StoreFront 2507 长期服务版本概述

StoreFront 是一个企业应用商店，它将来自 (/zh-cn/citrix-virtual-apps-desktops.html) 站点和 (/zh-cn/citrix-daas.html) 的应用程序和桌面聚合到一个易于用户使用的商店中。

StoreFront 部署在您网络上的服务器中。有关 Citrix 托管服务，请参阅 (/zh-cn/citrix-workspace)。

在 StoreFront 中，您可以配置一个或多个商店。每个商店都有自己的配置，包括：

- 用户用于登录的 (/zh-cn/storefront/2507-ltsr/stores/authentication.html)。
- StoreFront 查询以枚举用户可用资源的 (/zh-cn/storefront/2507-ltsr/stores/sites.html) 列表。
- 商店的 (/zh-cn/storefront/2507-ltsr/stores/websites/customize-appearance.html)。
- 商店是否可以通过 NetScaler Gateway (/zh-cn/storefront/2507-ltsr/stores/remote-access.html)。

用户可以使用本地安装的 (/zh-cn/citrix-workspace-app) 或 Web 浏览器访问 StoreFront 商店。有关详细信息，请参阅 (/zh-cn/storefront/2507-ltsr/get-started/user-access-options.html)。

要开始使用，请 (/zh-cn/storefront/2507-ltsr/get-started/plan.html)、查看 (/zh-cn/storefront/2507-ltsr/get-started/system-requirements.html) 并 (/zh-cn/storefront/2507-ltsr/get-started/install.html)。

新增功能

使用以下链接了解此版本中的新功能、已修复问题和已知问题。

新增功能

早期版本

要了解有关早期版本的更多信息，请参阅 (/zh-cn/storefront/)。

有关从早期版本升级的步骤，请参阅 (/zh-cn/storefront/2507-ltsr/manage-deployment/upgrade.html)。

支持生命周期

StoreFront 当前版本 (CR) 和长期服务版本 (LTSR) 的产品生命周期策略在 生命周期里程碑 中进行了描述。StoreFront 的其他生命周期信息在 CTX200356 中提供。

新增功能

2507 LTSR 包含以下版本。

- 2507 LTSR CU2
- 2507 LTSR CU1
- 2507 初始版本

累积更新 2 (CU2)

发布日期：August 18, 2026

关于此版本

要了解 Citrix Product Subscription Advantage Eligibility Dates，请单击此链接。

适用于 HTML5 的 Citrix Workspace 应用程序

此版本包括 Citrix Workspace app for HTML5 2603.10。

2507 LTSR CU2 中的新增功能

累积更新 2 (CU2) 是 StoreFront 2507 LTSR 的最新版本。请参阅 新增功能。

此版本包含 StoreFront 2507 LTSR 累积更新 2 (CU2) 的修复。自那时起， 已报告以下问题。

2507 LTSR CU2 中已修复的问题

StoreFront 2507 LTSR CU2 包含以下修复：

- 当 StoreFront 加入 Citrix Analytics 时，您可能会发现 CPU 使用率显著增加。
- 在管理控制台中，当管理员更改 UI 体验然后选择“**取消**”时，更改仍会保存在控制台中。
- 执行计算机控制操作时，StoreFront 不会将客户端名称和地址传递给 DDC，导致它们在日志文件中缺失。
- StoreFront 管理控制台不显示以前上传的徽标。
- 用于设置样式的 PowerShell 命令的帮助文本具有误导性。

- 更改启动设置时，Citrix Workspace 应用程序下载会重新启用。
- 重命名站点会删除该站点的所有最佳 HDX 路由。
- 在管理控制台外观选项卡上，“重置为默认值”按钮不起作用。
- X-XSS-Protection 标头已弃用，应将其删除。
- 当 StoreFront 配置为 Citrix Gateway Service 类型时，升级到 StoreFront 2507 可能会导致启动失败。在 Gateway 配置中，Cloud Connector 选项卡错误地包含了端口 8090，这会阻止 StoreFront 访问云连接器以进行 STA 票证请求。

2507 LTSR CU2 中的已知问题

累积更新 2 中没有新的已知问题。

累积更新 1 (CU1)

发布日期：December 16, 2025

关于此版本

StoreFront（初始版本）

如果 StoreFront 已加入 Citrix Analytics，则 Citrix 不建议安装此版本。有关详细信息，请参阅已知问题。

Citrix 产品订阅权益资格日期

适用于 HTML5 的 Citrix Workspace 应用程序

此版本包括 Citrix Workspace app for HTML5 2511。

2507 LTSR CU1 中的新增功能

累积更新 1 (CU1) 是 StoreFront 2507 LTSR 的最新版本。请参阅新增功能。

如果您已将服务器加入 Citrix Analytics，则 Citrix 建议您不要安装此版本。有关详细信息，请参阅已知问题。

从 CU1 版本开始，当您登录 StoreFront 时，可以看到有关 Citrix Workspace app for HTML5 启动状态的及时且相关的信息。有关详细信息，请参阅改进的 Virtual Apps and Desktops 启动体验。

支持具有 Entra ID 身份的用户（预览版）

以前，StoreFront 要求用户存在于 Active Directory 中。在此版本中，如果用户在 Citrix Gateway 上使用 OIDC 和 Microsoft Entra ID 进行身份验证，则具有 Entra ID 的用户可以枚举并启动分配给其 Entra ID 身份的 Citrix DaaS 资源。对于具有混合身份的用户，StoreFront 还会枚举分配给其 Active Directory 身份的任何资源。

它具有以下限制：

- 使用 SAML 进行身份验证的用户仍被视为仅具有 Active Directory 身份，并且无法枚举分配给 Entra ID 身份的资源。
- 用户必须通过 Citrix Gateway 进行身份验证，而不是直接登录 StoreFront。
- 如果用户位于大量 Entra 组中，则 StoreFront 服务器上可能会出现高内存使用率。
- 不支持 Citrix Virtual Apps and Desktops 站点。Citrix Virtual Apps and Desktops 站点中的资源可能无法枚举。
- 管理控制台中不提供配置。管理员必须使用 PowerShell。
- FAS 在用户具有纯 Entra ID 身份的商店中不受支持。

有关详细信息，请参阅 通过 OIDC 进行 Entra ID 身份验证。

Entra ID 单点登录到 VDA（预览版）

如果用户已使用 Entra ID 进行身份验证，那么当他们启动托管在已加入 Entra 的 VDA 上的资源时，他们可以单点登录到已加入 Entra ID 的 VDA。

它具有以下限制：

- 仅当通过 Citrix Gateway 进行身份验证时才支持此功能，并且使用通过 OIDC 而非 SAML 连接到 Entra ID。
- 这必须使用 PowerShell 进行配置。
- 管理控制台中不提供配置。管理员必须使用 PowerShell。
- 在启用 Entra ID SSO 的商店中不支持 FAS。

有关详细信息，请参阅 单点登录到 VDA。

已修复的问题

StoreFront 2507 LTSR CU1 包含以下修复：

- 禁用 NTLM 身份验证时，StoreFront **收藏夹**不会在 StoreFront 服务器之间同步。

- 用户尝试通过内部 StoreFront (SF) URL 访问某些应用程序时，会遇到“**无法启动应用程序**”错误。
- StoreFront 服务器间歇性地记录事件 4010 和 4011，这表示 XML 运行状况检查到交付控制器 (DDC) 失败。这会导致用户偶尔出现枚举失败。
- 安装 Citrix Web 扩展并禁用协议处理程序时，ICA 文件会下载而不是启动应用程序。发生这种情况是因为当协议处理程序被禁用时，系统无法正确检测到 Citrix Workspace 应用程序。此修复现在会显示“Citrix Workspace 应用程序已通过浏览器扩展成功检测到”，并允许用户在需要时重新进行客户端检测。

已知问题

- 如果 StoreFront 已加入 Citrix Analytics，您可能会发现 CPU 使用率显著增加。

2507 中的新增功能（初始版本）

StoreFront 2507 LTSR 包含自 StoreFront 2402 LTSR 以来的以下新增功能和增强功能：

移除 Citrix Workspace™ 应用程序检测作为混合启动场景的 App Protection 的先决条件

从 2507 LTSR 版本开始，Citrix Workspace 应用程序检测不再是 App Protection for hybrid launches 正常运行的先决条件。此更改简化了混合启动场景中 App Protection 的启用。

以前，当 StoreFront™ 配置为启用混合启动的 App Protection 时，用户界面仅在通过 Citrix Workspace Web 扩展或 Citrix Workspace 启动器检测到特定版本的 Citrix Workspace 应用程序时，才显示需要 App Protection 的资源。这阻止了在无法使用 Citrix Workspace 启动器或 Citrix Workspace Web 扩展的情况下使用 App Protection。此检查已删除，现在无论是否检测到 Citrix Workspace 应用程序，用户界面都会显示此类资源。

通过此更改，在下载 ICA 文件以及使用未实施 App Protection 的旧版 Citrix Workspace 应用程序的情况下，会显示需要 App Protection 的资源。这使得用户可以通过篡改 ICA 文件或使用未启用 App Protection 的 Citrix Workspace 应用程序版本来避免应用 App Protection。因此，如果您已为混合启动启用了 App Protection，那么同时启用 App Protection Posture Check 和 Policy Tampering Detection 非常重要。

增强的 Scout 功能

Scout 现在支持在“收集”页面上显示“添加计算机”按钮。此增强功能使您能够手动添加同一群集中的多个 StoreFront 服务器计算机并同时触发收集，从而提高 StoreFront 部署中数据收集的效率。

移除 Citrix 客户体验改善计划

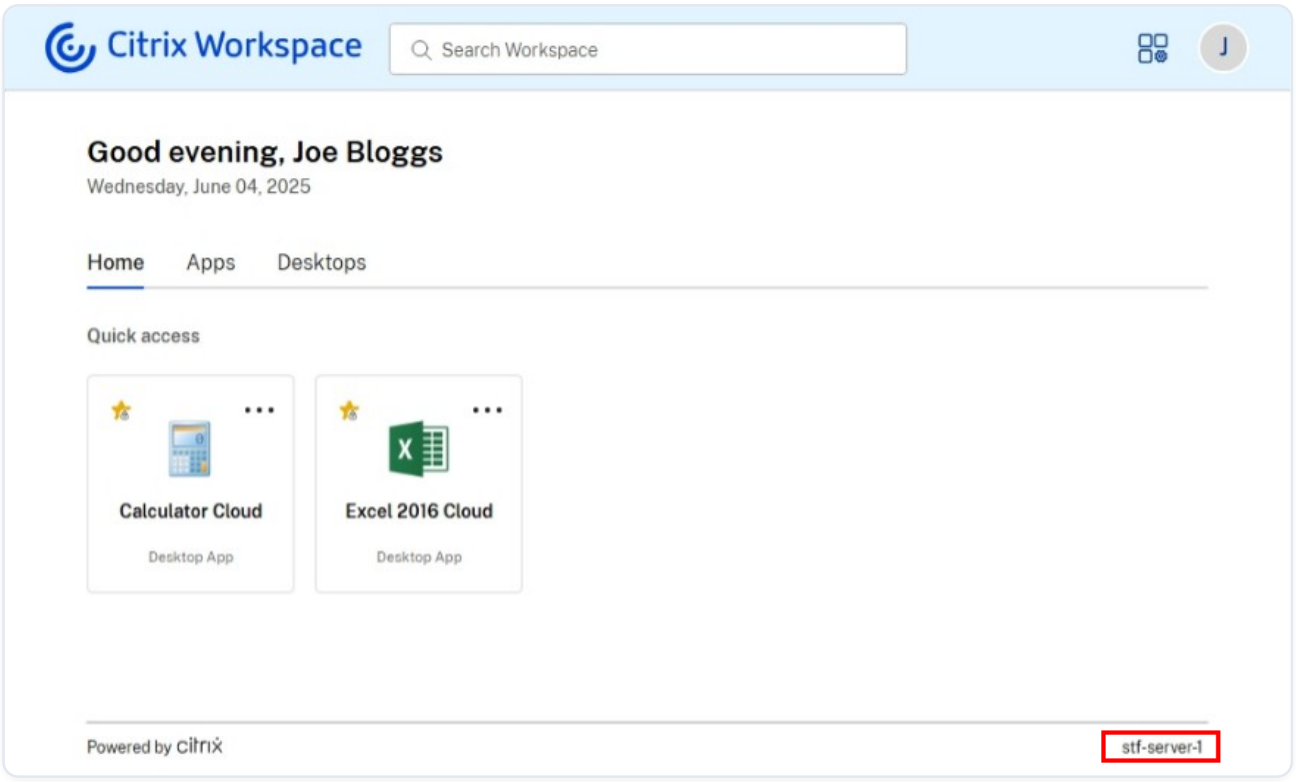
StoreFront 不再向 Citrix 客户体验改善计划发送数据。

适用于 HTML5 HDX 客户端的 Citrix Workspace 应用程序

此版本包括 适用于 HTML5 HDX 客户端的 Citrix Workspace 应用程序 2505。

在最终用户 UI 中显示 StoreFront 服务器名称

使用现代体验时，用户连接到的服务器名称会显示在桌面屏幕底部以及所有平台上的错误消息中。这有助于支持团队快速查找相关的服务器日志。



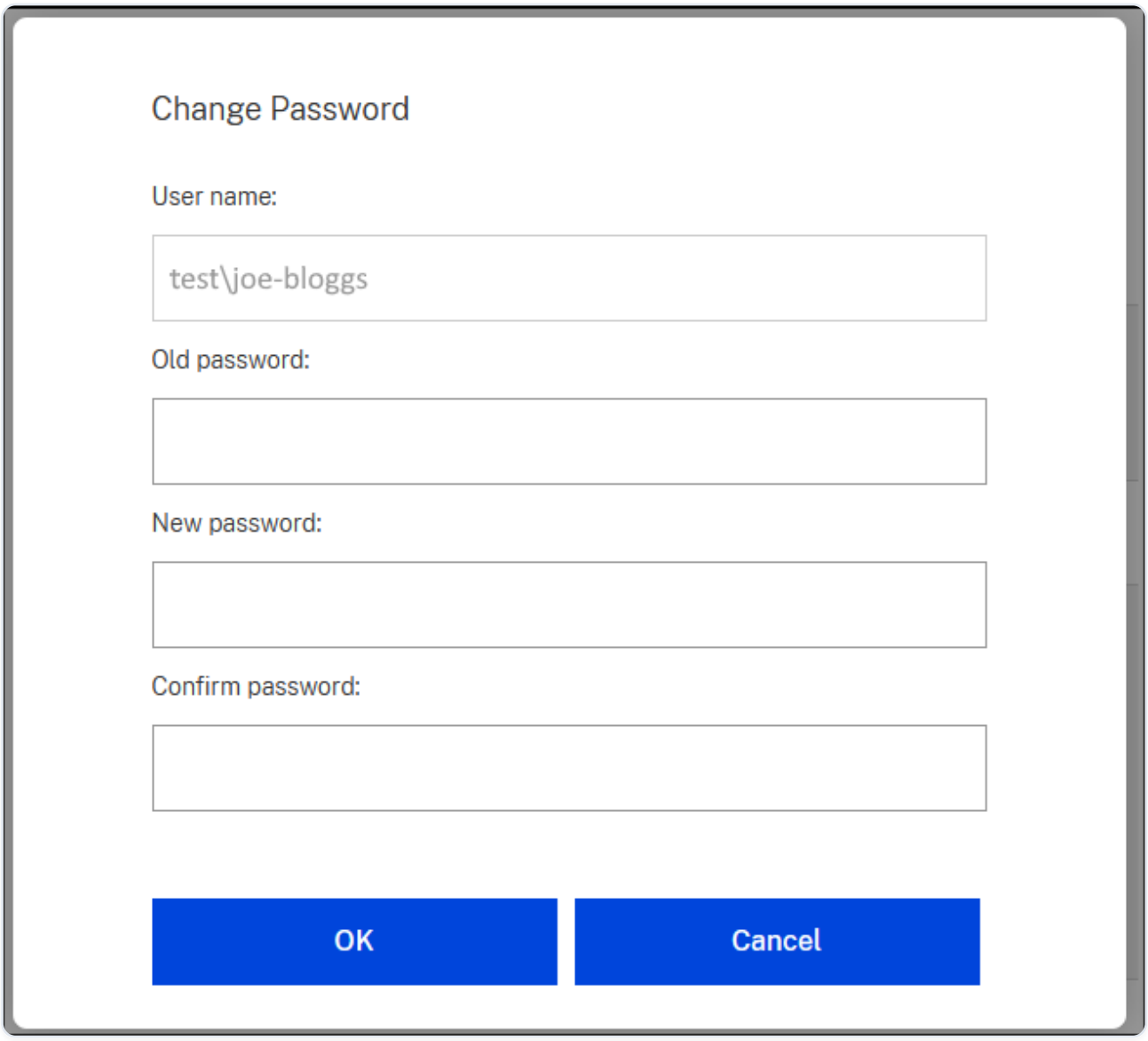
适用于 Android、iPhone 和 iPad 设备的 Citrix Workspace Launcher

Citrix Workspace Launcher 允许 Web 浏览器与 Citrix Workspace 应用程序通信，以启动资源而无需下载 ICA 文件。以前，此功能仅在 Windows、macOS 和 Linux 上可用。现在，Android、iPhone 和 iPad 也支持 Citrix Workspace Launcher。当 Android、iPhone 或 iPad 用户首次在其 Web 浏览器中打开应用商店网站时，该网站会使用 Citrix Workspace Launcher 检测 Citrix Workspace 应用程序。如果检测成功，Citrix Workspace Launcher 将用于所有后续启动。这简化了启动体验，并通过避免将 ICA 文件保存到设备来提高安全性。

这需要适用于 Android 25.03 或更高版本的 Citrix Workspace 应用程序以及适用于 iOS 25.03 或更高版本的 Citrix Workspace 应用程序。经典体验和现代体验均提供此功能。

使用现代体验随时更改密码

以前，在使用现代体验时，用户可以在登录时更改已过期的密码，但无法在其他时间更改密码。使用 StoreFront 2503，如果在密码选项中配置，则帐户设置中有一个选项可以随时更改密码，类似于经典体验。

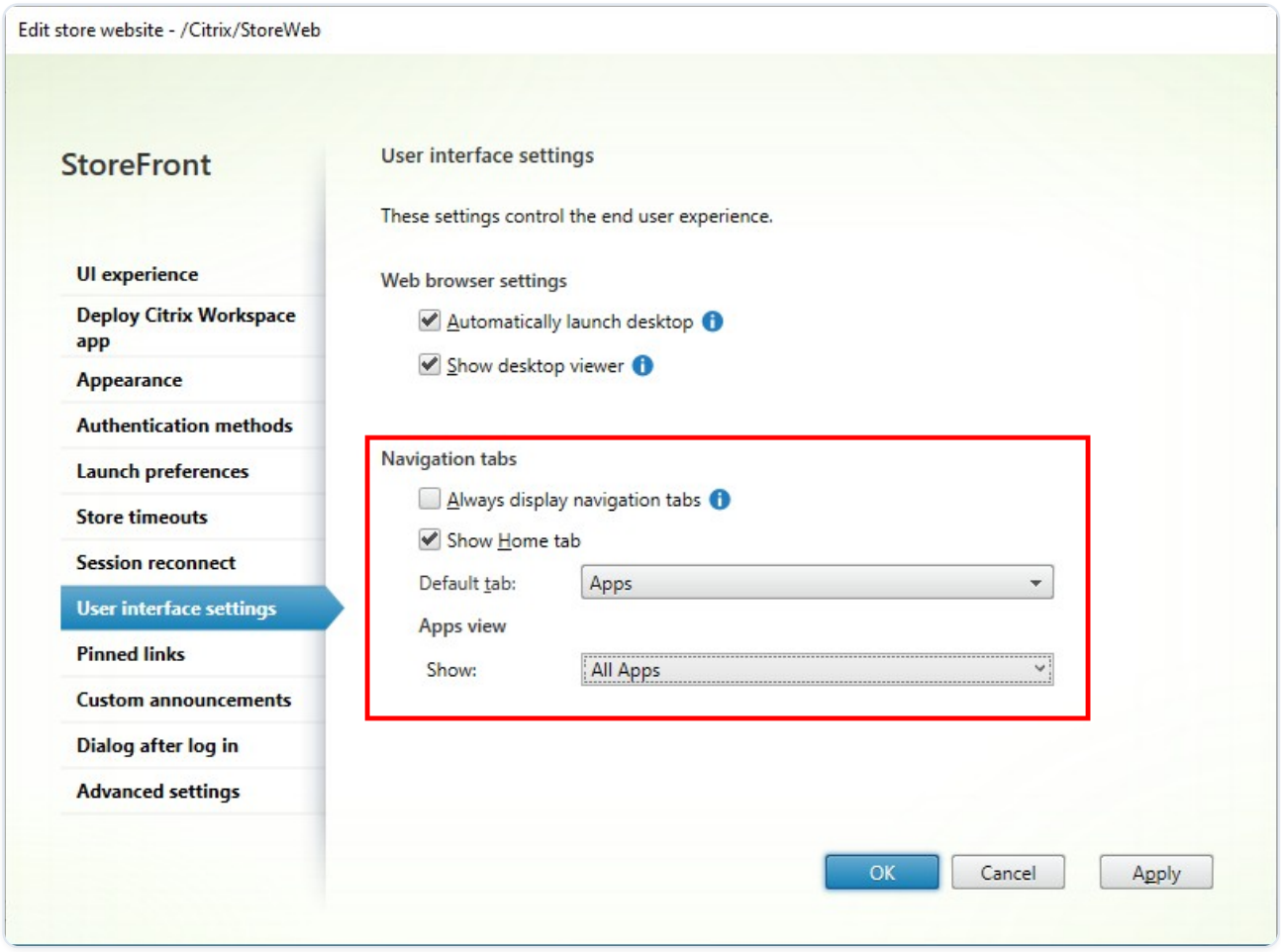


有关详细信息，请参阅更改密码。

使用现代体验增强导航和默认选项卡配置

使用现代体验时，管理员可以自定义最终用户导航选项卡。管理员可以配置以下选项：

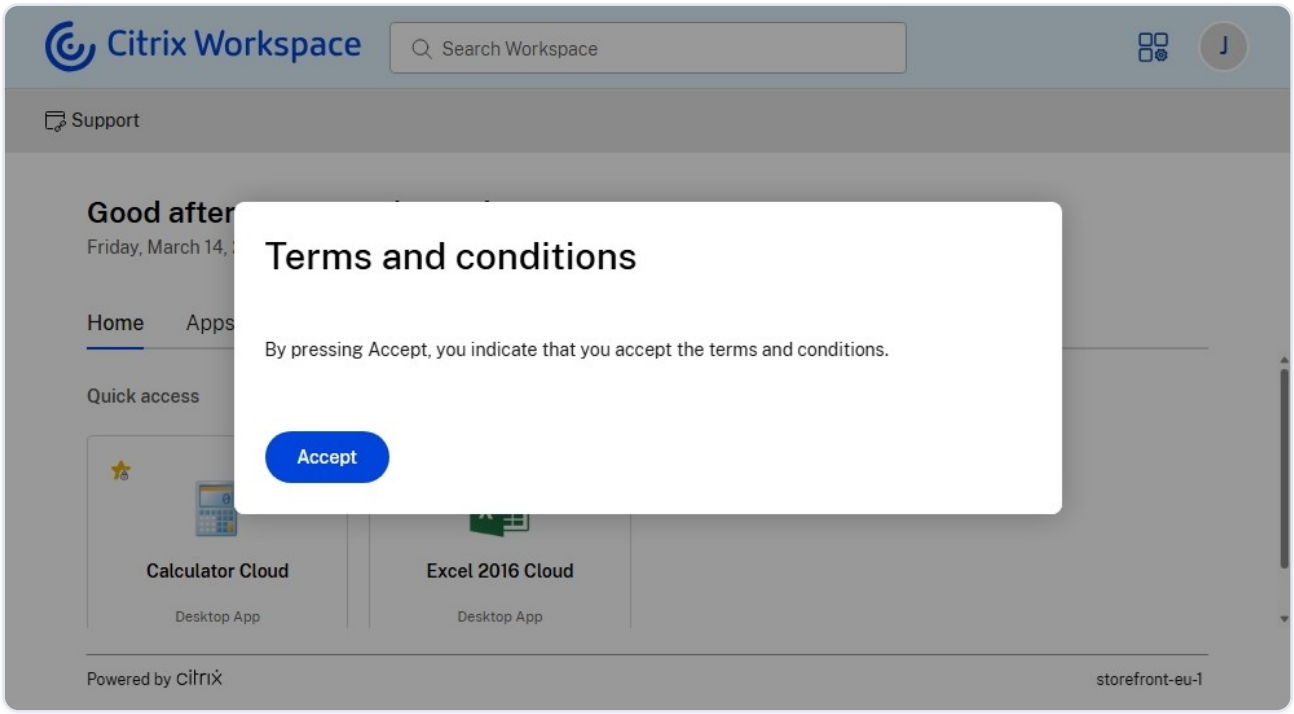
- 始终显示导航选项卡。
- 显示主页选项卡
- 默认选项卡



有关详细信息，请参阅导航选项卡

登录后显示对话框

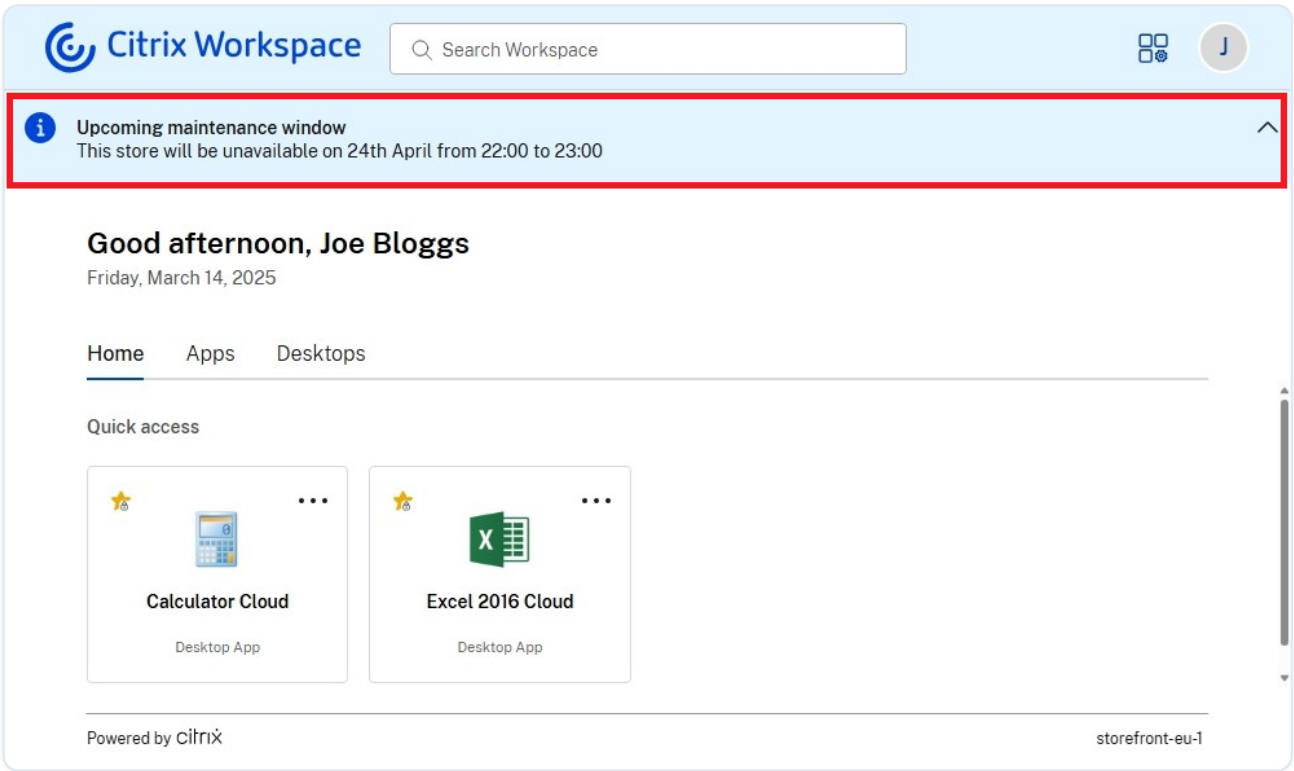
使用现代体验时，管理员可以配置一个弹出对话框，该对话框在用户登录后显示给最终用户，用户必须接受后才能与 StoreFront 交互。您可以使用此功能向用户告知重要信息，例如法规信息、策略确认、内部策略、指导内容、安全通知、系统更新和法律免责声明。此功能仅在使用现代体验时可用。



有关如何配置此功能的更多信息，请参阅登录后对话框。

自定义公告

使用现代体验时，管理员可以配置一个横幅，该横幅显示给最终用户，例如通知他们即将进行的更改或维护窗口。有关更多信息，请参阅自定义公告。



使用现代体验的会话重新连接

会话重新连接（以前称为 Workspace Control）现在在使用现代体验时可用。以前，它仅在使用经典体验时可用。通过会话重新连接，您可以为通过 Web 浏览器连接的用户配置以下设置：

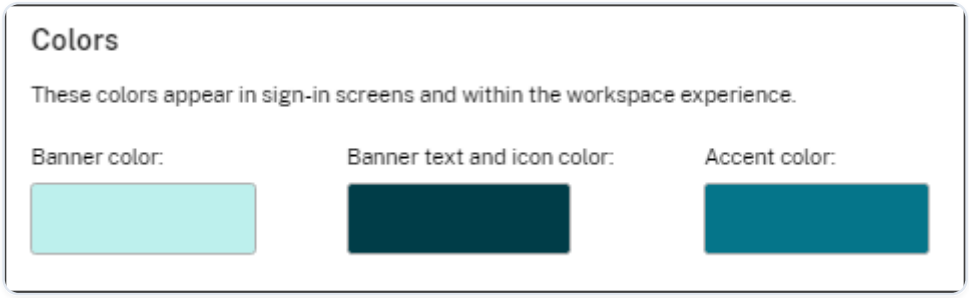
- 应用商店注销操作 - 是保持会话活动、断开会话连接还是注销会话。
- 用户登录时是否自动重新连接到会话。

有关更多信息，请参阅会话重新连接

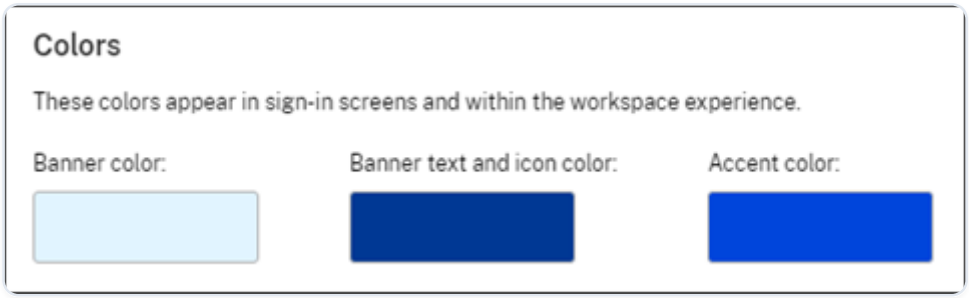
使用现代体验的颜色自定义

默认颜色已更新。

旧默认颜色：



新默认颜色：

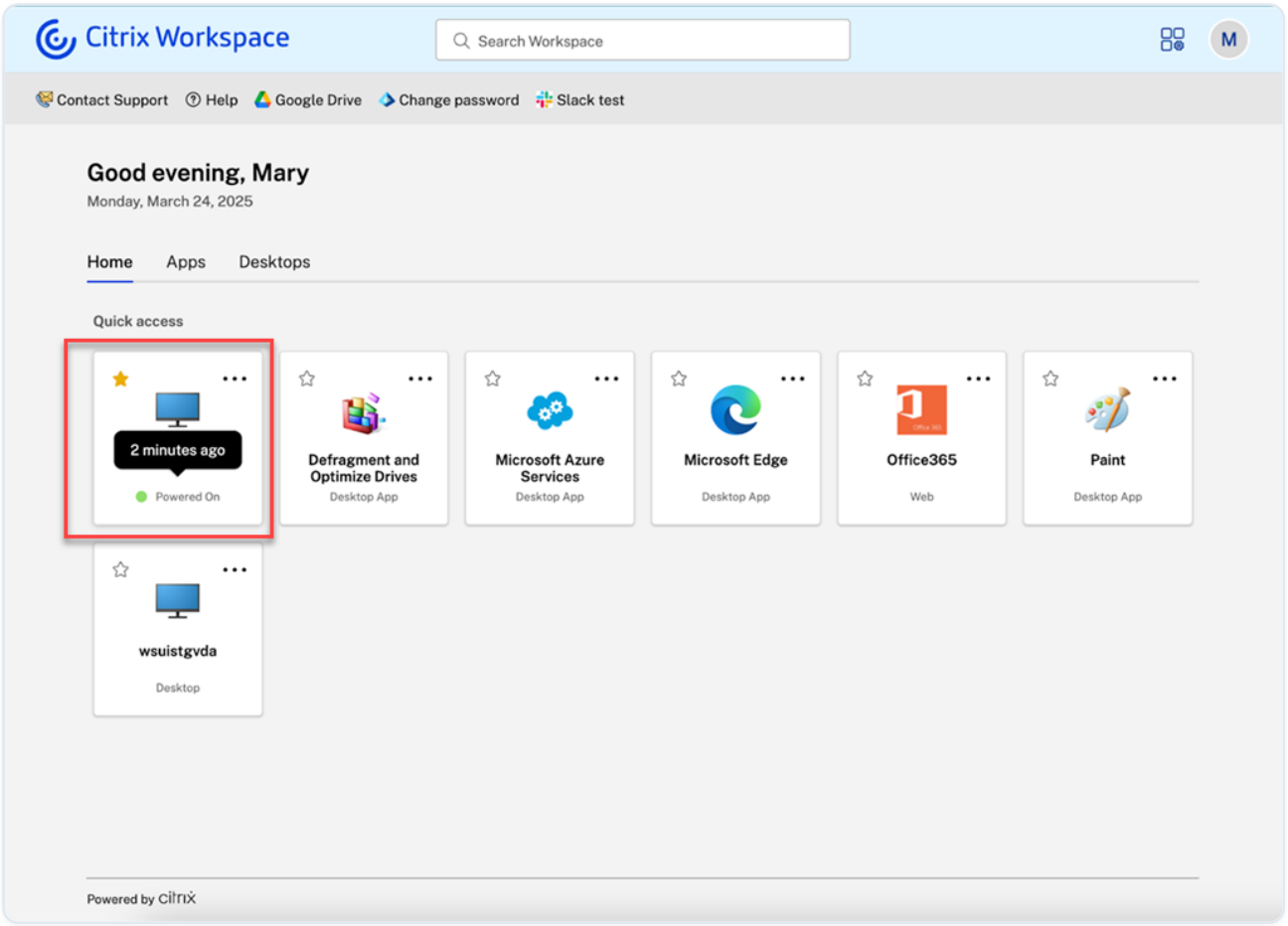


此外，颜色现在更一致地应用于按钮、链接和加载指示器。

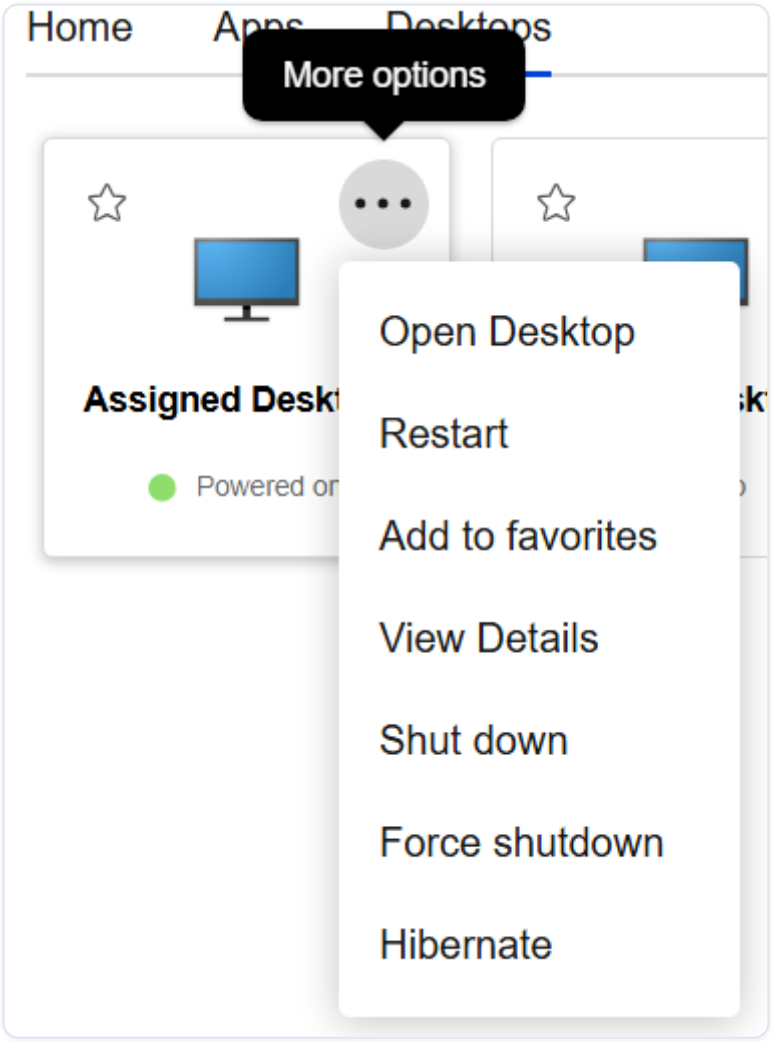
有关详细信息，请参阅外观。

显示已分配桌面的电源状态

最终用户界面现在在使用现代 DaaS 体验时，可显示用户已分配桌面的电源状态。电源状态指示已分配桌面是已开机、已关机还是处于挂起状态（休眠中）。此增强功能允许用户快速识别其桌面的状态，从而能够做出明智的决策并更有效地管理其资源。



用户可以使用“**更多**”选项菜单（省略号图标）直接从桌面磁贴执行电源相关操作。可用操作会根据桌面的当前电源状态动态变化。



有关详细信息，请参阅已分配桌面电源状态和磁贴操作。

注意：

- 此功能需要 Citrix DaaS。目前不适用于 Citrix Virtual Apps and Desktops。
- 对于启用了应用程序保护的桌面，不显示电源状态。
- 电源状态仅显示已分配桌面，不显示池化桌面。

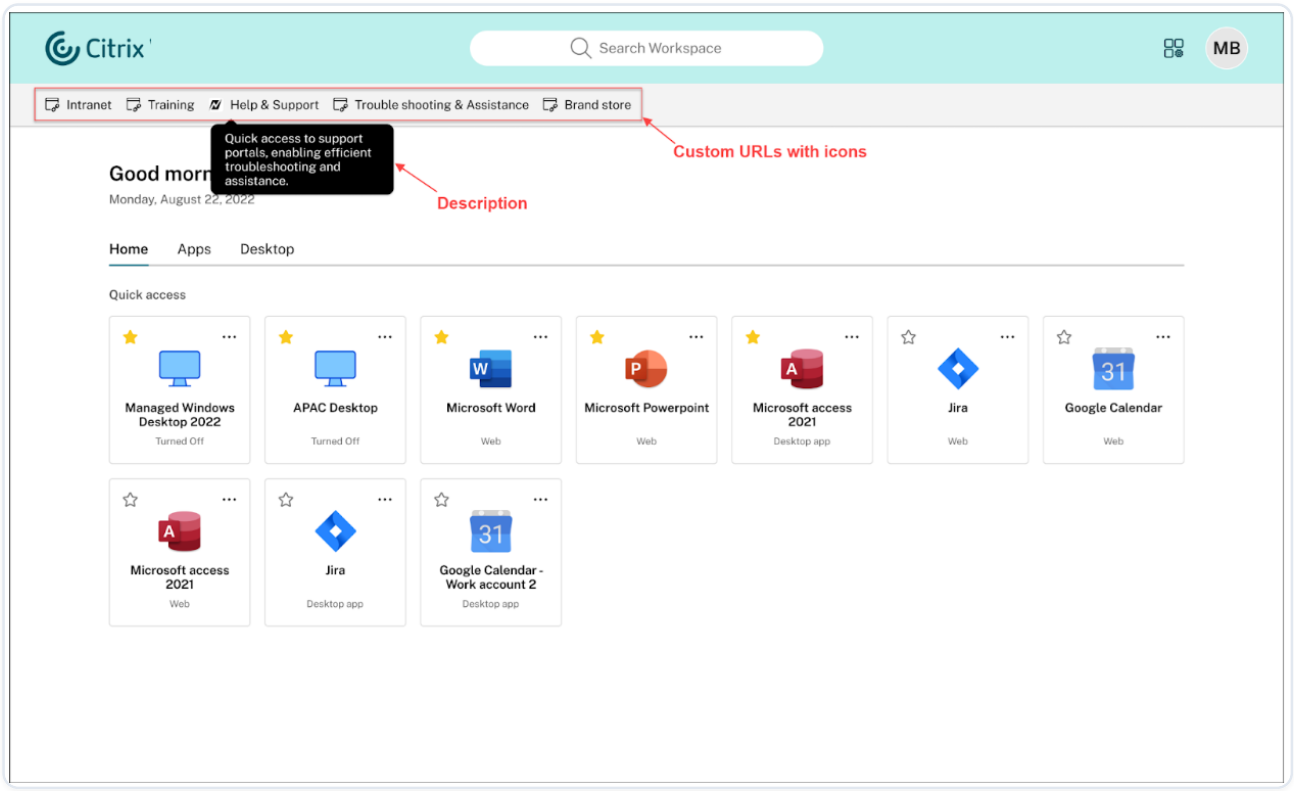
管理控制台中的术语已更新

管理控制台使用更新的术语。特别是以下内容已更新：

旧术语	新术语	备注
思杰接收器	Citrix Workspace 应用程序	Citrix Receiver 不再受支持，已被 Citrix Workspace app 取代。
HDX™ 引擎（插件）	Citrix Workspace 应用程序	HDX 客户端是 Citrix Workspace app 的一个组件。
Web 版接收器	网站	
统一体验	经典体验	在编辑网站时的“UI 体验”选项卡上。
下一代体验	现代体验	在编辑网站时的“UI 体验”选项卡上。
配置统一体验	设置 Citrix Workspace 应用程序网站	操作窗格上的链接。
交付控制器™	站点	这反映了每个实体都是一个站点，由多个交付控制器、DaaS 租户或 SPA 服务器组成。
工作区控制	会话重新连接	

固定链接

StoreFront UI 上的自定义 URL 是指客户定义的超链接，可提供对特定网站的快速访问。此功能充当快捷方式，帮助用户直接从 StoreFront UI 高效导航到网站。重要的链接，例如支持网站或公司门户，可以提供给用户，而无需他们搜索这些链接。这使得导航更轻松、更快捷。此功能仅在现代体验中可用。



有关详细信息，请参阅固定链接

要求最终用户仅使用本地安装的 Citrix 应用程序

管理员可以强制使用本机 Citrix Workspace 应用程序，从而消除用户在浏览器上访问 Citrix Workspace Web 客户端的选项。此功能专为希望充分利用本机应用程序优势的客户而设计。本机应用程序具有内置的应用程序保护服务、无浏览器版本兼容性问题、增强的安全性和用于监视和故障排除的遥测等优点。

有关详细信息，请参阅要求最终用户仅使用本地安装的 Citrix 应用程序

新建应用商店默认禁用 XenApp® Services

创建新应用商店时，XenApp Services 默认处于禁用状态。您可以在 GUI 中或使用 PowerShell 手动启用它。请注意，XenApp Services 已弃用，并将在未来版本中移除。

渐进式 Web 应用程序

Progressive Web App (PWA) 功能允许您安装商店网站，以便可以从您的开始菜单或桌面启动它，类似于本机应用程序。此功能仅在旧版 UI 中可用。有关详细信息，请参阅 Progressive Web App

Citrix 许可遥测

StoreFront 收集有关用户登录和您的配置的遥测数据。有关详细信息，请参阅 Citrix 许可数据收集程序。

适用于 StoreFront 的 Citrix Gateway Service

适用于 StoreFront 的 Citrix Gateway Service 提供 HDX 路由到您的资源，而无需托管您自己的网关。有关详细信息，请参阅 适用于 StoreFront 的 Gateway Service 和 添加 Citrix Gateway Service 。

如果您已选择将 适用于 StoreFront 的 Citrix Gateway Service（技术预览版） 与 StoreFront 2311 或 2402 结合使用，并且已配置 CloudGateway，则该配置在 StoreFront 2507 中不再有效。您必须删除现有网关并按照更新的文档创建新网关。

Citrix Web 扩展

Citrix Web 扩展 已为所有安装启用，无需使用 PowerShell 手动配置 StoreFront。

对 Windows Server 2025 的支持

StoreFront 2407 可以安装在 Windows Server 2025 Datacenter 和 Standard 版本上。

取消对 Windows Server 2016 的支持

StoreFront 2407 无法安装在 Windows Server 2016 上。请将 StoreFront 安装在 Windows Server 2019、2022 或 2025 上。有关已删除项目的更多信息，请参阅 弃用通知。

已修复的问题

此版本包含自 2402 CU2 以来的以下修复：

- 在管理控制台 > 管理身份验证方法屏幕中，如果您清除除 HTTP Basic 之外的所有身份验证方法，当您按“确定”保存更改时，将出现错误。
- 当您将“**启动选项**”更改为“**在 Citrix Workspace 应用程序中打开**”并保存更改时，StoreFront 可能会显示错误。当服务器上安装的 HTML5 HDX 版本与当前 StoreFront 版本默认安装的版本不同时，会发生此错误。
- 配置自定义公告时，可能会输入过长的标题和描述，导致显示不正确。
- 将 StoreFront 服务器添加到服务器组时，新服务器的 `Citrix Receiver for Web` 应用程序池会设置为定期回收，这可能会导致用户意外注销。通过此修复，应用程序池将设置为在 01:00 到 03:55 之间回收，以避开工作时间。
- 在非英语系统上安装 StoreFront 时，会记录多个遥测异常事件
- StoreFront 管理控制台引用了过时的术语“Unified Experience”。
- PowerShell 命令 `Get-STFWebReceiverSiteStyle` 可能会因错误 `Value cannot be null` 而失败。

- PowerShell 命令 `Set-STFWebReceiverSiteStyle` 可能会因错误 `Value cannot be null` 而失败。
- 网站“**外观**”选项卡上的更改可能无法正确保存。
- PowerShell 命令 `Set-STFWebReceiverSiteStyle` 会将未指定的参数重置为默认值，而不是保留其现有值。
- 当 Cloud Connector 在 LHC 模式下运行，并且用户尝试启动可从多个位置访问的资源时，如果资源未立即可用，会话可能会启动失败。出现此问题的原因是，在检查资源就绪状态后，StoreFront 可能会将请求发送到与最初用于启动资源的连接器不同的连接器。
- StoreFront 选择 FAS 服务器后，如果该 FAS 服务器后来变得不可用，则启动会失败。通过此修复，StoreFront 将改为选择不同的 FAS 服务器，从而允许启动继续进行。
- 如果 FAS 服务器无响应，StoreFront 会继续尝试联系每个用户，从而增加登录或启动时间（具体取决于配置）。通过此修复，当 FAS 服务器无响应时，StoreFront 会在一段时间内避免尝试使用同一服务器，这样后续用户就不会受到延迟的影响。
- 启用套接字池时，StoreFront 可能会显示高内存使用率和端口耗尽，导致服务不可用。
- 升级到新版本的 StoreFront 失败，日志中包含文本“VersionData:Load Failed due to exception: System.IndexOutOfRangeException”。当 StoreFront 创建的用户组的描述为空时，会出现此问题。
- StoreFront 升级间歇性失败。安装程序可能在向导出现之前静默失败，或者向导无响应，或者在单击向导后升级失败。出现此问题的原因是安装文件在需要之前被删除。
- 升级失败，并显示消息“There was an error adding user accounts in the Administrators local group to the CitrixStorefrontAdministrators local group”或类似消息。当 StoreFront 使用的用户组包含已删除的用户时，会出现此问题。
- 在中断期间，当连接器进入本地主机缓存模式时，StoreFront 需要将启动请求发送到与资源位于同一区域的连接器。当资源在多个区域中可用时，以前 StoreFront 只会尝试在一个区域中启动资源。通过此增强功能，如果在一个区域中启动资源的尝试失败，在某些情况下 StoreFront 服务器会尝试使用其他可用区域中的连接器再次尝试启动资源，以提高弹性。
- 连接到 StoreFront 2402 并使用 XenApp Services URL 时，移除在 Citrix Workspace app for Windows 2309 或更高版本中显示的额外通知 。
- 在 StoreFront Web API 中，列表端点应根据是否启用了收藏夹来设置 `isSubscriptionEnabled`。
- 在 Store Services API 中，资源枚举 端点应根据是否启用了收藏夹来设置订阅状态。
- 升级 StoreFront 后，您可能会注意到自定义文件夹 (`\StoreWeb\custom`) 中的自定义文件副本在升级过程完成后也可能出现在网站文件夹的根目录 (`\StoreWeb`) 中。

- 当使用 Citrix Gateway Service 并选择“**在可用时从两个云连接器请求票证**”时，只颁发一张票证。
- 当您将启动选项从“**在 Citrix Workspace app 中打开**”更改为“**让用户选择**”或“**在 Web 浏览器中打开**”并选择“**确定**”时，可能会出现错误“**在‘启动首选项’属性对话框上保存更改时发生错误。请检查事件查看器中的日志并重试。**”如果 HTML5 HDX 客户端意外地已安装，则会发生此情况。

经典 UI 体验的修复：

- 当“**启动选项**”设置为“**让用户选择**”时，“**欢迎使用 Citrix Workspace app**”屏幕显示文本“**undefined**”。
- 禁用“**允许用户跳过 Citrix Workspace app 检测**”后，以前跳过 Citrix Workspace app 检测的用户不受影响。通过此修复，此类用户下次打开应用商店网站时，需要完成 Citrix Workspace app 检测。
- 使用 Microsoft Edge 时，下载 Citrix Workspace app 后，缺少有关如何启动 Citrix Workspace 启动器的说明。
- 使用 Safari 时，在 Citrix Workspace app 检测屏幕上，缺少打开 Citrix Workspace 启动器的说明。
- 当“**启动选项**”设置为“**让用户选择**”且已安装 Citrix Web 扩展并检测到 Citrix Workspace app 时，无法将启动方法更改为在 Web 浏览器中打开资源。
- 当 Citrix Web 扩展成功检测到 Citrix Workspace app 后，应从设置页面隐藏“**下载 Citrix Workspace app**”的链接。
- 用户首次访问网站一年后，自动启动桌面功能失效。
- 内容安全策略应包含 `default-src: none`。
- 如果在检测到 Citrix Workspace 应用程序 后禁用/移除 Citrix Web 扩展，UI 会挂起。
- 使用非英语语言时，版权符号显示不正确。
- 在设置屏幕上，指示是否将使用 Citrix Workspace Web 扩展启动应用程序和桌面。
- 某些 Cookie 未设置 `SameSite`。通过此更改，所有 Cookie 的 `SameSite` 都设置为 `Lax`。
- 在使用巴西葡萄牙语的 Mozilla Firefox 时，更新客户端检测屏幕上的翻译。
- 更新了 HTML 文件 **http-equiv** 标签中定义的内容安全策略，以阻止内联脚本。如果您以使用 eval 或向 DOM 添加内联脚本的方式自定义了 StoreFront，则此操作会导致这些自定义失败。

现代 UI 体验的修复：

- 在 macOS 上使用安装了 Citrix Web 扩展的 Google Chrome 时，会话重新连接可能无法工作。
- 如果用户没有任何桌面，则应隐藏桌面选项卡。

- 在休眠资源的桌面磁贴上，**恢复**选项不可用。
- 当用户尝试从活动管理器重新启动桌面时，会收到错误“**无法重新启动桌面**”。
- 资源筛选规则不应应用于由**活动管理器**列出的会话。
- 在移动设备上，搜索栏旁边的**取消**按钮应为黑色而不是蓝色。
- 当所有资源都需要应用程序保护且用户选择在浏览器中启动时，连接到 Citrix Workspace 应用程序的选项不可用。
- 在休眠的持久桌面磁贴上，菜单不包含恢复桌面的选项。。
- 现代体验无法在适用于 Linux 的 Citrix Workspace 应用程序上加载
- 允许活动管理器处理比可同时枚举的站点更多的站点。

已知问题

- 在 iOS 上使用 Safari 时，完成 Citrix Workspace 应用程序检测并返回 Safari 后，网页可能会卡在加载屏幕上。为解决此问题，用户必须刷新网页。
- 在管理控制台外观选项卡上，“重置为默认值”按钮不起作用。
- StoreFront 管理控制台不显示以前上传的徽标。
- 如果 StoreFront 具有 Citrix Gateway Service 类型的网关，则在从 StoreFront 2407 或 2411 升级到 2507 时，使用该网关启动可能会失败。在网关配置窗口的“云连接器”选项卡上，云连接器错误地包含端口 8090，导致 StoreFront 无法访问云连接器以请求 STA 票证。要解决此问题，请从列表中每个云连接器的 URL 中删除端口。

入门

先决条件

1. 规划您的 StoreFront 部署
2. 安装并配置您希望 StoreFront 聚合的资源提供程序：
   - Citrix 虚拟应用和桌面
   - 思杰 DaaS
   - 安全私有访问。

   有关优化配置资源的更多信息，请参阅配置资源。
3. 查看系统要求并确保您具备安装 StoreFront 的先决条件。

部署 StoreFront

要创建您的 StoreFront™ 部署，请完成以下步骤：

1. 安装 StoreFront到新服务器上。
2. 创建新部署以及您的第一个应用商店。
3. 确定用户将如何访问应用商店。

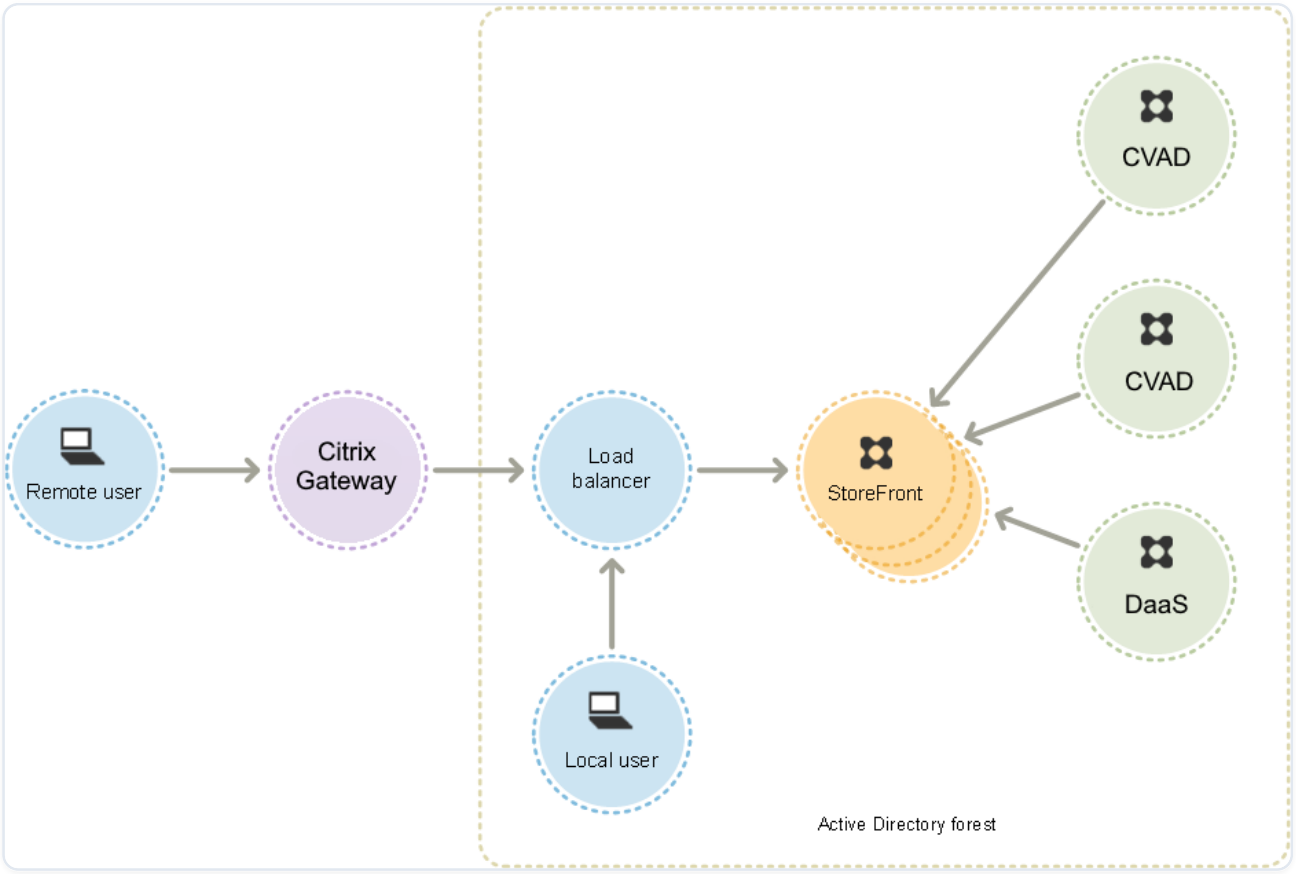
优化您的部署

1. 为了实现冗余和可伸缩性，请部署负载平衡器并将更多服务器添加到StoreFront 服务器组。
2. 保护您的部署安全。
3. 优化最终用户体验。
4. 使用Citrix Gateway启用远程访问。

规划您的 StoreFront 部署

StoreFront 与您的 Citrix Virtual Apps and Desktops 部署集成，为用户提供一个用于访问其桌面和应用程序的单一自助服务访问点。

该图显示了典型的 StoreFront 部署。



活动目录

StoreFront 使用 Active Directory 进行用户身份验证、查找组成员身份和其他详细信息，以及在 StoreFront 服务器之间同步数据。

对于单服务器部署，您可以在未加入域的服务器上安装 StoreFront，但某些功能将不可用；否则，StoreFront 服务器必须位于包含用户帐户的 Active Directory 域中，或者位于与用户帐户域具有信任关系的域中，除非您启用将身份验证委派给 Citrix Virtual Apps and Desktops 站点或场。组中的所有 StoreFront 服务器必须位于同一域中。

StoreFront 服务器组

StoreFront 可以配置为单服务器部署，也可以配置为多服务器部署，称为 StoreFront 服务器组。服务器组不仅提供额外的容量，还提供更高的可用性。StoreFront 确保配置信息和用户应用程序订阅的详细信息存储在服务器组中的所有服务器上并进行复制。这意味着，如果 StoreFront 服务器因任何原因变得不可用，用户可以使用其余服务器继续访问其应用商店。同时，当故障服务器重新连接到服务器组时，其配置和订阅数据会自动更新。订阅数据在服务器重新联机时更新，但如果服务器在脱机期间错过了任何配置更改，则必须传播这些更改。如果发生需要更换服务器的硬件故障，您

可以在新服务器上安装 StoreFront 并将其添加到现有服务器组。新服务器在加入服务器组时会自动配置并更新用户的应用程序订阅。

Citrix® 建议服务器组中最多包含六台服务器。如果服务器数量超过六台，数据同步的开销将超过额外服务器带来的好处，并且性能会下降。

StoreFront 服务器组部署仅在服务器组中服务器之间的链接延迟小于 40 毫秒（禁用订阅时）或小于 3 毫秒（启用订阅时）的情况下受支持。理想情况下，服务器组中的所有服务器都应位于同一位置（数据中心、可用区），但只要组中服务器之间的链接满足这些延迟标准，服务器组就可以跨同一区域内的不同位置。示例包括跨云区域内的可用区或跨大都市数据中心的服务器组。请注意，区域之间的延迟因云提供商而异。Citrix 不建议将跨位置作为灾难恢复配置，但它可能适用于高可用性。

负载平衡

对于 StoreFront 服务器组中的多台服务器，您必须配置外部负载平衡。使用具有内置监视器和会话持久性的负载平衡器，例如 NetScaler ADC。有关使用 NetScaler ADC 进行负载平衡的更多信息，请参阅 负载平衡。

用于远程访问的 Citrix Gateway

如果您计划从公司网络外部启用对 StoreFront 的访问，则需要 Citrix Gateway 为远程用户提供安全连接。将 Citrix Gateway 部署在公司网络外部，并使用防火墙将 Citrix Gateway 与公共网络和内部网络隔离开来。确保 Citrix Gateway 能够访问包含 StoreFront 服务器的 Active Directory 林。

全局服务器负载平衡器

在大型 Citrix 部署中，您可能在多个数据中心拥有 StoreFront 和 NetScaler 部署。使用全局服务器负载平衡器 (GSLB)，您可以配置一个全局 URL，GSLB 会将其重定向到其中一个区域中网关的特定 URL。通常，GSLB 会根据负载平衡算法（例如往返时间 (RTT) 或静态邻近度）选择最近的网关。

例如，您可能有 3 个区域网关：

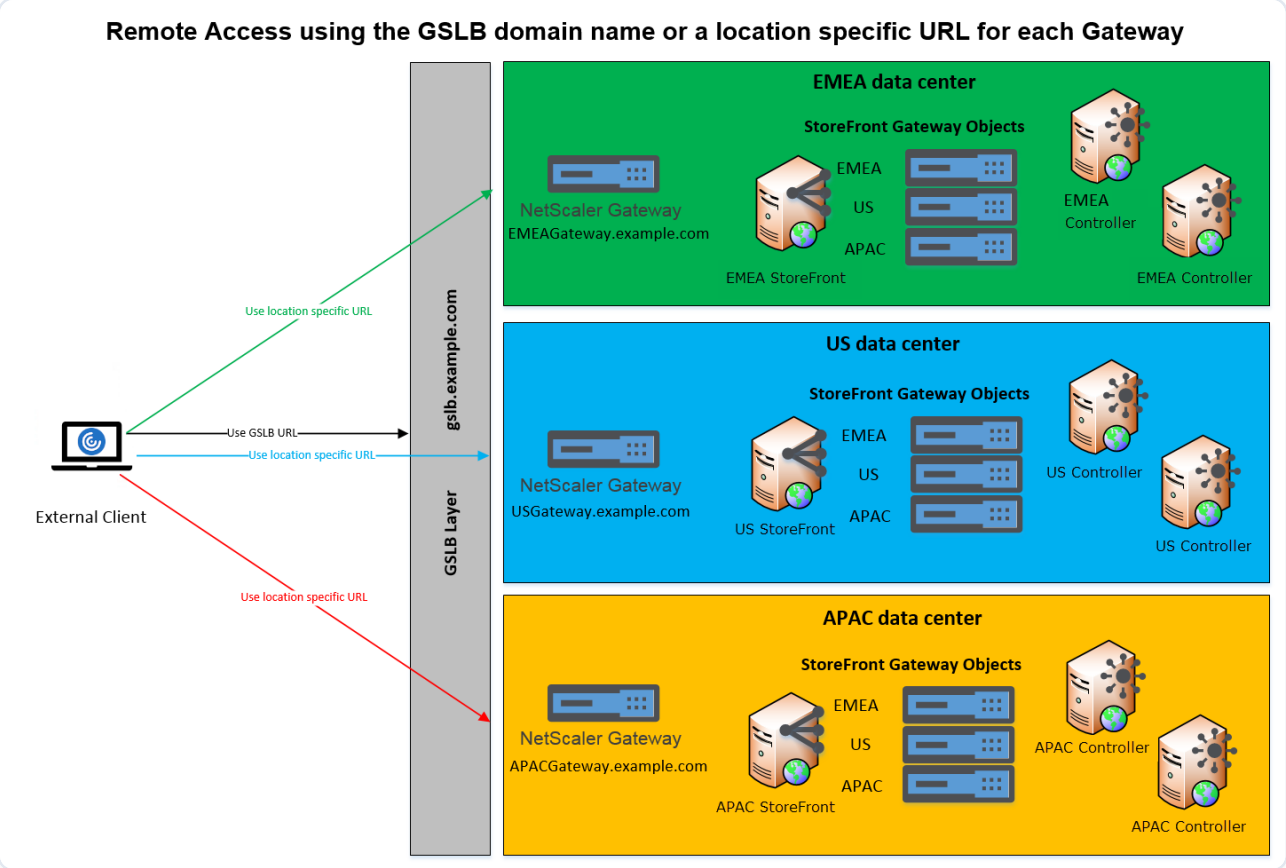
`emeagateway.example.com` - 欧洲网关

`usgateway.example.com` - 美国网关

`apacgateway.example.com` - 亚太网关

以及一个 GSLB：

`gslb.example.com`



在配置 GSLB 之前，请检查您已有的服务器证书以及您的组织如何执行 DNS 解析。您希望在 Citrix Gateway 和 StoreFront 部署中使用的任何 URL 都必须存在于您的服务器证书中。

StoreFront 没有内置机制来同步服务器组之间的配置；相反，管理员需要确保每个 StoreFront 服务器组都以相同的方式配置，以便用户无论连接到哪个服务器组都能获得一致的体验。

StoreFront 可以定期同步服务器组之间的订阅（收藏夹），请参阅 订阅同步。

当您将应用商店添加到 Citrix Workspace 应用程序时，它会通过基本 URL 和应用商店名称来识别应用商店。因此，如果您在 GSLB 后面有多个 StoreFront 部署，那么每个部署都必须具有相同的 基本 URL。

> **注意：**
>
> 当 Citrix Workspace 应用程序在 GSLB 后面的不同 StoreFront 部署之间漫游时，用户需要重新进行身份验证。因此，您应该配置持久性，以便在可能的情况下，用户的请求始终路由到相同的部署。

用户访问

请参阅 用户访问选项。

系统要求

在安装 StoreFront 之前，请查看 规划您的 StoreFront 部署。

StoreFront 服务器要求

软件

Citrix 已在以下平台上测试并支持 StoreFront 安装：

- Windows Server 2025 数据中心版和标准版
- Windows Server 2022 数据中心版和标准版
- Windows Server 2019 数据中心版和标准版

> **注意：**

> StoreFront 需要 Windows 桌面体验，因此无法安装在 Windows Server Core 上。

> 服务器组中的所有 StoreFront 服务器必须使用相同的操作系统版本、语言和区域设置。

不支持升级运行 StoreFront 的服务器上的操作系统版本。Citrix 建议您在新安装的操作系统上安装 StoreFront。

在安装 StoreFront 之前，必须在 Web 服务器上启用以下 Windows 功能。这些组件在新 Windows 安装中默认启用，因此除非已明确卸载，否则无需执行任何操作。

- NET-Framework-45 功能
  - .NET 框架 4.5 核心
- PowerShellRoot
  - PowerShell

如果安装的 .NET Framework 版本早于 4.8.0，安装程序会自动安装 .NET Framework 4.8.0。这要求已安装 **NET-Framework-45-Core** Windows 功能。

```
Starting with 2507 LTSR CU2, StoreFront requires .NET 10. If .NET 10 is
not already installed, the installer automatically installs it.
```

```
> **Note:**

>

> Earlier StoreFront builds (that is, 2507 and 2507 LTSR CU1) require .NET
8.
```

如果 StoreFront 安装程序检测到以下任何 Windows 功能缺失，它们将自动安装：

- Web 服务器
  - Web 服务器
    - 常见 HTTP 功能
      - 默认文档
      - HTTP 错误
      - 静态内容
      - HTTP 重定向
    - 运行状况
      - HTTP 日志记录
    - 安全性
      - 请求筛选
      - 基本身份验证
      - Windows 身份验证
    - 应用程序开发
      - .NET 扩展性 4.5
      - Web-AppInit
      - Web-Asp-Net45 功能
      - Web-ISAPI-扩展
      - Web-ISAPI-筛选器
    - Web-管理工具

        - Web-管理控制台
    - Web-脚本工具
- .NET Framework 4.5 功能
    - .NET 框架 4.5 ASP.NET 技术
    - .NET WCF 服务 4.5
        - NET-WCF-TCP-PortSharing45

在安装 StoreFront 之前，可以将 IIS 网站移动到不同的目录或驱动器。在服务器组中的所有服务器上，IIS 中 StoreFront 的相对路径必须相同。

硬件

Storefront™ 服务器必须满足以下要求：

- 处理器：最少 2 个虚拟 CPU，建议 4 个虚拟 CPU
- RAM: 4GB，加上每个用户每个可用资源 700 字节。
- 存储空间：
    - StoreFront 本身需要 250MB。
    - 每个应用商店 30MB，假设每个应用商店一个网站。
    - 对于每个启用了收藏夹的应用商店，需要 5MB，外加每 1000 个收藏夹 8MB。
    - 根据您的要求，为 IIS 日志文件提供足够的空间，请参阅 Microsoft 关于管理 IIS 日志文件存储的文档。
    - 为 StoreFront 诊断日志提供足够的空间。默认情况下，StoreFront 为每个服务保留 1GB 日志。StoreFront 部署通常有 1 个漫游服务以及每个应用商店 3 个服务（应用商店服务、身份验证服务和 Web 版 Receiver 服务）。有关详细信息，请参阅 日志文件。

网络

StoreFront 使用以下端口进行通信。请确保您的防火墙和其他网络设备允许访问这些端口。

- 客户端使用 HTTPS 或 HTTP 连接到 StoreFront，通常分别通过 TCP 端口 443 或 80。您可以允许客户端直接连接到 StoreFront，但通常客户端会连接到负载均衡器或网关，由其将流量转发到 StoreFront。您可以在 IIS 配置中修改所使用的端口。建议您使用 HSTS 强制 Web 浏览器使用 HTTPS。
- TCP 端口 808 用于：

  - 同步服务器组内的收藏夹。这仅适用于启用了收藏夹且您使用的是本地数据库而非外部 SQL Server 数据库的情况。
  - 同步服务器组之间的订阅。这仅适用于您已启用 同步订阅 的情况。

- 从所有未保留端口中随机选择一个 TCP 端口，用于服务器组中 StoreFront 服务器之间的通信。
- 如果您正在使用带有 StoreFront 监视器的 NetScaler 负载均衡器，它需要连接到 Citrix 服务监视器。默认情况下，此监视器在 TCP 端口 8000 上运行，但也可以配置为通过 HTTPS 在端口 443 上运行。请参阅 使用 NetScaler ADC 进行负载均衡。

安装 StoreFront 时，会配置 Windows 防火墙规则以允许访问 StoreFront 可执行文件。您必须确保内部网络上的任何防火墙或其他设备不会阻止流向任何未分配 TCP 端口的流量。

StoreFront 支持纯 IPv6 网络和双栈 IPv4/IPv6 环境。

活动目录

许多 StoreFront 功能要求安装 StoreFront 的 Windows 服务器加入 Active Directory 域。StoreFront 不能安装在域控制器上。

要使 StoreFront 针对 Microsoft Active Directory 对用户进行身份验证，请确保 StoreFront 服务器已加入包含用户帐户的域，或与用户帐户域具有信任关系的域。这对于 域直通 始终是必需的。对于 用户名和密码 身份验证，这是默认要求，或者您可以配置 StoreFront 将身份验证委托给交付控制器。

如果您在未加入域的服务器上安装 StoreFront，则以下功能不可用：

- 服务器组
- 收藏夹
- 除显式用户名和密码之外的身份验证方法，无论是直接连接到 StoreFront 还是通过网关。您必须配置 StoreFront 将身份验证委托给交付控制器。

使用 Microsoft SQL Server 存储订阅数据

您可以选择 使用 Microsoft SQL Server 存储订阅数据。StoreFront 支持与 Citrix Virtual Apps and Desktops 用于数据库的 Microsoft SQL Server 版本相同。在 Citrix Virtual Apps and Desktops 系统要求中，请参阅 数据库。

基础架构要求

Citrix 已测试并支持 StoreFront 与以下 Citrix 产品版本一起使用。

Citrix 虚拟应用和桌面™

StoreFront 支持以下版本的 Citrix Virtual Apps and Desktops：

- 思杰虚拟应用和桌面 2507 LTSR
- 思杰虚拟应用和桌面 2503
- 思杰虚拟应用和桌面 2411
- 思杰虚拟应用和桌面 2407
- 思杰虚拟应用和桌面 2402 LTSR
- 思杰虚拟应用和桌面 2203 LTSR

思杰 Gateway

以下版本的 Citrix Gateway 可用于为公共网络上的用户提供对 StoreFront 的访问。

- 思杰网关 14.1
- 思杰网关 13.1

通过 Citrix Gateway 的连接可以使用 ICA 代理、Citrix Gateway 插件或无客户端 VPN (cVPN) 进行。

用户设备要求

StoreFront 为用户提供了多种访问其桌面和应用程序的选项。Citrix 用户可以通过本地安装的 Citrix Workspace 应用程序访问应用商店，也可以在其浏览器中访问。有关详细信息，请参阅用户访问选项。

Citrix Workspace 应用程序

您可以使用所有当前支持的 Citrix Workspace 应用程序版本，通过内部网络连接和 Citrix Gateway 访问 StoreFront 应用商店。有关 Citrix Workspace 应用程序生命周期日期，请参阅 `<https://www.citrix.com/support/product-lifecycle/workspace-app.html>`。

旧版本的 Citrix Workspace™ 应用程序和 Citrix Receiver™ 可能可以工作，但不受支持。

在 Android、iOS 和 iPadOS 上，如果使用早于 24.12 版本的 Citrix Workspace 应用程序，则无法通过网关连接到配置了现代体验的应用商店。

Web 浏览器

最终用户可以使用 Web 浏览器访问应用商店。应用程序和桌面可以通过本地安装的 Citrix Workspace 应用程序（称为混合启动）或在 Web 浏览器中启动。根据您的网站配置，最终用户可以在两种启动方法之间切换。

