. 在用户配置节点下，转至管理模板 > **Citrix** 组件 > **Citrix Workspace** > 远程连接客户端设备 > 通用 **USB** 远程连接。
3. 选择 **USB** 设备规则策略。
4. 选择已启用。
5. 在 **USB** 设备规则文本框中，添加要自动连接的 USB 设备。

例如，CONNECT: vid=047F pid=C039 split=01 intf=00,03 – 允许拆分复合设备以及接口 00 和 03 接口的自动连接，并限制该设备的其他接口。

6. 单击应用和确定保存此策略。

更改 **USB** 设备自动连接首选项：

Citrix Workspace 应用程序根据为当前桌面资源设置的首选项自动连接带 CONNECT 操作标记的 USB 设备。可以在 **Desktop Viewer** 工具栏中更改首选项，如下图所示。



窗格底部的两个复选框控制设备是必须自动连接还是等待在会话中手动连接。默认情况下，不启用这些设置。如果必须自动连接通用 USB 设备，可以更改首选项。

或者，管理员可以通过从 Citrix Workspace 应用程序组策略对象管理模板部署相应的策略来覆盖用户首选项。可以在管理模板 > **Citrix** 组件 > **Citrix Workspace** > 远程连接客户端设备 > 通用 **USB** 远程连接下找到计算机和用户策略。相应的策略分别标记为“现有 USB 设备”和“新 USB 设备”。

更改拆分设备默认设置：

默认情况下，适用于 Windows 的 Citrix Workspace 应用程序仅拆分在设备规则中明确标记为 *Split=1* 的复合设备。但是，可以更改默认结构以拆分所有未在匹配设备规则中使用 *Split=0* 标记的复合设备。

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。

> 注意：
>
> Citrix 建议使用显式设备规则来识别需要拆分的特定设备或接口，而非更改默认设备规则。此设置会在将来的版本中弃用。

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。

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。

与标准键盘相比，Bloomberg 键盘提供其他功能，即允许用户访问财务市场数据并执行交易。

Bloomberg 键盘由内置在一个物理 shell 中的多个 USB 设备组成：

- 键盘
- 指纹读取器
- 音频设备
- 用于将所有这些设备连接到系统的 USB 集线器
- HID 按钮，例如音频设备的静音、调高音量和调低音量

除了这些设备的常规功能外，音频设备还支持某些按键、键盘控件和键盘 LED。

必须重定向音频设备作为 USB 设备，才能在会话中使用专用功能。此重定向可使音频设备对会话可用，但会阻止在本地使用音频设备。此外，专用功能只能与一个会话一起使用，不能在多个会话之间共享。

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 **5**：

必须配置 Bloomberg 键盘的各种接口。自适用于 Windows 的 Citrix Workspace 应用程序 2109 起，引入了一个新的 CONNECT 关键字，以允许在会话启动和设备插入时自动连接 USB 设备。当用户希望 USB 设备或接口自动连接时，可以使用 CONNECT 关键字替换、ALLOW 关键字。以下示例使用 CONNECT 关键字。

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. 在 **USB** 设备规则文本框中，添加以下规则（如果不存在）。
    - CONNECT: vid=1188 pid=A101 # Bloomberg 5 生物特征识别模块
    - DENY: vid=1188 pid=A001 split=01 intf=00 # Bloomberg 5 主键盘
    - CONNECT: vid=1188 pid=A001 split=01 intf=01 # Bloomberg 5 键盘 HID
    - DENY: vid=1188 pid=A301 split=01 intf=02 # Bloomberg 5 键盘音频通道
    - CONNECT: vid=1188 pid=A301 split=01 intf=00,01 # Bloomberg 5 键盘音频 HID

    > 注意：
    >
    > 换行符或分号可用于分隔规则，允许读取单行或多行注册表值。
6. 单击应用和确定保存此策略。
7. 在首选项窗口中，选择连接选项卡，然后自动选中与连接设备连接的一个或两个复选框。首选项窗口可从桌面工具栏或连接管理器访问。

此过程使 Bloomberg 键盘 5 可供使用。这些步骤中提及的 DENY 规则强制主键盘和音频通道不通过通用 USB 重定向，而是通过优化的通道进行重定向。CONNECT 规则允许自动重定向指纹模块、键盘上的特殊按键以及与音频控制有关的按键。

配置 **Bloomberg** 键盘 **4** 或 **3**：

> 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。

适用于 Windows 的联机插件 11.2 及后续版本中提供 Bloomberg 键盘 3 支持。

Bloomberg 键盘 4 支持适用于 Windows Receiver 4.8 及更高版本。

确定是否已启用 **Bloomberg** 键盘支持：

- 要检查联机插件中是否启用了对 Bloomberg 键盘的支持，请检查 Desktop Viewer 如何报告 Bloomberg 键盘设备。如果未使用 Desktop Viewer，可以在运行联机插件的计算机上检查注册表。

- 如果未启用对 Bloomberg 键盘的支持，Desktop Viewer 将显示：
  - 两台用于 Bloomberg 键盘 3 的设备，显示为 **Bloomberg Fingerprint Scanner**（Bloomberg 指纹扫描仪）和 **Bloomberg Keyboard Audio**（Bloomberg 键盘音频）。
  - 一个策略重定向的设备用于 Bloomberg 键盘 4。此设备显示为 **Bloomberg LP Keyboard 2013**（Bloomberg LP 键盘 2013）。
- 如果启用了对 Bloomberg 键盘的支持，Desktop Viewer 中将显示两个设备。其中一个与以前一样显示为 **Bloomberg Fingerprint Scanner**（Bloomberg 指纹扫描仪），另一个显示为 **Bloomberg Keyboard Features**（Bloomberg 键盘功能）。
- 如果未安装 Bloomberg 指纹扫描仪设备的驱动程序，Bloomberg 指纹扫描仪条目可能不会在 Desktop Viewer 中显示。如果缺少该条目，Bloomberg 指纹扫描仪可能无法进行重定向。您仍可以检查启用了 Bloomberg 键盘支持的其他 Bloomberg 设备的名称。
- 还可以检查注册表中的值，以确认是否启用了支持：
  `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICAClient\GenericUSB\EnableBloombergHID`

  如果值不存在或者为 0（零），则不启用对 Bloomberg 键盘的支持。如果值为 1，则将启用支持。

启用 **Bloomberg** 键盘支持：

> 注意：
>
> Citrix Receiver for Windows 4.8 通过 **SplitDevices** 策略引入了对复合设备的支持。但是，对于 Bloomberg 键盘 4，您必须使用 Bloomberg 键盘功能来代替此策略。

对 Bloomberg 键盘的支持将改变某些 USB 设备重定向到会话的方式。默认情况下不启用此支持。

- 要在安装期间启用支持，请在安装命令行中将 **ENABLE_HID_REDIRECTION** 属性的值指定为 TRUE。例如：

```
CitrixOnlinePluginFull.exe /silent
ADDLOCAL="ICA_CLIENT,PN_AGENT,SSON,USB"
ENABLE_SSON="no"INSTALLDIR="c:\test"
ENABLE_DYNAMIC_CLIENT_NAME="Yes"
DEFAULT_NDSCONTEXT="Context1,Context2"
SERVER_LOCATION="http://testserver.net"ENABLE_HID_REDIRECTION="TRUE"
```

- 要安装联机插件后启用支持，请编辑运行联机插件的系统中的 Windows 注册表：
  1. 打开“注册表编辑器”。
  2. 导航到以下注册表项：
     `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB`
  3. 如果值 **EnableBloombergHID** 存在，请进行修改，以使值数据为 1。
  4. 如果值 **EnableBloombergHID** 不存在，请创建一个名为 EnableBloombergHID 的 DWORD 值，并提供值数据 1。

禁用对 **Bloomberg** 键盘的支持：

可以按如下所示在联机插件中禁用对 Bloomberg 键盘的支持：

1. 在运行联机插件软件的系统中打开注册表编辑器。
2. 导航到以下注册表项：
   `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\GenericUSB`
3. 如果值 **EnableBloombergHID** 存在，请进行修改，以使值数据为 0（零）。

   如果值 **EnableBloombergHID** 不存在，则指示未启用对 Bloomberg 键盘的支持。在此类情况下，不需要修改任何注册表值。

在未启用支持的情况下使用 **Bloomberg** 键盘：

- 可以在联机插件中不启用 Bloomberg 键盘支持的情况下使用键盘。但是，无法在多个会话之间共享专用功能，并且可能会遇到音频中网络带宽增加的问题。
- Bloomberg 键盘普通按键的可用方式与任何其他键盘相同。不需要执行任何特殊操作。
- 必须将 Bloomberg 键盘音频设备重定向到会话中，才能使用专用 Bloomberg 按键。如果您使用的是 Desktop Viewer，则将显示 USB 设备的制造商名称和设备名称，并且 **Bloomberg** 键盘音频将针对 Bloomberg 键盘音频设备显示。
- 必须将设备重定向到 Bloomberg 指纹扫描仪，才能使用指纹读取器。如果未在本地安装指纹读取器的驱动程序，设备将只能显示以下内容：
  - 如果将联机插件设置为自动连接设备，或者
  - 以允许用户选择是否连接设备。

  此外，如果在建立会话之前已连接 Bloomberg 键盘，并且本地不存在指纹读取器驱动程序，指纹读取器将不会显示，并且在会话中无法使用。

> 注意：
>
> 对于 Bloomberg 3，单个会话或本地系统可以使用指纹读取器，并且无法共享。禁止 Bloomberg 4 进行重定向。

启用支持后使用 **Bloomberg** 键盘：

- 如果在联机插件中启用了对 Bloomberg 键盘的支持，您将能够在多个会话中共享专用键盘功能。您还会遇到音频中出现的网络带宽较低的问题。
- 启用对 Bloomberg 键盘的支持将阻止重定向 Bloomberg 键盘音频设备。而是改为提供一个新设备。如果您使用的是 Desktop Viewer，此设备称为 “Bloomberg Keyboard Features”（Bloomberg 键盘功能）。重定向此设备可为会话提供专用 Bloomberg 按键。

启用 Bloomberg 键盘支持仅影响专用 Bloomberg 按键和音频设备。因为使用普通按键和指纹读取器的方式与未启用支持时相同。

HDX Plug and Play USB 设备重定向

HDX Plug and Play USB 设备重定向可将媒体设备动态重定向到服务器。媒体设备包括相机、扫描仪、媒体播放器和 POS 设备。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：
>
> 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。

将客户端 COM 端口映射到服务器 COM 端口

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

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

> 重要：
>
> 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
   ```

   提示将显示映射的驱动器、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。

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。对于升级，导入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`。

大容量存储设备

仅适用于大容量存储设备，除了 USB 支持外，还可以通过客户端驱动器映射进行远程访问。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 > 客户端驱动器映射对其进行配置。应用此策略时，用户登录时，用户设备上的驱动器将自动映射到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”

如果同时启用了通用 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。

客户端驱动器映射

客户端驱动器映射支持在主机和客户端之间以流的形式传输数据。文件传输适应不断变化的网络吞吐量条件。它还将使用任何可用的额外带宽来加快数据传输速率。

默认情况下，启用此功能。

要禁用此功能，请设置以下注册表项，然后重新启动服务器：

路径：HKEY_LOCAL_MACHINE\System\Currentcontrolset\services\picadm\Parameters
名称：DisableFullStreamWrite
类型：REG_DWORD
值：
0x01 - 禁用，
0 或空白 - 启用

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，这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。

禁用用户设备映射

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。在服务器上仅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。当您在服务器上启用了客户端文件夹重定向，并且用户在用户设备上配置了客户端文件夹重定向时，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

客户端驱动器映射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	服务器可通过以下方式访问：
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。因此，服务器驱动器盘符将更改为更高的驱动器盘符。
在下例中，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	服务器可通过以下方式访问：
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。如果您将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，该网络驱动器映射将无效。

除非禁用了自动客户端设备映射，否则将用户设备连接到服务器会重新建立客户端映射。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。

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（其中 Citrix Workspace 应用程序在托管会话的 VDA 上运行）中，您现在可以控制 Citrix Workspace 应用程序是否启动：

- VDA 上安装的应用程序的本地实例（如果可作为本地应用程序使用）或
- 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 的 Windows 注册表中搜索应用程序的安装路径。如果存在，则启动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不在 VDA 上，Citrix Workspace 应用程序将启动托管应用程序。有关 StoreFront 如何处理本地启动的详细信息，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。对于升级，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。
5. 从允许应用程序下拉列表中，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）。然后，它将在 VDA 上启动该应用程序，而非在托管应用程序上启动。
   - 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。
6. 单击应用和确定。
7. 重新启动会话以使更改生效。

限制：

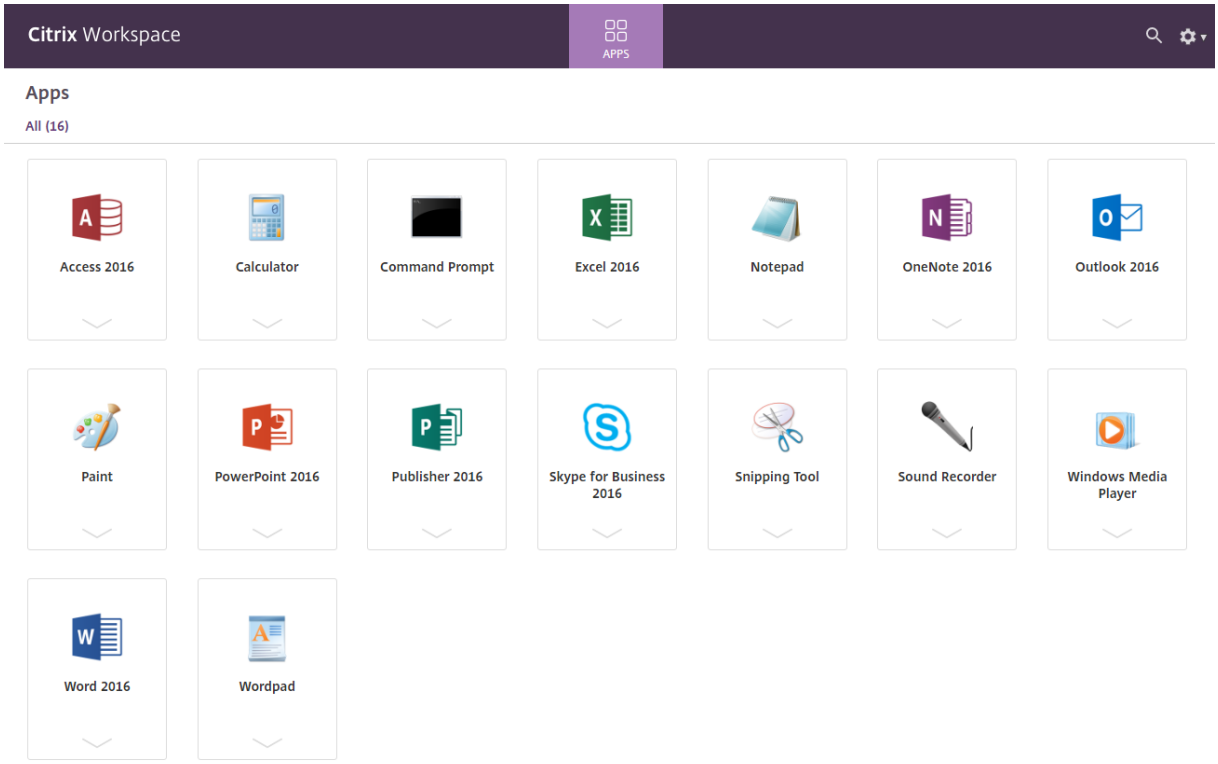
- 适用于 Web 的 Workspace 不支持此功能。

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”。



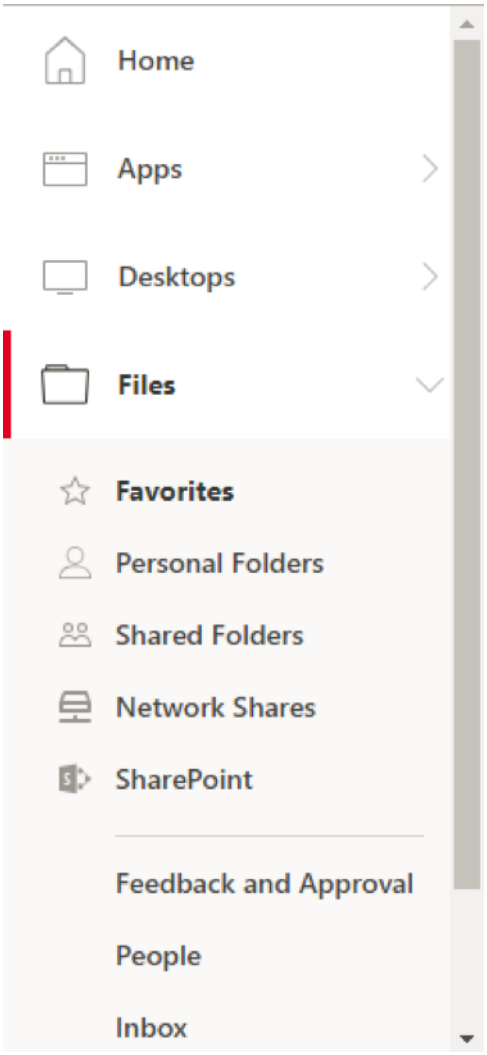
Content Collaboration Service 集成

此版本引入了 Citrix Content Collaboration Service 与 Citrix Workspace 应用程序的集成。您可以利用 Citrix Content Collaboration 轻松、安全地交换文档、通过电子邮件发送大型文档、安全地处理向第三方的文档传输以及访问协作空间。Citrix Content Collaboration 提供了多种工作方式，包括基于 Web 的界面、移动客户端、桌面应用程序以及与 Microsoft Outlook 和 Gmail 的集成。

可以使用 Citrix Workspace 应用程序中显示的文件选项卡从 Citrix Workspace 应用程序访问 Citrix Content Collaboration 功能。仅当从 Citrix Cloud 控制台中的 Workspace 配置中启用了 Content Collaboration Service 时，才能看到文件选项卡。

> 注意：
>
> 由于操作系统中的安全选项，Windows Server 2012 和 2016 不支持 Citrix Workspace 应用程序中的 Citrix Content Collaboration 集成。

下图显示了新 Citrix Workspace 应用程序的文件选项卡的示例内容：



限制：

- 重置 Citrix Workspace 应用程序不会注销 Citrix Content Collaboration。
- 在 Citrix Workspace 应用程序中切换应用商店不会注销 Citrix Content Collaboration。

使用注册表编辑器为 **Citrix Files** 配置下载位置：

1. 启动注册表编辑器并导航到 `HKEY_CURRENT_USER\Software\Citrix\Dazzle\`。
2. 按名称 **DownloadPreference** 创建“字符串值”注册表项。
3. 将 Citrix Files 的首选下载路径复制并粘贴到“值”列。
4. 如果希望每次下载时都出现提示，请将“值”列设置为 *。

有关使用高级首选项 UI 配置 Citrix Files 下载位置的信息，请参阅适用于 Windows 的 Citrix Workspace 应用程序文档中的使用高级首选项配置下载位置。

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 Single Sign-On 一起提供。管理员现在可以保护组织的网络和最终用户设备免受恶意软件和数据泄露的侵害。管理员可以通过过滤对特定 Web 站点和 Web 站点类别的访问来实现此目的。

适用于 Windows 的 Citrix Workspace 应用程序支持通过 Citrix Secure Private Access 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 Single Sign-On 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。
- Single Sign-on – 使用 Single Sign-On 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。

Citrix Workspace 应用程序在 Citrix Enterprise Browser（以前称为 Citrix Workspace Browser）上启动 SaaS 应用程序。有关信息，请参阅 Citrix Enterprise Browser 文档。

限制：

1. 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时，您仍然可以保存 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

适用于 Windows 的 Citrix Workspace 应用程序支持在会话中进行 PDF 打印。通过 Citrix PDF 通用打印机驱动程序，您可以打印使用 Citrix Virtual Apps and Desktops 和 Citrix DaaS 上运行的托管应用程序和桌面启动的文档。

当您从打印对话框中选择 **Citrix PDF** 打印机选项时，打印机驱动程序会将文件转换为 PDF 并将此 PDF 传输至本地设备。随后此 PDF 会使用默认的 PDF 查看器启动以进行查看，并从本地连接的打印机打印。

Citrix 建议使用 Google Chrome 浏览器或 Adobe Acrobat Reader 查看 PDF。

可以在 Delivery Controller 上使用 Citrix Studio 启用 Citrix PDF 打印。

必备条件：

- 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。

在启用了触控功能的客户端设备上，当您连接或重新连接到会话时，Windows 10 VDA 将检测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，您可以像带键盘和鼠标的 PC 一样进行交互。

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

浏览器内容重定向

浏览器内容重定向会阻止在 VDA 端呈现允许列表中的 Web 页面。此功能会使用 Citrix Workspace 应用程序在客户端实例化相应的呈现引擎，该引擎会从 URL 提取 HTTP 和 HTTPS 内容。

> 注意：
>
> 可以使用阻止列表指定要重定向到 VDA 端（以及不在客户端重定向）的 Web 页面。

除 Internet Explorer 浏览器外，浏览器内容重定向功能还支持 Google Chrome 浏览器。浏览器内容重定向功能将 Web 浏览器的内容重定向到客户端设备，并创建在 Citrix Workspace 应用程序中嵌入的相应浏览器。此功能将网络

使用、页面处理和图形呈现卸载到端点。这样做可以改进浏览要求高的 Web 页面（尤其是包含 HTML5 或 WebRTC 视频的 Web 页面）时的用户体验。

- cookie 在会话中持久存在：退出并重新启动浏览器时，系统不会提示您重新输入凭据。
- 浏览器现在支持本地系统语言。

有关详细信息，请参阅浏览器内容重定向。

配置浏览器内容重定向叠加浏览器临时数据存储的路径

自 Citrix Workspace 应用程序 2303 版本起，要求您为基于 Chromium Embedded Framework (CEF) 的浏览器配置临时数据存储路径。要配置路径，请执行以下操作：

1. 打开注册表编辑器。
2. 导航到 `HKCU\Software\Citrix\HdxMediaStream` 注册表路径。
3. 创建具有以下属性的注册表值：
   - 注册表项名称：`BCRProfilePath`
   - 注册表值：字符串 `<folder for CEF based BCRtmp files>`
4. 重新启动 Citrix Workspace 应用程序以使所做的更改生效。

Citrix Analytics

Citrix Workspace 应用程序已经过检测，可以安全地将日志传输到 Citrix Analytics。启用后，将在 Citrix Analytics 服务器上分析和存储日志。有关 Citrix Analytics 的详细信息，请参阅 Citrix Analytics。

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：
>
> - IP 地址传输是在最佳情况下所做的努力。尽管 Citrix Workspace 应用程序会传输启动该应用程序的每个 IP 地址，但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。

Citrix Workspace 应用程序经过检测，可以从您从浏览器启动的 ICA 会话安全地将数据传输到 Citrix Analytics 服务。

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

相对鼠标

相对鼠标功能决定自窗口或屏幕中最后一帧起鼠标移动的距离。
相对鼠标使用两次鼠标移动之间的像素增量。例如，使用鼠标控件更改相机的方向时，该功能非常有效。应用程序通常也会隐藏鼠标光标，因为在操作 3D 对象或场景时，与光标相对于屏幕坐标的位置不相关。

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解释。

您可以在每用户和每会话基础上配置该功能，这样可以更精细地控制功能的可用性。

> 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。

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`

- 名称：RelativeMouse
- 类型：REG_SZ
- 值：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。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 为在创建时为其指定的名称。对于 StoreFront 客户，默认.ica 文件通常位于 `C:\inetpub\wwwroot\Citrix\<Storename>\App_Data\default.ica`，其中 `storename` 是创建应用商店时为其设置的名称。
2. 在 WFClient 部分中添加一个名为 RelativeMouse 的注册表项。将其值设置为与 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。

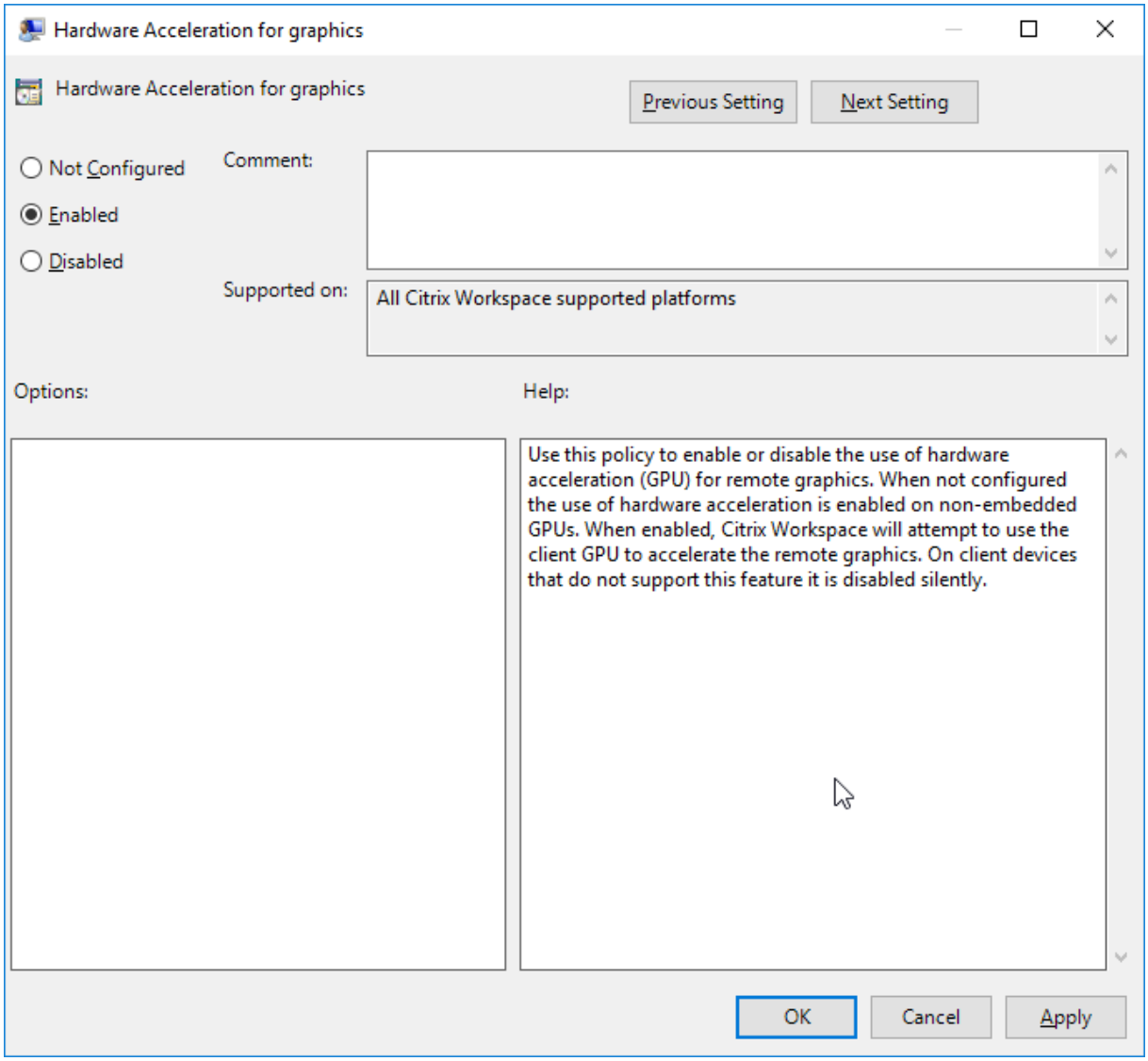
> 注意：
>
> 从 Desktop Viewer 配置相对鼠标仅将该功能应用于每会话。

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。



要验证是否为活动的 ICA 会话设置了策略以及是否使用了硬件加速，请检查以下注册表项：

注册表路径：`HKEY_CURRENT_USER\SOFTWARE\Citrix\ICA Client\CEIP\Data\GfxRender`。

> 提示
>
> **Graphics_GfxRender_Decoder** 和 **Graphics_GfxRender_Renderer** 的值必须为 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，请不要在用户的 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。可以将本地安装的麦克风用于：

- 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 和 Citrix DaaS 查看器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，请检查以下各项：

- 用户设备配置为支持多个显示器。
- 操作系统可以检测到每台显示器。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，然后在任务窗格中选择：
      - 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）和
    - 设置用于每个会话的图形的最大内存。

检查设置是否足够大（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 计算会话的图形内存要求，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”，并修改“图像压缩”和“图像和字体缓存”选项。

屏幕键盘控制

要允许您从 Windows 平板电脑触控访问虚拟应用程序和桌面，Citrix Workspace 应用程序将在以下情况下自动显示屏幕键盘：

- 您激活了文本输入字段时，以及
- 当设备处于帐篷模式或平板电脑模式时。

在某些设备上，在某些情况下，Citrix Workspace 应用程序无法准确检测设备的模式。屏幕键盘也可能在您不希望其出现时出现。

要在使用可转换设备时禁止显示屏幕键盘，请执行以下操作：

- 在 `HKEY\\_CURRENT\\_USER\\SOFTWARE\\Citrix\\ICA Client\\Engine\\Configuration\\Advanced\\Modules\\MobileReceiver` 中创建 REG_DWORD 值 DisableKeyboardPopup，并
- 将值设置为 1。

> 注意：
>
> 在 64 位计算机上，请在 HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\MobileReceiver 中创建该值。

按键可以设置为以下 3 种不同的模式：

- **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。

Citrix Workspace 应用程序支持 **32** 位色图标：

Citrix Workspace 应用程序支持 32 位增强色图标。为了针对无缝应用程序提供，它会自动为以下对象选择颜色深度：

- 连接中心对话框中可见的应用程序，
- “开始” 菜单以及
- 任务栏

> 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。

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功能，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可为用户组提供无缝的桌面体验。也适用于需要以一致的方式访问一组核心应用程序的用户。

此标志称为 **SelfServiceMode**，且默认情况下设置为 `True`。当管理员将 **SelfServiceMode** 标志设置为 `False` 时，您无法访问自助服务用户界面。相反，您可以从 “开始” 菜单和和桌面快捷方式（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。如果从桌面中删除快捷方式图标，当用户选择通知区域中的 Citrix Workspace 应用程序图标上的

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，无法阻止用户配置更多应用商店。管理员可以授予用户使用组策略对象模板添加多个帐户的特殊权限。管理员还可以通过在客户端计算机上手动添加注册表项 (HideEditStoresDialog) 来提供特殊权限。如果管理员向用户授予此权限，用户将可以在通知区域中看到“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。编辑注册表设置后，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 10 不允许在“开始”菜单中创建嵌入式文件夹。应用程序单独显示或显示在根文件夹下。但是，不在使用 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。
- 使用注册表项 `AutoReInstallModifiedApps` 可以启用“自动重新安装修改后的应用程序”功能。启用 `AutoReInstallModifiedApps` 后，对服务器上已发布的应用程序和桌面属性所做的任何更改都会在客户端计算机上显示。禁用 `AutoReInstallModifiedApps` 后，应用程序和桌面属性将不会更新，并且在客户端上删除的快捷方式在刷新时也不会恢复。默认情况下，`AutoReInstallModifiedApps` 处于启用状态。

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。
> - 在配置应用商店之前更改注册表项。如果您或用户在任何时候想要自定义注册表项，您或该用户必须：
>
> 1. 重置 Citrix Workspace 应用程序
> 2. 配置注册表项，然后
> 3. 重新配置应用商店。

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。通过工作区控制功能，医院的临床医生可以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。也可以使用组策略对加入域的客户端设备执行工作区控制。

> 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 = 在 Windows 登录时重新连接
- 11 = 3 和 8 的组合

禁用工作区控制

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`

将以下注册表项从默认值 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：
>
> 如果您不想创建注册表项，也可以将 **WSCReconnectAll** 注册表项设置为 false。

32 位计算机的注册表项

注册表项：**WSCSupported**

值：`True`

注册表项路径：