使用以下浏览器的最新版本。

在 Windows 上：

- 微软 Edge
- 谷歌 Chrome
- 火狐浏览器
- Internet Explorer 浏览器 11*

* Internet Explorer 可用于连接配置为使用经典体验而非现代体验的 Store 网站。HTML5 HDX 客户端不支持 Internet Explorer，因此您必须使用 Citrix Workspace 应用程序连接到资源。

在 Mac 上：

- Safari 浏览器
- 谷歌 Chrome
- 火狐浏览器

在 Linux 上：

- 谷歌 Chrome
- 火狐浏览器

有关使用适用于 HTML5 的 Citrix Workspace 应用程序通过 Web 浏览器连接到资源的更多信息，请参阅 适用于 HTML5 的 Citrix Workspace 应用程序文档。

Citrix Web 扩展

为了获得更好的体验，建议用户将 Citrix Web 扩展添加到其 Web 浏览器。有关要求，请参阅 Citrix Web 扩展。

旧版设备

旧版 Citrix 客户端可以使用 XenApp Services URL 访问功能受限的 StoreFront 商店。XenApp Services URL 为 Citrix Receiver 3.4 Enterprise 及更早版本客户端建立的连接提供向后兼容的旧版支持。此功能已弃用，并将在未来的版本中移除。

智能卡要求

将 Citrix Workspace 应用程序与智能卡结合使用

Citrix 测试了与美国国防部通用访问卡 (CAC)、美国国家标准与技术研究院个人身份验证 (NIST PIV) 卡以及某些 USB 智能卡令牌的兼容性。您可以使用符合 USB 芯片/智能卡接口设备 (CCID) 规范并被德国中央信贷委员会 (ZKA) 归类为 1 类智能卡读卡器的接触式读卡器。ZKA 1 类接触式读卡器要求用户将智能卡插入读卡器。不支持其他类型的智能卡读卡器，包括 2 类读卡器（带有用于输入 PIN 的键盘）、非接触式读卡器以及基于可信平台模块 (TPM) 芯片的虚拟智能卡。

对于 Windows 设备，智能卡支持基于 Microsoft 个人计算机/智能卡 (PC/SC) 标准规范。作为最低要求，智能卡和读卡器必须受操作系统支持并已获得 Windows 硬件认证。

有关 Citrix 兼容智能卡和中间件的更多信息，请参阅 Citrix Virtual Apps and Desktops 文档中的智能卡，以及 `<http://www.citrix.com/ready>`。

Citrix Analytics 服务要求

您可以配置 Citrix StoreFront，以便 Citrix Workspace 应用程序可以将数据发送到 Citrix Analytics 服务。配置详细信息在Citrix Analytics 服务中进行了描述。此功能支持以下场景：

- 通过 Web 浏览器访问的 Store。
- 通过适用于 Windows 的 Citrix Workspace 应用程序 1903 或更高版本访问的 Store。
- 通过适用于 Linux 的 Citrix Workspace 应用程序 1901 或更高版本访问的 Store。

配置资源

当使用 Citrix Virtual Apps and Desktops、Citrix Desktops as a Service 或 Secure Private Access 交付资源时，配置资源时请考虑以下事项。有关使用 Citrix Virtual Apps and Desktops 交付应用程序的更多信息，请参阅 应用程序。

- 输入您希望资源在您的应用商店中显示的名称。
- （可选）输入描述。展开应用程序详细信息时，此描述会与任何 关键字 一起显示在应用商店中。
- 选择一个图标，以帮助用户在 StoreFront 网站上直观地识别应用程序。
- （可选）输入类别。在类别名称中包含 `\` 以创建文件夹层次结构。例如，您可以根据类型对应用程序进行分组，或者为组织中的不同用户角色创建文件夹。在应用商店网站的“**应用程序**”选项卡中，“**类别**”视图会显示类别列表以及每个类别中的应用程序。

关键字

您可以通过将字符串 `KEYWORDS:[keywordname]` 附加到应用程序描述来为资源添加关键字。多个关键字之间只能用空格分隔；例如，`KEYWORDS:Accounts Featured`。关键字可以通过多种方式使用：

- 筛选应用程序 - 请参阅 高级应用商店设置。
- 创建 特色应用程序组。
- 某些关键字具有特殊含义。

关键字名称	描述
强制	将应用程序添加到“主页”选项卡。与收藏夹不同，用户无法从“主页”选项卡中删除强制性应用程序。如果为应用商店禁用了收藏夹，则此操作无效。
自动	当用户登录到应用商店时，应用程序或桌面会自动收藏并添加到其“主页”选项卡。用户可以取消收藏此类应用程序。如果为应用商店禁用了收藏夹，则此操作无效。
TreatAsApp	适用于桌面，强制 StoreFront 将其视为应用程序。桌面显示在“**应用程序**”选项卡而不是“**桌面**”选项卡上。此外，即使站点配置为对其他桌面执行此操作，当用户登录到应用商店网站时，桌面也不会自动启动，并且不会通过 Desktop Viewer 访问。
偏好="*应用程序*"	其中 *application* 标识本地安装的应用程序。仅适用于 Windows 上 Citrix Workspace 应用程序中的已发布应用程序。这表示如果本地安装的应用程序版本和等效的交付实例都可用，则应优先使用本地安装的版本。有关详细信息，请参阅配置本地应用程序访问应用程序。
主要 和 **次要**	使用多站点聚合时，指定关键字 **primary** 的站点始终优先于指定关键字 **secondary** 的站点。

智能访问标签

StoreFront™ 设置某些智能访问标签。您可以在 Studio 中定义访问策略，这些策略可用于根据这些智能访问标签允许或拒绝访问交付组。这需要：

- Citrix Virtual Apps and Desktops 2407 或更高版本。有关详细信息，请参阅关于访问策略规则。
- Citrix Desktops as a Service。有关详细信息，请参阅关于访问策略规则。

StoreFront 设置以下智能访问标签：

名称	描述	示例
`Citrix.ClientUserAgent`	客户端的用户代理	`Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36`
`Citrix.StoreFrontStoreUrl`	用户连接到的应用商店的 URL	`https://storefront.example.com/Citrix/Store`

安装 StoreFront

安装前

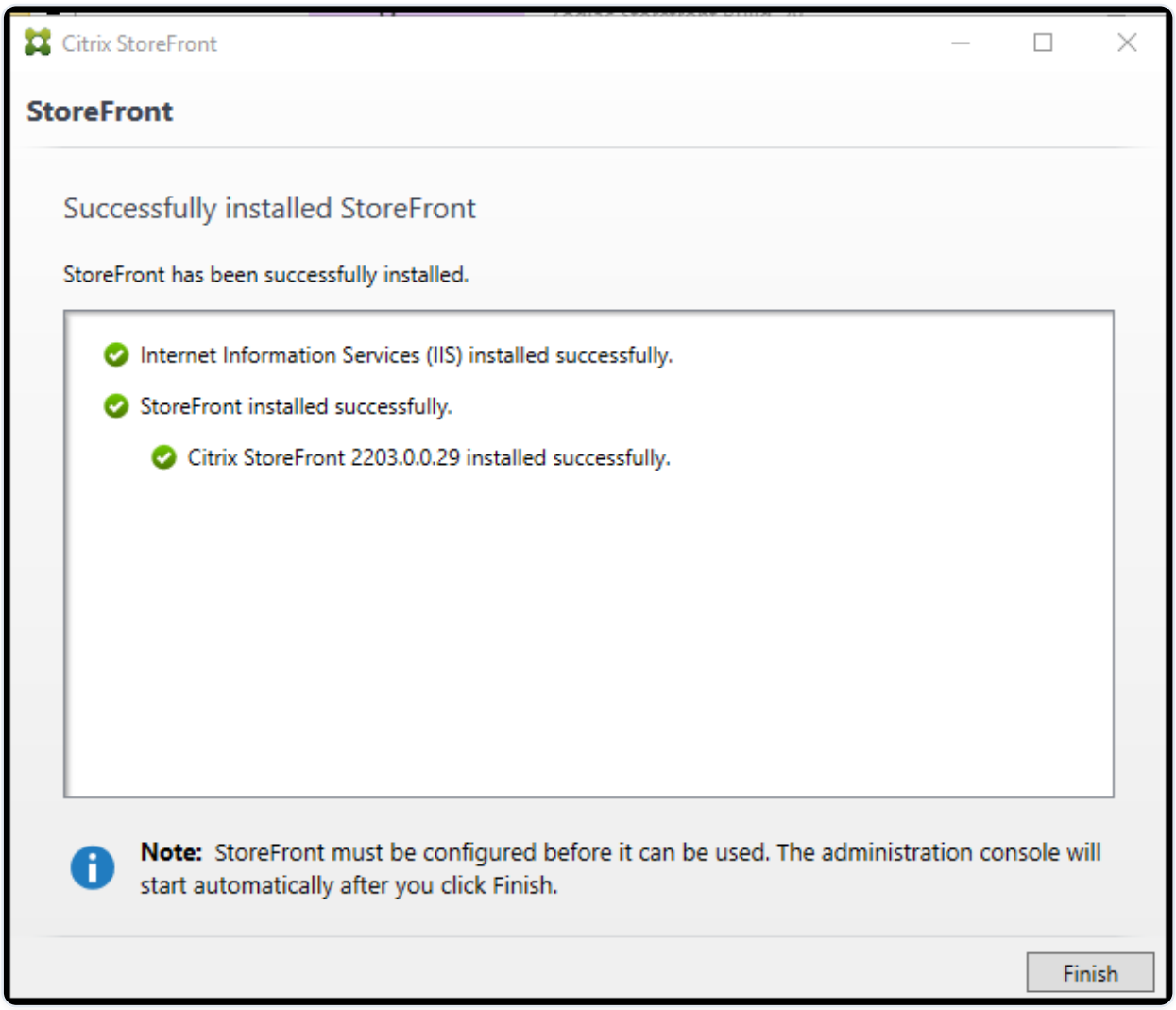
在安装和配置 StoreFront 之前，请查看系统要求。

安装 StoreFront

> **重要**
>
> 为避免在安装 StoreFront 时出现潜在错误和数据丢失，请确保所有应用程序均已关闭，并且目标系统上没有运行其他任务或操作。

1. 从StoreFront 下载页面下载安装程序。安装程序也可以在 Citrix Virtual Apps and Desktops 映像的 `\x64\Storefront` 目录中找到。
2. 使用具有本地管理员权限的帐户登录到 StoreFront 服务器。

3. 找到 CitrixStoreFront-x64.exe，并以管理员身份运行该文件。
4. 阅读并接受许可协议，然后单击**下一步**。
5. 如果出现“查看必备条件”页面，请单击**下一步**。
6. 在“准备安装”页面上，检查列出的要安装的必备条件和 StoreFront 组件，然后单击**安装**。
7. 安装完成后，单击**完成**。



8. StoreFront 可能会要求重新启动以完成安装。单击**是**立即重新启动。
9. 为 HTTPS 配置 Microsoft Internet Information Services (IIS)。有关步骤，请参阅使用 HTTPS 保护 StoreFront。

通过命令提示符安装 StoreFront

1. 使用具有本地管理员权限的帐户登录到 StoreFront 服务器。
2. 浏览您的安装介质或下载包，找到 CitrixStoreFront-x64.exe，并将该文件复制到服务器上的临时位置。
3. 在命令提示符下，导航到包含安装文件的文件夹并键入以下命令。

```
CitrixStoreFront-x64.exe [-silent] [-INSTALLDIR installationlocation]
[-WINDOWS_CLIENT filelocation\filename.exe] [-MAC_CLIENT
filelocation\filename.dmg]
```

使用 **-silent** 参数以静默方式安装 StoreFront 及其必备组件。默认情况下，StoreFront 安装在 C:\Program Files\Citrix\Receiver StoreFront。但是，您可以使用 **-INSTALLDIR** 参数指定不同的安装位置，其中 *installationlocation* 是安装 StoreFront 的目录。如果您打算将服务器作为服务器组的一部分，则 StoreFront 安装位置和 IIS 网站设置、物理路径和站点 ID 必须在所有服务器上保持一致。

当用户在 Windows 或 macOS 上的 Web 浏览器中打开应用商店时，如果默认情况下无法检测到 Citrix Workspace app，系统会提示用户从 Citrix 网站下载并安装适用于其平台的相应 Citrix Workspace app。您可以修改此行为，以便用户从 StoreFront 服务器下载 Citrix Workspace app 安装文件。有关详细信息，请参阅配置如何向用户显示资源。

如果您计划进行此配置更改，请指定 **-WINDOWS_CLIENT** 和 **-MAC_CLIENT** 参数，以分别将适用于 Windows 的 Citrix Receiver 或适用于 Windows 的 Citrix Workspace app，以及适用于 Mac 的 Citrix Receiver 或适用于 Mac 的 Citrix Workspace app 安装文件复制到 StoreFront 部署中的相应位置。将 *filelocation* 替换为包含要复制的安装文件的目录，将 *filename* 替换为安装文件的名称。适用于 Windows 的 Citrix Workspace app 以及适用于 Mac 的 Citrix Receiver 或适用于 Mac 的 Citrix Workspace app 安装文件包含在您的 Citrix Virtual Apps and Desktops 安装介质中。

Windows Server 2019 上的 .Net Framework 4.8 重启步骤

.Net Framework 4.8 是 Windows Server 2022 上的预安装组件，但不是 Windows Server 2019 上的预安装组件。如果不存在 .Net Framework 4.8，CitrixStoreFront-x64.exe 安装程序将运行 .Net Framework 4.8 安装程序。如果正在使用现有的 .Net Framework 库，则可能需要重新启动服务器才能完成 .Net Framework 4.8 的安装，然后才能安装 StoreFront。如果您正在运行 PowerShell 会话，则可能会发生这种情况。

如果需要重新启动，CitrixStoreFront-x64.exe 将退出，之后需要手动重新启动。如果安装处于静默模式，它将以错误代码退出，否则将提示用户允许重新启动。在这种情况下，CitrixStoreFront-x64.exe 进程将返回 .Net Framework 4.8 安装程序中的任何非成功退出代码。具体的重新启动退出代码为：

- ERROR_SUCCESS_REBOOT_REQUIRED **3010**
- ERROR_SUCCESS_REBOOT_INITIATED **1641**

对于通过 PowerShell 脚本静默安装 CitrixStoreFront-x64.exe，如果服务器上尚未安装 .Net Framework 4.8，请预先安装它。

作为 Citrix Virtual Apps and Desktops™ 的一部分进行安装

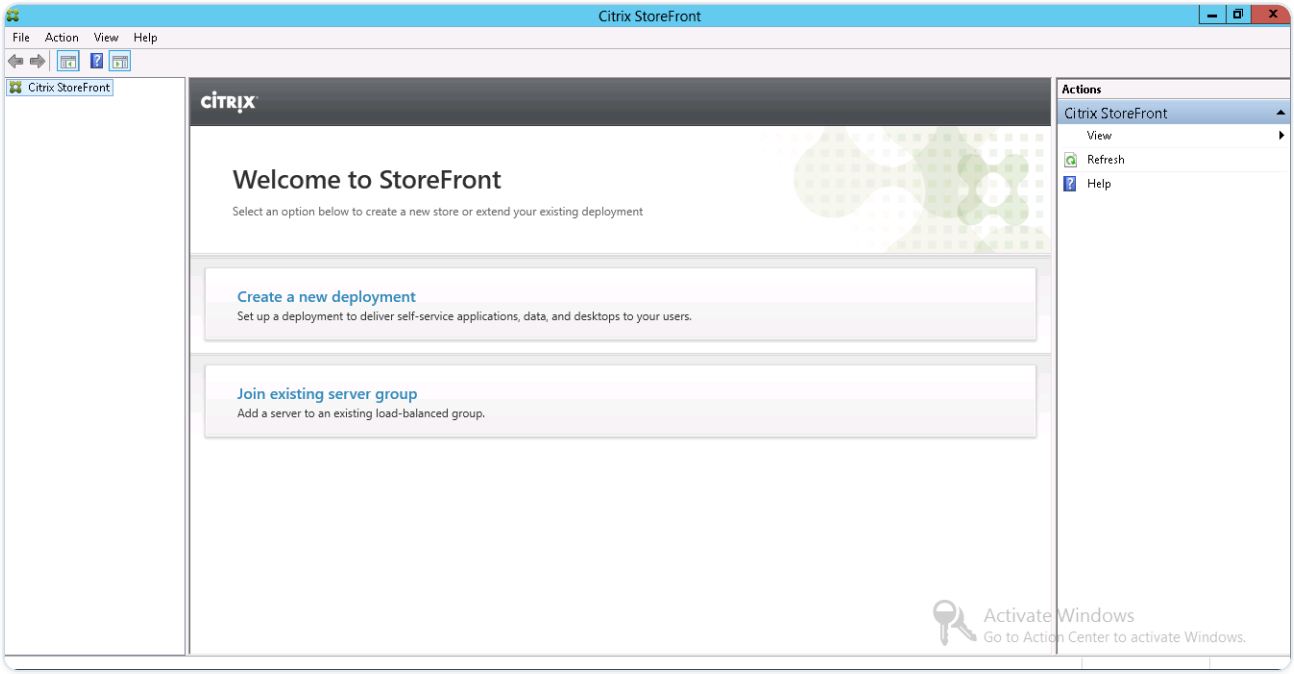
您可以将 StoreFront 与 Citrix Virtual Apps and Desktops 安装在同一台服务器上。运行 Citrix Virtual Apps and Desktops 安装程序，然后在**扩展部署**下选择**Citrix StoreFront**。

安装日志

有关日志文件的更多详细信息，请参阅 日志文件。

配置 StoreFront

完成安装后，Citrix StoreFront 管理控制台会自动启动。您也可以从“开始”菜单打开 StoreFront。Citrix StoreFront 管理控制台首次启动时，会提供两个选项。



- 创建部署。在新 StoreFront 部署中配置第一台服务器。单服务器部署非常适合评估 StoreFront 或小型生产部署。配置第一台 StoreFront 服务器后，您可以随时向组中添加更多服务器以增加部署容量。
- 加入现有服务器组。将另一台服务器添加到现有 StoreFront 部署。选择此选项可快速增加 StoreFront 部署的容量。多服务器部署需要外部负载平衡。要添加服务器，您需要访问部署中的现有服务器。

您的应用商店现在可供用户通过浏览器或本地安装的 Citrix Workspace 应用程序访问。请参阅用户体验。

创建新部署

1. 如果在安装 StoreFront 后 StoreFront 管理控制台 尚未打开，请将其打开。

   欢迎使用 StoreFront 的屏幕截图(/en-us/storefront/2507-ltsr/media/get-started/welcome-to-storefront.png)

2. 在 Citrix StoreFront 管理控制台的结果窗格中，单击 **创建新部署**。
3. 如果有多个 IIS 站点，请从 **IIS 站点** 下拉列表中选择要使用的站点。
4. 如果使用单个 StoreFront 服务器，请输入服务器 URL **基本 URL**。如果要在负载均衡器后面配置多个 StoreFront 服务器，请输入负载均衡 URL 作为 **基本 URL**。

   如果尚未设置负载均衡环境，请输入服务器 URL。您可以随时修改部署的基本 URL。

   创建部署的屏幕截图(/en-us/storefront/2507-ltsr/media/secure/create-deployment-base-url.png)

5. 单击 **下一步**，然后按照 创建应用商店 中的说明配置您的第一个应用商店。
6. 完成所有配置步骤后，单击 **创建** 以创建部署和应用商店。
7. StoreFront 显示其创建的应用商店的摘要。单击 **完成**。

使用 PowerShell 创建新部署

要使用 PowerShell 创建部署，请运行 cmdlet Add-STFDeployment。

多个 互联网信息服务 (IIS) 网站

StoreFront 允许您在每个 Windows 服务器的不同 IIS 网站中部署不同的应用商店，以便每个应用商店可以具有不同的主机名和证书绑定。

要创建多个网站，请参阅 Microsoft IIS 文档。

无法使用管理控制台创建多个 StoreFront 部署；您必须使用 PowerShell。例如，要创建两个 IIS 网站部署，一个用于应用程序，一个用于桌面，请使用以下命令：

```
Add-STFDeployment -SiteID 1 -HostBaseURL "https://apps.example.com"

Add-STFDeployment -SiteID 2 -HostBaseURL "https://desktops.example.com"
```

启用多个站点后，StoreFront 会禁用管理控制台，并且无法将 StoreFront 恢复到单站点模式。您必须使用 PowerShell 模块执行所有 StoreFront 配置，并在每个命令中包含 `SiteID`。

最终用户访问

用户可以通过三种不同的方法访问 StoreFront 商店。

- 本地安装的 Citrix Workspace 应用程序 - 拥有兼容版本的 Citrix Workspace 应用程序的用户可以在 Citrix Workspace 应用程序用户界面中访问 StoreFront 商店。这提供了最佳的用户体验和最强大的功能。
- Web 浏览器 - 拥有兼容 Web 浏览器的用户可以通过浏览到商店的网站来访问 StoreFront 商店。默认情况下，用户还需要兼容版本的 Citrix Workspace 应用程序才能访问其桌面和应用程序，这称为混合启动。但是，您可以配置您的网站，以使用户无需安装 Citrix Workspace 应用程序即可通过浏览器访问其资源。
- XenApp® Services URL - 拥有无法升级的旧版 Citrix® 客户端的用户可以使用商店的 XenApp Services URL 访问商店。创建新商店时，XenApp Services URL 默认启用。

Citrix Workspace™ 应用程序

从本地安装的 Citrix Workspace 应用程序 访问商店可提供最佳、最安全的用户体验。有关可用于以这种方式访问商店的 Citrix Workspace 应用程序版本，请参阅系统要求。

与使用 Web 浏览器相比，Citrix Workspace 应用程序具有以下优势：

- **增强的安全性**，因为 `.ica` 文件会得到安全处理，并且从不下载。
- **增强的可靠性**，无需在 Citrix Web 扩展上部署即可打开应用程序和桌面。
- **内置应用程序保护服务**提供额外的安全层，以防止键盘记录和屏幕捕获恶意软件。
- **更好的遥测**，因为本机应用程序提供了用于监视的广泛信息。
- **增强的 HDX™ 功能**，具有优化的编解码器压缩和高效的音视频压缩等增强功能。这些改进可确保涉及高清内容或图形密集型应用程序的任务具有高质量和高性能。

通常，一个商店只有一个网站，该网站显示在 Citrix Workspace 应用程序中。可以配置多个网站，在这种情况下，您可以配置在 Citrix Workspace 应用程序中显示哪个网站。

信标

Citrix Workspace 应用程序使用内部和外部 URL 作为信标点。通过尝试联系这些信标点，Citrix Workspace 应用程序可以确定用户是连接到本地网络还是公共网络。它使用此信息直接连接到 StoreFront 或通过 Citrix Gateway 连接。有关详细信息，请参阅配置信标点。

要求使用 Citrix Workspace 应用程序

您可以配置 StoreFront，以便当用户在其浏览器中打开应用商店网站时，它会自动打开 Citrix Workspace 应用程序，并且不允许用户继续使用其 Web 浏览器。如果未检测到 Citrix Workspace

应用程序，则网站会向用户提供安装它的选项。此外，网站会自动配置 Citrix Workspace 应用程序以连接到应用商店。有关详细信息，请参阅 要求使用 Citrix Workspace 应用程序。此功能也可以通过插件在 Citrix Gateway 中实现，请参阅 通过网关连接时要求使用 Citrix Workspace 应用程序。

将应用商店添加到 Citrix Workspace 应用程序

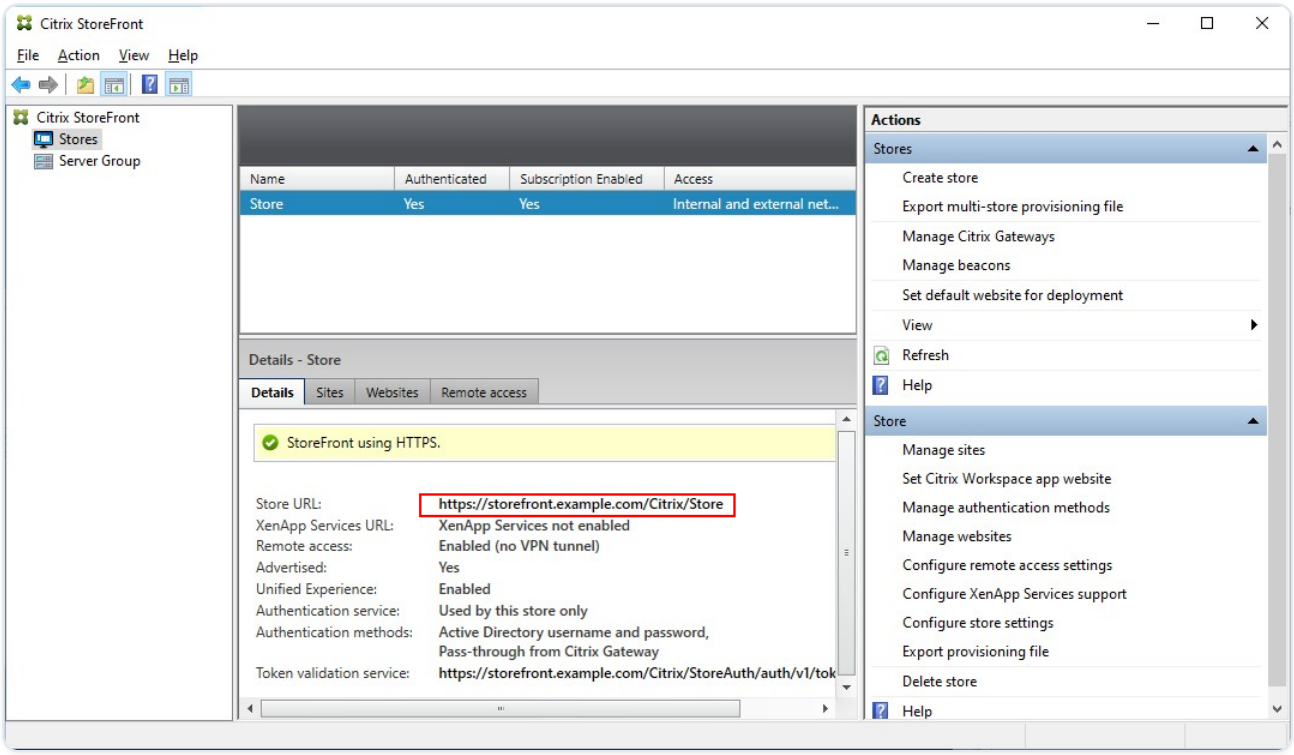
安装后，必须使用为用户提供桌面和应用程序的应用商店的连接详细信息来配置 Citrix Workspace 应用程序。您可以使用应用商店 URL、预配文件或配置电子邮件发现来配置 Citrix Workspace 应用程序。

有关配置适用于 Windows 的 Citrix Workspace 应用程序的详细信息，请参阅 适用于 Windows 的 Citrix Workspace 应用程序文档。

> **重要提示：**
>
> 默认情况下，Citrix Workspace 应用程序要求与应用商店建立 HTTPS 连接。如果 StoreFront 未配置为 HTTPS，则用户必须执行额外的配置步骤才能使用 HTTP 连接。Citrix 强烈建议您不要在生产环境中启用不安全的 StoreFront 用户连接。有关详细信息，请参阅适用于 Windows 的 Citrix Workspace 应用程序文档中的 应用商店配置参数。

应用商店 URL

要获取应用商店 URL，请在管理控制台中选择应用商店。应用商店 URL 显示在应用商店详细信息中。



。

如果右键单击应用商店 URL，则会显示将其复制到剪贴板的选项。

预配文件

您可以向用户提供包含其应用商店连接详细信息的预配文件。安装 Citrix Workspace 应用程序后，用户打开 .cr 文件以自动配置应用商店帐户。默认情况下，网站会为配置了该站点的单个应用商店向用户提供预配文件。您可以指示用户访问他们想要访问的应用商店的网站，并从这些网站下载预配文件。或者，为了获得更高级别的控制，您可以使用 Citrix StoreFront 管理控制台生成包含一个或多个应用商店连接详细信息的预配文件。然后，您可以将这些文件分发给相应的用户。有关详细信息，请参阅 为用户导出应用商店预配文件。

全局应用程序配置服务

使用全局应用程序配置服务为您的 StoreFront 应用商店配置 Citrix Workspace 应用程序。请参阅 配置本地应用商店的设置。

Web 浏览器

作为使用本地安装的 Citrix Workspace 应用程序的替代方案，用户可以通过 Web 浏览器访问其应用商店。

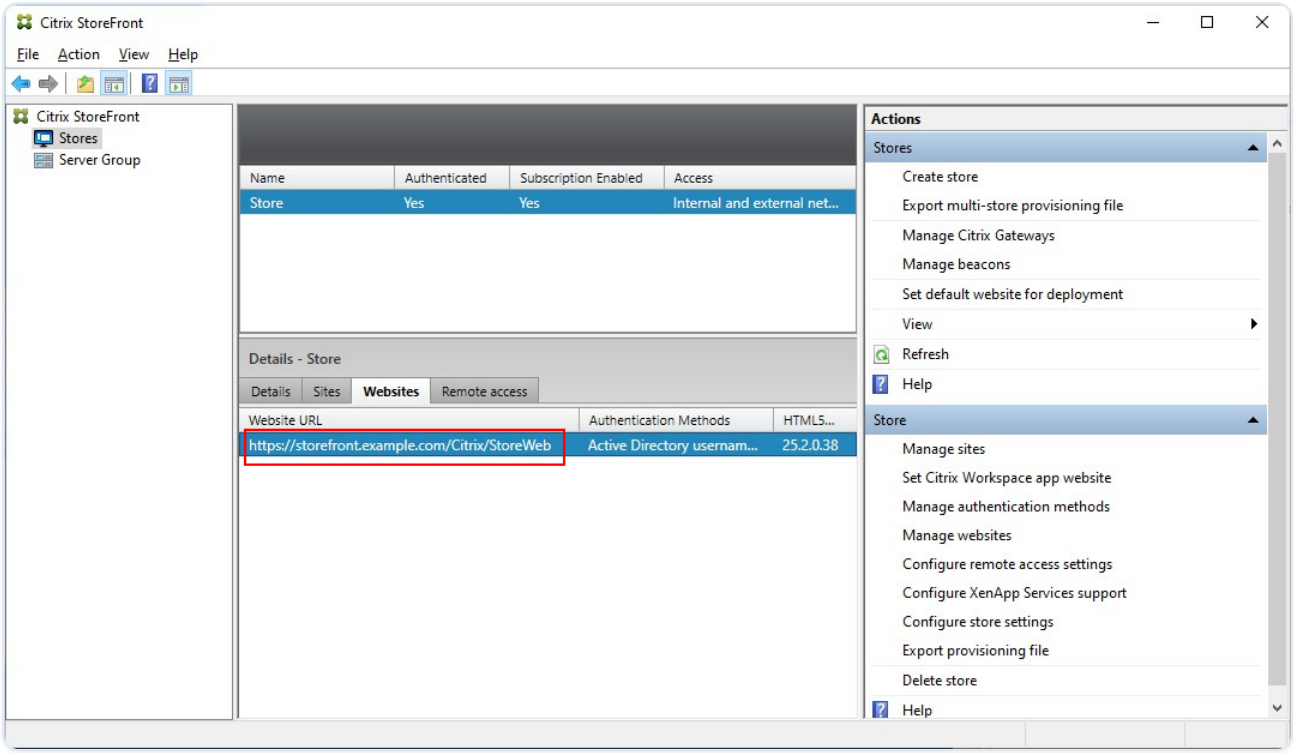
通常，一个应用商店只有一个网站，但您可以配置多个网站，每个网站都有自己的 URL 和配置。有关详细信息，请参阅管理网站。

内部用户可以直接导航到应用商店网站 URL。如果您的 StoreFront 部署中有多个网站，您可以将其中一个配置为默认 URL，当用户导航到基本 URL 时，用户将被重定向到该 URL。

如果您已部署 Citrix Gateway，则外部用户导航到网关 URL。这通常是一个不同的 URL，但可以配置为使用相同的 URL。

> **注意：**
>
> 从 Web 浏览器使用的应用商店网站 URL 与用于配置 Citrix Workspace 应用程序的应用商店 URL 不同。

> 要获取应用商店网站 URL，请在管理控制台中选择应用商店。网站 URL 显示在“**网站**”选项卡上。



如果右键单击网站 URL，则有一个选项可以将其复制到剪贴板。

当用户启动其资源时，有两种可能性：

1. 资源在本地安装的 Citrix Workspace 应用程序中启动。这称为混合启动。这为用户提供了最佳体验，因为它可以利用完整的操作系统集成。有关更多详细信息，请参阅混合启动
2. 资源在浏览器中启动。这使得用户无需在本地安装任何软件即可访问资源。

默认配置是要求本地安装 Citrix Workspace 应用程序以进行混合启动。您可以更改配置，以始终在浏览器中启动资源或让用户选择。请参阅部署 Workspace 应用程序。

如果管理员选择了“**让用户选择**”，那么当用户首次在浏览器中打开应用商店网站时，用户可以选择单击“**使用 Web 浏览器**”以在其 Web 浏览器中启动资源。

在浏览器中打开资源的要求

对于内部网络上的用户，默认情况下禁用通过 Web 浏览器访问 Citrix Virtual Apps and Desktops 提供的资源。要使用 Web 浏览器启用对桌面和应用程序的本地访问，请在 Citrix Virtual Apps and Desktops 服务器上启用 ICA WebSockets 连接策略。Citrix Virtual Apps and Desktops 使用端口 8008 进行 Citrix Workspace 应用程序的 HTML5 连接。确保您的防火墙和其他网络设备允许访问此端口。有关详细信息，请参阅WebSockets 策略设置。

为了成功启动 Citrix Virtual Apps and Desktops 资源，请配置到托管应用程序和桌面的 VDA 的 TLS 连接。通过 Citrix Gateway 的远程连接可以使用 Citrix Workspace app for HTML5 启动资源，而无需配置到 VDA 的 TLS 连接。

混合启动

当用户首次在其 Web 浏览器中打开应用商店，但通过本地安装的 Citrix Workspace 应用程序启动应用程序时，这称为混合启动。Web 站点可以通过多种方式与本地安装的 Workspace 应用程序通信以启动资源。

Citrix Web 扩展

为了获得最佳用户体验，请部署 Citrix Web 扩展。这些是常用 Web 浏览器的扩展，可改善用户检测本地安装的 Citrix Workspace 应用程序以及启动虚拟应用程序和桌面的体验。与 Citrix Workspace 启动器 相比，这提供了更好的用户体验，并避免了全局服务器负载均衡器的问题。

要启用基于浏览器扩展的客户端检测，请执行以下操作：

- 在客户端设备上部署浏览器扩展。
- 部署适用于 Windows 2303、Mac 2304 或 Linux 2302 或更高版本的 Citrix Workspace 应用程序。

用户首次在受支持的平台上访问应用商店网站时，系统会提示用户检测本地安装的 Workspace 应用程序。它首先尝试使用 Web 扩展，如果失败，则尝试使用 Citrix Workspace Launcher。已完成 Workspace 应用程序检测的现有用户可以转到**帐户设置**，选择**更改启动方法**（经典体验）或**验证连接**（现代体验）以重新检测 Citrix Workspace 应用程序。

> **重要**

> 如果用户未安装 Citrix Web 扩展，则 Citrix Workspace 应用程序检测将额外花费 6 秒超时，尝试联系 Citrix Web 扩展。如果您尚未部署 Citrix Web 扩展，则可能需要禁用它或修改超时。有关详细信息，请参阅 启动首选项。

Citrix Workspace 启动器

当用户首次使用受支持的操作系统和浏览器访问 StoreFront 网站且未安装 Citrix Web 扩展时，它会尝试调用 Citrix Workspace Launcher。有关用户体验的更多信息，请参阅 经典体验 和 现代体验。

如果安装了受支持版本的 Citrix Workspace 应用程序，则该应用程序会通知 StoreFront。浏览器会记住这一点，并在启动应用程序时使用 Citrix Workspace Launcher。

使用以下浏览器时，应用商店网站会调用 Citrix Workspace Launcher：

- Firefox 52 或更高版本
- Chrome 42 或更高版本
- Safari 12 或更高版本
- Edge 25 或更高版本

Citrix Workspace Launcher 需要以下最低版本的 Citrix Workspace 应用程序或 Citrix Receiver。

- 适用于 Windows 的 Citrix Receiver 4.3 或更高版本，或任何带有 WebHelper 组件的适用于 Windows 的 Citrix Workspace 应用程序版本（此组件默认安装）
- 适用于 Mac 的 Citrix Receiver 12.0 或更高版本，或任何适用于 Mac 的 Citrix Workspace 应用程序版本
- 适用于 Linux 的 Citrix Workspace 应用程序 2003 或更高版本
- {适用于 iOS 的 Citrix Workspace 应用程序 2503 或更高版本
- 适用于 Android 的 Citrix Workspace 应用程序 2503 或更高版本

如果 Citrix Workspace 启动器不可用，或者用户不允许其打开，则它将无法检测到本地安装的 Citrix Workspace 应用程序。用户可以选择重试，或单击**已安装**，在这种情况下，它将回退到使用 ICA 文件下载 启动应用程序。用户稍后可以通过转到“设置”屏幕并单击**更改 Citrix Workspace 应用程序**来重试。

Citrix Workspace 启动器具有以下限制：

- 如果您在全球服务器负载均衡器后面使用多个活动的 StoreFront 服务器组，则 Citrix Workspace 启动器可能会间歇性失败。为避免此问题，您必须将全球服务器负载均衡器配置为强制用户

Web 会话在客户端检测过程的整个生命周期内持久连接到一个 StoreFront 服务器组。有关更多信息，请参阅 CTX460312。

- 通过 Citrix Gateway 连接到网站时，Citrix Workspace 启动器使用网关的 HDX 路由将来自 Citrix Workspace 应用程序的请求代理回 StoreFront 服务器。如果网关配置为**仅身份验证**（而非 HDX 路由），则 Citrix Workspace 启动器无法连接到 StoreFront。要解决此问题，请确保您的 Citrix Gateway 配置了 HDX 路由和适当的 STA 服务器。编辑 Citrix Gateway，将**用途或角色**设置为**身份验证和 HDX 路由**，并配置 STA 服务器。
- 如果 Citrix Gateway 前面有一个经过身份验证的代理，则 Citrix Workspace 应用程序无法与 Citrix Gateway 建立 SOCKS 连接，因此 Citrix Workspace 启动器会失败。
- 通过 Citrix Gateway 使用智能卡身份验证时，Citrix Workspace 启动器不起作用。

作为替代方案，请部署 (#citrix-web-extensions)。

Internet Explorer 浏览器

用户首次在 Internet Explorer 中打开应用商店网站时，系统会提示用户安装 Citrix Workspace 应用程序，其中包括适用于 Internet Explorer 的 Citrix ICA Client 附加组件。安装插件后，即可通过本地安装的 Citrix Workspace 应用程序启动应用程序和桌面。

ICA 文件下载

如果网站无法通过任何其他方式检测到本地安装的 Citrix Workspace 应用程序，或者用户单击**跳过检测**，则当用户启动应用程序或桌面时，系统会下载一个 .ica 文件。用户可以使用本地安装的 Citrix Workspace 应用程序打开此文件。不建议使用此启动方法，因为：

- 将 ICA 文件存储在磁盘上存在安全风险。
- 使用 (/zh-cn/storefront/2507-ltsr/stores/websites/workspace-control.html) 时，网站无法重新连接到现有会话。
- 域直通身份验证不可用。

此选项可以禁用，有关详细信息，请参阅 (/zh-cn/storefront/2507-ltsr/stores/websites/launch-preferences.html#allow-users-to-skip-citrix-workspace-app-detection)。

资源快捷方式

您可以生成 URL，以提供对应用商店中可用的桌面和应用程序的访问权限。将这些链接嵌入内部网络上托管的网站中，以便用户快速访问资源。用户单击链接后，将被重定向到应用商店网站，如果尚未登录，则会在此处登录。应用商店网站会自动启动资源。有关生成资源快捷方式的详细信息，请参阅 (/zh-cn/storefront/2507-ltsr/stores/websites/website-shortcuts.html)。

创建应用程序快捷方式时，请确保应用商店中没有其他应用程序具有相同的名称。快捷方式无法区分具有相同名称的应用程序的多个实例。同样，如果您从单个桌面组创建了桌面的多个实例并在应用商店中提供，则无法为每个实例创建单独的快捷方式。快捷方式无法将命令行参数传递给应用程序。

要创建应用程序快捷方式，您需要使用将托管快捷方式的内部网站的 URL 配置 StoreFront。当用户单击网站上的应用程序快捷方式时，StoreFront 会根据您输入的 URL 列表检查该网站，以确保请求源自受信任的网站。

XenApp Services URL 地址

> **注意：**
>
> 自 StoreFront 2308 起，XenApp Services（也称为 PNAgent）已弃用。建议您使用 Citrix Workspace 应用程序通过 Store URL 连接到 StoreFront。

> 无法升级的旧版 Citrix 客户端用户可以通过为其客户端配置商店的 XenApp Services URL 来访问商店。您还可以通过 XenApp Services URL 允许域加入的桌面设备和运行 Citrix Desktop Lock 的重新利用的 PC 访问您的商店。在此上下文中，域加入是指已加入包含 StoreFront 服务器的 Microsoft Active Directory 林中某个域的设备。

StoreFront 支持通过 Citrix Workspace 应用程序使用近距离卡对 XenApp Services URL 进行直通身份验证。Citrix Ready 合作伙伴产品使用 Citrix Fast Connect API，通过适用于 Windows 的 Citrix Receiver 或适用于 Windows 的 Citrix Workspace 应用程序简化用户登录，以使用 XenApp Services URL 连接到商店。用户使用近距离卡对工作站进行身份验证，并快速连接到 Citrix Virtual Apps and Desktops 提供的桌面和应用程序。有关详细信息，请参阅最新的 适用于 Windows 的 Citrix Workspace 文档。

创建新商店时，商店的 XenApp Services URL 默认启用。商店的 XenApp Services URL 格式为 `http[s]://serveraddress/Citrix/storename/PNAgent/config.xml`，其中 `serveraddress` 是 StoreFront 部署的服务器或负载平衡环境的完全限定域名，`storename` 是创建商店时指定的名称。这允许只能使用 PNAgent 协议的 Citrix Workspace 应用程序连接到 StoreFront。有关可通过 XenApp Services URL 访问商店的客户端，请参阅 用户设备要求。

重要注意事项

XenApp Services URL 旨在支持无法升级到 Citrix Workspace 应用程序的用户，以及在没有其他访问方法可用的情况下使用。当您决定是否使用 XenApp Services URL 为用户提供对商店的访问权限时，请考虑以下限制。

- 您无法修改商店的 XenApp Services URL。
- 您无法通过编辑配置文件 config.xml 来修改 XenApp Services URL 设置。
- XenApp Services URL 支持显式身份验证、域直通身份验证、智能卡身份验证以及带智能卡的直通身份验证。显式身份验证默认启用。每个 XenApp Services URL 只能配置一种身份验证方法，并且每个商店只有一个 URL 可用。如果您需要启用多种身份验证方法，则必须为每种身份验证方法创建单独的商店，每个商店都有一个 XenApp Services URL。然后，您的用户必须连接到与其身份验证方法相对应的商店。有关详细信息，请参阅 基于 XML 的身份验证。
- 工作区控制默认对 XenApp Services URL 启用，无法配置或禁用。
- 用户更改密码的请求将直接通过为商店提供桌面和应用程序的 Citrix Virtual Apps and Desktops 服务器路由到域控制器，从而绕过 StoreFront 身份验证服务。

管理部署

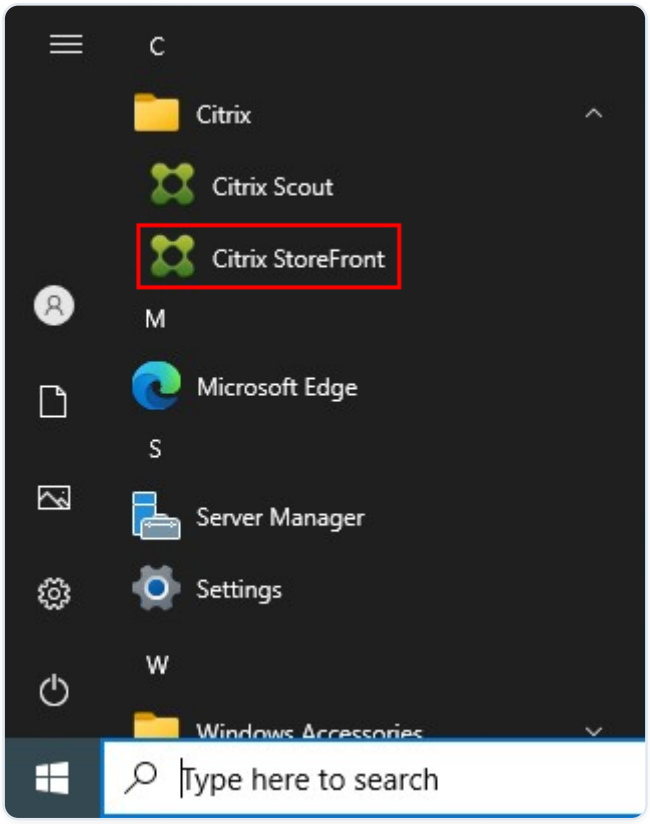
本节介绍如何管理您的 StoreFront 部署。它包含以下主题：

主题	描述
StoreFront 管理控制台	打开 StoreFront 管理控制台 GUI 以配置 StoreFront
StoreFront PowerShell 模块	使用 StoreFront PowerShell 模块自动执行 StoreFront 配置
配置基本 URL	配置用户用于连接到部署的基本 URL。
配置服务器组	在 StoreFront 服务器组中添加和删除服务器，并将配置传播到组中的其他服务器。
管理订阅数据库	选择 StoreFront 存储订阅的位置，管理数据库中的数据并在服务器组之间同步数据。
升级 StoreFront	将旧版本的 StoreFront 升级到此版本。
导出和导入 StoreFront 配置(/zh-cn/storefront/2507-ltsr/manage-deployment/export-import-storefront-config.html)	从一个 StoreFront 部署导出配置并将其导入到另一个部署。
部署的默认网站(/zh-cn/storefront/2507-ltsr/manage-deployment/default-website.html)	配置用户在其 Web 浏览器中访问基本 URL 时重定向到的网站。
将服务器重置为出厂默认设置(/zh-cn/storefront/2507-ltsr/manage-deployment/reset-server-to-factory-defaults.html)	删除所有 StoreFront 配置，以便您可以重新配置它，或将其添加到现有服务器组。
卸载 StoreFront(manage-deployment/uninstall.html)	从服务器中删除 StoreFront

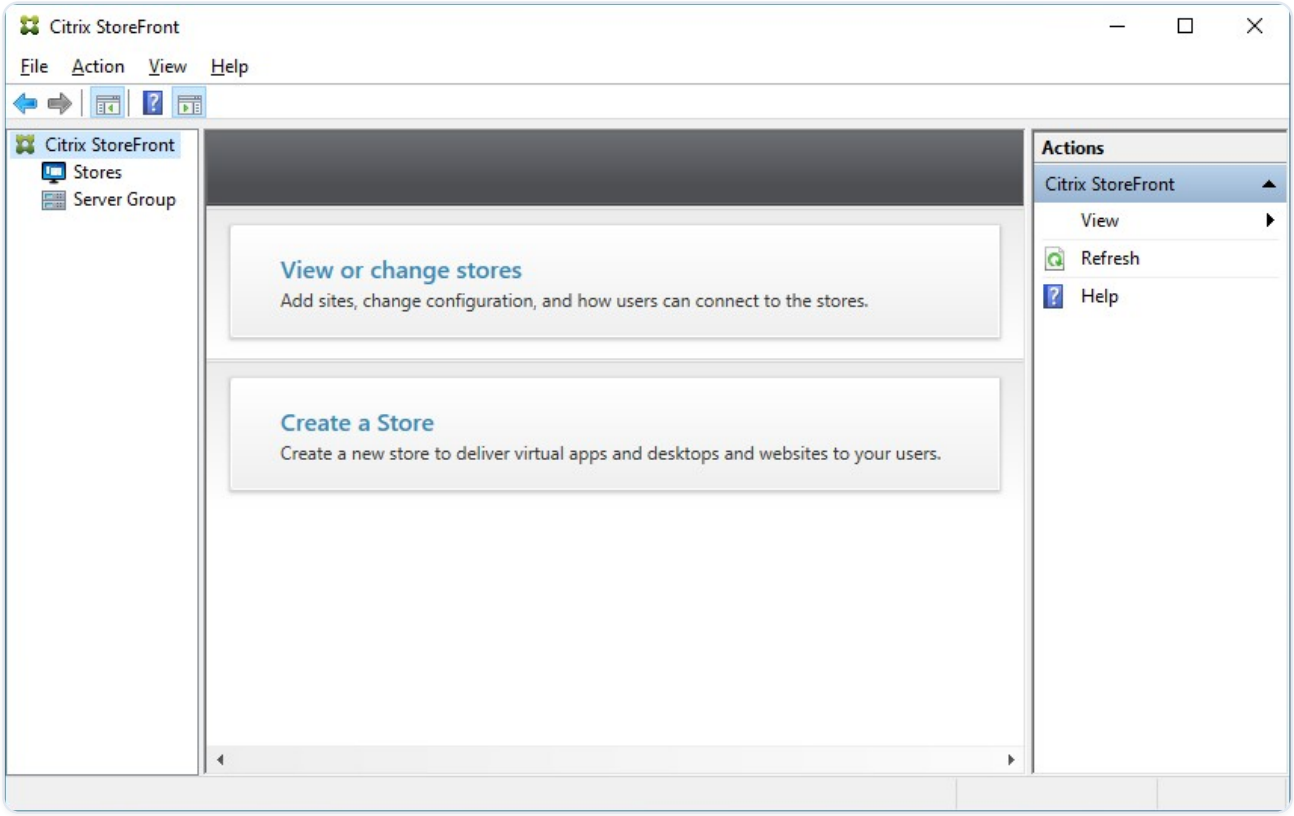
StoreFront™ 管理控制台

StoreFront 的大多数方面都可以使用 StoreFront 管理控制台进行配置。

要打开管理控制台，请打开“**开始**”菜单，展开“**Citrix**”文件夹，然后选择“**Citrix StoreFront**”。



这将打开 StoreFront 管理控制台。



创建部署后(/zh-cn/storefront/2507-ltsr/get-started/create-new-deployment.html)，左侧会显示一个树状视图，其中包含以下各项：

- **应用商店**。选择此项可查看和管理应用商店和网关。
- **服务器组**。选择此项可管理服务器组并配置基本 URL。

在树状视图中选择节点时，屏幕的其余部分会相应更新。

窗口的中心部分包含有关应用商店或服务器组的信息。

右侧是“**操作**”窗格。

某些高级配置任务在管理控制台中不可用，并且需要使用StoreFront PowerShell 模块。

StoreFront PowerShell 模块

Citrix StoreFront 提供了许多 Microsoft Windows PowerShell 2.0 版模块，这些模块在您安装 StoreFront 时会一并安装。借助这些模块，您可以执行与使用 StoreFront 管理控制台 相同的任务，以及仅使用控制台无法完成的任务。

> **注意：**
>
> StoreFront PowerShell 模块与 PowerShell 6 或更高版本不兼容。

> 有关 PowerShell 模块参考，请参阅 StoreFront 开发人员文档。

入门

1. 确保 StoreFront 管理控制台已关闭。
2. 以管理员身份启动 PowerShell 命令行提示符或 **Windows PowerShell ISE**。

   您必须使用 StoreFront 服务器上本地管理员组的成员身份运行 shell 或脚本。
3. 要在脚本中使用 cmdlet，请将 PowerShell 中的执行策略设置为 RemoteSigned。有关 PowerShell 执行策略的更多信息，请参阅 Microsoft 文档。
4. 您可以将 示例脚本 用作起点。
5. 使用 **Get-Help** cmdlet 并提供 cmdlet 名称和 **-Full** 参数，以获取有关特定命令的更多信息。

虚拟路径

用于获取或创建应用商店、网站或身份验证服务的 cmdlet 接受 `VirtualPath` 参数。这是应用程序在 IIS 中托管的路径。应用商店和网站路径也可以在 StoreFront 管理控制台中找到。通常，按照惯例，身份验证路径与应用商店路径相同，并带有后缀 `Auth`，而网站路径与应用商店路径相同，

并带有后缀 `Web`。例如，对于应用商店虚拟路径 `/Citrix/Store`，身份验证服务的路径为 `/Citrix/StoreAuth`，网站的路径为 `/Citrix/StoreWeb`。

例如，要获取路径为 `/Citrix/Store` 的应用商店服务，请运行以下命令：

```
Get-STFStoreService -VirtualPath '/Citrix/Store'
```

如果您省略 VirtualPath，则它会返回所有服务。如果只有一个服务，则 PowerShell 会将其视为单个对象。

站点 ID

某些 cmdlet 包含 `SiteId` 参数。如果您在同一服务器上的不同 IIS 站点上有多个部署，则必须指定 `SiteId`。如果您只有一个站点，则不需要该参数。

示例脚本

StoreFront 包含一些示例脚本，这些脚本位于 **%ProgramFiles%\Citrix\Receiver StoreFront\PowerShellSDK\Examples** 文件夹中。您可以将这些脚本用作创建自己的脚本的模板。

```
-  Use the PowerShell ISE, Visual Studio Code or a similar tool to edit
the script.

-  Use variables to assign values that are to be reused or modified.

-  Remove any commands that are not required.

-  Note that StoreFront cmdlets can be identified by the prefix STF.
```

示例	描述
创建简单部署	脚本：创建一个简单部署，其中包含一个配置了单个 CVAD 站点的 StoreFront 控制器。
创建远程访问部署	脚本：在前一个脚本的基础上，为部署添加远程访问功能。
创建具有最佳启动网关的远程访问部署	脚本：在前一个脚本的基础上，添加首选的最佳启动网关，以提供更好的用户体验。

创建简单部署

以下示例展示了如何创建配置了一个 CVAD 站点的简单部署。

开始之前，请确保按照 Get Started 中详述的步骤操作。此示例可以自定义，以生成用于自动化 StoreFront 部署的脚本。

本节解释了脚本的每个部分正在做什么。这将有助于您自定义自己的脚本。

- 设置错误处理要求并导入所需的 StoreFront 模块。在现代 PowerShell 版本中，不需要导入。

```
Param(

    [Parameter(Mandatory=$true)]

    [Uri]$HostbaseUrl,

    [long]$SiteId = 1,

    [ValidateSet("XenDesktop","XenApp","AppController","VDIinaBox")]

    [string]$Farmtype = "XenDesktop",

    [Parameter(Mandatory=$true)]

    [string[]]$FarmServers,

    [string]$StoreVirtualPath = "/Citrix/Store",

    [bool]$LoadbalanceServers = $false,

    [int]$Port = 80,

    [int]$SSLRelayPort = 443,

    [ValidateSet("HTTP","HTTPS","SSL")]

    [string]$TransportType = "HTTP"

    )

    # Import StoreFront modules. Required for versions of PowerShell
earlier than 3.0 that do not support autoloading
```

```
    Import-Module Citrix.StoreFront

    Import-Module Citrix.StoreFront.Stores

    Import-Module Citrix.StoreFront.Authentication

    Import-Module Citrix.StoreFront.WebReceiver
```

- 根据提供的 `$StoreVirtualPath` 自动化身份验证和 Citrix Receiver for Web 服务的虚拟路径。`$StoreVirtualPath` 等同于 `StoreIISPath`，因为虚拟路径始终是 IIS 中的路径。因此，在 PowerShell 中，它们的值为 `/Citrix/Store`、`/Citrix/StoreWeb` 或 `/Citrix/StoreAuth`。

```
# Determine the Authentication and Receiver virtual path to use based
of the Store

$authenticationVirtualPath = "$($StoreIISPath.TrimEnd('/'))Auth"

$receiverVirtualPath = "$($StoreVirtualPath.TrimEnd('/'))Web"
```

- 如果尚未存在部署，则创建一个新部署，为添加所需的 StoreFront 服务做准备。**-Confirm:$false** 抑制了确认部署可以继续的要求。

```
# Determine if the deployment already exists

$existingDeployment = Get-STFDeployment

if(-not $existingDeployment)

{

    # Install the required StoreFront components

    Add-STFDeployment -HostBaseUrl $HostbaseUrl -SiteId $SiteId
-Confirm:$false

}

elseif($existingDeployment.HostbaseUrl -eq $HostbaseUrl)
```

```
{

    # The deployment exists but it is configured to the desired
hostbase url

    Write-Output "A deployment has already been created with the
specified hostbase url on this server and will be used."

}

else

{

    Write-Error "A deployment has already been created on this server
with a different host base url."

}
```

- 如果在指定的虚拟路径不存在，则创建一个新的身份验证服务。默认的用户名和密码身份验证方法已启用。

```
# Determine if the authentication service at the specified virtual path
exists

$authentication = Get-STFAuthenticationService -VirtualPath
$authenticationVirtualPath

if(-not $authentication)

{

    # Add an Authentication service using the IIS path of the Store
appended with Auth

    $authentication = Add-STFAuthenticationService
$authenticationVirtualPath

}

else
```

```
{

    Write-Output "An Authentication service already exists at the
specified virtual path and will be used."

}
```

- 如果在指定的虚拟路径不存在，则创建一个新的商店服务，该服务配置有一个站点（也称为场），并使用数组 **$XenDesktopServers** 中定义的服务器。

```
# Determine if the store service at the specified virtual path exists

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

if(-not $store)

{

# Add a Store that uses the new Authentication service configured to
publish resources from the supplied servers

$store = Add-STFStoreService -VirtualPath $StoreVirtualPath
-AuthenticationService $authentication -FarmName $Farmtype -FarmType
$Farmtype -Servers $FarmServers -LoadBalance $LoadbalanceServers `

        -Port $Port -SSLRelayPort $SSLRelayPort -TransportType
$TransportType

}

else

{

    Write-Output "A Store service already exists at the specified
virtual path and will be used. Farm and servers will be appended to
this store."

    # Get the number of farms configured in the store

    $farmCount = (Get-STFStoreFarmConfiguration $store).Farms.Count
```

```
    # Append the farm to the store with a unique name

    Add-STFStoreFarm -StoreService $store -FarmName "Controller$
($farmCount + 1)" -FarmType $Farmtype -Servers $FarmServers
-LoadBalance $LoadbalanceServers -Port $Port `

        -SSLRelayPort $SSLRelayPort -TransportType $TransportType

}
```

- 在指定的 IIS 虚拟路径添加一个网站，以访问在上面创建的商店中发布的应用程序。

```
# Determine if the receiver service at the specified virtual path
exists

$receiver = Get-STFWebReceiverService -VirtualPath $receiverVirtualPath

if(-not $receiver)

{

    # Add a Receiver for Web site so users can access the applications
and desktops in the published in the Store

    $receiver = Add-STFWebReceiverService -VirtualPath
$receiverVirtualPath -StoreService $store

}

else

{

    Write-Output "A Web Receiver service already exists at the
specified virtual path and will be used."

}
```

- 为商店启用 XenApp 服务，以便较旧的 Citrix Receiver 或 Citrix Workspace 应用程序客户端可以连接到已发布的应用程序。

```
# Determine if PNA is configured for the Store service

$storePnaSettings = Get-STFStorePna -StoreService $store

if(-not $storePnaSettings.PnaEnabled)

{

# Enable XenApp services on the store and make it the default for this
server

Enable-STFStorePna -StoreService $store -AllowUserPasswordChange
-DefaultPnaService

}
```

示例：创建远程访问部署

以下示例在前一个脚本的基础上添加了一个具有远程访问功能的部署。

开始之前，请确保按照 (#get-started) 中详述的步骤操作。可以使用所述方法自定义此示例，以生成用于自动化 StoreFront 部署的脚本。

本节解释了 StoreFront 生成的脚本的每个部分的作用。这将有助于您自定义自己的脚本。

- 设置错误处理要求并导入所需的 StoreFront 模块。在现代版本的 PowerShell 中不需要导入。

```
Param(

    [Parameter(Mandatory=$true)]

    [Uri]$HostbaseUrl,

    [Parameter(Mandatory=$true)]

    [long]$SiteId = 1,

    [string]$Farmtype = "XenDesktop",

    [Parameter(Mandatory=$true)]

    [string[]]$FarmServers,
```

```
    [string]$StoreVirtualPath = "/Citrix/Store",

    [bool]$LoadbalanceServers = $false,

    [int]$Port = 80,

    [int]$SSLRelayPort = 443,

    [ValidateSet("HTTP","HTTPS","SSL")]

    [string]$TransportType = "HTTP",

    [Parameter(Mandatory=$true)]

    [Uri]$GatewayUrl,

    [Parameter(Mandatory=$true)]

    [Uri]$GatewayCallbackUrl,

    [Parameter(Mandatory=$true)]

    [string[]]$GatewaySTAUrls,

    [string]$GatewaySubnetIP,

    [Parameter(Mandatory=$true)]

    [string]$GatewayName

)

Set-StrictMode -Version 2.0



# Any failure is a terminating failure.

$ErrorActionPreference = 'Stop'

$ReportErrorShowStackTrace = $true

$ReportErrorShowInnerException = $true
```

```
# Import StoreFront modules. Required for versions of PowerShell
earlier than 3.0 that do not support autoloading

Import-Module Citrix.StoreFront

Import-Module Citrix.StoreFront.Stores

Import-Module Citrix.StoreFront.Roaming
```

- 通过调用前面的示例脚本来创建内部访问 StoreFront 部署。基本部署将扩展以支持远程访问。

```
# Create a simple deployment by invoking the SimpleDeployment example

$scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.Definition
-Parent

$scriptPath = Join-Path $scriptDirectory "SimpleDeployment.ps1"

& $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -FarmServers
$FarmServers -StoreVirtualPath $StoreVirtualPath -Farmtype $Farmtype \`

    -LoadbalanceServers $LoadbalanceServers -Port $Port  -SSLRelayPort
$SSLRelayPort -TransportType $TransportType
```

- 获取在简单部署中创建的服务，因为需要更新它们以支持远程访问场景。

```
# Determine the Authentication and Receiver sites based on the Store

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$authentication = Get-STFAuthenticationService -StoreService $store

$receiverForWeb = Get-STFWebReceiverService -StoreService $store
```

- 在 Citrix Receiver™ for Web 服务上启用 CitrixAGBasic，该服务是使用 Citrix Gateway 进行远程访问所必需的。从支持的协议中获取 Citrix Receiver for Web CitrixAGBasic 和 ExplicitForms 身份验证方法。

```
# Get the Citrix Receiver for Web CitrixAGBasic and ExplicitForms
authentication method from the supported protocols

# Included for demonstration purposes as the protocol name can be used
directly if known

$receiverMethods = Get-STFWebReceiverAuthenticationMethodsAvailable |
Where-Object { $_ -match "Explicit" -or $_ -match "CitrixAG" }

# Enable CitrixAGBasic in Receiver for Web (required for remote access)

Set-STFWebReceiverService $receiverForWeb -AuthenticationMethods
$receiverMethods
```

- 在身份验证服务上启用 CitrixAGBasic。这是远程访问所必需的。

```
# Get the CitrixAGBasic authentication method from the protocols
installed.

# Included for demonstration purposes as the protocol name can be used
directly if known

$citrixAGBasic = Get-STFAuthenticationProtocolsAvailable | Where-Object
{ $_ -match "CitrixAGBasic" }

# Enable CitrixAGBasic in the Authentication service (required for
remote access)

Enable-STFAuthenticationServiceProtocol -AuthenticationService
$authentication -Name $citrixAGBasic
```

- 添加一个新的远程访问网关，提供可选的子网 IP 地址，并将其注册到商店以进行远程访问。

```
# Add a new Gateway used to access the new store remotely

Add-STFRoamingGateway -Name "NetScaler10x" -LogonType Domain -Version
Version10_0_69_4 -GatewayUrl $GatewayUrl `

    -CallbackUrl $GatewayCallbackUrl -SecureTicketAuthorityUrls
$GatewaySTAUrls
```

```
# Get the new Gateway from the configuration (Add-STFRoamingGateway
will return the new Gateway if -PassThru is supplied as a parameter)

$gateway = Get-STFRoamingGateway -Name $GatewayName

# If the gateway subnet was provided then set it on the gateway object

if($GatewaySubnetIP)

{

    Set-STFRoamingGateway -Gateway $gateway -SubnetIPAddress
$GatewaySubnetIP

}

# Register the Gateway with the new Store

Register-STFStoreGateway -Gateway $gateway -StoreService $store
-DefaultGateway
```

示例：创建具有最佳启动网关的远程访问部署

以下示例基于之前的脚本，添加了一个具有最佳启动网关远程访问的部署。

开始之前，请确保按照 入门 中详述的步骤操作。此示例可以使用所述方法进行自定义，以生成用于自动化 StoreFront 部署的脚本。

了解脚本

本节解释了 StoreFront 生成的脚本的每个部分的作用。这将有助于您自定义自己的脚本。

- 设置错误处理要求并导入所需的 StoreFront 模块。在现代 PowerShell 版本中，不需要导入。

```
Param(

    [Parameter(Mandatory=$true)]

    [Uri]$HostbaseUrl,

    [long]$SiteId = 1,

    [string]$Farmtype = "XenDesktop",
```

```
    [Parameter(Mandatory=$true)]
    [string[]]$FarmServers,
    [string]$StoreVirtualPath = "/Citrix/Store",
    [bool]$LoadbalanceServers = $false,
    [int]$Port = 80,
    [int]$SSLRelayPort = 443,
    [ValidateSet("HTTP","HTTPS","SSL")]
    [string]$TransportType = "HTTP",
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayUrl,
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayCallbackUrl,
    [Parameter(Mandatory=$true)]
    [string[]]$GatewaySTAUrls,
    [string]$GatewaySubnetIP,
    [Parameter(Mandatory=$true)]
    [string]$GatewayName,
    [Parameter(Mandatory=$true)]
    [Uri]$OptimalGatewayUrl,
    [Parameter(Mandatory=$true)]
    [string[]]$OptimalGatewaySTAUrls,
    [Parameter(Mandatory=$true)]
```

```
    [string]$OptimalGatewayName

)

Set-StrictMode -Version 2.0

# Any failure is a terminating failure.

$ErrorActionPreference = 'Stop'

$ReportErrorShowStackTrace = $true

$ReportErrorShowInnerException = $true

# Import StoreFront modules. Required for versions of PowerShell
earlier than 3.0 that do not support autoloading

Import-Module Citrix.StoreFront

Import-Module Citrix.StoreFront.Stores

Import-Module Citrix.StoreFront.Roaming
```

- 调用远程访问部署脚本以配置基本部署并添加远程访问。

```
# Create a remote access deployment

$scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.Definition
-Parent

$scriptPath = Join-Path $scriptDirectory "RemoteAccessDeployment.ps1"

& $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -FarmServers
$FarmServers -StoreVirtualPath $StoreVirtualPath -Farmtype $Farmtype `

    -LoadbalanceServers $LoadbalanceServers -Port $Port  -SSLRelayPort
$SSLRelayPort -TransportType $TransportType `

    -GatewayUrl $GatewayUrl -GatewayCallbackUrl $GatewayCallbackUrl
-GatewaySTAUrls $GatewaySTAUrls -GatewayName $GatewayName
```

- 添加首选的最佳启动网关，并从已配置网关列表中获取它。

```
# Add a new Gateway used for remote HDX access to desktops and apps

$gateway = Add-STFRoamingGateway -Name $OptimalGatewayName -LogonType
UsedForHDXOnly -GatewayUrl $OptimalGatewayUrl
-SecureTicketAuthorityUrls $OptimalGatewaySTAUrls -PassThru
```

- 获取商店服务以使用最佳网关，注册它并将其分配给来自指定站点的启动。

```
# Get the Store configured by SimpleDeployment.ps1

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

# Register the Gateway with the new Store for launch against all of the
farms (currently just one)

$farmNames = @($store.FarmsConfiguration.Farms | foreach
{ $_.FarmName })

Register-STFStoreOptimalLaunchGateway -Gateway $gateway -StoreService
$store -FarmName $farmNames
```

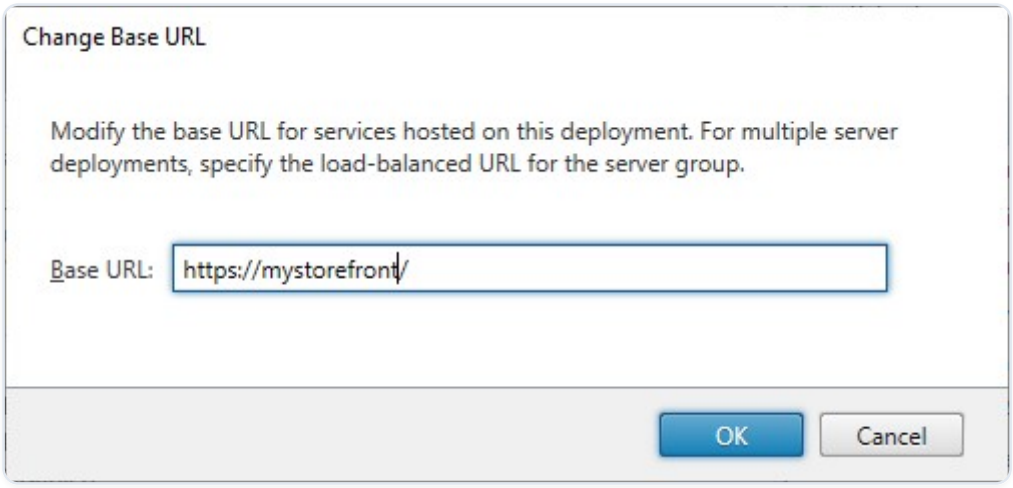
配置基本 URL

基本 URL 用作部署上托管的商店和其他 StoreFront 服务的 URL 根。您必须输入用户用于直接连接到部署（而非通过 Citrix Gateway）的 URL，例如 `https://storefront.example.com`。方案必须是 `http` 或 `https`。建议您始终使用 `https`。

- 对于没有负载均衡器的单服务器部署，请输入服务器的 URL。
- 如果用户通过负载均衡器连接，请输入负载均衡器的 URL。您还必须启用环回通信，以便 StoreFront 绕过负载均衡器进行内部通信。

要更改基本 URL：

1. 在 Citrix StoreFront 管理控制台的左侧窗格中，选择“**服务器组**”节点。
2. 在操作窗格中，单击“**更改基本 URL...**”。
3. 输入新 URL。
4. 按“**确定**”。



配置服务器组

为了实现冗余和可伸缩性，您应该在负载均衡器后面，以服务器组的形式部署 2 台或更多相同的 StoreFront 服务器。StoreFront 会在服务器之间同步配置和收藏夹数据。

要管理多服务器部署，请一次只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。完成更改后，(#propagate-local-changes-to-a-server-group)以确保整个部署中的配置一致。

查看服务器组

在 StoreFront 管理控制台中，在左侧的树状视图中，选择 **Server Group**。这将显示服务器组中的服务器数量、基本 URL、服务器列表及其同步状态。

将服务器添加到服务器组

在您要添加到组的服务器上安装 StoreFront 之前，请确保以下事项：

- 您要添加的服务器必须与组中其他服务器具有相同版本的 StoreFront。
- 您要添加的服务器与组中的其他服务器位于同一位置。确保服务器之间具有低延迟和可靠的连接。
- 您要添加的服务器运行的操作系统版本和区域设置必须与组中其他服务器相同。不支持包含混合操作系统版本和区域设置的 StoreFront 服务器组。
- IIS 配置的网站配置（例如物理路径和站点 ID）必须与组中其他服务器相同。

> **注意：**

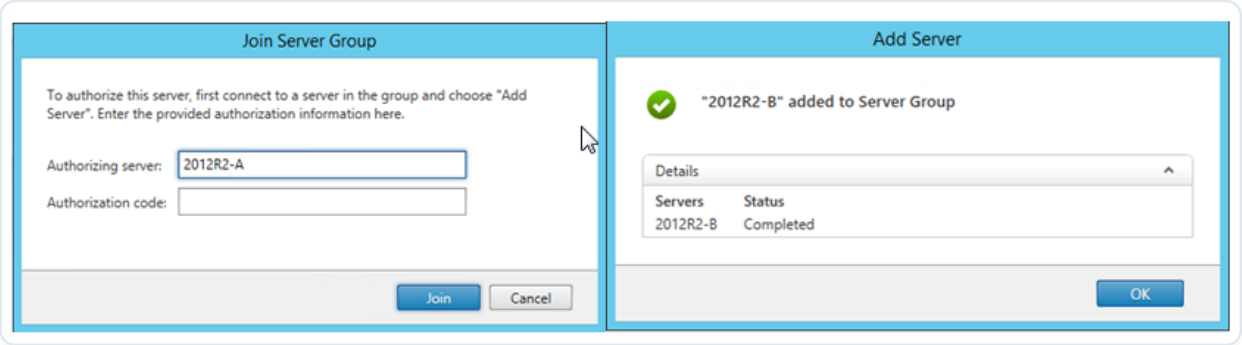
> 有关服务器组大小的建议，请参阅 (/zh-cn/storefront/2507-ltsr/get-started/plan.html#storefront-server-groups)。

> 如果您要添加的 StoreFront 服务器以前属于某个服务器组并已被删除，则在将其重新添加到相同或不同的服务器组之前，必须将 StoreFront 服务器重置为出厂默认状态。请参阅 (/zh-cn/storefront/2507-ltsr/manage-deployment/reset-server-to-factory-defaults.html)

> **重要提示：**
>
> 将新服务器添加到服务器组时，StoreFront 服务帐户将作为本地管理员组的成员添加到新服务器上。这些服务需要本地管理员权限才能加入服务器组并与之同步。如果您使用组策略阻止向本地管理员组添加新成员，或者限制服务器上本地管理员组的权限，则 StoreFront 无法加入服务器组。

1. 登录到您希望加入的 StoreFront 部署中的服务器，然后打开 Citrix StoreFront 管理控制台。在控制台的左侧窗格中选择“服务器组”节点，然后在“操作”窗格中选择 **Add Server**。记下显示的授权码。
2. 连接到新服务器。在 StoreFront 管理控制台中，选择 **加入现有服务器组**。
3. 在“加入服务器组”对话框中，在“授权服务器”框中指定现有服务器的名称。输入从该服务器获取的授权码，然后选择 **加入**。

   加入组后，新服务器的配置将更新以匹配现有服务器的配置。组中的所有其他服务器都将使用新服务器的详细信息进行更新。



4. 将服务器添加到负载均衡器。

要管理多服务器部署，一次只能使用一台服务器对服务器组的配置进行更改。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。您所做的任何配置更改都必须传播到组中的其他服务器，以确保整个部署的配置一致。

从服务器组中删除服务器

1. 从负载均衡器中删除服务器。
2. 登录到服务器组中除您希望删除的服务器之外的任何一台服务器。
3. 打开 StoreFront 管理控制台。
4. 在树状视图中，选择 **服务器组**
5. 选择 **删除服务器**。
6. 选择您希望删除的服务器。

在已删除的 StoreFront 服务器可以再次添加到相同或不同的服务器组之前，您必须将其重置为出厂默认状态。请参阅 将服务器重置为出厂默认设置

将本地更改传播到服务器组

对一台服务器进行配置更改后，必须将这些更改传播到服务器组中的所有其他服务器。配置信息的传播是手动启动的，这样您就可以控制组中的服务器何时以及是否使用配置更改进行更新。在运行此传播时，在组中的所有服务器都更新之前，您无法进行任何进一步的更改。

要传播更改，请从操作窗格中选择**传播更改**。

> **重要提示：**

> 在传播期间，组中其他服务器上所做的任何更改都将被丢弃。如果您更新了服务器的配置，请将更改传播到组中的其他服务器，以避免在以后从部署中的不同服务器传播更改时丢失这些更改。

> 组中服务器之间传播的信息包括：

- 所有 `web.config` 文件的内容，其中包含 StoreFront 配置。
- `C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients` 的内容，例如 `C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients\Windows\CitrixWorkspaceAppWeb.exe` 和 `C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients\MAC\CitrixWorkspaceAppWeb.dmg`。
- 对于每个应用商店网站（例如 `c:\inetpub\wwwroot\Citrix\StoreWeb`），`contrib`、`custom` 和 `customweb` 文件夹的内容。这些文件夹用于保存网站自定义项。
- Citrix Delivery Services 证书存储的内容，但手动导入的任何证书吊销列表 (CRL) 除外。（有关分发本地 CRL 的详细信息，请参阅证书吊销列表 (CRL) 检查。）.