```
- 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
```

注册表项：**WSCReconnectAll**

值：True

注册表项路径：

```
- `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`
```

注册表项：**WSCReconnectMode**

值：3

注册表项路径：

```
- 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
```

注册表项：**WSCReconnectModeUser**

值：在安装期间不创建注册表。

注册表项路径：

```
- 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：

注册表项：**WSCSupported**

值：True

注册表项路径：

```
- 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
```

注册表项：**WSCReconnectAll**

值：True

注册表项路径：

```
-  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
```

注册表项：**WSCReconnectMode**

值：3

注册表项路径：

```
-  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
```

注册表项：**WSCReconnectModeUser**

值：在安装期间不创建注册表。

注册表项路径：

```
- HKEY_CURRENT_USER\Software\Citrix\Dazzle
- HKEY_CURRENT_USER\Software\Citrix\Receiver\SR\Store" + primaryStoreID
    +\Properties
```



```
3  - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Policies\Citrix\Dazzle
4  - HKEY_LOCAL_MACHINE\Software\Wow6432Node\Citrix\Dazzle
```

Desktop Viewer

不同的企业可能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可能会因用户的不同和企业需求的变化而不同。连接到虚拟桌面的用户体验以及用户可以配置连接的程度取决于适用于 Windows 的 Citrix Workspace 应用程序的设置。

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：
>
> 应使用 Citrix Workspace 应用程序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、筛选键和切换键等某些 Microsoft 辅助功能的按键通常指向本地计算机。

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。组合键序列（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。

> 注意：
>
> 不能对 Desktop Viewer 中显示的虚拟桌面（即虚拟应用程序和桌面会话）使用热键序列。但是，您可以将其用于已发布的应用程序，即虚拟应用程序会话。

虚拟桌面

在桌面会话中，用户无法连接到同一个虚拟桌面。如果用户尝试执行此操作，请断开现有桌面会话的连接。因此，Citrix 建议：

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

本地登录到用作虚拟桌面的计算机的用户会阻止与该桌面进行连接。

定义设备映射：

- 如果您的用户从虚拟桌面连接到通过虚拟应用程序发布的虚拟应用程序，并且
- 贵组织有单独的虚拟应用程序管理员。

设备映射将检查桌面设备在桌面和应用程序会话中的映射是否一致。在桌面会话中，本地驱动器显示为网络驱动器，因此虚拟应用程序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，请执行以下步骤：

1. 启动注册表编辑器。
2. 导航到以下路径：
   - 在 64 位计算机上：HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA CLIENT\Engine
   - 在 32 位计算机上：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA CLIENT\Engine\
3. 创建如下注册表项：
   - 类型：REG_DWORD
   - 名称：SI INACTIVE MS
   - 值：4（如果您希望状态指示器尽快消失）。

配置此注册表项时，状态指示器可能会频繁出现并消失。这种行为是有意为之。要禁止显示状态指示器，请执行以下操作：

1. 启动注册表编辑器。
2. 导航到以下路径：
   - 在 64 位计算机上：HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA CLIENT\
   - 在 32 位计算机上：HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA CLIENT\
3. 创建如下注册表项：
   - 类型：REG_DWORD
   - 名称：NotificationDelay
   - 值：以毫秒为单位的任何值（例如，120000）

Workspace 会话的不活动超时

管理员可以配置不活动超时值，以指定在用户自动从 Citrix Workspace 应用程序会话注销之前的空闲时间量。如果鼠标、键盘或触控在指定的时间间隔内处于空闲状态，您将自动从 Workspace 中注销。不活动超时不会影响活动的虚拟应用程序和桌面会话或 Citrix StoreFront 应用商店。

不活动超时值可以设置为从 1 分钟到 1440 分钟。默认情况下，不配置不活动超时。管理员可以使用 PowerShell 模块配置 inactivityTimeoutInMinutes 属性。单击此处下载适用于 Citrix Workspace 配置的 PowerShell 模块。

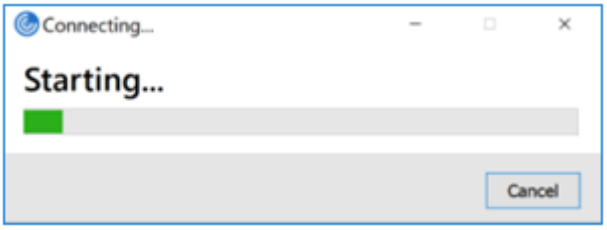
最终用户体验如下：

- 在注销前三分钟，您的会话窗口中将显示一条通知，提示一个用于保持登录或注销的选项。
- 只有在配置的不活动超时值大于或等于 5 分钟时，通知才显示。
- 用户可以单击保持登录消除通知并继续使用应用程序，在这种情况下，不活动计时器将重置为已配置的值。也可以单击注销结束当前应用商店的会话。

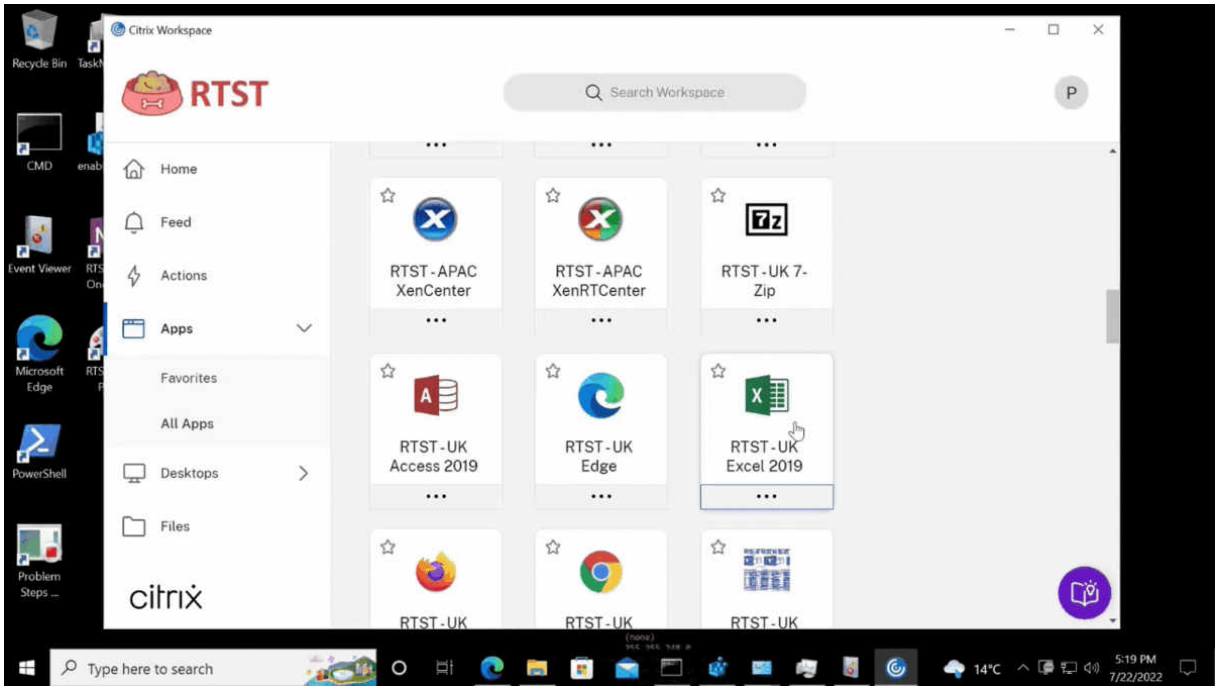
> 注意：
>
> 管理员只能为 Workspace（云）会话配置不活动超时。

改善了虚拟应用程序和桌面的启动体验 [技术预览版]

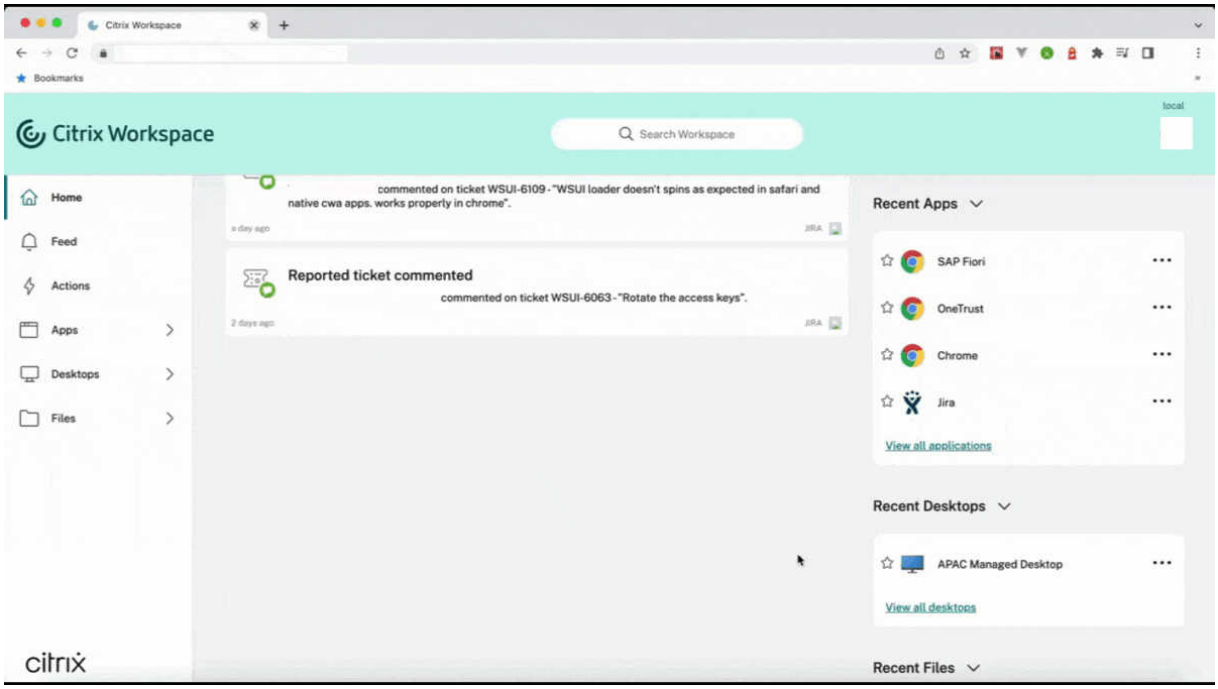
以前，启动进度对话框对用户来说不直观。它使用户假设启动过程没有响应，并且用户关闭了对话框，因为通知消息是静态的。



改进后的应用程序和桌面启动体验信息更丰富、更新式，并且在适用于 Windows 的 Citrix Workspace 应用程序上提供了用户友好的体验。这有助于让用户及时了解有关启动状态的相关信息。通知显示在屏幕的右下角。



适用于 Web 的 Workspace 也支持此功能。用户可以查看有关启动进度的有意义的通知，而不仅仅是微调器。如果正在启动并且用户尝试关闭浏览器，则会显示一条警告消息。



可以使用以下注册表启用此功能。

1. 打开注册表编辑器。
2. 导航到 `HKLM\SOFTWARE\WOW6432Node\Citrix\Dazzle`。
3. 创建并添加一个名为 NewLaunchExpSupport 的注册表字符串，然后将其值设置为 True。

4. 重新启动 Citrix Workspace 应用程序以使所做的更改生效。

> 注意：
>
> 这仅适用于 Workspace（云）会话。

已知问题：

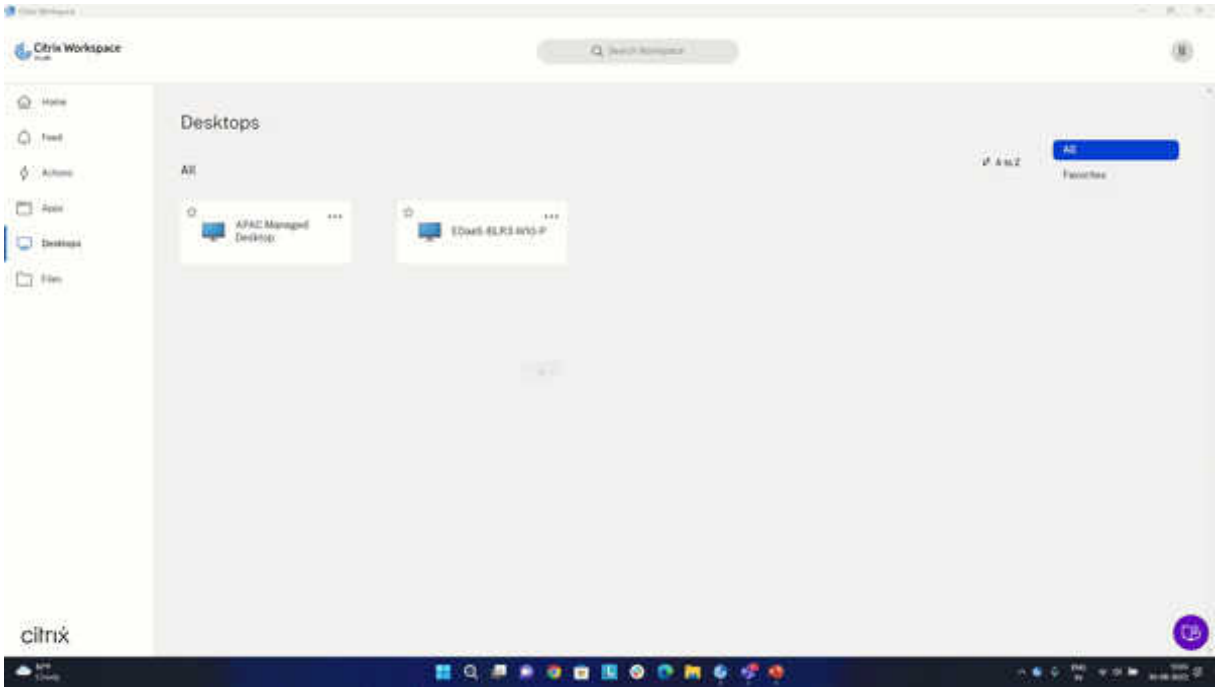
- 在多显示器设置中，Citrix Workspace 应用程序的桌面会话中的应用程序窗口移至不同的显示器。当您断开并重新连接会话时会出现此问题。
- 基于浏览器的启动不支持此功能。

可以通过 Podio 表单提供有关此功能的反馈。

> 注意：
>
> 技术预览版可供客户在其非生产环境或有限生产环境中进行测试，并为客户提供共享反馈的机会。Citrix 不接受功能预览版的支持案例，但欢迎提供改进这些功能的反馈。Citrix 可能会根据反馈的严重性、紧迫性和重要性对反馈执行操作。建议不要在生产环境中部署 Beta 版本。

快速启动断开连接的桌面 [技术预览版]

通过启用此功能，您可以立即打开以前断开连接的桌面。启用此功能后，Citrix Workspace 应用程序将在隐藏模式下启动断开连接的会话。启动桌面后，会话将立即显示。



> 注意：
>
> 这仅适用于 Workspace（云）会话。

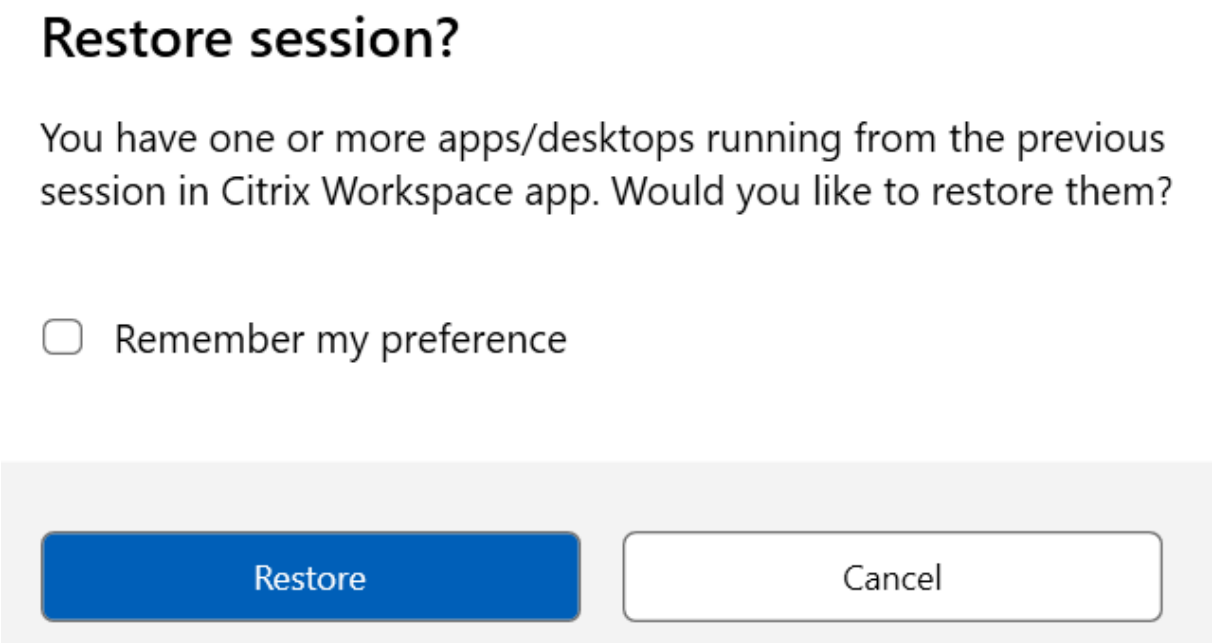
可以使用 Podio 表单注册此技术预览版。

> 注意：
>
> 技术预览版可供客户在其非生产环境或有限生产环境中进行测试，并为客户提供共享反馈的机会。Citrix 不接受功能预览版的支持案例，但欢迎提供改进这些功能的反馈。Citrix 可能会根据反馈的严重性、紧迫性和重要性对反馈执行操作。建议不要在生产环境中部署 Beta 版本。

改进了虚拟应用程序和桌面的重新连接体验

Citrix Workspace 2302 版本在重新连接到已断开连接的虚拟应用程序和桌面时提供了增强的用户体验。

当 Citrix Workspace 应用程序尝试刷新断开连接的 Citrix Workspace 应用程序或作为 Workspace 控制功能的一部分启动新虚拟应用程序或桌面时，会出现以下提示：



仅当 Global App Configuration Service 中的显示重新连接会话的重新连接提示设置为 true 时，才会出现此提示。

单击还原进行重新连接以打开新的和断开连接的虚拟应用程序和桌面。如果您只想启动新选定的应用程序和桌面，请单击取消。

也可以选择记住我的首选项，在下次登录时应用选定的首选项。

之前的新还原会话**?** 仅在以下情况下才会出现提示：

- 用户尝试启动属于工作区应用商店的应用程序，
- 没有为 Workspace 控制功能配置管理员策略或应用程序配置设置，
- Workspace 控制重新连接选项在客户端上设置为默认值。

> 注意：
>
> 重新连接选项中的重新连接设置优先于在对话框中设置的首选项。有关详细信息，请参阅使用“高级首选项”对话

> 框配置重新连接选项。

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。	此数据有助于 Citrix 提高 Citrix Workspace 应用程序的质量、功能和性能，为产品开发目的适当分配资源，维持服务水平并管理人员配置和基础结构投资。

收集的数据

如上所述，Citrix 会收集 Workspace 应用程序配置和使用情况数据，以提高 Workspace 应用程序的质量、功能和性能，并允许 Citrix 为产品开发目的适当分配资源，以及维持服务水平并管理人员配置和基础结构投资。数据仅以汇总形式使用和分析。未挑选出任何用户或其计算机，也不会根据 CEIP 数据对特定的最终用户进行分析。

Google Analytics 收集的特定 CEIP 数据元素包括：

操作系统版本 *	Workspace 应用程序版本 *	身份验证配置	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	应用程序保护配置	脱机横幅的原因
设备型号/特性	Citrix Virtual Apps and Desktops 会话启动状态	虚拟应用程序/桌面名称	自动更新状态
连接租约详细信息	StoreFront 到 Workspace URL 迁移功能用法	Citrix Enterprise Browser 使用情况	自动更新通道
不活动超时详细信息	Citrix Enterprise Browser 版本		

> 注意：
>
> 自版本 2206 起，Citrix Workspace 应用程序不会从位于欧盟 (EU)、欧洲经济区 (EEA)、瑞士和英国 (UK) 的用户那里收集任何 CEIP 数据。如果您希望利用此功能，请更新您的 Workspace 应用程序。

数据收集首选项

自版本 2205 起，用户和管理员都可以按照以下步骤停止发送 CEIP 数据（下面的“备注”中指定的可阻止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。

还可以使用用户身份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：
>
> 一旦您选择不，谢谢或将 `Enable_CEIP` 注册表项设置为 `False`，还可以通过导航到以下注册表项并设置值来停止发送最后两个 CEIP 数据元素（即操作系统和 Workspace 应用程序版本）：

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

注册表项：`DisableHeartbeat`

值：`True`

其他信息

Citrix 根据您与 Citrix 签订的合同条款处理您的数据，并按照 Citrix Services Security Exhibit（Citrix 服务安全性展示）中的规定对其进行保护。“Citrix Services Security Exhibit”（Citrix 服务安全性展示）可在 Citrix Trust Center（Citrix 信任中心）获取。

区域设置

Citrix Workspace 应用程序根据浏览器或端点设备的区域设置显示日期、时间和数字。

自 Citrix Workspace 应用程序 2106 起，您可以通过“区域设置”自定义区域日期、时间和数字格式。在这些设置中所做的更改将为单个用户保存，并跨所有设备应用。

> 注意：
>
> 此选项仅适用于云部署。

有关详细信息，请参阅区域设置。

Microsoft Teams

- 屏幕共享
- 编码器性能估算器
- 声学回声消除

WebRTC 的升级版，适用于经过优化的 Microsoft Teams

自版本 2209 起，用于优化的 Microsoft Teams 的 WebRTC 版本已升级到版本 M98。

使用 HDX 进行的 Microsoft Teams 优化的背景模糊和效果

适用于 Windows 的 Citrix Workspace 应用程序现在支持使用 HDX 进行的 Microsoft Teams 优化中的背景模糊和效果。

您可以模糊背景或者使用自定义图像替换背景，并通过帮助对话专注于轮廓（身体和面部）来避免意外干扰。该功能可用于 P2P 或电话会议。

> 注意：
>
> 此功能现在已与 Microsoft Teams UI/按钮集成。多窗口支持是要求 VDA 更新到 2112 或更高版本的必备条件。有关详细信息，请参阅多窗口会议和聊天。