注意：

订阅数据与 Propagate Changes 机制独立地与其他服务器同步。它会自动发生，无需启动 Propagate Changes 任务。

管理订阅数据库

当您创建应用商店时，StoreFront 会在服务器本地创建一个 Microsoft 可扩展存储引擎 (ESENT) 数据库，用于存储收藏夹（也称为订阅）数据。在 StoreFront 服务器组环境中，每台服务器都维护自己的数据库副本。对收藏夹的任何更改都会传播到其他服务器，以确保用户无论连接到哪台服务器都能看到相同的收藏夹。

此外，您还可以将收藏夹存储在 SQL Server 数据库中。有关详细信息，请参阅 使用 Microsoft SQL Server 存储订阅数据。

要查看应用商店是使用本地 ESENT 数据库还是 SQL Server 数据库，请使用以下 PowerShell 脚本：

```
$store=Get-STFStoreService -VirtualPath '/Citrix/Store'

Get-STFStoreSubscriptionsDatabase -StoreService $store
```

管理收藏夹数据

使用 ESENT 数据库时，您可以使用 PowerShell 管理收藏夹数据。有关详细信息，请参阅 管理收藏夹数据。使用 SQL Server 数据库时，您可以使用 SQL 管理记录。

在服务器组之间同步收藏夹

订阅会在服务器组中的服务器之间自动同步。如果您有多个服务器组，则可以配置 Citrix Files 以定期在服务器组之间同步订阅。有关详细信息，请参阅 订阅同步。

管理订阅数据

如果使用本地数据库，则可以使用 PowerShell cmdlet 管理商店的收藏夹。

清除订阅数据

部署中的每个商店都有一个包含收藏夹数据的文件夹和数据存储。

1. 在 StoreFront 服务器上停止 Citrix Subscriptions Store 服务。如果 Citrix Subscriptions Store 服务正在运行，则无法删除任何商店的订阅数据。
2. 在 StoreFront 服务器上找到订阅存储文件夹：`C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore\1__Cit`
3. 删除订阅存储文件夹的内容，但不要删除文件夹本身。
4. 在 StoreFront 服务器上重新启动 Citrix Subscriptions Store 服务。

您可以使用以下 PowerShell 脚本清除商店的订阅数据。以管理员身份运行此 PowerShell 函数，该管理员具有停止或启动服务以及删除文件的权限。此 PowerShell 函数可实现与上述手动步骤相同的结果。

要成功运行 cmdlet，Citrix Subscriptions Store 服务必须在服务器上运行。

```
function Remove-SubscriptionData

{

    [CmdletBinding()]



    [Parameter(Mandatory=$False)][String]$Store = "Store"



    $SubsService = "Citrix Subscriptions Store"



    # Path to Subscription Data in StoreFront version 2.6 or later



    $SubsPath = "C:
\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\Subscriptio
nsStore\1__Citrix_$Store\*"



    Stop-Service -displayname $SubsService
```

```
    Remove-Item $SubsPath -Force -Verbose


    Start-Service -displayname $SubsService


    Get-Service -displayname $SubsService
}


Remove-SubscriptionData -Store "YourStore"
```

导出订阅数据

您可以使用 cmdlet Export-STFStoreSubscriptions 获取商店订阅数据的备份（以制表符分隔的 .txt 文件形式），例如：

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/
<yourstore>"

Export-STFStoreSubscriptions -StoreService $StoreObject -FilePath
"$env:USERPROFILE\Desktop\Subscriptions.txt"
```

如果您正在管理多服务器部署，则可以在 StoreFront 服务器组中的任何服务器上运行此 PowerShell cmdlet。服务器组中的每台服务器都维护其对等服务器的订阅数据的相同同步副本。如果您认为 StoreFront 服务器之间的订阅同步存在问题，请从组中的所有服务器导出数据并进行比较以查看差异。

恢复订阅数据

使用 Restore-STFStoreSubscriptions 覆盖现有订阅数据。您可以使用之前使用 Export-STFStoreSubscriptions 创建的制表符分隔的 .txt 文件备份来恢复商店的订阅数据。

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/
<yourstore>"
```

```
Restore-STFStoreSubscriptions -StoreService $StoreObject -FilePath
"$env:USERPROFILE\Desktop\Subscriptions.txt"
```

有关 Restore-STFStoreSubscriptions 的更多信息，请参阅 `<https://developer-docs.citrix.com/zh-cn/storefront-powershell-sdk/2507/Restore-STFStoreSubscriptions/>`

在单个 StoreFront 服务器上还原数据

在单个服务器部署中，无需关闭订阅存储服务。在还原订阅数据之前，也无需清除现有订阅数据。

在 StoreFront 服务器组上还原数据

要将订阅数据还原到服务器组，需要执行以下步骤。

包含三个 StoreFront 服务器的服务器组部署示例。

- StoreFrontA
- StoreFrontB
- StoreFrontC

1. 备份三个服务器中任何一个的现有订阅数据。
2. 停止服务器 StoreFrontB 和 C 上的订阅存储服务。此操作可防止服务器在更新 StoreFrontA 期间发送或接收订阅数据。
3. 清除服务器 StoreFrontB 和 C 上的订阅数据。这可以防止还原的订阅数据不匹配。
4. 使用 **Restore-STFStoreSubscriptions** cmdlet 在 StoreFrontA 上还原数据。无需停止订阅存储服务，也无需清除 StoreFrontA 上的订阅数据（它将在还原操作期间被覆盖）。
5. 重新启动服务器 StoreFrontB 和 StoreFrontC 上的订阅存储服务。然后，这些服务器可以从 StoreFrontA 接收数据副本。
6. 等待所有服务器之间发生同步。所需时间取决于 StoreFrontA 上存在的记录数量。如果所有服务器都位于本地网络连接上，则同步通常会很快发生。通过 WAN 连接同步订阅可能需要更长时间。
7. 从 StoreFrontB 和 C 导出数据以确认同步已完成，或查看 Store 订阅计数器。

导入订阅数据

当 Store 没有订阅数据时，请使用 **Import-STFStoreSubscriptions**。此 cmdlet 还允许将订阅数据从一个 Store 传输到另一个 Store，或者在将订阅数据导入到新预配的 StoreFront 服务器时使用。

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/
<yourstore>"

Import-STFStoreSubscriptions -StoreService $StoreObject -FilePath
"$env:USERPROFILE\Desktop\Subscriptions.txt"
```

有关 Import-STFStoreSubscriptions 的更多信息，请参阅 `<https://developer-docs.citrix.com/zh-cn/storefront-powershell-sdk/2507/Import-STFStoreSubscriptions/>`

订阅数据文件详细信息

订阅数据文件是一个文本文件，其中每行包含一个用户订阅。每行都是一个由制表符分隔的值序列：

`<user-identifier> <resource-id> <subscription-id> <subscription-status> <property-name> <property-value> <property-name> <property-value> ...`.

其中：

- `<user-identifier>` - 必需。标识用户的字符序列。此标识符是用户的 Windows 安全标识符。
- `<resource-id>` - 必需。标识已订阅资源的字符序列。
- `<subscription-id>` - 必需。唯一标识订阅的字符序列。此值未使用（尽管数据文件中必须存在一个值）。
- `<subscription-status>` - 必需。订阅状态：已订阅或未订阅。
- `<property-name>` 和 `<property-value>` - 可选。零个或多个属性名称/值对序列。这些表示 StoreFront 客户端（通常是 Citrix Workspace 应用程序）与订阅关联的属性。具有多个值的属性由具有相同名称的多个名称/值对表示（例如，“… MyProp A MyProp B …”表示值为 A、B 的属性 MyProp）。

示例

S-0-0-00-0000000000-0000000000-0000000000-0000 XenApp.Excel 21EC2020-3AEA-4069-A2DD-08002B30309D 已订阅 炫目:位置 1

StoreFront 服务器磁盘上的订阅数据大小

记录数	大小 MB
0	6.02
1,000	7.02
10,000	40.00
100,000	219.00
200,000	358.00
500,000	784.00
800,000	1213.02
1,000,000	1597.15
1,300,000	1919.15
1,500,000	2205.15
2,000,000	2915.15

导入和导出 .txt 文件的大小

记录数	大小 MB
0	0.00
1,000	0.13
10,000	1.30
100,000	12.80
200,000	25.60
500,000	64.10
800,000	102.00
1,000,000	128.00

记录数	大小 MB
1,300,000	166.00
1,500,000	192.00
1,700,000	218.00
2,000,000	256.00

StoreFront 订阅计数器

您可以使用 Microsoft Windows 性能监视器计数器 (**开始 > 运行 > perfmon**)，例如，显示服务器上的订阅记录总数，或 StoreFront 服务器组之间同步的记录数。

使用 PowerShell 查看订阅计数器

```
Get-Counter -Counter "\Citrix Subscription Store(1__citrix_store)
\Subscription Entries Count (including unpurged deleted records)"



Get-Counter -Counter "\Citrix Subscription Store
Synchronization\Subscriptions Store Synchronizing"



Get-Counter -Counter "\Citrix Subscription Store Synchronization\Number
Subscriptions Synchronized"



Get-Counter -Counter "\Citrix Subscription Store Synchronization\Number
Subscriptions Transferred"
```

使用 Microsoft SQL Server 存储订阅数据

注意：

本文档假设您具备 MS SQL Server 和 T-SQL 查询的基础知识。管理员在尝试遵循本文档之前，必须熟悉 SQL Server 的配置、使用和管理。

简介

ESENT 是一个可嵌入的事务性数据库引擎，Windows 可以使用它。默认情况下，所有版本的 StoreFront 都支持使用内置的 ESENT 数据库。如果商店配置为使用 SQL 连接字符串，它们还可以连接到 Microsoft SQL Server 实例。

将 StoreFront 切换为使用 SQL 而非 ESENT 的主要优势在于，您可以轻松使用 SQL 更新语句来管理、修改或删除订阅记录。如果使用 SQL，则在对订阅数据进行微小更改时，无需导出、修改和重新导入整个 ESENT 订阅数据。

要将现有订阅数据从 ESENT 迁移到 Microsoft SQL Server，需要将从 StoreFront 导出的平面 ESENT 数据转换为 SQL 友好格式以进行批量导入。对于没有任何新订阅数据的新部署，此步骤不是必需的。数据转换步骤只需执行一次。

注意：

由于网络中断导致无法连接到 StoreFront 用于存储订阅数据的 SQL Server 实例，并不会导致 StoreFront 部署无法使用。中断只会导致用户体验暂时下降；在 SQL Server 连接恢复之前，用户无法添加、删除或查看收藏的资源。在中断期间，资源仍然可以被枚举和启动。预期行为与使用 ESENT 时 Citrix Subscription Store 服务停止的情况相同。

提示：

使用 ESENT 或 SQL 时，配置了 KEYWORDS:Auto 或 KEYWORDS:Mandatory 的资源行为方式相同。如果用户的资源中包含任一 KEYWORD，则当用户首次登录时，会自动创建新的 SQL 订阅记录。

ESENT 和 SQL Server 的优势

ESENT	SQL
默认设置，无需额外配置即可“开箱即用”StoreFront。	更易于管理，可以使用 T-SQL 查询轻松操作或更新订阅数据。允许删除或更新每个用户的记录。允许轻松统计每个应用程序、交付控制器或用户的记录。允许轻松删除已离职用户的不必要用户数据。允许轻松更新交付控制器引

ESENT	SQL
	用，例如当管理员切换到使用聚合或预配新的交付控制器时。
使用订阅同步和拉取计划，可以更简单地配置不同服务器组之间的复制。请参阅 配置订阅同步	与 StoreFront 解耦，因此在 StoreFront 升级之前无需备份订阅数据，因为数据保存在单独的 SQL Server 上。订阅备份独立于 StoreFront，并使用 SQL 备份策略和机制。
当不需要订阅管理时，SQL 是不必要的。如果订阅数据永远不需要更新，ESENT 很可能满足客户需求。	服务器组所有成员共享订阅数据的单个副本，从而减少服务器之间数据差异或数据同步问题的可能性。

ESENT 和 SQL Server 的缺点

ESENT	SQL
无法轻松且精细地管理订阅数据。需要通过导出的 .txt 文件进行订阅操作。必须导出并重新导入整个订阅数据库。可能需要使用查找和替换技术更改数千条记录，这既费力又容易出错。	需要基本的 SQL 专业知识和基础设施。可能需要购买 SQL 许可证，这会增加 StoreFront 部署的总拥有成本。不过，Citrix Virtual Apps and Desktops 数据库实例也可以与 StoreFront 共享以降低成本。
服务器组中的每个 StoreFront 服务器都必须维护 ESENT 数据库的副本。在极少数情况下，此数据库可能会在服务器组内或不同服务器组之间出现不同步。	在服务器组之间复制订阅数据并非易事。它需要每个数据中心有多个 SQL 实例以及它们之间的事务复制。这需要专业的 MS SQL 知识。
	需要从 ESENT 迁移数据并将其转换为 SQL 友好格式。此过程只需执行一次。
	可能需要额外的 Windows 服务器和许可证。
	部署 StoreFront 的额外步骤。

部署方案

> **注意：**
>
> 如果要支持用户订阅，StoreFront 中配置的每个应用商店都需要 ESENT 数据库或 Microsoft SQL 数据库。订阅数据的存储方法是在 StoreFront 中的应用商店级别设置的。

> Citrix® 建议所有应用商店数据库都驻留在同一个 Microsoft SQL Server 实例上，以降低管理复杂性并减少配置错误的可能性。

多个应用商店可以共享同一个数据库，前提是它们都配置为使用相同的连接字符串。它们是否使用不同的交付控制器无关紧要。多个应用商店共享数据库的缺点是无法判断每个订阅记录对应哪个应用商店。

在具有多个应用商店的单个 StoreFront 部署上，两种数据存储方法的组合在技术上是可行的。可以将一个应用商店配置为使用 ESENT，将另一个配置为使用 SQL。但不建议这样做，因为这会增加管理复杂性并可能导致配置错误。

您可以使用以下四种方案将订阅数据存储在 SQL Server 中：

方案 1：使用 ESENT 的单个 STOREFRONT 服务器或服务器组（默认）

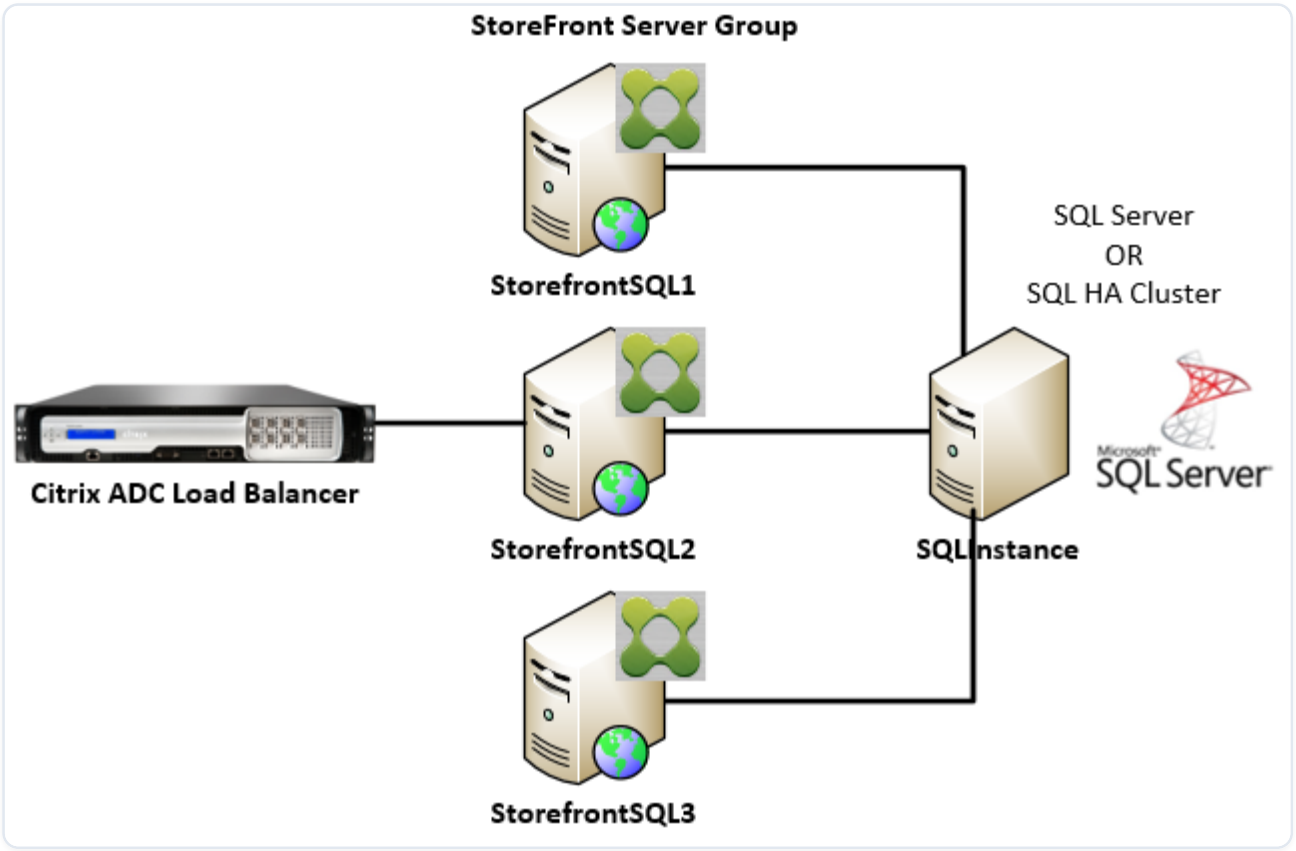
默认情况下，自 2.0 版以来的所有 StoreFront 版本都使用平面 ESENT 数据库在服务器组成员之间存储和复制订阅数据。服务器组的每个成员都维护订阅数据库的相同副本，该副本与服务器组的所有其他成员同步。此方案无需额外配置步骤。此方案适用于大多数不期望频繁更改 Delivery Controller 名称或不需要对其订阅数据（例如删除或更新旧用户订阅）执行频繁管理任务的客户。

方案 2：安装了单个 STOREFRONT 服务器和本地 MICROSOFT SQL SERVER 实例

StoreFront 使用本地安装的 SQL Server 实例，并且这两个组件都位于同一服务器上。此方案适用于简单的单个 StoreFront 部署，其中客户可能需要频繁更改 Delivery Controller 名称，或者需要对其订阅数据（例如删除或更新旧用户订阅）执行频繁管理任务，但他们不需要高可用性 StoreFront 部署。Citrix 不建议将此方案用于服务器组，因为它会在托管 Microsoft SQL 数据库实例的服务器组成员上创建单点故障。此方案不适用于大型企业部署。

方案 3：配置为高可用性的 STOREFRONT 服务器组和专用 MICROSOFT SQL SERVER 实例（推荐）

所有 StoreFront 服务器组成员都连接到同一个专用 Microsoft SQL Server 实例或 SQL 故障转移群集。这是大型企业部署最合适的模型，其中 Citrix 管理员希望频繁更改交付控制器名称，或者希望对其订阅数据（例如删除或更新旧用户订阅）执行频繁管理任务，并且需要高可用性。

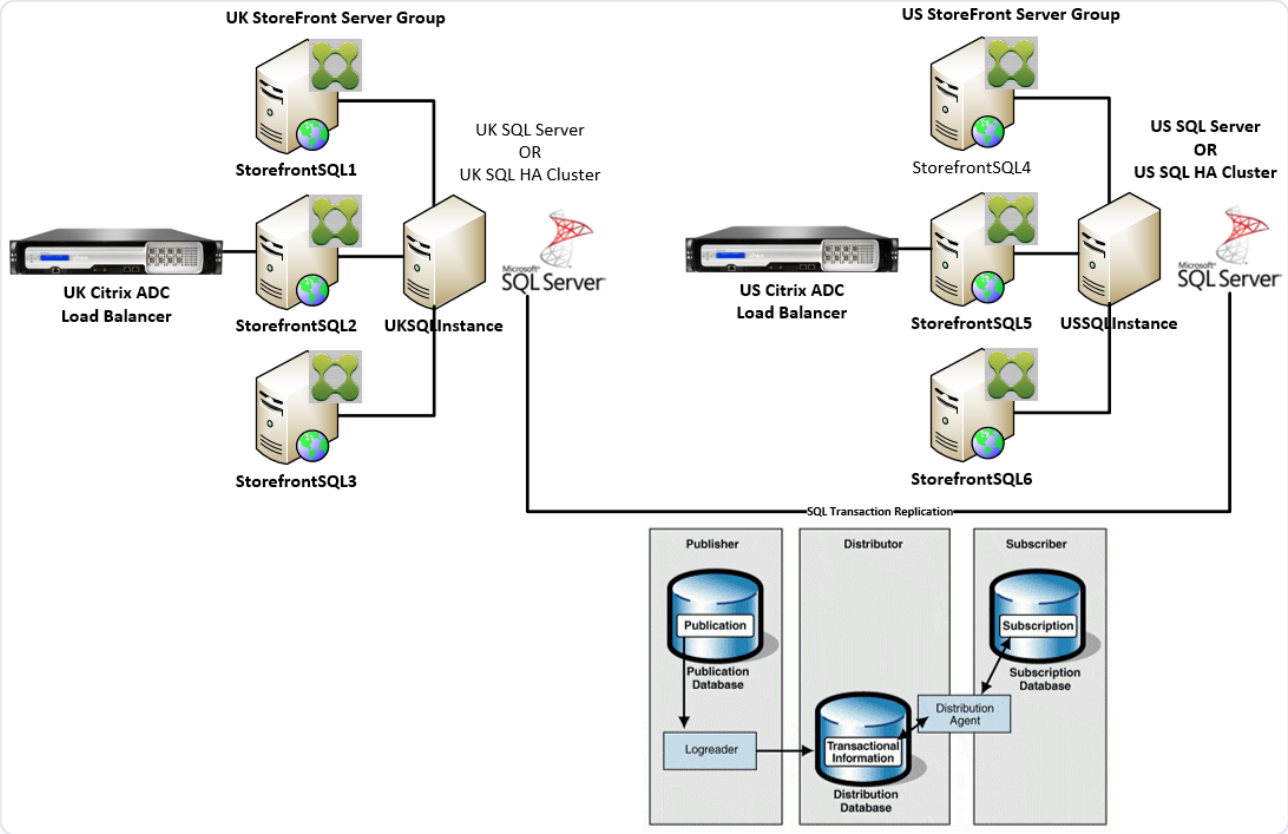


方案 4：每个数据中心每个服务器组的多个 STOREFRONT 服务器组和专用 MICROSOFT SQL SERVER 实例

注意：

这是一种高级配置。仅当您是熟悉事务复制的经验丰富的 SQL Server 管理员，并且具备成功部署它所需的技能时，才尝试此操作。

这与方案 3 相同，但将其扩展到需要在不同远程数据中心部署多个 StoreFront 服务器组的情况。Citrix 管理员可以选择在相同或不同数据中心的不同服务器组之间同步订阅数据。数据中心中的每个服务器组都连接到其自己的专用 Microsoft SQL Server 实例，以实现冗余、故障转移和性能。此方案需要大量的额外 Microsoft SQL Server 配置和基础架构。它完全依赖于 Microsoft SQL 技术来复制订阅数据及其 SQL 事务。



资源

您可以从 `<https://github.com/citrix/sample-scripts/tree/master/storefront>` 下载以下脚本以帮助您：

配置脚本

- **Set-STFDatabase.ps1** – 为每个 Store 设置 MS SQL 连接字符串。在 StoreFront 服务器上运行。
- **Add-LocalAppPoolAccounts.ps1** – 授予本地 StoreFront 服务器的应用程序池对 SQL 数据库的读写访问权限。在 SQL 服务器上为场景 2 运行。
- **Add-RemoteSFAccounts.ps1** – 授予服务器组中的所有 StoreFront 服务器对 SQL 数据库的读写访问权限。在 SQL 服务器上为场景 3 运行。
- **Create-StoreSubscriptionsDB-2016.sql** – 创建 SQL 数据库和架构。在 SQL 服务器上运行。

数据转换和导入脚本

- **Transform-SubscriptionDataForStore.ps1** – 将 ESENT 中现有的订阅数据导出并转换为 SQL 友好格式以供导入。
- **Create-ImportSubscriptionDataSP.sql** – 创建一个存储过程，用于导入由 Transform-SubscriptionDataForStore.ps1 转换的数据。在使用 Create-StoreSubscriptionsDB-2016.sql 创建数据库架构后，在 SQL 服务器上运行此脚本一次。

在 SQL Server 上配置 StoreFront 服务器的本地安全组

场景 2：安装了单个 StoreFront 服务器和本地 Microsoft SQL Server 实例

在 Microsoft SQL Server 上创建一个名为 `<SQLServer>\StoreFrontServers` 的本地安全组，并添加 `IIS APPPOOL\DefaultAppPool` 和 `IIS APPPOOL\Citrix Receiver for Web` 的虚拟帐户，以允许本地安装的 StoreFront 对 SQL 进行读写。此安全组在创建存储订阅数据库架构的 .SQL 脚本中被引用，因此请确保组名匹配。

您可以下载脚本 Add-LocalAppPoolAccounts.ps1 来帮助您。

在运行 *Add-LocalAppPoolAccounts.ps1* 脚本之前安装 StoreFront。该脚本依赖于定位 `IIS APPPOOL\Citrix Receiver for Web` 虚拟 IIS 帐户的能力，该帐户在 StoreFront 安装和配置之前不存在。`IIS APPPOOL\DefaultAppPool` 通过安装 IIS Web 服务器角色自动创建。

```
# Create Local Group for StoreFront servers on DB Server

$LocalGroupName = "StoreFrontServers"

$Description = "Contains StoreFront Server Machine Accounts or StoreFront
AppPool Virtual Accounts"



# Check whether the Local Group Exists

if ([ADSI]::Exists("WinNT://$env:ComputerName/$LocalGroupName"))

{

    Write-Host "$LocalGroupName already exists!" -ForegroundColor "Yellow"

}

else

{

Write-Host "Creating $LocalGroupName local security group"
-ForegroundColor "Yellow"
```

```
# Create Local User Group

$Computer = [ADSI]"WinNT://$env:ComputerName,Computer"

$LocalGroup = $Computer.Create("group",$LocalGroupName)

$LocalGroup.setinfo()

$LocalGroup.description = $Description

$Localgroup.SetInfo()

Write-Host "$LocalGroupName local security group created" -ForegroundColor
"Green"

}

$Group = [ADSI]"WinNT://$env:ComputerName/$LocalGroupName,group"



# Add IIS APPPOOL\DefaultAppPool

$objAccount = New-Object System.Security.Principal.NTAccount("IIS
APPPOOL\DefaultAppPool")

$StrSID =
$objAccount.Translate([System.Security.Principal.SecurityIdentifier])

$DefaultSID = $StrSID.Value



$Account = [ADSI]"WinNT://$DefaultSID"

$Group.Add($Account.Path)



# Add IIS APPPOOL\Citrix Receiver for Web

$objAccount = New-Object System.Security.Principal.NTAccount("IIS
APPPOOL\Citrix Receiver for Web")
```

```
$StrSID =
$objAccount.Translate([System.Security.Principal.SecurityIdentifier])

$WebRSID = $StrSID.Value



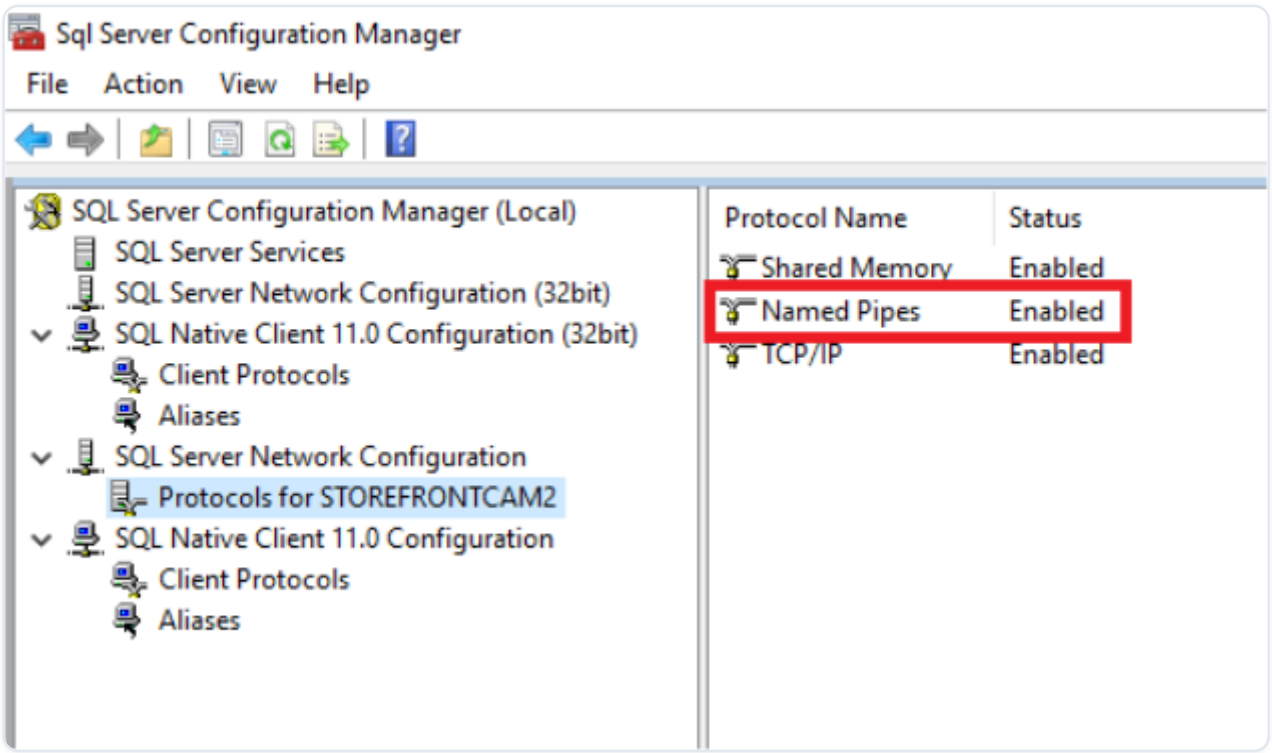
$Account = [ADSI]"WinNT://$WebRSID"

$Group.Add($Account.Path)



Write-Host "AppPools added to $LocalGroupName local group"
-ForegroundColor "Green"
```

使用 SQL Server 配置管理器在本地 SQL 实例中启用命名管道。StoreFront 和 SQL Server 之间的进程间通信需要命名管道。



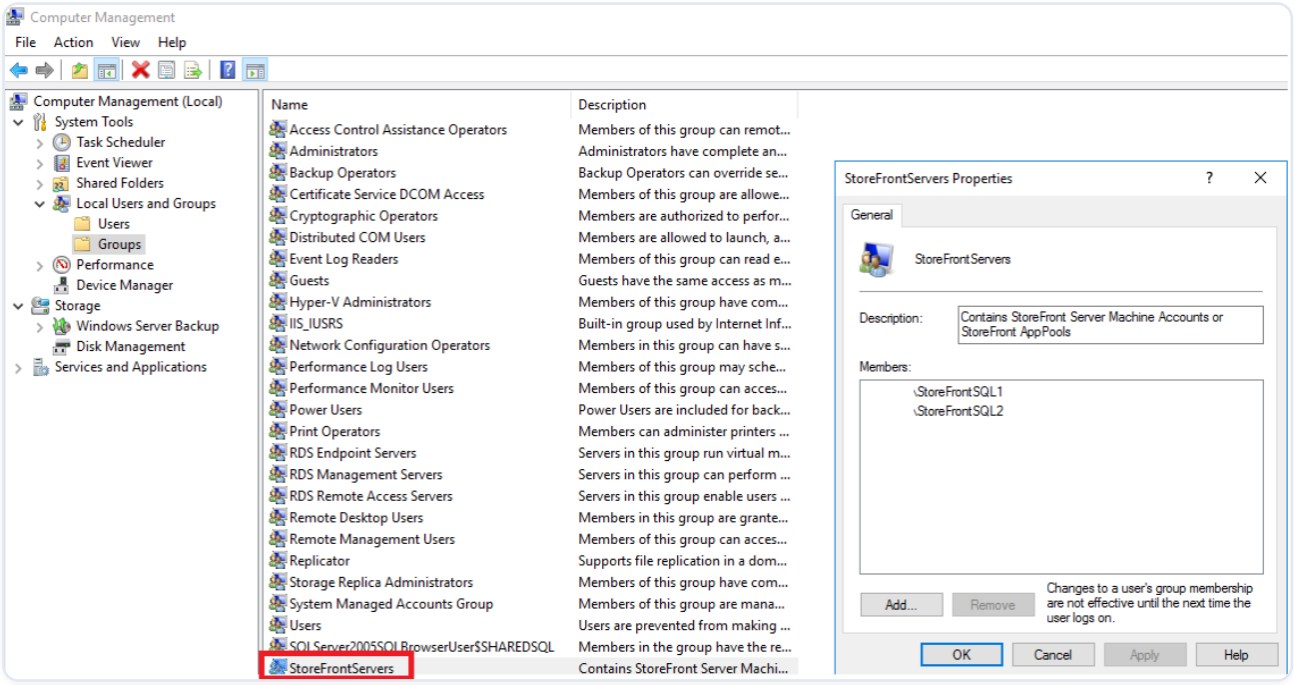
确保 Windows 防火墙规则已正确配置，以允许使用特定端口或动态端口的 SQL Server 连接。有关如何在您的环境中执行此操作，请参阅 Microsoft 文档。

提示：

> 如果连接到本地 SQL 实例失败，请检查连接字符串中使用的 localhost 或 `<hostname>` 是否解析为正确的 IPv4 地址。Windows 可能会尝试使用 IPv6 而非 IPv4，并且 localhost 的 DNS 解析可能会返回 ::1 而非 StoreFront 和 SQL 服务器的正确 IPv4 地址。可能需要完全禁用主机服务器上的 IPv6 网络堆栈才能解决此问题。

场景 3：StoreFront 服务器组和专用 Microsoft SQL Server 实例

在 Microsoft SQL Server 上创建一个名为 `<SQLServer>\StoreFrontServers` 的本地安全组，并添加 StoreFront 服务器组的所有成员。此安全组稍后将在 **Create-StoreSubscriptionsDB-2016.sql** 脚本中引用，该脚本用于在 SQL 中创建订阅数据库架构。



将所有 StoreFront 服务器组域计算机帐户添加到 `<SQLServer>\StoreFrontServers` 组。如果 SQL Server 使用 Windows 身份验证，则只有组中列出的 StoreFront 服务器域计算机帐户才能在 SQL 中读取和写入订阅记录。脚本 Add-RemoteSFAccounts.ps1 中提供的以下 PowerShell 函数创建本地安全组，并将名为 StoreFrontSQL1 和 StoreFrontSQL2 的两台 StoreFront 服务器添加到其中。

```
function Add-RemoteSTFMachineAccounts

{

[CmdletBinding()]

param([Parameter(Mandatory=$True)][string]$Domain,

[Parameter(Mandatory=$True)][array]$StoreFrontServers)
```

```
# Create Local Group for StoreFront servers on DB Server

$LocalGroupName = "StoreFrontServers"

$Description = "Contains StoreFront Server Machine Accounts or StoreFront
AppPool virtual accounts"



# Check whether the Local Security Group already exists

if ([ADSI]::Exists("WinNT://$env:ComputerName/$LocalGroupName"))

{

    Write-Host "$LocalGroupName already exists!" -ForegroundColor "Yellow"

}

else

{

    Write-Host "Creating $LocalGroupName local group" -ForegroundColor
"Yellow"



    # Create Local Security Group

    $Computer = [ADSI]"WinNT://$env:ComputerName,Computer"

    $LocalGroup = $Computer.Create("group",$LocalGroupName)

    $LocalGroup.setinfo()

    $LocalGroup.description = $Description

    $Localgroup.SetInfo()

Write-Host "$LocalGroupName local group created" -ForegroundColor "Green"
```

```
}

Write-Host "Adding $StoreFrontServers to $LocalGroupName local group"
-ForegroundColor "Yellow"



foreach ($StoreFrontServer in $StoreFrontServers)

{

    $Group = [ADSI]"WinNT://$env:ComputerName/$LocalGroupName,group"

    $Computer = [ADSI]"WinNT://$Domain/$StoreFrontServer$"

    $Group.Add($Computer.Path)

}

Write-Host "$StoreFrontServers added to $LocalGroupName" -ForegroundColor
"Green"

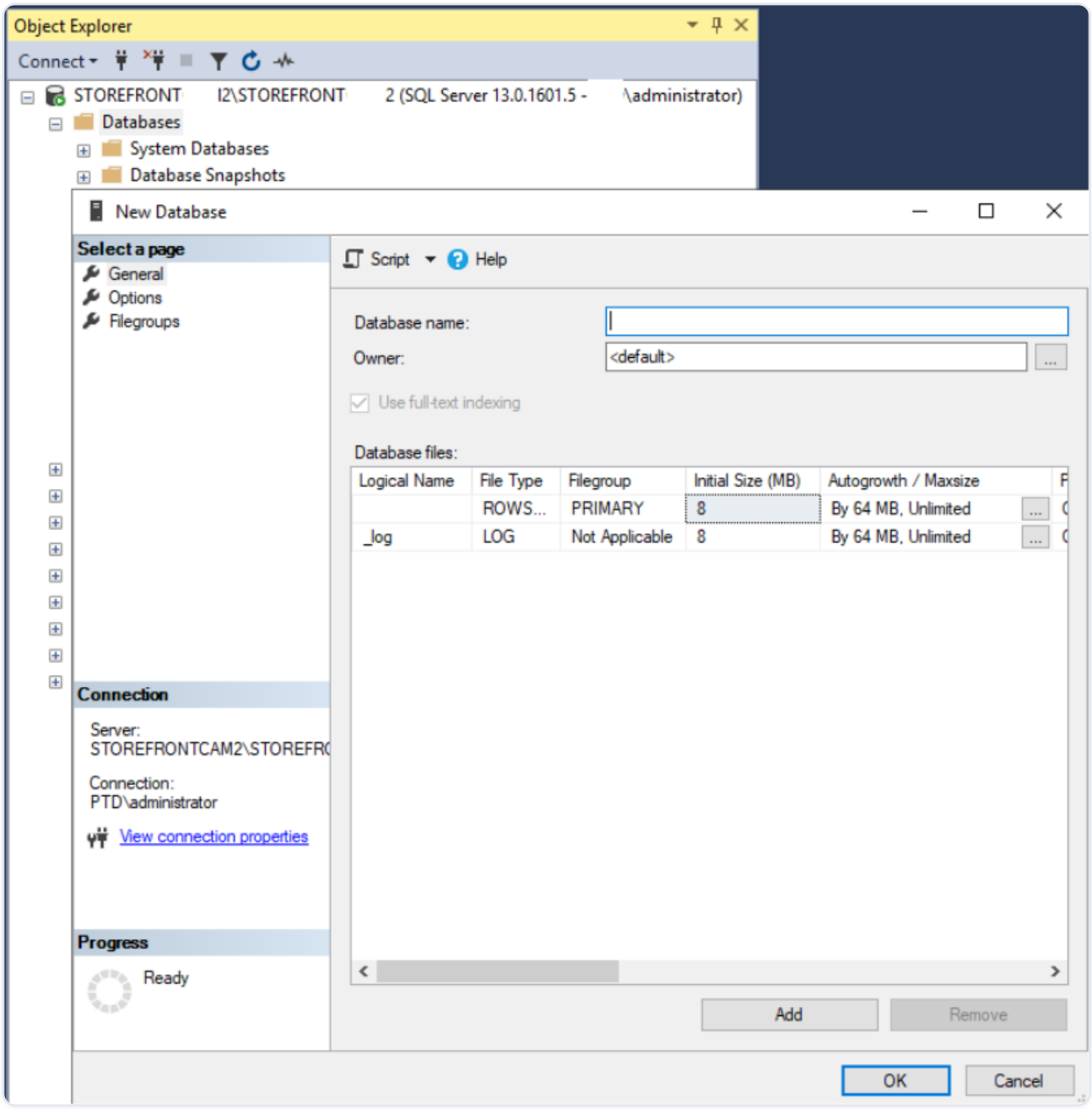
}

Add-RemoteSTFMachineAccounts -Domain "example" -StoreFrontServers
@("StoreFrontSQL1","StoreFrontSQL2")
```

为每个应用商店在 Microsoft SQL Server 中配置订阅数据库架构

在 Microsoft SQL Server 上创建一个命名实例供 StoreFront 使用。将 .SQL 脚本中的路径设置为与您的 SQL 版本安装位置或其数据库文件存储位置相对应。示例脚本 Create-StoreSubscriptionsDB-2016.sql 使用 SQL Server 2016 Enterprise。

通过右键单击“**数据库**”，然后选择“**新建数据库**”，使用 SQL Server Management Studio (SSMS) 创建一个空数据库。



键入与您的应用商店匹配的“**数据库名称**”，或选择其他名称，例如 *STFSubscriptions*。

运行脚本之前，对于 StoreFront 部署中的每个应用商店，修改示例脚本中的引用以匹配您的 StoreFront 和 SQL 部署。例如，修改：

- 将您创建的每个数据库命名为与 `USE [STFSubscriptions]` 中 StoreFront 的应用商店名称匹配。
- 将数据库 .mdf 和 .ldf 文件的路径设置为您希望存储数据库的位置。

  ```
  C:\Program Files\Microsoft SQL Server\MSSQL13.SQL2016\MSSQL\DATA\STFSubscriptions.mdf
  ```

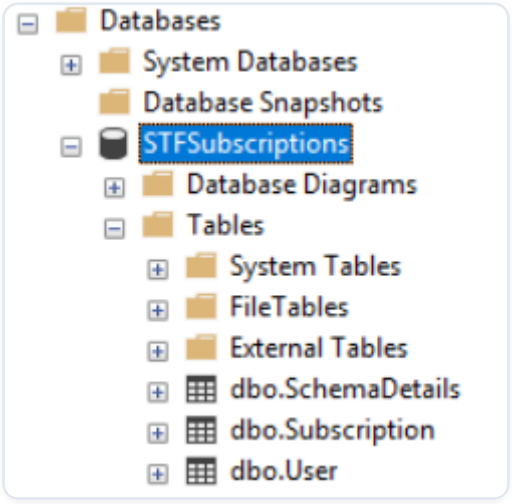
```
C:\Program Files\Microsoft SQL
Server\MSSQL13.SQL2016\MSSQL\DATA\STFSubscriptions.ldf
```

- 在脚本中设置对 SQL Server 名称的引用：

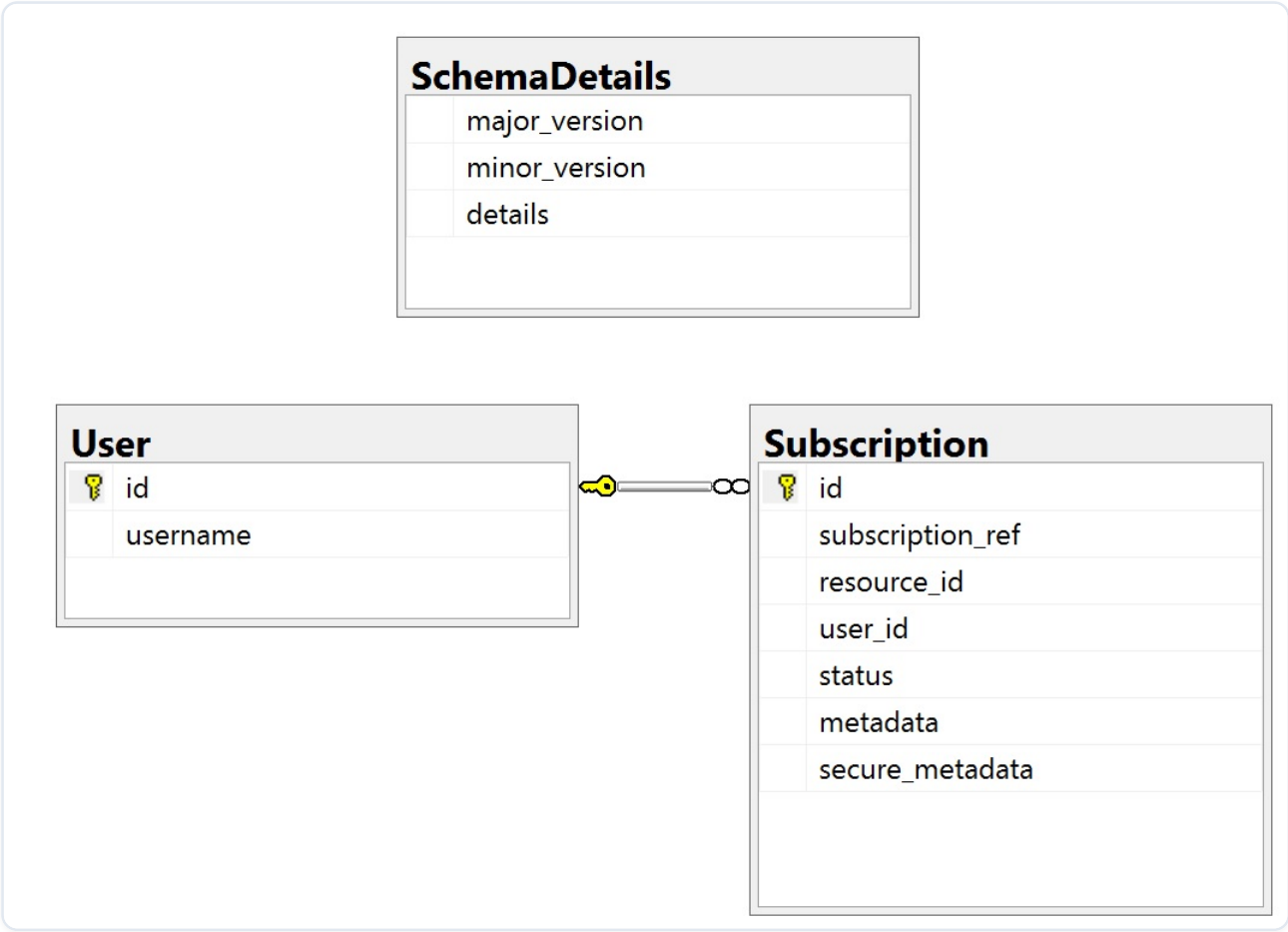
```
CREATE LOGIN [SQL2016\StoreFrontServers] FROM WINDOWS;
```
;

```
ALTER LOGIN [SQL2016\StoreFrontServers]
```

运行脚本。成功配置架构后，将创建三个数据库表：*SchemaDetails*、*Subscription* 和 *User*。



以下数据库图显示了由 *Create-StoreSubscriptionsDB-2016.sql* 脚本创建的订阅数据库架构：



为每个 StoreFront 存储配置 SQL Server 连接字符串

场景 1

> **提示：**
>
> 存储在 ESENT 数据库磁盘上的原始订阅数据不会被销毁或删除。如果您决定从 Microsoft SQL Server 恢复为使用 ESENT，可以删除存储连接字符串并简单地切换回使用原始数据。在存储使用 SQL 期间创建的任何额外订阅将不会存在于 ESENT 中，用户也看不到这些新的订阅记录。所有原始订阅记录仍将存在。

在存储上重新启用 ESENT 订阅

打开 PowerShell ISE 并选择 **以管理员身份运行**。

使用 **-UseLocalStorage** 选项指定要重新启用 ESENT 订阅的存储：

```
$SiteID = 1

$StoreVirtualPath = "/Citrix/Store1"



# Sets SQL DB Connection String

$StoreObject = Get-STFStoreService -SiteID $SiteID -VirtualPath
$StoreVirtualPath



# Removes the SQL DB Connection string and reverts back to using ESENT

Set-STFStoreSubscriptionsDatabase -StoreService $StoreObject
-UseLocalStorage

Get-STFStoreSubscriptionsDatabase -StoreService $StoreObject
```

场景 2、3 和 4

打开 PowerShell ISE 并选择 **以管理员身份运行**。

使用 **\$StoreVirtualPath** 指定要为其设置连接字符串的存储

```
$SiteID = 1

$VirtualPath= "/Citrix/Store1"

$DBName = "Store1"

$DBServer = "SQL2016Ent"

$DBLocalServer = "localhost"

$SQLInstance = "StoreFrontInstance"



# For a remote database instance
```

```
$ConnectionString = "Server=$DBServer\
$SQLInstance;Database=$DBName;Trusted_Connection=True;"
```

或

```
# For a locally installed database instance

$ConnectionString = "$DBLocalServer\
$SQLInstance;Database=$DBName;Trusted_Connection=True;"



# Sets SQL DB Connection String

$StoreObject = Get-STFStoreService -SiteID $SiteID -VirtualPath "/Citrix/
Store"

Set-STFStoreSubscriptionsDatabase -StoreService $StoreObject
-ConnectionString $ConnectionString

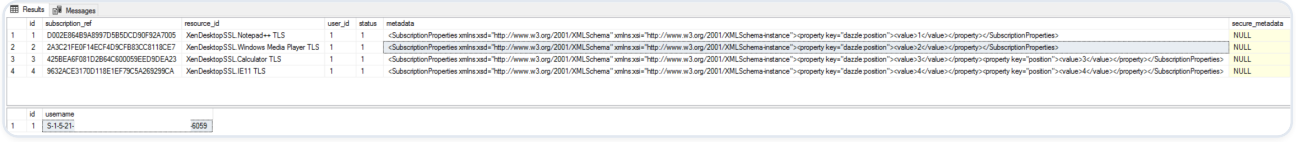
Get-STFStoreSubscriptionsDatabase -StoreService $StoreObject
```

如果您想将部署中的所有存储都配置为使用 SQL 连接字符串，请对每个存储重复此过程。

将现有数据从 ESENT 迁移到 Microsoft SQL Server

要将现有 ESENT 数据迁移到 SQL，需要一个两步数据转换过程。提供了两个脚本来帮助您执行此一次性操作。如果 StoreFront 中的连接字符串和 SQL 实例配置正确，则所有新订阅都会在 SQL 中以正确的格式自动创建。迁移后，历史 ESENT 订阅数据将转换为 SQL 格式，用户也可以看到他们以前订阅的资源。

示例：同一域用户的四个 SQL 订阅



步骤 1 使用 TRANSFORM-SUBSCRIPTIONDATAFORSTORE.PS1 脚本将 ESENT 数据转换为适合批量导入的 SQL 格式

登录到要从中转换 ESENT 数据的 StoreFront 服务器。

服务器组中的任何成员都适用，前提是它们都包含相同数量的订阅记录。

打开 PowerShell ISE 并选择 **以管理员身份运行**。

运行脚本 Transform-SubscriptionDataForStore.ps1，该脚本将 `<StoreName>.txt` 文件从 ESENT 数据库导出到当前用户的桌面。

PowerShell 脚本会针对处理的每一行订阅提供详细反馈，以帮助调试并评估操作的成功性。这可能需要很长时间才能处理完成。

脚本完成后，转换后的数据将写入当前用户桌面上的 `<StoreName>SQL.txt`。脚本会汇总唯一用户记录的数量和已处理的订阅总数。

对于要迁移到 SQL Server 的每个存储，重复此过程。

步骤 2 使用 T-SQL 存储过程批量 SQL 导入转换后的数据

每个存储的数据必须一次导入一个存储。

将步骤 1 中创建的 `<StoreName>SQL.txt` 文件从 StoreFront 服务器的桌面复制到 Microsoft SQL Server 上的 `C:\`，并将其重命名为 SubscriptionsSQL.txt。

Create-ImportSubscriptionDataSP.sql 脚本创建一个 T-SQL 存储过程，用于批量导入订阅数据。它会删除每个唯一用户的重复条目，以便生成的 SQL 数据正确规范化并拆分到正确的表中。

在执行 *Create-ImportSubscriptionDataSP.sql* 之前，请将 `USE [STFSubscriptions]` 更改为与您要创建存储过程的数据库匹配。

使用 SQL Server Management Studio 打开 *Create-ImportSubscriptionDataSP.sql* 文件并执行其中的代码。此脚本会将 *ImportSubscriptionDataSP* 存储过程添加到您之前创建的数据库中。

成功创建存储过程后，SQL 控制台中会显示以下消息，并且 ImportSubscriptionDataSP 存储过程会添加到数据库中：

`Commands completed successfully.`.

存储过程已添加到数据库中(/en-us/storefront/2507-ltsr/media/manage-deployment/sql-server-stored-procedure-added.png)

右键单击存储过程，然后选择 **Execute Stored Procedure**，再单击 **OK** 以执行它。

执行存储过程屏幕截图(/en-us/storefront/2507-ltsr/media/manage-deployment/sql-server-execute-procedure.png)

返回值 0 表示所有数据均已成功导入。导入过程中出现的任何问题都会记录到 SQL 控制台。存储过程成功运行后，请将 Transform-SubscriptionDataForStore.ps1 提供的订阅记录总数和唯一用户数与下面两个 SQL 查询的结果进行比较。这两个总数应该匹配。

转换脚本中的订阅总数应与 SQL 报告的总数匹配，通过

```
SELECT COUNT(*) AS TotalSubscriptions

FROM [Subscription]
```

转换脚本中的唯一使用次数应与 SQL 报告的用户表中的记录数匹配，通过

```
SELECT COUNT(*) AS TotalUsers

FROM [User]
```

如果转换脚本显示 100 个唯一用户和 1000 条订阅记录总数，那么在成功迁移后，SQL 也应显示相同的两个数字。

登录 StoreFront 以检查现有用户是否可以看到其订阅数据。当用户订阅或取消订阅其资源时，SQL 中的现有订阅记录会更新。新用户和订阅记录也会在 SQL 中创建。

步骤 3 在导入的数据上运行 T-SQL 查询

> **注意：**
>
> 所有 Delivery Controller 名称都区分大小写，并且必须与 StoreFront 中使用的名称和大小写完全匹配。

```
-- Get all SQL subscription records

Use [STFSubscriptions]

SELECT * FROM [Subscription]

SELECT * FROM [User]
```

```
-- Get all subscription records for a particular user SID

Use [STFSubscriptions]

SELECT * FROM [Subscription]
```

```
INNER JOIN [User]

ON [Subscription].[user_id] = [User].[id]

WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-xxxx'



-- Get total number of Subscription records for a particular user SID

Use [STFSubscriptions]

SELECT COUNT(Subscription.id)

FROM [Subscription]

INNER JOIN [User]

ON [Subscription].[user_id] = [User].[id]

WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-xxxx'
```

```
-- Get all subscription records for a particular delivery controller

Use [STFSubscriptions]

SELECT * FROM [Subscription]

WHERE [resource_id] LIKE 'DeliveryController.%'



-- OR for aggregated resources use the name of the aggregation group

Use [STFSubscriptions]

SELECT * FROM [Subscription]

WHERE [resource_id] LIKE 'DefaultAggregationGroup.%'
```

```
-- Get all subscription records for a particular application

Use [STFSubscriptions]

SELECT * FROM [Subscription]

WHERE [resource_id] = ' DeliveryController.Application'
```

使用 T-SQL 更新或删除现有订阅记录

免责声明：

所有示例 SQL 更新和删除语句均由您自行承担风险。Citrix 不对因不正确使用所提供的示例而导致的订阅数据丢失或意外更改负责。以下 T-SQL 语句旨在作为执行简单更新的指南。在尝试更新订阅或删除过时记录之前，请务必对 SQL 数据库中的所有订阅数据进行完整备份。未能执行必要的备份可能会导致数据丢失或损坏。在对生产数据库执行您自己的 T-SQL UPDATE 或 DELETE 语句之前，请在虚拟数据或生产数据的冗余副本上进行测试，远离实时生产数据库。

注意：

所有站点名称都区分大小写，并且必须与 StoreFront 中使用的大小写和名称完全匹配。

```
-- Update the site name used in all subscriptions.

Use [STFSubscriptions]

UPDATE [Subscription]

SET [resource_id] = REPLACE(resource_id,'OldSiteName.','NewSiteName.')

WHERE [resource_id] LIKE 'OldDeliveryController.%'
```

```
-- After enabling multi-site aggregation, update the resource_id

Use [STFSubscriptions]
```

```
UPDATE [Subscription]

SET [resource_id] =
REPLACE(resource_id,'OldDeliveryController.','DefaultAggregationGroup.')

WHERE [resource_id] LIKE 'OldDeliveryController.%'
```

```
-- Delete all subscription records for a particular site

Use [STFSubscriptions]

DELETE FROM [Subscription]

WHERE [resource_id] LIKE 'site.%'
```

```
-- OR for aggregated resources use the name of the aggregation group

Use [STFSubscriptions]

DELETE FROM [Subscription]

FROM [Subscription]

WHERE [resource_id] LIKE 'DefaultAggregationGroup.%'
```

```
-- Delete all subscription records for a particular application

Use [STFSubscriptions]

DELETE FROM [Subscription]

FROM [Subscription]

WHERE [resource_id] LIKE '%.Application'
```

```
-- Delete all subscription records for an application published via a
specific site

Use [STFSubscriptions]
```

```
DELETE FROM [Subscription]

FROM [Subscription]

WHERE [resource_id] = 'Site.Application'
```

```
-- Delete all subscription records for a particular user SID

-- relies on cascade to delete records from [Subscription]

Use [STFSubscriptions]

DELETE FROM [User]

WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-xxxx'
```

```
-- Delete ALL subscription data from a particular database and reset the
primary key clustered index to start numbering from 0.

-- USE WITH EXTREME CARE AND NOT ON LIVE PRODUCTION DATABASES.

-- Can be useful whilst debugging data import issues to start with a clean
database.



Use [STFSubscriptions]

DELETE FROM [Subscription]

DBCC CHECKIDENT ([Subscription], RESEED, 0)

DELETE FROM [User]

DBCC CHECKIDENT ([User], RESEED, 0)
```

订阅同步

StoreFront 会自动同步收藏夹（也称为订阅）在 StoreFront 服务器组中的服务器之间。如果您有多个服务器组（通常位于不同的地理位置），则可以配置从不同 StoreFront 部署中的存储区定期拉取用户订阅的同步。这必须使用 PowerShell 完成。

> **注意：**
>
> StoreFront 和 PowerShell 控制台不能同时打开。在使用 PowerShell 控制台管理 StoreFront 配置之前，请务必关闭 StoreFront 管理控制台。同样，在打开 StoreFront 控制台之前，请关闭所有 PowerShell 实例。

> 在建立订阅同步时，请注意，配置的站点在同步的存储区之间必须命名相同，包括大小写。未能完全复制站点名称可能会导致用户在同步的存储区中拥有不同的订阅。如果您正在从聚合资源同步订阅，则两个存储区使用的聚合组名称也必须匹配。站点名称和聚合组名称区分大小写；例如，*CVAD_US* 与 *Cvad_Us* 不同。

1. 使用具有本地管理员权限的帐户启动 Windows PowerShell ISE。
2. 要配置同步，请使用 Publish-STFServerGroupConfiguration 命令。您可以指定开始时间、重复间隔或时间列表。例如，要在 08:00 开始同步，然后每 30 分钟同步一次：

   ```
   Add-STFSubscriptionSynchronizationSchedule -RecurringStartTime 08:00:00
   -RecurringInterval 30
   ```

   我们建议您错开拉取计划，以避免两个服务器组同时尝试从彼此拉取订阅数据。例如，从每个服务器组每 60 分钟拉取一次数据的计划将配置如下。服务器组 1 在 01:00、02:00、03:00 等时间从服务器组 2 拉取数据。服务器组 2 在 01:30、02:30、03:30 等时间从服务器组 1 拉取数据。
3. 要指定包含要同步的存储区的远程 StoreFront 部署，请键入以下命令。您必须为每个驻留 StoreFront 服务器组的数据中心配置此项，以便它可以从其他远程数据中心拉取订阅数据。请参阅以下美国和英国数据中心示例：

   - 在美国数据中心 StoreFront 服务器上运行以从英国数据中心服务器拉取数据：

     ```
     $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/Citrix/
     Store"

     Add-STFSubscriptionSynchronizationSource -FriendlyName
     ```

```
"SyncFromUKStore" -StoreService $StoreObject
-RemoteStoreFrontAddress "UKloadbalancedStoreFront.example.com"
```

- 在英国数据中心 StoreFront 服务器上运行以从美国数据中心服务器拉取数据：

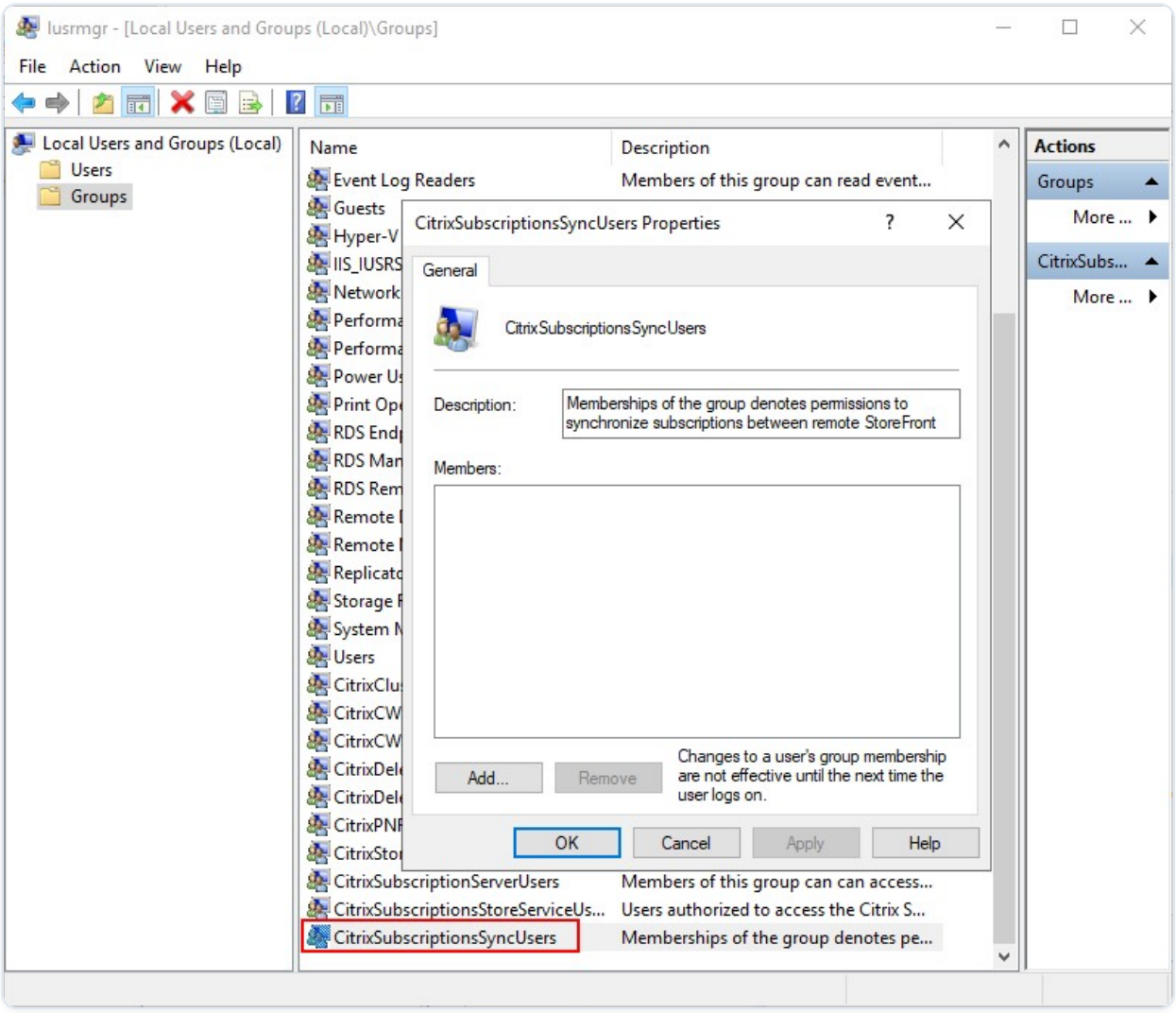
```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/Citrix/
Store"

Add-STFSubscriptionSynchronizationSource -FriendlyName
"SyncFromUSStore" -StoreService $StoreObject
-RemoteStoreFrontAddress "USloadbalancedStoreFront.example.com"
```

其中 *FriendlyName* 是一个帮助您识别远程部署的名称，*RemoteStoreFrontAddress* 是远程部署的 StoreFront 服务器或负载均衡服务器组的 FQDN。要在两个或更多存储区之间同步应用程序订阅，所有要同步的存储区在其各自的 StoreFront 部署中必须具有相同的名称。

4. 将远程部署中每个 StoreFront 服务器的 Microsoft Active Directory 域计算机帐户添加到当前服务器上的本地 Windows 用户组 CitrixSubscriptionSyncUsers。

   配置同步计划后，这允许当前服务器从 CitrixSubscriptionSyncUsers 中列出的远程服务器拉取新的或更新的订阅数据。有关修改本地用户组的更多信息，请参阅 `<https://docs.microsoft.com/zh-cn/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc772524(v=ws.11)>`。



5. 按照您的意图配置计划后，使用 Citrix StoreFront 管理控制台或下面的 PowerShell，将订阅同步计划和源传播到组中的所有其他服务器。

```
Publish-STFServerGroupConfiguration
```

有关在多服务器 StoreFront 部署中传播更改的更多信息，请参阅 配置服务器组。

6. 要删除现有订阅同步计划，请运行以下命令，然后将配置更改传播到部署中的其他 StoreFront 服务器。

```
Clear-STFSubscriptionSynchronizationSchedule

Publish-STFServerGroupConfiguration
```

7. 要删除特定的订阅同步源，请运行以下命令，然后将配置更改传播到部署中的其他 StoreFront 服务器。

```
Remove-STFSubscriptionSynchronizationSource -FriendlyName
"SyncFromUKStore"

Publish-STFServerGroupConfiguration
```

8. 要删除所有现有订阅同步源，请运行以下命令，然后将配置更改传播到部署中的其他 StoreFront 服务器。

```
Clear-STFSubscriptionSynchronizationSource

Publish-STFServerGroupConfiguration
```

9. 要列出当前为 StoreFront 部署配置的订阅同步计划，请运行以下命令。

```
Get-STFSubscriptionSynchronizationSchedule
```

10. 要列出当前为 StoreFront 部署配置的订阅同步源，请运行以下命令。