限制：

- 不支持管理员和用户定义的背景替换。
- 背景效果不会在会话之间持续存在。当您关闭并重新启动 Microsoft Teams 或重新连接 VDA 时，背景效果将重置为关闭。
- 重新连接 ICA 会话后，效果将关闭。但是，Microsoft Teams UI 显示一个对勾，指示之前的效果仍处于启用状态。Citrix 和 Microsoft 正在共同努力解决此问题。
- 更换背景图像时，设备必须连接到 Internet。

> 注意：
>
> 此功能仅在 Microsoft Teams 推出将来的更新后可用。Microsoft 推出此更新时，请查看 CTX253754 和 Microsoft 365 Public roadmap（Microsoft 365 公开路线图）以获取文档更新和公告。

屏幕共享

自版本 2006.1 起，在使用 HDX 优化的 Microsoft Teams 应用程序的传出屏幕共享功能中引入了新功能。

使用 Microsoft Teams 共享的内容仅限于 **Desktop Viewer** 窗口的内容。**Desktop Viewer** 窗口外部的区域（客户端本地桌面、应用程序）将显示为黑色。

在 Windows 10 操作系统中，以下对象在与 **Desktop Viewer** 窗口重叠时不会停止运行：

- “开始”菜单、“搜索”菜单和“任务视图”。
- 在任务栏右侧显示的通知栏和通知。
- 在设置了不同 DPI 设置的多显示器上，如果本地应用程序与 2 个不同的显示器重叠，并且其 DPI 与具有 Desktop Viewer 窗口的主显示器 DPI 不匹配。
- 将鼠标悬停在任务栏中的应用程序的图标上时会显示“应用程序和预览”。

编码器性能估算器

`HdxRtcEngine.exe` 是嵌入在 Citrix Workspace 应用程序中的 WebRTC 媒体引擎，用于处理 Microsoft Teams 重定向。自 Citrix Workspace 应用程序 1912 或更高版本起，`HdxRtcEngine.exe` 可以预估端点的 CPU 在不超载的情况下可以承受的最佳编码分辨率。可能的值为 240p、360p、480p、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。编解码器协商包括尽可能高的分辨率。编解码器协商可以是对等方之间的协商，也可以是对等方与会议服务器之间的协商。

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 (1920x1080 16:9 @ 30 fps)	3
中	720p (1280x720 16:9 @ 30 fps)	2
慢	360p（640x360 16:9 @ 30 fps 或 640x480 4:3 @ 30 fps）	1
非常慢	240p（320x180 16:9 @ 30 fp 或 320x240 4:3 @ 30 fps）	0

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 并创建以下注册表项：

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 表示慢，3 表示快。

有关配置端点编码器的信息，请参阅编码性能估算器。

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

声学回声消除

可以禁用 HdxRtcEngine.exe 中的回声消除功能，以解决音频性能问题或与具有内置 AEC 功能的外围设备的兼容性。

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

名称：EnableAEC
类型：REG_DWORD
数据：0
(0 表示禁用 AEC。1 表示启用 AEC。如果 Regkey 不存在，HdxRtcEngine 中的默认行为为启用 AEC，而无论外围设备的硬件功能如何。)

Microsoft Teams 优化的增强功能

- 自适用于 Windows 的 Citrix Workspace 应用程序 2112.1 起，以下功能（多窗口和授予控制权/获取控制权）仅在 Microsoft Teams 将来推出更新后才可用。

  Microsoft 推出此更新时，您可以查看 CTX253754 以获取文档更新和公告。

  - 面向 **Microsoft Teams** 的多窗口聊天和会议：在 Citrix Virtual Apps and Desktops（2112 或更高版本）中通过 HDX 优化后，您可以在 Microsoft Teams 中使用多个窗口进行聊天和会议。可以通过各种方式弹出对话或会议。有关弹出窗口功能的详细信息，请参阅 Microsoft Office 365 站点上的 Teams Pop-Out Windows for Chats and Meetings（Teams 用于聊天和会议的弹出窗口）。

    如果您正在运行较旧版本的 Citrix Workspace 应用程序或 Virtual Delivery Agent (VDA)，Microsoft 将来可能会弃用单窗口代码。但是，在该功能公开上市后的九个月之前，您可以升级到支持多个窗口（2112 或更高版本）的 VDA 或 Citrix Workspace 应用程序版本。

  - 授予控制权：可以使用授予控制权按钮将共享屏幕的控制权限授予参加会议的其他用户。另一位参与者可以通过键盘、鼠标和剪贴板输入进行选择和修改共享的屏幕。双方都可以控制共享屏幕，并且可以随时收回控制权。

- 获取控制权：在屏幕共享会话期间，任何参与者都可以通过请求控制权按钮请求控制权限。然后，共享屏幕的人员可以批准或拒绝该请求。拥有控制权后，您可以控制共享的屏幕上的键盘和鼠标输入，以及释放控制权以停止共享控制权。

限制：

在优化的用户与端点上运行的本机 Microsoft Teams 桌面客户端上的用户之间的点对点通话期间，请求控制权选项不可用。解决方法：用户可以加入会议以获取请求控制权选项。

- **Dynamic e911**：Citrix Workspace 应用程序支持动态紧急呼叫。在 Microsoft 通话套餐、接线员连接和直接路由中使用时，它提供了用于执行以下操作的选项：
  * 配置和路由紧急呼叫
  * 通知安全人员

  发送通知的依据是端点上运行的 Citrix Workspace 应用程序的当前位置，而非 VDA 上运行的 Microsoft Teams 客户端。
  Ray Baum 法律要求将 911 呼叫者的可调度位置传送到相应的公共安全应答点 (PSAP)。自适用于 Windows 的 Citrix Workspace 应用程序 2112.1 起，使用 HDX 的 Microsoft Teams 优化遵从 Ray Baum 的法律。
- 应用程序共享：以前，当您在 Citrix Studio 中启用了 HDX 3D Pro 策略时，将无法使用 Microsoft Teams 中的屏幕共享功能共享应用程序。

自适用于 Windows 的 Citrix Workspace 应用程序 2112.1 和 Citrix Virtual Apps and Desktops 2112 起，屏幕共享功能允许您在 Microsoft Teams 中共享应用程序。启用 HDX 3D Pro 策略后，您可以共享应用程序。

- 自适用于 Windows 的 Citrix Workspace 应用程序 2109.1 起，以下功能可用：
  - 支持 **WebRTC 1.0**：适用于 Windows 的 Citrix Workspace 应用程序 2109.1 支持 WebRTC 1.0，可提供更好的视频会议体验以及库视图。
  - 屏幕共享增强功能：您可以使用 Microsoft Teams 中的屏幕共享功能来共享各个应用程序、窗口或整个屏幕。使用此功能必须安装 Citrix Virtual Delivery Agent 2109。
  - 应用程序保护兼容性：启用应用程序保护后，现在可以通过具有 HDX 优化功能的 Microsoft Teams 共享内容。借助此功能，您可以共享在虚拟桌面中运行的应用程序窗口。使用此功能必须安装 Citrix Virtual Delivery Agent 2109。

  > 注意：
  >
  > 为交付组启用应用程序保护时，将禁用完全监视或桌面共享。

- 适用于 Windows 的 Citrix Workspace 应用程序 2109.1 在 VM 托管应用程序上的经过优化的 Microsoft Teams 中支持以下功能：
  - 点对点音频和视频通话
  - 电话会议

- 屏幕共享

- 自适用于 Windows 的 Citrix Workspace 应用程序 2106 起：
  - Desktop Viewer 处于全屏模式时，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。

- 自适用于 Windows 的 Citrix Workspace 应用程序 2105 起：
  - 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。禁用 ADM2 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。

- 自适用于 Windows 的 Citrix Workspace 应用程序 2103.1 起：
  - 默认情况下，VP9 视频编解码器现在处于禁用状态。
  - 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**。
  - DirectShow 现在为默认呈现器。

    要更改默认呈现器，请执行以下操作：

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

       其他可能的值：

       * 0：媒体基础
       * 1：DirectShow（默认）

4. 重新启动 Citrix Workspace 应用程序。

- 自适用于 Windows 的 Citrix Workspace 应用程序 2012 起：
  - 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。
  - WebRTC 媒体引擎现在支持在客户端设备上配置的代理服务器。
- 自适用于 Windows 的 Citrix Workspace 应用程序 2009.6 起：
  - Microsoft Teams 在首选设备列表中显示以前使用过的外围设备。
  - WebRTC 媒体引擎可以准确地确定端点上可能的最大编码分辨率。WebRTC 媒体引擎每天进行多次预估，而不仅仅是在首次启动时。
  - Citrix Workspace 应用程序安装程序已与 Microsoft Teams 铃声一起打包。
  - 回声消除改进功能 - 当对等机具有产生回声的扬声器或麦克风时，回声级别降低。
  - 屏幕共享改进功能 - 当您共享屏幕时，仅以本机位图格式捕获 **Desktop Viewer** 屏幕。以前，叠加在 **Desktop Viewer** 窗口顶部的客户端本地窗口将停止。
- 自适用于 Windows 的 Citrix Workspace 应用程序 2002 起：
  - 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。
- 自适用于 Windows 的 Citrix Workspace 应用程序 2302 起：
  - 更新了优化后的 **Microsoft Teams** 的音频设备选择行为 - 当您更改端点上的声音设置中的默认音频设备时，Citrix VDI 中经过优化的 Microsoft Teams 会更改当前的音频设备选择以匹配端点默认值。

    但是，如果您在 Microsoft Teams 中明确选择了设备，您的选择将优先，并且不遵循端点默认值。在清除 Microsoft Teams 缓存之前，您的选择持续不变。
- 自适用于 Windows 的 Citrix Workspace 应用程序 2303 起：
  - 改善了优化的 Microsoft Teams 视频会议通话的体验：默认情况下，对优化的 Microsoft Teams 视频会议通话启用了联播支持。有了这种支持，通过调整到适当的分辨率以便为所有呼叫者提供最佳通话体验，可以改善跨不同端点的视频会议通话的质量和体验。

通过这种改进的体验，每个用户都可以提供分辨率不同（例如 720p、360p 等）的多个视频流，具体取决于多种因素，包括端点能力、网络条件等。接收端点随后会请求其能够处理的最大质量分辨率，从而为所有用户提供最佳视频体验。

> 注意：
>
> 此功能仅在 Microsoft Teams 推出更新后可用。有关 ETA 的信息，请转至并搜索 Microsoft 365 路线图。Microsoft 推出此更新时，您可以查看 CTX253754 以获取文档更新和公告。

配置到 **Workspace** 应用程序的单点登录

April 6, 2023

使用 **Azure Active Directory** 的单点登录

本部分内容介绍了如何使用 Azure Active Directory (AAD) 作为身份提供程序，在混合或 AAD 注册的端点中使用已加入域的工作负载来实现单点登录 (SSO)。使用此配置，您可以在注册到 AAD 的端点上使用 Windows Hello 或 FIDO2 向 Workspace 进行身份验证。

> 注意：
>
> 如果使用 Windows Hello 作为独立的身份验证，则可以实现对 Citrix Workspace 应用程序的单点登录。但是，在访问已发布的虚拟应用程序或桌面时，系统会提示您输入用户名和密码。解决方法：请考虑实施联合身份验证服务 (FAS)。

必备条件

- 与 Citrix Cloud 的活动 Azure Active Directory 连接。有关详细信息，请参阅将 Azure Active Directory 连接到 Citrix Cloud。
- Azure Active Directory 工作区身份验证。有关详细信息，请参阅为工作区启用 Azure AD 身份验证。
- 验证您是否已配置 Azure AD 连接。有关详细信息，请参阅 Getting started with Azure AD Connect using express settings（使用快速设置开始使用 Azure AD Connect）。
- 在 Azure AD Connect 上激活直通身份验证。此外，请验证单点登录和直通选项在 Azure 门户上是否有效。有关详细信息，请参阅 Azure Active Directory 直通身份验证：快速入门。

配置

请执行以下步骤，以在您的设备上配置 SSO：

1. 使用带 `includeSSON` 选项的 Windows 命令行安装 Citrix Workspace 应用程序：

```
CitrixWorkspaceApp.exe /includeSSON
```

1. 重新启动您的设备。
2. 通过运行 `gpedit.msc` 打开 Citrix Workspace 应用程序组策略对象管理模板。
3. 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。
4. 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。
5. 在 Internet Explorer 中修改用户身份验证设置。要修改设置，请执行以下操作：

- 从“控制面板”中打开 **Internet** 属性。
- 导航到常规属性 > 本地 **Intranet**，然后单击站点。
- 在本地 **Intanet** 窗口中，单击高级，添加可信站点，添加以下可信站点，然后单击关闭：
  - `https://aadg.windows.net.nsatc.net`
  - `https://autologon.microsoftazuread-sso.com`
  - `The name of your tenant, for example: https://xxxtenantxxx.cloud.com`

6. 通过禁用租户中的 `prompt=login` 属性禁用额外的身份验证提示。有关详细信息，请参阅 User Prompted for Additional Credentials on Workspace URLs When Using Federated Authentication Providers（使用联合身份验证提供程序时提示用户在 Workspace URL 上输入其他凭据）。您可以联系 Citrix 技术支持以禁用租户中的 `prompt=login` 属性，以成功配置单点登录。
7. 在 Citrix Workspace 应用程序客户端上启用域直通身份验证。有关详细信息，请参阅域直通身份验证。
8. 重新启动 Citrix Workspace 应用程序以使所做的更改生效。

使用 **Okta** 和联合身份验证服务进行单点登录

本部分内容介绍如何使用 Okta 作为身份提供程序以及加入域的设备和联合身份验证服务 (FAS) 来实现单点登录 (SSO)。通过此配置，您可以使用 Okta 向 Workspace 进行身份验证，以启用单点登录并防止出现第二次登录提示。要使此身份验证机制起作用，您需要将 Citrix 联合身份验证服务与 Citrix Cloud 结合使用。有关详细信息，请参阅将 Citrix 联合身份验证服务连接到 Citrix Cloud。

必备条件

- Cloud Connector。有关安装 Cloud Connector 的详细信息，请参阅 Cloud Connector 安装。
- Okta 代理。有关安装 Okta 代理的详细信息，请参阅 Install the Okta Active Directory agent（安装 Okta Active Directory 代理）。此外，您可以将 Okta IWA Web 代理配置为从已加入 Windows 域的设备登录。有关详细信息，请参阅 Install and configure the Okta IWA Web agent for Desktop single sign-on（安装和配置用于桌面单点登录的 Okta IWA Web 代理）
- 与 Citrix Cloud 的活动 Azure Active Directory 连接。有关详细信息，请参阅将 Azure Active Directory 连接到 Citrix Cloud。
- 联合身份验证服务。有关详细信息，请参阅安装联合身份验证服务。

配置

请执行以下步骤，以在您的设备上配置 SSO：

将 **Citrix Cloud** 连接到您的 **Okta** 组织：

1. 下载并安装 Okta Active Directory 代理。有关详细信息，请参阅 Install the Okta Active Directory agent（安装 Okta Active Directory 代理）。
2. 登录到 Citrix Cloud，网址为 `https://citrix.cloud.com`。
3. 在 Citrix Cloud 菜单中，选择 **Identity and Access Management**（身份和访问管理）。
4. 找到 Okta，然后从省略号菜单中选择 **Connect**（连接）。
5. 在 **Okta URL** 中，输入您的 Okta 域。
6. 在 **Okta API Token**（Okta API 令牌）中，输入您的 Okta 组织的 API 令牌。
7. 在 **Client ID**（客户端 ID）和 **Client Secret**（客户端密码）中，输入您之前创建的 OIDC Web 应用程序集成中的客户端 ID 和密码。要从 Okta 控制台复制这些值，请选择 **Applications**（应用程序）并找到您的 Okta 应用程序。在 **Client Credentials**（客户端凭据）下，对每个值使用 **Copy to Clipboard**（复制到剪贴板）按钮。
8. 单击 **Test and Finish**（测试并完成）。Citrix Cloud 会验证您的 Okta 详细信息并测试连接。

为工作区启用 **Okta** 身份验证：

1. 在 Citrix Cloud 菜单中，选择 **Workspace Configuration**（工作区配置）> **Authentication**（身份验证）。
2. 选择 **Okta**。出现提示时，请选择 **I understand the impact on the subscriber experience**（我了解对订阅者体验产生的影响）。
3. 单击 **Accept**（接受）接受权限申请。

启用联合身份验证服务：

1. 在 Citrix Cloud 菜单中，选择 **Workspace Configuration**（工作区配置），然后选择 **Authentication**（身份验证）。
2. 单击 **Enable FAS**（启用 FAS）。此更改最多可能需要五分钟才能应用到订阅者会话。

之后，联合身份验证服务将对从 Citrix Workspace 启动的所有虚拟应用程序和桌面启用。

当订阅者登录其工作区并在与 FAS 服务器相同的资源位置启动虚拟应用程序或桌面时，应用程序或桌面将在不提示输入凭据的情况下启动。

> 注意：
>
> 如果资源位置中的所有 FAS 服务器都已关闭或处于维护模式，应用程序启动将成功，但单点登录未激活。系统会提示订阅者输入其 AD 凭据以访问每个应用程序或桌面。

客户端应用程序管理

March 29, 2023

适用于 Windows 的 Citrix Workspace 应用程序提供客户端应用程序管理功能，使 Citrix Workspace 应用程序成为端点安装和管理 Secure Access Agent 和端点分析 (EPA) 插件等代理所需的单个客户端应用程序。

借助此功能，管理员可以轻松地从单个管理控制台部署和管理所需的代理。

> 注意：
>
> 此功能仅适用于 Workspace（云）会话。

客户端应用程序管理包括以下步骤：

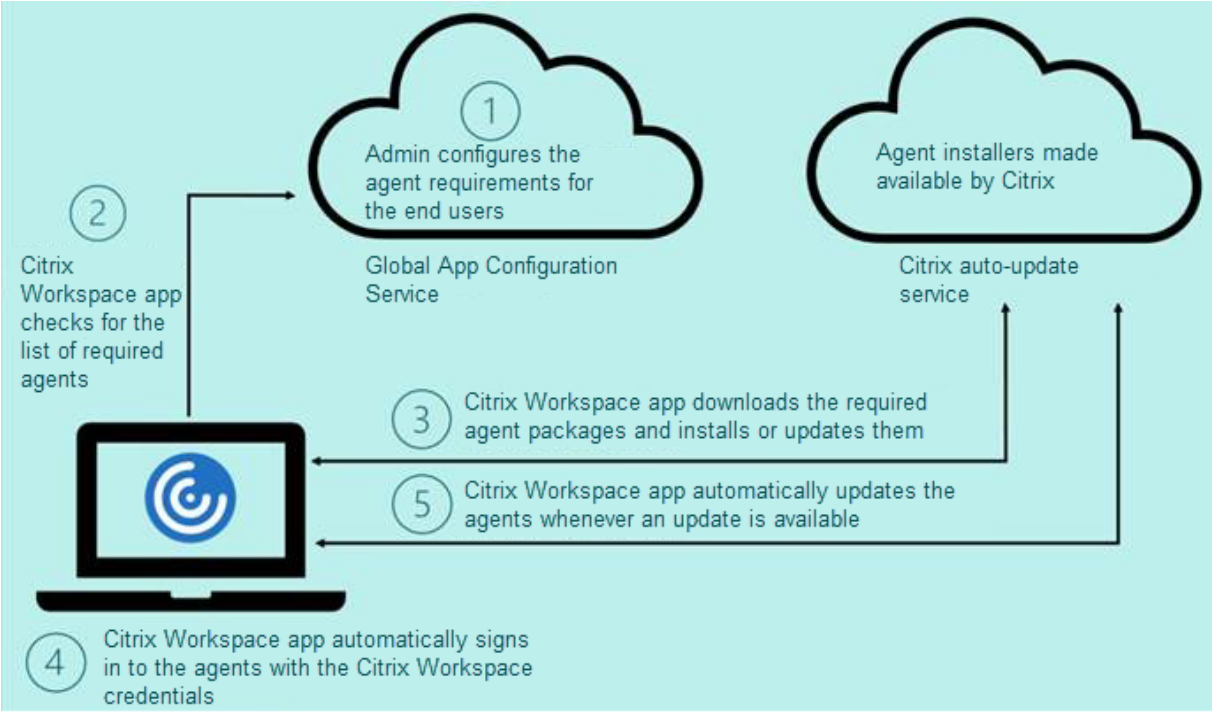
- 管理员必须在 Global App Configuration Service 中指定最终用户的设备上所需的代理。管理员可以指定 Secure Access Agent 和端点分析 (EPA) 代理。
- Citrix Workspace 应用程序从 Global App Configuration Service 获取代理列表。
- 根据从 Global App Configuration Service 获取的列表，Citrix Workspace 应用程序通过自动更新服务下载代理软件包。如果之前未在端点上安装代理，Citrix Workspace 应用程序将触发代理的安装。如果已安装代理，Citrix Workspace 应用程序会触发代理更新（如果下载的代理版本高于安装的版本）。

Citrix Workspace 应用程序可确保在将来有更新时自动更新代理。

Citrix Workspace 应用程序使用 Citrix Workspace 凭据自动登录代理。

> 备注：
>
> - 如果 EPA 和 ZTNA 插件不存在，则会在首次添加应用商店或帐户时下载和安装插件。
> - 如果应用商店或帐户以及插件已存在，并且安装程序包含更高版本，插件将在自动更新周期内更新。

下图说明了工作流程：



> 重要：
>
> 需要 Global App configuration Service 才能启用客户端应用程序管理功能。
>
> - 对于云应用商店，可以在 Citrix Cloud 管理门户的 **Workspace** 配置部分中访问 Global App configuration Service UI。
> - 要加载本地应用商店或者客户需要为云应用商店设置基于电子邮件的发现，请参阅 Global App configuration Service 文档。

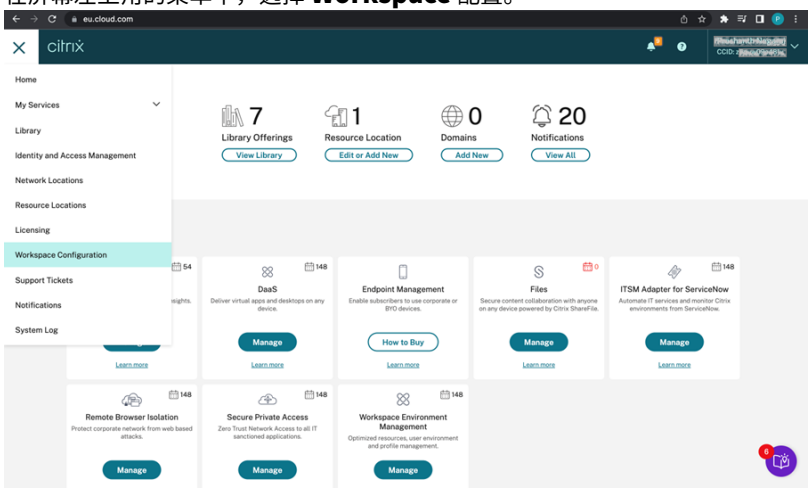
可以使用以下方法启用客户端应用程序管理功能：

- 使用 Global App configuration Service UI - 使用此方法可部署最新版本的客户端。
- 使用 Global App configuration Service API - 使用此方法可通过参数自定义安装，以控制版本、部署模式、自动更新时间间隔等。

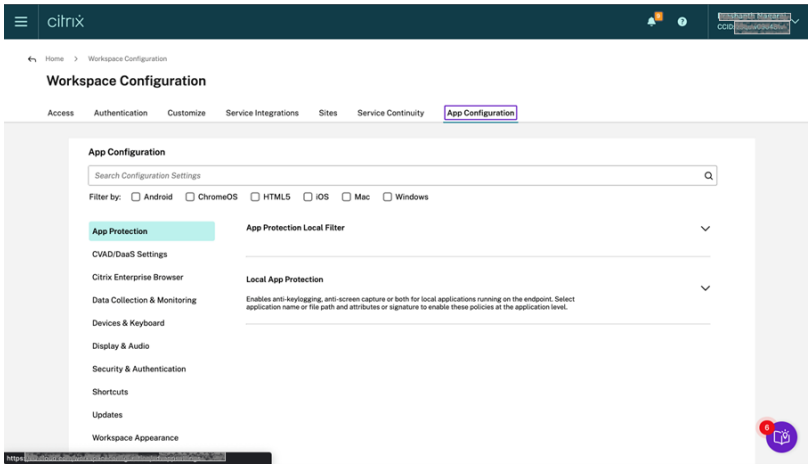
使用 **Global App configuration Service UI** 启用客户端应用程序管理

此方法仅适用于云应用商店，管理员可以使用 UI 部署代理（EPA/Secure Access、Zoom 插件或 WebEx 插件）。

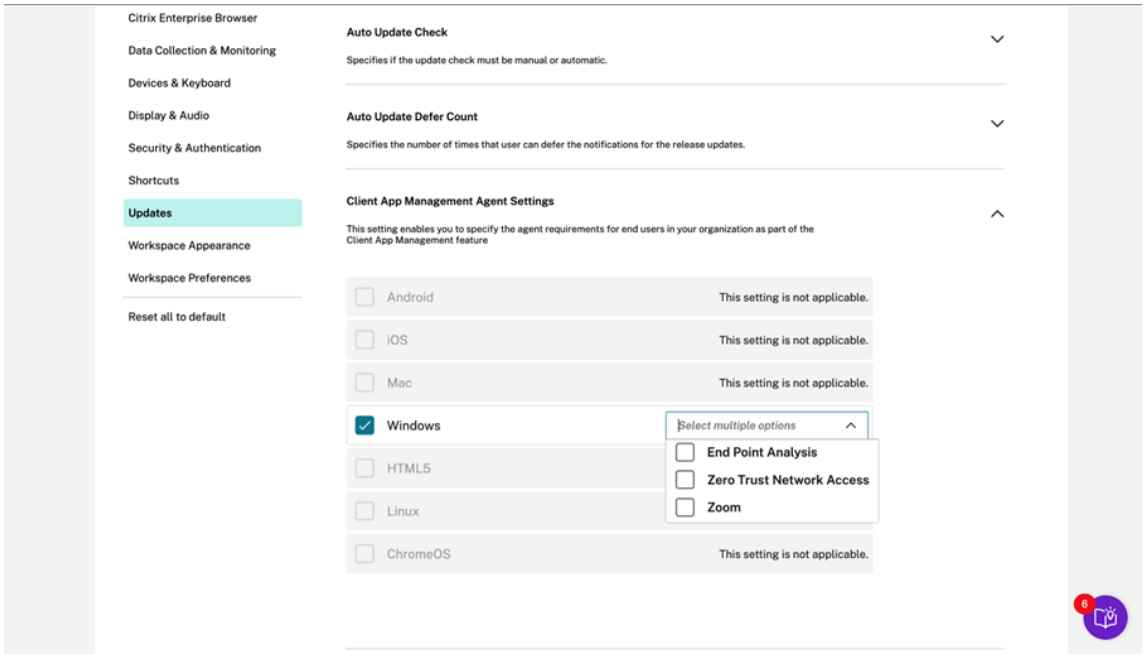
1. 登录 Citrix Cloud。
2. 在屏幕左上角的菜单中，选择 **Workspace** 配置。