```
Get-STFSubscriptionSynchronizationSource
```

升级 StoreFront™

升级会保留您的 StoreFront 配置，并使用户的收藏夹保持不变。相比之下，卸载 StoreFront 会删除 StoreFront 及相关服务、站点、收藏夹（在独立服务器上）和相关配置。

支持的升级路径

您可以从以下版本升级到 StoreFront 2507：

- StoreFront 2503.1
- StoreFront 2503
- StoreFront 2407
- StoreFront 2402 LTSR（任何 CU）
- StoreFront 2203 LTSR（任何 CU）
- StoreFront 1912 LTSR CU10

无法从 2402 CU2 或更高版本的 CU 升级到 2407 或 2411。

须知

- StoreFront 不支持包含不同产品版本的多个服务器部署，因此，在授予对部署的访问权限之前，服务器组中的所有服务器都必须升级到同一版本。
- 多个服务器部署不支持并发升级，服务器必须按顺序升级。
- 在 StoreFront 升级运行之前，它会执行一些预升级检查。如果任何预升级检查失败，升级将不会启动，并且您会收到失败通知。您的 StoreFront 安装保持不变。修复失败原因后，重新运行升级。
- 如果 StoreFront 升级本身失败，您现有的 StoreFront 安装可能会丢失其初始配置。将您的 StoreFront 安装恢复到正常运行状态，然后重新运行升级。要将 StoreFront 恢复到正常运行状态，请考虑以下方法：
  - 恢复您在升级前创建的 VM 快照，
  - 导入您在升级前导出的 StoreFront 配置，请参阅导出和导入 StoreFront 配置，
  - 执行解决升级问题中的故障排除建议。
- Citrix Virtual Apps and Desktops 元安装程序导致的任何 StoreFront 升级失败都会在对话框中报告，并提供相关失败日志的链接。

准备升级

在开始升级之前，我们建议您执行以下步骤，以防止升级失败：

- 在升级前规划您的备份策略。
- 验证您是否正在从受支持的版本升级。
- 从 Citrix 网站下载 StoreFront 安装程序。

升级单个 StoreFront 服务器

1. 通过创建 VM 快照来备份服务器。
2. 导出现有 StoreFront 配置。如果服务器组中有多个服务器，则只需从其中一个服务器导出服务器组配置。只要您已在它们之间传播了所有更改，服务器组中的所有服务器都会维护配置的相同副本。此备份使您可以轻松构建新的服务器组，以便在出现问题时轻松恢复配置。请注意，您只能将此备份恢复到运行与导出时相同版本的服务器中。
3. 如果您修改了 `C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data` 或 `C:\inetpub\wwwroot\Citrix\<StoreName>Auth\App_Data` 中的文件（例如 default.ica 和 usernamepassword.tfrm），请为每个应用商店备份它们。升级后，您可以恢复它们以重新应用您的修改。

4. 通过从任何负载平衡器中移除服务器或以其他方式阻止连接来阻止用户连接。
5. 重新启动服务器。
6. 确保没有正在运行的应用程序，包括 StoreFront 管理控制台、命令行和 PowerShell 窗口，或任何其他可能锁定 StoreFront 文件的应用程序。这可确保安装程序在升级期间可以访问所有 StoreFront 文件。如果安装程序无法访问任何文件，则这些文件将不会被替换，并且升级将失败，从而导致现有 StoreFront 配置被删除。
7. 确保没有在包含 StoreFront 文件的目录中打开任何 Windows 资源管理器或命令提示符。
8. 禁用所有防病毒应用程序。
9. 运行所需 StoreFront 版本的安装文件。

在计划的维护停机期间升级 StoreFront 服务器组

要在计划的停机期间升级包含多个服务器的 StoreFront 服务器组，请完成以下步骤：

1. 通过禁用负载平衡 URL 来禁用用户对服务器组的访问。这可以防止用户在升级过程中连接到部署。
2. 按照 升级单个 StoreFront 服务器 中的说明升级每台服务器。
3. 检查所有服务器是否正常运行。
4. 通过启用负载平衡 URL 来启用用户对已升级服务器组的访问。

在不停机的情况下升级 StoreFront 服务器组

不支持同时升级实时 StoreFront 服务器组中的服务器。但是，您可以通过创建具有相同配置的新服务器组，对其进行升级，然后将用户连接迁移到新服务器组来实现实时升级。用户在服务器组之间转移时需要重新向 StoreFront 进行身份验证。

例如，要升级包含三台服务器 A、B 和 C 的 StoreFront 服务器组：

1. 使用 **Export-STFConfiguration** 导出 StoreFront 配置。此备份是必需的，因为服务器稍后将在过程中恢复出厂设置，这将删除配置数据。
2. 使用 **Export-STFStoreSubscriptions** 从服务器 A 导出订阅数据。此备份是必需的，因为服务器稍后将在过程中恢复出厂设置，这将删除订阅数据。请参阅 管理商店的订阅数据。
3. 禁用用户访问服务器 C，方法是将其从负载均衡器中移除。这可以防止用户在升级过程中连接到服务器 C。负载均衡器会继续将请求发送到服务器 A 和 B。
4. 使用服务器 A 将服务器 C 从组中移除。 服务器 A 和 B 继续为用户提供对其资源的访问。服务器 C 现在已从服务器组中脱离，并已恢复出厂设置。
5. 使用 **Clear-STFDeployment** 将脱离的服务器 C 重置为出厂默认设置。

6. 使用 **Import-STFConfiguration** 将您之前导出的 StoreFront 配置导入到服务器 C。服务器 C 现在具有与旧服务器组相同的配置。以后*无需*再次重复此步骤。只需一台服务器拥有配置数据的副本，即可将其传播到加入组的任何其他服务器。
7. 按照 升级单个 StoreFront 服务器 中的说明升级服务器 C。服务器 C 现在具有与旧服务器组相同的配置，并已升级到新版本的 StoreFront。
8. 将您之前导出的订阅数据导入到服务器 C。以后*无需*再次重复此步骤。只需一台服务器拥有订阅数据的副本，即可将其传播到加入组的任何其他服务器。
9. 使用服务器 B 重复步骤 3、4、5 和 7（不要重复步骤 6）。在此期间，只有服务器 A 为用户提供对资源的访问。因此，建议在工作量较小的时段执行此步骤，此时 StoreFront 服务器组的负载预计会很小。
10. 使用 加入现有服务器组 过程将服务器 B 加入服务器 C。这会在当前版本的 StoreFront 上提供单个服务器部署（服务器 A），并在新版本的 StoreFront 上提供一个新的双节点服务器组（服务器 B 和 C）。
11. 将服务器 B 和 C 添加到负载均衡服务，以便它们可以接替服务器 A。
12. 从负载均衡器中移除服务器 A，以便用户被定向到新升级的服务器 B 和 C。
13. 使用服务器 A 重复步骤 5、7、10 和 11（不要重复步骤 6）。服务器组升级过程现已完成。服务器 A、B 和 C 具有与原始组相同的配置和订阅数据。

> **注意：**
>
> 在服务器 A 是唯一可访问服务器的短暂期间，收藏夹可能会丢失（步骤 9）。这可能导致新服务器组在升级后拥有略微过时的订阅数据库副本，并且任何新的收藏夹都会丢失。
>
> 这没有功能影响，因为收藏夹数据对于用户登录和启动资源并非必不可少。但是，在服务器 A 恢复出厂设置并加入新升级的组后，用户需要再次收藏资源。尽管不太可能丢失超过少数几个收藏夹记录，但这是在不停机的情况下升级实时 StoreFront 生产环境可能导致的结果。

解决升级问题

1. 在 *C:\Windows\Temp\StoreFront* 中，打开最新的 *CitrixMsi*.log* 并搜索任何异常错误。

   Thumbs.db 访问 异常：由 *C:\inetpub\wwwroot\citrix* 内部或其子目录中的 *thumbs.db* 文件引起。删除找到的任何 *thumbs.db* 文件。

   无法获取独占文件访问权限 \正在使用 异常：如果可用，恢复快照/备份，或重新启动服务器，并手动停止任何 StoreFront 服务。

服务无法启动 异常：如果可用，恢复快照/备份，或安装完整版 .NET framework 4.5（而非客户端配置文件）。

2. 如果 *CitrixMsi*.log* 中没有异常错误，请检查服务器的 **事件查看器 > 交付服务**，查找包含上述异常错误消息的任何错误。遵循相应的建议。
3. 如果事件查看器中没有异常错误，请检查 *C:\Program Files\Citrix\Receiver StoreFront\logs* 中的管理员日志，查找包含上述异常错误消息的任何错误。遵循相应的建议。

有关日志文件的更多详细信息，请参阅 安装日志。

导出和导入 StoreFront 配置

> 注意：
>
> 您只能导入与目标 StoreFront 安装版本相同的 StoreFront 配置。
>
> 您可以导出 StoreFront 部署的整个配置。这包括单服务器部署和服务器组配置。如果导入服务器上已存在现有部署，则当前配置将被擦除，然后替换为备份存档中包含的配置。如果目标服务器是干净的出厂默认安装，则将使用备份中存储的导入配置创建一个新的部署。导出的配置备份如果未加密，则为单个 .zip 存档形式；如果您选择在创建备份文件时对其进行加密，则为 .ctxzip 形式。

可使用配置导出和导入的场景

- 仅备份处于正常工作且受信任状态的 StoreFront 部署。对配置的任何更改都需要进行新的备份来替换旧的备份。您无法修改现有备份，因为 backup.zip 文件的文件哈希值会阻止修改。
- 在升级 StoreFront 之前进行备份以进行灾难恢复。
- 克隆现有测试 StoreFront 部署以投入生产
- 通过将生产部署克隆到测试环境中来创建用户验收环境。
- 在操作系统迁移期间移动 StoreFront，例如将托管从 Windows Server 2019 升级到 Windows 2022。不支持就地操作系统升级。
- 在多地理部署中构建额外的服务器组，例如在拥有多个数据中心的大型企业中。

导出和导入 StoreFront 配置时要考虑的事项

- 您当前是否使用任何 Citrix® 发布的身份验证 SDK 示例，例如 Magic Word 身份验证或第三方身份验证自定义？如果是，则在导入包含额外身份验证方法的配置之前，必须在所有导入服务器上

安装这些软件包。如果任何导入服务器上未安装所需的身份验证 SDK 软件包，则配置导入将失败。如果将配置导入服务器组，请在组的所有成员上安装身份验证软件包。

- 您可以加密或解密配置备份。导出和导入 PowerShell cmdlet 支持这两种用例。
- 您可以稍后解密加密备份 (.ctxzip)，但 StoreFront 无法重新加密未加密的备份文件 (.zip)。如果需要加密备份，请使用包含您选择的密码的 PowerShell 凭据对象再次执行导出。
- StoreFront 当前安装在 IIS 中的网站 (导出服务器) 的 SiteID 必须与您要恢复备份的 StoreFront 配置的 IIS 中的目标网站 (导入服务器) 的 SiteID 匹配。

PowerShell cmdlet 命令

Export-STFConfiguration

参数	描述
-TargetFolder (字符串)	备份存档的导出路径。示例: "\$env:userprofile\desktop\"
-Credential (PSCredential 类型的对象)	指定一个凭据对象，以便在导出期间创建加密的 .ctxzip 备份存档。PowerShell 凭据对象应包含用于加密和解密的密码。请勿同时使用 **-Credential** 和 **-NoEncryption** 参数。示例: \$CredObject
-NoEncryption (开关)	指定备份存档应为未加密的 .zip 文件。请勿同时使用 **-NoEncryption** 和 **-Credential** 参数。
-ZipFileName (字符串)	StoreFront 配置备份存档的名称。请勿添加文件扩展名，例如 .zip 或 .ctxzip。文件扩展名将根据导出期间是否指定了 **-Credential** 或 **-NoEncryption** 参数自动添加。示例: "backup"
-Force (布尔值)	此参数会自动覆盖与指定导出位置中已存在的备份文件同名的备份存档。

重要提示：

StoreFront 3.5 中的 **SiteID** 参数在 3.6 版本中已弃用。执行导入时不再需要指定 **SiteID**，因为备份存档中包含的 SiteID 始终会被使用。确保 SiteID 与导入服务器上 IIS 中已配置的现有 StoreFront 网站匹配。不支持 **SiteID 1** 到 **SiteID 2** 的配置导入。

Import-STFConfiguration

参数	描述
-ConfigurationZip (字符串)	要导入的备份存档的完整路径。这也应包含文件扩展名。未加密的备份存档使用 .zip，加密的备份存档使用 .ctxzip。示例：`$env:userprofile\desktop\backup.ctxzip`
-Credential (PSCredential 对象)	指定一个凭据对象，用于在导入期间解密加密备份。示例：`$CredObject`
-HostBaseURL (字符串)	如果包含此参数，则使用您指定的主机基本 URL，而不是导出服务器中的主机基本 URL。示例：`https://<importingserver>.example.com`

Unprotect-STFConfigurationBackup

参数	描述
-TargetFolder (字符串)	备份存档的导出路径。示例：`$env:userprofile\desktop`
-凭据 (PSCredential 对象)	使用此参数创建加密备份存档的未加密副本。指定包含用于解密的密码的 PowerShell 凭据对象。示例：`$CredObject`
-EncryptedConfigurationZip (字符串)	要解密的加密备份存档的完整路径。您必须指定文件扩展名 .ctxzip。示例：`$env:userprofile\\desktop\\backup.ctxzip`
-OutputFolder (字符串)	用于创建加密 (.ctxzip) 备份存档的未加密副本 (.zip) 的路径。备份的原始加密副本将保留，以便可以重复使用。请勿为未加密副本指定文件名和文件扩展名。示例：`$env:userprofile\desktop`
-Force (布尔值)	此参数会自动覆盖与指定导出位置中已存在的现有备份文件具有相同文件名的备份存档。

配置导出和导入示例

将 StoreFront cmdlet 导入当前 PowerShell 会话

在 StoreFront 服务器上打开 PowerShell 集成脚本环境 (ISE) 并运行：

```
$env:PSModulePath =
[Environment]::GetEnvironmentVariable('PSModulePath','Machine')

$SDKModules = 'C:\Program Files\Citrix\Receiver
StoreFront\PowerShellSDK\Modules\Citrix.StoreFront'

Import-Module "$SDKModules\Citrix.StoreFront.psd1" -verbose

Import-Module
"$SDKModules.Authentication\Citrix.StoreFront.Authentication.psd1"
-verbose

Import-Module "$SDKModules.Roaming\Citrix.StoreFront.Roaming.psd1"
-verbose

Import-Module "$SDKModules.Stores\Citrix.StoreFront.Stores.psd1" -verbose

Import-Module "$SDKModules.WebReceiver\Citrix.StoreFront.WebReceiver.psd1"
-verbose
```

单服务器场景

在服务器 A 上创建现有配置的未加密备份并将其还原到同一部署

导出您希望备份的服务器配置。

```
Export-STFConfiguration -targetFolder "$env:userprofile\desktop\"
-zipFileName "backup" -NoEncryption
```

将 backup.zip 文件复制到安全位置。您可以使用此备份进行灾难恢复，将服务器还原到其以前的状态。

```
Import-STFConfiguration -configurationZip
"$env:userprofile\desktop\backup.zip" -HostBaseURL "https://
storefront.example.com"
```

备份服务器 A 上的现有配置并将其还原到服务器 B，以创建现有服务器的克隆

导出您希望备份的服务器配置。

```
Export-STFConfiguration -targetFolder "$env:userprofile\desktop\"
-zipFileName "backup" -NoEncryption
```

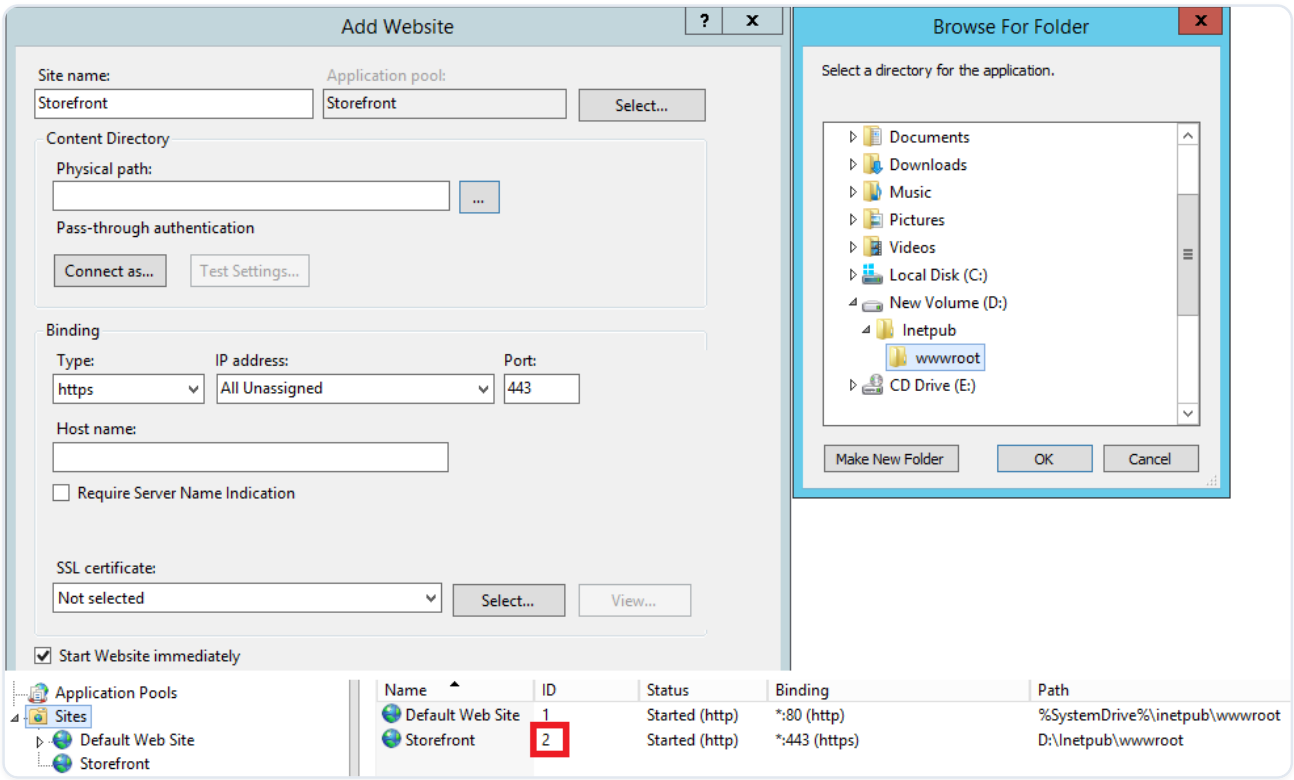
将 backup.zip 文件复制到服务器 B 的桌面。

```
Import-STFConfiguration -configurationZip
"$env:userprofile\desktop\backup.zip" -HostBaseURL "https://
serverB.example.com"
```

StoreFront 已部署到 IIS 中的自定义网站。将配置还原到另一个自定义网站部署

服务器 A 已将 StoreFront 部署到自定义网站位置，而不是 IIS 中常见的默认网站。在 IIS 中创建的第二个网站的 IIS SiteID 为 2。StoreFront 网站的物理路径可以位于非系统驱动器（例如 d:\）或默认的 c:\ 系统驱动器上，但应使用大于 1 的 IIS SiteID。

IIS 中已配置了一个名为 StoreFront 的新网站，它使用 **SiteID = 2**。StoreFront 已部署在 IIS 中的自定义网站上，其物理路径位于驱动器 `d:\inetpub\wwwroot` 上。



1. 导出服务器 A 配置的副本。
2. 在服务器 B 上，使用名为 **StoreFront** 的新网站配置 IIS，该网站也使用 **SiteID 2**。

3. 将服务器 A 配置导入到服务器 B。备份中包含的站点 ID 将被使用，并且必须与您要导入 StoreFront 配置的目标网站匹配。

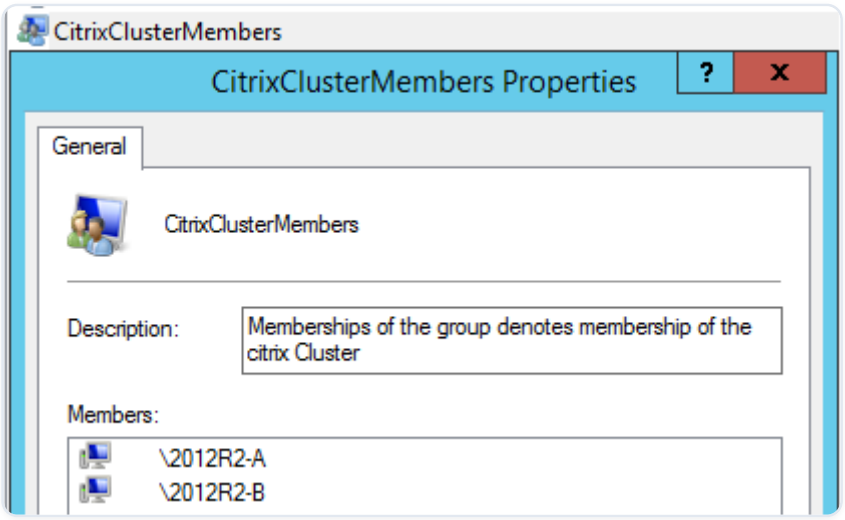
```
Import-STFConfiguration -configurationZip
"$env:userprofile\desktop\backup.ctxzip" -HostBaseURL "https://
serverB.example.com"
```

服务器组场景

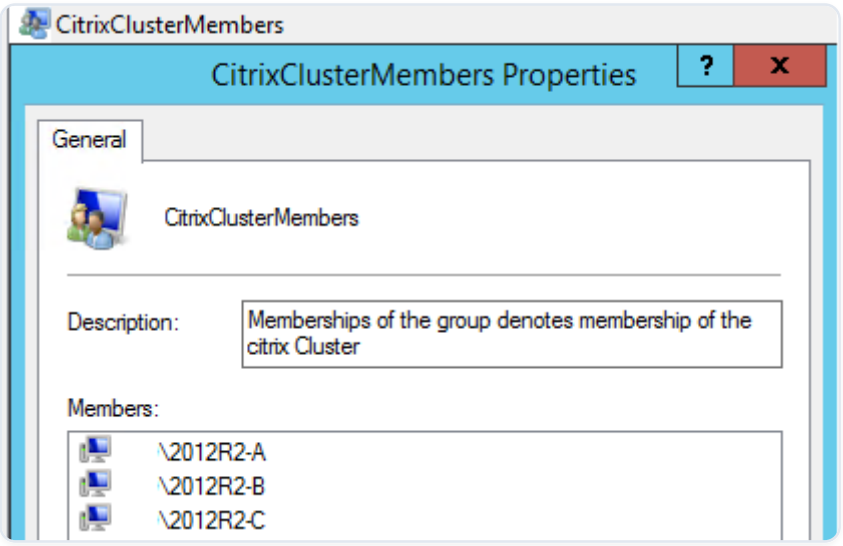
场景 1：备份现有服务器组配置，然后将其恢复到同一服务器组部署中

之前的配置备份是在只有两台 StoreFront 服务器（2012R2-A 和 2012R2-B）是服务器组成员时进行的。备份存档中包含备份时 **CitrixClusterMembership** 的记录，其中仅包含两台原始服务器 2012R2-A 和 2012R2-B。由于业务需求，自原始备份以来，StoreFront 服务器组部署的规模已有所增加，因此已向服务器组添加了额外的节点 2012R2-C。备份中包含的服务器组底层 StoreFront 配置未更改。即使导入的旧备份仅包含两个原始服务器组节点，也必须维护当前包含三台服务器的 CitrixClusterMembership。在导入期间，当前群集成员身份将得到保留，并在配置成功导入到主服务器后写回。如果自原始备份以来服务器组节点已从服务器组中删除，导入还会保留当前的 CitrixClusterMembership。

1. 从 2012R2-A 导出服务器组 1 配置，2012R2-A 是用于管理整个服务器组的主服务器。



2. 稍后，您将额外的服务器 2012R2-C 添加到现有服务器组。



3. 服务器组的配置必须恢复到已知的先前工作状态。StoreFront 在导入过程中备份当前包含三台服务器的 CitrixClusterMembership，并在导入成功后将其恢复。
4. 将服务器组 1 配置重新导入到节点 2012R2-A。

```
Import-STFConfiguration -configurationZip
"$env:userprofile\desktop\backup.ctxzip" -HostBaseURL "https://
servergroup1.example.com"
```

5. 将新导入的配置传播到整个服务器组，以便所有服务器在导入后都具有一致的配置。

场景 2：备份服务器组 1 中的现有配置，并将其用于在不同的出厂默认安装上创建新的服务器组，然后将其他新的服务器组成员添加到新的主服务器

创建服务器组 2，其中包含两台新服务器：2012R2-C 和 2012R2-D。服务器组 2 配置将基于现有部署（服务器组 1）的配置，服务器组 1 也包含两台服务器 2012R2-A 和 2012R2-B。创建新服务器组时，不使用备份存档中包含的 CitrixClusterMembership。当前的 CitrixClusterMembership 始终会备份，并在导入成功后恢复。使用导入的配置创建新部署时，CitrixClusterMembership 安全组仅包含导入服务器，直到其他服务器加入新组。服务器组 2 是一个新部署，旨在与服务器组 1 共存。指定 -HostBaseURL 参数。服务器组 2 将使用新的出厂默认 StoreFront 安装创建。

1. 从 2012R2-A 导出服务器组 1 配置，2012R2-A 是用于管理整个服务器组的主服务器。
2. 将服务器组 1 配置导入到节点 2012R2-C 上，该节点将成为用于管理新创建的服务器组 2 的主服务器。

```
Import-STFConfiguration -configurationZip
"$env:userprofile\desktop\backup.ctxzip" -HostBaseURL "https://
servergroup2.example.com"
```

3. 加入将成为新服务器组 2 部署一部分的任何其他服务器。从服务器组 1 导入的新配置会自动传播到服务器组 2 的所有新成员，因为这是添加新服务器时正常加入过程的一部分。

场景 3：备份服务器组 A 中的现有配置并使用它覆盖服务器组 B 中的现有配置

服务器组 1 和服务器组 2 已存在于两个独立的数据中心。许多 StoreFront 配置更改是在服务器组 1 上进行的，您应该将这些更改应用到另一个数据中心中的服务器组 2。您可以将更改从服务器组 1 移植到服务器组 2。请勿在服务器组 2 上的备份存档中使用 **CitrixClusterMembership**。在导入期间指定 **-HostBaseURL** 参数，因为服务器组 2 的主机基本 URL 不应更改为服务器组 1 当前使用的相同 FQDN。服务器组 2 是一个现有部署。

1. 从 2012R2-A 导出服务器组 1 配置，2012R2-A 是用于管理整个服务器组的主服务器。
2. 将服务器组 1 配置导入到节点 2012R2-C 上的出厂默认安装中，该节点将成为新服务器组 2 的主服务器。

```
Import-STFConfiguration -configurationZip
"$env:userprofile\desktop\backup.zip" -NoEncryption -HostBaseURL
"https://servergroup2.example.com"
```

创建服务器配置的加密备份

PowerShell 凭据对象包含 Windows 帐户用户名和密码。PowerShell 凭据对象可确保您的密码在内存中受到保护。

> **注意：**
>
> 要加密配置备份存档，您只需要密码即可执行加密和解密。凭据对象中存储的用户名不使用。您必须在用于导出和导入服务器的 PowerShell 会话中创建包含相同密码的凭据对象。在凭据对象中，您可以指定任何用户。
>
> PowerShell 要求您在创建新凭据对象时指定用户。此示例代码为方便起见获取当前登录的 Windows 用户。

在导出服务器上的 PowerShell 会话中创建 PowerShell 凭据对象。

```
$User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name

$Password = "Pa55w0rd"
```

```
$Password = $Password | ConvertTo-SecureString -asPlainText -Force

$CredObject = New-Object System.Management.Automation.PSCredential($User,
$Password)
```

将配置导出到 backup.ctxzip，这是一个加密的 zip 文件。

```
Export-STFConfiguration -targetFolder "$env:userprofile\desktop\"
-zipFileName "backup" -Credential $CredObject
```

在导入服务器上的 PowerShell 会话中创建相同的 PowerShell 凭据对象。

```
Import-STFConfiguration -configurationZip
"$env:userprofile\desktop\backup.ctxzip" -Credential $CredObject
-HostBaseURL "https://storefront.example.com"
```

取消保护现有加密备份存档

```
$User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name

$Password = "Pa55w0rd"

$Password = $Password | ConvertTo-SecureString -asPlainText -Force

$CredObject = New-Object System.Management.Automation.PSCredential($User,
$Password)



Unprotect-STFConfigurationExport -encryptedConfigurationZip
"$env:userprofile\desktop\backup.ctxzip" -credential $CredObject
-outputFolder "c:\StoreFrontBackups" -Force
```

部署的默认网站

当用户在其 Web 浏览器中打开基本 URL 时，您可以将 StoreFront 配置为将用户重定向到特定网站。

1. 打开 StoreFront 管理控制台。

2. 在“**操作**”窗格中，选择“**设置部署的默认网站**”。
3. 如果要设置默认网站，请执行以下操作：
    a. 选择“**设置服务器的默认网站**”
    b. 选择一个“**应用商店**”
    c. 选择一个“**网站路径**”。
4. 选择“**确定**”以保存更改。

设置默认网站窗口的屏幕截图(/en-us/storefront/2507-ltsr/media/manage-deployment/default-website.png)

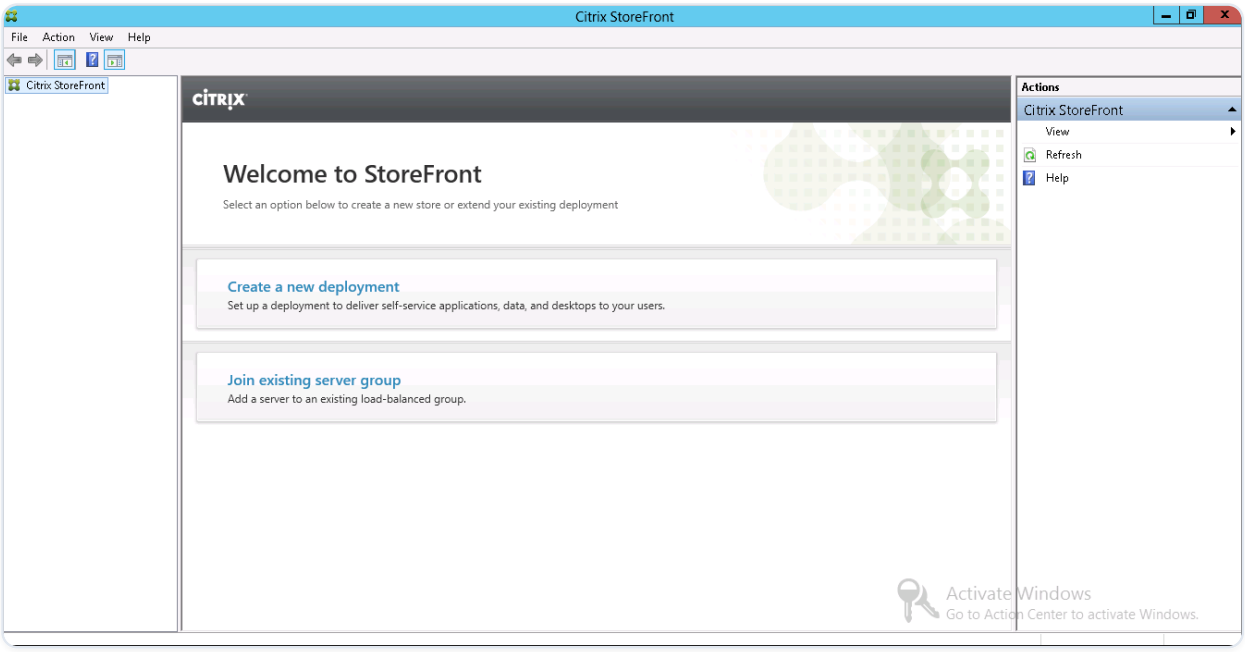
将服务器重置为出厂默认设置

在某些情况下，需要将 StoreFront 安装重置为其初始安装状态。例如，在将 StoreFront 服务器重新添加到服务器组之前，这是必需的。可以执行手动卸载和重新安装，但这更耗时，并可能导致其他不可预见的问题。相反，您可以使用 PowerShell 模块 将配置重置为默认值。

1. 确保 StoreFront 管理控制台已关闭。
2. 打开 PowerShell 控制台。
3. 运行命令 Clear-STFDeployment。

```
Clear-STFDeployment -Confirm $False
```

4. 命令成功完成后，打开 StoreFront 管理控制台并确认所有设置均已重置。**创建新部署**或**加入现有服务器组**的选项可用。



卸载 StoreFront

除了产品本身，卸载 StoreFront 还会删除身份验证服务、应用商店、网站、XenApp Services URL 及其相关配置。包含用户应用程序订阅数据的订阅应用商店服务也会被删除。因此，在单服务器部署中，用户应用程序订阅的详细信息将丢失。但是，在多服务器部署中，这些数据会保留在组中的其他服务器上。StoreFront 安装程序启用的先决条件（例如 .NET Framework 功能和 Web 服务器 (IIS) 角色服务）在卸载 StoreFront 时不会从服务器中删除。

1. 使用具有本地管理员权限的帐户登录到 StoreFront 服务器。
2. 如果 StoreFront 管理控制台已打开，请将其关闭。
3. 关闭所有可能已用于管理 StoreFront 的 PowerShell 会话。
4. 打开“**开始**”菜单，按“**设置**”（齿轮图标），然后转到“**应用**”。
5. 在“**程序和功能**”窗口中，选择 **Citrix StoreFront**，然后单击“**卸载**”以从服务器中删除所有 StoreFront 组件。
6. 在“**卸载 Citrix StoreFront**”对话框中，单击“**是**”。卸载完成后，单击“**确定**”。

手动删除 StoreFront

卸载 StoreFront 后，为确保 StoreFront 已完全删除：

1. 删除“**Web 服务器 (IIS)**”角色。有关详细信息，请参阅 Microsoft Learn。
2. 删除文件夹 `C:\Program Files\Citrix\Receiver StoreFront`。
3. 删除 `C:\Program Files\Citrix\StoreFront Install` 下的任何子目录。

4. 删除文件夹 `C:\Inetpub`。

您现在可以 重新安装 StoreFront。

安装日志

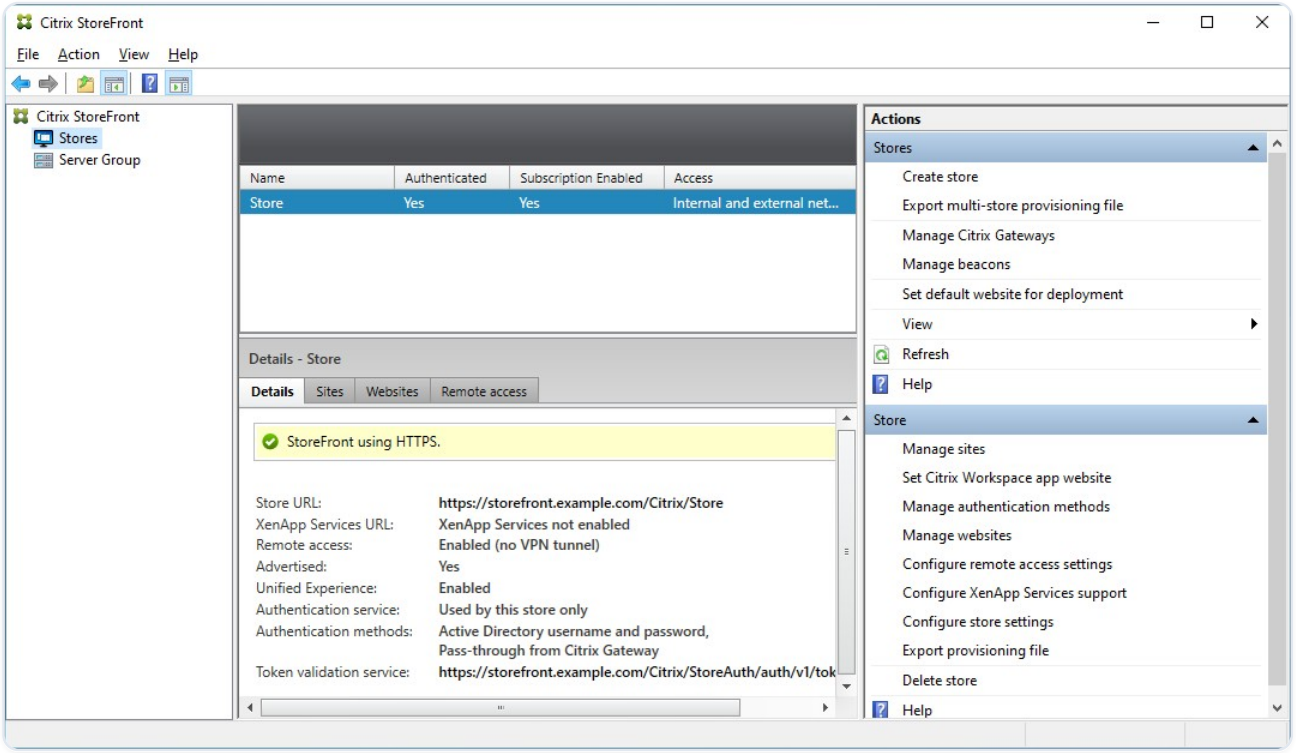
有关日志文件的更多详细信息，请参阅安装日志。

管理应用商店

在 Citrix StoreFront 中，您可以创建一个或多个应用商店，以允许最终用户访问其资源。每个应用商店都定义了用户如何进行身份验证、聚合哪些资源以及外观。最终用户可以通过 Web 浏览器打开这些应用商店，或者将其添加到本地安装的 Citrix Workspace 应用程序中。

查看应用商店

1. 在 (/zh-cn/storefront/2507-ltsr/manage-deployment/management-console.html) 中，选择左侧窗格中的“**应用商店**”节点。
2. 选择要查看的应用商店。



在“**详细信息**”窗格中，您可以查看以下选项卡：

选项卡	详细信息
详细信息	提供应用商店详细信息，例如 URL 和身份验证方法
站点	列出为该应用商店配置的所有站点

选项卡	详细信息
网站	列出为该应用商店配置的所有 (/zh-cn/storefront/2507-ltsr/stores/websites.html)。
远程访问	有关是否使用 Citrix Gateway 启用远程访问的详细信息

创建应用商店

在**操作**窗格的**应用商店**部分，按**创建应用商店**。有关详细信息，请参阅创建应用商店。

配置应用商店

在“操作”窗格的**应用商店**部分，您可以执行以下应用商店配置操作：

操作	详细信息
管理站点	添加和删除站点。
设置 Citrix Workspace 应用程序网站	配置使用 Citrix Workspace 应用程序访问应用商店时使用的网站
管理身份验证方法	选择用户可用于向应用商店进行身份验证的方法
管理网站	管理用于访问应用商店的网站
配置远程访问设置	为从公共网络连接的用户配置通过 Citrix Gateway 访问应用商店。
配置 XenApp® 服务支持	启用或禁用 XenApp 服务 URL
配置应用商店设置	打开“配置应用商店设置”窗口，您可以在其中配置收藏夹、Kerberos 委派、最佳 HDX 路由、发布应用商店和高级设置

您可以在管理控制台之外执行以下高级应用商店配置：

任务	详细信息
默认 ICA 设置	通过将 HDX 设置添加到 default.ica 来配置它们

任务	详细信息
Citrix Workspace 应用程序配置	使用 StoreFront 配置 Citrix Workspace 应用程序
配置联合身份验证服务	配置联合身份验证服务 (FAS) 以实现对 VDA 的单点登录

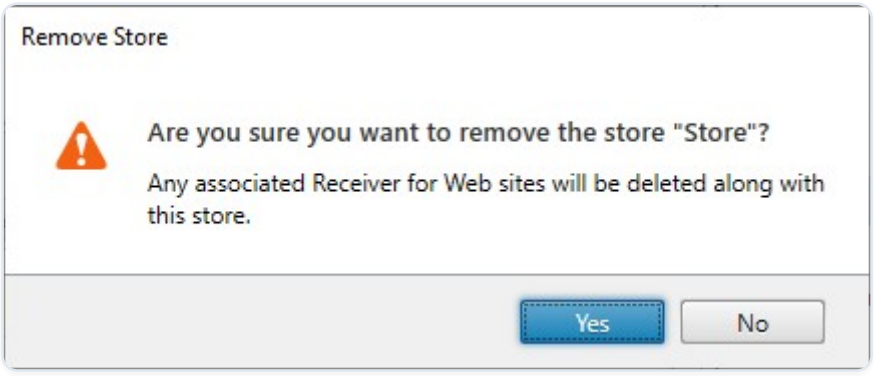
导出预配文件

您可以生成包含一个或多个应用商店的连接详细信息的文件，包括为该应用商店配置的任何 Citrix Gateway 部署和信标。有关详细信息，请参阅导出预配文件。

删除应用商店

要删除应用商店：

1. 在 Citrix StoreFront 管理控制台的左窗格中选择“**应用商店**”节点
2. 在“**操作**”窗格中，单击“**删除应用商店**”
3. 在确认窗口中，点击 **是**。



当您删除商店时，任何关联的网站也会被删除。

创建应用商店

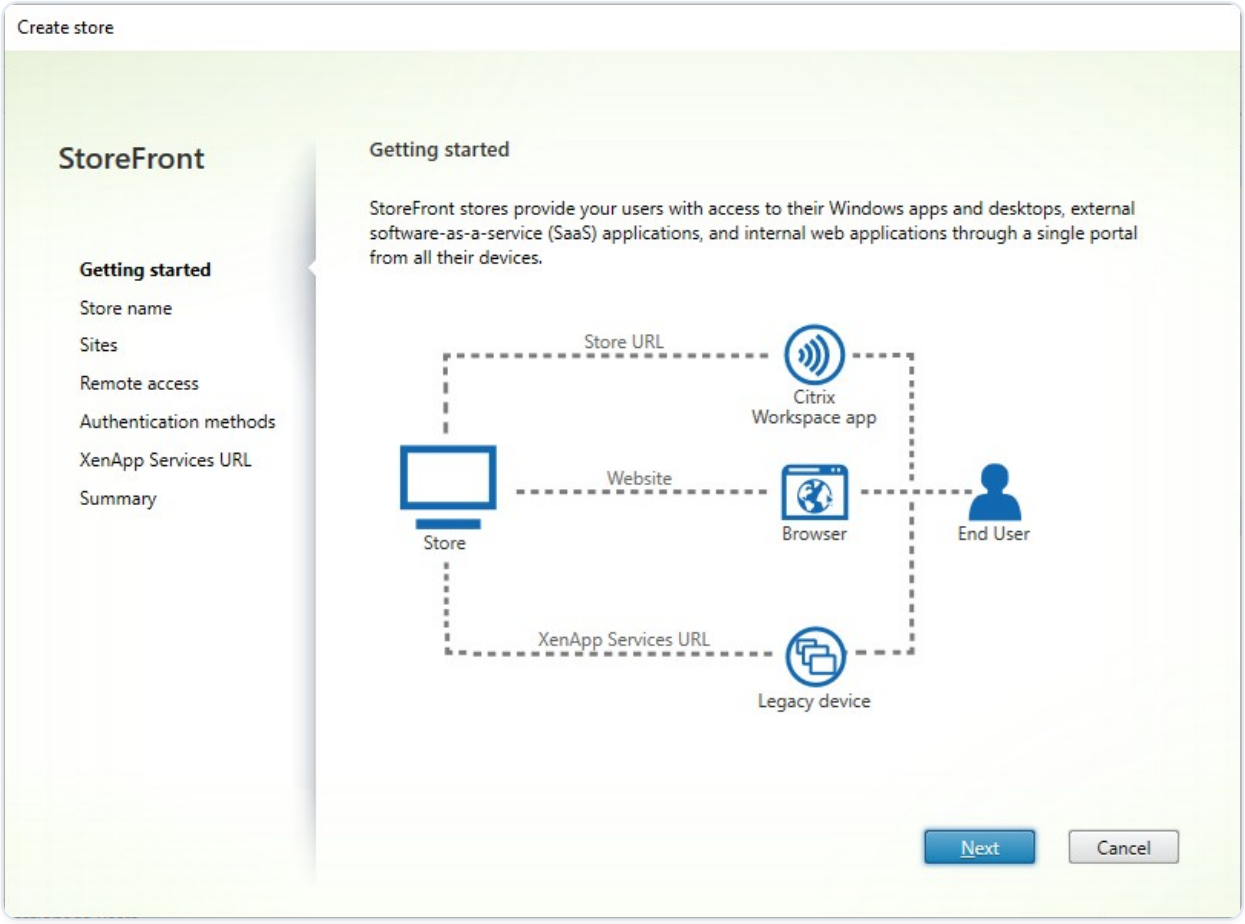
您可以根据需要创建任意数量的应用商店；例如，您可以为特定用户组创建应用商店，或将特定资源集组合在一起。

> 重要提示：

> 在多服务器部署中，一次只能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，将配置更改传播到服务器组，以便更新部署中的其他服务器。

> 要创建应用商店，您需要识别并配置与提供您希望在应用商店中提供的资源的服务器的通信。然后，您可以选择通过 Citrix Gateway 配置对应用商店的远程访问。

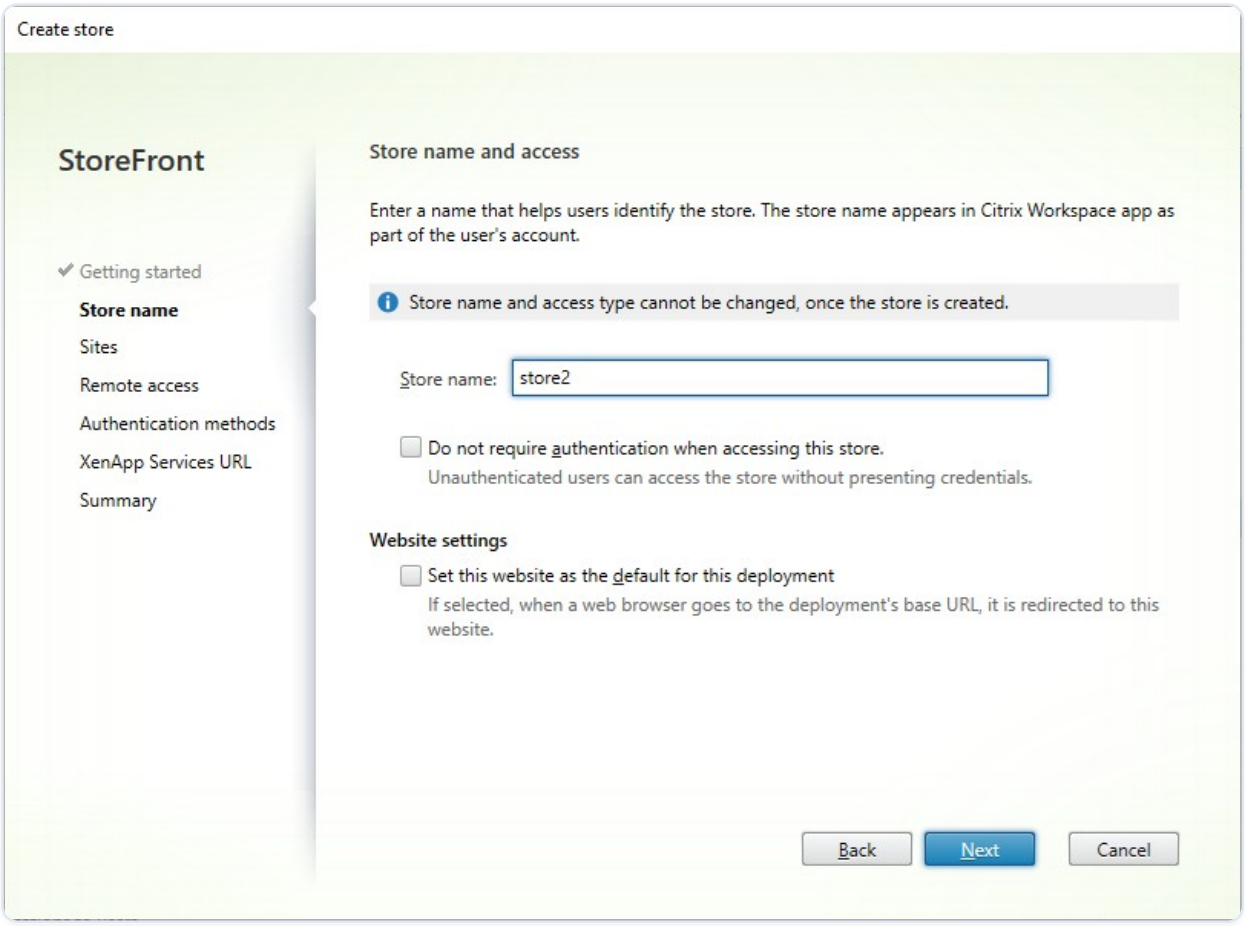
1. 在操作窗格中，单击“**创建应用商店**”。



单击“**下一步**”

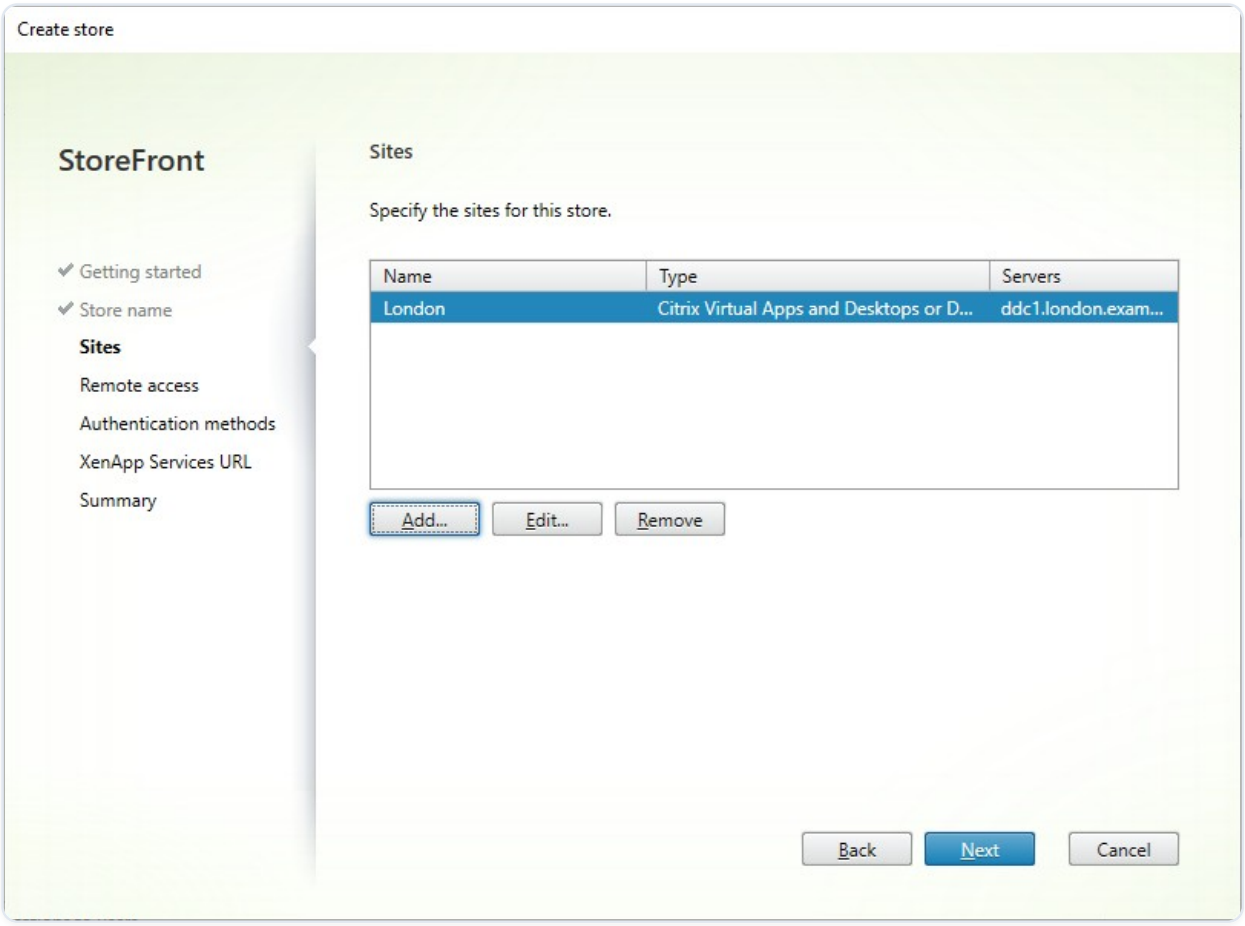
2. 在“**应用商店名称**”选项卡上填写以下内容：

   - 输入应用商店名称
   - 如果您希望允许用户匿名或未经身份验证地访问应用商店，请勾选“**仅允许未经身份验证的用户访问此应用商店**”。当您创建未经身份验证的应用商店时，“**身份验证方法**”和“**远程访问**”页面将不可用，并且左侧和操作窗格中的“**服务器组节点**”将替换为“**更改基本 URL**”。（这是唯一可用的选项，因为服务器组在未加入域的服务器中不可用。）



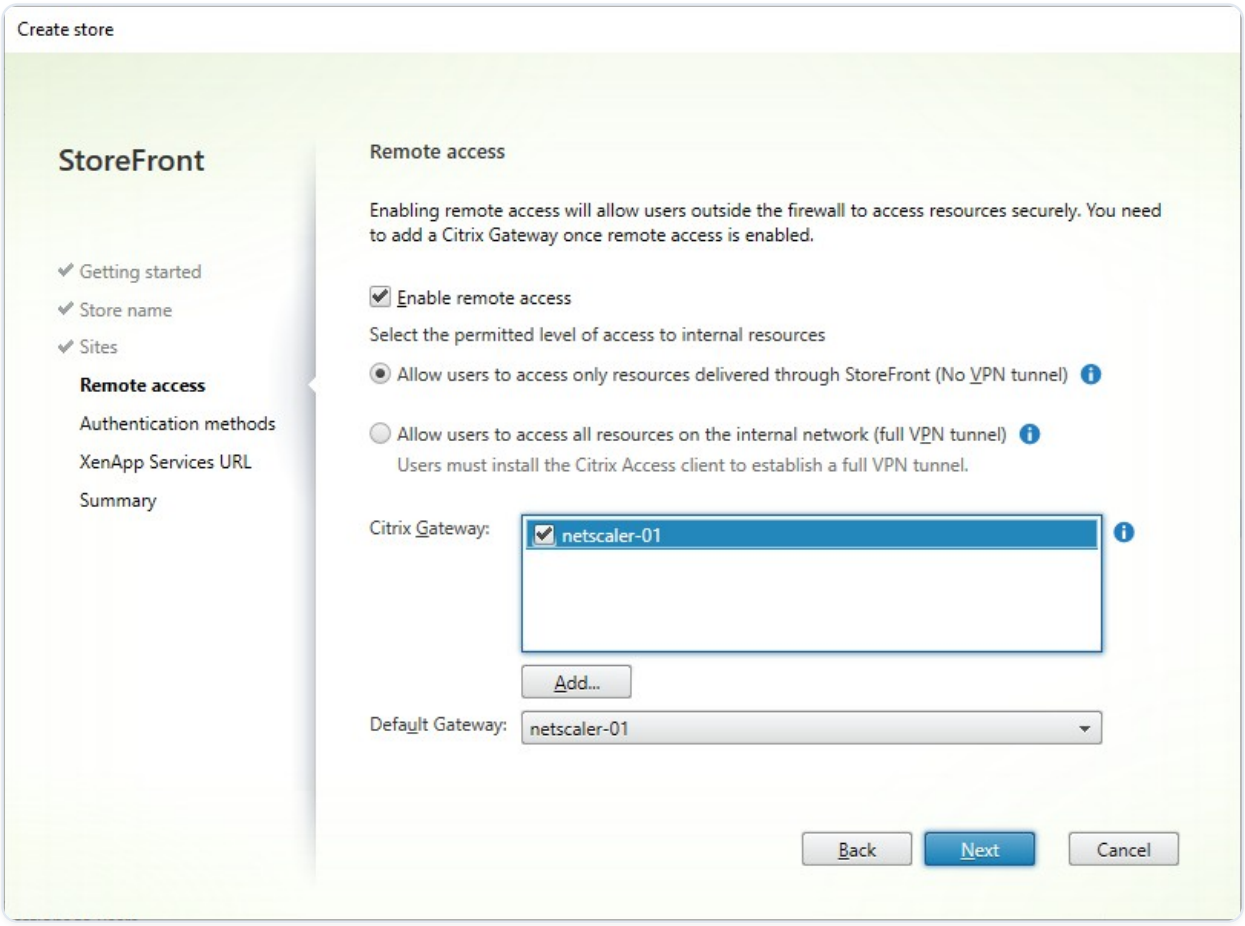
单击“**下一步**”

3. 在“**站点**”选项卡上，为您的虚拟桌面和应用程序添加站点。有关更多详细信息，请参阅管理站点



单击**下一步**。

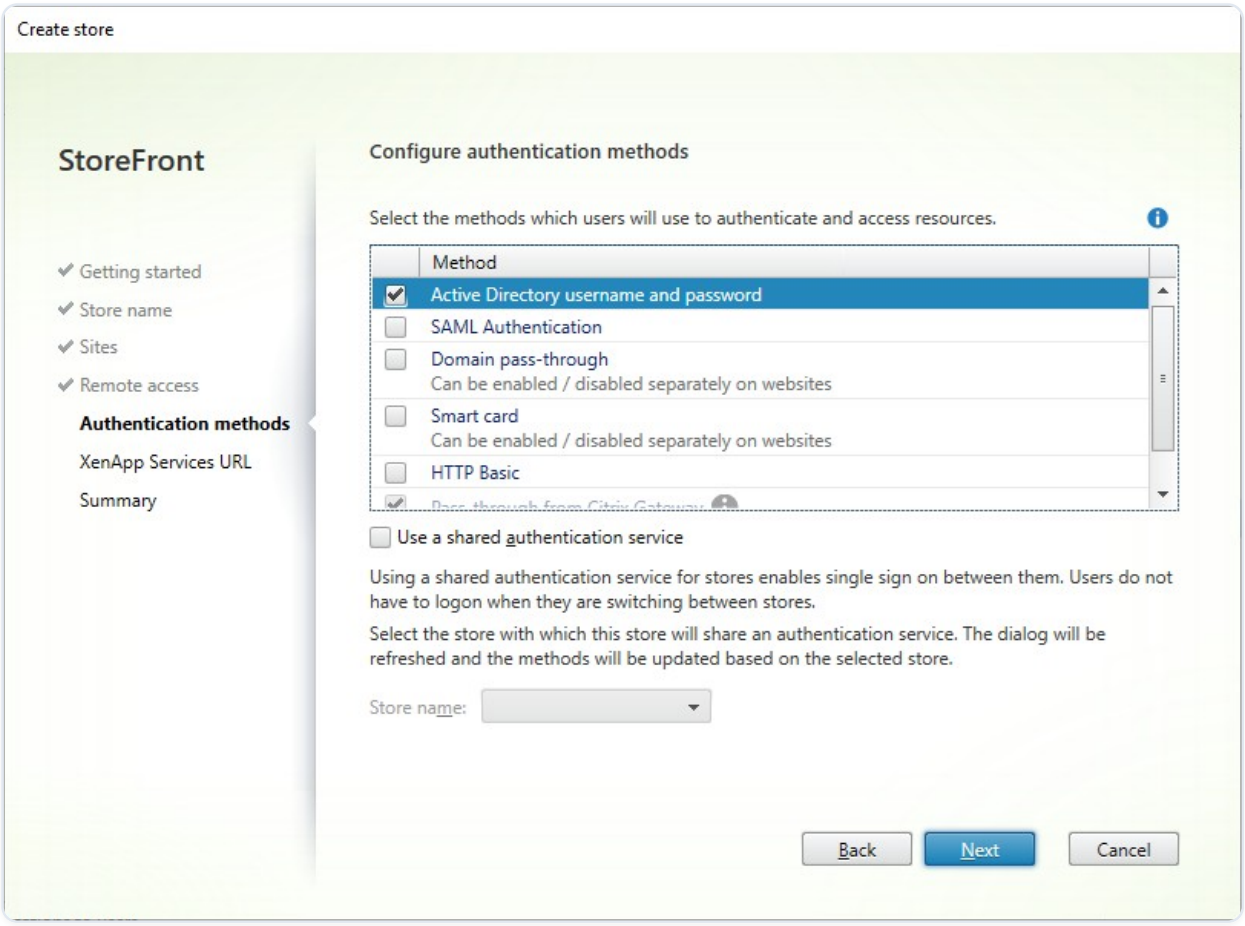
4. 在“**远程访问**”选项卡上，选择是否要通过 Citrix Gateway 使应用商店可用。有关详细信息，请参阅通过 Citrix Gateway 管理对应用商店的远程访问。



5. 在“**身份验证方法**”选项卡上，选择用户将用于向应用商店进行身份验证的方法，然后单击“**下一步**”。

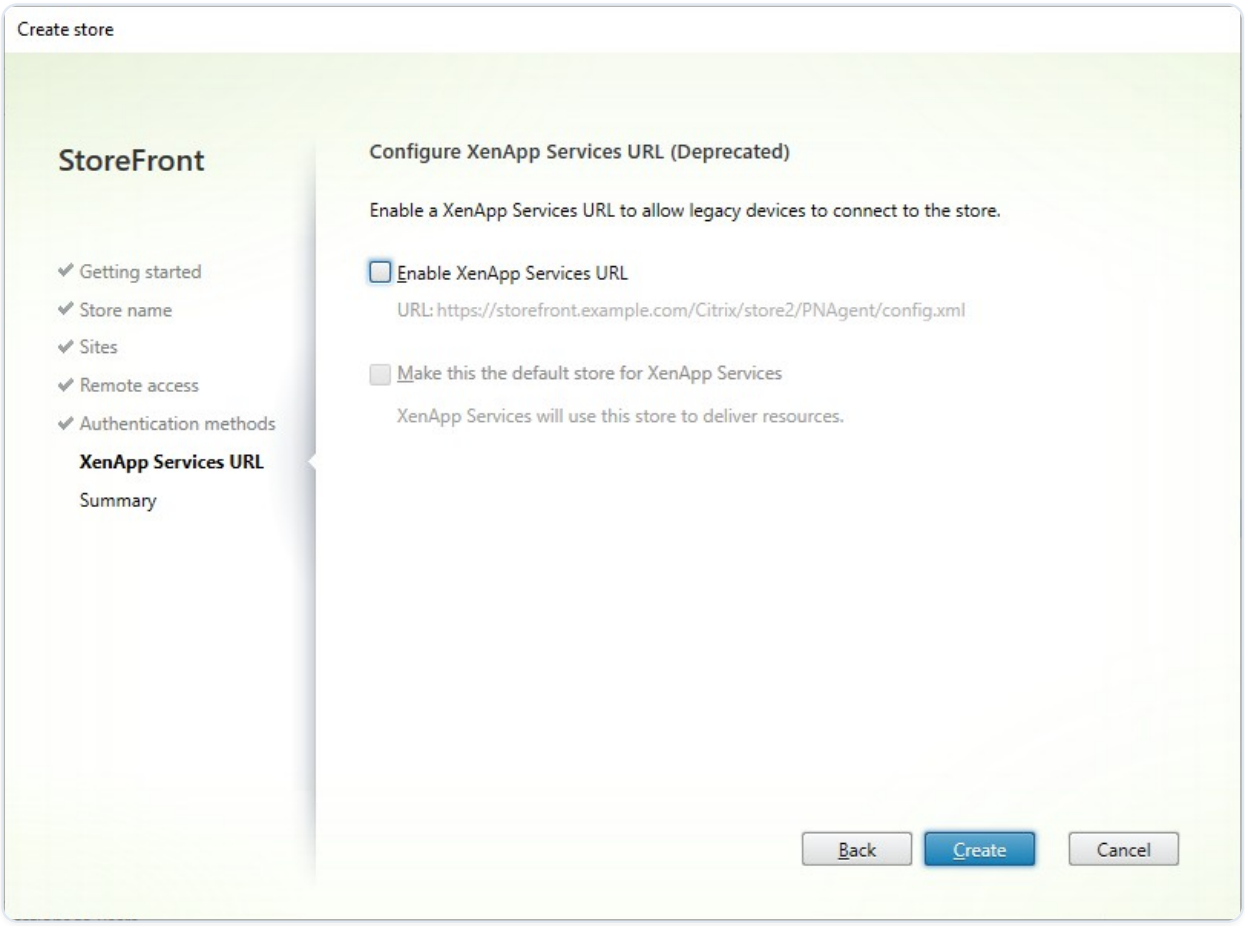
   有关可用身份验证方法的更多详细信息，请参阅配置身份验证。

   除了为此应用商店单独配置身份验证方法外，还可以与其他应用商店共享身份验证配置。为此，请勾选“**使用共享身份验证服务**”，然后选择一个现有应用商店。



单击“**下一步**”

6. 在“**XenApp® Services URL**”选项卡上，如果您有需要 PNAgent 的旧设备，请选择“**启用 XenApp Services URL**”，否则请清除此选项。



单击“**创建**”

> **注意：**
>
> XenApp 服务已弃用，并将在未来版本中移除。

7. 应用商店创建完成后，单击“**完成**”。

创建新应用商店时，还会创建一个新网站以允许用户访问该应用商店。您可以配置此网站或创建其他网站。

PowerShell

要使用 PowerShell 创建应用商店：

1. 使用 Add-STFAuthenticationService 创建身份验证服务。按照惯例，虚拟路径通常为 `/Citrix/[StoreName]Auth`。或者，您可以使用 Get-STFAuthenticationService 获取现有身份验证服务。匿名应用商店不需要此步骤。
2. 根据需要配置身份验证服务。请参阅配置身份验证。
3. 调用 Add-STFStoreService。

- 为应用商店选择一个虚拟路径，并将其设置为 `-VirtualPath` 参数。通常为 /Citrix/。
- 将 `-AuthenticationService` 设置为在步骤 1 中创建的身份验证服务。或者，对于匿名应用商店，请设置 `-Anonymous $True`
- 您可以包含一个站点的详细信息。其他站点必须单独配置。

管理站点

使用**管理站点**屏幕添加、修改和删除由 Citrix Virtual Apps and Desktops、Citrix Desktops as a Service 和 Citrix Secure Private Access 提供的站点。

查看站点

1. 在 Citrix StoreFront 管理控制台中，在左侧窗格中选择**应用商店**节点。
2. 在结果窗格中选择一个应用商店
3. 在**操作**窗格中，单击**管理站点**。

使用 PowerShell 查看站点

要使用 PowerShell 查看站点，请运行 cmdlet Get-STFStoreFarm。

添加站点

添加 Citrix 虚拟应用和桌面™ 站点

1. 在**管理站点**屏幕中，单击**添加**。
2. 输入一个**显示名称**，以帮助您识别该源。
3. 将**类型**选择为**Citrix Virtual Apps and Desktops 或 DaaS**。
4. 在每个 DDC 的**服务器**下，单击**添加**并输入 DDC（或相应的负载平衡器）的地址。
   - 如果您在 DDC 前面放置了负载平衡器，则输入负载平衡器的地址。如果您不使用负载平衡器，则单独列出每个 DDC。
   - 至少包含 2 个 DDC 以实现冗余。
   - 如果您的服务器使用 HTTPS（推荐），请确保您在服务器列表中指定的名称与这些服务器证书上的名称完全匹配（包括大小写）。
5. 可选地选择 **服务器已负载平衡**。如果选中，StoreFront 会随机选择一个服务器。如果未选中，StoreFront 将使用列表中的第一个服务器，除非该服务器不可用，在这种情况下，它会向下遍历列表，直到找到一个响应的服务器。您可以使用向上和向下箭头来定义优先级顺序。

- 如果所有 DDC 都具有相似的延迟，则建议您选择 **服务器已负载平衡**，以便 StoreFront 将负载分布到所有 DDC。
- 如果您有一个多区域地理分散部署，其中 DDC 具有不同的延迟，您可能希望将延迟最低的 DDC 放在列表顶部并取消选择 **服务器已负载平衡**，以便 StoreFront 优先选择延迟较低的服务器。考虑使用单独的负载平衡器来分配同一位置中不同 DDC 之间的负载。

6. 从 **传输类型** 列表中，选择 StoreFront 用于与服务器通信的连接类型。

   - 要通过未加密的连接发送数据（不推荐），请选择 **HTTP**。如果选择此选项，您必须自行安排 StoreFront 与服务器之间的连接安全。
   - 要通过加密的 TLS 连接发送数据（推荐），请选择 **HTTPS**。您必须在交付控制器上启用 TLS 或在 DDC 前面的负载平衡器上启用 TLS。

     支持以下 TLS 1.3 密码套件：

     - TLS_AES_256_GCM_SHA384
     - TLS_AES_128_GCM_SHA256

     支持以下 TLS 1.2 密码套件：

     - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
     - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
     - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
     - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

7. 指定 StoreFront 用于连接服务器的端口。HTTP 连接的默认端口是 80，HTTPS 连接的默认端口是 443。指定的端口必须是 Citrix XML Service 使用的端口。
8. 按下 **确定**

   添加站点窗口的屏幕截图(/en-us/storefront/2507-ltsr/media/stores/add-delivery-controller-cvad.png)

9. 如果您已配置 安全密钥（推荐），则必须使用 PowerShell 添加密钥。例如：

```
$store = Get-STFStoreService -VirtualPath [path to store]

$farm = Get-STFStoreFarm -StoreService $store -FarmName [site name]
```

```
Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true
-XMLValidationSecret [Security key]
```

使用 PowerShell 添加 Citrix Virtual Apps and Desktops™ 站点

要添加站点（也称为场），请运行 cmdlet Add-STFStoreFarm 并使用 `FarmType` `XenDesktop`

例如，要添加一个名为“CVAD”且带有安全密钥的站点：

```
$store = Get-STFStoreService -VirtualPath [path to store]

Add-STFStoreFarm -StoreService $store -FarmName "CVAD" -FarmType
XenDesktop -Port 443 -TransportType HTTPS -Servers
@("ddc1.example.com","ddc2.example.com") -XMLValidationEnabled $true
-XMLValidationSecret "MySecret"
```

添加 Citrix 桌面即服务站点

1. 在 **管理站点** 屏幕中，单击 **添加**。
2. 输入一个 **显示名称**，以帮助您识别此源。
3. 将 **类型** 选择为 **Citrix Virtual Apps and Desktops 或 DaaS**。
4. 在每个 Cloud Connector 的 **服务器** 下，单击 **添加** 并输入 Cloud Connector（或相应的负载均衡器）的名称。

   - 如果您在 Cloud Connector 或 DDC 前面放置了负载均衡器，则输入负载均衡器的名称。如果您未使用负载均衡器，则单独列出每个 DDC 或 Cloud Connector。
   - 如果您有多个资源位置，Citrix 建议您添加包含 VDA 的所有资源位置中的 Cloud Connector，以便在发生中断时 StoreFront 可以使用本地主机缓存 (Local Host Cache) 在适当的位置启动 VDA。
   - 如果您正在使用负载均衡器，那么为每个资源位置使用单独的负载均衡器非常重要。如果一个负载均衡器位于多个资源位置的服务器前面，这在正常操作中无关紧要。然而，在本地主机缓存 (Local Host Cache) 模式下，它将阻止 StoreFront 将启动请求直接发送到正确的资源位置，从而导致启动失败。
   - 如果您的服务器使用 HTTPS（推荐），请确保您在服务器列表中指定的名称与这些服务器证书上的名称完全匹配（包括大小写）。

5. 可选地选择“**服务器已负载均衡**”。如果选中，StoreFront 会随机选择一个服务器。如果未选中，StoreFront 将使用列表中的第一个服务器，除非该服务器不可用，在这种情况下，它会向下遍历列表，直到找到一个响应的服务器。您可以使用向上和向下箭头来定义优先级顺序。

   - 如果所有服务器的延迟相似，建议您选择“**服务器已负载均衡**”，以便 StoreFront 将负载分配到所有 DDC。
   - 如果您有一个多区域地理分散部署，其中 DDC 具有不同的延迟，您可能希望将延迟最低的服务器放在列表顶部并清除“**服务器已负载均衡**”，以便 StoreFront 优先选择延迟较低的服务器。考虑使用单独的负载均衡器来分配同一资源位置或区域中不同服务器之间的负载。

6. 从“**传输类型**”列表中，选择 StoreFront 用于与服务器通信的连接类型。

   - 要通过未加密连接发送数据（不推荐），请选择“**HTTP**”。如果选择此选项，您必须自行安排以保护 StoreFront 与您的 Cloud Connector 之间的连接。
   - 要通过加密连接发送数据（推荐），请选择“**HTTPS**”。您必须为 HTTPS 配置 Cloud Connector。

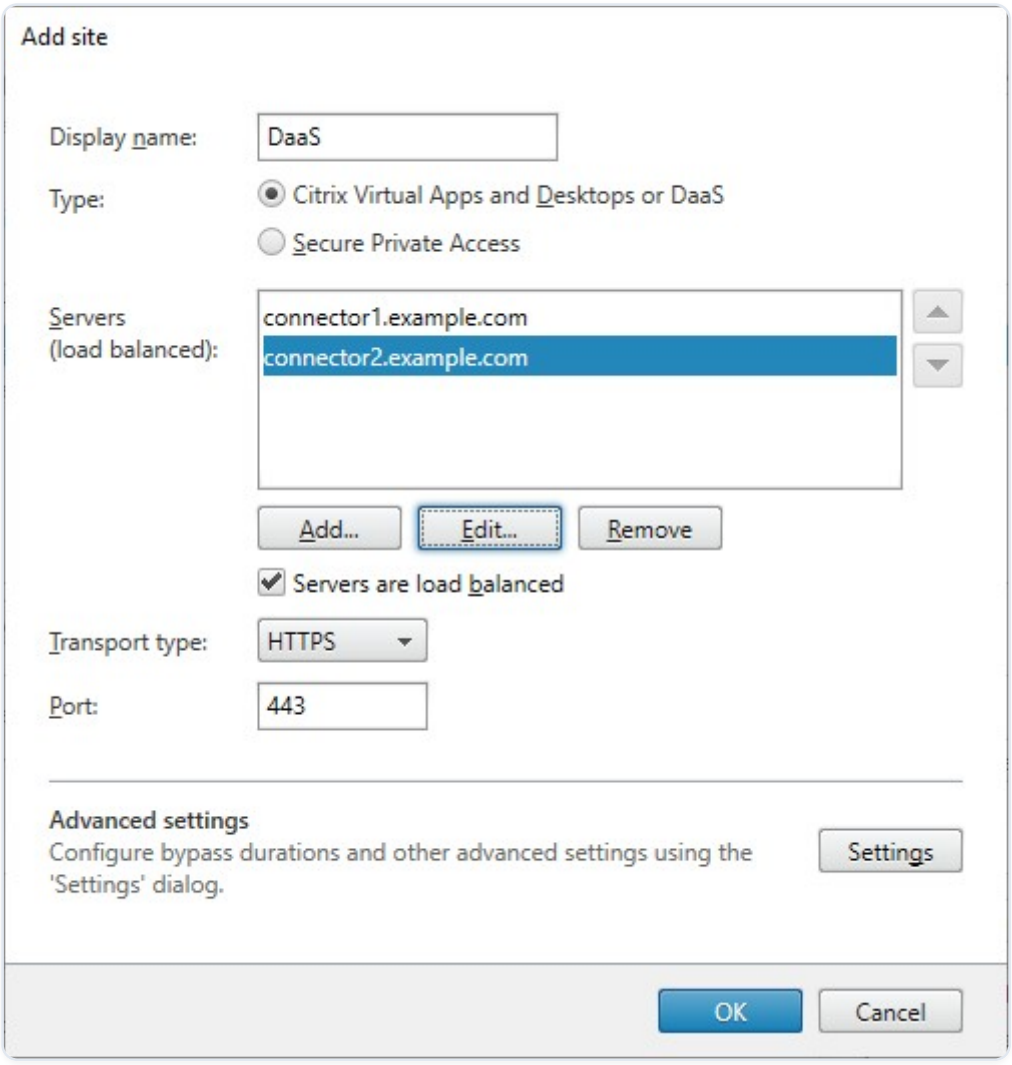
     支持以下 TLS 1.3 密码套件：

     - TLS_AES_256_GCM_SHA384
     - TLS_AES_128_GCM_SHA256

     支持以下 TLS 1.2 密码套件：

     - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
     - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
     - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
     - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

7. 指定 StoreFront 用于连接服务器的端口。HTTP 连接的默认端口是 80，HTTPS 连接的默认端口是 443。
8. 按“**确定**”。



9. 如果您已配置安全密钥（推荐），则必须使用 PowerShell 添加密钥。例如：

```
$store = Get-STFStoreService -VirtualPath [Path to store]

$farm = Get-STFStoreFarm -StoreService $store -FarmName [Site name]

Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true
-XMLValidationSecret [Security key]
```

使用 PowerShell 添加 Citrix Desktops as a Service 站点

要添加站点（也称为场），请运行 cmdlet Add-STFStoreFarm 并使用 `FarmType` `XenDesktop`。

例如，要添加一个名为“DaaS”且带安全密钥的站点：

```
$store = Get-STFStoreService -VirtualPath [path to store]

Add-STFStoreFarm -StoreService $store -FarmName "DaaS" -FarmType
XenDesktop -Port 443 -TransportType HTTPS -Servers
```

```
@("connector1.example.com","connector2.example.com") -XMLValidationEnabled
$true -XMLValidationSecret "MySecret"
```

添加 Citrix 安全私有访问 站点

如果您的 StoreFront 服务器配置为 Citrix Secure Private Access，则可以添加 Citrix Secure Private Access 站点。

1. 在 StoreFront 上导航到 **Stores** > **Manage sites**。
2. 选择“**添加**”。
3. 在“**添加站点**”窗口中，提供一个“**显示名称**”以标识源。
4. 将“**类型**”选择为“**Citrix Secure Private Access**”。
5. 输入 Citrix Secure Private Access 服务器名称。
6. 从“**传输类型**”下拉列表中，选择可用于与服务器通信的连接类型。
   - **HTTP**：通过未加密的连接发送数据（不推荐）。
   - **HTTPS**：通过使用传输层安全性 (TLS) 的安全 HTTPS 连接发送数据（推荐）。
7. 指定用于连接服务器的端口。**HTTP** 的默认端口是 80，**HTTPS** 的默认端口是 443。
8. 选择“**确定**”。
9. 如果您已配置安全密钥（推荐），则必须使用 PowerShell 添加该密钥。例如：