此时将出现 **Workspace** 配置页面。



3. 单击应用程序配置选项卡。
4. 单击更新。
5. 确保选中 **Windows** 复选框。
6. 从 **Client App Management Agent Settings**（客户端应用程序管理代理设置）下拉列表中选择 **Windows** 旁边的所需代理。



使用 **Gobal App Configuration Service API** 启用客户端应用程序管理

1. 使用 API 配置设置并将其加载到 Global App Config Service。有关详细信息，请参阅映射服务 URL 和配置设置。
2. 需要为应用商店/帐户加载以下 Global App Configuration 设置才能加载 EPA 和 ZTNA/Secure Access Client：


```
{

  "serviceURL": {

    "url": "https://storefront.acme.com:443"
   }
 ,
  "settings": {

    "name": "Install and update plugins",
    "description": "Install and update plugins",
    "useForAppConfig": true,
    "appSettings": {

      "windows": [{

        "AutoUpdate": {

          "AutoUpdatePluginsSettings": [{

              "pluginId": "8A8AF6C0-11F6-4343-BA2D-A85A766170D4",
              "pluginName": "Citrix EPA Client",
              "pluginSettings": {

                "isFTU": true,
                "isBlocking": true,
                "delayGroup": "Fast",
                "deployment Mode": "InstallAndUpdate",
                "detectRule": "UpgradeCode:{
37A181F7-870E-4BDF-B0EA-E3B4766119FE }
",
                "maximumAllowedVersion": "22.10.1.9",
                "minimumAllowedVersion": "0.0.0.0",
                "stream": "Current",
                "upgradeToLatest": true
               }

             }
 ,
            {

              "pluginId": "9A8AF6C0-11F6-4343-BA2D-A85A766170D5",
              "pluginName": "Citrix Secure Access Client",
              "pluginSettings": {
```



```
                "isFTU": true,
                "isBlocking": false,
                "delayGroup": "Fast",
                "deploymentMode": "InstallAndUpdate",
                "detectRule": "UpgradeCode:{
F0ED53AB-11BE-4E9C-87E5-CD4A81DA2A4D }
",
                "maximumAllowedVersion": "22.10.1.9",
                "minimumAllowedVersion": "0.0.0.0",
                "stream": "Current",
                "upgradeToLatest": true
              }

            }

          ],
          "userOverride": false
        }

      }
]
    }

  }

}


<!--NeedCopy-->
```

下表列出了客户端应用程序管理设置架构、值和说明。

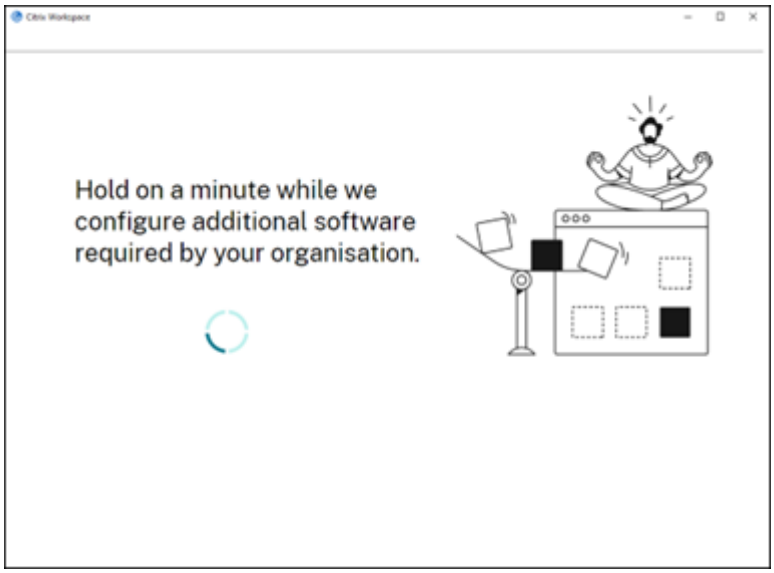
架构设置	值	说明
isBlocking	True 或 False	当 isBlocking 参数设置为 true 时，该插件被视为必需插件，并且登录页面仅在安装了所需的插件时出现。Citrix 建议您将 EPA 设置为必需插件。
pluginName		插件的友好名称。pluginName 可以修改。
pluginId		插件的 ID，不得修改。
delayGroup	快、中、慢
必须更新插件的自动更新时间间隔。|
deploymentMode	InstallAndUpdate/Update	InstallAndUpdate：插件可以全新安装，并且可以使用新版本进行更新。Update：只允许更新，不允许全新安装。

|None|| 此插件无需执行任何操作。|
|detectRule| 不得修改值。| 检查插件是否已安装。|
|maximumAllowedVersion| | 插件允许的最高版本。|
|minimumAllowedVersion| 插件允许的最低版本。|
|upgradeToLatest|True 或 False|
必须设置为 false 才能支持 maximumAllowedVersion 和 minimumAllowedVersion。True：更新期间考虑插件的最新版本。|
|Stream|Current| 必须设置为 “Current” 才能接收安装或自动更新插件 |

用户工作流程

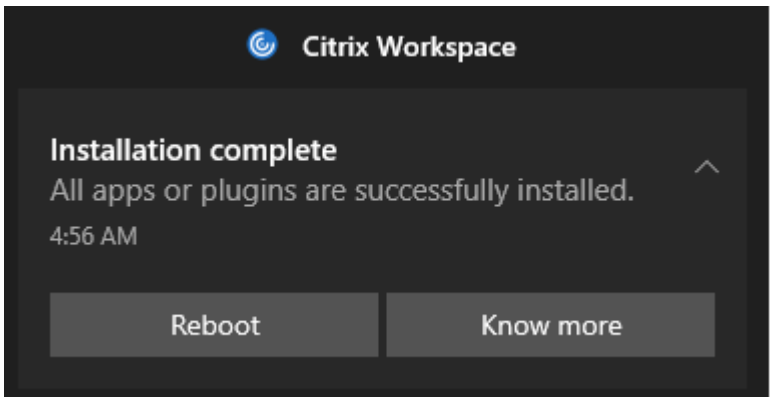
1. 下载并安装适用于 Windows 的 Citrix Workspace 应用程序版本 2212。
2. 在安装结束时单击添加帐户。
3. 添加载入了应用程序配置设置的应用商店/帐户。

   安装必需插件时出现以下消息：

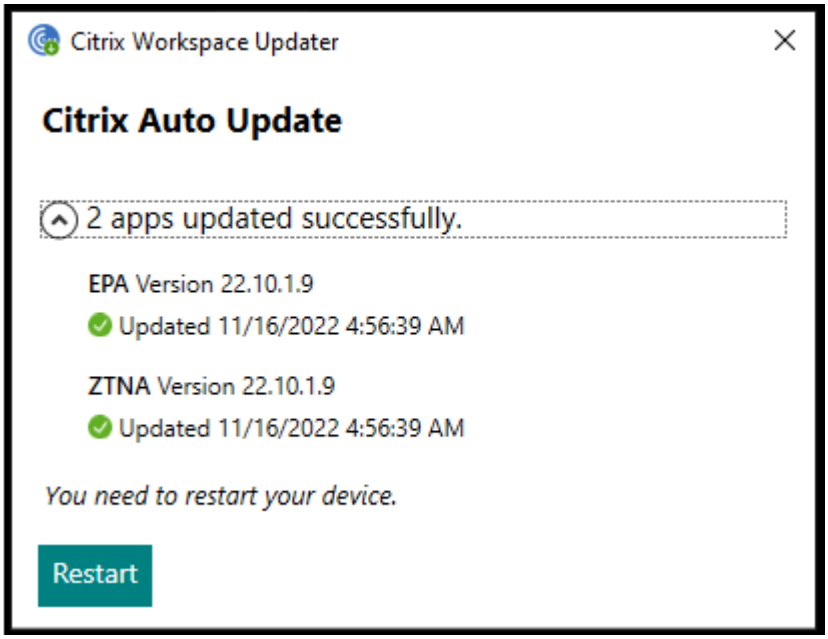


（安装暂停）

4. 安装完成后，将显示以下 Toast 通知：



5. 单击了解更多以了解已安装的插件。



Zoom 插件的客户端应用程序管理

还支持 Zoom 插件的下载、安装和自动更新，其处理方式与 EPA 和 ZTNA 插件相同。

> 注意：
>
> 此功能仅适用于 Workspace（云）会话。

应用商店/帐户需要启用以下 Global App Configuration 设置才能利用此功能：

```
{

  "serviceURL": {

    "url": "https://storefront.acme.com:443"

   }
 ,

  "settings": {

    "name": "Install and update plugins",

    "description": "Install and update plugins",
```



```
18
19      "useForAppConfig": true,
20
21      "appSettings": {
22
23
24        "windows": [{
25
26
27          "AutoUpdate": {
28
29
30            "AutoUpdatePluginsSettings": [{
31
32
33                    "pluginSettings": {
34
35
36                      "upgradeToLatest": true,
37
38                      "deployment Mode": "InstallAndUpdate",
39
40                      "stream": "Current",
41
42                      "isFTU": false,
43
44                      "isBlocking": false,
45
46                      "detectRule": "UpgradeCode:{
47  34225638-14F3-4059-BE34-175AC9B35435 }
48  ",
49
50                      "maximumAllowedVersion": "5.11.2872",
51
52                      "minimumAllowedVersion": "0.0.0",
53
54                      "delayGroup": "Fast"
55
56                     }
57  ,
58
59                    "pluginName": "Zoom VDI AutoUpgrade Plugin",
60
61                    "pluginId": "1A4BB471-022C-4C87-BDCD-0B64FB42869C"
62
```



```
                    }
                ],

              "userOverride": false

            }


          }
    ]

        }


      }

    }
```

WebEx 插件的客户端应用程序管理 [技术预览版]

自 2303 版本起，支持 WebEx 插件的下载、安装和自动更新，其处理方式与 Zoom 插件相同。应用商店/帐户需要启用以下 Global App Configuration 设置才能使用此功能：

```
{

  "pluginId": "C03BAE37-F3AC-4D63-8BC1-3C9CD2BC9E8D",
  "pluginName": "WebEx VDI AutoUpgrade Plugin",
  "pluginSettings":
  {

    "delayGroup": "Fast",
    "deploymentMode": "InstallAndUpdate",
    "detectRule": "UpgradeCode:{
 AA2AACDC-D30B-433F-A602-3E25975010A6 }
 ",
    "isBlocking": false,
    "isFTU": false,
    "maximumAllowedVersion": "3.1.0.24263",
    "minimumAllowedVersion": "0.0.0",
    "stream": "Current",
```



```
18      "upgradeToLatest": true
19     }
20
21   }
22
23
24 <!--NeedCopy-->
```

> 注意：
>
> 技术预览版可供客户在其非生产环境或有限生产环境中进行测试，并为客户提供共享反馈的机会。Citrix 不接受功能预览版的支持案例，但欢迎提供改进这些功能的反馈。Citrix 可能会根据反馈的严重性、紧迫性和重要性对反馈执行操作。建议不要在生产环境中部署 Beta 版本。

可以通过 Podio 表单提供有关此功能的反馈。

身份验证

March 29, 2023

Citrix Workspace 应用程序，包括域直通身份验证（单点登录或 SSON）、智能卡以及 Kerberos 直通身份验证，可以配置各种不同类型的身份验证。

域直通（单点登录）身份验证

域直通（单点登录或 SSON）允许您向域进行身份验证，并且无需重新进行身份验证即可使用 Citrix Virtual Apps and Desktops 和 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）。

> 注意：
>
> 如果您在组策略对象模板中禁用了 **Enable MPR notifications for the System**（为系统启用 MPR 通知）策略，则 Windows 11 不支持域直通（单点登录）身份验证功能。

启用后，域直通（单点登录）会缓存您的凭据，这样您就可以连接到其他 Citrix 应用程序，而不必每次都登录。请确保您的设备上仅运行符合公司政策的软件，以降低凭据泄露的风险。

当您登录 Citrix Workspace 应用程序时，您的凭据将随应用程序和桌面以及“开始”菜单设置一起传递到 StoreFront。配置单点登录后，您可以登录 Citrix Workspace 应用程序并启动虚拟应用程序和桌面会话，而不需要重新键入您的凭据。

所有 Web 浏览器都要求您使用组策略对象 (GPO) 管理模板来配置单点登录。有关使用组策略对象 (GPO) 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 Single Sign-On：

- 命令行接口
- GUI

> 注意：
>
> 在本文档中，术语域直通、单点登录和 SSON 可以互换使用。

在全新安装过程中配置 **Single Sign-On**

要在全新安装过程中配置单点登录，请执行以下步骤：

1. StoreFront 上的配置。
2. 在 Delivery Controller 上配置 XML 信任服务。
3. 修改 Internet Explorer 设置。
4. 安装具有 Single Sign-On 的 Citrix Workspace 应用程序。

在 **StoreFront** 上配置单点登录

单点登录允许您对域进行身份验证，并使用来自相同域的 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 Single Sign-On 后，可以添加应用商店、枚举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。

根据 Citrix Virtual Apps and Desktops 部署，可以使用管理控制台在 StoreFront 上配置单点登录身份验证。

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
StoreFront 上已配置的 SSON	启动 Citrix Studio，然后转至应用商店 > 管理身份验证方法 **-** 应用商店 > 启用域直通。	当没有为 Citrix Workspace 应用程序配置单点登录时，它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 **-** 应用商店 > 启用域直通。	当没有为 Citrix Workspace 应用程序配置单点登录时，它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）。

通过 **Citrix Gateway** 配置 **Single Sign-On**

使用组策略对象管理模板对 Citrix Gateway 启用 Single Sign-On。

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，然后选择通过 **Citrix Gateway** 实现 **Single Sign-On** 策略。
3. 选择已启用。
4. 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。

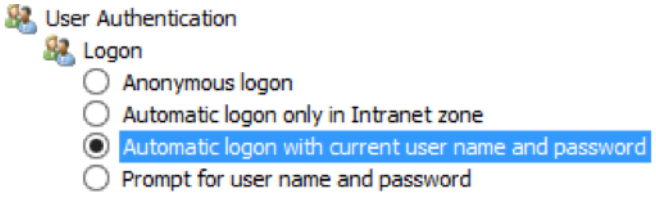
在 **Delivery Controller** 上配置 **XML** 信任服务

在 Citrix Virtual Apps and Desktops 和 Citrix DaaS 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。要添加：
   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 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。要修改：
   a) 从控制面板启动 **Internet** 选项。
   b) 单击安全选项卡 > 本地 **Intranet**。
   c) 单击自定义级别。此时将显示安全设置 — 本地 **Intranet** 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。



   e) 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 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：
>
> 安装适用于 Windows 的 Citrix Workspace 应用程序但未安装 Single Sign-On 组件时，不支持使用 / includeSSON 开关升级到 Citrix Workspace 应用程序的最新版本。

使用 **GUI** 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。

您现在不需要输入用户凭据即可使用 Citrix Workspace 应用程序登录到现有应用商店（或配置一个新应用商店）。

在适用于 **Web** 的 **Workspace** 中配置 **Single Sign-On**

可以使用组策略对象管理模板在适用于 Web 的 Workspace 上配置 Single Sign-On。

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. 选择本地用户名和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 Single Sign-on，并检查 ssonsvr.exe 进程是否正在运行。

使用 **Active Directory** 配置 **Single Sign-On**

请完成以下步骤以使用 Active Directory 组策略为 Citrix Workspace 应用程序配置直通身份验证。在这种情况下，可以实现 Single Sign-On 身份验证，而无需使用企业软件部署工具，例如 Microsoft System Center Configuration Manager。

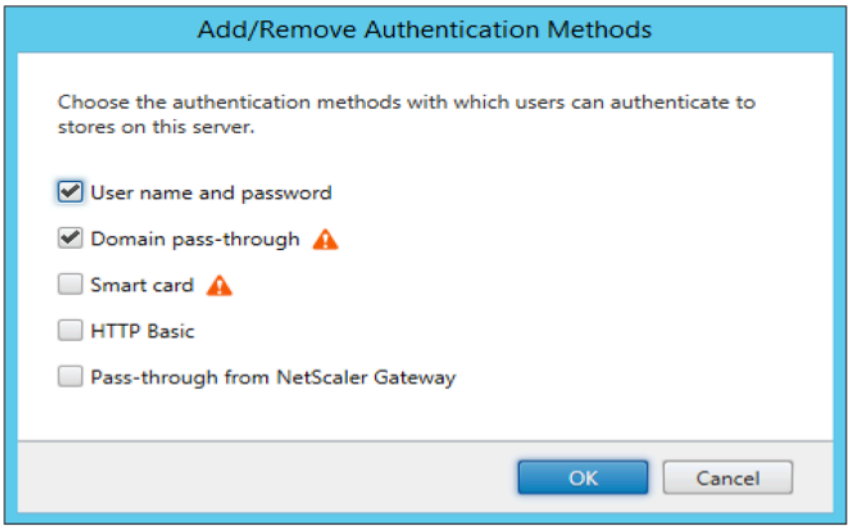
1. 下载 Citrix Workspace 应用程序安装文件 (CitrixWorkspaceApp.exe) 并将其放在合适的网络共享上。在其上安装了 Citrix Workspace 应用程序的目标计算机必须能够访问该安装文件。
2. 从适用于 Windows 的 Citrix Workspace 应用程序下载页面获取 CheckAndDeployWorkspacePerMachineStartu .bat 模板。
3. 编辑内容以反映 CitrixWorkspaceApp.exe 的位置和版本。
4. 在 **Active Directory** 组策略管理控制台中，键入 CheckAndDeployWorkspacePerMachineStartupScript .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 `receiver.adml` 文件。
6. 添加 `receiver.adml` 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。有关添加模板文件的详细信息，请参阅组策略对象管理模板。
7. 选择本地用户名和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** 上配置单点登录

StoreFront 配置

1. 在 StoreFront 服务器上启动 **Citrix Studio**，然后选择应用商店 > 管理身份验证方法 **-** 应用商店。
2. 选择域直通。



身份验证令牌

身份验证令牌会加密并存储在本地磁盘上，这样您就不需要在系统或会话重新启动时重新输入凭据。Citrix Workspace 应用程序提供了用于禁止在本地磁盘上存储身份验证令牌的选项。

为了增强安全性，我们现在提供了组策略对象 (GPO) 策略来配置身份验证令牌存储。

> 注意：
>
> 此配置仅在云部署中适用。

要使用组策略对象 **(GPO)** 策略禁用存储身份验证令牌，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** 组件 > 自助服务。

3. 在存储身份验证令牌策略中，选择以下选项之一：
   - 已启用：指示身份验证令牌存储在磁盘上。默认情况下，设置为“已启用”。
   - 已禁用：指示身份验证令牌未存储在磁盘上。系统或会话重新启动时，请重新输入您的凭据。
4. 单击应用和确定。

自版本 2106 起，Citrix Workspace 应用程序提供用于禁止在本地磁盘上存储身份验证令牌的其他选项。除了现有 GPO 配置外，还可以使用 Global App Configuration Service 禁止在本地磁盘上存储身份验证令牌。

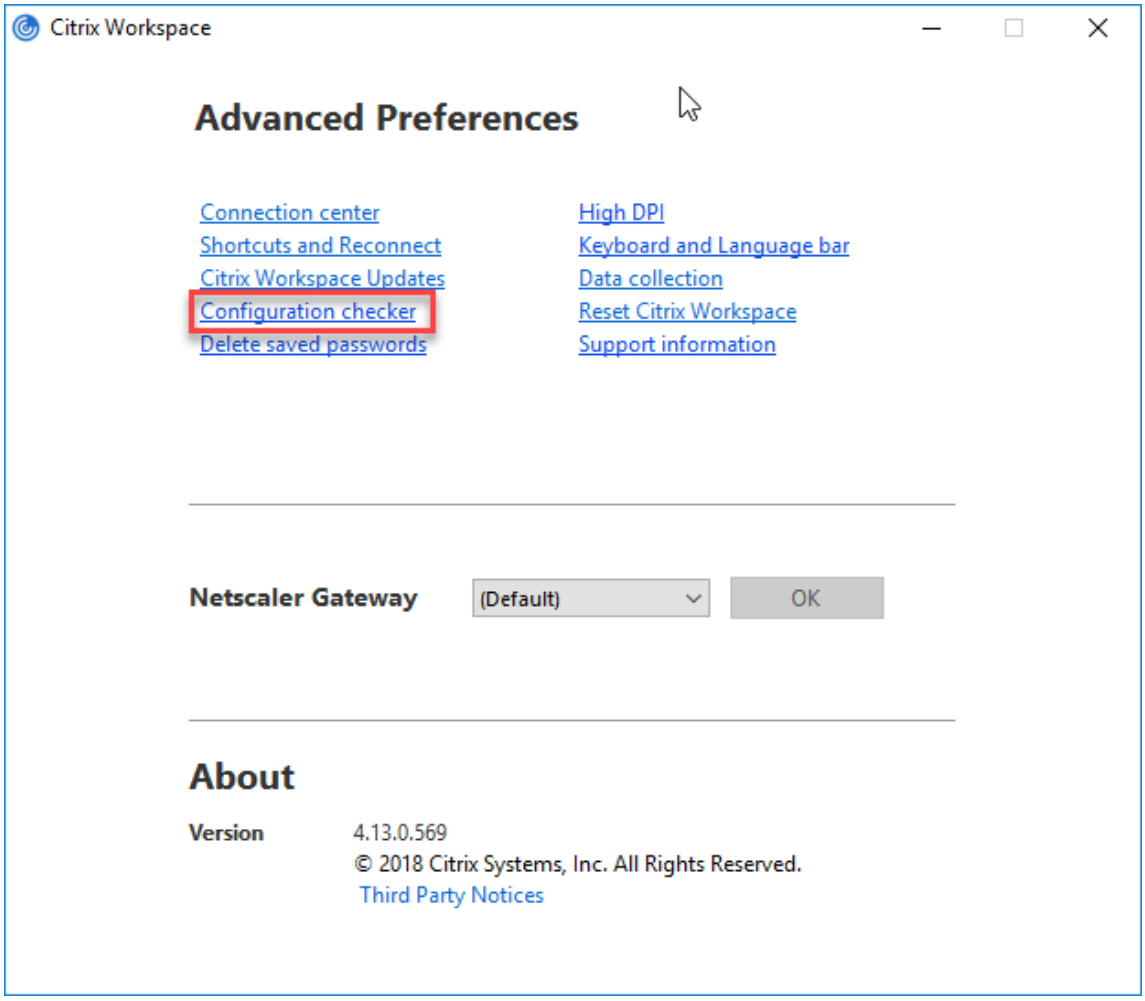
在 Global App Configuration Service 中，将 `Store Authentication Tokens` 属性设置为 `False`。

有关详细信息，请参阅 Global App Configuration Service 文档。

配置检查器

可以使用配置检查器运行测试，检查 Single Sign-On 是否正确配置。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 Single Sign-On。
3. 套件：指示测试的类别。例如，安装。
4. 测试：指示运行的具体测试的名称。
5. 详细信息：提供有关测试的其他信息，包括通过和未通过。

用户获得有关每个检查点和相应结果的详细信息。

完成了以下测试：

1. 已随 Single Sign-On 安装。
2. 登录凭据捕获。
3. 网络提供程序注册：只有将 “Citrix Single Sign-On” 设置为网络提供程序列表中的第一个时，针对网络提供程序注册的测试结果才会显示一个绿色复选标记。如果 Citrix Single Sign-On 显示在列表中的任何其他位置，则针对网络提供程序注册的测试结果会显示一个蓝色的 “I”，并包含其他信息。
4. Single Sign-On 进程正在运行。
5. 组策略：默认情况下，此策略配置在客户端上。
6. Internet 的安全区域设置：请务必将 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. StoreFront 的身份验证方法。

> 注意：
>
> - 如果要访问适用于 Web 的 Workspace，则测试结果不适用。
> - 如果 Citrix Workspace 应用程序配置有多个应用商店，则会在所有已配置的应用商店上运行身份验证方法测试。
> - 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 GPO 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 Citrix Virtual Apps and Desktops 服务器上 “信任发送到 XML Service 的请求” 配置的检查点。

信标测试

Citrix Workspace 应用程序允许您使用信标检查器（作为配置检查器实用程序的一部分提供）执行信标测试。信标测试可帮助确认信标 (ping.citrix.com) 是否可访问。此诊断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）选项并单击运行。

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 应用程序可以间歇性地联系信标。

> 注意：
>
> - 在适用于 Web 的 Workspace 中，这些测试结果不适用。
> - 测试结果可以保存为报告。报告的默认格式为.txt。

通过 **Kerberos** 进行域直通（单点登录）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（单点登录或 SSON）身份验证。Kerberos 是集成 **Windows** 身份验证 **(IWA)** 中包含的一种身份验证方法。

启用后，无需 Citrix Workspace 应用程序的密码即可进行 Kerberos 身份验证。因此，请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，例如指纹读取器等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 Single Sign-On 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 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（之前称为 ICA 客户端）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，请检查您的 Kerberos 配置是否符合以下条件。

- 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。请信任服务器进行委派，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。请确保在编辑注册表之前进行备份。

通过 **Kerberos** 实现的域直通（单点登录）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 文档中的保护部署部分。

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

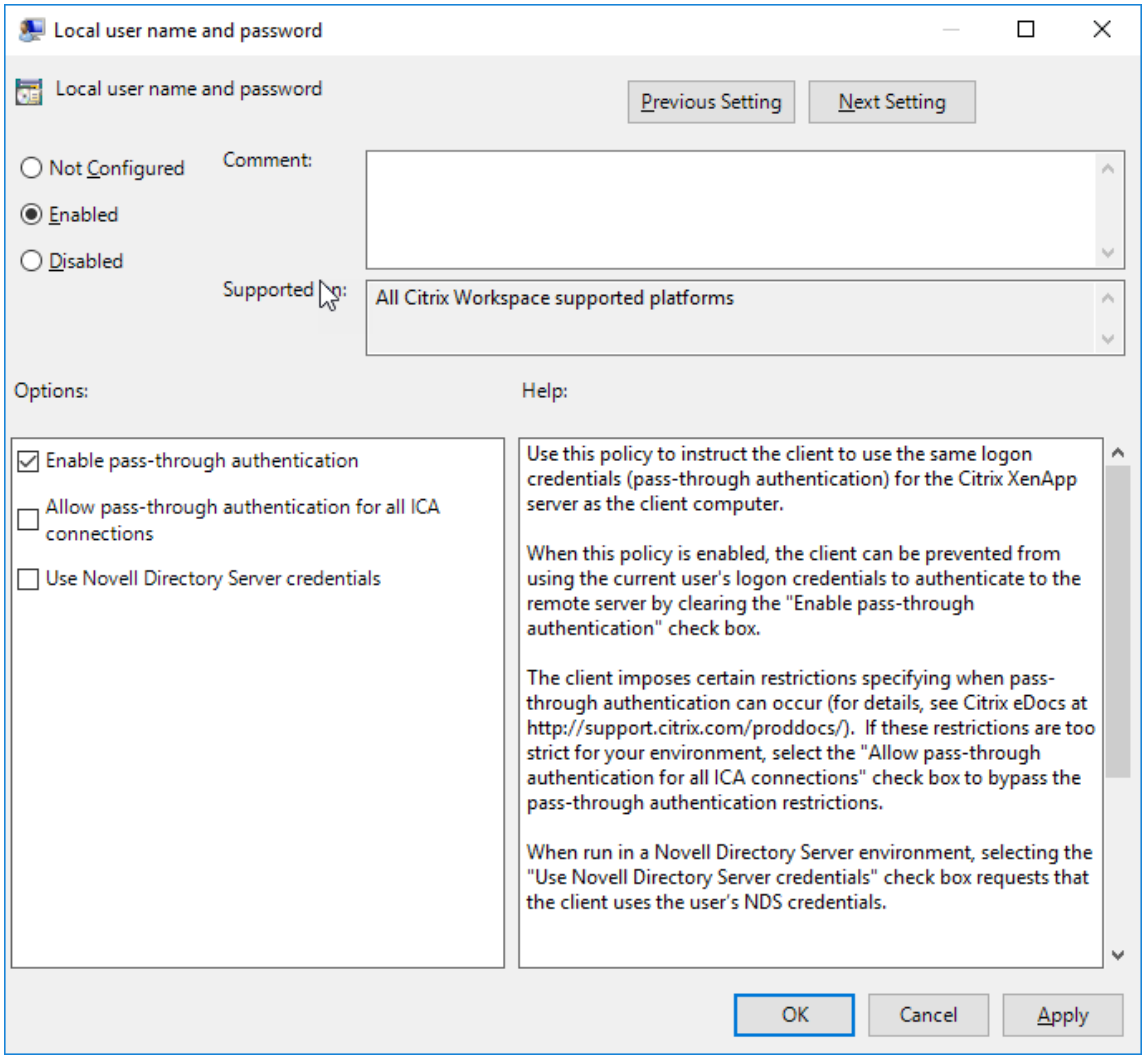
- /includeSSON

  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 获取此 PIN 码。

  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。

支持 **Azure Active Directory** 中的条件访问

条件访问是 Azure Active Directory 强制执行组织策略所用的工具。Workspace 管理员可以为向 Citrix Workspace 应用程序进行身份验证的用户配置并强制执行 Azure Active Directory 条件访问策略。运行 Workspace 应用程序的 Windows 计算机必须已安装 Microsoft Edge WebView2 Runtime 99 或更高版本。

有关使用 Azure Active Directory 配置条件访问策略的完整详细信息和说明，请参阅 **Azure AD** 条件访问文档，地址为 *Docs.microsoft.com/zh-cn/azure/active-directory/conditional-access/*。

> 注意：
>
> 此功能仅在 Workspace (Cloud) 部署中受支持。

支持 **StoreFront** 应用商店的新式身份验证方法

适用于 Windows 的 Citrix Workspace 应用程序 2303 支持 StoreFront 应用商店的新式验证。可以使用下面的任何一种方式向 Citrix StoreFront 应用商店进行身份验证：

- 使用 Windows Hello 和 FIDO2 安全密钥。有关详细信息，请参阅其他身份验证方式。
- 从 Azure Active Directory (AAD) 作为身份提供程序的已加入 AAD 的计算机单点登录到 Citrix StoreFront 应用商店。有关详细信息，请参阅其他身份验证方式。
- Workspace 管理员可以为对 Citrix StoreFront 应用商店进行身份验证的用户配置和强制执行 Azure Active Directory 条件访问策略。有关详细信息，请参阅支持 Azure AD 中的条件访问。

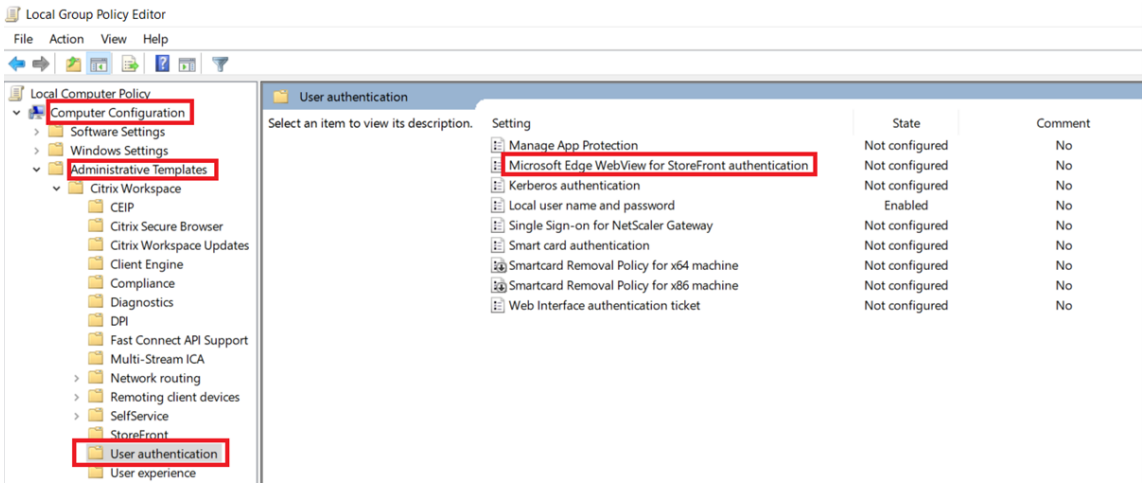
必须使用 Microsoft Edge WebView2 作为底层浏览器进行直接 StoreFront 和网关身份验证，才能启用此功能。

> 注意：
>
> 请确保 Microsoft Edge WebView2 Runtime 版本为 102 或更高版本。

可以使用 GPO 模板为 StoreFront 应用商店启用新式验证方法。

启用该功能：

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** > 用户身份验证。
3. 单击 **Microsoft Edge WebView for StoreFront authentication**（适用于 StoreFront 的 Microsoft Edge WebView 身份验证）策略并将其设置为 **Enabled**（已启用）。



4. 单击应用，然后单击确定。

禁用此策略后，Citrix Workspace 应用程序使用 Internet Explorer WebView。因此，不支持 Citrix StoreFront 应用商店的新式验证方法。

其他身份验证方式

您可以使用 Citrix Workspace 应用程序配置以下身份验证机制。为使以下身份验证机制正常发挥作用，运行 Workspace 应用程序的 Windows 计算机必须安装了 Microsoft Edge WebView2 Runtime 99 或更高版本。

1. 基于 Windows Hello 的身份验证 – 有关配置基于 Windows Hello 的身份验证的说明，请参阅配置 **Windows Hello** 企业版策略设置 **-** 证书信任，地址为 Docs.microsoft.com/zh-cn/windows/security/identity-protection/hello-for-business/hello-cert-trust-policy-settings。

   > 注意：
   >
   > 不支持使用域直通（单点登录或 SSON）的基于 Windows Hello 的身份验证。

2. 基于 FIDO2 安全密钥的身份验证 – FIDO2 安全密钥为企业员工提供了一种无需输入用户名或密码即可无缝进行身份验证的方式。您可以配置向 Citrix Workspace 进行基于 FIDO2 安全密钥的身份验证。如果希望用户使用 FIDO2 安全密钥通过其 Azure AD 帐户向 Citrix Workspace 进行身份验证，请参阅启用无密码安全密钥登录，地址为 *Docs.microsoft.com/zh-cn/azure/active-directory/authentication/howto-authentication-passwordless-security-key*。

3. 此外，您还可以从加入了 Microsoft Azure Active Directory (AAD) 且 AAD 为身份提供程序的计算机单点登录 (SSO) 到 Citrix Workspace 应用程序。有关配置 Azure Active Directory 域服务的更多详细信息，请参阅配置 **Azure Active Directory** 域服务，网址为 *Docs.microsoft.com/en-us/azure/active-directory-domain-services/overview*。有关如何将 Azure Active Directory 连接到 Citrix Cloud 的信息，请参阅将 Azure Active Directory 连接到 Citrix Cloud。

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，用户必须再次键入凭据才可启动虚拟桌面或应用程序。

  直通身份验证需要使用 StoreFront 和 Citrix 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。如果您将智能卡插入读卡器，则这些证书适用于在用户设备上运行的所有应用程序，包括 Citrix Workspace 应用程序。

- 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 仅在用户会话期间缓存在非分页内存中，不会存储在磁盘中。
- 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。要将 VPN 与智能卡身份验证结合使用，请安装 Citrix Gateway 插件。使用智能卡和 PIN 登录 Web 页面，在每一步操作中进行身份验证。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 应用程序更新程序与 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。请确保在编辑注册表之前进行备份。

要为智能卡身份验证启用 **Single Sign-On**，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`

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

- 在注册表编辑器中，导航到以下路径并将 `SSONCheckEnabled` 字符串设置为 `False`（如果您尚未安装单点登录组件）。

  ```
  HKEY_CURRENT_USER\Software{ Wow6432 } \Citrix\AuthManager\protocols\
  integratedwindows\
  ```

  ```
  HKEY_LOCAL_MACHINE\Software{ Wow6432 } \Citrix\AuthManager\protocols\
  integratedwindows\
  ```

  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，并允许 Citrix Workspace 应用程序向 StoreFront 进行身份验证。

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。
- 如果用户使用其他身份验证方法（例如用户名和密码）登录端点，则命令行为：

  ```
  /includeSSON LOGON_CREDENTIAL_CAPTURE_ENABLE=No
  ```

此类型的身份验证可防止在登录时捕获凭据，并允许 Citrix Workspace 应用程序在 Citrix Workspace 应用程序登录期间存储 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。可以改为将 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。
- 密钥用法必须包括数字签名。
- 使用者备用名称必须包括用户主体名称 (UPN)。
- 增强型密钥用法必须包括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 握手时发送的允许使用的可分辨名称 (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。

- 将以下项值添加到注册表项 HKEY_CURRENT_USER OR HKEY_LOCAL_MACHINE\Software\[Wow6432Node\Citrix\AuthManager：CertificateSelectionMode={ Prompt | SmartCardDefault | LatestExpiry }。

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

删除智能卡时，Citrix Virtual Apps 会话将注销。如果在 Citrix Workspace 应用程序中已将智能卡配置为身份验证方法，请在适用于 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。而用户在 Citrix Workspace 应用程序会话中仍然保持登录状态。

限制：

使用智能卡身份验证登录 Citrix Workspace 应用程序站点时，用户名显示为已登录。

快速智能卡

快速智能卡是对现有基于 HDX PC/SC 的智能卡重定向的改进。在高延迟 WAN 环境中使用智能卡时，可以提高性能。

仅 Linux VDA 支持快速智能卡。

要在 **Citrix Workspace** 应用程序中启用快速智能卡登录，请执行以下操作：

默认情况下，快速智能卡登录在 VDA 上处于启用状态，在 Citrix Workspace 应用程序中处于禁用状态。要启用快速智能卡登录，请在关联的 StoreFront 站点的 **default**.ica 文件中包含以下参数：

```
1 copy[WFClient]
2 SmartCardCryptographicRedirection=On
3 <!--NeedCopy-->
```

要在 **Citrix Workspace** 应用程序中禁用快速智能卡登录，请执行以下操作：

要在 Citrix Workspace 应用程序中禁用快速智能卡登录，请从关联的 StoreFront 站点的 **default**.ica 文件中删除 SmartCardCryptographicRedirection 参数。

有关详细信息，请参阅智能卡。

面向 **Citrix Workspace** 的无提示身份验证

Citrix Workspace 应用程序引入了组策略对象 (GPO) 策略以启用面向 Citrix Workspace 的无提示身份验证。此策略使 Citrix Workspace 应用程序能够在系统启动时自动登录 Citrix Workspace。仅当为加入了域的设备上的 Citrix Workspace 配置了域直通（单点登录或 SSON）时，才使用此策略。

要使此策略起作用，必须满足以下条件：

- 必须启用单点登录。
- 必须在注册表编辑器中将 `SelfServiceMode` 密钥设置为 `Off`。

启用无提示身份验证：

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。
3. 单击面向 **Citrix Workspace** 的无提示身份验证策略并将其设置为已启用。
4. 单击应用和确定。

阻止适用于 **Windows** 的 **Citrix Workspace** 应用程序缓存密码和用户名

默认情况下，适用于 Windows 的 Citrix Workspace 应用程序会自动填充上次输入的用户名。要清除用户名字段的自动填充，请编辑用户设备上的注册表：

1. 创建 REG_SZ 值 HKLM\SOFTWARE\Citrix\AuthManager\RememberUsername。
2. 将其值设置为 “false”。

要禁用 **Remember my password**（记住我的密码）复选框并阻止自动登录，请在安装了适用于 Windows 的 Citrix Workspace 应用程序的客户端计算机上创建以下注册表项：

- 路径：HKLM\Software\wow6432node\Citrix\AuthManager
- 类型：REG_SZ
- 名称：SavePasswordMode
- 值：从不

> 注意：
>
> 注册表编辑器使用不当可能导致严重问题，可能需要重新安装操作系统。Citrix 无法保证因注册表编辑器使用不当导致出现的问题能够得以解决。使用注册表编辑器需自担风险。请确保在编辑注册表之前进行备份。

要防止缓存 StoreFront 应用商店的凭据，请参阅 StoreFront 文档中的阻止适用于 Windows 的 Citrix Workspace 应用程序缓存密码和用户名。

域直通访问列表

February 16, 2023

如果您使用的是 Citrix Workspace 并希望实现域直通，子部分中的表格介绍了不同的方案以及是否可以为每种方案实现域直通。

表格中的不同标题元素以及有关标题元素的附加信息如下所示：

- 端点已加入到：表示端点所加入的目录。该目录提供对本地资源的访问控制。这可以是本地 Active Directory (AD)、Azure Active Directory (AAD) 或混合。
- 身份提供程序 (IdP)：用于向 Citrix Workspace 提供身份验证服务的实体。它允许您连接到资源。
- 联合身份验证服务 (FAS)：有关详细信息，请参阅使用 Citrix 联合身份验证服务对工作区启用单点登录。
- Virtual Delivery Agent (VDA)：有关详细信息，请参阅安装 VDA。
- VDA 已加入到：表示 VDA 设备加入到的目录。有关详细信息，请参阅身份识别和访问管理。
- Citrix Workspace/VDA 的单点登录 (SSO)：“是” 或 “否” 值表示是否支持域直通到 Citrix Workspace 或 VDA。
- Citrix Workspace 应用程序：要实现单点登录，请参阅在全新安装过程中在域直通身份验证中配置单点登录。

> 注意：
>
> 对于下面某些情况，您可能需要最新版本的 Citrix Workspace 应用程序才能获得域直通支持。

Citrix Workspace 的域直通支持

端点已加入到	IdP	VDA 已加入到	单点登录到 Citrix Workspace	单点登录到 VDA	文档
AD	本地 Citrix Gateway	AD	是	Citrix Workspace 应用程序/FAS	使用本地 Citrix Gateway 作为身份提供程序域直通到 Citrix Workspace。

端点已加入到	IdP	VDA 已加入到	单点登录到 Citrix Workspace	单点登录到 VDA	文档
AD	自适应身份验证	AD	是	Citrix Workspace 应用程序/FAS	要配置自适应身份验证，请参阅自适应身份验证服务，并按照使用本地 Citrix Gateway 作为身份提供程序域直通到 Citrix Workspace 中的说明进行操作。
AD	Citrix Gateway 与另一个 IdP 联合 (AAD/Okta)	AD	是	Citrix Workspace 应用程序/FAS	使用配置 SAML 单点登录配置 IdP，并参阅用于配置域直通的 IdP 的文档。
AD	Okta	AD	是	Citrix Workspace 应用程序/FAS	使用 Okta 作为身份提供程序域直通到 Citrix Workspace。
已加入 AD/混合	AAD（使用 AAD Connect 的 AD）	AD	是	Citrix Workspace 应用程序/FAS **	使用 Azure Active Directory 作为身份提供程序域直通到 Citrix Workspace。
AD	任何基于 SAML 的 IdP（不包括 ADFS）	AD	是	Citrix Workspace 应用程序/FAS	请参阅将 SAML 作为身份提供程序连接到 Citrix Cloud，并参阅用于配置域直通的 IdP 的文档。
AD	AD	AD	否	不支持	不适用

端点已加入到	IdP	VDA 已加入到	单点登录到 Citrix Workspace	单点登录到 VDA	文档
AD	AD+OTP	AD	否	不支持	不适用
AD	AAD	AAD	否	不支持	不适用
AAD	无本地 AD 的 AAD	AD	是	FAS	Citrix Workspace 使用 Microsoft Edge WebView，它允许单点登录到 Workspace。通过 FAS 支持单点登录到 VDA。有关详细信息，请参阅使用 Citrix 联合身份验证服务对工作区启用单点登录。
AAD	AAD	AAD	是	用户必须输入凭据。	Citrix Workspace 使用 Microsoft Edge WebView，它允许单点登录到 Workspace。不支持单点登录到 VDA。

端点已加入到	IdP	VDA 已加入到	单点登录到 Citrix Workspace	单点登录到 VDA	文档
未加入域	支持无密码身份验证的 IdP - 链接	AD	否	FAS	Citrix Workspace 使用 Microsoft Edge WebView，它允许单点登录到 Workspace。通过 FAS 支持单点登录到 VDA。有关详细信息，请参阅对 Citrix Workspace 进行身份验证的其他方法。

备注：

- AD 必须能够访问客户端，Kerberos 才能正常运行。
- **Citrix Single Sign-on (SSONSVR.exe) 只能与客户端上的用户名或密码结合使用。如果用户使用 Windows Hello 登录，则需要 FAS。
- 如果启用了 LLT 或者配置了最终用户接受策略，则云中的身份验证可能不会完全无提示。
- 建议配置 FAS，因为它适用于非 Windows 平台。

StoreFront 支持域直通

端点已加入到	IdP	VDA 已加入到	单点登录到 Citrix Workspace	单点登录到 VDA	文档
AD	StoreFront	AD	是	Citrix Workspace 应用程序	域直通身份验证

端点已加入到	IdP	VDA 已加入到	单点登录到 Citrix Workspace	单点登录到 VDA	文档
已加入 AD/混合/Windows Hello 企业版	StoreFront	AD	是 (1)	Citrix Workspace 应用程序 /FAS(2)	域直通身份验证和使用 Citrix 联合身份验证服务对工作区启用单点登录。
AD	Citrix Gateway - 高级身份验证	AD	是	Citrix Workspace 应用程序 (3)	
AD	Citrix Gateway - 基本身份验证	AD	是	Citrix Workspace 应用程序 (4)	域直通身份验证。

> 备注：
>
> 1. 在注册表编辑器中，导航到以下路径并将 `SSONCheckEnabled` 字符串设置为 `False`（如果您尚未安装单点登录组件）。
>
>   `HKEY_LOCAL_MACHINE\Software{ Wow6432 } \Citrix\AuthManager\protocols\integratedwindows\`
>
>   The key prevents the Citrix Workspace app authentication manager from checking for the single sign-on component and allows Citrix Workspace app to authenticate to StoreFront.
>
> 2. 如果您使用 Windows Hello 登录，则需要 FAS 和注册表配置才能启用 SSO。
> 3. 要求 AD 能够访问客户端，因为它使用 Kerberos。
> 4. 即使 AD 无法访问客户端，也能正常运行。未使用 Kerberos。

使用本地 **Citrix Gateway** 作为身份提供程序域直通到 **Citrix Workspace**

January 17, 2023

> 重要：
>
> 本文有助于配置域直通身份验证。如果您已将本地网关设置为 IdP，请跳到在 Citrix Gateway 中将域直通配置为身份验证方法部分。

Citrix Cloud 支持使用本地 Citrix Gateway 作为身份提供程序对登录到其工作区的订阅者进行身份验证。

通过使用 Citrix Gateway 身份验证，您可以：

- 继续通过现有 Citrix Gateway 对用户进行身份验证，以便其能够通过 Citrix Workspace 访问本地 Virtual Apps and Desktops 部署中的资源。
- 将 Citrix Gateway 身份验证、授权和审核功能与 Citrix Workspace 结合使用。
- 使用直通身份验证、智能卡、安全令牌、条件访问策略、联合身份验证等功能，为您的用户提供通过 Citrix Workspace 访问所需资源的权限。

支持 Citrix Gateway 身份验证与以下产品版本结合使用：

- Citrix Gateway 13.1.4.43 Advanced Edition 或更高版本

必备条件：

- Cloud Connector - 至少需要两台服务器来安装 Citrix Cloud Connector 软件。
- Active Directory，并确保域已注册。
- Citrix Gateway 要求
  - 由于已弃用经典策略，请在本地网关上使用高级策略。
  - 配置网关以对 Citrix Workspace 的订阅者进行身份验证时，网关将充当 OpenID Connect 提供商。Citrix Cloud 与网关之间的消息符合 OIDC 协议，该协议涉及对令牌进行数字签名。因此，您必须配置证书以对这些令牌进行签名。
  - 时钟同步 - 必须将 Citrix Gateway 同步到 NTP 时间。

有关详细信息，请参阅 Citrix Cloud 文档中的 Prerequisites（必备条件）。

在创建 OAuth IdP 策略之前，您需要先设置 Citrix Workspace 或 Citrix Cloud，以便在 IdP 中使用网关作为身份验证选项。有关如何设置的详细信息，请参阅 Connect an on-premises Citrix Gateway to Citrix Cloud（将本地 Citrix 网关连接到 Citrix Cloud）。完成设置后，将生成创建 OAuth IdP 策略所需的客户端 ID、密钥和重定向 URL。

如果您使用的是 Internet Explorer、Microsoft Edge、Mozilla Firefox 和 Google Chrome，则会启用适用于 Web 的 Workspace 的域直通。仅当成功检测到客户端时，才会启用域直通。

> 注意：
>
> 如果用户首选 HTML5 客户端或者管理员强制使用该客户端，则不会启用域直通身份验证方法。

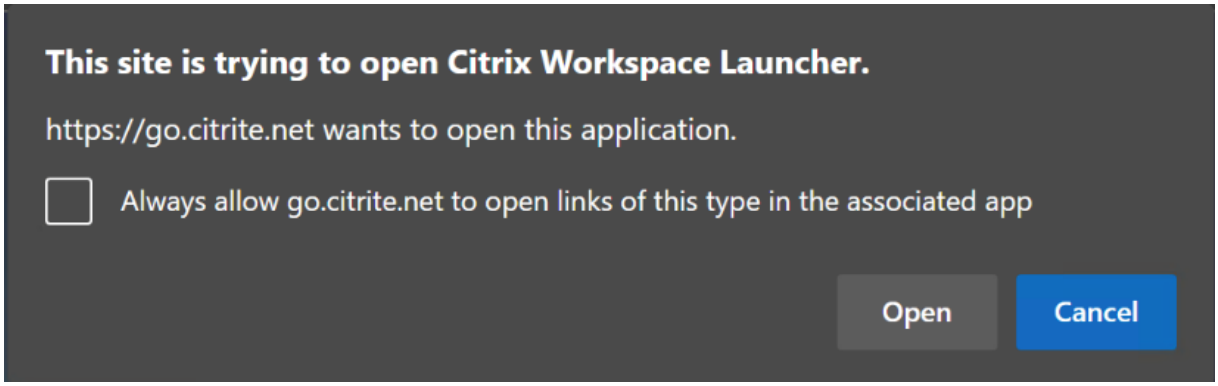
在浏览器中启动 StoreFront URL 时，将显示检测 **Receiver** 提示。

如果设备处于托管状态，请将组策略配置为禁用此提示，而非禁用客户端检测。有关详细信息，请参阅：

- Microsoft 文档中的 URLAllowlist。
- Google Chrome 文档中的 URLAllowlist。

> 注意：
>
> Workspace 应用程序使用的协议处理程序为 **receiver:**。请将其配置为允许使用的其中一个 URL。

用户还可以选中该复选框，如以下示例提示所示，以便在客户端检测提示中输入 StoreFront URL。选中此复选框还可以避免提示后续启动。



以下步骤说明了如何将 Citrix Gateway 设置为 IdP。

在本地 **Citrix Gateway** 上创建 **OAuth IdP** 策略

创建 OAuth IdP 身份验证策略涉及以下任务：

1. 创建 OAuth IdP 配置文件。
2. 添加 OAuth IdP 策略。
3. 将 OAuth IdP 策略绑定到虚拟服务器。
4. 全局绑定证书。

创建 **OAuth IdP** 配置文件

1. 要使用 CLI 创建 OAuth IdP 配置文件，请在命令提示符下键入以下命令：

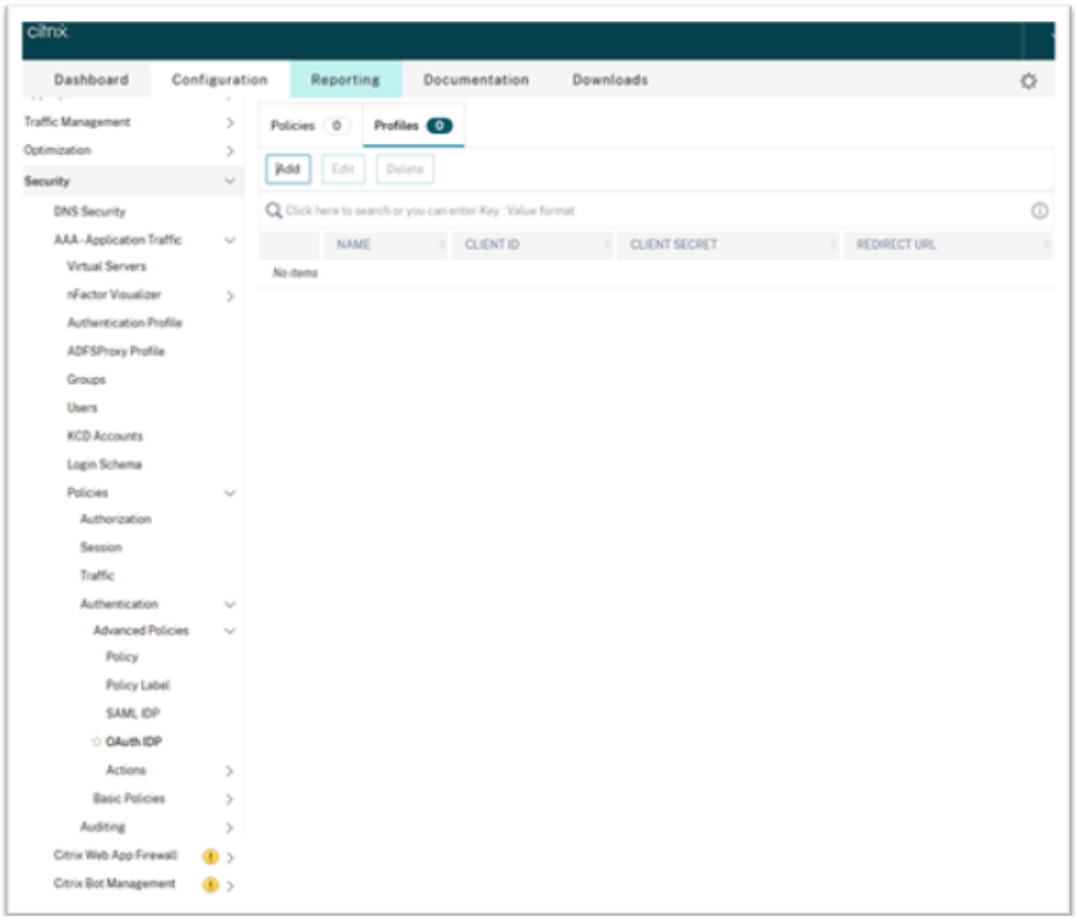
```
add authentication OAuthIdPProfile <name> [-clientID <string>][-
    clientSecret ][-redirectURL <URL>][-issuer <string>][-audience
    <string>][-skewTime <mins>] [-defaultAuthenticationGroup <
    string>]

add authentication OAuthIdPPolicy <name> -rule <expression> [-
    action <string> [-undefAction <string>] [-comment <string>][-
    logAction <string>]

add authentication ldapAction <name> -serverIP <IP> -ldapBase "dc=
    aaa,dc=local"

ldapBindDn <administrator@aaa.local> -ldapBindDnPassword <password
    > -ldapLoginName sAMAccountName

add authentication policy <name> -rule <expression> -action <
    string>