```
$store = Get-STFStoreService -VirtualPath [Path to store]

$farm = Get-STFStoreFarm -StoreService $store -FarmName [Site name]

Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true
-XMLValidationSecret [Security key]
```

使用 PowerShell 添加 Citrix Secure Private Access 站点

要添加站点（也称为场），请运行 cmdlet Add-STFStoreFarm，并使用 `FarmType` `SPA`

例如，要添加一个名为“SPA Apps”且带有安全密钥的站点：

```
$store = Get-STFStoreService -VirtualPath [path to store]

$farm = Add-STFStoreFarm -StoreService $store -FarmName "SPA Apps"
-FarmType SPA -Port 443 -TransportType HTTPS -ServiceUrls https://spa-
```

```
service.example.com -XMLValidationEnabled $true -XMLValidationSecret
"MySecret"
```

编辑站点

在“**管理站点**”屏幕中，选择一个站点，然后单击“**编辑**”。

警告：

如果您重命名站点，则：

- 该站点将从任何 Optimal HDX 路由 配置中删除。您必须将该站点重新添加到您的 Optimal HDX 路由配置中。
- 该站点的任何用户收藏夹 Favorites 将会消失（除非您正在使用多站点聚合）。这是因为收藏夹记录按名称引用站点。收藏夹记录不会被删除，因此如果您将站点重命名回其原始名称，则收藏夹会重新出现。要解决此问题，如果您使用的是 SQL Server 数据库，则可以更新数据库中的记录。否则，您可以导出收藏夹，更正名称并重新导入。有关详细信息，请参阅 管理订阅数据。

使用 PowerShell 编辑站点

要使用 PowerShell 修改站点，请运行 cmdlet Set-STFStoreFarm

删除站点

在“**管理站点**”屏幕中，选择一个站点，然后单击“**删除**”。

使用 PowerShell 删除站点

要使用 PowerShell 删除站点，请使用命令 Remove-STFStoreFarm

健康检查和服务器旁路行为

为了在提供资源的某些服务器不可用时提高性能，StoreFront 会暂时绕过无响应的服务器。当服务器被绕过时，StoreFront 会忽略该服务器，不使用它来访问资源。这避免了尝试连接不可用服务器时造成的延迟。

使用这些参数指定旁路行为的持续时间：

- **后台健康检查轮询周期** - 指定 StoreFront 检查每个服务器可用性的频率。默认值为 1 分钟。要配置此项，请参阅后台健康检查轮询周期。
- **旁路持续时间** - 启用后台健康检查时，此值应至少设置为轮询周期，但超出此范围则无影响。如果禁用后台健康检查（不建议），则服务器将被旁路，直到持续时间到期。默认值为 60 分钟。
- **所有失败旁路持续时间** - 仅在禁用后台健康检查时使用（不建议）。指定 StoreFront 在特定站点的所有服务器都被旁路时，替代**旁路持续时间**使用的缩短的持续时间（以分钟为单位）。默认值为 0 分钟，表示 StoreFront 不旁路任何服务器。

更改旁路参数

通常无需修改这些设置。

1. 在 Citrix StoreFront 管理控制台中，在左侧窗格中选择**应用商店**节点。
2. 在结果窗格中选择一个应用商店。
3. 在**操作**窗格中，单击**管理站点**。
4. 选择一个控制器，单击**编辑**，然后在**编辑站点**屏幕上单击**设置**。
5. 在“高级设置”下，单击**设置**。
6. 在“配置高级设置”对话框中：
    a. 在**所有失败旁路持续时间**行中，单击第二列并输入一个时间（以分钟为单位），该时间表示在所有服务器无响应后，交付控制器被视为脱机的时间。
    b. 在“**旁路持续时间**”行中，单击第二列并输入一个时间（以分钟为单位），在此时间内，单个服务器在未能响应后被视为脱机。

将用户映射到站点

默认情况下，访问应用商店的用户会看到为该应用商店配置的所有站点中可用的所有资源的聚合。要为不同用户提供不同的资源，可以配置单独的应用商店，甚至单独的 StoreFront 部署。或者，您可以根据用户所属的 Microsoft Active Directory 组来提供对特定部署的访问权限。这使您能够通过单个应用商店为不同的用户组配置不同的体验。

例如，您可以在一个部署上为所有用户分组通用资源，并在另一个部署上为财务部门分组财务应用程序。在这种配置中，不属于“帐户”用户组的用户在访问应用商店时只能看到通用资源。“帐户”用户组的成员将同时看到通用资源和财务应用程序。

或者，您可以为高级用户创建部署，该部署提供与您的其他部署相同的资源，但具有更快、更强大的硬件。这使您能够为业务关键型用户（例如您的执行团队）提供增强的体验。所有用户登录到应

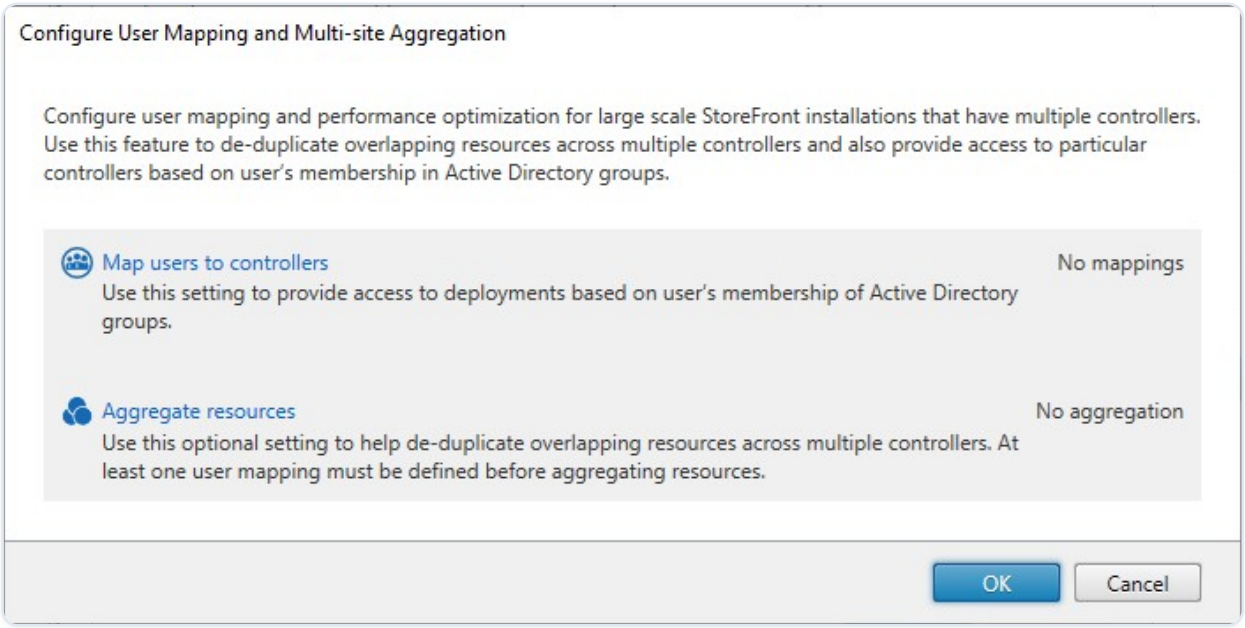
用商店时都会看到相同的桌面和应用程序，但“高管”用户组的成员将优先连接到高级用户部署提供的资源。

> 注意：
>
> 这会筛选整个站点。此外，在站点内，应用程序可以在 Citrix Virtual Apps and Desktops Studio 配置中按用户组进行筛选。

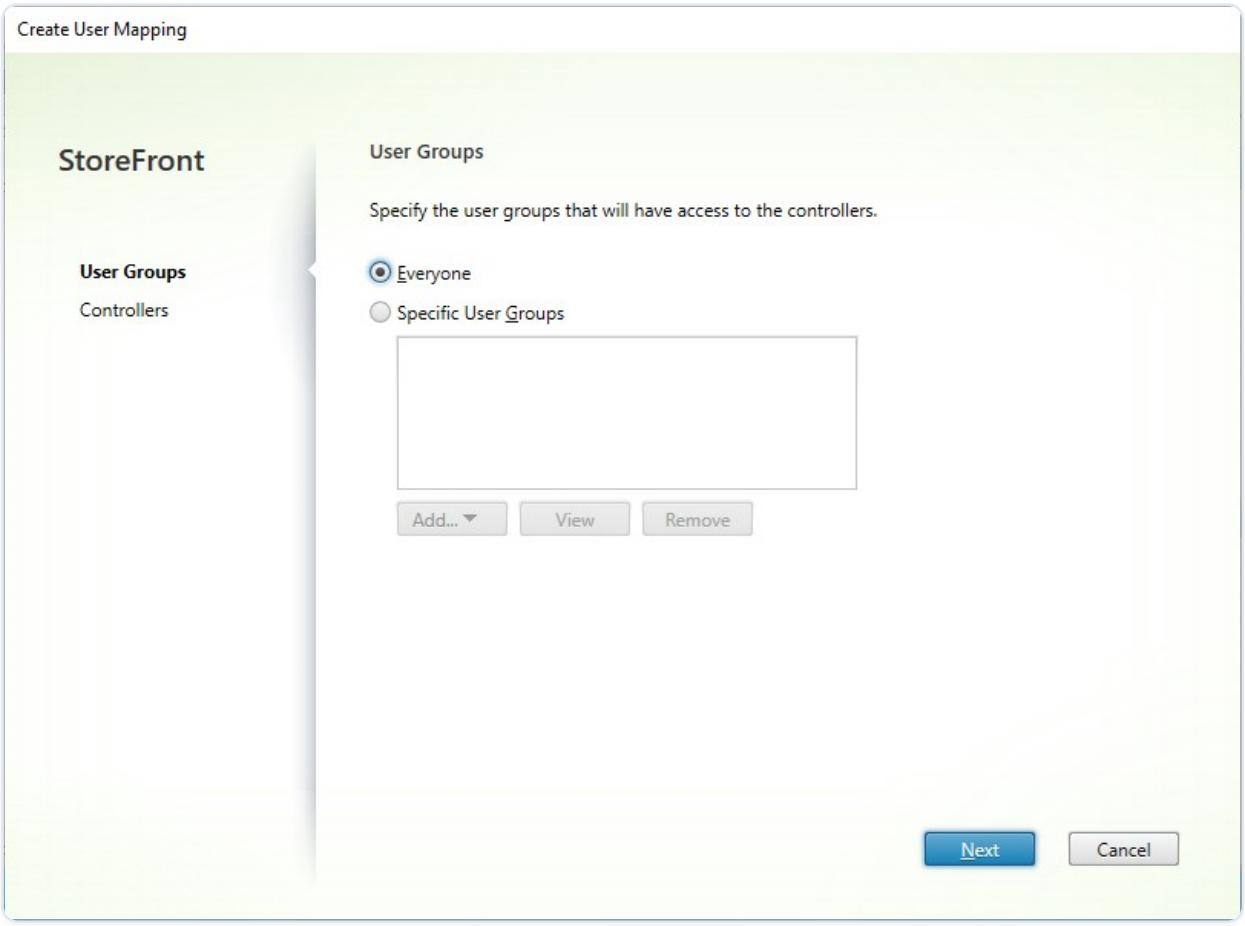
为特定用户组配置特定站点：

1. 在“**管理站点**”屏幕中，在“**用户映射和多站点聚合配置**”下，单击“**配置**”。仅当配置了两个或更多站点时，此选项才可用。

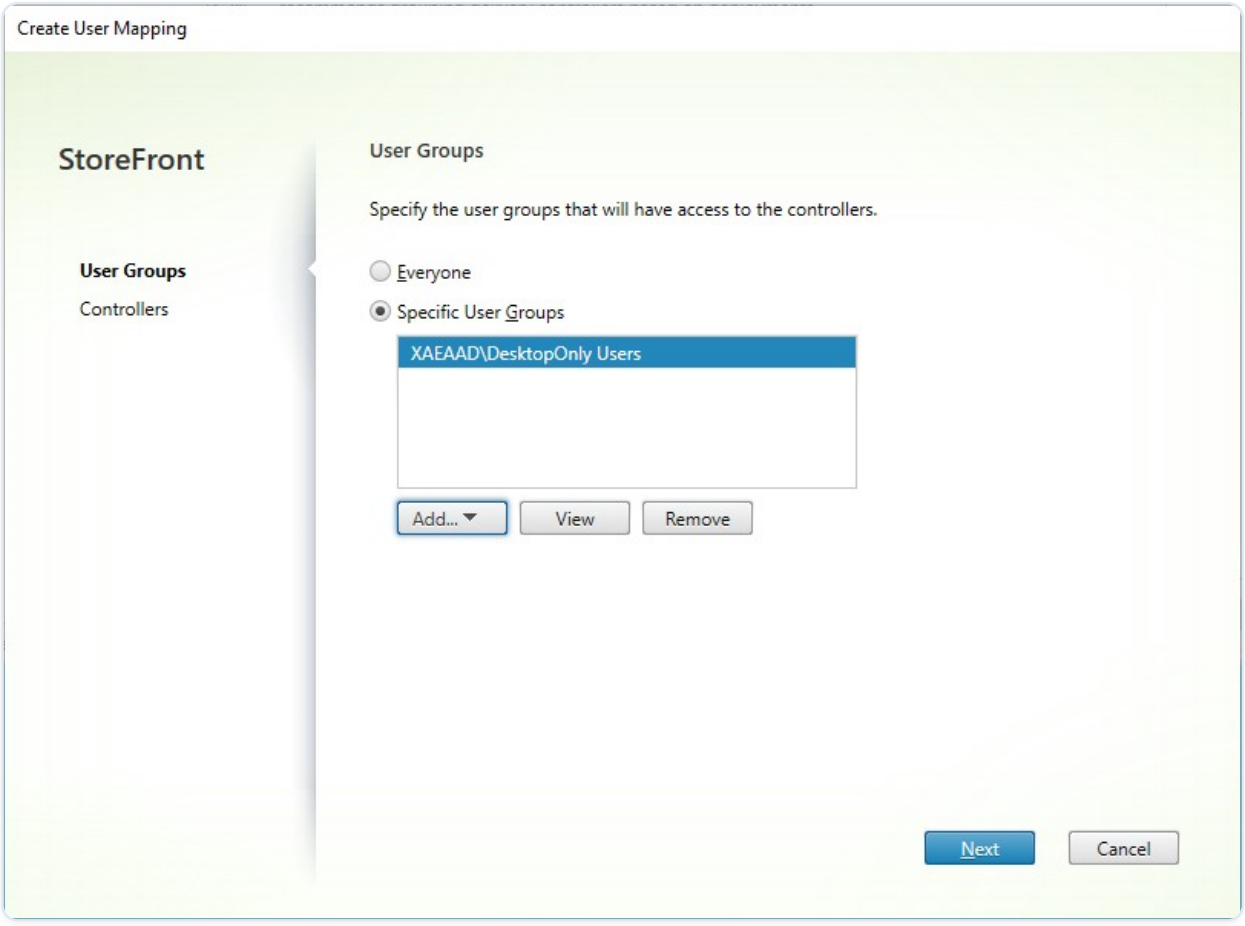
   这将打开“**配置用户映射和多站点聚合**”屏幕。



2. 单击“**将用户映射到站点**”。这将打开“**创建用户映射**”屏幕以创建您的第一个映射。您以后可以创建更多映射。



3. 选择“**所有人**”或选择“**特定用户组**”并添加一个或多个组。



4. 单击“**下一步**”。这将带您进入“**站点**”选项卡。

   创建用户映射屏幕用户组选项卡的屏幕截图(/en-us/storefront/2507-ltsr/media/stores/user-mapping-controllers-empty.png)

5. 单击 **添加** 并添加一个或多个控制器。

   已选择控制器的创建用户映射屏幕用户组选项卡的屏幕截图(/en-us/storefront/2507-ltsr/media/stores/user-mapping-controllers-selected.png)

6. 单击“**创建**”。

   已选择控制器的创建用户映射屏幕用户组选项卡的屏幕截图(/en-us/storefront/2507-ltsr/media/stores/aggregation-map-users-configured.png)

7. 根据需要单击 **添加...** 以创建更多映射。

使用 PowerShell 将用户映射到资源

您可以使用 PowerShell 将用户映射到资源。

1. 对于每个站点（在 SDK 中称为场），创建一个 EquivalentFarmset。所有站点都必须是场集的一部分，否则它们将不适用于任何用户。使用以下参数调用 New-STFEquivalentFarmset：

   - `Name` - EquivalentFarmSet 的唯一名称
   - `PrimaryFarms` - 非聚合站点（场）的名称。

2. 对于需要访问不同站点集的用户集，请在这些用户与每个 EquivalentFarmSet 之间创建映射。要创建 UserFarmMapping，请使用以下参数调用 Add-STFUserFarmMapping：

   - `StoreService` - 要添加 UserFarmMapping 的 Store 服务。
   - `Name` - 映射的唯一名称。
   - `GroupMembers` - 包含作为映射一部分的用户组的名称和 SID 的哈希表。名称仅用于显示；SID 定义组。要添加所有用户，请在哈希表中创建一个条目，其名称为 `Everyone`，值为 `Everyone`。
   - `EquivalentFarmSet` - 在上一步中创建的 EquivalentFarmSet。

   您必须确保每个站点（场）都包含在至少一个 UserFarmMapping 中，否则任何用户都无法访问该资源。

多站点聚合

默认情况下，StoreFront 会枚举为商店提供桌面和应用程序的所有部署，并将所有这些资源视为独立的。这意味着如果同一资源可从多个部署中获得，用户会看到每个资源的图标，如果这些资源具有相同的名称，这可能会令人困惑。当您设置高可用性多站点配置时，您可以将提供相同桌面或应用程序的 Citrix Virtual Apps and Desktops 部署进行分组，以便为用户聚合相同的资源。分组的部署不必完全相同，但资源在每个服务器上必须具有相同的名称和路径才能进行聚合。

通过多站点聚合，当桌面或应用程序可从为特定商店配置的多个 Citrix Virtual Apps and Desktops 部署中获得时，StoreFront 会聚合该资源的所有实例，并向用户呈现单个图标。当用户启动聚合资源时，StoreFront 会根据以下因素确定最适合该用户的资源实例：

- 服务器可用性。
- 用户是否已有活动会话。
- `Primary` 和 `Secondary` 关键字。
- 用户的区域偏好。
- 您在配置中指定的交付源顺序。

StoreFront 会动态监控未能响应请求的服务器，因为这些服务器可能过载或暂时不可用。用户将被定向到其他服务器上的资源实例，直到通信重新建立。在提供资源的服务器支持的情况下，StoreFront 会尝试重用现有会话以交付其他资源。如果用户在提供所请求资源的部署上已有活动会话，StoreFront 会在会话与该资源兼容时重用该会话。最大限度地减少每个用户的会话数量可以缩短启动额外桌面或应用程序所需的时间，并可以更有效地利用产品许可证。

您可以覆盖单个 Citrix Virtual Apps and Desktops 资源的指定部署顺序，以定义用户在访问特定桌面或应用程序时连接的首选部署。例如，这使您可以指定用户优先连接到专门用于交付特定桌面或应用程序的部署，但将其他部署用于其他资源。为此，请将字符串 `KEYWORDS:Primary` 附加到首选部署上的桌面或应用程序的描述中，并将 `KEYWORDS:Secondary` 附加到其他部署上的资源。在可能的情况下，无论您在配置中指定的部署顺序如何，用户都将连接到提供主要资源的部署。当首选部署不可用时，用户将连接到提供辅助资源的部署。

作为 StoreFront 站点配置的一部分，您可以指定这些资源所在的区域。如果用户通过 GSLB 访问 StoreFront，您可以配置 GSLB 以插入区域偏好标头。然后，StoreFront 会尝试启动托管在首选部署上的应用程序，然后再联系其他部署。

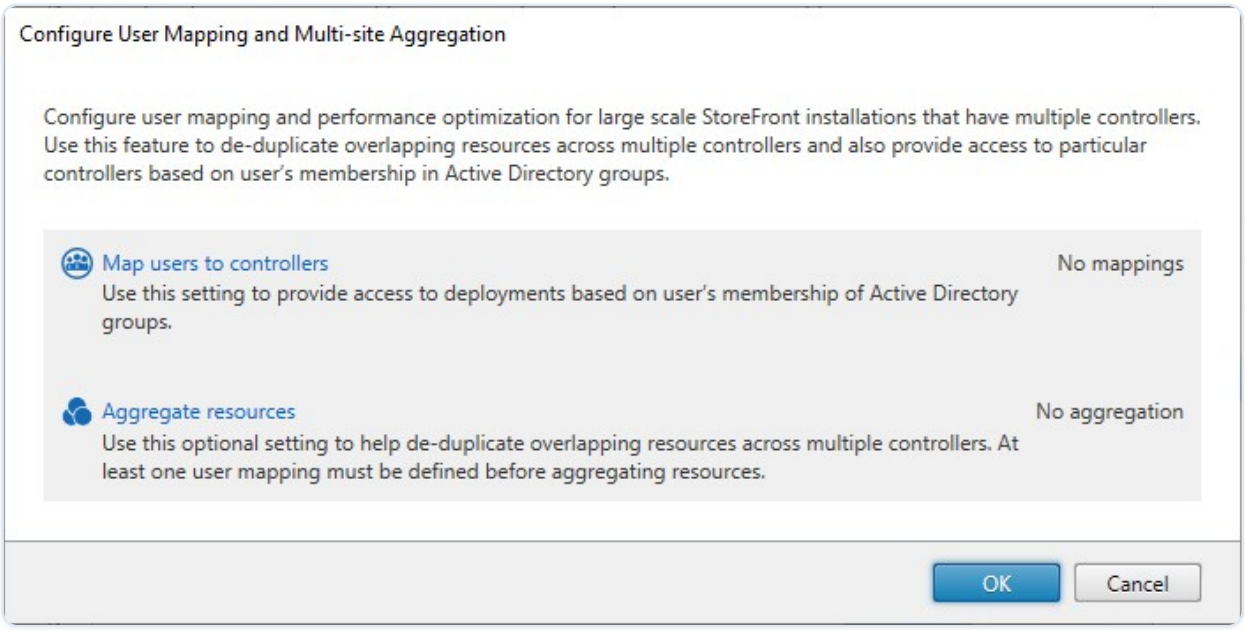
在检查其他因素后，StoreFront 会使用您在配置中指定的顺序来确定用户连接到的部署。如果用户有多个等效部署可用，您可以指定用户连接到第一个可用部署，或者随机连接到列表中的任何部署。将用户连接到第一个可用部署可以最大限度地减少当前用户数量所使用的部署数量。随机连接用户可以在所有可用部署之间提供更均匀的用户分布。

如果从一个站点启动失败，StoreFront 会尝试其他合适的站点，除非：

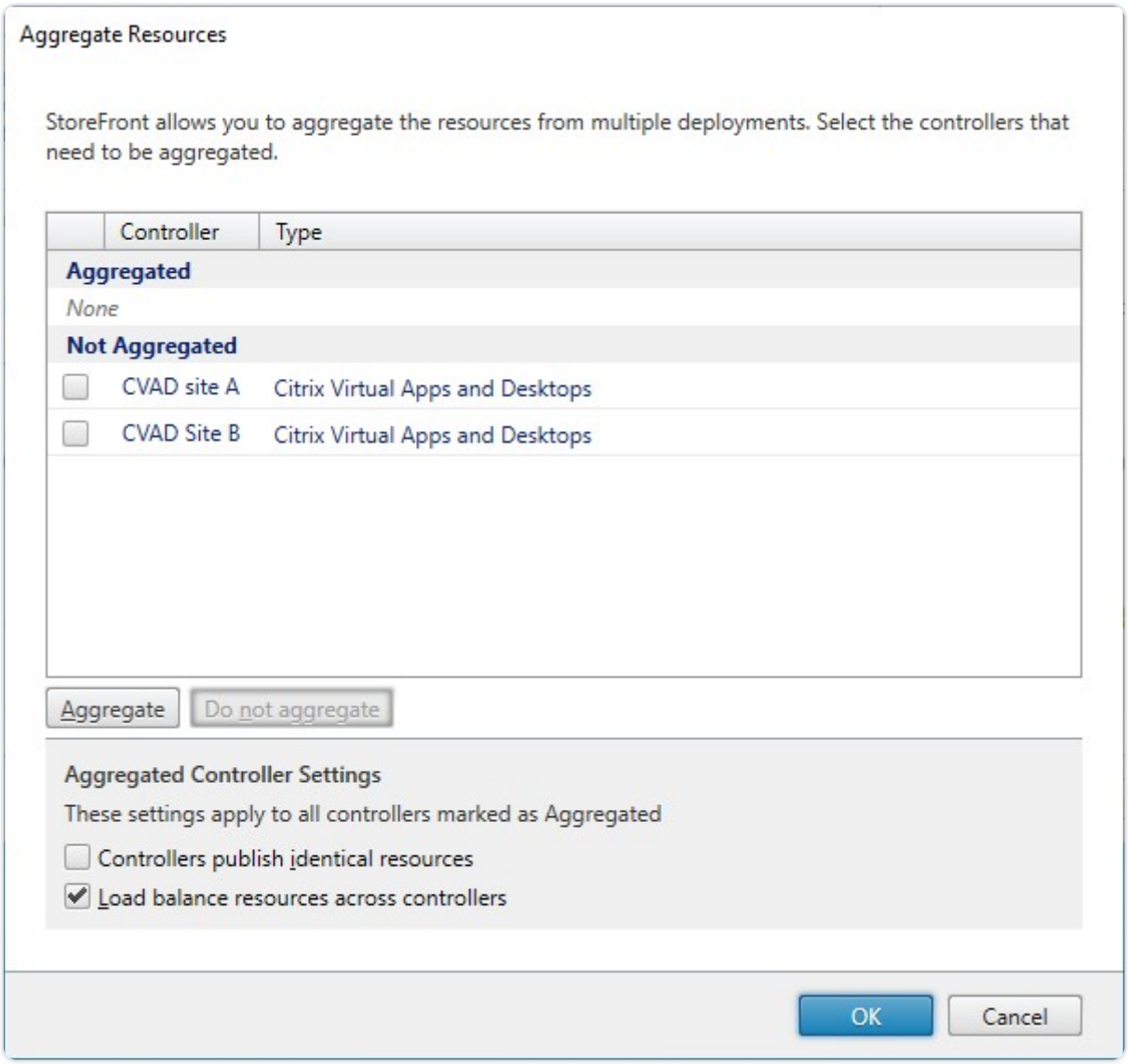
- 控制器报告用户已达到其分配的桌面限制。
- 控制器报告凭据失败（例如，无效、过期或超出时间）。StoreFront 不会尝试使用任何其他交付控制器，因为它预计会得到相同的结果，并避免重复尝试导致帐户锁定。
- 启动超时。这只会在存在大量具有高延迟的控制器等极端情况下发生。

要配置多站点聚合：

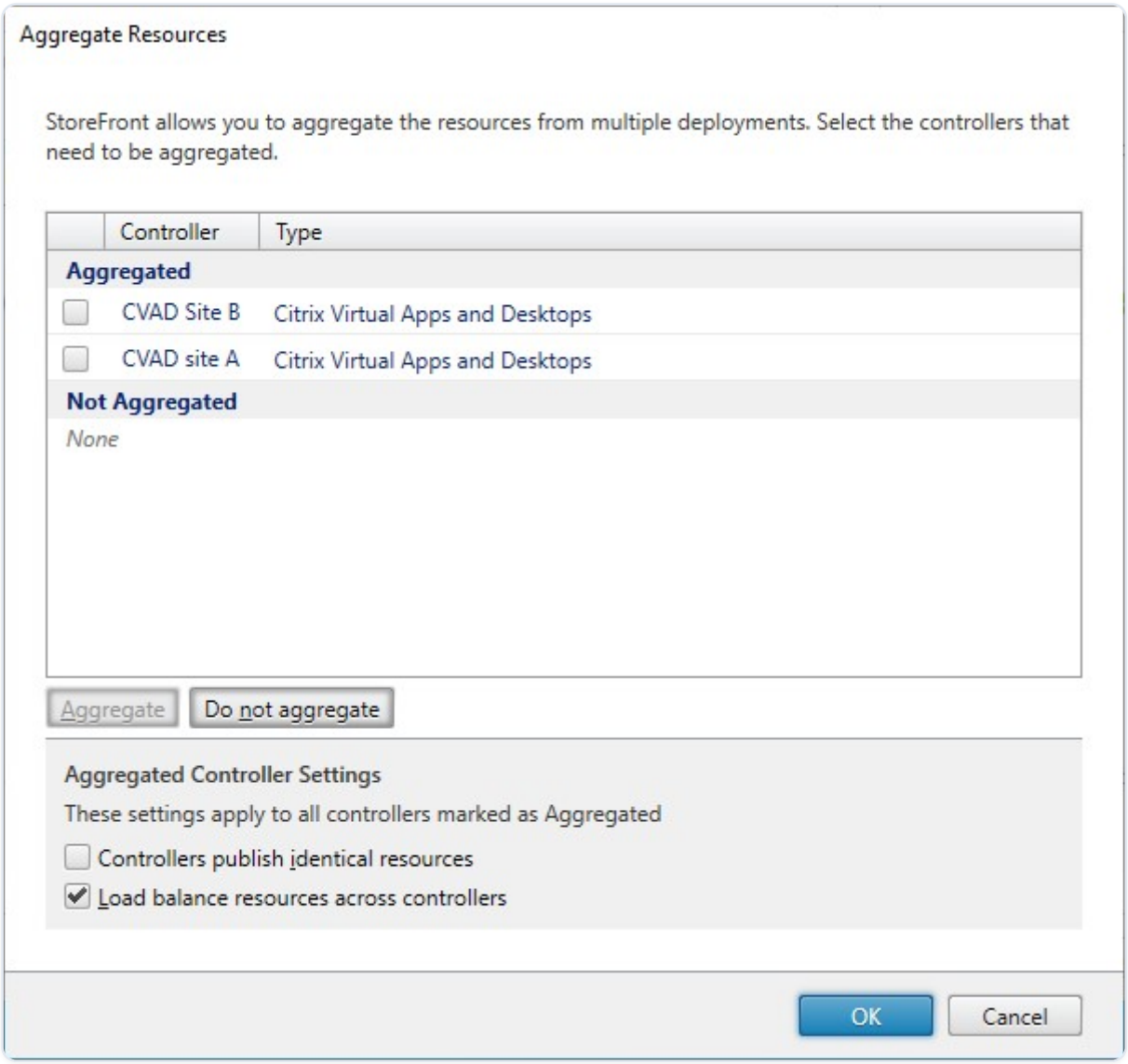
1. 在“**管理站点**”屏幕上，在“**用户映射和多站点聚合配置**”下单击“**配置**”。此选项仅在配置了两个或更多站点时可用。



2. 单击“**聚合资源**”。这将显示“**聚合资源**”屏幕。



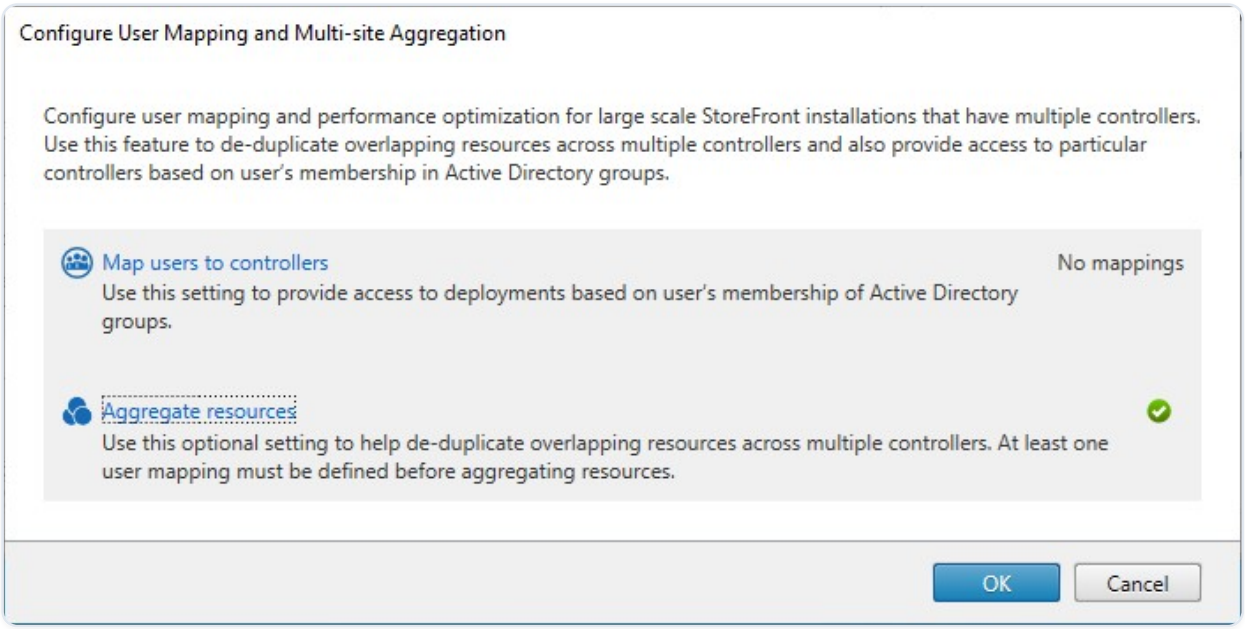
3. 选择具有相同资源的站点，然后单击“**聚合**”。



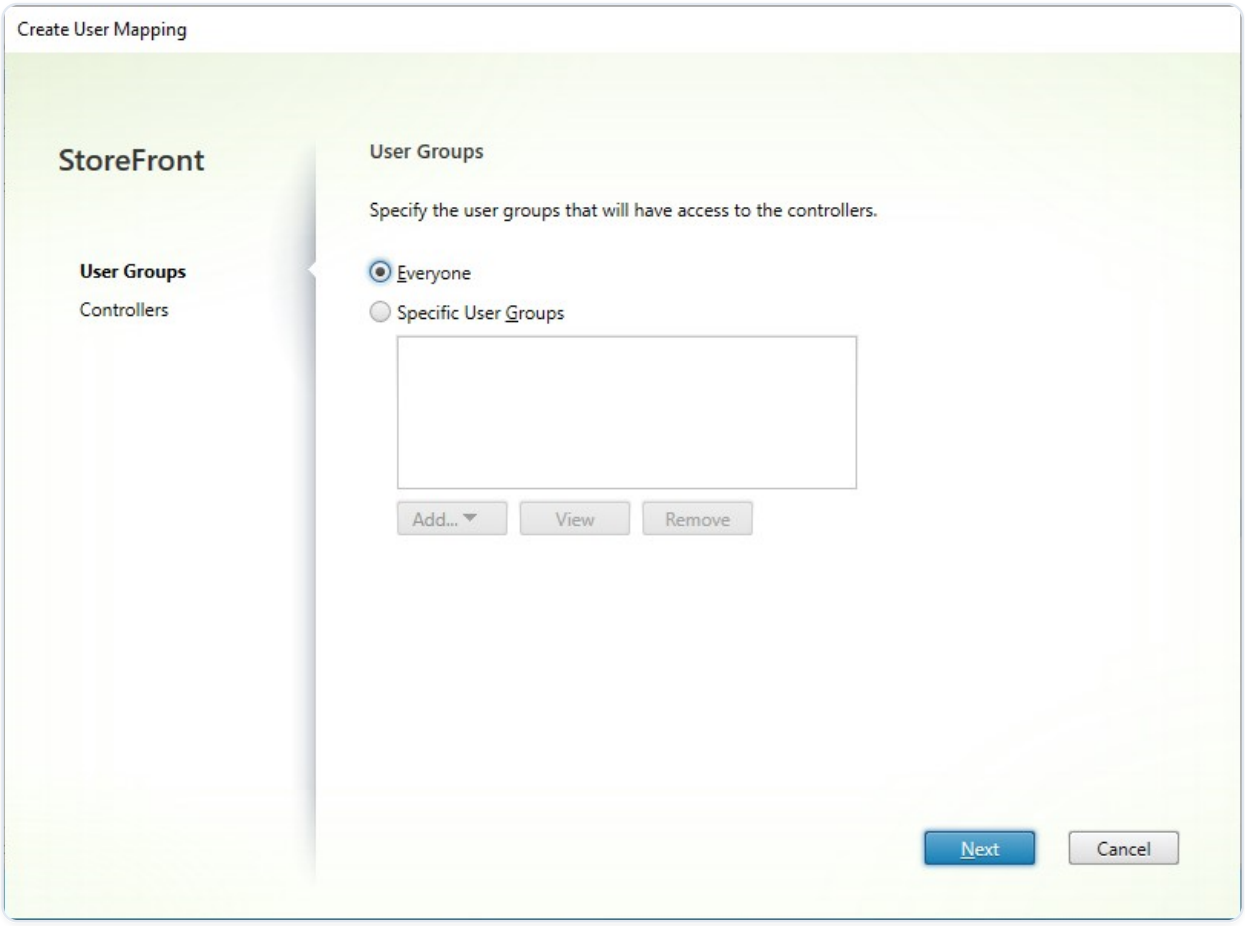
4. 根据需要选择“**聚合控制器设置**”选项：

   - **站点发布相同的资源** - 选中此选项后，StoreFront 仅从聚合集中的一个控制器枚举资源。未选中此选项时，StoreFront 会从聚合集中的所有控制器枚举资源（以累积用户可用的全部资源）。选择此选项可在枚举资源时提高性能，但除非您确定所有聚合源中的资源列表都相同，否则我们不建议这样做。
   - **跨控制器负载平衡资源** - 选中此选项后，启动会在可用站点之间均匀分布。未选中此选项时，启动将定向到用户映射对话框屏幕中指定的第一个站点，如果启动失败，则故障转移到后续站点。

5. 单击“**确定**”返回到“**配置用户映射和多站点聚合**”屏幕。“**聚合资源**”现在已选中。

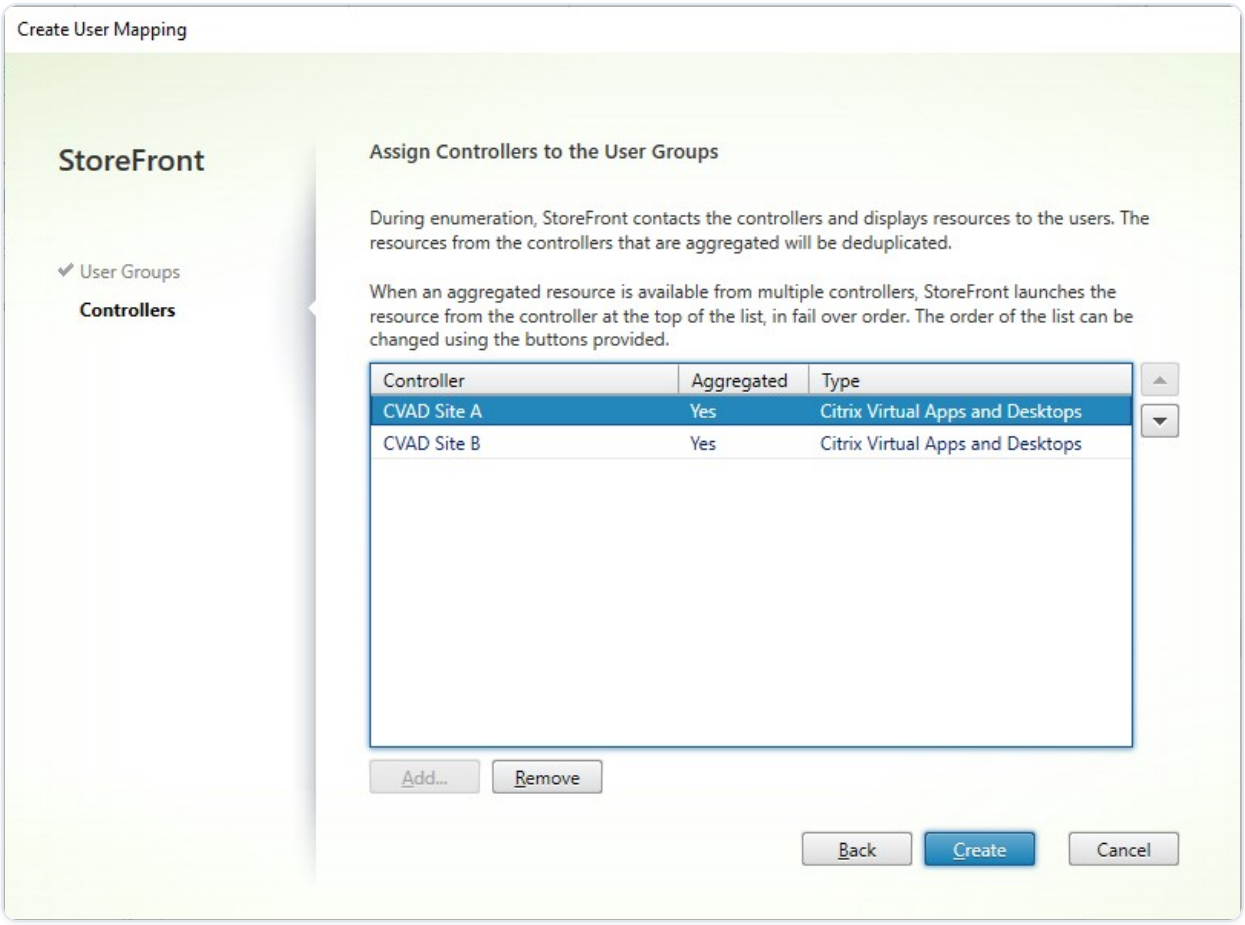


6. 聚合资源后，默认情况下，没有用户可以访问这些资源，因此您必须添加用户映射。单击“**将用户映射到站点**”。这将打开“**创建用户映射**”屏幕。

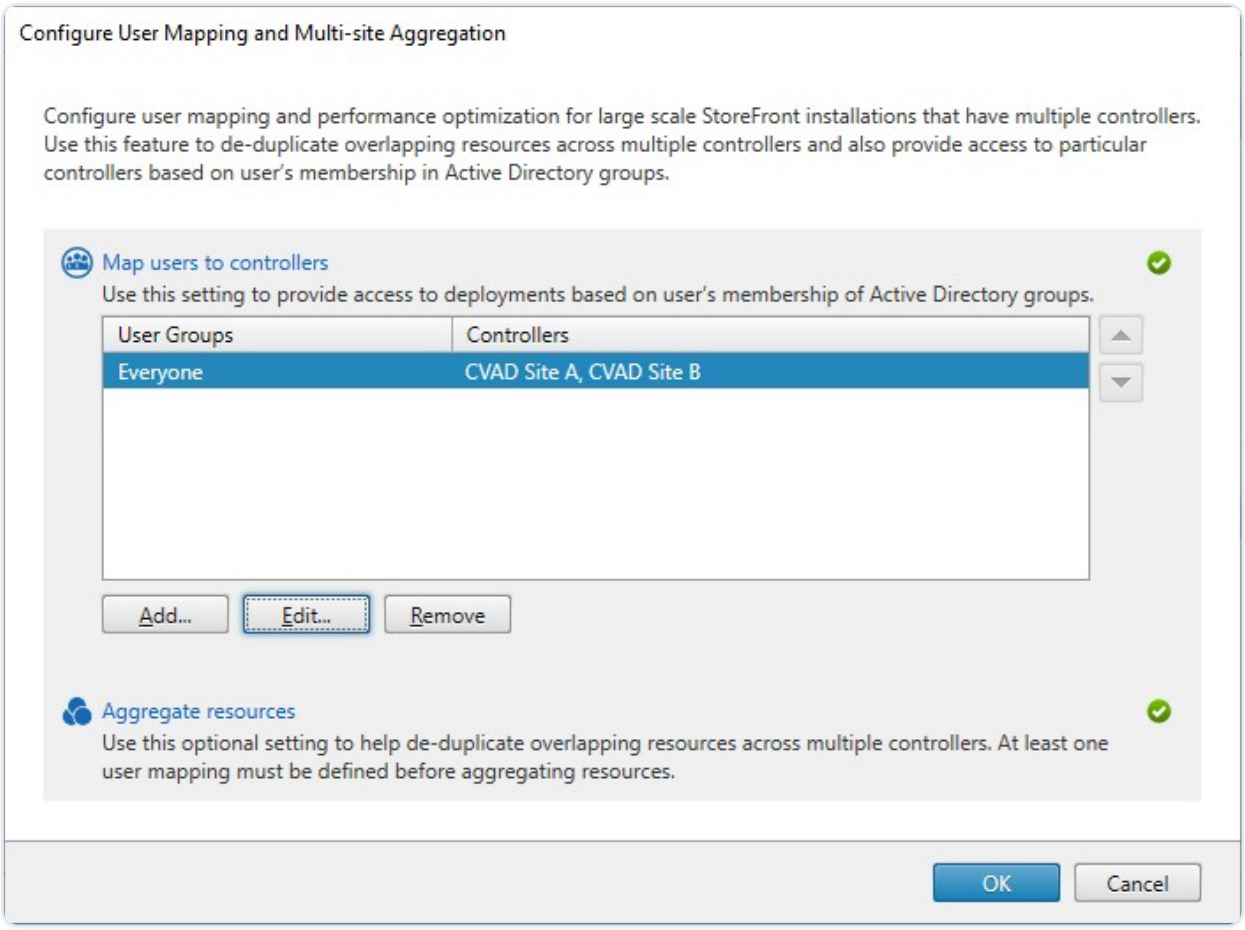


7. 选择**所有人**，或选择**特定用户组**并添加一个或多个组。例如，您可能希望选择一个代表特定位置用户的组。
8. 添加聚合站点。您必须添加所有聚合站点，任何未包含的站点都将变为未聚合。您还可以包含非聚合资源。

9. 如果您未勾选**跨控制器负载平衡资源**，则可以选择 StoreFront 启动资源的优先顺序。



10. 按**创建**返回到**配置用户映射和多站点聚合**。



11. 根据需要添加更多映射。确保每个站点都映射到一个用户组，否则这些资源将无法供任何人使用。
12. 单击“**确定**”。

使用 PowerShell 进行高级配置

您可以使用 StoreFront 管理控制台配置许多常见的多站点和高可用性操作。您还可以使用 PowerShell 配置 StoreFront，它提供以下额外功能：

- 能够为聚合指定多个部署分组。
  - 管理控制台只允许单个部署分组，这在大多数情况下已足够。
  - 对于具有许多部署且资源集不相交的商店，多个分组可能会带来性能改进。
- 能够为聚合部署指定复杂的首选顺序。管理控制台允许聚合部署进行负载平衡或用作单个故障转移列表。使用 PowerShell，您可以拥有多组进行负载平衡并在不同组之间进行故障转移的源。

> **警告：**
>
> 使用 PowerShell 配置高级多站点选项后，无法使用管理控制台修改这些选项。

1. 决定要使用哪些聚合组。在聚合组中，具有相同显示名称的应用程序将聚合到一个图标中。每个聚合组都需要一个名称。使用管理控制台只能创建一个聚合组。通过 PowerShell，您可以定义多个聚合组。
2. 对于每个聚合组，创建一个或多个 EquivalentFarmset，列出您希望聚合的站点（在 SDK 中称为场）。如果聚合组中的不同站点将分配给不同的用户，则必须为每组用户创建一个单独的 EquivalentFarmSet，但共享相同的 `AggregationGroupName`。要创建 EquivalentFarmSet，请使用以下参数调用 New-STFEquivalentFarmset：

   - `Name` - EquivalentFarmset 的唯一名称。
   - `AggregationGroupName` - 场集所属的聚合组的名称。
   - `LoadBalanceMode` - `LoadBalanced` 或 `Failover`。
   - `PrimaryFarms` - 您希望聚合的场。如果 `LoadBalanceMode` 是 `Failover`，请确保场按所需顺序排列。如果一个聚合组有多个 EquivalentFarmSet，则此顺序将与 UserFarmMapping 中定义的 IndexNumber 结合使用，以评估使用哪个站点启动资源。
   - `BackupFarms` - 在没有主场可用时使用的场列表。此功能已弃用。请改为添加具有更高 IndexNumber 的其他 EquivalentFarmSet。

3. 对于不属于聚合组的每个站点，创建一个不指定 `AggregationGroupName` 的 EquivalentFarmset。所有站点（场）都必须是场集的一部分。请使用以下参数调用 New-STFEquivalentFarmset：

   - `Name` - EquivalentFarmSet 的唯一名称
   - `PrimaryFarms` - 未聚合场的名称。

4. 对于需要访问不同站点集的每组用户，请在这些用户和每个 EquivalentFarmSet 之间创建映射。要创建 UserFarmMapping，请使用以下参数调用 Add-STFUserFarmMapping：

   - `StoreService` - 要添加 UserFarmMapping 的 Store 服务。
   - `Name` - 映射的唯一名称。
   - `GroupMembers` - 包含属于映射的用户组的名称和 SID 的哈希表。名称仅用于显示；SID 定义组。要添加所有用户，请在哈希表中创建一个条目，其名称为 `Everyone`，值为 `Everyone`。
   - `EquivalentFarmSet` - 在上一步中创建的 EquivalentFarmSet。
   - `IndexNumber` - 设置评估站点的顺序。这设置了启动资源时使用哪个站点的首选顺序。

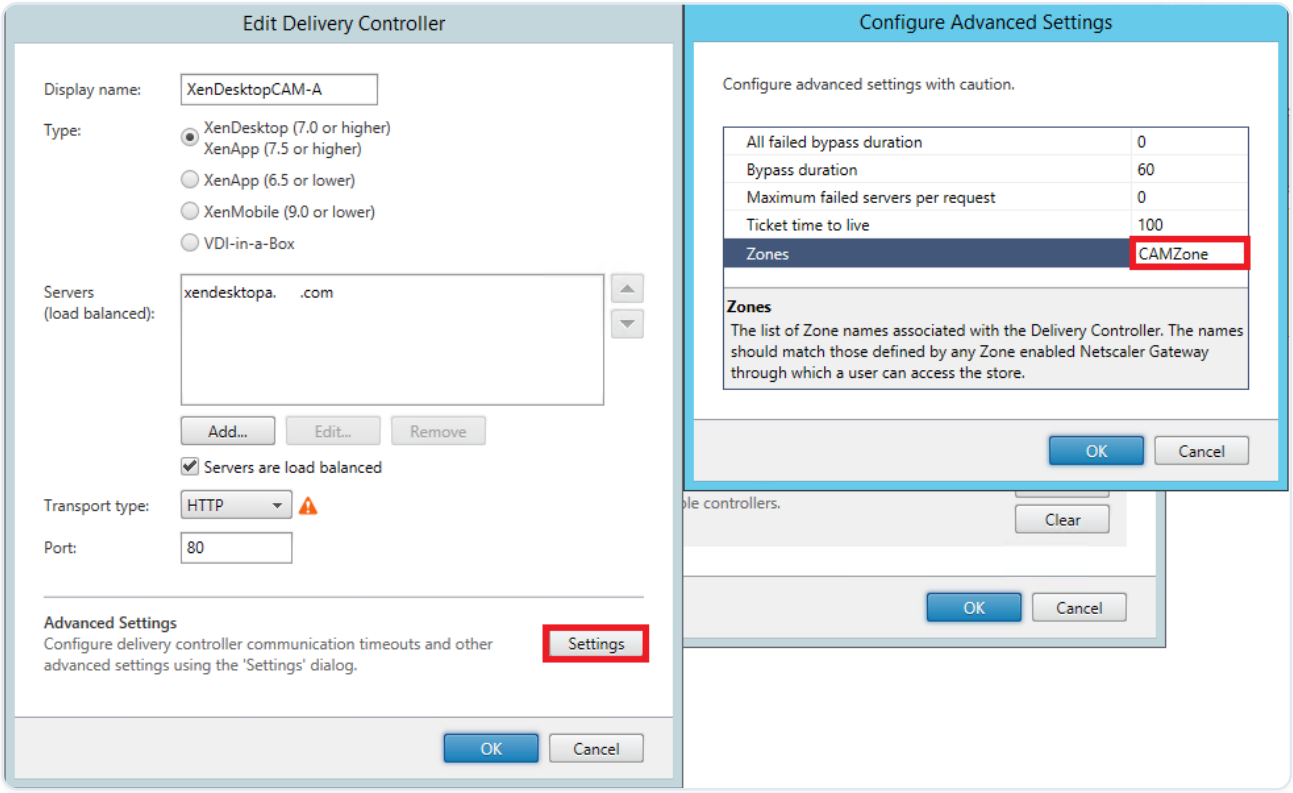
   您必须确保每个站点（场）都包含在至少一个 UserFarmMapping 中，否则任何用户都无法访问该资源。

区域首选项

如果您在不同区域有多个 CVAD 部署，您可以配置 NetScaler ADC 以通知 StoreFront 用户首选的 CVAD 部署。有关详细信息，请参阅全局服务器负载平衡 (GSLB) 驱动的区域首选项。

您必须手动配置 StoreFront，以告知它哪个 CVAD 部署包含哪些区域：

1. 在 Citrix StoreFront 管理控制台中，在左侧窗格中选择“**存储**”节点。
2. 在结果窗格中选择一个存储。
3. 在“**操作**”窗格中，单击“**管理站点**”。
4. 选择一个站点，单击“**编辑**”，然后在“**编辑站点**”屏幕上单击“**设置**”。
5. 在“高级设置”下单击“**设置**”。
6. 在“配置高级设置”对话框中，在“**区域**”行上，单击第二列。
7. 单击“**添加...**”，输入区域名称，然后按“**确定**”。对部署中的每个区域重复此操作。
8. 在“配置高级设置”对话框中，单击“**确定**”。



当用户启动聚合资源时，StoreFront 会遍历 `X-Citrix-ZonePreference` 标头中的区域列表，并查找配置了该区域名称的站点。如果匹配，它会将启动请求发送到该 CVAD 部署。如果不匹配，则会尝试其他部署。

如果 CVAD 部署包含多个区域，则无法将启动请求定向到该部署中的特定区域。

设置 Workspace 应用网站

使用 StoreFront 创建新应用商店时，会自动创建一个网站并将其与该应用商店关联。如果一个应用商店有多个网站，请选择用户使用 Citrix Workspace 应用访问该应用商店时显示的网站。

1. 在 Citrix StoreFront 管理控制台的左侧窗格中，选择 **应用商店** 节点。
2. 在中心窗格中选择一个应用商店，然后从 **操作** 窗格中，选择 **设置 Citrix Workspace™ 应用网站**。如果您没有网站，将显示一条消息，其中包含指向创建网站向导的链接。
3. 选择您希望在用户使用 Citrix Workspace 应用访问此应用商店时显示的网站。
4. 单击“**确定**”。

身份验证

身份验证方法

通常，用户可以直接向 StoreFront™ 进行身份验证，也可以向 StoreFront 前的 Citrix Gateway 进行身份验证。根据您的要求，有多种身份验证方法可用。

方法	详细信息
Active Directory 用户名和密码	用户输入其 Active Directory 用户名和密码。
域直通	Windows 设备使用其登录 Windows 的帐户进行单点登录。
智能卡	用户刷智能卡并输入 PIN。这会使用智能卡上存储的证书对用户进行身份验证。
SAML	使用 SAML 将身份验证委托给第三方身份提供程序。
HTTP 基本认证	允许第三方集成使用其 Active Directory 用户名和密码对用户进行身份验证。请参阅 Web API 开发人员文档 中的 Post Credentials API。HTTP Basic 不提供用户界面供用户进行身份验证。
从 Citrix Gateway 直通	允许用户在 Citrix Gateway 进行身份验证。

或者，在创建新应用商店时，您可以禁用身份验证，改为允许匿名访问应用商店。请参阅创建应用商店。

选择身份验证方法

对于每个应用商店，您可以选择一个或多个身份验证方法，这些方法在通过 Citrix Workspace 应用程序登录应用商店时可用。

1. 在 Citrix StoreFront 管理控制台的左窗格中选择“**应用商店**”节点，然后在“**操作**”窗格中单击“**管理身份验证方法**”。
2. 指定要为用户启用的访问方法。

身份验证方法管理屏幕截图(/en-us/storefront/2507-ltsr/media/stores/authentication/manage-authentication-methods-store.png)

修改应用商店的身份验证方法也会更新通过 Web 浏览器访问应用商店时使用的身份验证方法。要更改通过 Web 浏览器登录时的身份验证方法，请参阅身份验证方法。

使用 PowerShell 选择身份验证方法

要使用 PowerShell 配置身份验证：

1. 调用 Get-STFAuthenticationService 以获取应用商店或虚拟目录的身份验证服务并查看其当前配置。
2. 在身份验证服务上，启用或禁用所需的身份验证协议。要获取可用协议列表，请运行 Get-STFAuthenticationServiceProtocol。要启用协议，请运行 Enable-STFAuthenticationServiceProtocol 并提供要启用的协议列表。要禁用协议，请运行 Disable-STFAuthenticationServiceProtocol 并提供要禁用的协议列表。

身份验证方法设置

某些身份验证方法具有其他设置。选择“**设置**”下拉列表以查看可用选项。有关详细信息，请参阅该身份验证方法的页面。

共享身份验证服务设置

您可以将一个应用商店配置为共享另一个应用商店的身份验证服务，从而实现它们之间的单点登录。

1. 打开“**管理身份验证方法**”。
2. 从“**高级**”下拉菜单中，选择“**共享身份验证服务设置**”。
3. 选中“**使用共享身份验证服务**”复选框，并从“**商店名称**”下拉菜单中选择一个商店。

> **注意：**

> 共享身份验证服务和专用身份验证服务之间没有功能差异。两个以上商店共享的身份验证服务被视为共享身份验证服务，并且任何配置更改都会影响使用共享身份验证服务的所有商店的访问。

安装或卸载身份验证方法

您可以使用 Authentication SDK 自定义现有方法或创建自己的身份验证方法。

如果您在服务器上安装了新的自定义身份验证方法，则还必须将其安装到您希望使用它的每个现有商店中。在“**管理身份验证方法**”屏幕中，选择“**高级**”，然后选择“**安装或卸载身份验证方法**”。

单点登录到 VDA

某些身份验证方法包括单点登录到 VDA 的功能，有关详细信息，请参阅每种身份验证方法。否则，可以使用 Federated Authentication Service 实现单点登录。

Active Directory 用户名和密码身份验证

系统会提示用户输入其 Active Directory 用户名和密码。

用户名和密码身份验证屏幕截图(/en-us/storefront/2507-ltsr/media/stores/authentication/logon-username-password.png)。

如果用户的密码已过期或即将过期，则根据配置，用户可能会获得更改密码的选项。

要在使用 Citrix Workspace 应用程序时为应用商店启用或禁用用户名和密码身份验证，请在 身份验证方法 窗口中选中或取消选中 **Active Directory 用户名和密码**。

默认情况下，为应用商店启用用户名和密码身份验证也会为使用 Web 浏览器的用户启用该应用商店的所有网站的用户名和密码身份验证。您可以在 管理网站身份验证方法选项卡 上为特定网站禁用用户名和密码身份验证。

配置受信任的用户域

您可以限制使用显式域凭据登录的用户对应用商店的访问，无论是直接登录还是通过 Citrix Gateway 使用直通身份验证登录。

1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择“应用商店”节点，然后在结果窗格中选择相应的身份验证方法。在“操作”窗格中，单击**管理身份验证方法**。
2. 从**用户名和密码 > 设置**列表中，选择**配置受信任域**。

3. 选择**仅受信任域**，然后单击**添加**以输入受信任域的名称。在该域中拥有帐户的用户可以登录使用身份验证服务的所有应用商店。要修改域名，请在“受信任域”列表中选择该条目，然后单击**编辑**。要停止域中用户帐户对应用商店的访问，请在列表中选择该域，然后单击**删除**。

   指定域名的方式决定了用户输入其凭据的格式。如果您希望用户以域用户名格式输入其凭据，请将 NetBIOS 名称添加到列表中。要要求用户以用户主体名称格式输入其凭据，请将完全限定域名添加到列表中。如果您希望用户能够以域用户名格式和用户主体名称格式输入其凭据，则必须将 NetBIOS 名称和完全限定域名都添加到列表中。
4. 如果您配置了多个受信任域，请从“默认域”列表中选择用户登录时默认选中的域。
5. 如果要在登录页面上列出受信任域，请选中“在登录页面中显示域列表”复选框。

受信任域屏幕截图(/en-us/storefront/2507-ltsr/media/stores/authentication/authentication-trusted-domain.png)

PowerShell

要获取配置的域列表，请使用 cmdlet `Get-STFExplicitCommonOptions`。

要更新受信任的域，请使用 cmdlet `Set-STFExplicitCommonOptions`。

允许用户更改密码

您可以允许用户随时更改密码。或者，您可以将密码更改限制为密码已过期的用户。这意味着您可以确保用户永远不会因密码过期而无法访问其桌面和应用程序。

密码更改功能在以下客户端中可用：

CITRIX WORKSPACE 应用程序	如果 STOREFRONT 上启用了此功能，用户可以更改已过期的密码	用户会收到密码即将过期的通知	如果 STOREFRONT 上启用了此功能，用户可以在密码过期前更改密码
视窗	是		
Mac	是		
安卓			
iOS			
林纳克斯	是		
Web	是	是	是

默认配置会阻止 Citrix Workspace 应用程序和 Web 浏览器用户更改其密码，即使密码已过期。如果您决定启用此功能，请确保包含服务器的域的策略不会阻止用户更改其密码。允许用户更改密码会将敏感安全功能暴露给任何可以访问使用身份验证服务的任何应用商店的人员。如果您的组织有安全策略，规定用户密码更改功能仅供内部使用，请确保任何应用商店都无法从公司网络外部访问。

如果您允许用户随时更改密码，则密码即将过期的本地用户在登录时会收到警告。默认情况下，用户的通知期限由适用的 Windows 策略设置决定。或者，您可以配置自定义通知期限。

1. 在“**管理身份验证方法**”窗口中，从“**Active Directory 用户名和密码**”>“**设置**”下拉菜单中，选择“**管理密码选项**”
2. 要允许用户更改密码，请选中“**允许用户更改密码**”复选框。

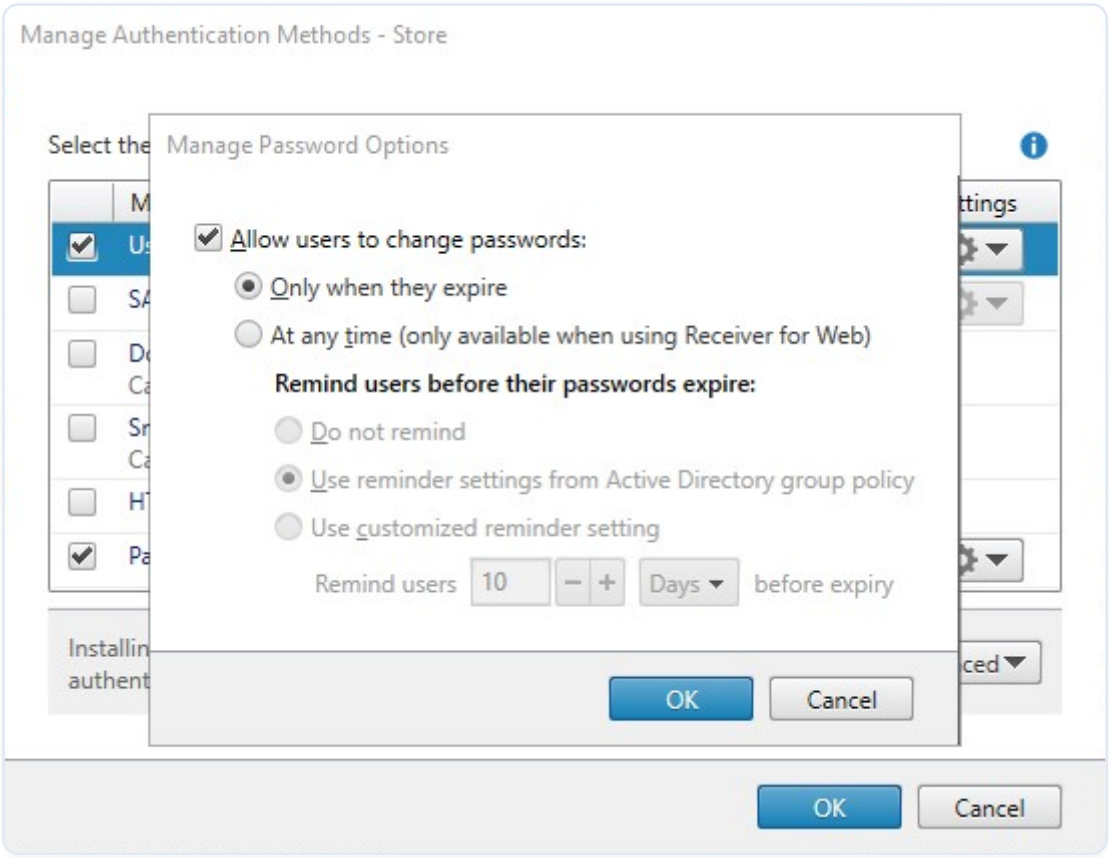
> **注意：**
>
> 如果您不选择此选项，则必须自行安排支持因密码过期而无法访问其桌面和应用程序的用户。

3. 选择是允许用户**仅在密码过期时**更改密码，还是**随时**更改密码。
4. 选择是否在用户密码过期前提醒他们。您可以选择以下选项：

   - **不提醒** - UI 不显示密码过期提醒。它只在密码过期时通知用户。
   - **使用 Active Directory 组策略中的提醒设置** - 登录后，如果用户的密码将在 组策略 中配置的天数内过期，用户界面会发出通知。用户可以选择更改密码。

     > **注意：**
     >
     > StoreFront 不考虑 精细密码策略。因此，如果您正在使用精细密码策略，则不应选择此选项。

   - **使用自定义提醒设置** - 登录后，如果用户的密码将在给定天数内过期，用户界面会通知用户。用户可以选择更改密码。



注意

注意 1：

确保您的 StoreFront 服务器上有足够的磁盘空间来存储所有用户的配置文件。要检查用户的密码是否即将过期，StoreFront 会在该服务器上为该用户创建一个本地配置文件。StoreFront 必须能够联系域控制器才能更改用户的密码。

注意 2：

如果您启用安全策略 **网络访问：限制允许对 SAM 进行远程调用的客户端**，则必须包含所有需要更改密码的用户。

注意 3：

如果您随时启用或禁用更改密码，这也会影响 Citrix Gateway 直通 身份验证的**管理密码选项**下的设置。

PowerShell

要获取受信任域列表，请使用 cmdlet `Get-STFExplicitCommonOptions`。

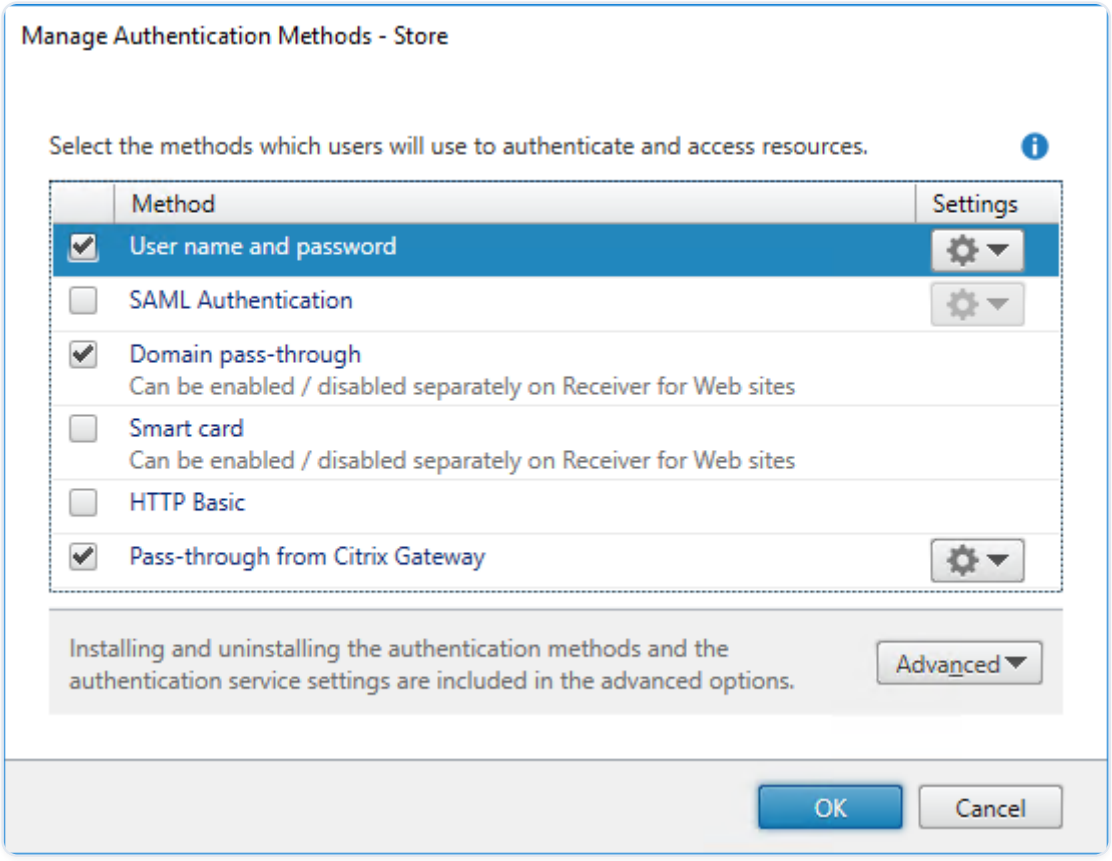
要更新受信任域，请使用 cmdlet `Set-STFExplicitCommonOptions`。

密码验证

通常，StoreFront 会要求 Windows 验证 Active Directory 中的凭据。这要求 Windows 服务器与用户位于同一域中，或者两个域之间存在信任关系。当无法建立 Active Directory 信任时，您可以配置 StoreFront 使用 Citrix Virtual Apps and Desktops 交付控制器来验证凭据。这也会影响 HTTP 基本身份验证和网关直通身份验证。

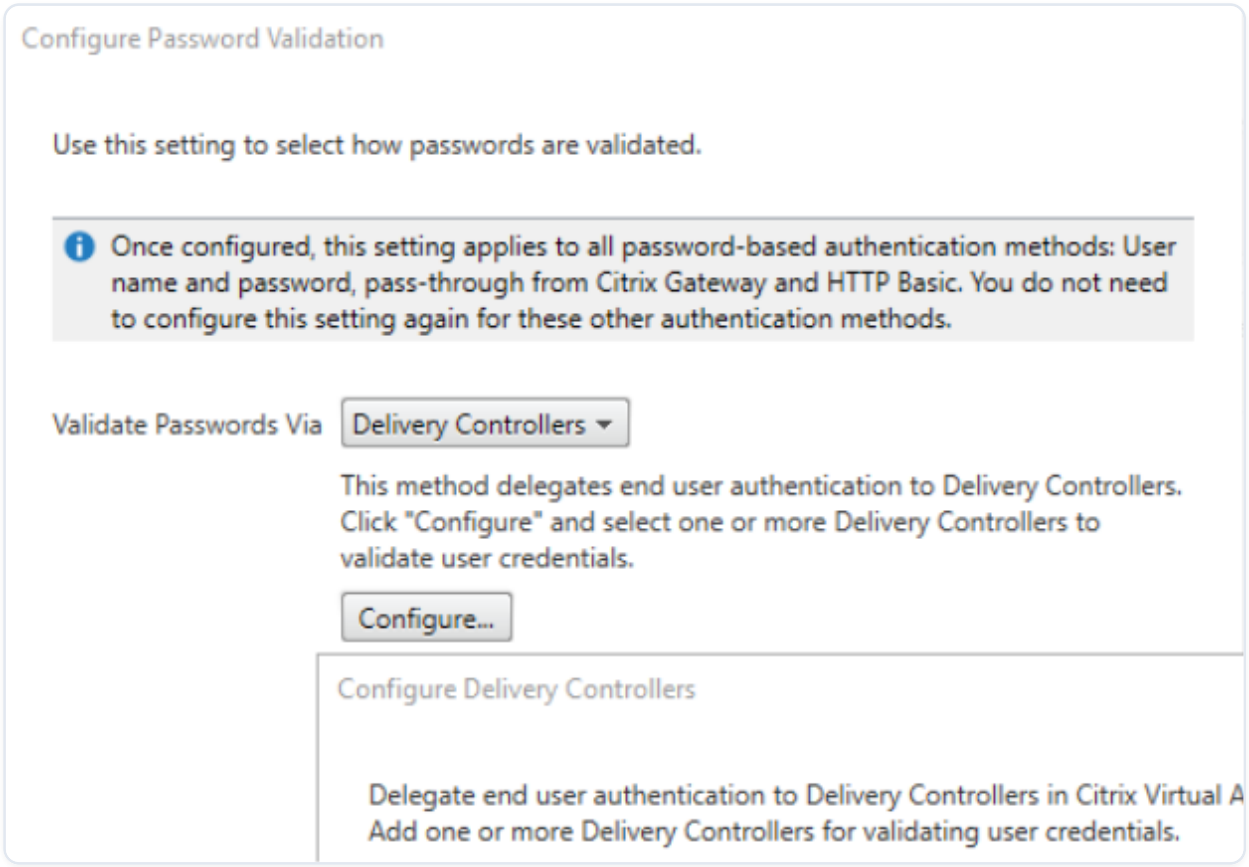
要配置 StoreFront 如何验证密码：

1. 在**管理身份验证方法**窗口中，从**用户名和密码 > 设置**下拉菜单中，选择**配置密码验证**。

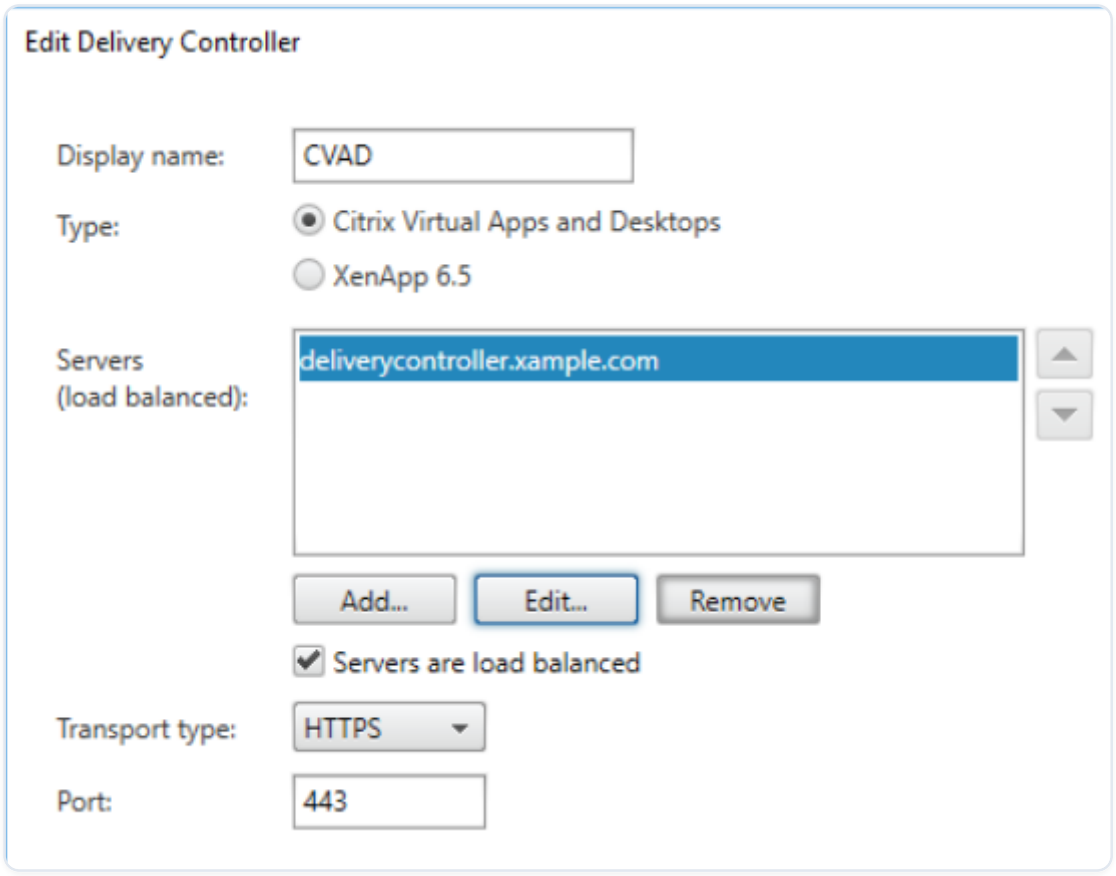


2. 从**通过以下方式验证密码**下拉列表中，选择：

   - **Active Directory** - 要求 Windows 在 Active Directory 中验证凭据
   - **Delivery Controllers** - 要求配置的 Delivery Controller™ 验证凭据。



3. 如果选择了**Delivery Controllers**，则选择**配置**。在**配置 Delivery Controllers**屏幕中，添加一个或多个**Delivery Controllers**以验证用户凭据，然后单击**确定**。



4. 选择“**确定**”。

PowerShell

要获取密码的验证方式，请使用 cmdlet `Get-STFExplicitAuthenticator`。

要通过交付控制器执行密码验证，请使用 cmdlet `Set-STFExplicitAuthenticator` 将验证器设置为 `xmlServiceAuthenticator`。要设置用于验证凭据的交付控制器，请使用 cmdlet Enable-STFXmlServiceAuthentication

单点登录到 VDA

当用户启动资源时，StoreFront 会将用户用于登录到商店的凭据传递给 VDA 进行单点登录。

如果为商店启用了 Federated Authentication Service (FAS)，则 StoreFront 会联系 FAS 服务器以提供证书，从而实现对商店的单点登录。此证书将传递给 VDA，而不是凭据。如果 StoreFront 无法联系 FAS 服务器，则无法对 VDA 进行单点登录。

自定义登录屏幕

登录屏幕是根据模板生成的，通常位于 `C:\inetpub\wwwroot\Citrix\[Store name]Auth\App_Data\Templates\UsernamePassword.tfrm`。该模板使用 Forms Template Language 定义。

以下示例添加标题并阻止适用于 Windows 的 Citrix Workspace 应用程序缓存密码：

标题文本

当用户登录到应用商店时，默认情况下登录对话框上不显示标题文本。您可以显示文本“请登录”或编写自己的自定义消息：

1. 使用文本编辑器打开身份验证服务的 `UsernamePassword.tfrm` 文件。
2. 在文件中找到以下行。

   ```
   @* @Heading("ExplicitAuth:AuthenticateHeadingText") *@
   ```

3. 通过删除前导 `@*` 和尾随 `*@` 来取消注释该语句。

   ```
   @Heading("ExplicitAuth:AuthenticateHeadingText")
   ```

   当 Citrix Workspace 应用程序用户登录到使用此身份验证服务的应用商店时，他们会看到默认标题文本“请登录”或此文本的相应本地化版本。

4. 要修改标题文本，请使用文本编辑器打开身份验证服务的 `ExplicitFormsCommon.xx.resx` 文件，该文件通常位于 `C:\inetpub\wwwroot\Citrix\[Store name]Auth\App_Data\resources\` 目录中。
5. 在文件中找到以下元素。编辑 `<value>` 元素中包含的文本，以修改用户在访问使用此身份验证服务的应用商店时在登录对话框上看到的标题文本。

```
<data name="AuthenticateHeadingText" xml:space="preserve">

    <value>My Company Name</value>

</data>
```

要修改其他区域设置中用户的登录对话框标题文本，请编辑本地化文件 *ExplicitAuth.languagecode.resx*，其中 **languagecode** 是区域设置标识符。

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，当用户登录到 StoreFront 应用商店时，适用于 Windows 的 Citrix Workspace 应用程序会存储用户的密码。要阻止适用于 Windows 的 Citrix Workspace 应用程序缓存用户的密码，请编辑身份验证服务的文件。

1. 使用文本编辑器打开文件 inetpub\wwwroot\Citrix\\Auth\App_Data\Templates\UsernamePassword.tfrm。
2. 在文件中找到以下行。

```
@SaveCredential(id: @GetTextValue("saveCredentialsId"), labelKey:
"ExplicitFormsCommon:SaveCredentialsLabel", initiallyChecked:
ControlValue("SaveCredentials"))
```

3. 按如下所示注释该语句。

```
<!-- @SaveCredential(id: @GetTextValue("saveCredentialsId"), labelKey:
"ExplicitFormsCommon:SaveCredentialsLabel", initiallyChecked:
ControlValue("SaveCredentials")) -->
```

用户每次登录使用此身份验证服务的商店时，都必须输入其密码。

默认情况下，Citrix Workspace app for Windows 会自动填充上次输入的用户名。要阻止填充用户名字段，或了解阻止缓存密码的替代机制，请参阅 阻止 Citrix Workspace app for Windows 缓存密码和用户名。

通过 Citrix Gateway 进行远程访问

您可以配置您的 Citrix Gateway，以便用户使用其域用户名和密码（可选地使用第二个因素）登录到网关。这些凭据会传递到 StoreFront 以登录到商店。要为 LDAP 用户名和密码身份验证配置您的 Citrix Gateway，请参阅 NetScaler 文档 - LDAP 身份验证。要配置 StoreFront，请参阅 从 Citrix Gateway 直通。

SAML 身份验证

SAML（安全断言标记语言）是一种开放标准，由身份和身份验证产品使用。使用 SAML，您可以将 StoreFront 配置为将用户重定向到外部身份提供程序进行身份验证。

> **注意**
>
> 配置 StoreFront 以使用 SAML 身份验证进行内部访问。对于外部访问，请使用 SAML 身份验证配置 Citrix Gateway，然后配置 StoreFront 以使用Gateway 直通身份验证。

> StoreFront 需要符合 SAML 2.0 的身份提供程序 (IdP)，例如：

- 使用 SAML 绑定（而非 WS-Federation 绑定）的 Microsoft AD Federation Services。有关详细信息，请参阅 CTX220638。
- Citrix Gateway（配置为 IdP）。
- Microsoft Entra ID。有关详细信息，请参阅 CTX237490。

SAML 断言必须包含一个 `<saml:NameID>` 元素，其中填充了用户的用户主体名称 (UPN)。StoreFront 会在 Active Directory 中查找此 UPN。StoreFront 不支持其他目录中的用户。使用 Entra ID 时，用户必须具有混合身份。

要为应用商店启用或禁用 SAML 身份验证，请在身份验证方法 窗口中选择 **SAML 身份验证**。默认情况下，为应用商店启用 SAML 身份验证会为该应用商店的所有网站启用它。您可以在身份验证方法 选项卡上独立禁用或启用每个网站的 SAML 身份验证。

StoreFront™ SAML 端点

要配置 SAML，您的身份提供程序可能需要以下端点：

- 实体 ID 的 URL。这是应用商店身份验证服务的路径，通常为 `https://[storefront host]/Citrix/[StoreName]Auth`
- 断言消费者服务的 URL，通常为 `https://[storefront host]/Citrix/[StoreName]Auth/SamlForms/AssertionConsumerService`
- 元数据服务，通常为 `https://[storefront host]/Citrix/[StoreName]Auth/SamlForms/ServiceProvider/Metadata`

此外还有一个测试端点，通常为 `https://[storefront host]/Citrix/[StoreName]Auth/SamlTest`

您可以使用以下 PowerShell 脚本列出指定应用商店的端点。

```
# Change this value for your Store

$storeVirtualPath = "/Citrix/Store"



$auth = Get-STFAuthenticationService -Store (Get-STFStoreService
-VirtualPath $storeVirtualPath)

$spId =
$auth.AuthenticationSettings["samlForms"].SamlSettings.ServiceProvider.Uri
.AbsoluteUri

$acs = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.VirtualPath
+ "/SamlForms/AssertionConsumerService")

$md = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.VirtualPath
+ "/SamlForms/ServiceProvider/Metadata")

$samlTest = New-Object System.Uri $auth.Routing.HostbaseUrl,
($auth.VirtualPath + "/SamlTest")

Write-Host "SAML Service Provider information:

Entity ID: $spId

Assertion Consumer Service: $acs

Metadata: $md
```

```
Test Page: $samlTest"
```

输出示例：

```
SAML Service Provider information:

Entity ID: https://storefront.example.com/Citrix/StoreAuth

Assertion Consumer Service: https://storefront.example.com/Citrix/
StoreAuth/SamlForms/AssertionConsumerService

Metadata: https://storefront.example.com/Citrix/StoreAuth/SamlForms/
ServiceProvider/Metadata

Test Page: https://storefront.example.com/Citrix/StoreAuth/SamlTest
```

使用元数据交换进行配置

To simplify configuration, you can exchange metadata (identifiers, certificates, endpoints and other configuration) between the Identity Provider and the Service Provider, which is StoreFront in this case.

如果您的身份提供程序支持元数据导入，则可以将其指向 StoreFront 元数据终结点。**注意**：此操作必须通过 HTTPS 完成。

要使用来自身份提供程序的元数据配置 StoreFront，请使用 Update-STFSamlIdPFromMetadata cmdlet，例如：

```
Get-Module "Citrix.StoreFront*" -ListAvailable | Import-Module



# Remember to change this with the virtual path of your Store.

$StoreVirtualPath = "/Citrix/Store"



$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$auth = Get-STFAuthenticationService -StoreService $store
```

```
# To read the metadata directly from the Identity Provider, use the
following:

# Note again this is only allowed for https endpoints

Update-STFSamlIdPFromMetadata -AuthenticationService $auth -Url https://
example.com/FederationMetadata/2007-06/FederationMetadata.xml



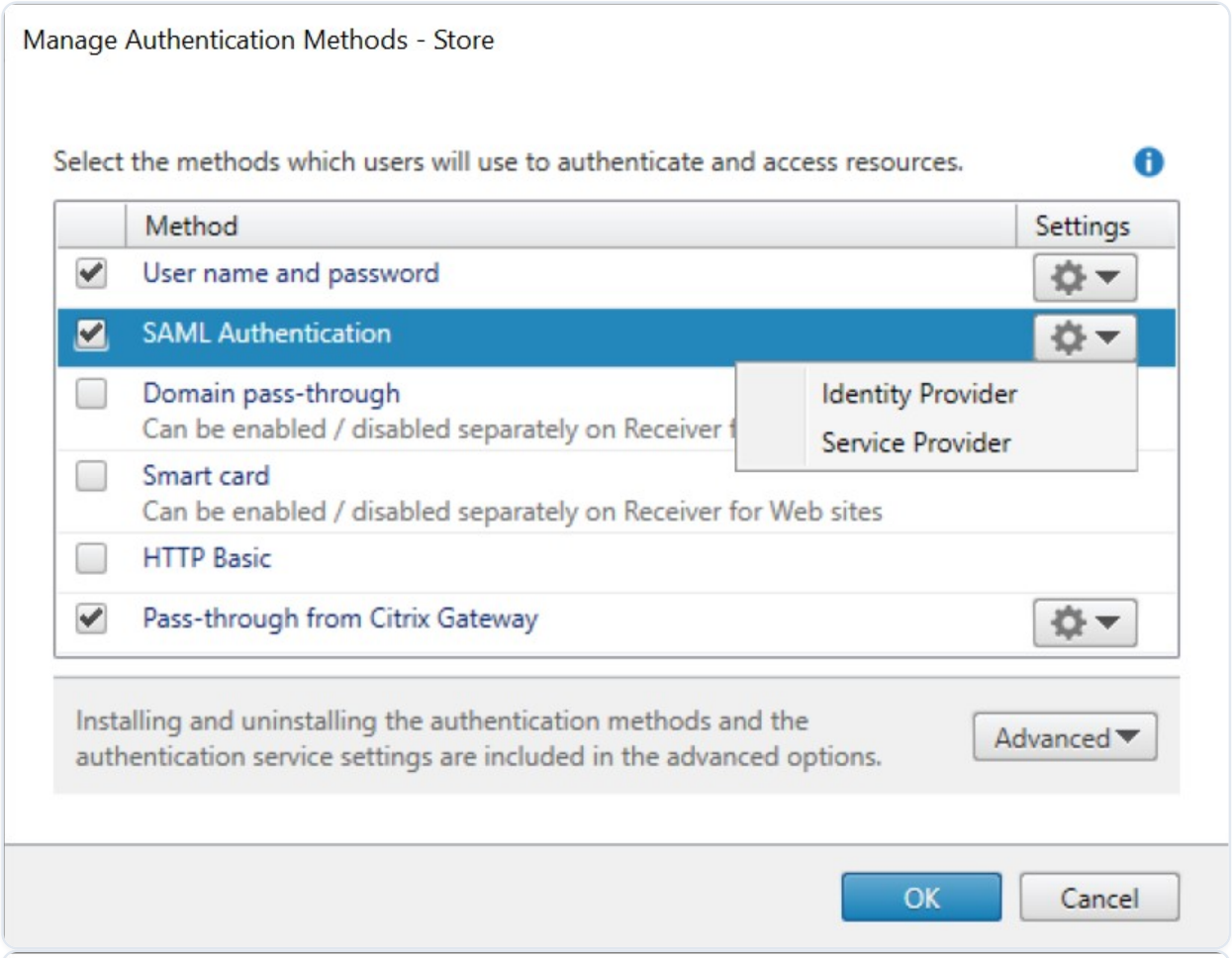
# If the metadata has already been download, use the following:

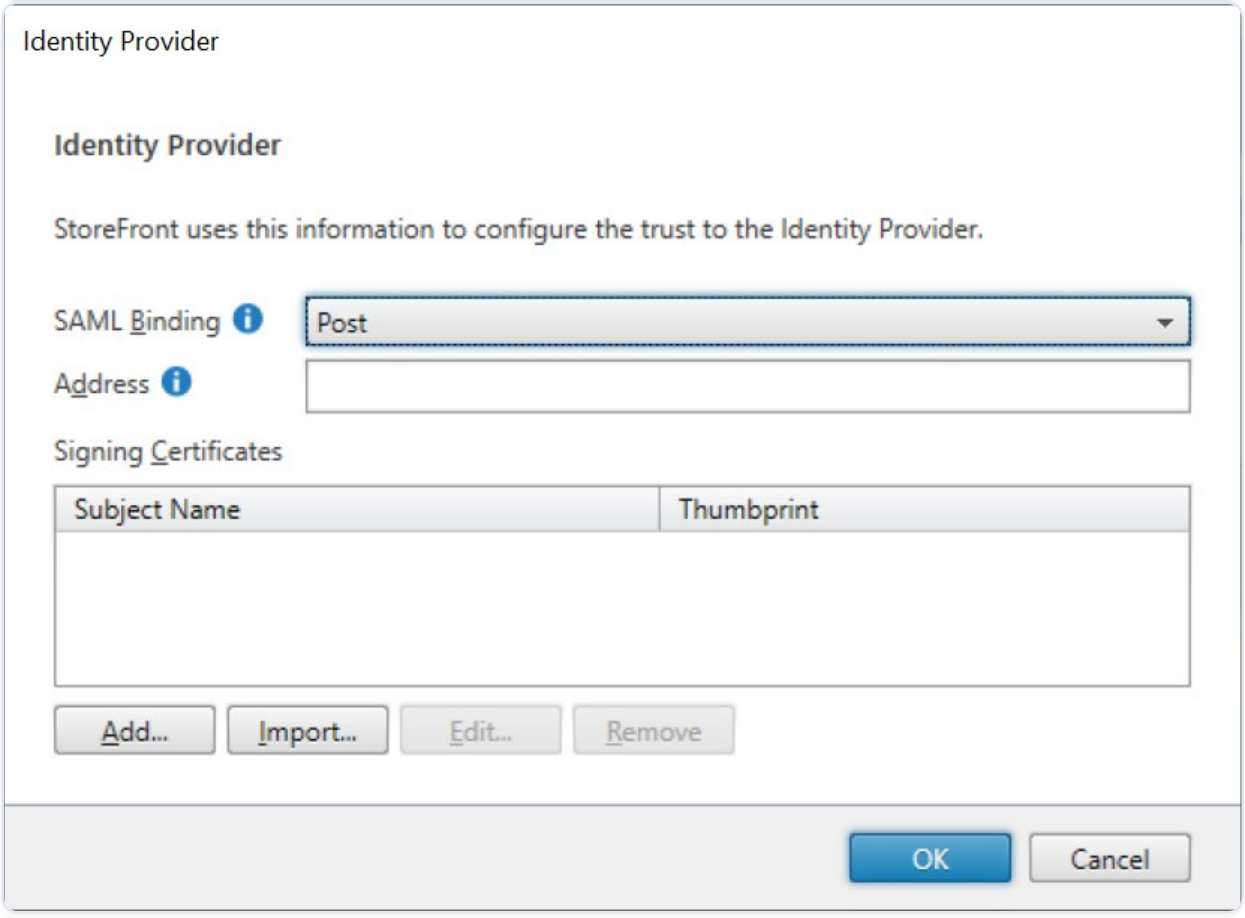
# Note: Ensure that the file is encoded as UTF-8

Update-STFSamlIdPFromMetadata -AuthenticationService $auth -FilePath "C:
\Users\exampleusername\Downloads\FederationMetadata.xml"
```

配置身份提供程序

1. 在 **SAML 身份验证** 行中单击设置下拉菜单，然后单击 **身份提供商**。





2. 选择 **SAML 绑定** 为 **Post** 或 **Redirect**。

3. 输入身份提供商的**地址**。
4. 导入用于签署 SAML 令牌的证书。
5. 按“**确定**”保存更改。

配置服务提供商

1. 点击 **SAML 身份验证** 行中的设置下拉菜单，然后点击 **服务提供商**。

   身份提供程序窗口的屏幕截图(/en-us/storefront/2507-ltsr/media/stores/authentication/saml-service-provider.png)
2. 可选地，选择一个**导出签名证书**，用于向身份提供程序签名消息。
3. 可选地，选择一个**导出加密证书**，用于解密从身份提供程序接收到的消息。
4. **服务提供程序标识符**已预填充商店的身份验证服务。
5. 按**确定**以保存更改。

PowerShell

使用 PowerShell：

- 要导入签名证书，请调用 cmdlet Import-STFSamlSigningCertificate。
- 要导入加密证书，请调用 cmdlet Import-STFSamlEncryptionCertificate。

测试

要测试 SAML 集成：

1. 转到 SAML 测试页面，请参阅 StoreFront SAML Endpoints。
2. 这会将您重定向到身份提供程序。输入您的凭据。
3. 您将被重定向回测试页面，该页面显示身份声明和断言。

配置 Delivery Controller™ 以信任 StoreFront

使用 SAML 身份验证时，StoreFront 无法访问用户的凭据，因此无法向 Citrix Virtual Apps and Desktops 进行身份验证。因此，您必须配置 Delivery Controller 以信任来自 StoreFront 的请求，请参阅 Citrix Virtual Apps and Desktops Security considerations and best practices。

使用联合身份验证服务对 VDA 进行单点登录

使用 SAML 身份验证时，StoreFront 无法访问用户的凭据，因此默认情况下无法对 VDA 进行单点登录。您可以使用联合身份验证服务来提供单点登录。

域直通身份验证

用户对其已加入域的 Windows 计算机进行身份验证，其凭据将用于自动登录到 Citrix Workspace 应用程序。此功能适用于 Windows 版 Citrix Workspace 应用程序和 Windows 上受支持的 Web 浏览器。

StoreFront 配置

要为 Windows 版 Citrix Workspace 应用程序启用域直通，请在 身份验证方法 中选择 **域直通**。

默认情况下，为某个应用商店启用域直通身份验证也会为该应用商店的所有网站启用 HTML5 版 Citrix Workspace 应用程序的域直通身份验证。您可以在 管理网站身份验证方法选项卡 上为特定网站禁用域直通身份验证。

配置 Delivery Controller™ 以信任 StoreFront

使用域直通身份验证时，StoreFront 无法访问用户凭据，因此无法向 Citrix Virtual Apps and Desktops 进行身份验证。因此，您必须配置 Delivery Controller 以信任来自 StoreFront 的请求，请参阅 Citrix Virtual Apps and Desktops 安全注意事项和最佳实践。

Web 浏览器配置

要通过 Web 浏览器使用域直通，网站必须使用 Citrix Web Extension 或 Citrix Workspace Launcher 成功检测到 Citrix Workspace 应用程序。您可能需要更新用户的 Web 浏览器配置以允许域直通身份验证。

IE浏览器、Edge浏览器 和 谷歌浏览器

大多数 Web 浏览器使用 Windows Internet Explorer 区域配置来决定是否启用单点登录。默认情况下，它仅对本地 Intranet 区域中的站点启用。要将您的站点添加到 Intranet 区域：

1. 打开“控制面板”
2. 打开“Internet 选项”
3. 转到“**安全**”选项卡。
4. 选择“**本地 Intranet**”
5. 单击“**站点**”。
6. 点击 **高级**。
7. 添加您的 StoreFront 网站。

这些设置可以使用组策略部署。

有关配置 Microsoft Edge 以进行 Windows 集成身份验证的更多信息，请参阅 Microsoft 文档。

火狐

修改浏览器高级设置，以信任 StoreFront 网站 URI，从而实现单点登录。

> **警告：**
>
> 错误地编辑高级设置可能会导致严重问题。请自行承担编辑风险。

1. 在将使用域直通进行身份验证的计算机上打开 Firefox。
2. 在地址栏中，输入 about:config。
3. 点击“我接受风险！”。
4. 在搜索栏中，输入 negotiate。
5. 双击 network.negotiate-auth.delegation-uris。
6. 输入您的公司 Windows 域名（例如，mydomain.com）。
7. 点击 OK。
8. 双击 network.negotiate-auth.trusted-uris。
9. 输入您的企业 Windows 域名（例如，mydomain.com）。
10. 单击确定。
11. 关闭并重新启动 Firefox。

单点登录到 VDA

要使用域凭据单点登录到 VDA，您必须使用适用于 Windows 的 Citrix Workspace 应用程序，并启用“**启用单点登录**”组件，请参阅 配置域直通身份验证。或者，您可以配置 联合身份验证服务 以单点登录到 VDA。

智能卡身份验证

通过智能卡身份验证，用户在访问其应用商店时使用智能卡和 PIN 码进行身份验证。可以通过 Citrix Workspace 应用程序、Web 浏览器和 XenApp Services URL 连接到应用商店的用户启用智能卡身份验证。

> **注意：**
>
> 如果用户使用智能卡登录 Windows，建议您启用域直通身份验证，而不是（或以及）智能卡身份验证。这可以实现对应用商店的单点登录，而无需使用智能卡重新进行身份验证。

> 使用智能卡身份验证可简化用户的登录过程，同时增强用户访问基础架构的安全性。对内部公司网络的访问通过使用公钥基础架构的基于证书的双因素身份验证进行保护。私钥受硬件控制保护，并且永远不会离开智能卡。您的用户可以使用智能卡和 PIN 码，方便地从各种公司设备访问其桌面和应用程序。

要启用智能卡身份验证，必须在包含 StoreFront 服务器的 Microsoft Active Directory 域中配置用户帐户，或者在与 StoreFront 服务器域具有直接双向信任关系的域中配置用户帐户。支持涉及双向信任的多林部署。

文档 Citrix 环境的智能卡配置 介绍了如何为使用特定智能卡类型的 Citrix 部署配置智能卡。其他供应商的智能卡也适用类似的步骤。

先决条件

- 确保所有用户帐户都已配置在您计划部署 StoreFront 服务器的 Microsoft Active Directory 域中，或者配置在与 StoreFront 服务器域具有直接双向信任关系的域中。
- 如果您计划启用智能卡身份验证的直通功能，请确保您的智能卡读卡器类型、中间件类型和配置以及中间件 PIN 缓存策略允许这样做。
- 在运行提供用户桌面和应用程序的 Virtual Delivery Agent 的虚拟或物理计算机上安装您的供应商的智能卡中间件。有关将智能卡与 Citrix Virtual Desktops 结合使用的更多信息，请参阅 智能卡 。
- 确保您的公钥基础架构已正确配置。检查证书到帐户的映射是否已为您的 Active Directory 环境正确配置，并且用户证书验证可以成功执行。

配置 StoreFront

- 您必须使用 HTTPS 进行 StoreFront 与用户设备之间的通信才能启用智能卡身份验证。请参阅 使用 HTTPS 保护 StoreFront。
- 要通过 Citrix Workspace 应用程序连接到应用商店时启用智能卡身份验证，请在 身份验证方法 中勾选或取消勾选“**智能卡**”。
- 默认情况下，为应用商店启用智能卡身份验证也会为该应用商店的所有网站启用智能卡身份验证。您可以在 管理网站身份验证方法选项卡 上独立启用或禁用特定网站的智能卡身份验证。
- 如果您同时配置智能卡和用户名密码身份验证，用户最初会收到使用智能卡和 PIN 码登录的提示，但如果他们的智能卡出现任何问题，可以选择显式身份验证。

配置 Delivery Controller™ 以信任 StoreFront

使用智能卡身份验证时，StoreFront 无法访问用户凭据，因此无法向 Citrix Virtual Apps and Desktops 进行身份验证。因此，您必须配置 Delivery Controller 以信任来自 StoreFront 的请求，请参阅 Citrix Virtual Apps and Desktops 安全注意事项和最佳实践。

通过 Citrix Gateway 进行远程访问

对于远程访问，您可以在 Citrix Gateway 上启用智能卡，然后通过委派身份验证启用直通身份验证到 StoreFront。有关更多详细信息，请参阅 Gateway 直通。

为确保用户在建立与其资源的连接时不会在虚拟服务器上收到额外的凭据提示，请创建第二个网关并在安全套接字层 (SSL) 参数中禁用客户端身份验证。有关详细信息，请参阅 配置智能卡身份验证。通过具有智能卡身份验证的网关访问 StoreFront 时。通过此虚拟服务器配置最佳 Citrix Gateway 路由，以连接到为应用商店提供桌面和应用程序的部署。有关详细信息，请参阅 为应用商店配置最佳 HDX 路由。

单点登录到 VDA

您可以通过直通用户的智能卡凭据来启用对 VDA 的单点登录。可以通过 Web 浏览器或适用于 Windows 的 Citrix Workspace™ 应用程序访问应用商店，但资源必须在适用于 Windows 的 Citrix Workspace 应用程序中打开。在其他操作系统上或通过浏览器访问资源时，用户在连接到 VDA 时必须重新输入其凭据。

1. 在安装适用于 Windows 的 Citrix Workspace 时，包含单点登录组件并将其配置为单点登录。请参阅 配置域直通身份验证。
2. 使用文本编辑器打开应用商店的 default.ica 文件。请参阅 Default ica。
3. 要为不通过 Citrix Gateway 访问应用商店的用户启用智能卡凭据直通，请在 部分中添加以下设置。

   ```
   DisableCtrlAltDel=Off
   ```

   此设置适用于应用商店的所有用户。要同时启用域直通和智能卡身份验证直通到桌面和应用程序，您必须为每种身份验证方法创建单独的应用商店。然后，将用户引导至适合其身份验证方法的应用商店。
4. 要为通过 Citrix Gateway 访问应用商店的用户启用智能卡凭据直通，请在 部分中添加以下设置。

   ```
   UseLocalUserAndPassword=On
   ```

此设置适用于应用商店的所有用户。要为某些用户启用直通身份验证，并要求其他用户登录才能访问其桌面和应用程序，您必须为每组用户创建单独的应用商店。然后，将用户引导至适合其身份验证方法的应用商店。

或者，您可以配置 Federated Authentication Service 以单点登录到 VDA

重要注意事项

将智能卡用于 StoreFront 用户身份验证需满足以下要求和限制。

- 要将虚拟专用网络 (VPN) 隧道与智能卡身份验证结合使用，用户必须安装 Citrix Gateway 插件并通过网页登录，在每个步骤中使用智能卡和 PIN 进行身份验证。对于智能卡用户，通过 Citrix Gateway 插件对 StoreFront 进行直通身份验证不可用。
- 可以在同一用户设备上使用多张智能卡和多个读卡器，但如果启用智能卡身份验证的直通，用户必须确保在访问桌面或应用程序时只插入一张智能卡。
- 当在应用程序中使用智能卡时（例如用于数字签名或加密），用户可能会看到额外的提示，要求插入智能卡或输入 PIN。如果同时插入了多张智能卡，则可能会发生这种情况。这也可能是由于配置设置（例如通常使用组策略配置的 PIN 缓存等中间件设置）造成的。当智能卡已在读卡器中时，如果系统提示用户插入智能卡，则用户必须单击“取消”。如果系统提示用户输入 PIN，则他们必须再次输入 PIN。
- 如果您为不通过 Citrix Gateway 访问应用商店的已加入域设备的适用于 Windows 用户的 Citrix Workspace 应用程序启用智能卡身份验证的直通到 Citrix Virtual Apps and Desktops，则此设置适用于应用商店的所有用户。要同时启用域直通和智能卡身份验证的直通到桌面和应用程序，您必须为每种身份验证方法创建单独的应用商店。然后，您的用户必须连接到适合其身份验证方法的应用商店。
- 如果您为通过 Citrix Gateway 访问应用商店的已加入域设备的适用于 Windows 用户的 Citrix Workspace 应用程序启用智能卡身份验证的直通到 Citrix Virtual Apps and Desktops，则此设置适用于应用商店的所有用户。要为某些用户启用直通身份验证并要求其他用户登录其桌面和应用程序，您必须为每组用户创建单独的应用商店。然后，将您的用户引导至适合其身份验证方法的应用商店。
- 每个 XenApp® Services URL 只能配置一种身份验证方法，并且每个应用商店只有一个 URL 可用。如果除了智能卡身份验证之外，您还需要启用其他类型的身份验证，则必须为每种身份验证方法创建单独的应用商店，每个应用商店都有一个 XenApp Services URL。然后，将您的用户引导至适合其身份验证方法的应用商店。
- 安装 StoreFront 后，Microsoft Internet Information Services (IIS) 中的默认配置仅要求为 StoreFront 身份验证服务的证书身份验证 URL 的 HTTPS 连接提供客户端证书。IIS 不会为任何其他 StoreFront URL 请求客户端证书。此配置使您能够为智能卡用户提供回退到显式身份验证

的选项，以防他们的智能卡出现任何问题。根据相应的 Windows 策略设置，用户还可以移除智能卡而无需重新进行身份验证。

如果您决定将 IIS 配置为要求所有 StoreFront URL 的 HTTPS 连接提供客户端证书，则身份验证服务和应用商店必须位于同一服务器上。您必须使用对所有应用商店都有效的客户端证书。使用此 IIS 站点配置，智能卡用户无法通过 Citrix Gateway 连接，也无法回退到显式身份验证。如果用户从设备中移除智能卡，则必须再次登录。

从 Citrix Gateway 直通

用户向 Citrix Gateway 进行身份验证，并在访问其应用商店时自动登录。首次配置对应用商店的远程访问时，默认启用 Citrix Gateway 身份验证直通。用户可以通过 Citrix Gateway 使用本地安装的 Citrix Workspace 应用程序或 Web 浏览器连接到应用商店。有关为 Citrix Gateway 配置 StoreFront 的详细信息，请参阅 配置 Citrix Gateway。

StoreFront 支持以下 Citrix Gateway 身份验证方法的直通。

- **域** 用户使用其 Active Directory 用户名和密码登录。
- **RSA** 用户使用由安全令牌生成的令牌代码（有时与个人识别码结合）派生的密码登录。如果您仅通过安全令牌启用直通身份验证，请确保您提供的资源不需要额外或替代的身份验证形式，例如用户的 Microsoft Active Directory 域凭据。
- **智能卡** 用户使用与其 Active Directory 帐户关联的智能卡登录。
- **RSA + 域** 用户使用其域凭据和安全令牌密码登录。
- **SAML** 用户被重定向到第三方 IdP 以通过 SAML 登录。SAML 断言必须包含用户 Active Directory 帐户的 UPN。
- **通过 OIDC 的 Entra ID**（CU1 及更高版本）用户被重定向到 Microsoft Entra ID 进行身份验证。用户可以是纯 Entra ID 用户，也可以是混合身份用户。有关详细信息，请参阅 使用 OIDC 进行 Entra ID 身份验证。

如果您在 Citrix Gateway 上禁用了身份验证或禁用了单点登录，则不使用直通，您必须配置其他身份验证方法之一。

如果您为从 Citrix Workspace 应用程序内部访问应用商店的远程用户配置了到 Citrix Gateway 的双源身份验证，则必须在 Citrix Gateway 上创建两个身份验证策略。将 RADIUS（远程身份验证拨号用户服务）配置为主要身份验证方法，将 LDAP（轻量级目录访问协议）配置为辅助方法。修改凭据索引以在会话配置文件中使用辅助身份验证方法，以便将 LDAP 凭据传递给 StoreFront。将 Citrix Gateway 设备添加到 StoreFront 配置时，将登录类型设置为“域和安全令牌”。有关详细信息，请参阅 `<http://support.citrix.com/article/CTX125364>`

要通过 Citrix Gateway 到 StoreFront 启用多域身份验证，请在每个域的 Citrix Gateway LDAP 身份验证策略中将 SSO 名称属性设置为 userPrincipalName。您可以要求用户在 Citrix Gateway 登录页面上指定一个域，以便确定要使用的相应 LDAP 策略。配置到 StoreFront 的 Citrix Gateway 会话配置文件时，请勿指定单点登录域。您必须配置每个域之间的信任关系。确保允许用户从任何域登录到 StoreFront，而不是仅限制访问显式信任的域。

在您的 Citrix Gateway 部署支持的情况下，您可以使用 SmartAccess 根据 Citrix Gateway 会话策略控制用户对 Citrix Virtual Apps and Desktops 资源的访问。

启用 Gateway 直通

要在通过 Workspace 应用程序连接时为应用商店启用或禁用网关直通身份验证，请在 身份验证方法 窗口中勾选或取消勾选 **从 Citrix Gateway 直通**。

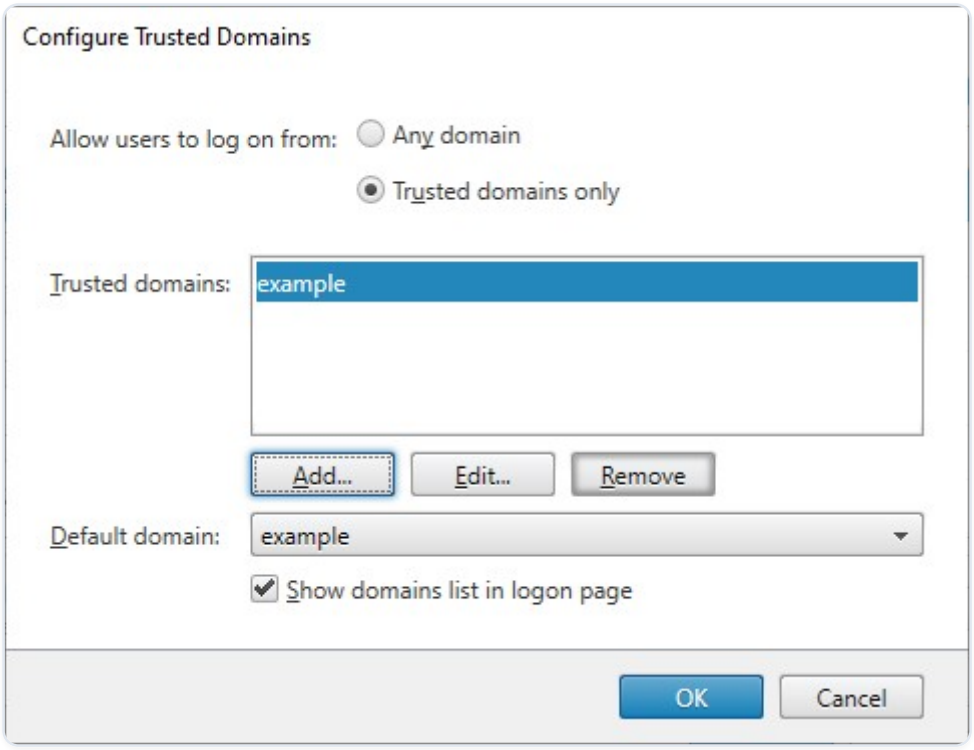
默认情况下，为某个应用商店启用 Citrix Gateway 直通身份验证也会为该应用商店的所有网站启用此功能。您可以在身份验证方法选项卡上禁用特定网站的用户名和密码身份验证。

配置受信任的用户域

如果您的 Citrix Gateway 配置为使用 LDAP 身份验证，则可以限制对特定域的访问。

1. 在“管理身份验证方法”窗口中，从 **Citrix Gateway 直通** > **设置** 下拉菜单中，选择 **配置受信任域**。
2. 选择 **仅受信任域**，然后单击 **添加** 以输入受信任域的名称。在该域中拥有帐户的用户能够登录到使用身份验证服务的所有应用商店。要修改域名，请在“受信任域”列表中选择该条目，然后单击 **编辑**。要停止该域中用户帐户对应用商店的访问，请在列表中选择该域，然后单击 **删除**。

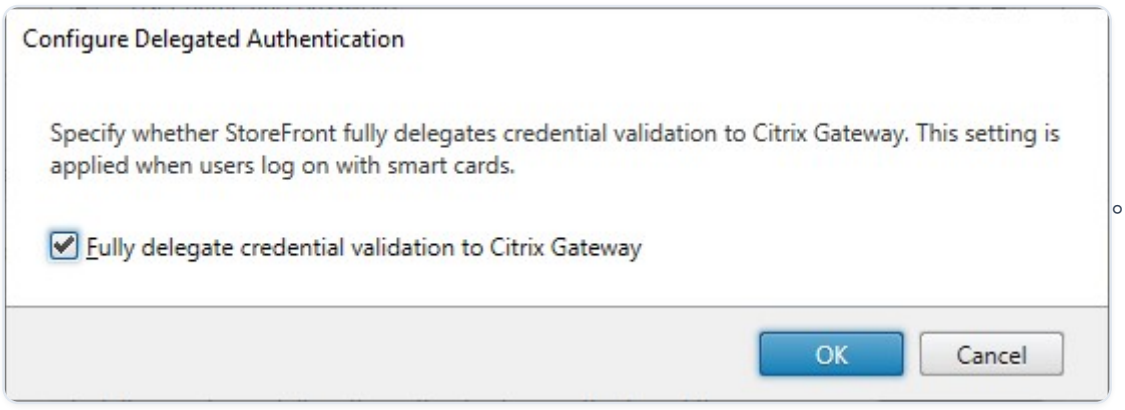
   指定域名的方式决定了用户输入其凭据的格式。如果您希望用户以域用户名格式输入其凭据，请将 NetBIOS 名称添加到列表中。要要求用户以用户主体名称格式输入其凭据，请将完全限定域名添加到列表中。如果您希望用户能够以域用户名格式和用户主体名称格式输入其凭据，则必须将 NetBIOS 名称和完全限定域名都添加到列表中。
3. 如果配置了多个受信任域，请从“默认域”列表中选择用户登录时默认选择的域。
4. 如果您希望在登录页面上列出受信任域，请选中“在登录页面中显示域列表”复选框。



委派身份验证

默认情况下，StoreFront 会验证从 Citrix Gateway 接收到的用户名和密码。如果您的 Citrix Gateway 不通过 LDAP 使用 Active Directory 凭据作为因素（例如，在使用 SAML 或智能卡时），则必须将 StoreFront 配置为信任网关执行的验证。在这种情况下，务必在配置网关时输入回调 URL，以便 StoreFront 可以验证请求是否来自 Citrix Gateway，请参阅管理 Citrix Gateway。

1. 在 **管理身份验证方法** 窗口中，从 **Citrix Gateway 直通** > **设置** 下拉菜单中，选择 **配置委派身份验证**。
2. 选择 **将凭据验证完全委派给 Citrix Gateway**。



。

PowerShell

要使用 PowerShell 将应用商店配置为将身份验证委派给 Citrix Gateway，请运行 cmdlet Set-STFCitrixAGBasicOptions。

- 要将身份验证委托给网关，请将 `CredentialValidationMode` 设置为 `Auto`。
- 要让 StoreFront 验证凭据，请将 `CredentialValidationMode` 设置为 `Password`。

密码验证

您可以选择 StoreFront 是自行验证凭据，还是要求交付控制器验证凭据。有关详细信息，请参阅用户名和密码身份验证 - 密码验证。

如果选择了**将凭据验证完全委托给 Citrix Gateway**，则使用交付控制器验证密码的设置将不起作用。在这种情况下，StoreFront 必须能够在 Active Directory 中查找用户，因此 StoreFront 服务器的域必须始终与用户域具有信任关系。

允许用户在登录时更改过期密码

如果您的 Citrix Gateway 配置为使用 LDAP（用户名和密码）身份验证，则可以将 NetScaler 配置为允许在登录时更改过期密码。

1. 登录 NetScaler® 管理网站
2. 在侧面菜单中，转至**身份验证** > **控制板**。
3. 单击身份验证服务器。
4. 在**其他设置**下，勾选**允许更改密码**。

允许用户在登录后更改密码

您可以将 StoreFront 配置为允许用户在登录后更改密码。此功能仅在网关使用 LDAP 身份验证且用户通过浏览器（而非本地安装的 Citrix Workspace 应用程序）访问应用商店时可用。

默认的 StoreFront 配置会阻止用户更改密码，即使密码已过期。如果您决定启用此功能，请确保包含您服务器的域的策略不会阻止用户更改密码。允许用户更改密码会将敏感的安全功能暴露给任何可以访问使用身份验证服务的任何应用商店的人。如果您的组织有安全策略规定用户密码更改功能仅供内部使用，请确保任何应用商店都无法从公司网络外部访问。

1. 在**管理身份验证方法**窗口中，从**从 Citrix Gateway 直通** > **设置**下拉菜单中，选择**管理密码选项**
2. 要允许用户更改密码，请选中“**允许用户更改密码**”复选框。

管理密码选项的屏幕截图(/en-us/storefront/2507-ltsr/media/stores/authentication/gateway-authentication-change-password.png)

> **注意：**

> 如果选中或清除“**允许用户更改密码**”，这也会影响 用户名和密码 身份验证的“**管理密码选项**”下的设置。

PowerShell

要使用 PowerShell 修改更改密码选项，请运行 cmdlet Set-STFExplicitCommonOptions。

配置 Delivery Controller™ 以信任 StoreFront

当 Citrix Gateway 配置为 LDAP 身份验证时，它会将凭据传递给 StoreFront。对于其他身份验证方法，StoreFront 无法访问凭据，因此无法向 Citrix Virtual Apps and Desktops 进行身份验证。因此，您必须配置 Delivery Controller 以信任来自 StoreFront 的请求，请参阅 Citrix Virtual Apps and Desktops 安全注意事项和最佳实践。

单点登录到 VDA

使用 Active Directory 凭据

当网关配置为 LDAP 身份验证时，它会将凭据传递给 StoreFront，以便可以单点登录到 VDA。无需额外配置。

使用联合身份验证服务

对于 LDAP 以外的网关身份验证方法，StoreFront 无法访问用户凭据，因此默认情况下无法进行单点登录。您可以使用 联合身份验证服务 提供单点登录。

使用 Entra ID

当网关配置为通过 OIDC 使用 Entra ID 身份验证时，您可以启用 Entra ID 单点登录。这需要 CU1 或更高版本。有关详细信息，请参阅 配置 VDA Entra ID 单点登录。

管理网站

创建应用商店时，系统会自动为其创建一个网站，用户可以通过浏览器或 Citrix Workspace 应用程序访问该网站。您必须至少有一个网站。您可以向现有应用商店添加其他网站。这允许您为用户提供具有不同配置的不同 URL。但是，多个网站只能通过 Web 浏览器访问，因为 Citrix Workspace 应用程序配置为使用一个特定网站作为应用商店，请参阅 (/zh-cn/storefront/2507-ltsr/stores/workspace-app-website.html)。

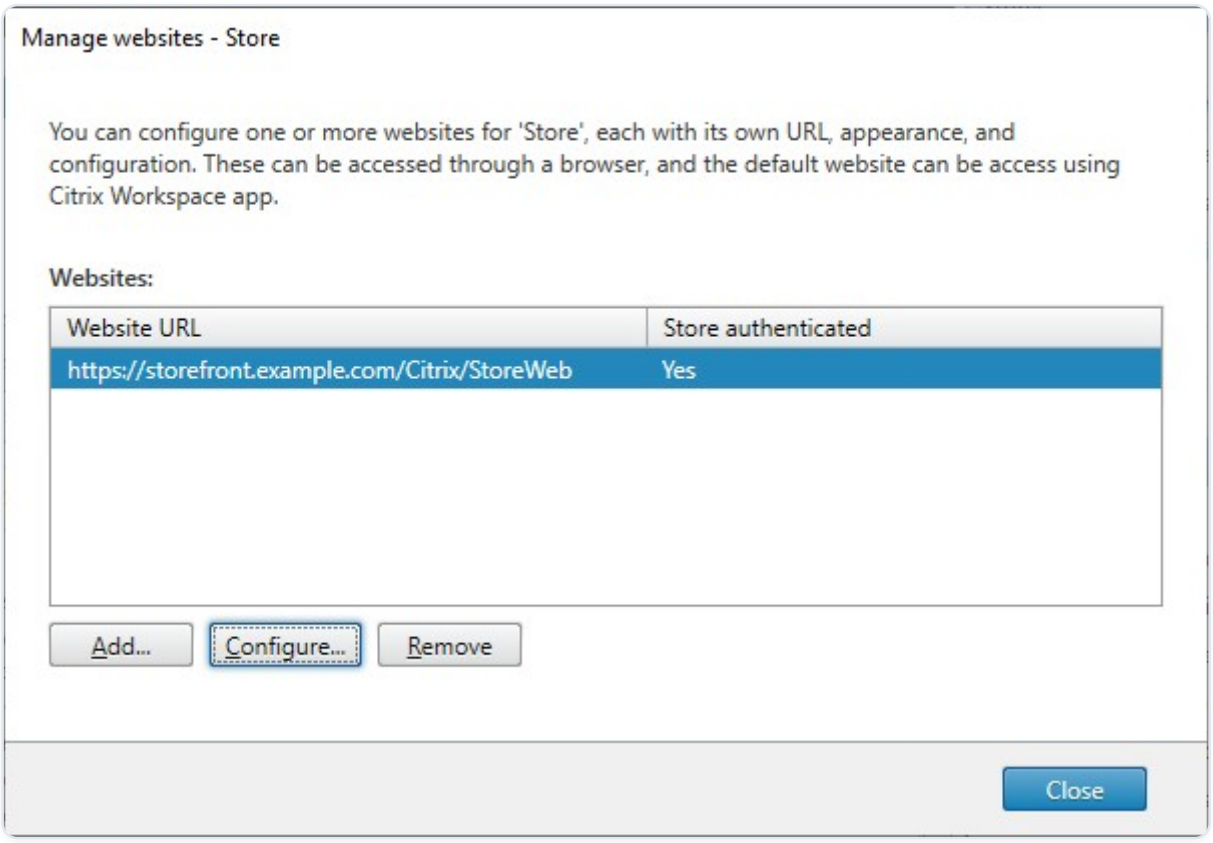
> 重要提示：

> 在多服务器部署中，一次只能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， 将配置更改传播到服务器组 以便更新部署中的其他服务器。

查看网站

要查看应用商店的网站，请执行以下操作：

1. 在管理控制台中，选择左窗格中的“**应用商店**”节点。
2. 选择要配置的应用商店。
3. 在“**操作**”窗格中，选择“**管理网站**”。



在“**管理网站**”屏幕中，您可以执行以下操作：

操作	详细信息
(#create-a-website)	创建网站，使用户能够通过网页或 Workspace 应用程序访问应用商店。
(#configure-a-website)	修改网站设置。
删除网站	删除 Citrix Receiver™ for Web 站点。

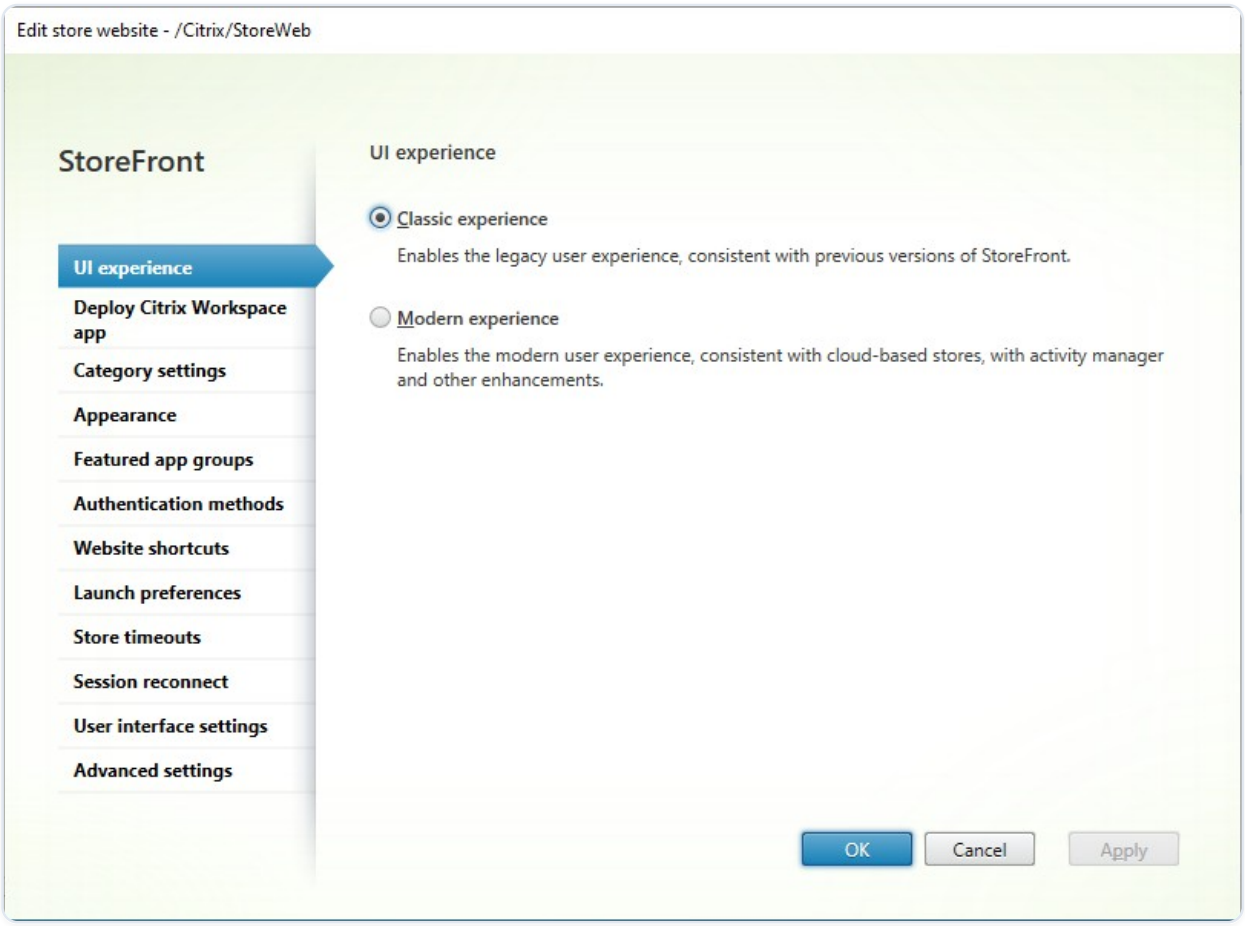
PowerShell

要获取网站列表，请使用 cmdlet Get-STFWebReceiverService。

配置网站

要配置网站：

1. 选择一个网站，然后按 **配置...**



2. 修改相应选项卡上的设置。

- UI 体验
- 部署 Citrix Receiver/Workspace 应用程序
- 类别设置
- 自定义外观
- 特色应用程序组
- 身份验证方法
- 网站快捷方式
- 启动首选项

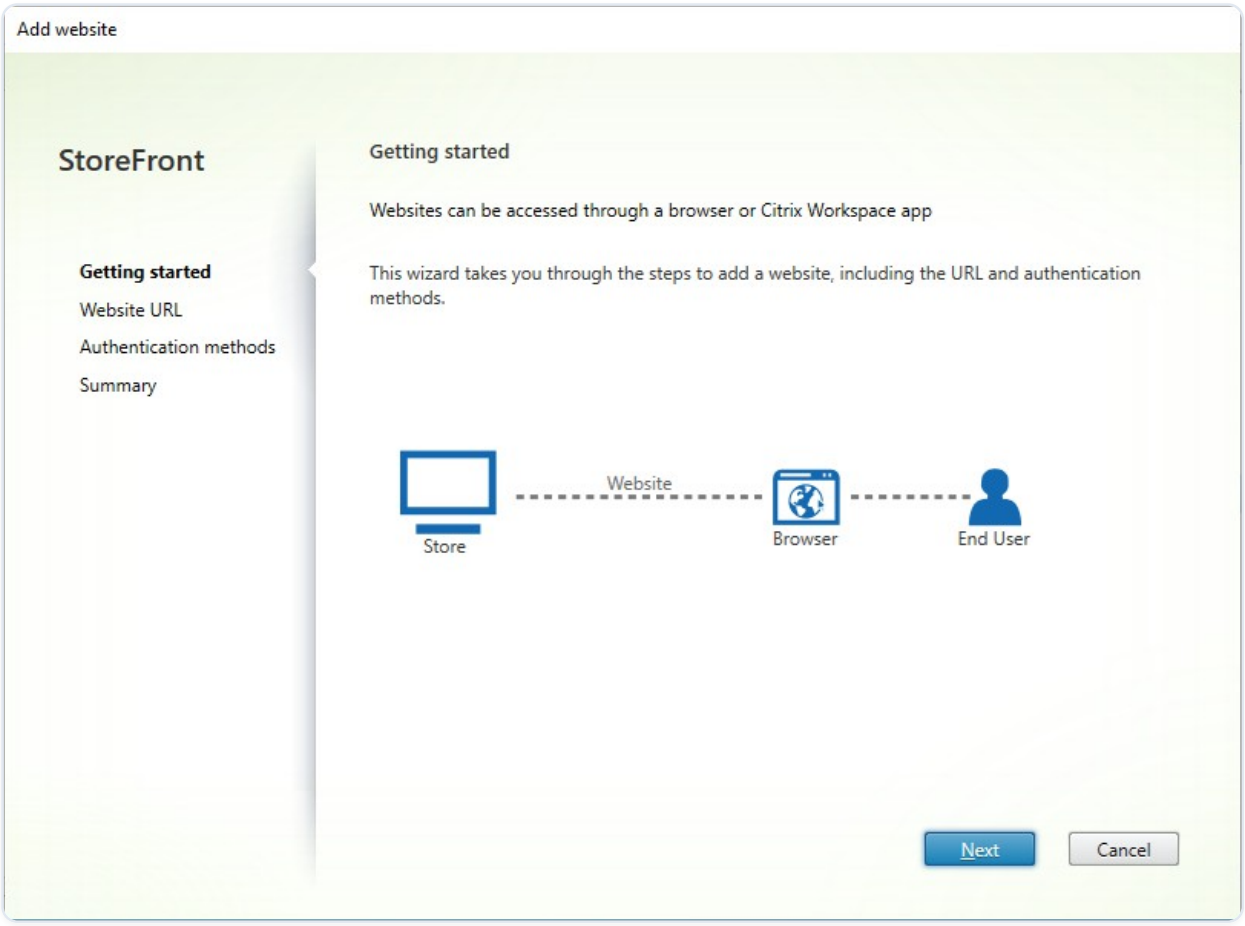
- 会话设置
- 工作区控制
- 客户端界面设置
- 固定链接
- 自定义公告
- 登录后对话框
- 高级设置

3. 完成更改后，单击 **确定**。
4. 要配置 应用程序保护，您必须使用 PowerShell。在运行 PowerShell 命令之前，请确保关闭 StoreFront 管理控制台。

创建网站

创建应用商店时，会自动为其创建一个网站。您可以向现有应用商店添加其他网站。这允许您为用户提供具有不同配置的不同 URL。但是，多个网站只能通过 Web 浏览器访问，因为 Citrix Workspace Apps 配置为对一个应用商店使用一个特定网站，请参阅 配置 Workspace 应用程序网站。

1. 选择 **添加...**。



2. 在 **入门** 选项卡上，选择 **下一步**。
3. 键入所需的 **网站路径**，选择是否希望将其作为基本 URL 的默认网站，然后选择 **下一步**。

   添加网站屏幕截图，网站 URL 选项卡(/en-us/storefront/2507-ltsr/media/stores/websites/add-site-url.png)
4. 勾选或取消勾选所需的身份验证方法。某些方法仅在为应用商店配置后才可用。按下**下一步**。

   添加网站屏幕截图，身份验证方法选项卡(/en-us/storefront/2507-ltsr/media/stores/websites/add-site-authentication.png)
5. 网站创建完成后，单击**完成**。
6. 选择新创建的网站，然后按下**编辑**以根据需要配置您的网站，请参阅配置网站。

PowerShell

要使用PowerShell创建网站，请运行 cmdlet `Add-STFWebReceiverService`。

删除网站

1. 在 Citrix StoreFront 管理控制台的左窗格中选择**应用商店**节点，选择要为其创建 Citrix Receiver for Web 站点的应用商店，然后在**操作**窗格中单击**管理网站**。

2. 选择一个站点，然后单击**删除**。删除站点后，用户将无法再使用该网页访问应用商店。

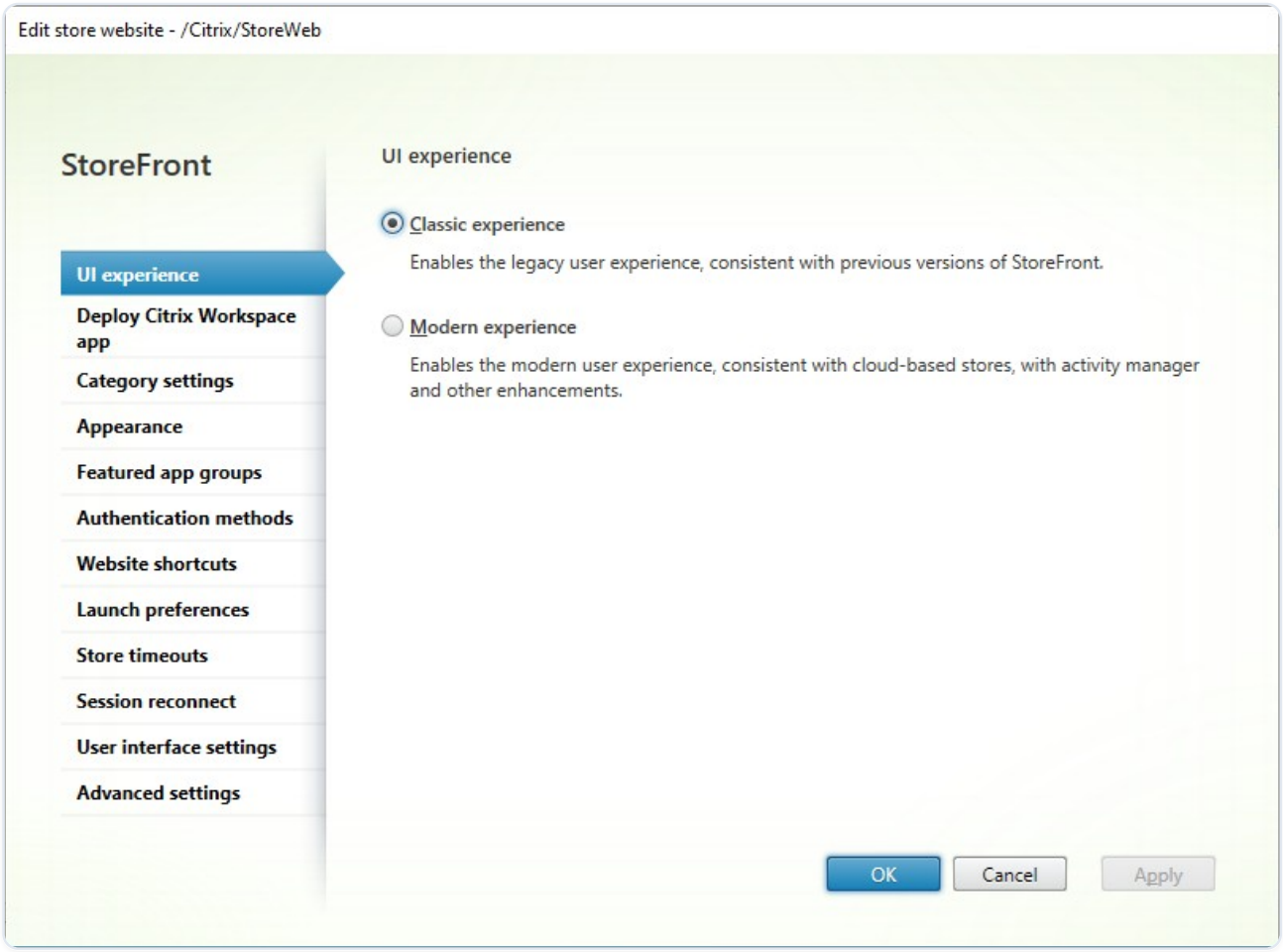
PowerShell

要使用PowerShell删除网站，请运行 cmdlet `Remove-STFWebReceiverService`。

UI 体验

在 UI 体验选项卡上，您可以为最终用户选择 UI 体验。您可以选择以下选项：

- **经典体验** - 有关详细信息，请参阅经典体验。
- **现代体验** - 有关详细信息，请参阅现代体验。



如果您使用 Citrix Gateway 进行远程访问，您可以选择一个主题来匹配所选体验。有关详细信息，请参阅 NetScaler 文档。

PowerShell

要使用 PowerShell 获取 UI 体验，请调用 cmdlet `Get-STFWebReceiverService` 并查看 `WebReceiver.WebUIExperience` 属性。

例如：

```
(Get-STFWebReceiverService -VirtualPath "/Citrix/
StoreWeb").WebReceiver.WebUIExperience
```

`WebUIExperience` 采用以下值：

- `ReceiverForWeb` - 经典体验
- `Workspace` - 现代体验

要使用 PowerShell 更改 UI 体验，请调用 cmdlet `Set-STFWebReceiverService` 并使用参数 `WebUIExperience`。

例如，要使用经典体验：

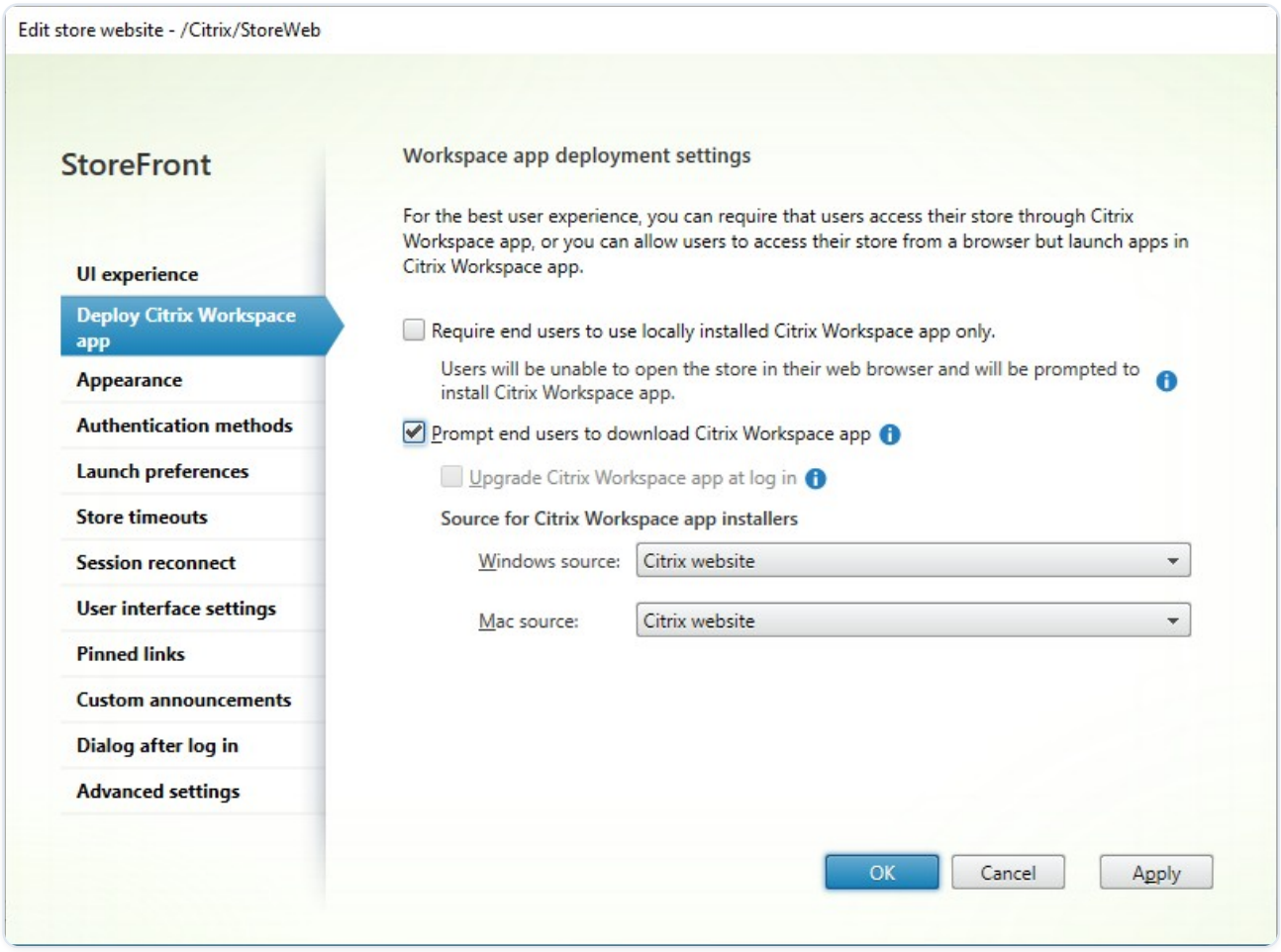
```
$rfw=Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"

Set-STFWebReceiverService -WebReceiverService $rfw -WebUIExperience
Workspace
```

Citrix Workspace 应用程序部署

默认情况下，当用户首次在 Windows、macOS 或 Linux 上的 Web 浏览器中打开应用商店时，StoreFront 会尝试确定是否已在本地安装 Citrix Workspace 应用程序。如果无法检测到本地部署的 Citrix Workspace 应用程序，系统会提示用户下载并安装它。默认下载位置是 Citrix 网站，但您也可以将安装程序托管在 StoreFront 服务器或其他位置。安装后，用户可以打开本地安装的 Citrix Workspace 应用程序并将其连接到应用商店，或者继续在浏览器中操作，但连接到本地安装的 Citrix Workspace 应用程序 HDX 客户端中的虚拟应用程序和桌面。

另外，无法在本地安装 Citrix Workspace 应用程序的用户可以使用 Web 浏览器访问应用商店并连接到虚拟应用程序和桌面。



要修改部署选项，请转到 编辑应用商店网站 并选择“**部署 Citrix Workspace 应用程序**”选项卡。

要求使用 Citrix Workspace™ 应用程序

管理员可以强制使用本机 Citrix Workspace 应用程序，从而消除用户使用 Web 浏览器连接到应用商店的选项。此功能专为希望充分利用 Citrix Workspace 应用程序优势的客户而设计。Citrix Workspace 应用程序具有内置的应用程序保护服务、避免浏览器版本兼容性问题、增强的安全性和用于监视和故障排除的遥测等优势。有关详细信息，请参阅 用户访问选项。

使用现代体验时，可以在管理控制台中启用此功能。使用经典体验或 Citrix Gateway 时，可以通过插件获得此功能。

支持的平台

自动配置 Citrix Workspace 应用程序需要以下版本。

- 适用于 Windows 的 Citrix Workspace 应用程序 24.9.0 或更高版本
- 适用于 Mac 的 Citrix Workspace 应用程序 24.5.0 或更高版本
- 适用于 Android 的 Citrix Workspace 应用程序 24.9.0 或更高版本
- {适用于 iOS 的 Citrix Workspace 应用程序 24.9.0 或更高版本

使用现代体验在 StoreFront 上进行配置

管理员可以按照以下步骤要求在连接到 StoreFront 的用户设备上使用 Citrix Workspace 应用程序：

1. 在左侧窗格中选择“**存储**”节点，然后在“**操作**”窗格中单击“**管理网站**”。
2. 单击“**配置**”>“**部署 Citrix Workspace 应用程序**”。

   本机应用程序强制(/en-us/storefront/2507-ltsr/media/stores/websites/native-app-mandate-config.png)
3. 选择选项“**要求最终用户仅使用本地安装的 Citrix Workspace 应用程序**”。
4. 单击“**确定**”。

使用经典体验进行配置

1. 从 Citrix 下载 下载插件。
2. 将 zip 文件和 citrix-ui-plugin.tar.gz 解压到 StoreFront 服务器上的任意目录。它包含 PowerShell 文件、Javascript 文件和配置文件。
3. 在文本编辑器中打开 plugin.config 文件。按如下方式配置：

   如果要启用本机应用程序强制功能，请保留如下键值对：`<param name="requireNativeAppUse" value="true" />`

   如果要禁用本机应用程序强制功能，请保留如下键值对：`<param name="requireNativeAppUse" value="false" />`
4. 以管理员身份打开 PowerShell。
5. 导航到解压后的文件夹。
6. 运行 `./CitrixPluginInstaller.ps1 -VirtualPath /Citrix/<store web name>`。
7. 对 StoreFront 服务器组中的每个服务器重复此操作。
8. 通过打开 Web 浏览器并导航到应用商店网站来验证其是否已正确安装。

使用 Citrix Gateway 进行配置

如果用户通过 Citrix Gateway 访问其应用商店，则可以在网关上安装一个插件，以要求使用 Citrix Workspace 应用程序。有关详细信息，请参阅通过网关要求使用 Citrix Workspace 应用程序。

用户体验

有关此功能的最终用户体验的详细信息，请参阅最终用户体验。

允许用户下载 Citrix Workspace 应用程序

> **注意：**
>
> 如果您未要求用户在 Citrix Workspace 应用程序中打开应用商店，并且已将启动首选项配置为始终在 Web 浏览器中打开资源，则这些设置不适用。

> 如果您选择**允许用户下载 Citrix Workspace 应用程序**，则用户首次登录 Windows 或 Mac 设备时，系统会提供下载该应用程序的选项。

登录时升级 Workspace 应用程序

如果您选择**登录时升级 Citrix Workspace 应用程序**，则用户登录时会收到升级本地安装的 Citrix Workspace 应用程序客户端的选项。用户可以选择跳过升级，除非清除其浏览器 Cookie，否则不会再次提示升级。要启用此功能，请确保 Citrix Workspace 应用程序文件在 StoreFront 服务器上可用。

下载源

当最终用户单击下载按钮时，您可以选择是将其重定向到 Citrix 网站，还是直接从服务器下载文件。您可以选择**Citrix 网站**、**StoreFront 服务器上的本地文件**或**远程服务器上的文件（通过 URL）**。

PowerShell

要使用 PowerShell 配置这些设置，请运行 cmdlet Set-STFWebReceiverPluginAssistant。

渐进式 Web 应用程序（预览版）

如果用户无法安装 Citrix Workspace 应用程序，渐进式 Web 应用程序 (PWA) 功能允许您安装应用商店网站，以便可以从“开始”菜单或桌面启动它，类似于本机应用程序。此功能仅在经典体验中可用。

先决条件

要将 Web 客户端用作渐进式 Web 应用程序，请确保满足以下条件：

- 用户必须通过 HTTPS 访问 StoreFront。
- 启动选项必须设置为**始终使用 Receiver for HTML5**。
- 在 Windows、Mac 或 Linux 上使用 Google Chrome 或 Microsoft Edge 浏览器。
- 此功能默认关闭，必须(#enable-progressive-web-app)。

已知限制

- 在 StoreFront 部署上设置单选项卡模式时，它不适用于 PWA 启动。

- 不支持会话共享应用程序启动期间的混合场景。例如，从 PWA 启动应用程序，然后尝试在浏览器中启动会话共享应用程序将不起作用。
- 从 PWA 会话窗口切换到浏览器窗口不起作用。

启用渐进式 Web 应用程序

此功能默认禁用。管理员可以按如下方式启用此功能：

1. 在“**编辑应用商店网站**”窗口中，转到“启动首选项”选项卡，并将(/zh-cn/storefront/2507-ltsr/stores/websites/launch-preferences.html#launch-option)设置为“**在 Web 浏览器中打开**”。
2. 保存设置并关闭管理控制台。
3. 运行 PowerShell 命令 Set-STFWebReceiverUserInterface