```



```
bind authentication vserver auth_vs -policy <ldap_policy_name> -
    priority <integer> -gotoPriorityExpression NEXT

bind authentication vserver auth_vs -policy <OAuthIdPPolicyName> -
    priority <integer> -gotoPriorityExpression END

bind vpn global  - certkey <>

<!--NeedCopy-->
```

2. 要使用 GUI 创建 OAuth IdP 配置文件，请执行以下操作：

   a) 登录到您的本地 Citrix Gateway 管理门户，然后导航到 **Security**（安全）> **AAA – Application Traffic**（AAA — 应用程序流量）> **Policies**（策略）> **Authentication**（身份验证）> **Advanced Policies**（高级策略）> **OAuth IdP**。



   b) 在 **OAuth IdP** 页面中，单击 **Profiles**（配置文件）选项卡，然后单击 **Add**（添加）。

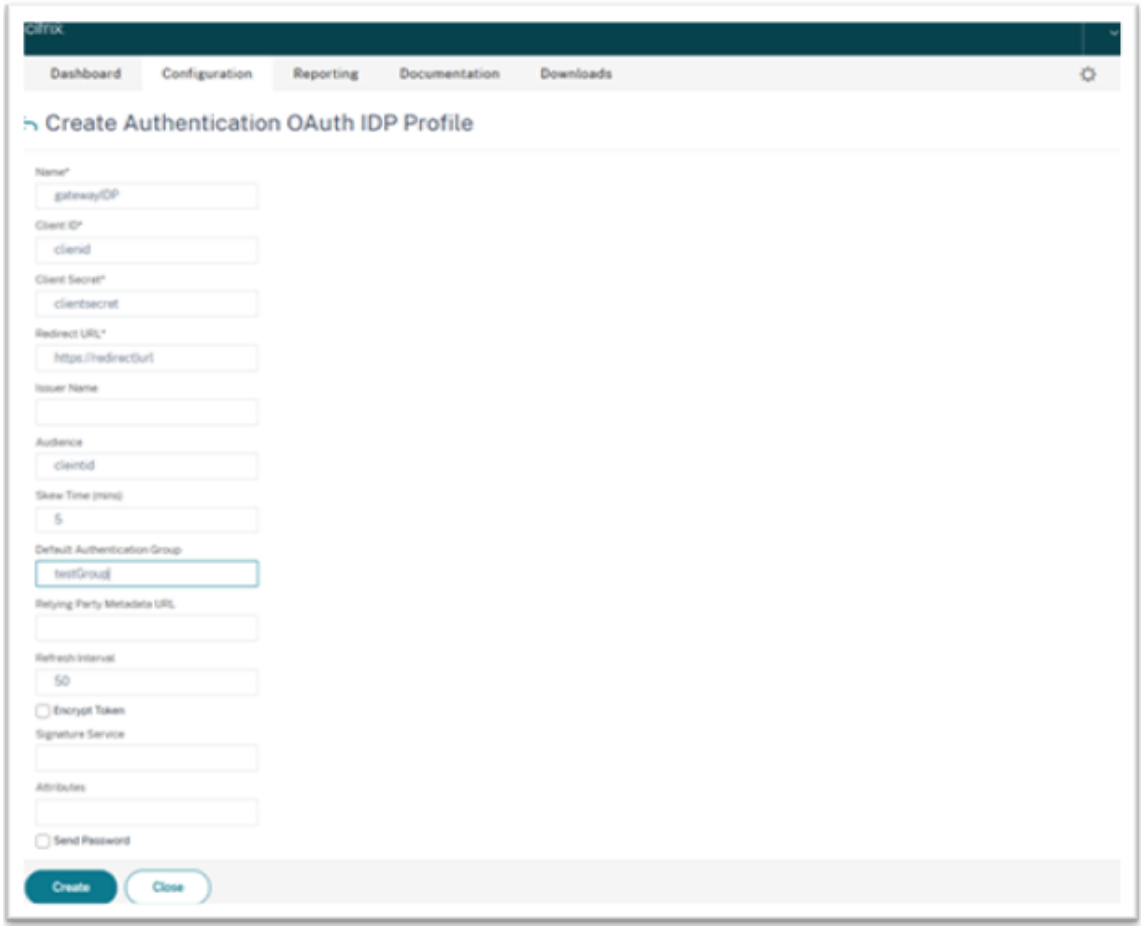
   c) 配置 OAuth IdP 配置文件。

> 注意：
>
> - 从 **Citrix Cloud** > **Identity and Access Management**（身份识别和访问管理）> **Authentication**（身份验证）选项卡中复制并粘贴客户端 ID、密钥和重定向 URL 值，以建立与 Citrix Cloud 的连接。
> - 在 **Issuer Name**（发行者名称）示例中正确输入网关 URL。例如，`https://GatewayFQDN.com`。
> - 还可以在 **Audience**（受众）字段中复制并粘贴客户端 ID。
> - **Send Password**（发送密码）：启用此选项以获得单点登录支持。默认情况下，此选项处于禁用状态。

d) 在 **Create Authentication OAuth IdP Profile**（创建身份验证 OAuth IdP 配置文件）页面上，设置以下参数的值，然后单击 **Create**（创建）。

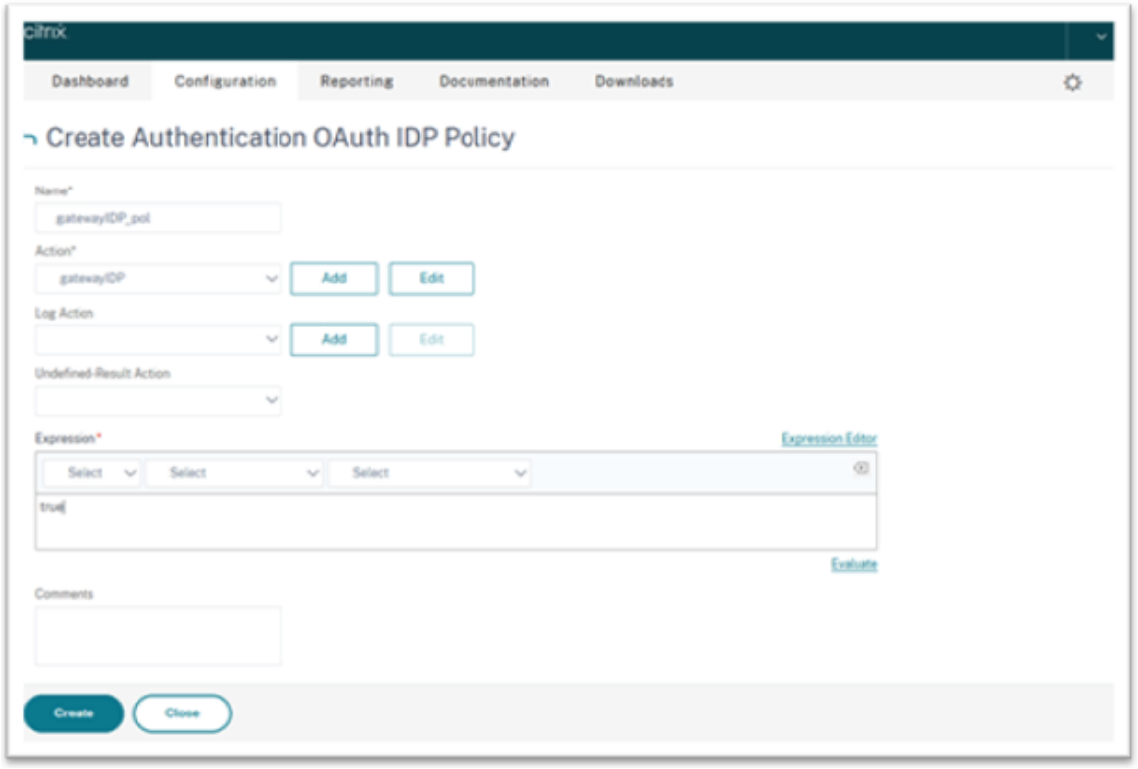
- **Name**（名称）- 身份验证配置文件的名称。必须以字母、数字或下划线字符 (_) 开头。名称只能包含字母、数字以及连字符 (-)、句点 (.)、井号 (#)、空格 ()、at 符号 (@)、等号 (=)、冒号 (:) 和下划线字符。创建配置文件后，您无法更改名称。
- **Client ID**（客户端 ID）- 标识 SP 的唯一字符串。授权服务器使用此 ID 推断客户端配置。最大长度：127。
- 客户端密钥 - 由用户和授权服务器建立的密钥字符串。最大长度：239。
- **Redirect URL**（重定向 URL）- 必须向其发布代码/令牌的 SP 上的端点。
- 颁发者名称 - 要接受其令牌的服务器的标识。最大长度：127。示例：`https://GatewayFQDN.com`。
- **Audience**（受众）- IdP 发送的令牌的目标收件人。收件人负责验证此令牌。
- **Skew Time**（偏差时间）- 此选项指定 Citrix ADC 在传入令牌上允许的时钟偏差（以分钟为单位）。例如，如果 skewTime 为 10，则令牌的有效期为（当前时间 - 10）分钟到（当前时间 + 10）分钟，总共为 20 分钟。默认值：5。
- **Default Authentication Group**（默认身份验证组）- 当 IdP 选择可在 nFactor 流程中使用的配置文件时，则指添加到会话内部组列表中的组。它可以在身份验证策略的表达式 (AAA.USER.IS_MEMBER_OF(“xxx”)) 中使用，以标识与信赖方相关的 nFactor 流程。最大长度：63

组将添加到此配置文件的会话中，以简化策略评估过程并帮助自定义策略。除了提取的组外，此组是身份验证成功时选择的默认组。最大长度：63。



添加 **OAuth IdP** 策略

1. 在 “OAuth IdP” 页面中，单击 **Policies**（策略），然后单击 **Add**（添加）。
2. 在 **Create Authentication OAuth IdP Policy**（创建身份验证 OAuth IdP 策略）页面上，设置以下参数的值，然后单击 **Create**（创建）。
   - **Name**（名称）- 身份验证策略的名称。
   - **Action**（操作）- 之前创建的配置文件的名称。
   - **Log Action**（日志操作）- 请求与此策略匹配时要使用的消息日志操作的名称。非强制性提交。
   - **Undefined-Result Action**（未定义的结果操作）- 策略评估结果未定义 (UNDEF) 时应执行的操作。非必填字段。
   - **Expression**（表达式）- 策略用于响应特定请求的默认语法表达式。例如，true。
   - **Comments**（评论）- 对策略的任何评论。



> 注意：
>
> 当 sendPassword 设置为 “ON”（默认设置为 “OFF”）时，用户凭据将加密并通过安全通道传递到 Citrix Cloud。通过安全通道传递用户凭据允许您在启动时为 Citrix Virtual Apps and Desktops 启用 SSO。

将 **OAuthIDP** 策略和 **LDAP** 策略绑定到虚拟身份验证服务器

现在，您需要将 OAuth IdP 策略绑定到本地 Citrix Gateway 上的虚拟身份验证服务器。

1. 登录本地 Citrix Gateway 管理门户，然后导航到 **Configuration**（配置）> **Security**（安全）> **AAA-Application Traffic**（AAA-应用程序流量）> **Policies**（流量）> **Authentication**（身份验证）> **Advanced Policies**（高级策略）> **Actions**（操作）> **LDAP**。
2. 在 **LDAP Action**（LDAP 操作）屏幕上，单击 **Add**（添加）。
3. 在 “Create Authentication LDAP Server”（创建身份验证 LDAP 服务器）屏幕上，设置以下参数的值，然后单击 **Create**（创建）。
   - **Name**（名称）- LDAP 服务器操作的名称。
   - **ServernName/serverIP**（服务器名称/服务器 IP）- 提供 LDAP 服务器的 FQDN 或 IP。
   - 为 **Security Type**（安全类型）、**Port**（端口）、**Server Type**（服务器类型）、**Time-Out**（超时）选择适当的值。
   - 确保已选中 **Authentication**（身份验证）。
   - **Base DN**（基础 DN）- 开始 LDAP 搜索的基础。例如，`dc=aaa`、`dc=local`。

- **Administrator Bind DN**（管理员绑定 DN）：绑定到 LDAP 服务器的用户名。例如，`admin@aaa.local`。
- **Administrator Password/Confirm Password**（管理员密码/确认密码）：用于绑定 LDAP 的密码。
- 单击 **Test Connection**（测试连接）测试您的设置。
- **Server Logon Name Attribute**（服务器登录名属性）：选择 “sAMAccountName”。
- 其他字段不是必填字段，因此可以根据需要进行配置。

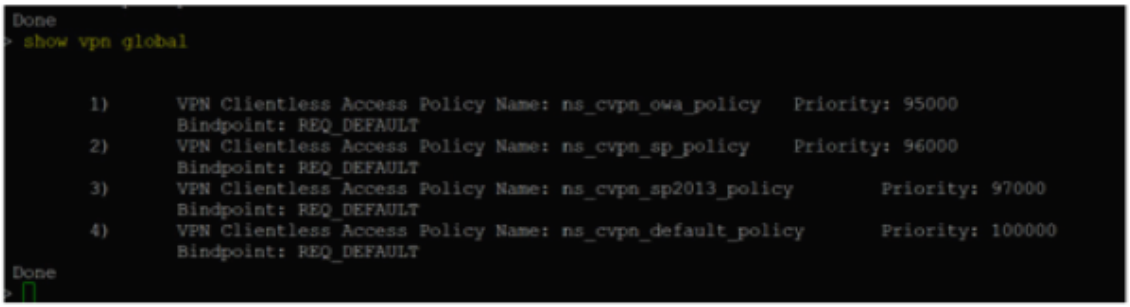
4. 导航到 **Configuration**（配置）> **Security**（安全）> **AAA - Application Traffic**（AAA - 应用程序流量）> **Policies**（策略）> **Authentication**（身份验证）> **Advanced Policies**（高级策略）> **Policy**（策略）。
5. 在 **Authentication Policies**（身份验证策略）屏幕上，单击 **Add**（添加）。
6. 在 **Create Authentication Policy**（创建身份验证策略）页面上，设置以下参数的值，然后单击 **Create**（创建）。

   - **Name**（名称）- LDAP 身份验证策略的名称。
   - **Action Type**（操作类型）- 选择 “LDAP”。
   - **Action**（操作）- 选择 LDAP 操作。
   - **Expression**（表达式）- 策略用于响应特定请求的默认语法表达式。例如，true**。

将证书全局绑定到 **VPN**

将证书全局绑定到 VPN 需要对本地 Citrix Gateway 进行 CLI 访问权限。使用 Putty（或类似）通过 SSH 登录本地 Citrix Gateway。

1. 启动命令行实用程序，例如 Putty。
2. 使用 SSH 登录本地 Citrix Gateway。
3. 键入以下命令：
   ```
   show vpn global
   ```
   > 注意：
   >
   > 不得绑定任何证书。

4. 要列出本地 Citrix Gateway 上的证书，请键入以下命令：
   ```
   show ssl certkey
   ```


5. 选择相应的证书，然后键入以下命令以将证书全局绑定到 VPN：

   ```
   bind vpn global -certkey cert_key_name
   ```

   其中 cert_key_name 是证书的名称。

6. 键入以下命令以检查证书是否已全局绑定到 VPN：

   ```
   show vpn global
   ```

在 **Citrix Gateway** 中将域直通配置为身份验证方法

完成将 Citrix Gateway 设置为 IdP 后，请执行以下步骤以在 Citrix Gateway 中将域直通配置为身份验证方法。

将域直通设置为身份验证方法时，客户端将使用 Kerberos 票证而非凭据进行身份验证。
Citrix Gateway 同时支持模拟和 Kerberos 约束委派 (KCD)。但是，本文介绍了 KCD 身份验证。有关详细信息，请参阅 CTX236593。

配置域直通包括以下步骤：

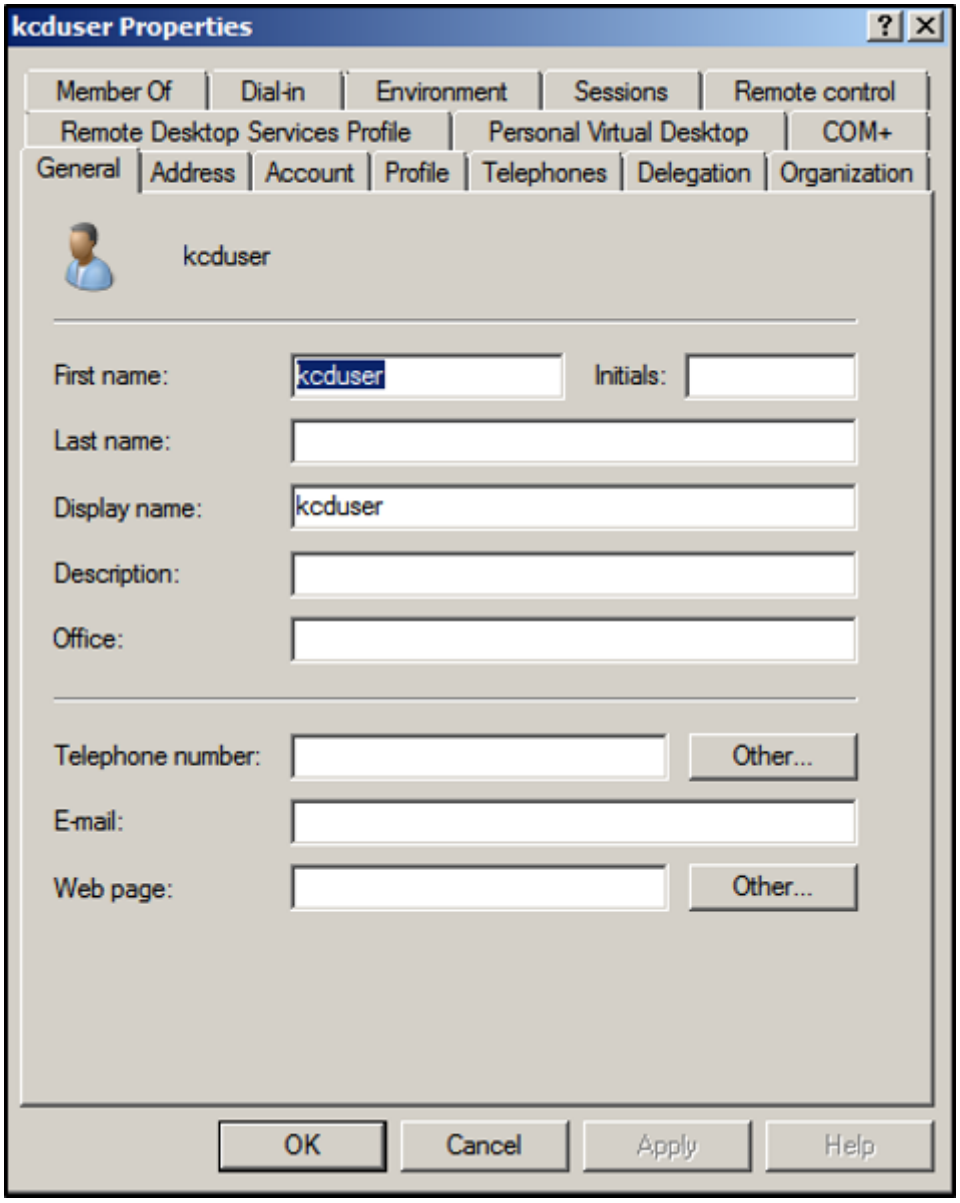
1. Kerberos 约束委派配置
2. 客户端配置

Kerberos 约束委派配置

1. 在 Active Directory 中创建 KCD 用户

   Kerberos 在票证授予系统中运行，以针对资源验证用户的身份，它涉及客户端、服务器和密钥分发中心 (KDC)。

   为了让 Kerberos 正常运行，客户端需要向 KDC 请求票证。客户端必须首先使用其用户名、密码和域向 KDC 进行身份验证，然后才能请求名为 AS 请求的票证。



2. 将新用户与服务主体名称 (SPN) 关联。

   客户端使用网关的 SPN 进行身份验证。

   - 服务主体名称 (SPN)：服务主体名称 (SPN) 是服务实例的唯一标识符。Kerberos 身份验证使用 SPN 将服务实例与服务登录帐户关联。此功能允许客户端应用程序请求帐户的服务身份验证，即使客户端没有帐户名亦如此。

   SetSPN 是用于在 Windows 设备上管理 SPN 的应用程序。使用 SetSPN，可以查看、编辑和删除 SPN 注册。

   a) 在 Active Directory 服务器中，打开命令提示符。

   b) 在命令提示窗口中，输入以下命令：

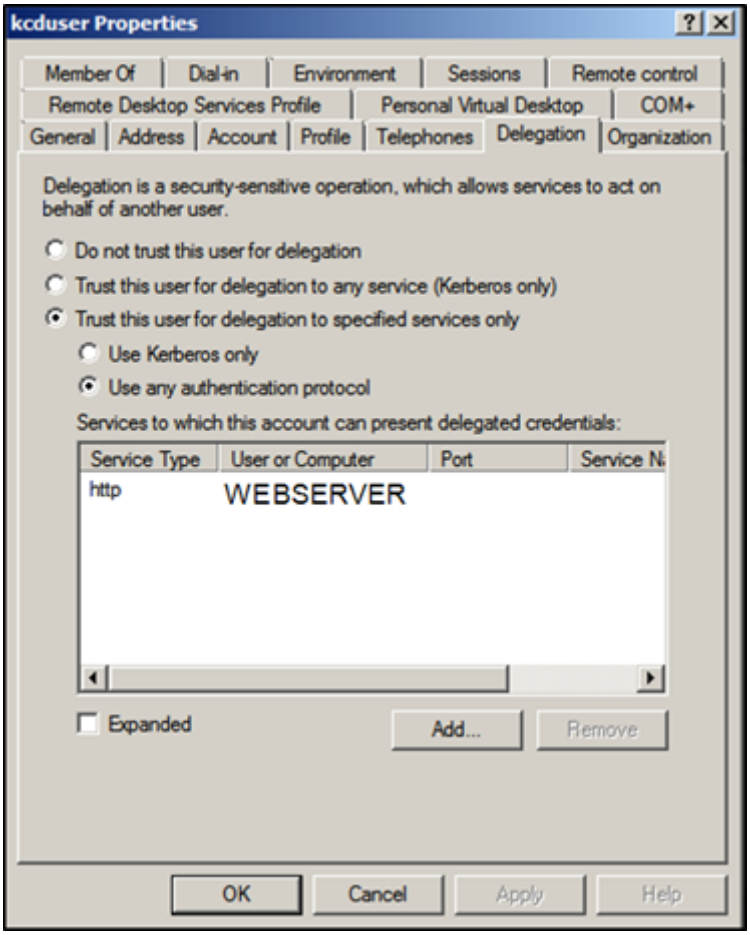
      ```
      setspn -A http/<LB fqdn> <domain\Kerberos user>
      ```


c) 要确认 Kerberos 用户的 SPN，请运行以下命令：

```
setspn -l <Kerberos user>
```

运行 `setspn` 命令后，会出现“委派”选项卡。

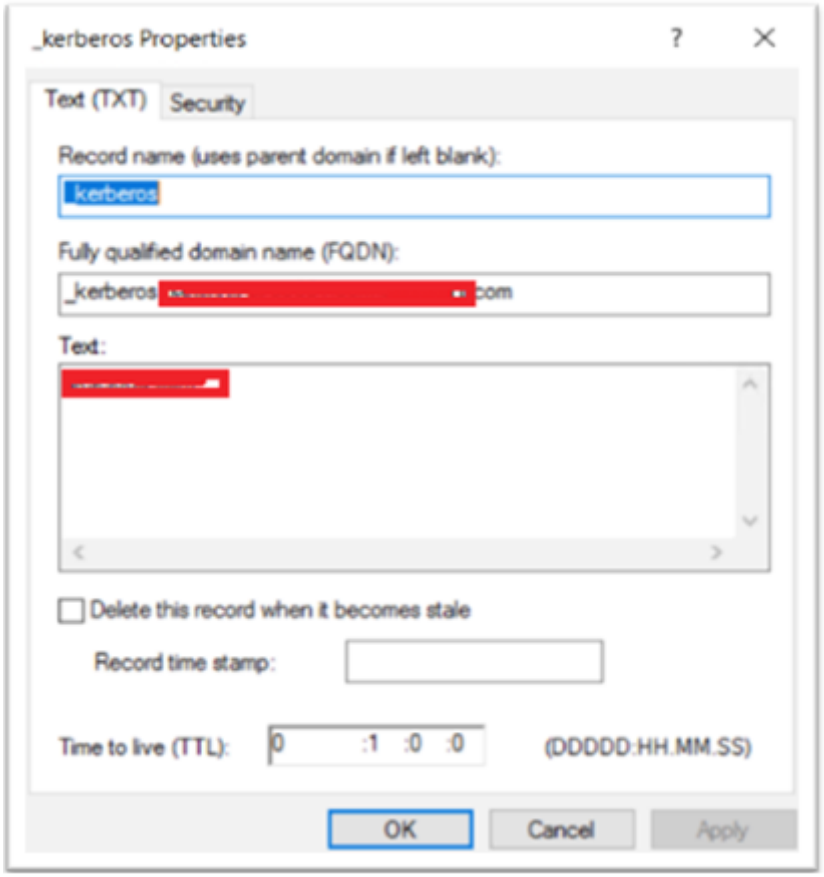
d) 选择 **Trust this user for delegation to specified services only**（仅信任此用户来委派给指定服务）选项和 **Use any authentication protocol**（使用任何身份验证协议）选项。添加 Web 服务器并选择 HTTP 服务。



3. 为客户端创建 DNS 记录以查找网关的 SPN：

在 Active Directory 中添加 TXT DNS 记录。

> 注意：
>
> 名称必须以 _Kerberos 开头，数据必须是域名。FQDN 必须显示 Kerberos。.