```
$receiver = Get-STFWebReceiverService

Set-STFWebReceiverUserInterface -WebReceiverService $receiver
-ProgressiveWebAppEnabled $true
```

用户体验

有关用户如何安装应用程序的更多信息，请参阅(/zh-cn/storefront/2507-ltsr/end-user-experience/classic-experience.html#installing-as-a-progressive-web-app-preview)。

类别设置

> **注意：**
>
> 此功能仅在使用经典体验时可用。

> 在 Citrix Virtual Apps and Desktops 中，您可以按照应用程序一文中的说明，将每个应用程序分配到一个类别。使用 `\` 符号创建类别的文件夹层次结构。在 StoreFront 中，您可以配置此文件夹层次结构的显示方式。

Studio 中应用程序属性的屏幕截图(/en-us/storefront/2507-ltsr/media/stores/websites/category-settings-studio-configuration.png)

要修改类别设置，请转到编辑应用商店网站并选择**类别设置**选项卡。

类别设置屏幕的屏幕截图(/en-us/storefront/2507-ltsr/media/stores/websites/category-settings.png)

类别视图

在展开视图中，StoreFront 显示顶级类别列表。当用户单击顶级类别时，StoreFront 会在一个页面上显示所有子类别中的所有应用程序。

例如，如果您有一个类别“浏览器”及其子类别“旧版”，则它会在一个页面上显示所有浏览器，包括“旧版”下的浏览器：

类别设置屏幕的屏幕截图(/en-us/storefront/2507-ltsr/media/stores/websites/category-settings-expanded.png)

在折叠视图中，StoreFront 最初会显示顶级类别列表，并可选择显示所有未分类的应用程序。当用户单击某个类别时，StoreFront 仅显示所选类别的直接内容（子类别和应用程序）。用户可以单击每个子类别以展开其内容。

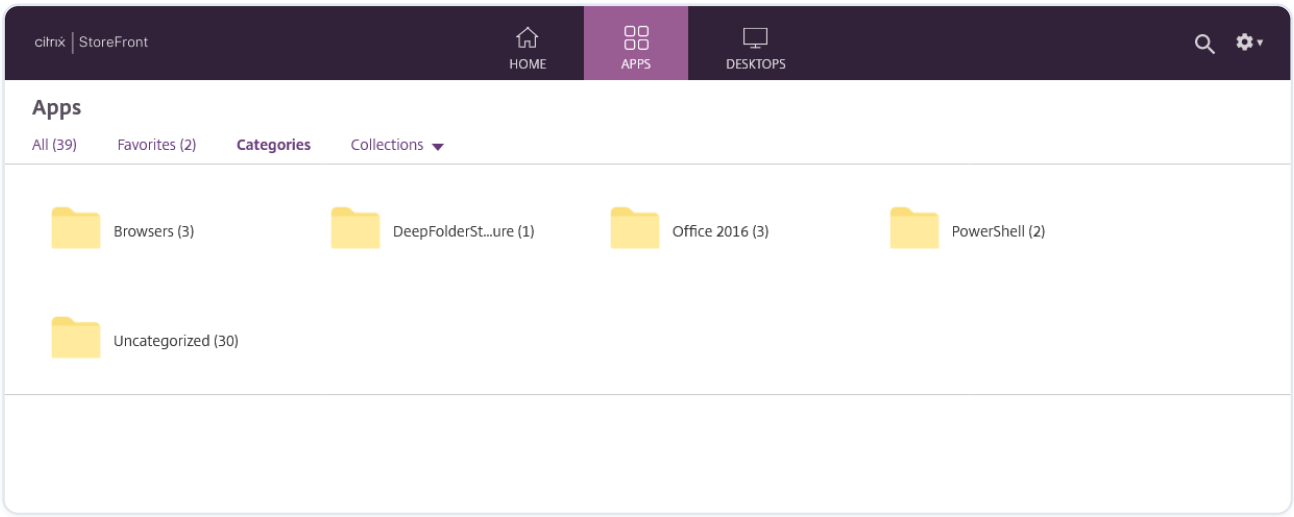
类别设置屏幕的屏幕截图(/en-us/storefront/2507-ltsr/media/stores/websites/category-settings-collapsed.png)

未分类的应用程序

在折叠视图中，清除**将未分类的应用程序移动到“未分类”文件夹中**选项，以在初始视图中显示所有未分类的应用程序和桌面。此行为与早期版本的 StoreFront 类似。

类别设置屏幕的屏幕截图(/en-us/storefront/2507-ltsr/media/stores/websites/category-settings-uncategorised.png)

在折叠视图中，选中**将未分类的应用程序移动到“未分类”文件夹中**，以将所有未分类的应用程序和桌面移动到单独的**未分类**文件夹中。



隐藏类别视图

要隐藏**类别**视图，请在“高级设置”选项卡上，清除启用文件夹视图。

配置类别设置 PowerShell

要使用 PowerShell 启用或禁用类别视图，请使用参数 `EnableAppsFolderView` 调用 cmdlet Set-STFWebReceiverUserInterface。

要使用 PowerShell 更改类别视图，请使用参数 `CategoryViewCollapsed` 调用 cmdlet Set-STFWebReceiverUserInterface。

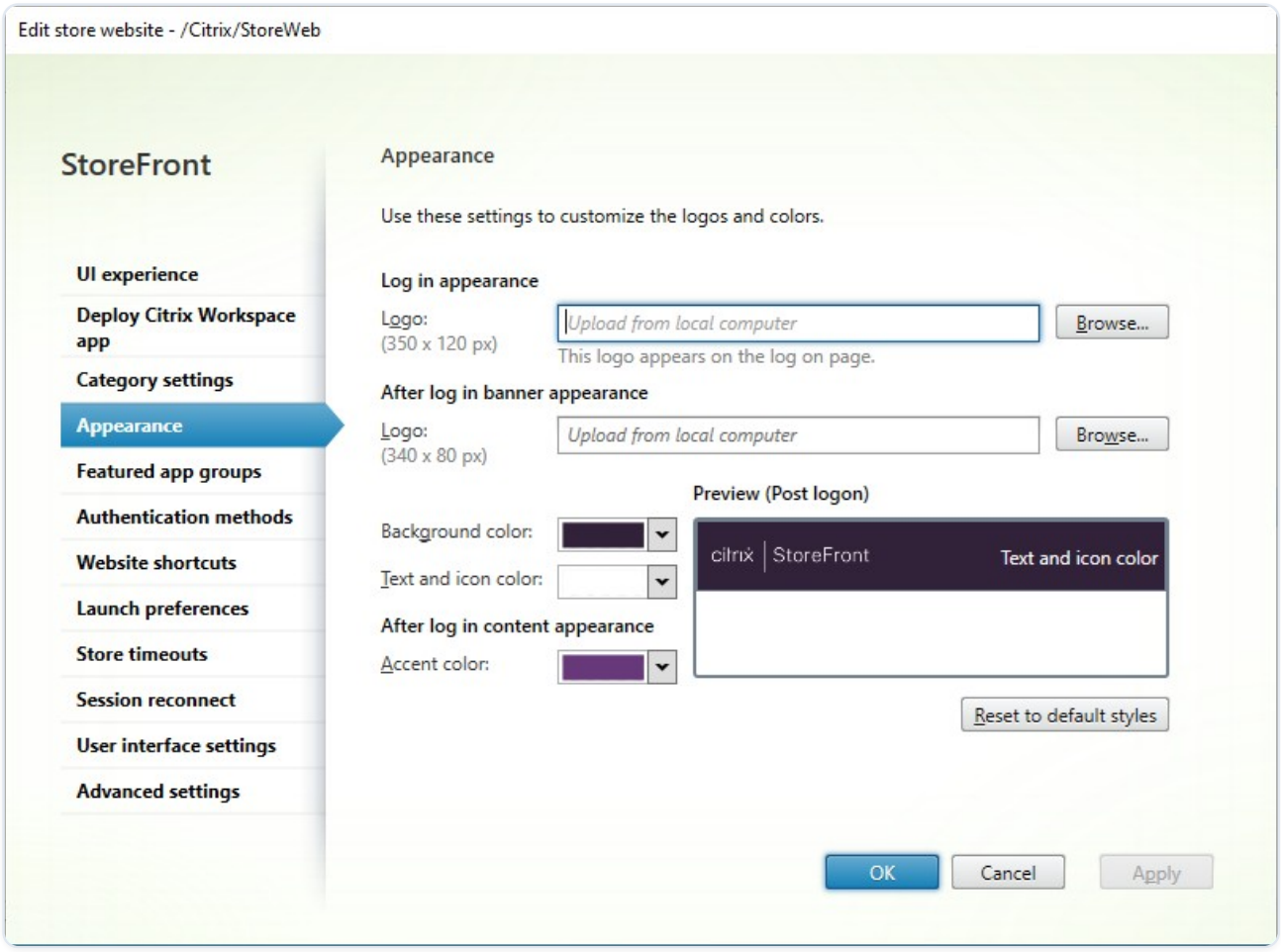
外观

您可以修改商店网站中使用的徽标和颜色。

编辑徽标和颜色

要自定义外观，请转到编辑商店网站并选择**自定义外观**选项卡。您可以修改以下内容：

- **登录品牌徽标** - 在登录屏幕上显示的徽标。通过 Citrix Gateway 或使用 Citrix Workspace 应用程序登录时不会显示。按**浏览...**并选择 .jpg、.jpeg、.png、.gif 或 .bmp 类型的文件。建议您使用大小为 350px x 120px 的图像。
- **标题品牌徽标**。登录后显示在左上角的徽标。按**浏览...**并选择 .jpg、.jpeg、.png、.gif 或 .bmp 类型的文件。建议您使用大小为 340px x 80px 的图像。
- **背景颜色** - 页面顶部导航部分的背景颜色。
- **文本和图标颜色** - 页面顶部导航部分中图标的颜色。
- **强调色** - 用于指示哪个项目具有焦点以及用于按钮和链接的颜色。



默认设置因您使用的是经典体验还是现代体验而异，但任何自定义设置都适用于两者。

使用 PowerShell 编辑徽标和颜色

使用 PowerShell，运行 cmdlet Set-STFWebReceiverSiteStyle。

将外观重置为默认值

按**重置为默认样式**可将徽标和颜色恢复为默认值。

使用 PowerShell 将外观重置为默认值

使用 PowerShell，运行 cmdlet Clear-STFWebReceiverSiteStyle。

使用 Javascript 和 CSS 进行自定义

使用经典体验时，您可以使用 StoreFront Client UI Customization API 进一步自定义网站。这不适用于现代体验。

精选应用组

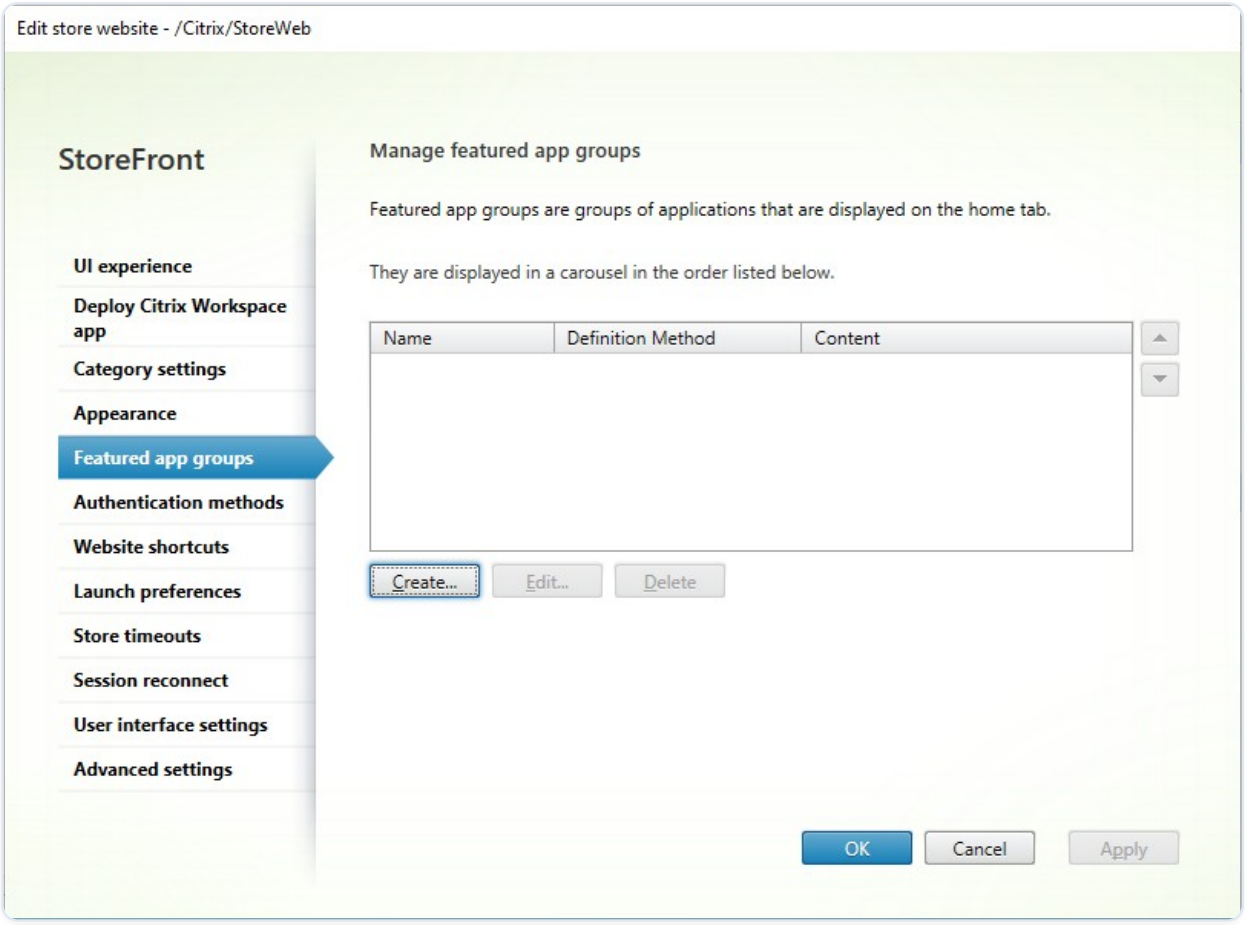
> **注意：**

> 此功能仅在使用统一体验时可用。

> 您可以为最终用户创建与特定类别相关或符合特定类别的产品精选应用组。例如，您可以创建一个包含该部门使用的应用程序的销售部门精选应用组。您可以通过使用应用程序名称或使用在 Studio 控制台中定义的关键字或应用程序类别，在 StoreFront 管理控制台中定义精选应用程序。

创建精选应用组

1. 在编辑商店网站屏幕中，选择**精选应用组**选项卡。



2. 单击**创建**以定义新的精选应用组。
3. 指定精选应用组名称、描述（可选）、背景以及定义精选应用组的方法。您可以选择关键字、应用程序名称或应用程序类别。

选项	描述
关键字	根据关键字匹配应用程序，在 Studio 中通过在应用程序描述中包含关键字来定义，例

选项	描述
	如“用于发送和接收电子邮件 KEYWORDS:collaboration”
应用程序类别	匹配在 Studio 中输入的特定应用程序类别中的应用程序。
应用程序名称	使用应用程序名称定义精选应用组。在“创建精选应用组”对话框屏幕中与此处包含的名称匹配的所有应用程序名称都将包含在精选应用组中。StoreFront 不支持应用程序名称中的通配符。匹配不区分大小写，但匹配整个单词。例如，如果您键入 Excel，StoreFront 将匹配名为 Microsoft Excel 2013 的已发布应用程序，但键入 `Exc` 不会匹配任何内容。

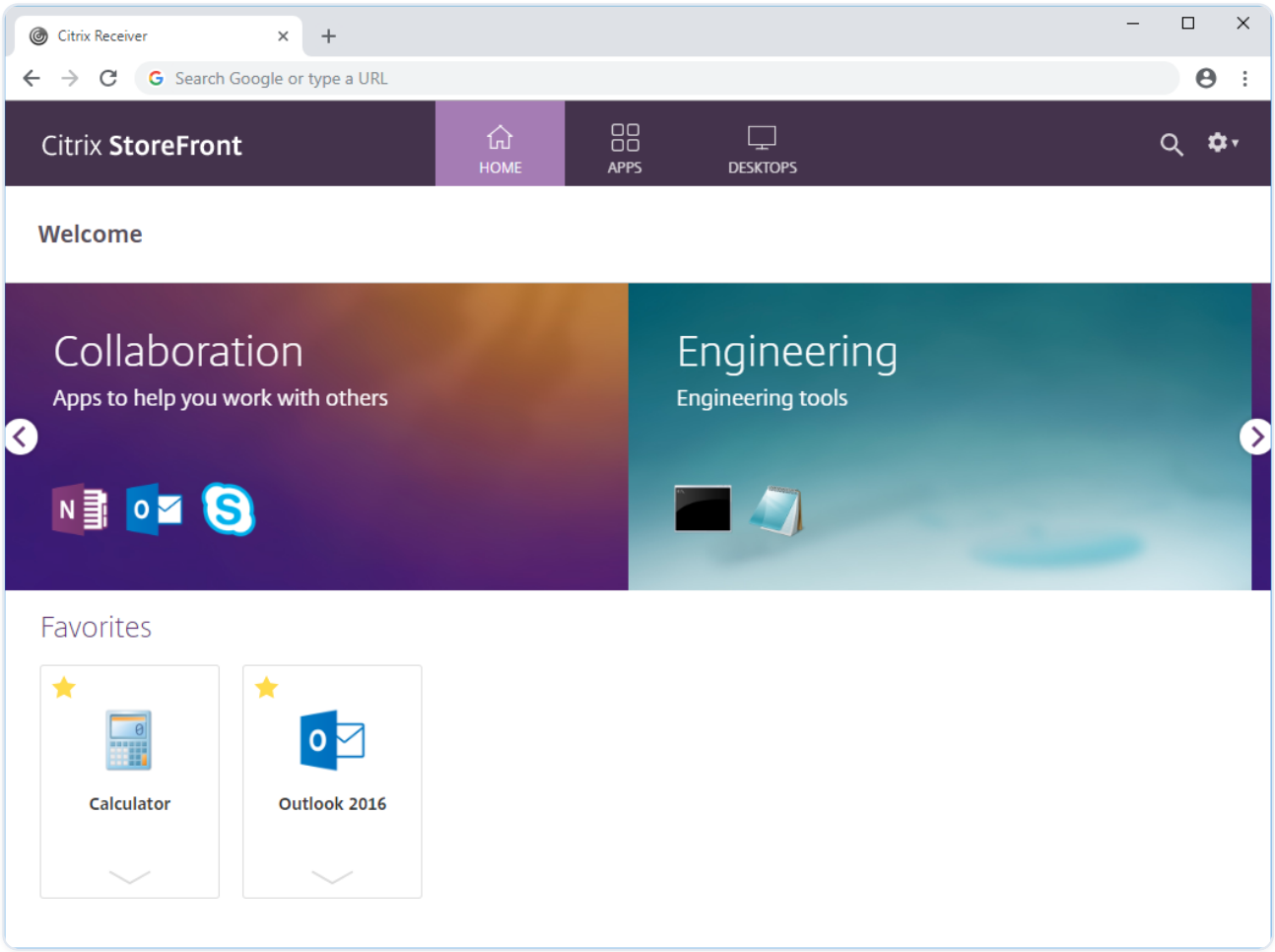
创建特色应用组屏幕截图(/en-us/storefront/2507-ltsr/media/stores/websites/featured-app-groups-create.png)

4. 单击“**确定**”

示例：

我们创建了两个特色应用组：

- 协作 - 通过匹配 Studio 中“**协作**”类别中的应用创建。
- 工程 - 通过命名应用组并指定应用名称集合创建。



使用 PowerShell 创建特色应用组

要使用 PowerShell 添加特色应用组，请运行 cmdlet New-STFWebReceiverFeaturedAppGroup。

编辑特色应用组

在 编辑应用商店网站 屏幕中，选择“**特色应用组**”选项卡。选择要编辑的组，然后单击“**编辑...**”.

使用 PowerShell 编辑特色应用组

要使用 PowerShell 修改特色应用组，请运行 cmdlet Set-STFWebReceiverFeaturedAppGroup。

删除特色应用组

在 编辑应用商店网站 屏幕中，选择“**特色应用组**”选项卡。选择要编辑的组，然后单击“**删除...**”.

使用 PowerShell 删除特色应用组

要使用 PowerShell 删除特色应用组，请使用 cmdlet Remove-STFWebReceiverFeaturedAppGroup；要删除所有特色应用组，请使用 cmdlet Clear-STFWebReceiverFeaturedAppGroup。

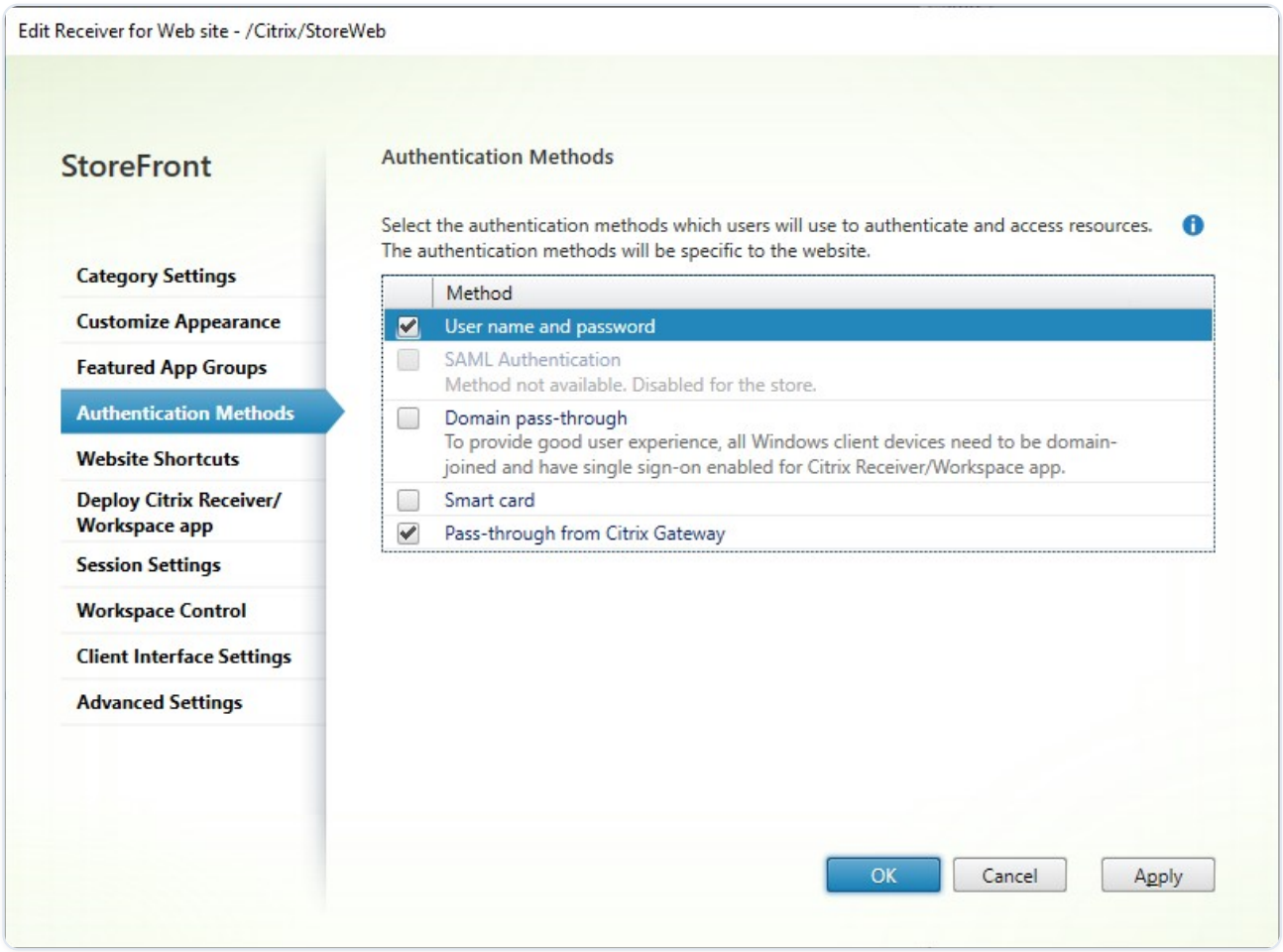
身份验证方法

要配置商店可用的身份验证方法，请参阅 配置身份验证。您可以为特定网站覆盖其中一些设置。这些覆盖仅在用户通过 Web 浏览器打开商店时适用。本地安装的 Citrix Workspace 应用程序使用商店的设置，而不是网站的设置。

警告：

每当您更改商店的身份验证方法时，这都会覆盖该商店所有网站的设置，因此必须重新应用任何更改。

要在使用 Web 浏览器时修改身份验证方法，请转到 编辑商店网站 并选择**身份验证方法**选项卡。



- 选中**Active Directory 用户名和密码**复选框，以允许所有用户通过输入其用户名和密码进行身份验证。请参阅 用户名和密码身份验证。此选项仅在为商店启用时可用。
- 选中**SAML 身份验证**复选框以启用与 SAML 身份提供程序的集成。请参阅 SAML 身份验证。此选项仅在为商店启用时可用。

- 选择**域直通**以启用从用户设备直通 Active Directory 域凭据。请参阅 域直通身份验证。此选项仅在为商店启用时可用。
- 选择**智能卡**以启用智能卡身份验证。请参阅 智能卡身份验证。
- 选择**从 Citrix Gateway 直通**以启用从 Citrix Gateway 的直通身份验证。如果用户通过启用了身份验证的 Citrix Gateway 连接到 StoreFront，请启用此选项，以避免用户需要在 StoreFront 再次进行身份验证。请参阅 从 Citrix Gateway 直通。

如果您选择多种身份验证方法，则直接登录到 StoreFront™ 的用户的默认身份验证方法将根据以下优先级顺序确定：

1. 域直通
2. 智能卡
3. SAML
4. 用户名和密码

用户可以选择切换到不同的身份验证方法。一个例外是，如果您同时配置了 SAML 和用户名密码身份验证，则用户无法切换到用户名和密码身份验证。

当用户登出时，他们可以选择下次是否记住身份验证方法。

使用 PowerShell 进行配置

要使用 PowerShell 配置可用的身份验证方法，请运行 cmdlet Set-STFWebReceiverAuthenticationMethods。

网站快捷方式

> **注意：**

> 此功能仅在使用经典体验时可用。

> 使用网站快捷方式，为用户提供从内部网络上托管的受信任网站快速访问桌面和应用程序的途径。您可以为资源生成 URL，并将这些链接嵌入到您的网站上。用户单击链接后，将被重定向到应用商店网站，如果尚未登录，则在此处登录。网站会自动启动资源。

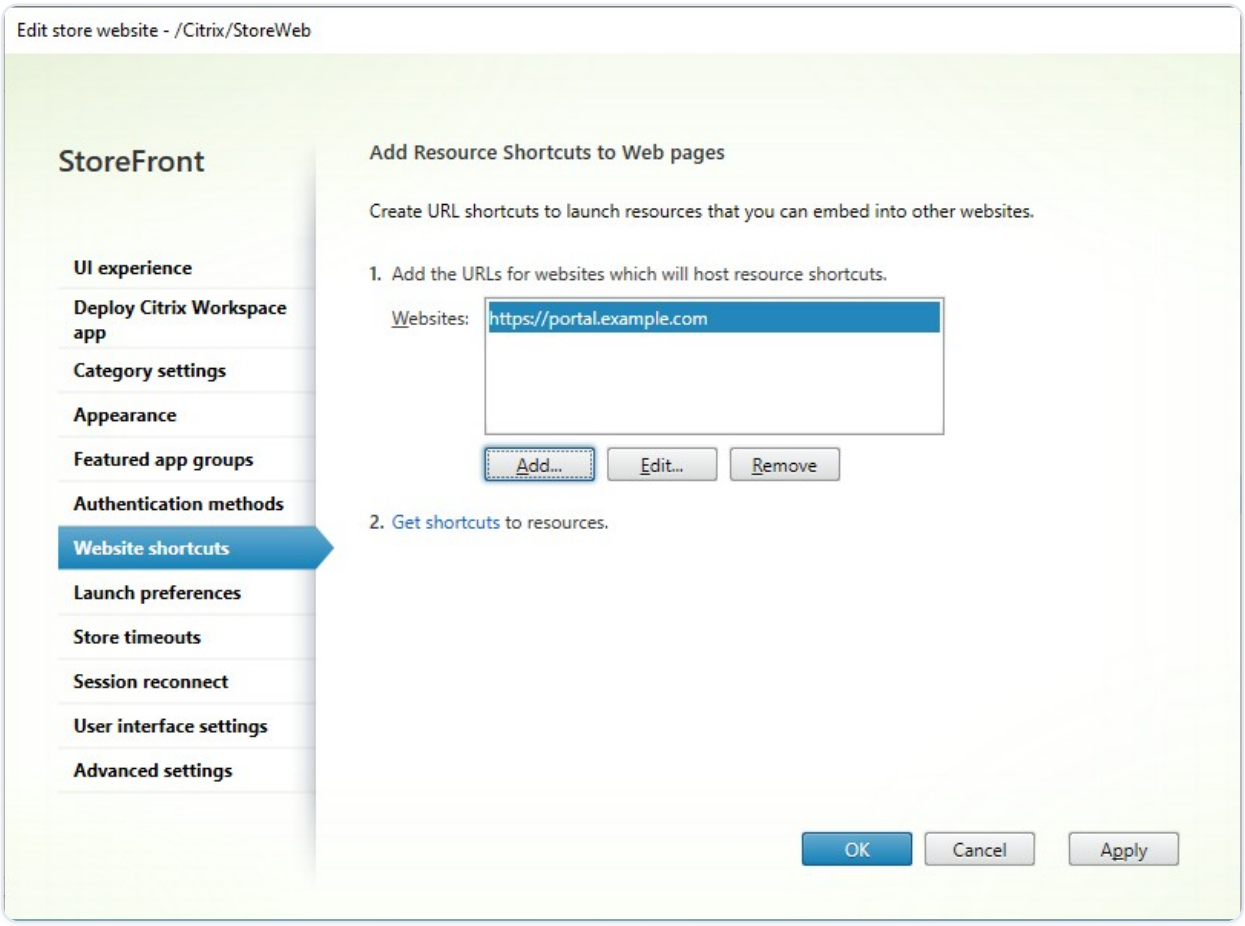
在生成资源快捷方式之前，必须使用 Citrix StoreFront 管理控制台或 PowerShell 将主机网站的 URL 添加到*受信任的 URL* 列表中。

默认情况下，如果用户尝试从不受信任的网站启动资源快捷方式，StoreFront 会发出警告，但用户仍然可以选择启动资源。要阻止这些警告出现，请在“高级设置”中，清除提示不受信任的快捷方式。

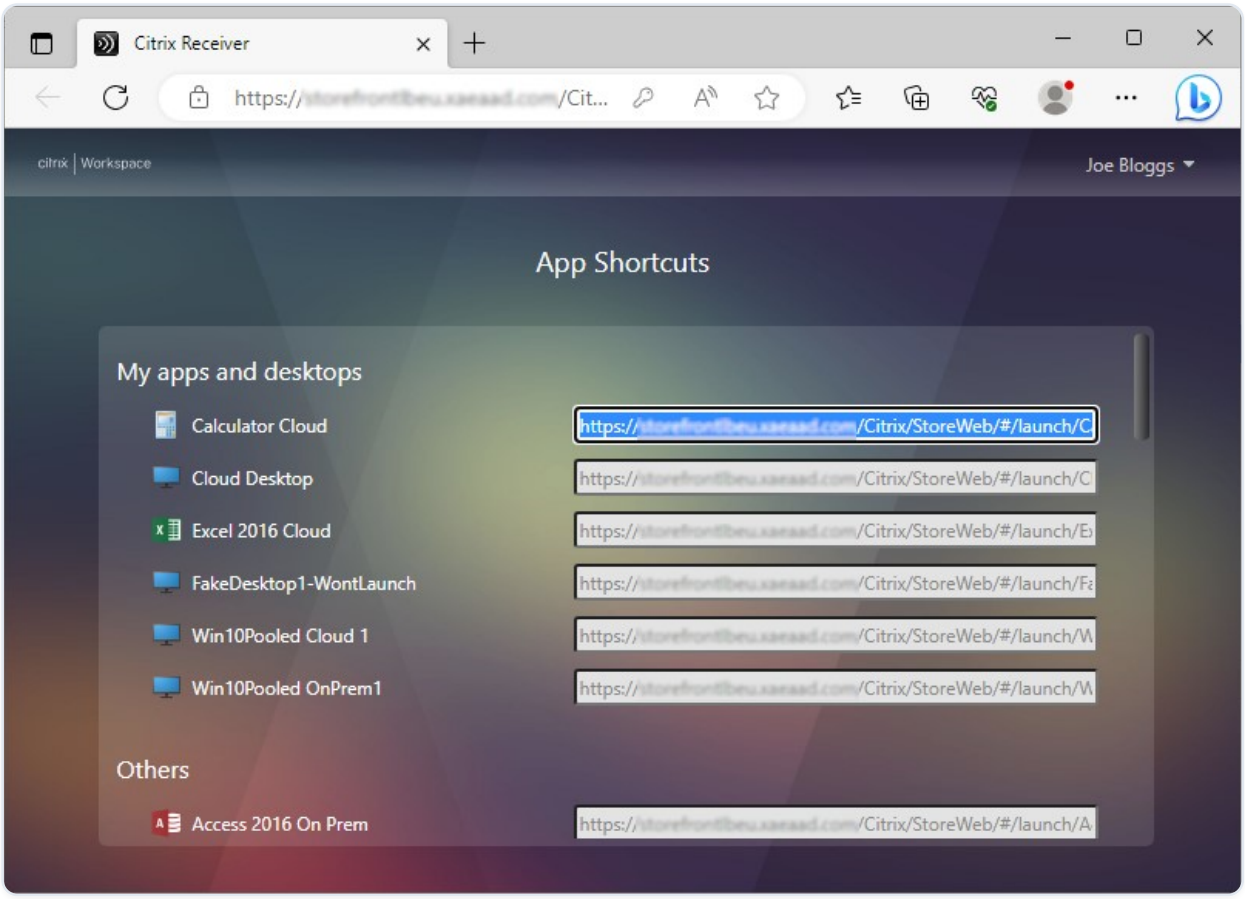
出于安全原因，Internet Explorer 用户可能会收到提示，要求确认他们是否要启动通过快捷方式访问的资源。请指导您的用户将 StoreFront 服务器 FQDN 添加到 Internet Explorer 的“本地 Intranet”或“受信任的站点”区域，以避免此额外步骤。

使用管理控制台添加受信任的网站

1. 在编辑应用商店网站屏幕上，选择**网站快捷方式**选项卡。



2. 单击**添加**以输入您计划托管快捷方式的网站 URL。URL 必须采用 *http\[s\]://hostname\[:port\]* 形式指定，其中主机名是网站主机的完全限定域名，端口是用于与主机通信的端口（如果协议的默认端口不可用）。不需要指定网站上特定页面的路径。要修改 URL，请在“网站”列表中选择该条目，然后单击**编辑**。在列表中选择一个条目，然后单击**删除**以删除您不再希望托管通过 Citrix Receiver for Web 站点提供的资源快捷方式的网站 URL。
3. 单击**获取快捷方式**并复制您的网站所需的 URL。

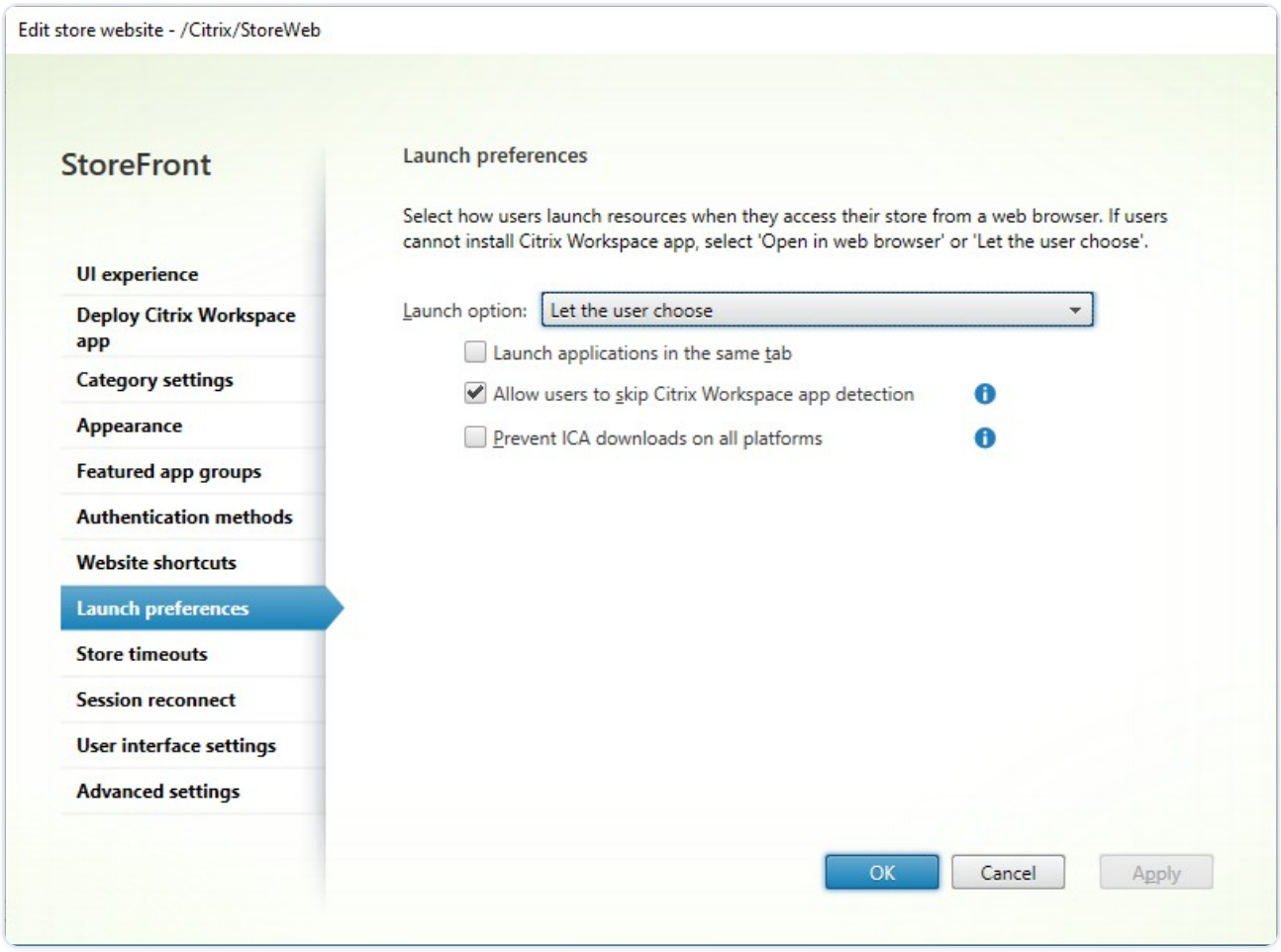


使用 PowerShell 添加受信任的网站

要使用 PowerShell 添加受信任的 URL，请运行 cmdlet Set-STFWebReceiverApplicationShortcuts 。

启动首选项

从**启动首选项**中，您可以选择用户在 Web 浏览器中打开其应用商店时可用的启动选项。这些设置在使用 Citrix Workspace 应用程序时不适用。有关启动选项的详细信息，请参阅用户访问选项。



要修改启动选项，请转至编辑应用商店网站并选择**启动首选项**选项卡。

启动选项

您可以选择以下选项之一：

- 选择**在 Web 浏览器中打开**，如果您希望用户始终通过 Web 浏览器访问资源，而无需提示用户在本地下载并安装 Citrix Workspace 应用程序。选择此选项后，HTML5 版 Workspace 用户始终直接通过其浏览器访问资源。
- 选择**让用户选择**，如果您希望应用商店网站提示用户在本地下载并安装 Citrix Workspace 应用程序，但如果无法安装 Citrix Workspace 应用程序，则回退到通过浏览器访问资源。没有 Citrix Workspace 应用程序的用户每次登录站点时都会收到下载并安装该应用程序的提示。
- 选择**在 Citrix Workspace 应用程序中打开**，如果您希望站点始终通过本地安装的 Citrix Workspace 应用程序访问资源。系统会提示用户下载并安装适用于其平台的相应 Citrix Workspace 应用程序。用户可以继续通过 Web 浏览器访问应用商店，但当他们启动资源时，资源会在本地安装的 Workspace 应用程序中打开。

在同一选项卡中启动应用程序

如果您选择了**在 Web 浏览器中打开**或**让用户选择**，默认情况下，在浏览器中启动的资源会在新的浏览器选项卡中打开。如果您希望资源在同一选项卡中打开（替换应用商店），请选择**在同一选项卡中启动应用程序**。

在现代体验中，此设置不可用，资源始终在新选项卡中打开。

允许用户跳过 Citrix Workspace™ 应用程序检测

当最终用户首次在浏览器中打开应用商店时，网站会尝试使用 Citrix Workspace 启动器检测本地安装的应用程序。随后，当用户启动资源时，Citrix Workspace 启动器会与本地安装的 Citrix Workspace 应用程序通信。如果用户选择**跳过检测**选项，则会跳过客户端检测过程。因此，当用户启动资源时，会下载一个 `.ica` 文件，用户可以使用本地安装的 Citrix Workspace 应用程序打开该文件。这不支持会话重新连接等功能。

下载的 `.ica` 文件可能存在安全风险。Citrix 建议您取消选择**允许用户跳过 Citrix Workspace 应用程序检测**。

阻止在所有平台上下载 ICA®

这通过完全阻止 `.ica` 在所有平台上的下载，提供了额外的保护级别。由于 Citrix Workspace 启动器在 ChromeOS 上不可用，ChromeOS 用户必须选择 **使用 Web 浏览器**（如果可用），或者他们必须将其应用商店添加到本地安装的 Citrix Workspace 应用程序中。

> **重要提示：**
>
> 如果同时选择了 **允许用户跳过 Citrix Workspace 应用程序检测**，则不应选择此选项。

Citrix Web 扩展

默认情况下，当用户首次使用 Web 浏览器登录时，或前往 **帐户设置** 并选择 **更改启动方法** 时，它会检查是否安装了 Citrix Web 扩展。如果找到，它会使用它来检测 Citrix Workspace 应用程序并启动虚拟应用程序和桌面。这通过避免浏览器提示和下载 ICA 文件，提供了最佳、最安全的体验。检测过程最长需要 6 秒（2 次尝试，每次超时 3 秒），以应对网页加载缓慢的情况，例如由于低带宽、低性能设备。因此，如果未检测到 Citrix Web 扩展，则首次使用的用户可能会遇到 6 秒的延迟。这不适用于使用现代体验或 Chrome 和 Edge 以外的 Web 浏览器的情况。您可以配置网站是否使用 Citrix Web 扩展以及它使用哪些超时设置。

要查看当前配置，请使用 PowerShell cmdlet Get-STFWebReceiverPluginAssistant。例如：

```
$receiver = Get-STFWebReceiverService "/Citrix/StoreWeb"

Get-STFWebReceiverPluginAssistant -WebReceiverService $receiver
```

要修改配置，请使用 cmdlet Set-STFWebReceiverPluginAssistant 和参数 `BrowserExtensionEnabled`、`BrowserExtensionTimeout` 和 `BrowserExtensionRetries`。例如，要禁用 Citrix Web 扩展：

```
$receiver = Get-STFWebReceiverService "/Citrix/StoreWeb"

Set-STFWebReceiverPluginAssistant -WebReceiverService $receiver
-BrowserExtensionEnabled $False
```

或者将超时时间缩短到 2 秒，只尝试一次：

```
$receiver = Get-STFWebReceiverService "/Citrix/StoreWeb"

Set-STFWebReceiverPluginAssistant -WebReceiverService $receiver
-BrowserExtensionTimeout 2000 -BrowserExtensionRetries 1
```

将超时时间从默认值缩短可能会导致网站无法检测到 Citrix Web 扩展。

PowerShell

要使用 PowerShell 配置这些设置，请运行 cmdlet Set-STFWebReceiverPluginAssistant。

要配置 阻止 ICA 下载，请运行 cmdlet Set-STFWebReceiverUserInterface 并使用参数 `PreventIcaDownloads`。

商店超时

要修改商店超时，请转到 编辑商店网站 屏幕，选择“**商店超时**”选项卡。

会话设置屏幕截图(/en-us/storefront/2507-ltsr/media/stores/websites/session-settings.png)

内部服务器通信尝试次数

StoreFront 内部 Web 代理和商店服务之间调用的尝试次数。通常无需修改此设置。

内部通信超时持续时间

StoreFront 内部 Web 代理和商店服务之间允许的调用时间量。通常无需修改此设置。

Web 浏览器不活动超时

通过 Web 浏览器访问 StoreFront 商店时，在指定的不活动期限后，会话将超时，用户将被注销。刷新网页或对资源执行操作会延长会话。不会导致网络活动的用户操作（例如在选项卡之间导航）不会延长会话。

超时在客户端和服务器上同时强制执行。会话到期前不久，UI 会提示用户延长会话。会话超时前一分钟，UI 会通知 StoreFront 以及（如果适用）Citrix Gateway 注销。这是为了允许客户端在服务器超时到期之前干净地注销。如果会话超时设置为 1 分钟，则客户端将在 30 秒后注销。这不影响本地安装的 Citrix Workspace 应用程序。

如果您修改会话超时使其大于 网关会话超时，则必须相应地增加网关会话超时。如果您修改会话超时使其大于 身份验证令牌生命周期 或 最大令牌生命周期，则这些值将自动增加以匹配会话超时。

PowerShell

要配置超时，请使用 cmdlet Set-STFWebReceiverService 和参数 `-SessionStateTimeout`。例如，要将网站“/Citrix/StoreWeb”的超时设置为 30 分钟：

```
$rfw = Get-STFWebReceiverService '/Citrix/StoreWeb'

Set-STFWebReceiverService $rfw -SessionStateTimeout 30
```

登录超时

在 Web 浏览器登录屏幕上，经过一段时间后，登录会超时并向用户显示一条消息。用户可以按“**登录**”返回登录屏幕。

身份验证令牌生命周期

当用户通过浏览器访问 StoreFront 商店时，默认情况下，无论是否有任何活动，用户都会在八小时后注销。这不影响本地安装的 Citrix Workspace 应用程序。该值不会显示在管理控制台中。

要查看当前值，请使用 Get-STFWebReceiverAuthenticationMethods 并检查 `TokenLifeTime` 属性。例如：

```
$rfweb=Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"

$rfauth = Get-STFWebReceiverAuthenticationMethods -WebReceiverService
$rfweb

$rfauth.TokenLifeTime.ToString()
```

要使用 PowerShell 设置超时，请使用 cmdlet Set-STFWebReceiverAuthenticationMethods 和参数 `TokenLifeTime`。例如：

```
$rfweb=Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"

$rfauth = Get-STFWebReceiverAuthenticationMethods -WebReceiverService
$rfweb

Set-STFWebReceiverAuthenticationMethods -WebReceiverService $rfweb
-TokenLifeTime "07:00:00"
```

如果将会话超时增加到 20 小时以上，则还必须增加 Authentication Service 的最大令牌生命周期。

思杰网关超时

有关网关超时的更多信息，请参阅 网关文档。

会话超时

如果在指定时间内没有网络活动，则会话超时将适用。刷新网页或对资源执行操作会延长会话。不会导致网络活动的用户操作（例如在选项卡之间导航）不会延长会话。

对于 Web 浏览器访问，您应该将 Citrix Gateway 的**会话超时**设置为略高于 StoreFront 的**会话超时**的值。这是为了确保当 StoreFront 会话超时并通知网关时，网关能够在自己的会话过期之前干净地注销。

本地安装的 Citrix Workspace 应用程序在连接到 StoreFront 商店时不会应用不活动超时。因此，网关是您需要应用不活动超时的唯一位置。该应用程序会定期刷新资源列表。为了使其生效，会话超时必须低于应用程序的刷新周期。默认情况下，应用程序的刷新周期为 60 分钟。要更改此设置，请参阅 CTX221465。

强制超时

在 Citrix Gateway 上，您可以设置**强制超时**，以在给定时间后断开会话，无论用户活动如何。

Authentication Service 的最大令牌生命周期

Authentication Service 颁发用于连接到商店的令牌。默认情况下，令牌在 20 小时后过期，这会导致用户注销。

如果用户通过 Citrix Gateway 进行身份验证，则当 StoreFront 令牌过期时，StoreFront 会向 Citrix Gateway 发出质询。如果网关的会话仍然处于活动状态，则它会提供凭据以重新登录 StoreFront。如果您希望阻止这种情况，则必须将网关的**强制超时**配置为与最大令牌生命周期相同。

通常，当在 Web 浏览器中使用商店时，不活动超时会导致会话在令牌过期之前注销，因此令牌生命周期主要与本地安装的 Citrix Workspace 应用程序相关。

要查看最大令牌生命周期，请运行以下 PowerShell：

```
$store = Get-STFStoreService -VirtualPath "[store path]"

$auth = Get-STFAuthenticationService -StoreService $store

$relyingParty = $auth.ProducerService.RelyingParties | Where-Object
{ $_.Id -eq $auth.ProducerService.Id }

$relyingParty.MaxLifetime.ToString()
```

将 `[store path]` 替换为适当的商店路径。

要配置最大令牌生命周期，请运行以下 PowerShell 命令：

```
$store = Get-STFStoreService -VirtualPath "[store path]"

$auth = Get-STFAuthenticationService -StoreService $store

$relyingParty = $auth.ProducerService.RelyingParties | Where-Object
{ $_.Id -eq $auth.ProducerService.Id }

$relyingParty.MaxLifetime = "[max lifetime]"

Save-STFService -Service $auth
```

将 `[store path]` 替换为适当的商店路径，并将 `[max lifetime]` 替换为所需的超时时间。对于不超过一天的值，请使用格式 `hh:mm:ss`。对于超过一天的值，请使用格式 `d.hh:mm:ss`。

会话重新连接

当用户在设备之间移动时，会话重新连接可确保他们正在使用的应用程序随之移动。用户可以在多个设备上继续使用相同的应用程序实例，而无需在每次登录新设备时重新启动所有应用程序。例如，这使医院的临床医生在从一个工作站移动到另一个工作站访问患者数据时可以节省时间。

当用户登录时，他们会自动重新连接到他们之前运行的任何应用程序。例如，假设用户登录到一个应用商店并启动了一些应用程序。如果用户随后使用相同的访问方法但在不同的设备上登录到同一个应用商店，则正在运行的应用程序会自动传输到新设备。当用户从特定应用商店注销时，用户从

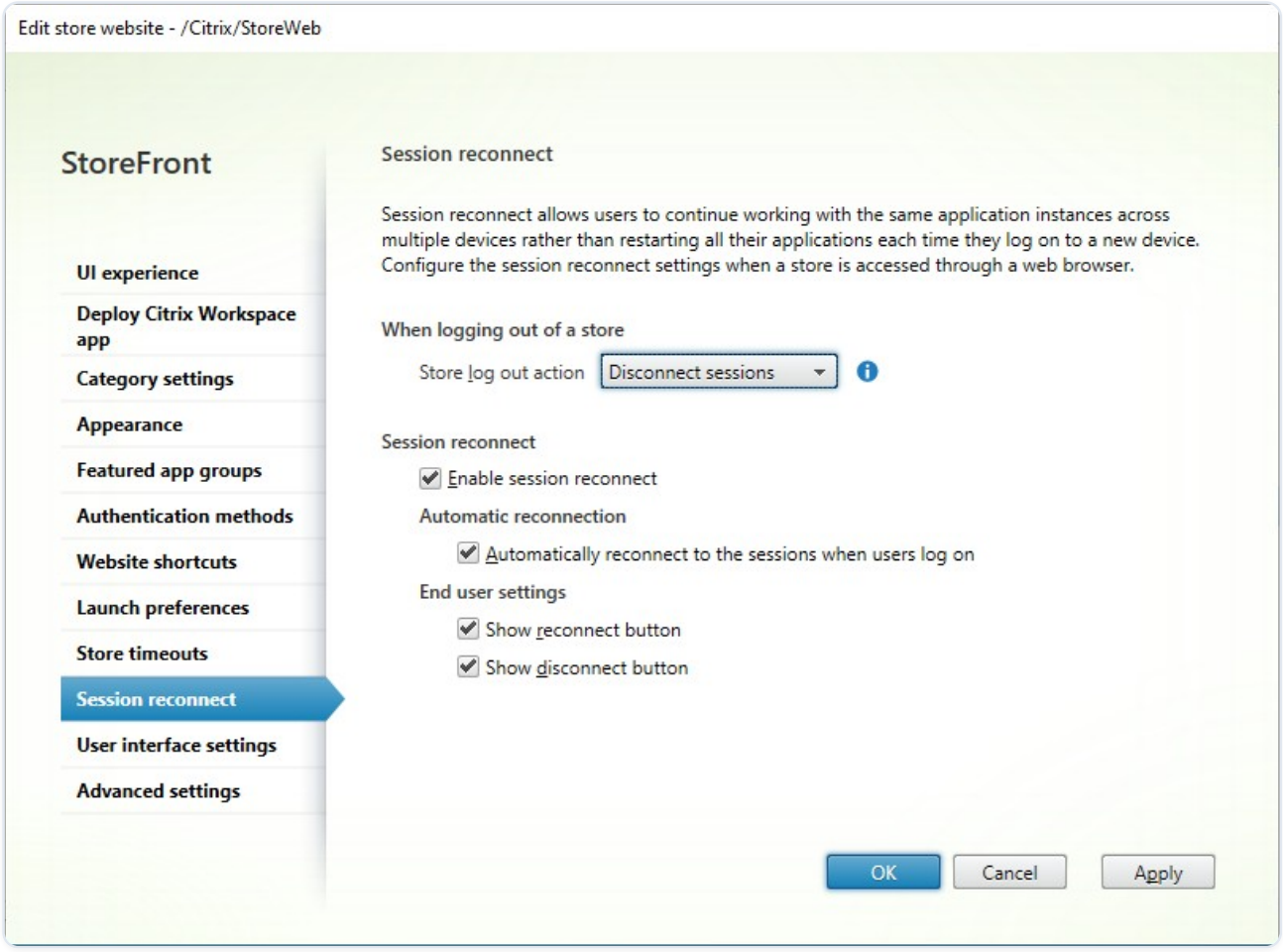
该应用商店启动的所有应用程序都会自动断开连接，但不会关闭。如果通过 Web 浏览器访问应用商店，则必须使用相同的浏览器登录、启动应用程序和注销。

在 Web 浏览器中配置会话重新连接

StoreFront 管理控制台中的会话重新连接设置仅在通过 Web 浏览器访问应用商店时适用。这受以下要求和限制的约束：

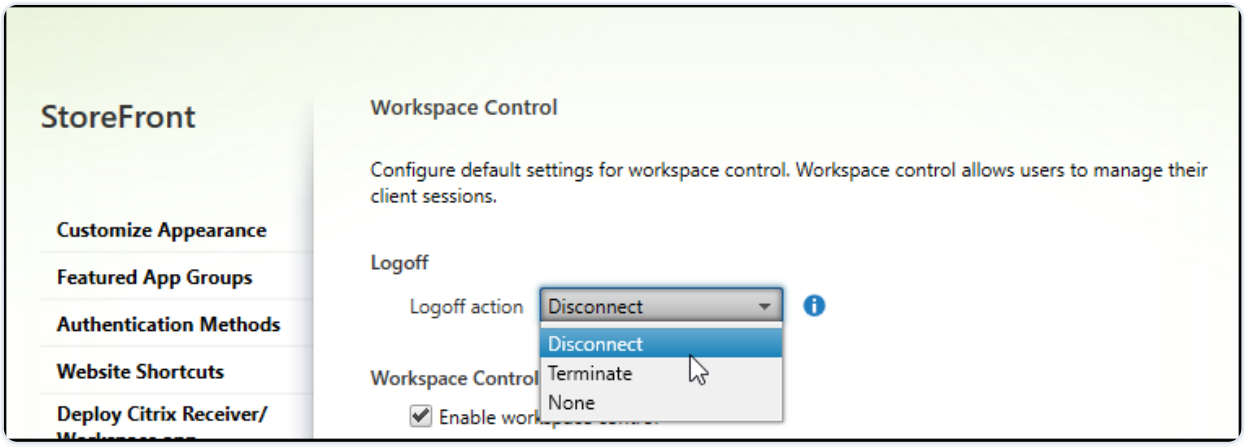
- 当 Web 浏览器在托管桌面或应用程序中运行时，会话重新连接不可用。
- 对于从 Windows 设备访问网站的用户，仅当站点可以检测到用户的设备上安装了适用于 Windows 的 Citrix Workspace 应用程序或资源通过 Web 浏览器打开时，才会启用会话重新连接。
- 要重新连接到已断开连接的应用程序，通过 Internet Explorer 访问网站的用户必须将该站点添加到“本地 Intranet”或“受信任站点”区域。
- 如果用户登录时，网站配置为自动启动单个桌面，并且用户只有一个桌面可用，则无论会话重新连接配置如何，该用户的应用程序都不会重新连接。
- 由于浏览器限制，Citrix Workspace 启动器 只能用于重新连接一个应用程序。要重新连接到多个应用程序，用户应安装 Citrix Web 扩展。
- 用户必须使用最初用于启动应用程序的同一浏览器断开与应用程序的连接。使用不同浏览器启动的资源，或使用 Citrix Workspace™ 应用程序从桌面或“开始”菜单本地启动的资源，无法从 Web 客户端断开连接或关闭。
- 当资源在同一浏览器选项卡中打开时，会话重新连接不可用。要配置此项，请参阅 Citrix Workspace 应用程序部署。

要在通过 Web 浏览器访问应用商店时修改会话重新连接设置，请在 编辑应用商店网站 屏幕上选择 **会话重新连接**。



按如下方式配置会话重新连接设置：

- 指定**注销操作**。注销操作如下：
  - **断开会话**：当您从网站注销时，应用程序和桌面会话会自动从客户端设备断开连接。
  - **注销会话**：当您从网站注销时，应用程序和桌面会话会自动在服务器上注销。
  - **无**：当您从网站注销时，应用程序和桌面会话将保持运行。



- **用户登录时自动重新连接会话** - 当用户登录时，所有断开连接的会话都会在本地设备上重新连接。

最终用户设置

使用经典体验时，您可以使用以下设置允许用户断开和重新连接会话：

- **显示重新连接按钮** - 显示一个**重新连接**按钮，用于重新连接当前设备上所有断开连接的会话。
- **显示断开连接按钮** - 显示一个**断开连接**按钮，用于重新连接当前设备上所有断开连接的会话。

这些设置对现代体验无效。请改用**活动管理器**来断开和重新连接会话。

使用 PowerShell 配置会话重新连接

要使用 PowerShell 配置会话重新连接，请运行 cmdlet Set-STFWebReceiverUserInterface。

在适用于 Windows 的 Workspace 应用程序上配置会话重新连接

要在适用于 Windows 的 Workspace 上配置会话重新连接，请参阅 管理工作区控制重新连接。

配置适用于 Mac 的 Workspace 应用程序上的会话重新连接

要配置适用于 Mac 的 Workspace 应用程序的会话重新连接，请参阅配置工作区控制设置。

禁用所有应用程序的会话重新连接

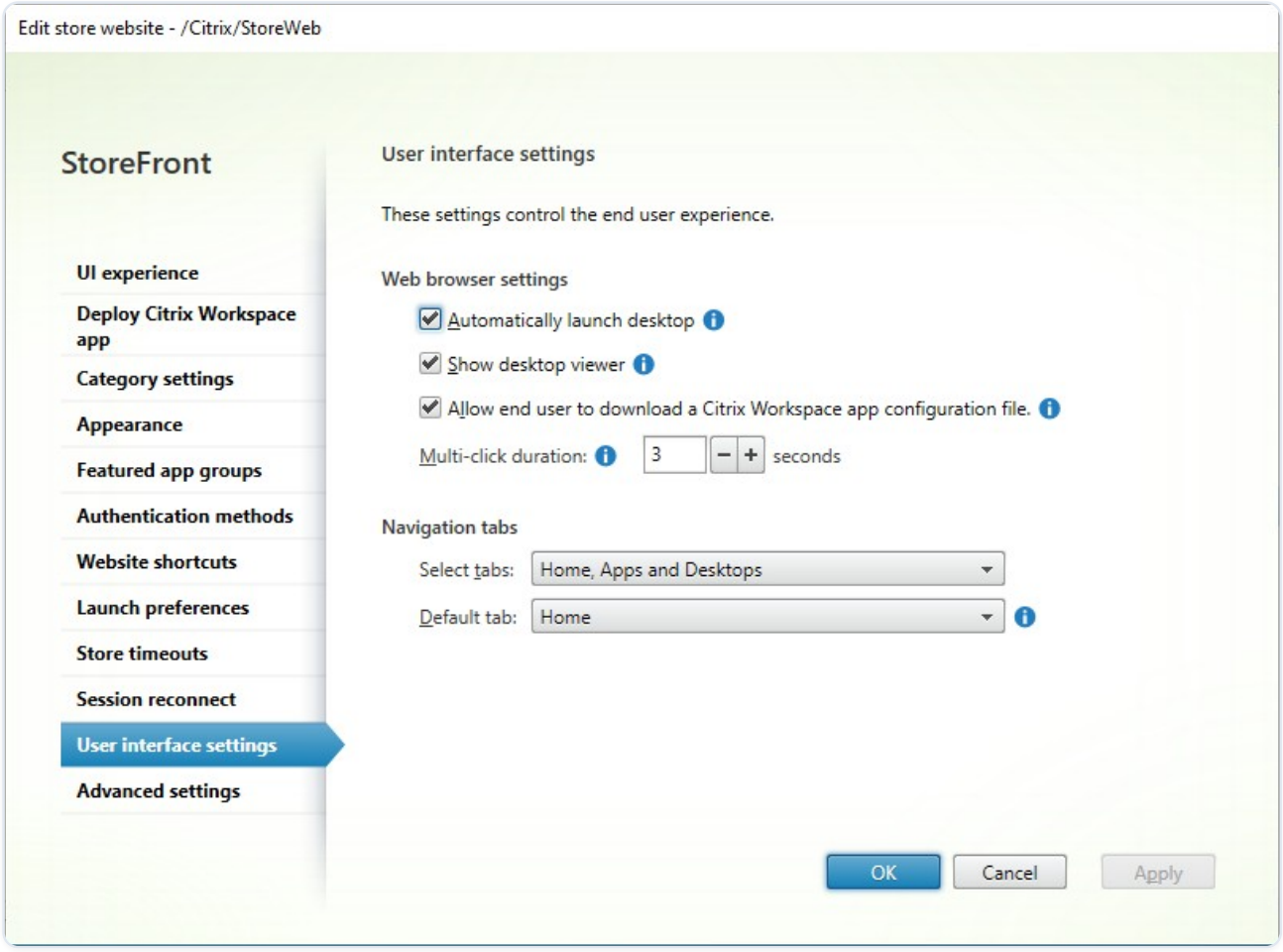
您可以在 StoreFront 中禁用所有 Workspace 应用程序的会话重新连接，无论它们如何配置。有关详细信息，请参阅允许会话重新连接。

用户界面设置

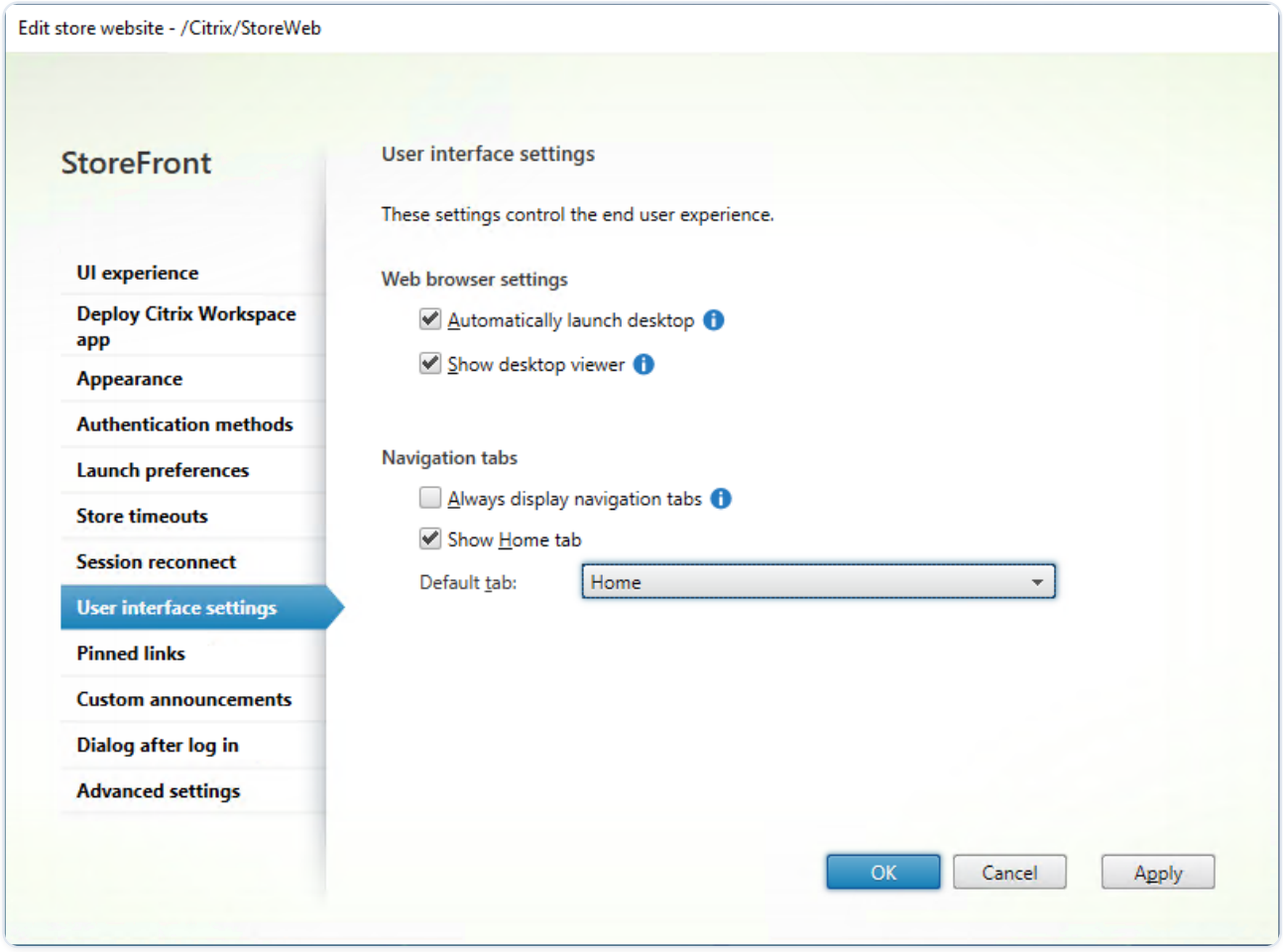
要修改用户界面设置，请打开 编辑商店网站 屏幕和 **用户界面设置** 选项卡。

可用的设置取决于选择了哪个 UI 体验。

对于经典体验：


Edit store website - /Citrix/StoreWeb
StoreFront
UI experience
Deploy Citrix Workspace app
Category settings
Appearance
Featured app groups
Authentication methods
Website shortcuts
Launch preferences
Store timeouts
Session reconnect
User interface settings
Advanced settings
User interface settings
These settings control the end user experience.
Web browser settings
Automatically launch desktop
Show desktop viewer
Allow end user to download a Citrix Workspace app configuration file.
Multi-click duration:
3
seconds
Navigation tabs
Select tabs:
Home, Apps and Desktops
Default tab:
Home
OK
Cancel
Apply

对于现代体验：



自动启动桌面

如果此设置已启用，并且用户只有一个桌面，则当用户登录时，该桌面将自动启动。

要使用 PowerShell 更改自动启动桌面设置，请运行 cmdlet Set-STFWebReceiverUserInterface 并带参数 `AutoLaunchDesktop`。

此设置在从 Web 浏览器启动资源时适用。从本地安装的 Citrix Workspace™ 应用程序启动资源时不适用。

要使用 PowerShell 更改此选项，请调用 cmdlet Set-STFWebReceiverUserInterface 并带参数 `AutoLaunchDesktop`。

显示桌面查看器

桌面查看器是提供轻松访问 HDX™ 首选项的工具栏。使用此设置选择是否显示此工具栏。桌面查看器提供最佳用户体验，并且默认启用。

此设置仅在通过 Web 浏览器使用 Windows、Linux 和其他本地安装的 HDX 客户端 混合启动 资源时适用。当用户使用 HTML5 HDX 客户端在其 Web 浏览器中启动资源时，无论此设置如何，它始终会显示工具栏。

要使用 PowerShell 更改此选项，请使用参数 `ShowDesktopViewer` 调用 cmdlet Set-STFWebReceiverResourcesService。

允许最终用户下载 Citrix Workspace 应用程序配置文件

如果选中此选项，则当用户使用 Web 浏览器访问应用商店时，可以下载一个预配文件，该文件用于为关联的应用商店配置 Citrix Workspace 应用程序。预配文件包含提供站点上资源的应用商店的连接详细信息，包括为应用商店配置的任何 Citrix Gateway 部署和信标的详细信息。

要使用 PowerShell 更改此选项，请使用参数 `ReceiverConfigurationEnabled` 调用 cmdlet Set-STFWebReceiverUserInterface。

多次单击持续时间

防止用户在配置的持续时间内多次启动同一应用程序。这仅在从 Web 浏览器启动资源时适用，而不适用于从本地安装的 Citrix Workspace 应用程序启动资源。

要使用 PowerShell 更改多次单击持续时间，请使用参数 `MultiClickTimeout` 运行 cmdlet Set-STFWebReceiverUserInterface。

此设置仅在从 Web 浏览器启动资源时适用。它不适用于本地安装的 Citrix Workspace 应用程序。

导航选项卡

可用设置取决于所选的 UI 体验。

现代体验

始终显示导航选项卡

默认情况下，如果资源少于 20 个，UI 会显示一个简单视图，其中所有资源都在一个屏幕上，没有选项卡。管理员可以选择“始终显示导航选项卡”选项，从而有效地禁用简单视图。选中此选项后，无论资源数量如何，用户都会看到导航选项卡。

禁用主页选项卡

默认情况下，UI 包含一个“主页”选项卡（简单视图除外），该选项卡显示收藏夹和最近使用的应用程序和桌面。“主页”选项卡提供对收藏夹和最近使用的应用程序和桌面的快速访问。管理员现在可以清除“显示主页选项卡”选项以将其隐藏。收藏夹仍可从各个“应用程序”或“桌面”选项卡中获取。

默认选项卡

默认情况下，登录后，用户会进入“主页”选项卡。您可以更改默认选项卡，以便用户进入“**应用程序**”或“**桌面**”选项卡。如果您选择了“**应用程序**”，则此外，您可以选择默认情况下是显示所有应用程序、特定类别的应用程序还是未分类的应用程序。

经典体验

当桌面和应用程序都可用时，网站默认显示单独的桌面和应用程序视图。收藏夹显示在“**主页**”视图中。用户登录站点时首先看到“**主页**”视图。

从“**选择选项卡**”下拉列表中，选择是显示应用程序、桌面，还是两者都显示。

从“**默认选项卡**”视图下拉列表中，选择用户首次登录时要显示的选项卡。

选项	描述
主页	显示“主页”选项卡
应用程序	显示“应用程序”选项卡
桌面	显示“桌面”选项卡

要使用 PowerShell 更改这些选项，请运行 cmdlet Set-STFWebReceiverUserInterface，并使用参数 `ShowAppsView`、`ShowDesktopsView` 和 `DefaultView`。

为首次使用的用户显示“个性化您的主屏幕”

使用现代体验时，没有收藏夹的用户首次登录时，将显示“**个性化您的主屏幕**”窗口。要管理此窗口，您必须使用 PowerShell。

要获取当前值，请调用 Get-STFWebReceiverUserInterface。例如：

```
$website = Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"

$websiteUI = Get-STFWebReceiverUserInterface -WebReceiverService $website

"Show personalization screen: $($websiteUI.ShowFirstTimeUse)"
```

要禁用或启用该窗口，请调用 Set-STFWebReceiverUserInterface 并使用参数 `ShowFirstTimeUse`。例如：

```
$website = Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"