窗口的已加入域的客户端使用 _kerberos.fqdn 请求票证。例如，如果客户端加入了 citrite.net，操作系统可以获取任何带 *.citrite.net 的 Web 站点的票证。但是，如果网关域像 gateway.citrix.com 一样位于外部域，客户端操作系统将无法获取 Kerberos 票证。

因此，必须创建一个 DNS TXT 记录，该记录将帮助客户端查找 _kerberos.gateway.com 并获取 Kerberos 票证以进行身份验证。

4. 将 Kerberos 配置为身份验证因素。

   a) 为 NetScaler 用户创建一个 KCD 帐户。在这里，我们选择手动执行此操作，但您可以创建 keytab 文件。

   > 注意：
   >
   > 如果您使用的是备用域（内部域和外部域），则必须将服务 SPN 设置为 HTTP/PublicFQDN.com@InternalDomain.ext

   - 领域 - Kerberos 领域。通常是您的内部域名后缀。
   - **User Realm**（用户领域）- 这是用户的内部域后缀。
   - **Enterprise Realm**（企业领域）- 只有在 KDC 需要企业用户名而非主体名称的某些 KDC 部署中才需要提供此选项。
   - **Delegated User**（委派用户）- 这是您在前面的步骤中在 AD 中创建的 KCD 的 NetScaler 用户帐户。确保密码正确。

b) 确保会话配置文件使用的是正确的 KCD 帐户。将会话策略绑定到身份验证、授权和审核虚拟服务器。

（配置会话配置文件）

c) 将身份验证策略绑定到身份验证、授权和审核虚拟服务器。这些策略使用不从客户端获取密码的身份验证、授权和审核方法，因此需要使用 KCD。但是，他们仍必须获取 UPN 格式的用户名和域信息。

> 注意：
>
> 可以使用 IP 地址或 EPA 扫描来区分已加入域的设备和未加入域的设备，并使用 Kerberos 或常规 LDAP 作为身份验证的因素。

配置客户端

要允许成功单点登录到 VDA，请执行以下步骤。

必备条件：

- 已加入域的计算机
- 启用了 SSO 的 Citrix Workspace 2112.1 或更高版本
- 信任检查连接是否安全的必要 URL
- 验证来自客户端和 AD 的 Kerberos。客户端操作系统必须连接到 AD 才能获取 Kerberos 票证。

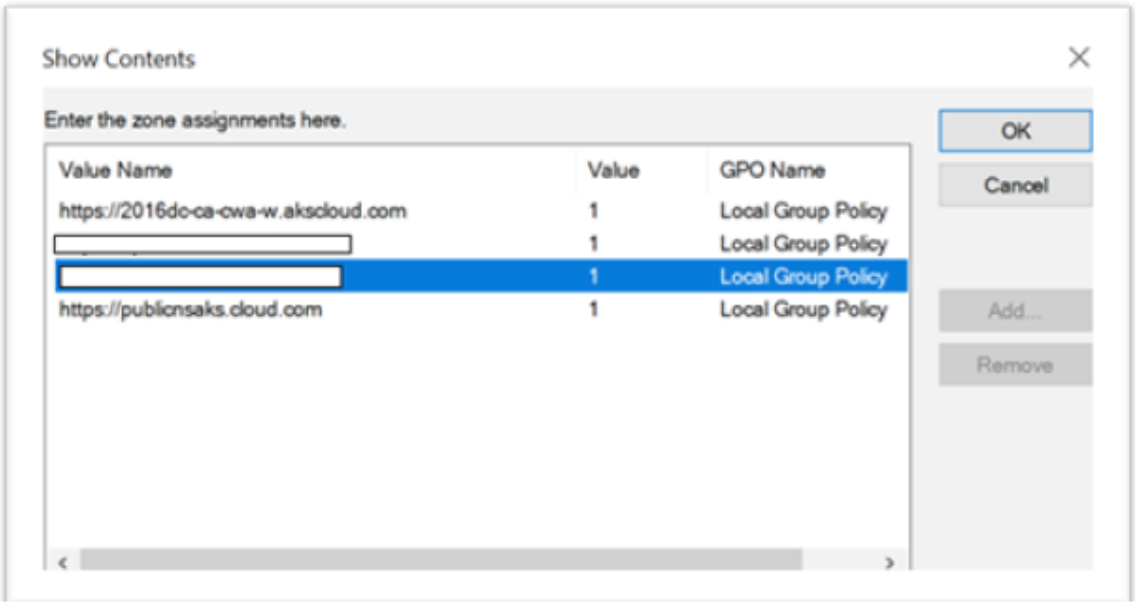
下面是在浏览器中值得信任的一些 URL：

- 网关 URL 或 FQDN
- AD FQDN
- 来自基于浏览器的启动的 SSO 的 Workspace URL。

1. 如果你使用的是 Internet Explorer、微软 Edge 或谷歌浏览器，请执行以下操作：

   a) 启动浏览器。

   b) 在客户端上打开本地组策略编辑器。



   a) 转到 计算机配置 > **Windows** 组件 > **IE** 浏览器 > **Internet** 控制面板 > 安全页面。

   b) 打开 “Site to zone Assignment”（站点到区域分配）列表，然后添加列出的所有 URL，值为一 (1)。

   c)（可选）运行 `Gpupdate` 以应用策略。

2. 如果您使用的是 Mozilla Firefox 浏览器，请执行以下操作：

   a) 打开浏览器。

   b) 在搜索栏中键入 `about:config`。

   c) 接受风险并继续。

d) 在搜索字段中，键入 **negotiate**。

e) 从填充的数据列表中，验证 **network.negotiate-auth.trusted-uris** 是否设置为域值。

这样就完成了客户端的配置。

3. 使用 Workspace 应用程序或浏览器登录到 Workspace。

这不得提示在加入了域的设备上输入用户名或密码。

Kerberos 故障排除

> 注意：
>
> 您必须是域管理员才能运行此验证步骤。

在命令提示符或 Windows PowerShell 中，运行以下命令以验证 SPN 用户的 Kerberos 票证验证：

```
KLIST get host/FQDN of AD
```

使用 **Azure Active Directory** 作为身份提供程序域直通到 **Citrix Workspace**

January 17, 2023

可以使用 Azure Active Directory (AAD) 作为身份提供程序来实现到 Citrix Workspace 的单点登录 (SSO)，其中包含已加入域的端点/VM、混合端点/VM 和注册了 Azure AD 的端点/VM。

使用此配置，您还可以使用 Windows Hello 通过注册了 AAD 的端点对 Citrix Workspace 进行单点登录。

- 可以使用 Windows Hello 向 Citrix Workspace 应用程序进行身份验证。
- 使用 Citrix Workspace 应用程序进行基于 FIDO2 的身份验证。
- 借助 AAD 从加入了 Microsoft AAD 的计算机（AAD 作为 IdP）和条件访问单点登录到 Citrix Workspace 应用程序。

要实现对虚拟应用程序和桌面的单点登录，您可以按如下所示部署 FAS 或配置 Citrix Workspace 应用程序。

> 注意：
>
> 只有在使用 Windows Hello 时，才能实现单点登录到 Citrix Workspace 资源。但是，在访问已发布的虚拟应

> 用程序和桌面时，系统会提示您输入用户名和密码。要解决此提示问题，您可以将 FAS 和 SSO 部署到虚拟应用程序和桌面。

必备条件：

1. 将 Azure Active Directory 连接到 Citrix Cloud。有关详细信息，请参阅 Citrix Cloud 文档中的将 Azure Active Directory 连接到 Citrix Cloud。
2. 启用 Azure AD 身份验证以访问工作区。有关详细信息，请参阅 Citrix Cloud 文档中的 Enable Azure AD authentication for workspaces（为工作区启用 Azure AD 身份验证）。

要实现对 Citrix Workspace 的单点登录，请执行以下操作：

1. 使用 includeSSON 配置 Citrix Workspace 应用程序。
2. 在 Citrix Cloud 中禁用 `prompt=login` 属性。
3. 使用 Azure Active Directory Connect 配置 Azure Active Directory 直通。

配置 **Citrix Workspace** 应用程序以支持 **SSO**

必备条件：

- Citrix Workspace 版本 2109 或更高版本。

> 注意：
>
> 如果您使用 FAS 进行 SSO，则不需要 Citrix Workspace 配置。

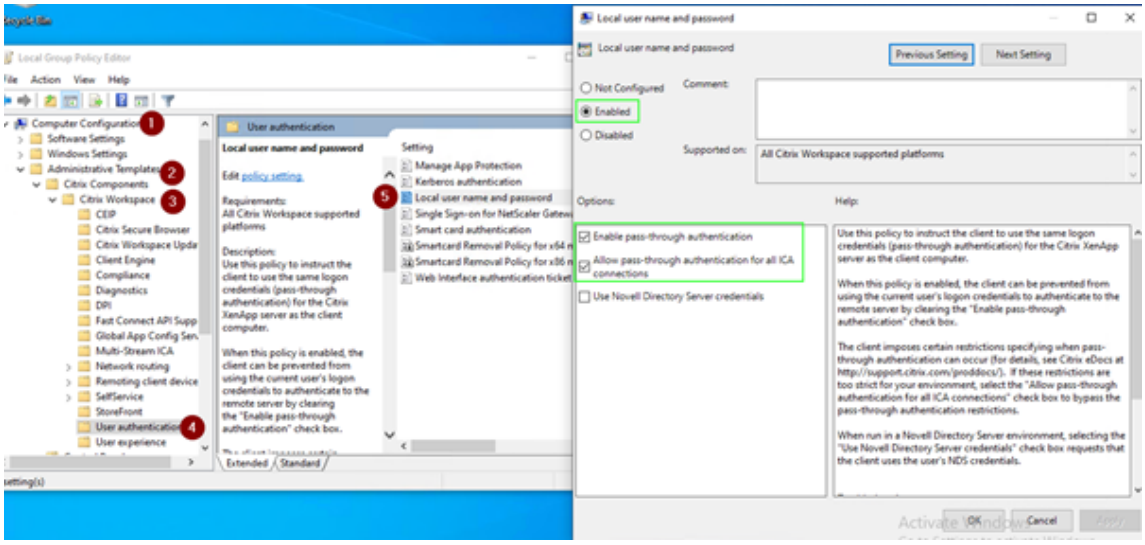
1. 从带选项 `includeSSON` 的管理命令行安装 Citrix Workspace 应用程序：

   ```
   CitrixWorkspaceApp.exe /includeSSON
   ```

2. 从 Windows 客户端注销并登录以启动 SSON 服务器。
3. 单击计算机配置 > 管理模板 > **Citrix** 组件 > **Citrix Workspace** > 用户身份验证将 Citrix Workspace GPO 更改为允许本地用户名和密码。

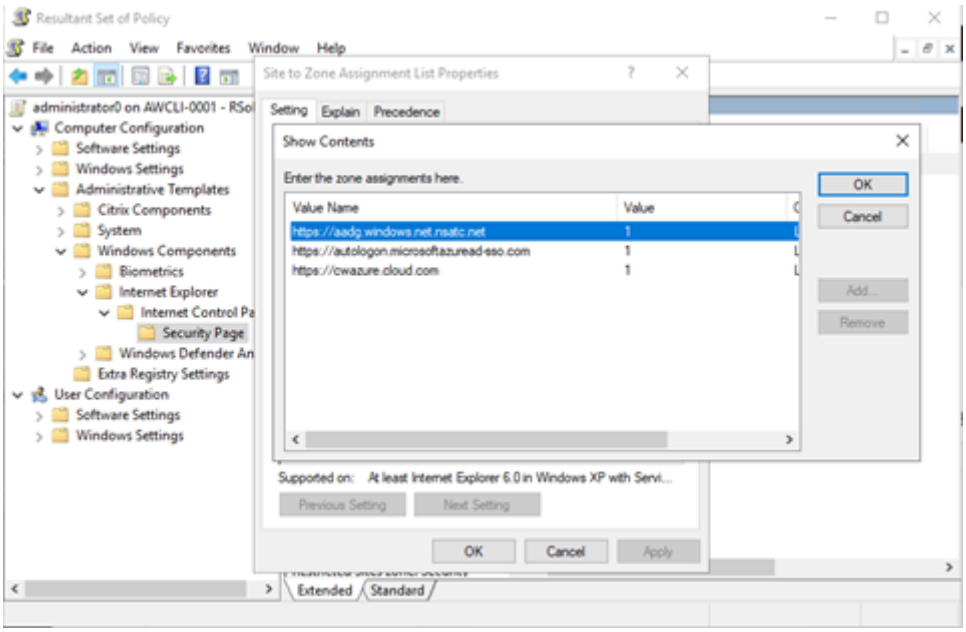
   > 注意：
   >
   > 这些策略可以通过 Active Directory 推送到客户端设备。仅当从 Web 浏览器访问 Citrix Workspace 时才需要执行此步骤。

4. 请根据屏幕截图启用该设置。



5. 通过 GPO 添加以下可信站点：

   - `https://aadg.windows.net.nsatc.net`
   - `https://autologon.microsoftazuread-sso.com`
   - `https://xxxtenantxxx.cloud.com`：Workspace URL

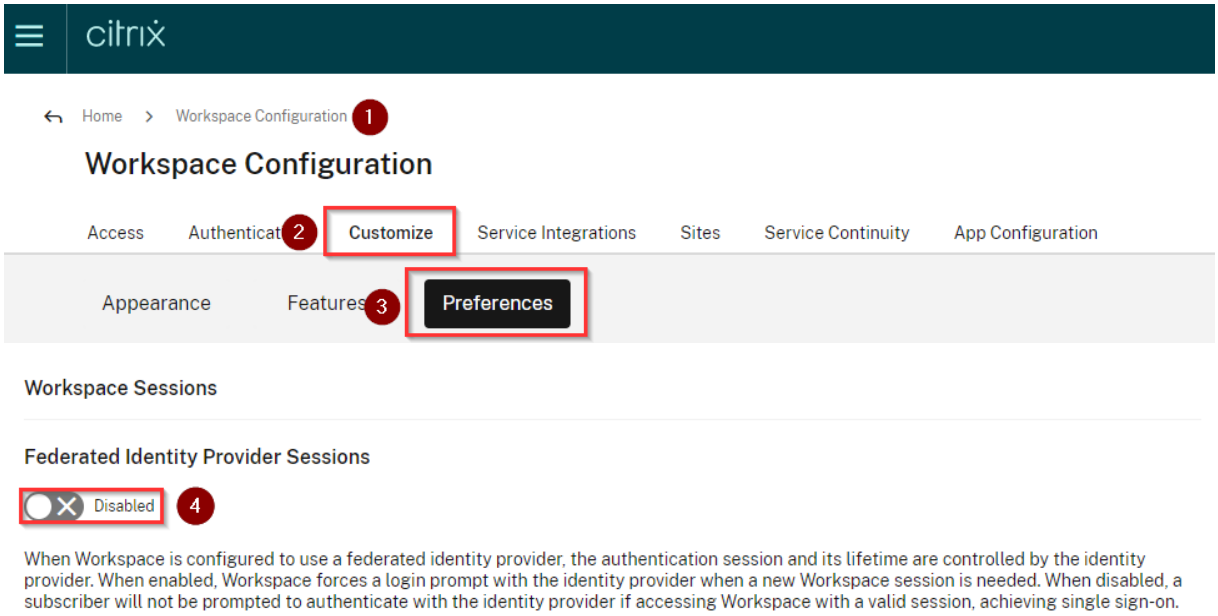


> 注意：
>
> 当 `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle` 中的 **AllowSSOForEdgeWebview** 注册表设置为 false 时，AAD 的单点登录将处于禁用状态。

在 Citrix Cloud 中禁用 prompt=login 参数

默认情况下为 Citrix Workspace 启用了 `prompt=login`，即使用户选择保持登录状态或者设备已加入 Azure AD，也会强制进行身份验证。

可以在您的 Citrix 云帐户中禁用 `prompt=login`。导航到 `Workspace Configuration\Customize\Preferences-Federated Identity Provider Sessions` 并禁用该开关。
有关详细信息，请参阅 Citrix 知识中心文章 CTX253779。



> 注意：
>
> 在已加入 AAD 或已加入混合 AAD 的设备上，如果 AAD 用作 Workspace 的 IdP，Citrix Workspace 应用程序不会提示输入凭据。用户可以使用工作帐户或学校帐户自动登录。
>
> 要允许用户使用其他帐户登录，请将以下注册表设置为 false。
>
> 在 `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle` 或 `Computer\HKEY_CURRENT_USER\SOFTWARE\Citrix\Dazzle` 下创建并添加一个名为 **AllowSSOForEdgeWebview** 的注册表字符串 REG_SZ，并将其值设置为 False。或者，如果用户从 Citrix Workspace 应用程序注销，则用户可以在下次登录时使用其他帐户登录。

使用 Azure Active Directory Connect 配置 Azure Active Directory 直通

- 如果您是首次安装 Azure Active Directory Connect，请在 **User sign-in**（用户登录）页面上选择 **Pass-through Authentication**（直通身份验证）作为登录方法。有关详细信息，请参阅 Microsoft 文档中的 Azure Active Directory Pass-through Authentication: Quickstart（Azure Active Directory 直通身份验证：快速入门）。
- 如果 Microsoft Azure Active Directory Connect 存在：

1. 选择 **Change user sign-in**（更改用户登录）任务，然后单击 **Next**（下一步）。
2. 选择 **Pass-through Authentication**（直通身份验证）作为登录方法。

> 注意：
>
> 如果客户端设备已加入 Azure AD 或已加入混合 Azure AD，则可以跳过此步骤。如果设备已加入 AD，则使用 kerberos 身份验证进行域直通身份验证。

使用 **Okta** 作为身份提供程序域直通到 **Citrix Workspace**

January 17, 2023

可以使用 Okta 作为身份提供程序 (IdP) 实现对 Citrix Workspace 的单点登录。

> 必备条件：
>
> - Citrix Cloud
>   - Cloud Connector
>
> 注意：
> 如果您不熟悉 Citrix Cloud，请定义资源位置并配置连接器。建议至少在生产环境中部署两个云连接器。有关如何安装 Citrix Cloud Connector 的信息，请参阅 Cloud Connector 安装。
>
> - Citrix Workspace
> - 联合身份验证服务（可选）
>
> - Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）
> - 已加入 AD 域的 VDA 或已加入 AD 的物理设备
> - Okta 租户
>   - Okta IWA 代理（集成 Windows 身份验证）
>   - Okta 验证（可以从应用商店下载 Okta 验证）（可选）
> - Active Directory

1. 部署 Okta AD 代理：
   a) 在 Okta 管理门户中，单击 **Directory**（目录）> **Directory Integrations**（目录集成）。
   b) 单击 **Add Directory**（添加目录）> **Add Active Directory**（添加 Active Directory）。
   c) 请按照涵盖代理体系结构和安装要求的工作流查看安装要求。
   d) 单击 **Set Up Active Directory**（设置 Active Directory）按钮，然后单击 **Download Agent**（下载代理）。

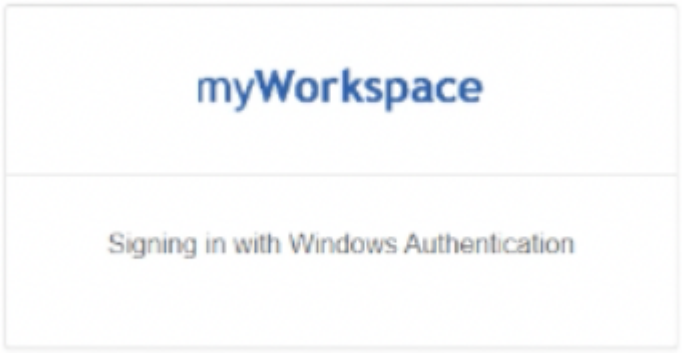
e) 按照 Install the Okta Active Directory agent（安装 Okta Active Directory 代理）中提供的说明将 Okta AD 代理安装到 Windows 服务器上。

> 注意：
>
> 在安装代理之前，请确保满足 Active Directory integration prerequisites（Active Directory 集成必备条件）中提到的必备条件。

2. 设置集成 Windows 身份验证 (IWA)：

a) 在 Okta 管理员门户上，单击 **Security**（安全），然后单击 **Delegated Authentication**（委派身份验证）。
b) 向下滚动到加载页面上的 **On-prem Desktop SSO**（本地桌面 SSO）部分，然后单击 **Download Agent**（下载代理）。
c) 为 IWA 设置 **Routing Rules**（路由规则）。有关详细信息，请参阅 Configure Identity Provider routing rules（配置身份提供程序路由规则）。

3. 启动 Okta 客户门户。

> 注意：
>
> - 安装 Okta IWA 代理且状态为已启用时，可以从已加入 Windows 域的设备登录。此配置还会跳过登录，并将您定向到 IWA 登录页面并传递用户凭据。
>
> 
>
>
> - 有关如何解决任何问题的详细信息，请参阅 Install and configure the Okta IWA Web agent for Desktop single sign-on（安装和配置用于桌面单点登录的 Okta IWA Web 代理）。

4. 通过登录 Citrix Cloud (`https://citrix.cloud.com`) 并启用 Okta 作为 IdP。有关信息，请参阅 Citrix Tech Zone 文档中的 Tech Insight: Authentication - Okta（技术洞察：身份验证 - Okta）。

> 注意：
>
> 可以从 Citrix Workspace 应用程序或浏览器登录，两者均可根据 Tech Zone 文档提供直通体验。

5. 要实现对虚拟应用程序和桌面的单点登录，您可以部署 FAS 或配置 Citrix Workspace 应用程序。

> 注意：
>
> 如果未部署 FAS，系统会提示您输入 AD 用户名和密码。有关如何启用 FAS 的信息，请参阅配置到

> Workspace 应用程序的单点登录中的“启用联合身份验证服务”。
> 如果未使用 FAS，请配置 Citrix Workspace 应用程序以支持 SSO。

安全通信

February 2, 2023

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，可以使用如下所示的一系列安全技术集成 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。
- 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。
- 支持传输层安全性 (TLS) 1.0 至 1.2 版。
- 用于在 Citrix Workspace 应用程序连接中建立信任关系的可信服务器。
- ICA 文件签名服务
- 本地安全机构 (LSA) 保护
- 仅限适用于 Citrix Virtual Apps 部署的代理服务器：SOCKS 代理服务器或安全代理服务器。代理服务器可帮助限制对网络的访问和来自网络的访问。这些服务器还处理 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。
- 出站代理

Citrix Gateway

Citrix Gateway（以前称为 Access Gateway）保护与 StoreFront 应用商店的连接。此外，还允许管理员详细控制用户对桌面和应用程序的访问权限。

要通过 Citrix Gateway 连接桌面和应用程序，请执行以下操作：

1. 使用以下方法之一指定管理员提供的 Citrix Gateway URL：
    - 首次使用自助服务式用户界面时，系统会提示您在添加帐户对话框中输入 URL。
    - 以后使用自助服务式用户界面时，可以通过单击首选项 > 帐户 > 添加来输入 URL
    - 如果要通过 storebrowse 命令建立连接，请在命令行中输入 URL

该 URL 指定网关和特定应用商店（选择性指定）：

- 要连接到 Citrix Workspace 应用程序找到的第一个应用商店，请使用以下格式的 URL：
    - https://gateway.company.com
- 要连接到特定应用商店，请使用格式为（例如）https://gateway.company.com?<storename> 的 URL。此动态 URL 的格式为非标准格式；请勿在该 URL 中包含 =（等号字符）。如果要通过 storebrowse 连接到特定应用商店，可能需要在 storebrowse 命令中用双引号引起 URL。

1. 系统提示时，使用您的用户名、密码和安全令牌连接到该应用商店（通过网关）。有关此步骤的详细信息，请参阅 Citrix Gateway 文档。

身份验证完成后，将显示您的桌面和应用程序。

通过防火墙进行连接

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。如果使用防火墙，适用于 Windows 的 Citrix Workspace 应用程序可以经由防火墙与 Web 服务器和 Citrix 服务器通信。

常用 **Citrix** 通信端口

源	类型	Port（端口）	详细信息
Citrix Workspace 应用程序	TCP	80/443	与 StoreFront 通信
ICA 或 HDX	TCP/UDP	1494	访问应用程序和虚拟桌面
具有会话可靠性的 ICA 或 HDX	TCP/UDP	2598	访问应用程序和虚拟桌面
ICA 或 HDX over TLS	TCP/UDP	443	访问应用程序和虚拟桌面

有关端口的详细信息，请参阅 Citrix 知识中心文章 CTX101810。

传输层安全性

传输层安全性 (TLS) 将取代 SSL（安全套接字层）协议。互联网工程工作小组 (IETF) 在接管 TLS 开放式标准的开发任务后，将其更名为 TLS。

TLS 通过提供服务器身份验证、数据流加密和消息完整性检查，来保障数据通信的安全。有些组织（包括美国政府组织）要求使用 TLS 来保障数据通信的安全。这些组织可能还要求使用验证的加密，例如联邦信息处理标准 (FIPS) 140。FIPS 140 是一个加密标准。

必须配置用户设备和 Citrix Workspace 应用程序，才能将 TLS 加密用作通信媒介。有关保护 StoreFront 通信的信息，请参阅 StoreFront 文档中的安全部分。有关保护 VDA 的信息，请参阅 Citrix Virtual Apps and Desktops 文档中的传输层安全性 (TLS)。

可以使用以下策略执行以下操作：

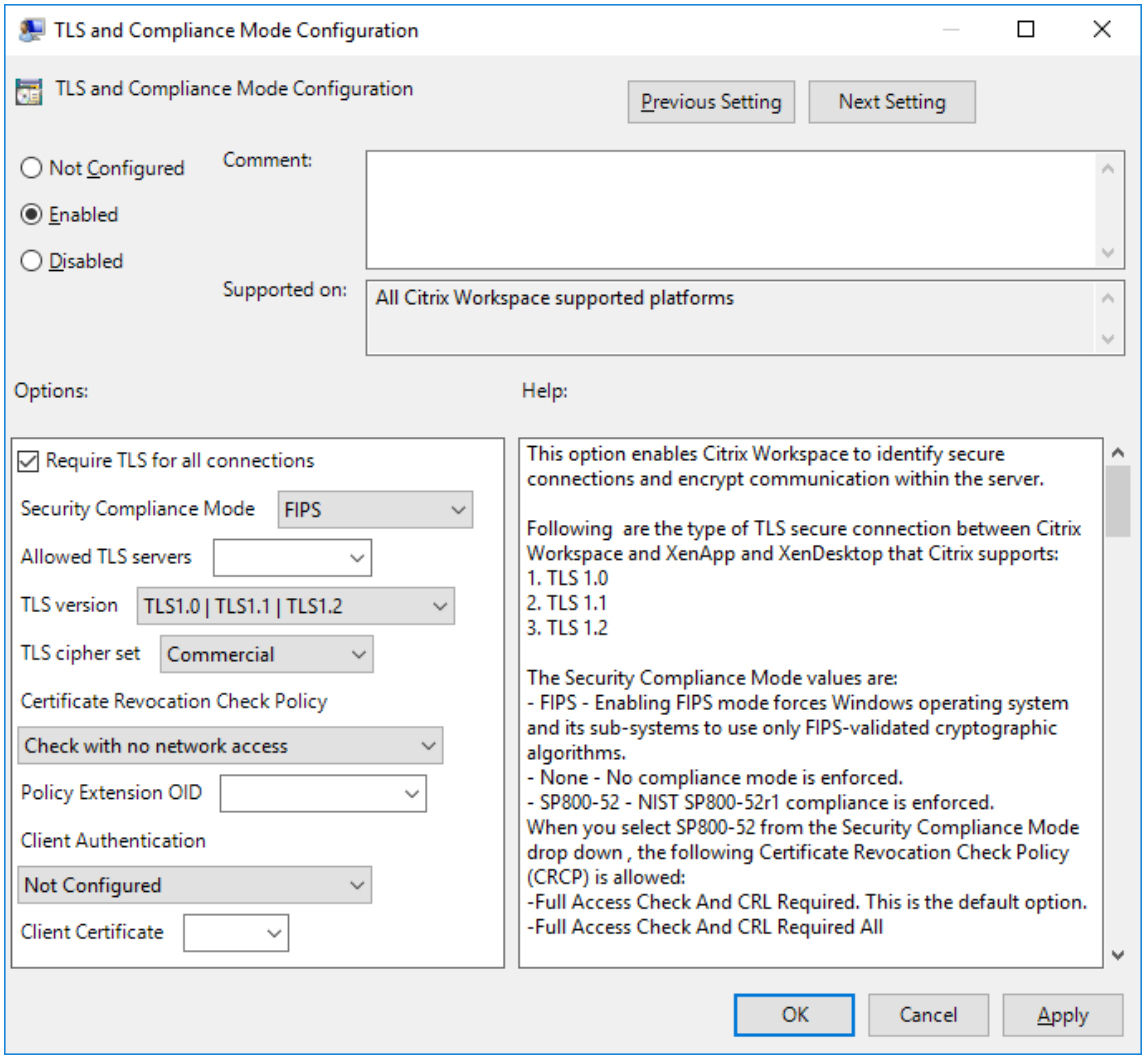
- 强制使用 TLS：我们建议您将 TLS 用于使用不受信任的网络（包括 Internet）的连接。
- 强制使用 FIPS（Federal Information Processing Standards，联邦信息处理标准）：得到认可的加密且遵从 NIST SP 800-52 中的建议。这些选项默认处于禁用状态。

- 强制使用特定版本的 TLS 和特定的 TLS 密码套件：Citrix 支持 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。
- 检查特定的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）。

> 重要：
> 为了增强安全性，以下密码套件已弃用：
>
> - 密码套件 RC4 和 3DES
> - 前缀为 “TLS_RSA_*” 的密码套件
> - TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
> - TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
> - TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
> - TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
> - TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
> - TLS_RSA_WITH_RC4_128_SHA (0x0005)
> - TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
>
> 有关受支持的密码套件的信息，请参阅 Citrix 知识中心文章 CTX250104。

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。此外，请启用 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**，请将证书吊销检查策略设置设为需要完全访问检查和 **CRL**。

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。此外，请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** 服务器下拉菜单中，选择端口号。使用逗号分隔的列表可确保 Workspace 应用程序仅连接到指定的服务器。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 无法识别或信任颁发者，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)。有关详细信息，请参阅 Citrix 知识中心文章 CTX250104。

b) 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 - 已完成证书吊销列表检查。仅使用本地证书吊销列表存储。所有分发点都被忽略。验证目标 SSL Relay/Citrix Secure Web Gateway 服务器提供的服务器证书的证书吊销列表检查不是强制性的。
- 完全访问检查 - 已完成证书吊销列表检查。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。证书吊销列表检查用于验证目标服务器提供的服务器证书并不重要。
- 需要完全访问检查和 **CRL** - 已完成证书吊销列表检查，但根证书颁发机构除外。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** - 已完成证书吊销列表检查，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 - 未完成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。

有关内部和外部网络连接列表的信息，请参阅 Citrix 知识中心文章 CTX250104。

可信服务器

强制执行可信服务器连接

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

使用此策略，管理员可以控制客户端如何识别其要连接到的已发布应用程序或桌面。客户端将确定信任级别，称为具有连接的信任区域。然后，信任区域将确定如何为连接配置客户端。

启用此策略可阻止连接到不在可信区域中的服务器。

默认情况下，区域识别基于客户端要连接到的服务器的地址。要成为可信区域的成员，服务器必须为 Windows 可信站点区域的成员。You can configure this using the **Windows Internet zone** setting.

或者，可以使用 Address 设置来特别信任服务器 地址。服务器地址必须是支持使用通配符的服务器的逗号分隔列表，例如 `cps*.citrix.com`。

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 > **Citrix** 组件 > **Citrix Workspace** > 网络路由 > 配置可信服务器配置。
3. 选择已启用以强制 Citrix Workspace 应用程序进行区域识别。
4. 选择强制使用可信服务器配置。此选项将强制客户端使用可信服务器执行识别。
5. 在 **Windows Internet** 区域下拉菜单中，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。

启用此策略且服务器不在可信区域中时，连接将被阻止，并显示错误消息。
要成功连接，必须将标识的服务器添加到 Windows 受信任的站点区域。例如，对于 SSL 连接，请将服务器添加为”http://” 或”https://”。

> 注意：
>
> 对于 SSL 连接，必须信任证书公用名。对于非 SSL 连接，必须逐个信任联系的所有服务器。

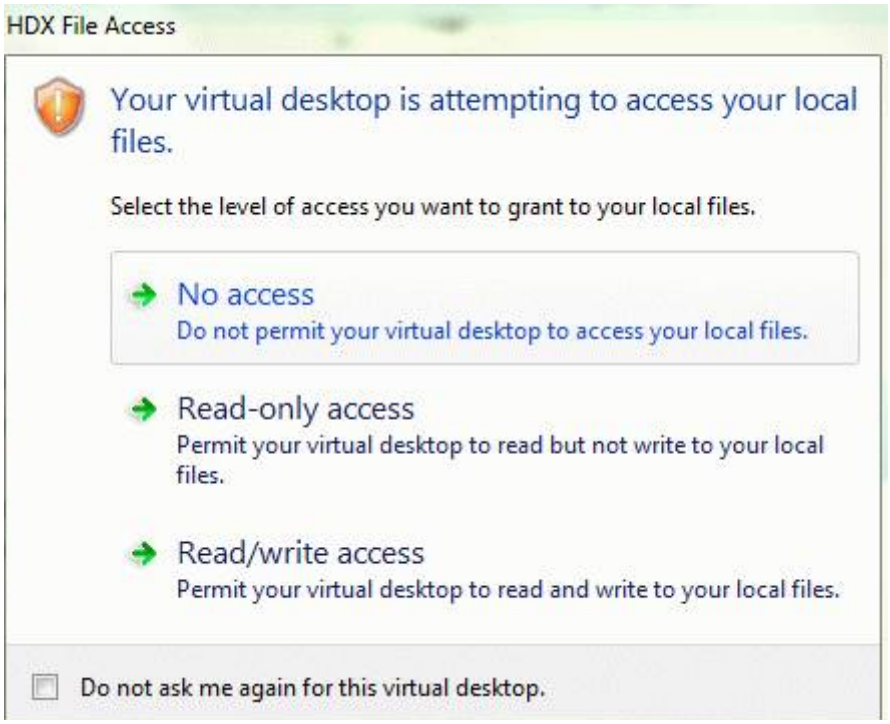
此外，请确保将内部 StoreFront FQDN 添加到本地 Intranet 区域或可信站点区域中。有关信息，请参阅身份验证部分中的修改 **Internet Explorer** 设置。

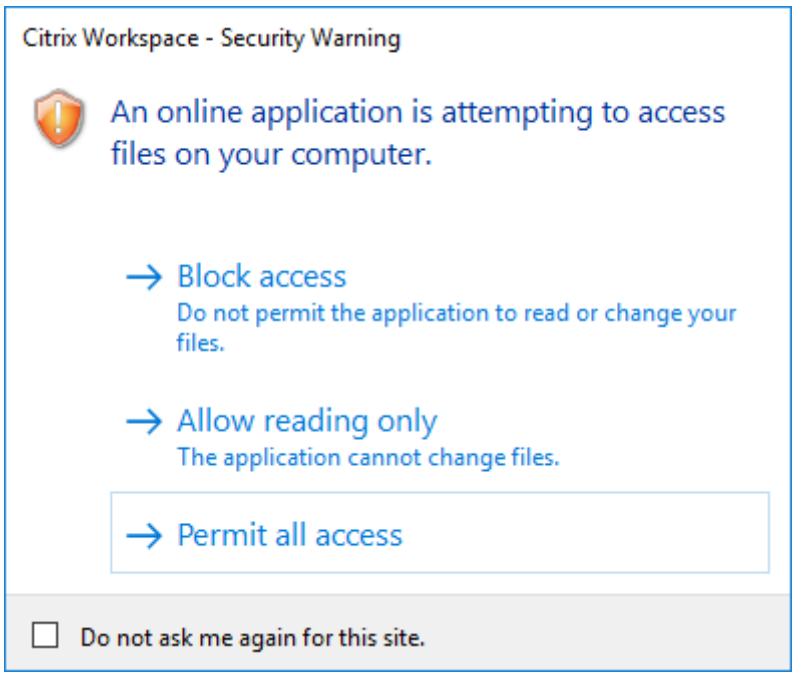
客户端选择性信任

除了允许或阻止与服务器的连接之外，客户端还会使用各个区域来识别文件、麦克风或网络摄像和 SSO 访问。

区域	资源	访问级别
Internet	文件、麦克风、Web	提示用户访问，不允许 SSO
Intranet	麦克风、Web	提示用户访问，允许 SSO
受限制的站点	全部	无访问权限且可能阻止连接
受信任	麦克风、Web	读取或写入，允许 SSO

当用户已选择某个区域的默认值时，可能会显示以下对话框：





管理员可以通过使用组策略或在注册表中创建和配置客户端选择性信任注册表项来修改此默认行为。有关如何配置客户端选择性信任注册表项的详细信息，请参阅知识中心文章 CTX133565。

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，ICA 文件签名功能未启用。

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。

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允许列表中。
    b) 信任证书 - 单击显示可从允许列表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和桌面启动。存在无效签名时，会出现安全警告。由于未授权，会话启动失败。
        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，我们建议您从以下优先级列表中进行选择：

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。
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。

本地安全机构 **(LSA)** 保护

Citrix Workspace 应用程序支持 Windows 本地安全机构 (LSA) 保护，它维护系统中与本地安全的所有方面有关的信息。此支持为托管桌面提供 LSA 级别的系统保护。

通过代理服务器进行连接

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 的服务器上远程配置的代理服务器设置。

在与 Web 服务器进行通信时，Citrix Workspace 应用程序将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。相应地配置用户设备上的默认 Web 浏览器的 **Internet** 设置。

要通过 StoreFront 上的 ICA 文件强制执行代理设置，请参阅 Citrix 知识中心文章 CTX136516。

出站代理支持

SmartControl 允许管理员配置和实施影响环境的策略。例如，您可能希望禁止用户将驱动器映射到其远程桌面。您可以使用 Citrix Gateway 上的 SmartControl 功能实现粒度。

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 SmartControl 功能，因为客户端域上不存在网关。然后，可以使用出站 ICA 代理。出站 ICA 代理功能允许您使用 SmartControl 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。使用出站代理插件来配置单个静态代理，或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或注册表编辑器来配置出站代理。

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"
```

连接和证书

连接

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

Certificates（证书）

> 注意：
>
> 适用于 Windows 的 Citrix Workspace 应用程序已经过数字签名。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

如果远程网关上存在专用证书，请在访问 Citrix 资源的用户设备上安装组织的证书颁发机构颁发的根证书。

> 注意：
>
> 如果在连接时无法验证远程网关的证书，则会显示不受信任的证书警告。当本地密钥库中缺少根证书时会出现此警告。用户选择忽略警告并继续时，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，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。请按照贵组织的安全策略使用通配符证书。通配符证书的替代项是指包含服务器名称列表和使用者备用名称 (SAN) 扩展的证书。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）。

证书吊销列表

证书吊销列表 (CRL) 允许 Citrix Workspace 应用程序检查服务器的证书是否已吊销。证书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的 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 应用程序配置为只检查其本地证书列表，也可以配置为同时检查本地和网络证书列表。还可以将证书检查机制配置为只有在验证了所有 CRL 之后才允许用户登录。

如果要在本地计算机中配置证书检查，请退出 Citrix Workspace 应用程序。检查是否已关闭所有 Citrix Workspace 组件（包括连接中心）。

有关详细信息，请参阅传输层安全性部分。

支持缓解中间人攻击

适用于 Windows 的 Citrix Workspace 应用程序可帮助您使用 Microsoft Windows 的企业证书固定功能降低中间人攻击的风险。中间人攻击是一种网络攻击，攻击者秘密拦截并转发两方之间的消息，这两方认为他们是直接相互通信的。

以前，当您联系存储服务器时，无法验证收到的响应是否来自您打算联系的服务器。使用 Microsoft Windows 的企业证书固定功能，您可以通过固定服务器的证书来验证服务器的有效性和完整性。

适用于 Windows 的 Citrix Workspace 应用程序已预先配置为使用证书固定规则知晓特定域或站点必须获得什么服务器证书。如果服务器证书与预配置的服务器证书不匹配，适用于 Windows 的 Citrix Workspace 应用程序会阻止会话进行。

有关如何部署企业证书固定功能的信息，请参阅 Microsoft 文档。

> 注意：
>
> 您必须知道证书的到期时间并正确更新组策略和证书信任列表。否则，即使没有受到攻击，您也可能无法启动会话。

Storebrowse

April 6, 2023

> 注意：
>
> 本文仅适用于 Citrix Workspace 的本地部署。有关云部署，请参阅 适用于 Workspace 的 Storebrowse 文档。

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

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

- 添加应用商店。
- 列出已配置的应用商店中的已发布应用程序和桌面。
- 通过手动选择任何已发布的虚拟应用程序和桌面生成 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 实用程序属于 `Authmanager` 组件。Citrix Workspace 应用程序安装完成后，**Storebrowse** 实用程序将位于 `AuthManager` 安装文件夹中。

要确认是否随 `Authmanager` 组件一起安装了 **Storebrowse** 实用程序，请检查以下注册表路径：

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

- 适用于 Windows 的 Citrix Workspace 应用程序 1808 或更高版本。
- 最少 530 MB 的可用磁盘空间。

- 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 Server 2022
Windows Server 2016
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 应用商店中，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：输入要访问应用商店需验证的凭据。默认情况下，在创建第一个应用商店时，显式身份验证处于启用状态。
- 域直通：对加入了域的 Windows 计算机进行身份验证后，您将自动登录到应用商店。要使用此选项，请在安装 Citrix Workspace 应用程序时启用直通身份验证。有关域直通的详细信息，请参阅配置直通身份验证。
- **HTTP Basic**：此方法由第三方客户端集成和 Web 门户网站使用，其中使用外部用户界面来捕获域限定的用户名和密码。StoreFront 使用 IIS 中的基本身份验证功能将凭据传输到 StoreFront 服务器。然后，StoreFront 使用域服务或 Broker XML Service 身份验证来验证凭据以及获取组信息。有关如何启用 HTTP Basic 身份验证的信息，请参阅管理身份验证方法文档中的 HTTP Basic。

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，请在 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。
- 使用适用于 Windows 的 Citrix Workspace 应用程序中包含的 `Authmanager`。当您使用域直通身份验证时，可以使用此方法。有关详细信息，请参阅域直通身份验证文档。

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。

添加应用商店

`-a、--addstore`

说明：

添加新应用商店。返回应用商店的完整 URL。如果返回失败消息，则报告错误。

> 注意：
>
> **Storebrowse** 实用程序支持多应用商店配置。

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>
```


帮助

/?

说明：

提供有关 **Storebrowse** 实用程序用法的详细信息。

列出应用商店

(-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
```

枚举

(-M 0x2000 -E)

说明：

枚举资源。

StoreFront 上的命令示例：

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

快速启动

-q、--quicklaunch

说明：

使用 **Storebrowse** 实用程序为已发布的应用程序和桌面生成 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。启动 URL，可以是 StoreFront 服务器，也可以是 Citrix Gateway URL。ICA 文件在 %LocalAppData%\Citrix\Storebrowse\cache 目录中生成。

可以运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 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_publ
 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_publ
 apps and desktops } <https://my.secondexmaplestore.com>
```

启动

-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。名称，可以是 StoreFront 服务器，也可以是 Citrix Gateway URL。ICA 文件在 %LocalAppData%\Citrix\Storebrowse\cache 目录中生成。

运行以下命令以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
```

之前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>
```

会话启动

`-S、--sessionlaunch`

说明：

使用此命令，您可以添加应用商店、验证和启动已发布的资源。此选项将以下对象作为参数：

- 用户名
- 密码
- 域
- 要启动的资源的名称
- 应用商店 URL

但是，如果用户不提供凭据，`AuthManager` 将提示输入凭据，然后启动资源。

可以运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
```

在之前的输出中以粗体显示的名称用作 `-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_
 } <https://my.secondexamplestore.com>
```

文件文件夹

`-f、--filefolder`

说明：

在已发布的应用程序和桌面的自定义路径中生成 ICA 文件。

启动选项需要文件夹名称和资源名称作为带 Store URL 的输入。应用商店 URL 可以是 StoreFront 服务器，也可以是 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 }
```

跟踪身份验证

`-t、--traceauthentication`

说明：

生成 `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 }
```

删除存储

`-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

单点登录功能允许您对某个域进行身份验证，并使用该域提供的 Citrix Virtual Apps and Desktops 和 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）。您可以登录，而无需对每个应用程序或桌面重新进行身份验证。添加应用商店时，您的凭据将随 Citrix Virtual Apps and Desktops 和 Citrix DaaS 和 “开始” 菜单设置传递到 Citrix Gateway 服务器。

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 Single Sign-On 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。

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：

- 在 StoreFront 服务器上启用 **HTTP Basic** 身份验证方法，以便通过 **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检查或启动已发布的虚拟应用程序和桌面，则不支持使用命令行选项执行凭据注入操作。解决方法：如果您未使用命令行提供凭据，请使用外部 `AuthManager` 模块。
- **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。

要为使用 ICOSDK 的第三方应用程序启用 SSON，请创建以下注册表：

- 注册表项：`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\NonIEAppsWithSson`
- 注册表值：第三方应用程序的完整路径
- 注册表类型：reg_multi_sz

示例：

- 注册表项：`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\ICA Client\NonIEAppsWithSson`
- 注册表值：C:\temp1\abc.exe;C:\temp2\xyz.exe
- 注册表类型：reg_multi_sz

> 注意：
>
> - 您可以提供多个用分号分隔的第三方应用程序。
> - 版本 2107 及更高版本支持此功能。

适用于 **Workspace** 的 **Storebrowse**

April 6, 2023

适用于 Windows 的 Citrix Workspace 应用程序为 Citrix Workspace 应用程序的自助服务和本地部署提供 **Storebrowse** 支持。它还使 **Storebrowse** 用户能够访问 Cloud 和 Workspace 功能。

> 注意：
>
> - 本文仅适用于 Citrix Workspace 的云部署。有关本地部署，请参阅 Storebrowse 文档。
> - 此功能仅为单点登录提供 **Storebrowse** 支持。
> - 必须具备系统要求和兼容性中提到的必备条件才能使用此功能。

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。

> 注意：
>
> - 此功能还支持 CTX200337 中提到的其他自助服务插件命令。
> - 可以在命令提示符下执行以下命令。

- `-a "discoveryurl"`：通过命令行添加应用商店。此命令不会在启用了 SSO 的位置显示身份验证提示。例如，AAD 域加入通过 webview 进行身份验证的设备。在其他设备上，将显示身份验证提示。
  - 示例：`SelfService.exe storebrowse -a "https://cwawiniwstest.cloudburrito.com/citrix/store/discovery"`
- `-d "discoveryurl"`：删除应用商店。
  - 示例：`SelfService.exe storebrowse -d "https://cwawiniwstest.cloudburrito.com/citrix/store/discovery"`
- `-e "discoveryurl"`：以 JSON 格式导出资源详细信息。此命令将 resource.json 文件存储在 `%LOCALAPPDATA%\citrix\selfservice` 默认位置。Citrix Workspace 应用程序必须处于活动状态才能运行此命令，并且用户必须登录。
  - 示例：`SelfService.exe storebrowse -e "https://cwawiniwstest.cloudburrito.com/citrix/store/discovery"`

  如果您不想将 resource.json 存储在默认位置，也可以指定自己的路径。

  - 示　　例：`.\SelfService.exe storebrowse -e "https://cwawiniwstest.cloudburrito.com/citrix/store/discovery""C:\Users\<username>\Documents\Fiddler2"`。这会将 resource.json 文件存储在 `C:\Users\<username>\Documents\Fiddler2` 中。

- `-q "FriendlyName""discoveryurl"`：使用此命令执行指定资源的快速启动。

  - 示例：`SelfService.exe storebrowse -q "Excel 2016""https://cwawiniwstest.cloudburrito.com/citrix/store/discovery"`

- `-launch "launchcommandline"`：使用 resource.json 中的 “launchcommandline” 启动资源。

> 注意：
>
> - 从 resource.json 中复制 “launchcommandline”。
> - 在执行命令之前，请从在 resource.json 文件中指定的 “launchcommandline” 中删除 **/**。

  - 示　　例：`SelfService.exe storebrowse -launch -s store0-5c3ec017 -CitrixID store0-5c3ec017@@a9a8e3ac-099d-4577-b84e-e33d0695df39. Notepad -ica "https://cwawiniwstest.cloudburrito.com/Citrix/Store/resources/v2/YTlhOGUzYWMtMDk5ZC00NTc3LWI4NGUtZTMzZDA2OTVkZjM5Lk5vdGVwYWQ-/launch/ica"-cmdline`

  执行 `-launch "launchcommandline"` 后，ica 文件将存储在 `%LOCALAPPDATA%\citrix\selfservice\cache` 目录中。双击 ica 文件以启动资源。

- `-liststore`：列出在 SSP 中添加的应用商店。应用商店列表中包含 storeID，每个应用商店的发现 URL。

  - 示例：`SelfService.exe storebrowse -liststore`

> 注意：
>
> Citrix Workspace 应用程序必须处于活动状态才能执行 `-liststore` 命令。

  `Selfservice.exe storebrowse -liststore` 命令将 storedetails.json 文件存储在 `AppData\Local\Citrix\SelfService` 中。

Citrix Workspace 应用程序 Desktop Lock

January 17, 2023

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 应用程序在已加入域的计算机上运行，这些计算机启用了单点登录并配置了应用商店。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 `/includeSSON` 标志安装适用于 Windows 的 Citrix Workspace 应用程序。使用 adm/admx 文件或命令行选项配置应用商店和单点登录。有关详细信息，请参阅安装。

然后，以管理员身份使用 Citrix 下载页面上提供的 `CitrixWorkspaceDesktopLock.msi` 安装 Citrix Workspace 应用程序 Desktop Lock。

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 10（包括周年纪念更新）和 Windows 11 上受支持。
- 仅限通过本机协议连接到 StoreFront。
- 加入域的终端。
- 用户设备必须连接到 LAN 或 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、双重身份验证或智能卡身份验证
- 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，但 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。
- 用户登录到系统时，将在终端设备上创建本地用户配置文件。即使用户注销，配置文件也会保留在终端设备上，并且基于配置文件管理配置。

> 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 LiveInDesktopDisconnectOnLo
> 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. 在命令提示符下，运行以下命令：

   例如：

   ```
   CitrixWorkspaceApp.exe
         /includeSSON
   STORE0="DesktopStore;https://my.storefront.server/Citrix/MyStore/
      discovery;on;Desktop Store"
   <!--NeedCopy-->
   ```

   该命令位于 Citrix Workspace 应用程序和安装介质上的 **Plug-ins** > **Windows** > **Citrix Workspace app** 文件夹中。有关命令详细信息，请参阅安装下的 Citrix Workspace 应用程序安装文档。
3. 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。
4. 安装完成时，重新启动用户设备。如果您有权访问桌面并以域用户身份登录，则使用 Citrix Workspace 应用程序 Desktop Lock 显示该设备。

您可以允许在安装之后管理用户设备，需要从替换 Shell 中排除安装 CitrixWorkspaceDesktopLock.msi 所用的帐户。如果该帐户稍后被删除，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

以非管理员身份登录时，Desktop Lock 会自动启动已分配的桌面会话。

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。

- 检查 receiver.admx（或 receiver.adml）和 receiver_usb.admx (.adml) 文件是否加载到组策略中（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。虚拟桌面控制 USB 设备并将其显示在用户界面中。
  - 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) 请务必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) 请确保 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) 将第一个交付组的 URL 添加到 Internet Explorer 的可信站点列表中。在表单 desktop://delivery-group-name 中添加 URL。
   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。Desktop Lock 可确保用户设备不会处于不一致的状态。这仅适用于具有 Citrix Workspace 应用程序 Desktop Lock 的用户设备。

删除 **Desktop Lock**

请务必删除列出的两个组件，如下所示：

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。

软件开发工具包 (SDK) 和 API

February 16, 2023

证书标识声明 SDK

证书标识声明 (CID) SDK 允许开发人员创建插件。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向 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。

Certificate Identity Declaration for Citrix Workspace for Windows（适用于 Windows 的 Citrix Workspace 证书身份声明）的最新版本为 **2212**。

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。该会话包括桌面会话、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 协议的更多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。

Virtual Channel SDK for Windows（适用于 Windows 的虚拟通道 SDK）的最新版本为 **2302**。

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 提供的接口用于向单点登录 (SSO) 功能提供用户凭据。此功能在适用于 Windows 的 Citrix Workspace 应用程序 4.2 及更高版本中可用。通过此 API，Citrix 合作伙伴可以提供身份验证以及 SSO 产品，该产品使用 StoreFront 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。

Fast Connect API for Citrix Workspace for Windows（适用于 Windows 的 Citrix Workspace 的 Fast Connect API）的最新版本为 **2212**。

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）。

用于部署适用于 **Windows** 的 **Citrix Workspace** 的脚本

这些是用于部署和配置 Citrix Workspace 应用程序的示例脚本。

Scripts for deploying Citrix Workspace for Windows（用于部署适用于 Windows 的 Citrix Workspace 的脚本）的最新版本为 **2212**。

ICA 设置参考

January 17, 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）