Set-STFWebReceiverUserInterface -WebReceiverService $website
-ShowFirstTimeUse $false
```

显示活动管理器

现代体验包括 活动管理器，以允许用户管理其会话。活动管理器默认启用。要管理此设置，您必须使用 PowerShell。要获取当前值，请调用 Get-STFWebReceiverUserInterface。例如：

```
$website = Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"

$websiteUI = Get-STFWebReceiverUserInterface -WebReceiverService $website

"Show Activity manager: $($websiteUI.ShowActivityManager)"
```

要禁用或启用活动管理器，请使用参数 `ShowActivityManager` 调用 Set-STFWebReceiverUserInterface。例如：

```
$website = Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"

Set-STFWebReceiverUserInterface -WebReceiverService $website
-ShowActivityManager $false
```

固定链接

注意：

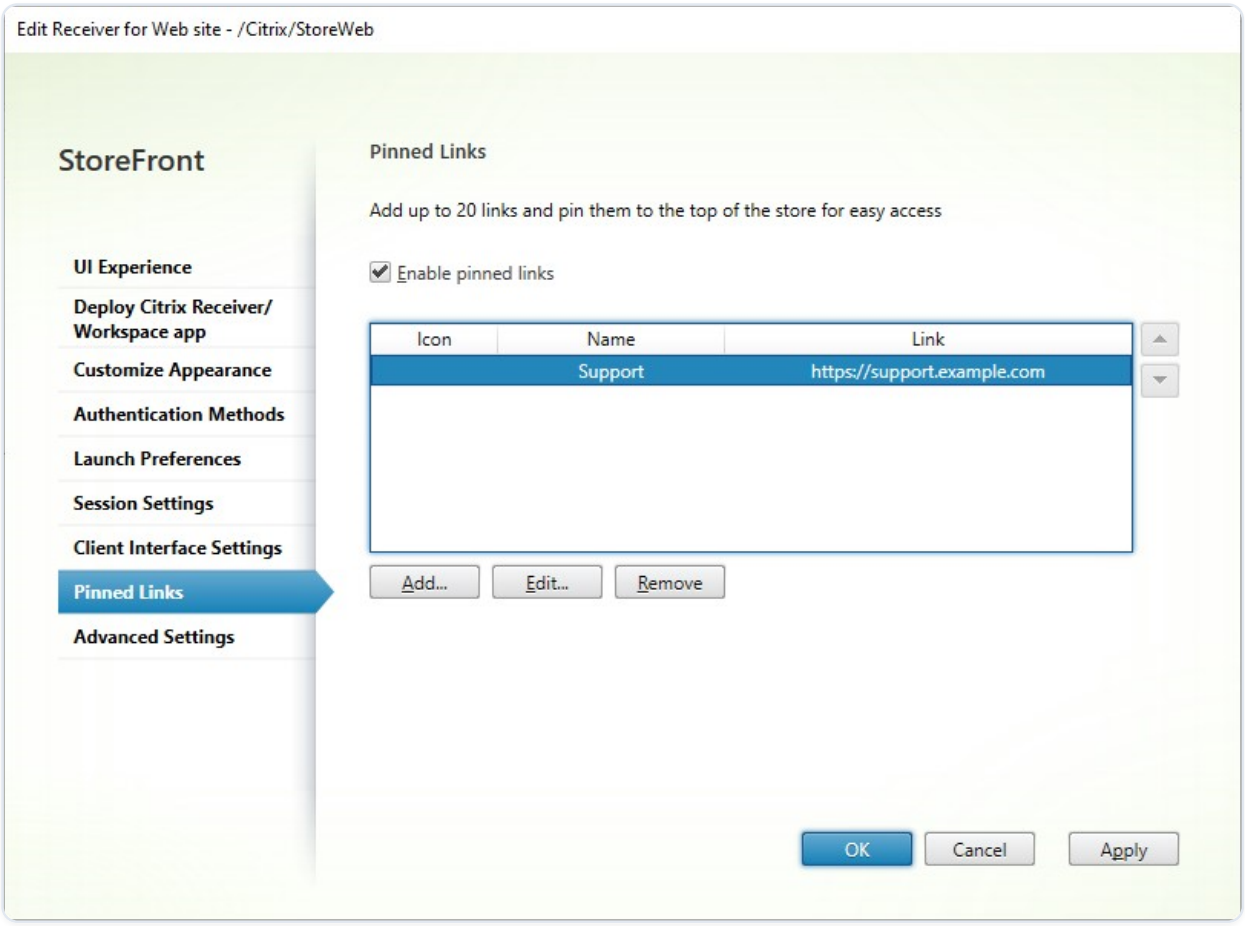
此功能仅在使用现代体验时可用。

StoreFront™ UI 上的自定义 URL 指的是客户定义的超链接，可提供对特定网站的快速访问。此功能充当快捷方式，帮助用户直接从 StoreFront UI 高效导航到网站。重要的链接，例如支持网站或公司门户，可以提供给用户，而无需他们搜索这些链接。它使导航变得轻松快捷。此功能仅在现代体验中可用。

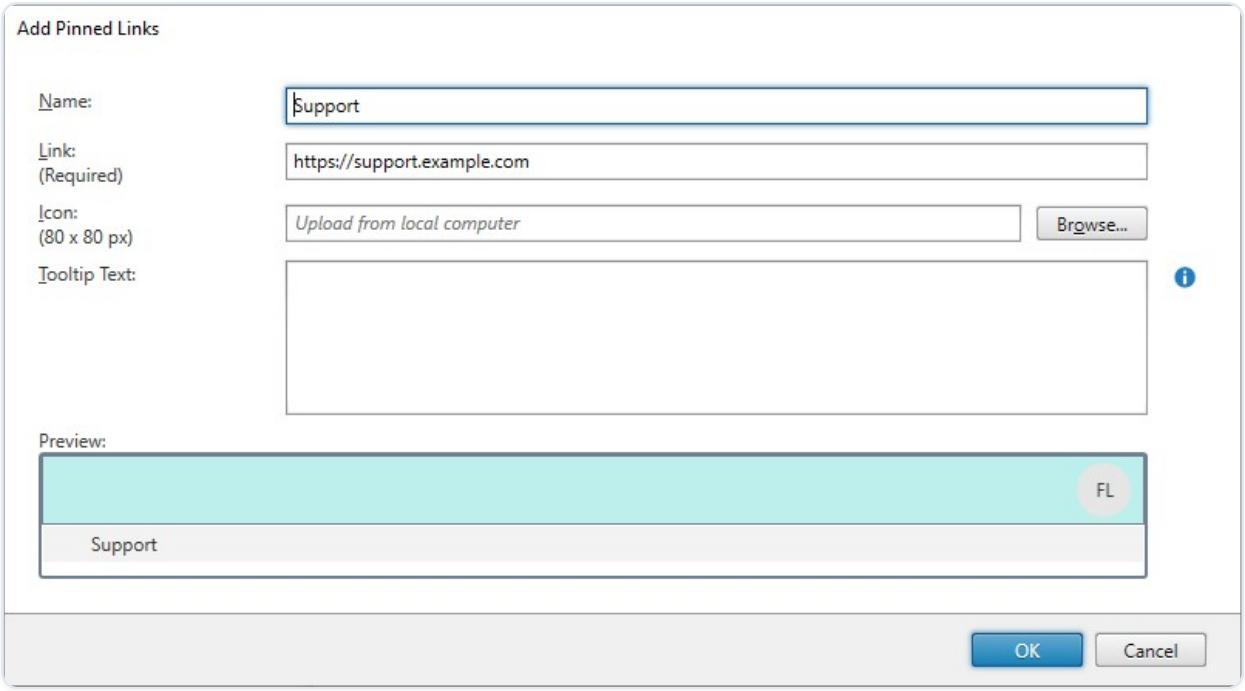
配置

要添加固定链接：

1. 转到编辑商店网站并选择**固定链接**选项卡。

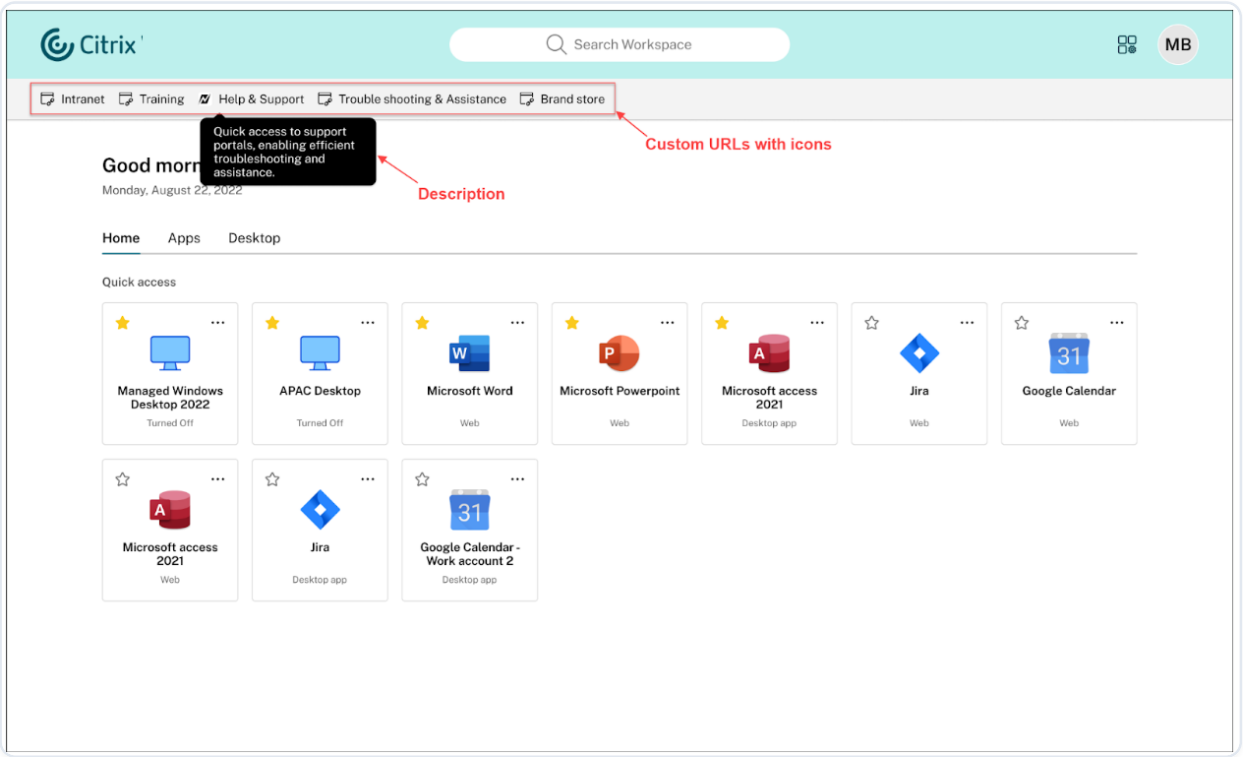


2. 单击 **添加**。



3. 输入名称、链接、工具提示，并浏览选择图标。
4. 预览更新并点击**确定**。

   这些链接显示在商店顶部，以便快速访问。



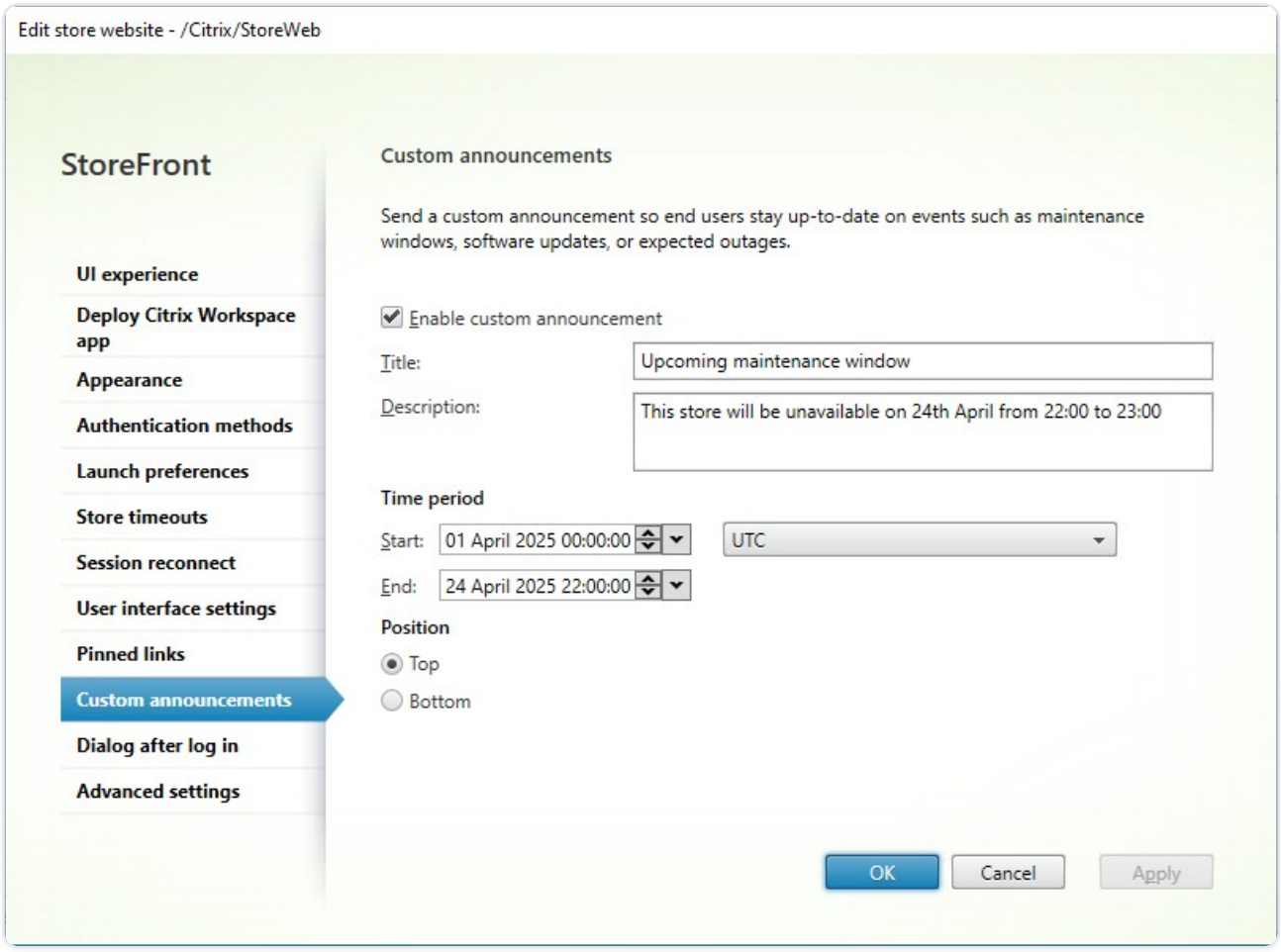
自定义公告

您可以配置一个横幅，向最终用户显示，例如通知他们即将进行的更改或维护窗口。

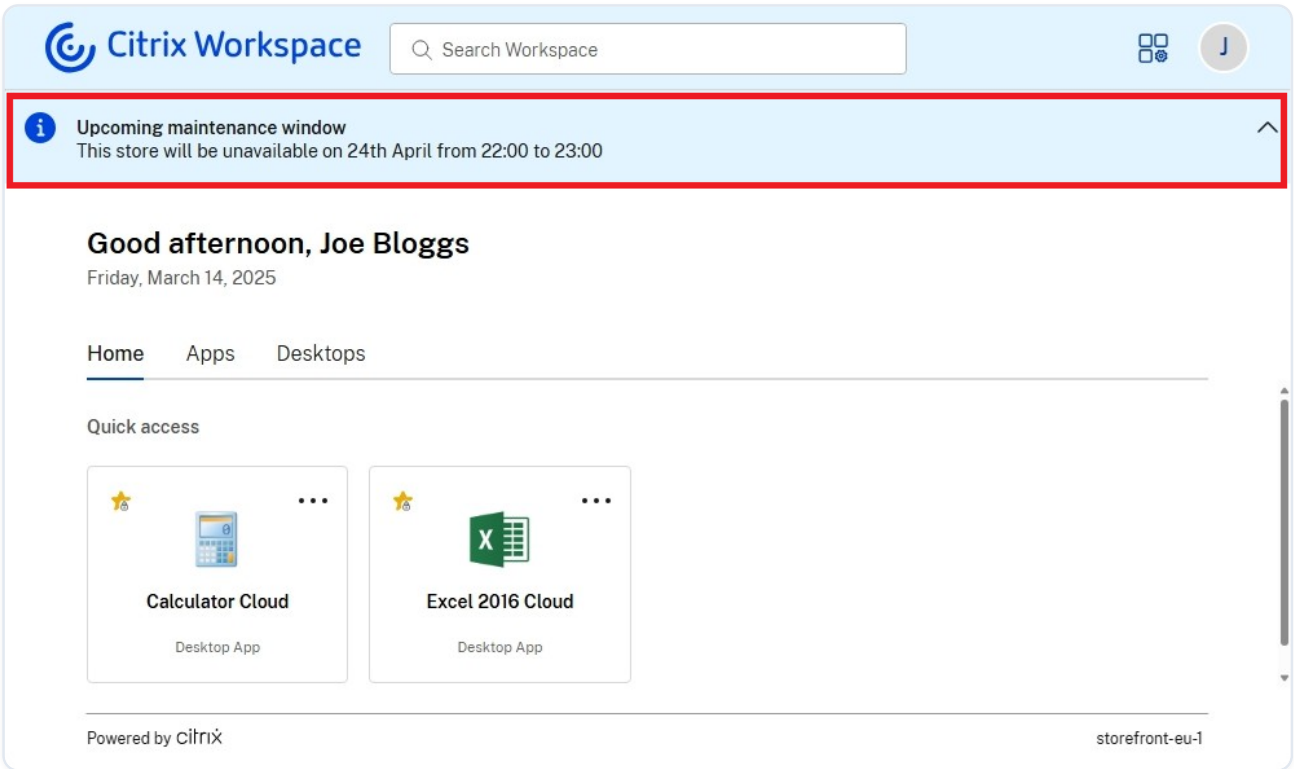
> **注意：**
>
> 此功能仅在使用 现代体验 时可用。如果您使用的是经典体验，则可以使用 StoreFront 客户端 UI 自定义 API 创建自定义公告。请参阅示例 添加动态标题。

要设置或修改自定义公告：

1. 转到 编辑商店网站
2. 选择**类别设置**选项卡。
3. 选择**启用自定义公告**。
4. 输入**标题**。
5. 输入**描述**。
6. 输入您希望自定义公告开始显示的日期和时间。
7. 输入您希望客户公告隐藏的日期和时间。
8. 选择是在屏幕顶部还是底部显示公告。



当用户登录时，公告会永久显示在屏幕的顶部或底部。



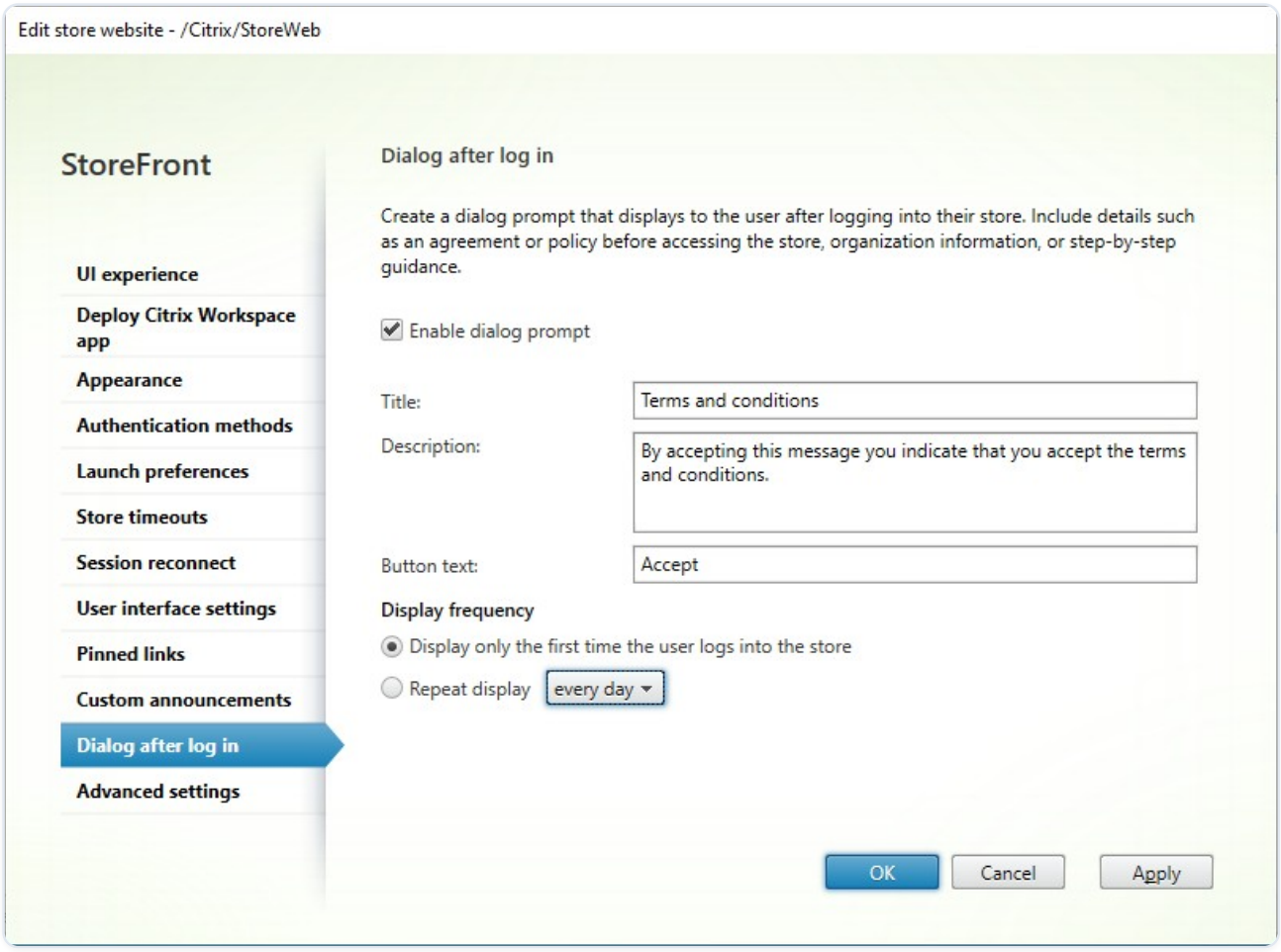
登录后对话框

您可以配置一个在登录后出现的弹出对话框，用户必须接受该对话框才能与 StoreFront 交互。您可以使用此功能向用户告知重要信息，例如法规信息、政策确认、内部政策、说明内容、安全通知、系统更新和法律免责声明。

> **注意：**
>
> 此功能仅在使用现代体验时可用。如果您使用的是经典体验，则可以使用StoreFront 客户端 UI 自定义 API添加类似的对话框。请参阅示例在登录前或登录后显示免责声明消息。

要设置或修改对话框：

1. 转到编辑商店网站
2. 选择**登录后对话框**选项卡。
3. 选择**启用对话框提示**。
4. 输入**标题**、**描述**和**按钮文本**。
5. 选择消息的显示频率。如果选择**重复显示**，则可以在**每天**、**每 7 天**和**每 30 天**之间进行选择。如果更改消息，则提示始终在用户下次登录时出现。



有关最终用户体验的更多信息，请参阅现代体验。

应用程序保护

应用程序保护通过阻止键盘记录和屏幕捕获提供额外的安全级别。有关详细信息，请参阅 应用程序保护 文档。

重要提示：

通过 Web 浏览器访问应用商店时，需要应用程序保护的应用默认处于隐藏状态。必须配置 StoreFront 以显示受保护的应用。通过 Citrix Workspace 应用程序访问应用商店时，无需进行 StoreFront 配置。

适用于从 Citrix Workspace 应用程序启动的应用程序保护

当用户使用 受支持的 Citrix Workspace 应用程序版本 访问应用商店时，StoreFront 会显示所有需要应用程序保护的资源。无需进行额外的 StoreFront 配置。

适用于混合启动的应用程序保护

当用户通过 Web 浏览器访问应用商店时，需要应用程序保护的虚拟应用程序和桌面默认处于隐藏状态。可以配置 StoreFront 2308 及更高版本以显示受保护的资源，除非使用 ChromeOS，或者用户选择在其 Web 浏览器中启动资源，因为这些不支持应用程序保护。

> **警告**
>
> 可以使用不应用应用程序保护的旧版 Citrix Workspace 应用程序启动应用程序。因此，在为混合启动启用应用程序保护之前，Citrix 建议您启用 应用程序保护姿态检查，该检查会阻止从不支持应用程序保护的 Citrix Workspace 应用程序版本启动虚拟应用程序和桌面。

> 如果使用 ICA 下载启动资源，用户可以编辑 ICA 文件以删除应用应用程序保护的指令。因此，在为混合启动启用应用程序保护之前，Citrix 建议您启用 策略篡改检测。

> 早于 2507 的 StoreFront 版本曾尝试使用 Citrix Web 扩展 或 Citrix Workspace 启动器 检测已安装的 Citrix Workspace 应用程序版本，并且仅当客户端满足某些最低版本要求时才显示具有应用程序保护的资源。但是，无法保证版本检测正确，这导致资源被错误地显示或隐藏。因此，此检查已被删除。

为混合启动启用应用程序保护

要允许 StoreFront 在受支持的 Citrix Workspace 应用程序版本上显示受保护的应用程序，请使用 PowerShell cmdlet Set-STFWebReceiverAppProtection。

1. 以管理员身份打开 PowerShell 控制台。
2. 如果您有多个网站，请找到要配置的网站的虚拟路径。这是用户 Web 浏览器中显示的路径，例如 `/Citrix/StoreWeb`。您可以使用命令 `Get-STFWebReceiverService` 获取所有网站及其路径的列表。
3. 运行 PowerShell：

```
$receiver = Get-STFWebReceiverService -VirtualPath "[virtual path]"

Set-STFWebReceiverAppProtection -WebReceiverService $receiver -Enabled
On
```

将 `[virtual path]` 替换为第一步中找到的路径。如果只有一个网站，则可以排除 `-VirtualPath`。

4. 如果用户选择通过其 Web 浏览器打开资源（无论是通过管理员配置还是因为用户选择了**使用 Web 浏览器**），则应用程序保护不可用。您可以选择将应用商店配置为始终使用本地安装的 Citrix Workspace 应用程序启动。有关详细信息，请参阅 Citrix Workspace 应用程序部署。
5. 用户首次打开应用商店网站时，如果 Citrix Web 扩展不可用，则会显示**检测 Citrix Workspace 应用程序**屏幕。如果用户选择**跳过检测**，则 StoreFront 无法确定应用程序版本，因此不显示受保护的应用程序和桌面。因此，建议您禁用**跳过检测**选项。有关详细信息，请参阅 允许用户跳过 Citrix Workspace 应用程序检测。

查看是否启用了混合启动的应用程序保护

要了解是否可以使用 PowerShell 为应用商店网站提供混合启动的应用程序保护，请运行 cmdlet Get-STFWebReceiverAppProtection。例如：

```
$receiver = Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"

Get-STFWebReceiverAppProtection -WebReceiverService $receiver
```

高级设置

要修改网站的高级设置，请打开 编辑商店网站 屏幕并选择 **高级设置** 选项卡。

高级设置选项卡的屏幕截图(/en-us/storefront/2507-ltsr/media/stores/websites/advanced-settings.png)

启用 Fiddler 跟踪

启用 Fiddler 跟踪 StoreFront 服务之间的流量，用于调试目的。环回通信也必须禁用。此功能默认关闭，仅在支持人员要求时才应启用。完成故障排除后，请禁用 Fiddler 跟踪。

启用文件夹视图

默认情况下，在 **应用程序** 选项卡上显示 **类别** 视图。要隐藏 **类别** 视图，请清除 **启用文件夹视图**。仅适用于经典体验。在使用现代体验时无效。有关类别显示的更多信息，请参阅 类别设置。

要使用 PowerShell 修改此设置，请运行 cmdlet `Set-STFWebReceiverUserInterface` 并使用参数 `EnableAppsFolderView`。

启用环回通信

启用 StoreFront™ 服务之间的直接通信，无需通过基本 URL。在使用负载均衡器时启用。可设置为以下值：

值	描述
开	StoreFront Web 代理使用环回地址与商店服务通信，确保通信保留在 StoreFront 服务器上。
关	StoreFront Web 代理使用基本 URL 中定义的 FQDN 与商店服务通信。如果基本 URL 是负载均衡器，则可能导致通信通过负载均衡器定向到不同的 StoreFront 服务器，从而导致请求失败。
使用 HTTP 开启	与 **开** 相同，但将协议从 HTTP 更改为 HTTPS。当使用终止 HTTPS 并通过 HTTP 连接到 StoreFront 的负载均衡器时，请选择此选项。要更改端口，请参阅 使用 HTTP 时的环回端口

要使用 PowerShell 修改此设置，请运行 cmdlet `Set-STFWebReceiverCommunication` 并使用参数 `Loopback`。

启用 Citrix Workspace 启动器

默认启用。当用户从 Web 浏览器打开应用商店时，这允许网站使用 Citrix Workspace 启动器 尝试检测是否安装了 Citrix Workspace 应用程序，然后启动资源。

当 Citrix Workspace 启动器被禁用且 启动选项 设置为 **让用户选择** 时，应用商店网站不会提示首次使用的用户选择启动方法。使用现代体验时，启动方法默认为下载 ICA 文件，但用户可以从设置屏幕更改此设置。使用经典体验时，资源会在 Web 浏览器中启动。

要使用 PowerShell 修改此设置，请运行 cmdlet `Set-STFWebReceiverPluginAssistant` 并使用参数 `Enabled`。

禁用此选项可能导致用户 下载 ICA 文件，不建议这样做。

启用严格传输安全性

启用后，会添加 `Strict-Transport-Security` 标头，以告知浏览器仅通过 HTTPS 连接到网站。

要使用 PowerShell 修改此设置，请运行 cmdlet `Set-STFWebReceiverStrictTransportSecurity` 并使用参数 `Enabled`。

还有其他方法可以启用 HSTS。有关详细信息，请参阅 HTTPS。

ICA 文件缓存过期

ICA 文件在服务器内存中缓存的秒数。客户端启动后，ICA 文件准备就绪，客户端必须在此时间内检索 ICA 文件。默认为 90 秒。

要使用 PowerShell 修改此设置，请运行 cmdlet `Set-STFWebReceiverResourcesService` 并使用参数 `IcaFileCacheExpiry`。

图标分辨率

要从服务器请求的图标文件大小。请注意，这不直接等同于 UI 中显示的图标大小。默认值为 128。

要使用 PowerShell 修改此设置，请运行 cmdlet `Set-STFWebReceiverResourcesService` 并使用参数 `IconSize`。

使用 HTTP 时的环回端口

当 启用环回通信 设置为 **使用 HTTP 开启** 时，此项设置端口。

要使用 PowerShell 修改此设置，请运行 cmdlet `Set-STFWebReceiverCommunication` 并使用参数 `LoopbackPortUsingHttp`。

提示不受信任的快捷方式

启动 网站快捷方式 时，默认情况下，如果引用方不在受信任站点列表中，则会提示用户确认。如果禁用此功能，用户可以从不受信任的网站启动资源。

登录后提示安装 Citrix Workspace 应用程序

当用户首次访问应用商店网站时，网站会尝试检测 Citrix Workspace 应用程序并提供下载 Citrix Workspace 应用程序的选项。默认情况下，当直接访问 StoreFront 时，这会在用户登录之前发生。或者，您可以选择 **登录后提示安装 Citrix Workspace 应用程序**。当用户通过 Citrix Gateway 登录时，此设置无效，因为这总是在用户到达 StoreFront Citrix Workspace 应用程序检测屏幕之前发生。

要使用 PowerShell 修改此设置，请运行 cmdlet `Set-STFWebReceiverPluginAssistant` 并使用参数 `ShowAfterLogin`。

资源详细信息

使用经典体验时，是获取 **默认** 还是 **完整** 资源详细信息。通常 **默认** 就足够了。如果您有使用 preProcessAppData 的 JavaScript 自定义项，则可以使用 **完整** 返回的额外数据。使用现代体验时无效。

严格传输安全策略持续时间

如果启用了 严格传输安全，则严格传输策略的强制持续时间，格式为 dd.hh:mm:ss。默认值为 90 天。

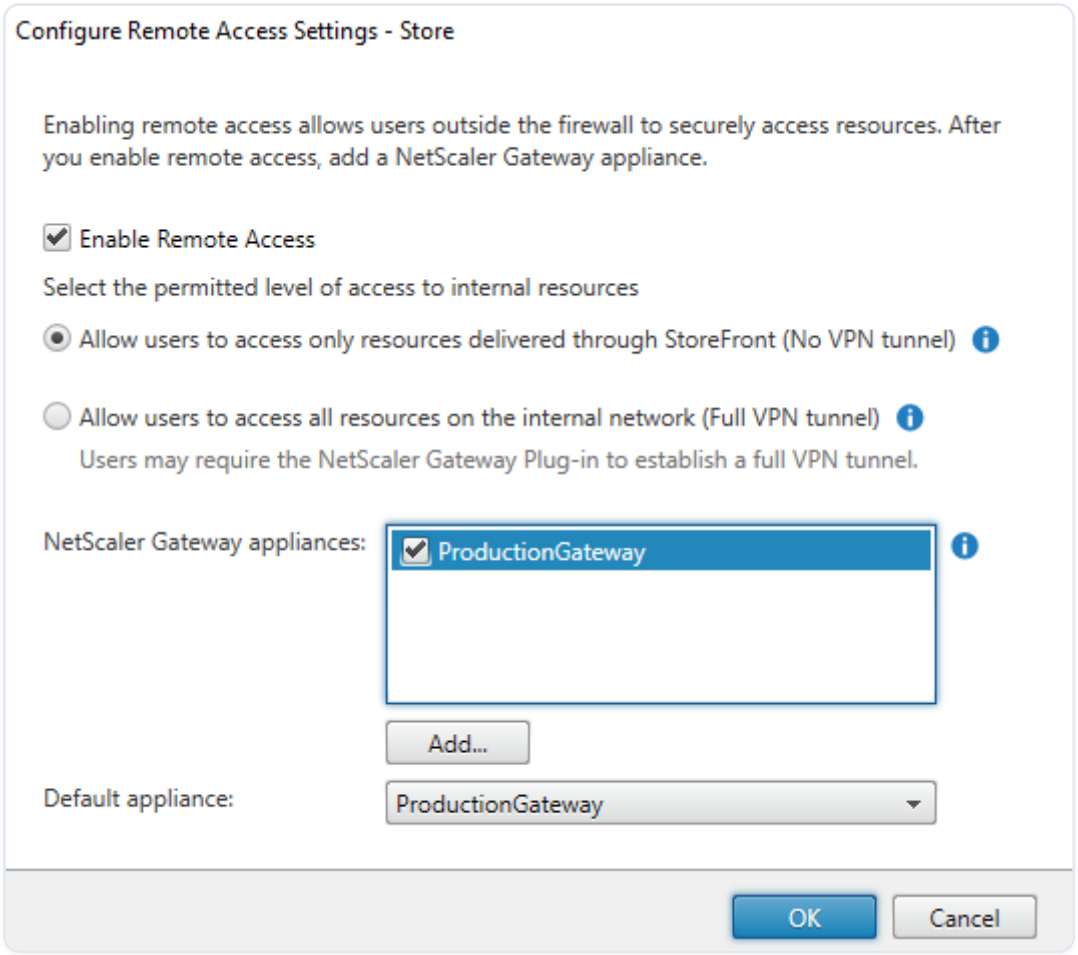
要使用 PowerShell 修改此设置，请运行 cmdlet `Set-STFWebReceiverStrictTransportSecurity` 并使用参数 `PolicyDuration`。

配置远程访问设置

您可以为从公共网络连接的用户配置通过 Citrix Gateway 访问应用商店。通过 Citrix Gateway 的远程访问不能应用于未经身份验证的应用商店。

> **重要提示：**
>
> 在多服务器部署中，一次只能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， 将配置更改传播到服务器组(/zh-cn/storefront/2507-ltsr/manage-deployment/configure-server-group.html)，以便更新部署中的其他服务器。

1. 在 Citrix StoreFront 管理控制台的右窗格中选择“应用商店”节点，然后在结果窗格中选择一个应用商店。
2. 在“操作”窗格中，单击**配置远程访问设置**。



3. 在“配置远程访问设置”对话框中，指定从公共网络连接的用户是否以及如何通过 Citrix Gateway 访问应用商店。

   - 要使应用商店对公共网络上的用户不可用，请勿选中**启用远程访问**。只有内部网络上的本地用户才能访问应用商店。
   - 要启用远程访问，请选中**启用远程访问**。
     - 要使通过应用商店交付的资源通过 Citrix Gateway 可用，请选择**无 VPN 隧道**。用户使用 ICAProxy 或无客户端 VPN (cVPN) 登录到 Citrix Gateway，无需使用 Citrix Gateway 插件来建立完整的 VPN。
     - 要通过安全套接字层 (SSL) 虚拟专用网络 (VPN) 隧道使应用商店和内部网络上的其他资源可用，请选择**完整 VPN 隧道**。用户需要 Citrix Gateway 插件来建立 VPN 隧道。

   启用对应用商店的远程访问时，将自动启用**从 Citrix Gateway 直通**身份验证方法。用户向 Citrix Gateway 进行身份验证，并在访问其应用商店时自动登录。

4. 如果已启用远程访问，请从**Citrix Gateway 设备**列表中选择用户可以通过其访问应用商店的部署。您之前为此应用商店和其他应用商店配置的任何部署都可在列表中选择。如果要向列表中添加更多部署，请单击**添加**并按照(/zh-cn/storefront/2507-ltsr/integrate-with-citrix-gateway-and-citrix-adc/configure-citrix-gateway.html)中的步骤操作。

5. 如果通过在列表中选择多个条目来启用通过多个设备的访问，请指定用于从 Citrix Workspace 应用程序访问应用商店的**默认设备**。
6. 单击**确定**以保存配置并关闭“配置远程访问”对话框。

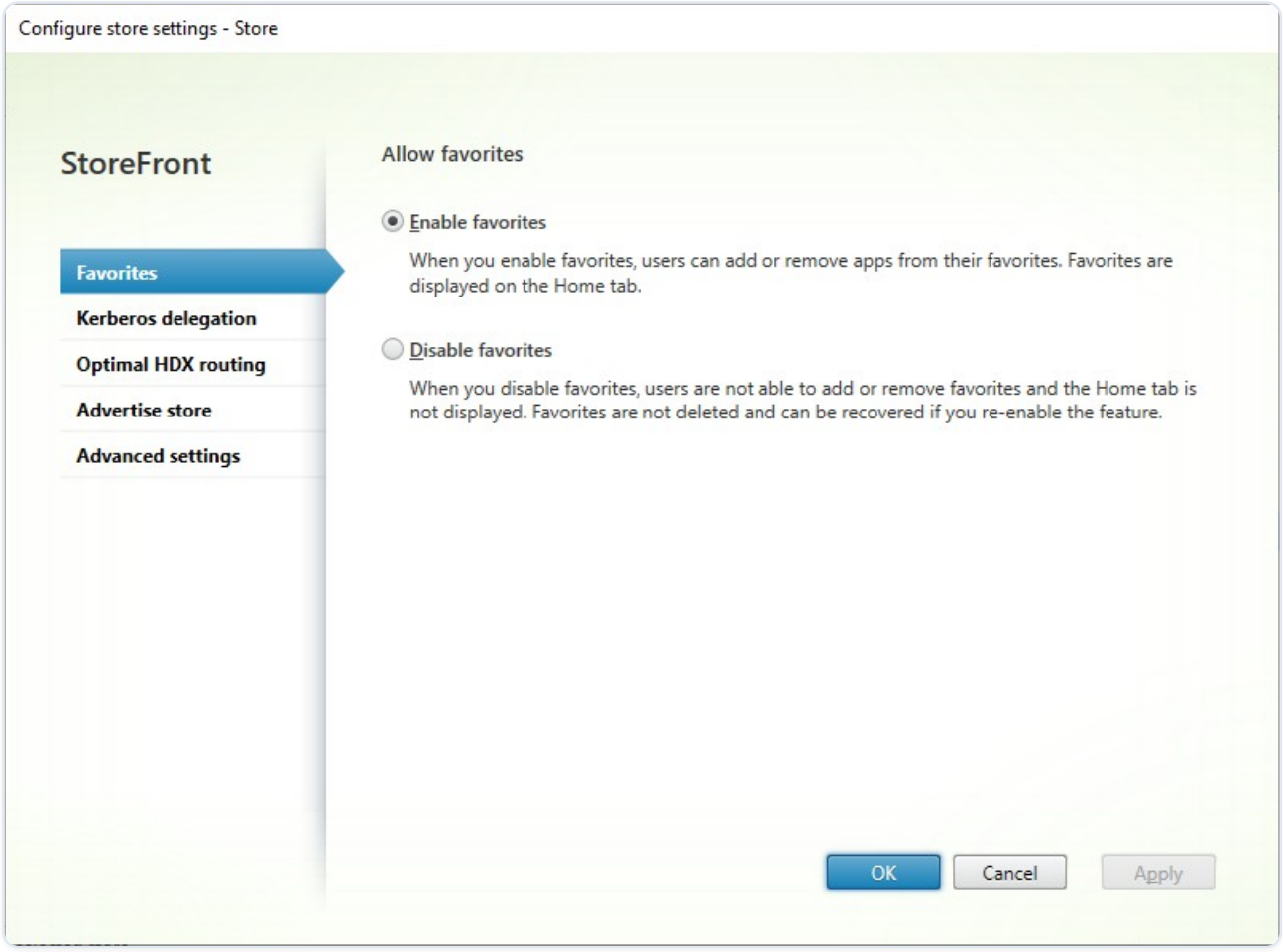
Citrix Workspace 应用程序使用信标点来确定用户是连接到本地网络还是公共网络，然后选择适当的访问方法。有关更改信标点的详细信息，请参阅配置信标点。

默认情况下，StoreFront 使用用户连接到应用商店的网关来启动资源。要配置 StoreFront 以使用备用网关或不使用网关来启动资源，请参阅最佳 HDX 路由。

配置应用商店

要修改应用商店设置，请执行以下操作：

1. 在 Citrix StoreFront 管理控制台的左窗格中选择“**应用商店**”节点，然后在“**操作**”窗格中单击“**配置应用商店设置**”。
2. 转到用户订阅选项卡以配置是否启用收藏夹。
3. 转到Kerberos 委派选项卡以配置应用商店是否使用 Kerberos 委派向交付控制器进行身份验证。
4. 转到最佳 HDX 路由选项卡以配置根据其位置启动应用程序和桌面时使用的网关。
5. 转到发布应用商店选项卡以配置用户输入 FQDN 或电子邮件地址时 Workspace 应用程序是否向用户显示应用商店。



收藏夹

您可以允许用户将资源设置为收藏夹。这些收藏夹显示在用户的主页选项卡上，以便快速访问。如果您使用的是经典体验并禁用了收藏夹，则会隐藏**主页**选项卡。

启用或禁用收藏夹

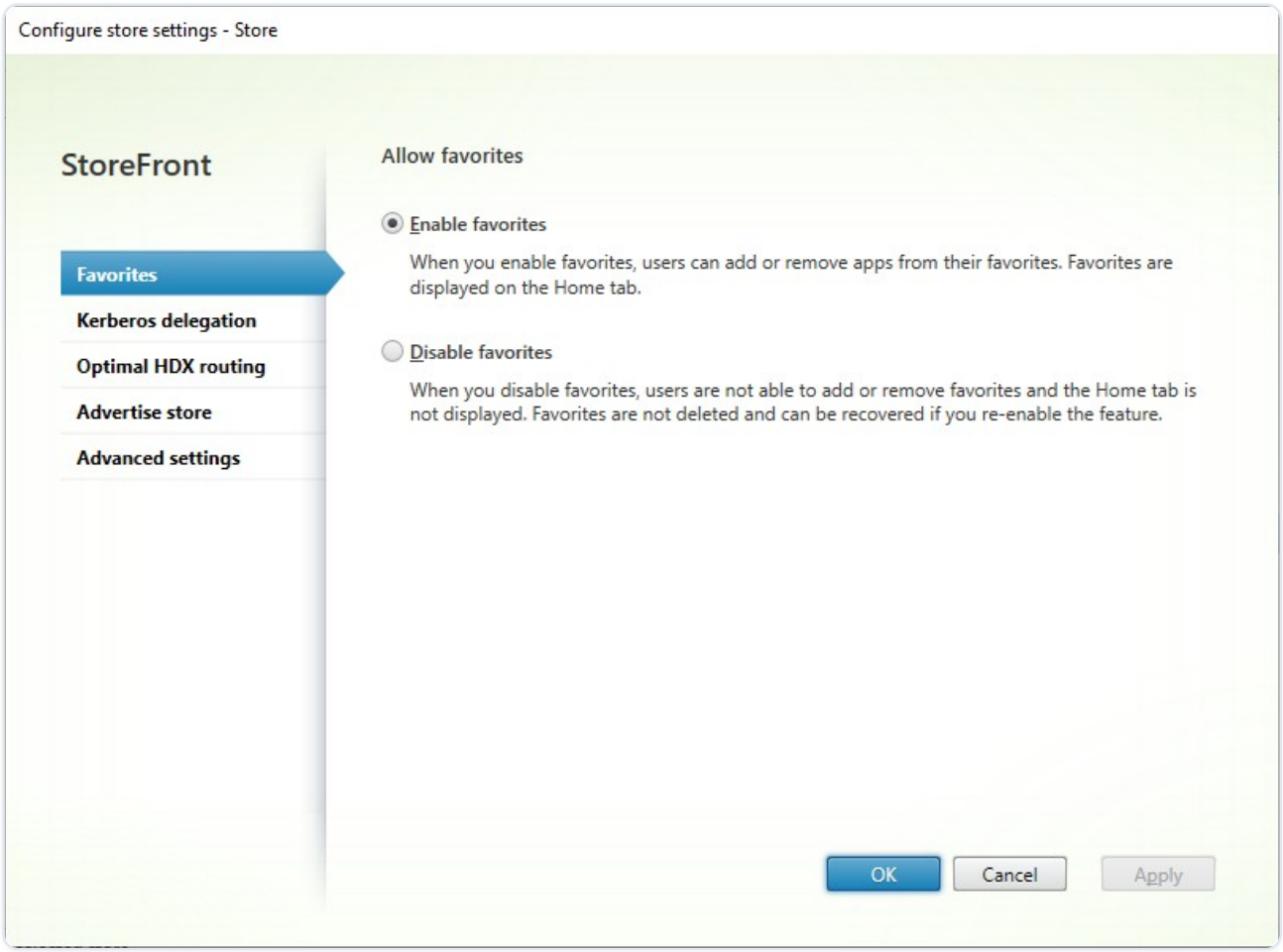
使用收藏夹选择以下选项之一：

- 允许用户创建和删除收藏夹。用户可以通过单击应用程序磁贴上的星形图标来收藏应用程序。用户可以再次单击星形图标以取消收藏应用程序。收藏的应用程序显示在**主页**选项卡上。
- 禁用收藏夹。用户无法收藏或取消收藏应用程序。主页选项卡不显示。

禁用订阅不会删除 Store 订阅数据。为 Store 重新启用订阅后，用户下次登录时将能够看到他们的收藏夹。

1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择**存储**节点，然后在结果窗格中选择一个存储。在**操作**窗格中，单击**配置存储设置**
2. 单击**用户收藏夹**选项卡以开启或关闭用户收藏夹功能。
3. 选择**启用用户收藏夹**以启用收藏夹。

4. 选择**禁用用户收藏夹**以禁用收藏夹。



或者，您可以使用 PowerShell cmdlet Set-STFStoreService 和 `LockedDown` 参数。例如，要禁用收藏夹：

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/
<yourstore>"

Set-STFStoreService -StoreService $StoreObject -LockedDown $True -Confirm:
$False
```

收藏夹数据库

默认情况下，收藏夹存储在本地数据库中，该数据库在服务器组中的服务器之间进行复制。或者，您可以将收藏夹存储在外部 SQL Server 数据库中。

要查看商店是使用本地数据库还是外部数据库，请运行 PowerShell cmdlet `Get-STFStoreSubscriptionsDatabase`。例如：

```
$store = Get-STFStoreService -VirtualPath [store path]

Get-STFStoreSubscriptionsDatabase -StoreService $store
```

这将返回：

- `UseLocalStorage` - 如果 `True`，收藏夹存储在本地数据库中（默认）。如果 `False`，收藏夹存储在外部数据库中。
- `DatabaseConnectionString` - 如果使用外部数据库，则此项包含连接字符串。否则为空。

有关详细信息，请参阅管理订阅数据库。

使用 SQL Server 数据库

要使用外部 SQL Server 数据库，请运行 PowerShell cmdlet `Set-STFStoreSubscriptionsDatabase`，并指定连接字符串。有关详细信息，请参阅使用 Microsoft SQL Server 存储订阅数据。

配置两个 StoreFront 商店以共享订阅数据存储

如果需要不同的配置设置，管理员通常会为相同的资源配置两个不同的 StoreFront 商店；例如，一个用于通过 Citrix Gateway 外部访问资源，另一个用于通过公司 LAN 内部访问资源。如果使用 SQL Server 数据库，请将两个商店都设置为使用相同的数据库连接字符串。使用本地数据库时，StoreFront 默认会为每个商店创建一个单独的数据库。因此，用户必须收藏两次相同的资源，每个商店一次。您可以将两个商店配置为使用相同的数据库，以便用户无论连接到哪个商店都能看到相同的收藏夹。

> **重要提示：**

> 由于站点名称是收藏夹密钥的一部分，因此您必须确保两个商店中的站点名称完全相同。

> 例如，假设您有两个名为“Internal”和“External”的商店。使用本地数据库时，请使用以下脚本将“External”商店配置为使用与“Internal”商店相同的订阅数据库。

```
$internalStore=Get-STFStoreService -VirtualPath '/Citrix/Internal'

$internalUri =
$internalStore.SubscriptionStoreClient.ClientEndpoint.Uri.ToString()
```

```
$externalStore=Get-STFStoreService -VirtualPath '/Citrix/External'

$externalStore.SubscriptionStoreClient.ClientEndpoint.Uri = $internalUri

Save-STFService $externalStore
```

将配置传播到服务器组中的其他服务器。

要检查商店正在使用哪个本地数据库，请运行以下脚本：

```
$store=Get-STFStoreService -VirtualPath '/Citrix/External'

$store.SubscriptionStoreClient.ClientEndpoint.Uri.ToString()
```

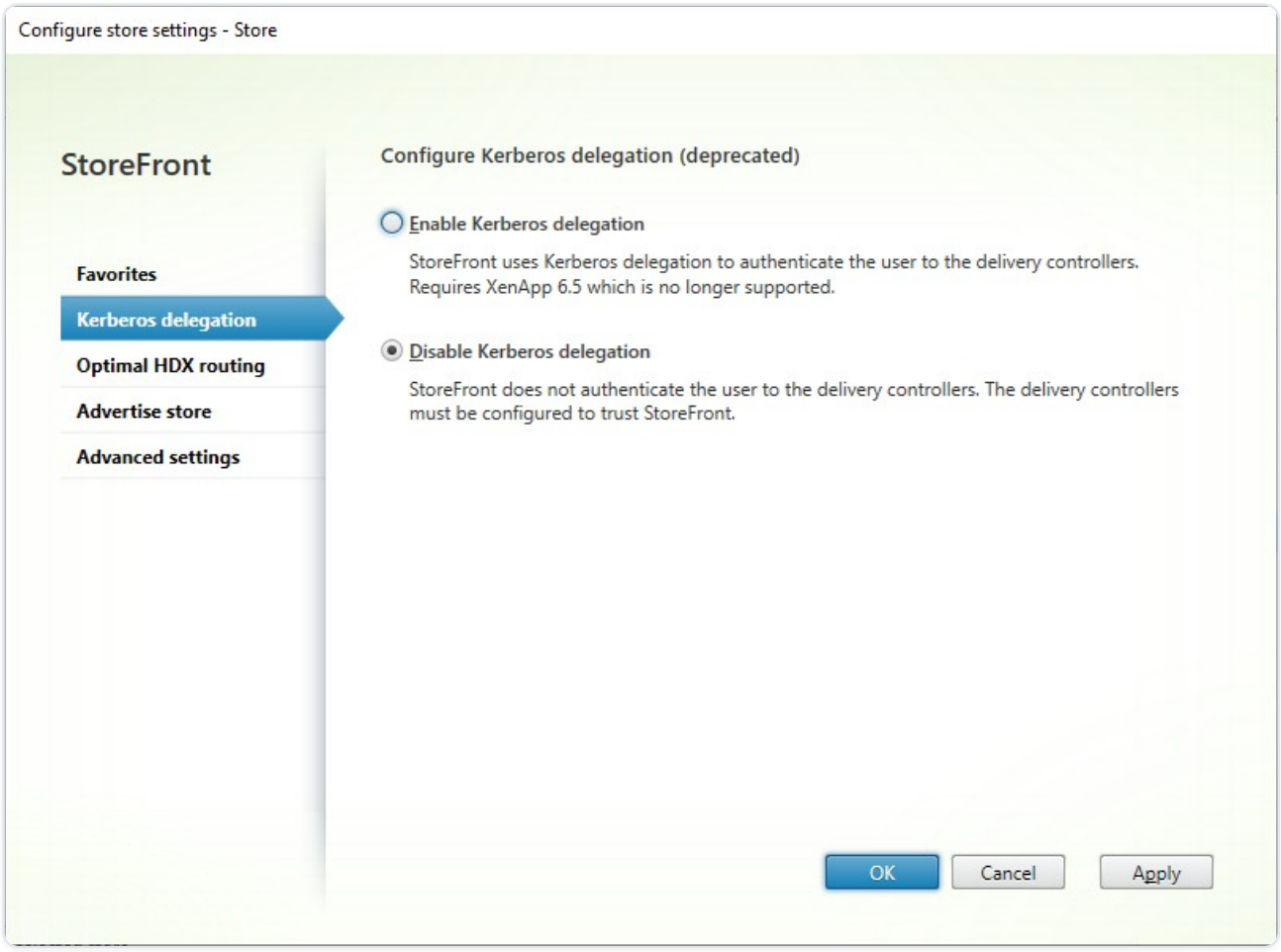
Kerberos 委派

注意：

Kerberos 委派已弃用，只能与 XenApp 6.5 及更早版本一起使用。它不能与任何受支持的 Citrix Virtual Apps and Desktops 版本一起使用。

当使用域直通或智能卡身份验证时（无论是直接使用还是通过 Citrix Gateway 使用），StoreFront 没有用户的凭据，因此无法使用用户的凭据向交付控制器进行身份验证。当使用 XenApp 6.5 及更早版本时，您可以启用 Kerberos 委派，以允许 StoreFront 模拟用户向交付控制器进行身份验证。这需要在 Active Directory 中配置委派。

1. 选择一个应用商店，并在“操作”窗格中单击 **配置应用商店设置**。
2. 选择 **Kerberos 委派** 选项卡。
3. 选择是**启用 Kerberos 委派**还是**禁用 Kerberos 委派**。
4. 按 **应用** 或 **确定** 以保存更改。



PowerShell

要配置 Kerberos 委派，请使用 cmdlet Set-STFStoreService 以及参数 `-KerberosDelegation`

配置应用商店的最佳 HDX™ 路由

配置最佳 Citrix Gateway 路由，以优化从 HDX 引擎到使用 StoreFront 发布的 Citrix Virtual Apps and Desktops 应用程序的 ICA 连接路由处理。通常，站点的最佳网关与站点位于同一地理位置。

您只需为用户通过其访问 StoreFront 的设备不是最佳网关的部署定义最佳 Citrix Gateway 设备。如果启动应通过发出启动请求的网关定向回去，StoreFront 会自动执行此操作。

您可以将网关映射到特定站点或区域。区域通常表示地理位置中的数据中心。您可以将最佳网关映射到多个区域，但通常应使用单个区域。预计每个区域至少有一个最佳 Citrix Gateway，用于与该区域内的资源建立 HDX 连接。

使用 Citrix Virtual Apps and Desktops 时，区域在 Studio 中定义，并且 StoreFront 中定义的任何区域必须与 Studio 中定义的区域名称完全匹配。有关详细信息，请参阅 区域。

使用 Citrix Desktops as a Service 时，区域等同于资源位置。资源位置在 Citrix Cloud 控制台中定义，并且 StoreFront 中定义的任何区域必须与 Citrix Cloud 控制台中定义的资源位置名称完全匹配。有关详细信息，请参阅 设置资源位置。

使用站点的示例场景

1 个英国网关 -> 1 个英国 StoreFront

- 英国本地应用程序和桌面
- 仅用于英国故障转移的美国应用程序和桌面

1 个美国网关 -> 1 个美国 StoreFront

- 美国本地应用程序和桌面
- 仅用于美国故障转移的英国应用程序和桌面

英国网关使用英国 StoreFront 提供对英国托管资源（例如应用程序和桌面）的远程访问。

英国 StoreFront 定义了基于英国和基于美国的 Citrix Gateway，并在其站点列表中包含英国和美国站点。英国用户通过其地理位置上共置的网关、StoreFront 和站点访问远程资源。如果其英国站点变得不可用，他们可以连接到美国资源作为临时故障转移替代方案。

如果没有最佳网关路由，所有 ICA 启动都将通过发出启动请求的英国网关，无论资源在地理上位于何处。默认情况下，StoreFront 会在发出请求时动态识别用于发出启动请求的网关。最佳网关路由会覆盖此设置，并强制美国连接通过最靠近提供应用程序和桌面的美国站点的网关。

> **注意：**
>
> 每个 StoreFront 商店每个站点只能映射一个最佳网关。

使用区域的示例场景

1 个 CAMZone -> 2 个英国 StoreFront

- 英国剑桥：应用程序和桌面
- 美国东部劳德代尔堡：应用程序和桌面
- 印度班加罗尔：应用程序和桌面

1 个 FTLZone -> 2 个美国 StoreFront

- 美国东部劳德代尔堡：应用程序和桌面

- 英国剑桥：应用程序和桌面
- 印度班加罗尔：应用程序和桌面

1 个 BGLZone -> 2 个印度 StoreFront

- 印度班加罗尔：应用程序和桌面
- 英国剑桥：应用程序和桌面
- 美国东部劳德代尔堡：应用程序和桌面

图 1. 次优网关路由

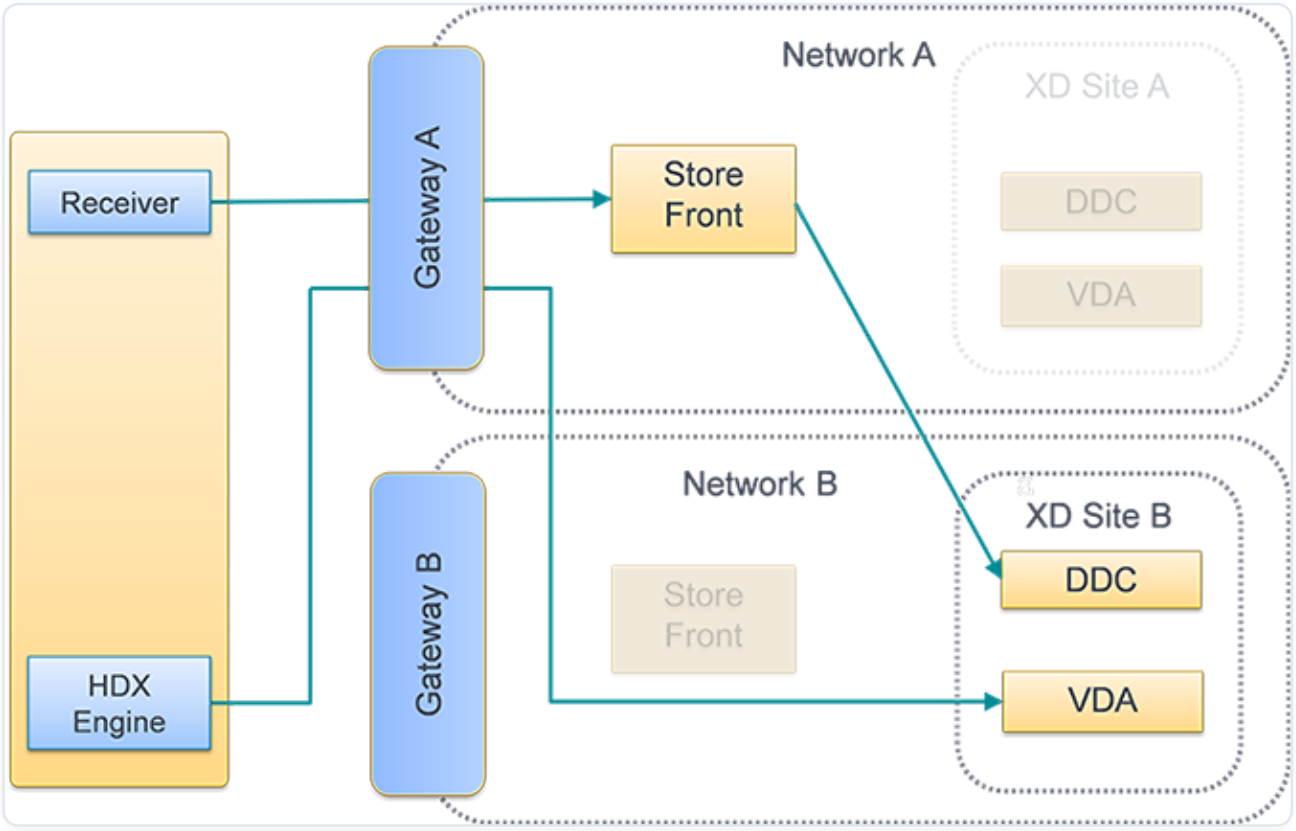
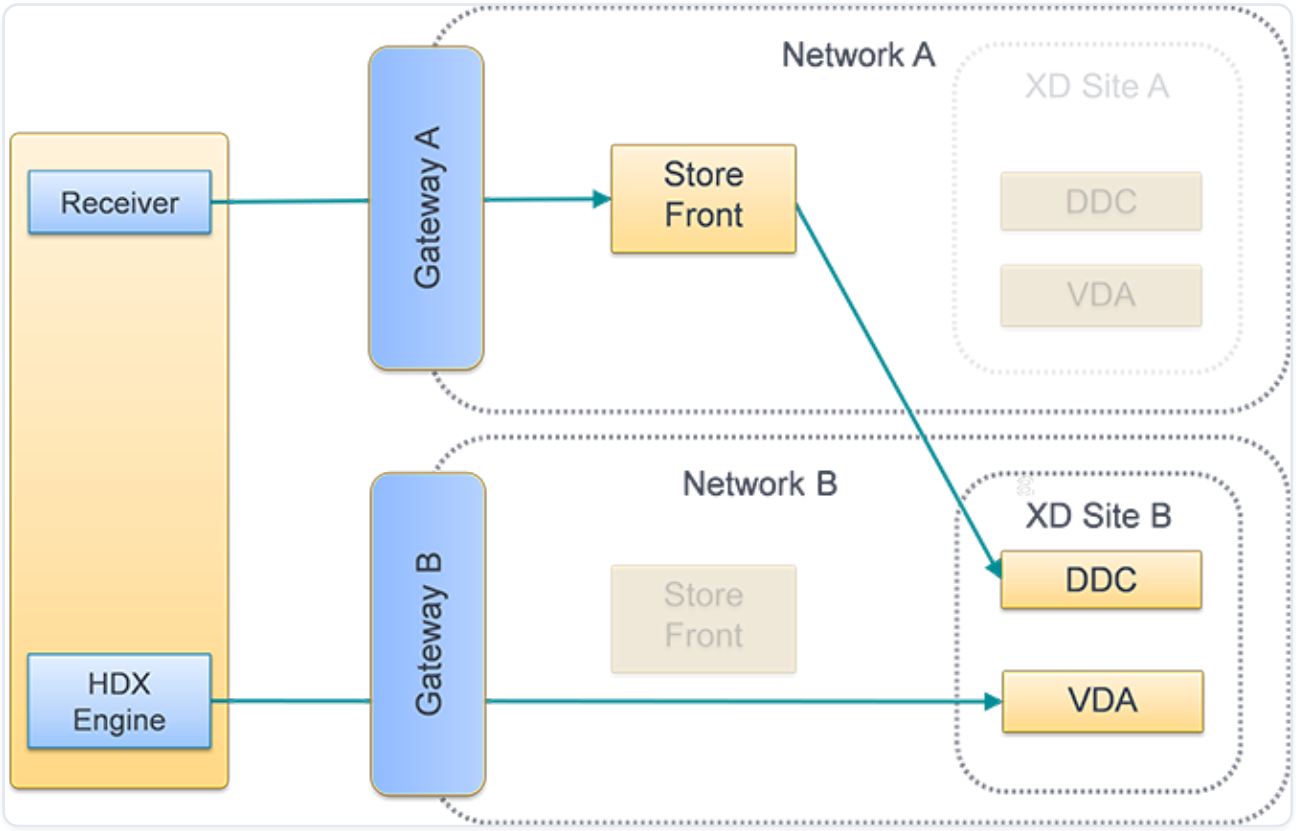
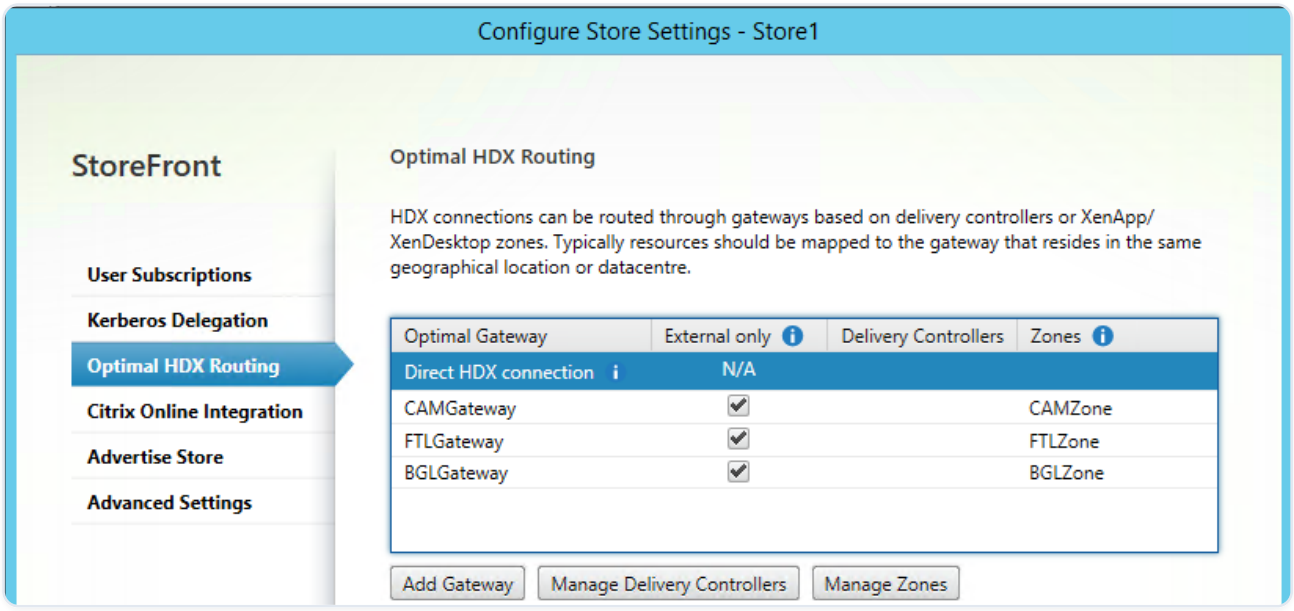


图 2. 最优网关路由



配置最优 HDX 路由

1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择 **Stores** 节点，并在结果窗格中选择一个应用商店。在 **Actions** 窗格中，单击 **Configure Store Settings**。
2. 选择 **Optimal HDX Routing** 选项卡。
3. 选择一个网关。
    a. 要在从特定站点访问资源时使用网关，请单击 **Manage sites** 并勾选一个或多个站点。
    b. 要在从特定区域访问资源时使用网关，请单击 **Manage Zones** 并输入一个或多个区域。
    c. 默认情况下，添加站点或区域后，**External Only** 会被勾选，这意味着 StoreFront 仅对通过网关连接到 StoreFront 的用户使用网关来启动 StoreFront。如果您希望也使用网关为直接连接到 StoreFront 而未通过网关的用户启动资源，请取消勾选 **External Only**。
4. 如果您希望始终直接连接到某些资源而不使用网关，即使对于通过网关远程访问 StoreFront 的用户也是如此，请选择 **Direct HDX connection** 并选择一些站点或区域。



。

使用 PowerShell 配置应用商店的最优 Citrix Gateway 路由

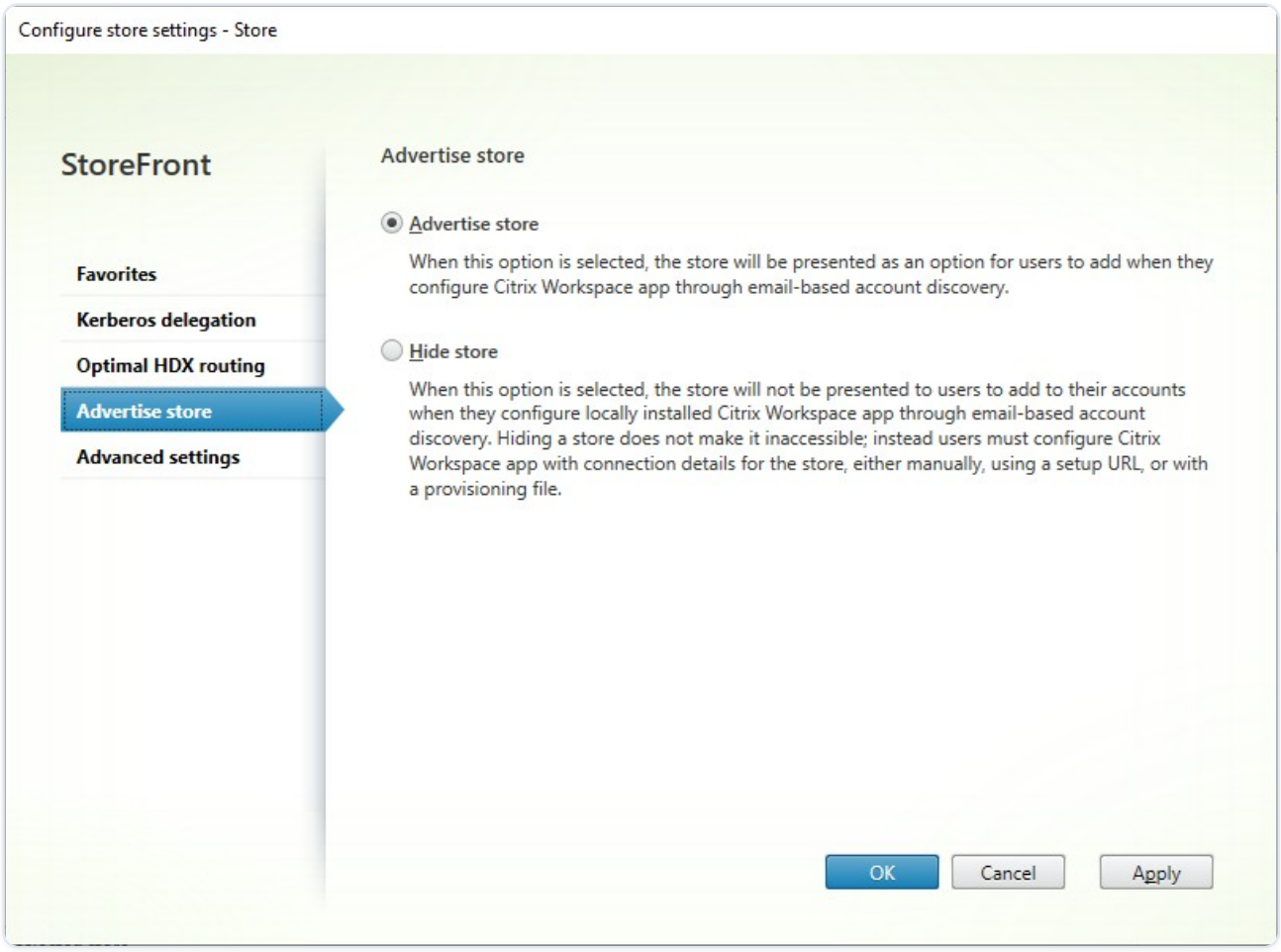
- 要为应用商店配置最优网关路由，请使用 Register-STFStoreOptimalLaunchGateway。
- 要移除商店的最佳网关路由，请使用 Unregister-STFStoreOptimalLaunchGateway。
- 要查看商店的最佳路由，请使用 Get-STFStoreRegisteredOptimalLaunchGateway。

向用户发布或隐藏应用商店

您可以选择是否向用户显示应用商店，以便他们在通过基于电子邮件的帐户发现或 FQDN 配置 Citrix Workspace 应用程序时将其添加到自己的帐户中。默认情况下，当您创建应用商店时，它会作为用户在发现托管该应用商店的 StoreFront 部署时，在 Citrix Receiver 中添加的选项显示。隐藏应用商店并不会使其无法访问，而是用户必须手动、使用设置 URL 或使用预配文件，通过应用商店的连接详细信息配置 Citrix Workspace 应用程序。

> 重要提示：
>
> 在多服务器部署中，一次只能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， 将您的配置更改传播到服务器组 以便更新部署中的其他服务器。

1. 在 Citrix StoreFront 管理控制台的左窗格中选择“**应用商店**”节点，然后在“**操作**”窗格中，单击“**配置应用商店设置**”>“**发布应用商店**”。
2. 在“**发布应用商店**”页面上，选择“**发布应用商店**”或“**隐藏应用商店**”。

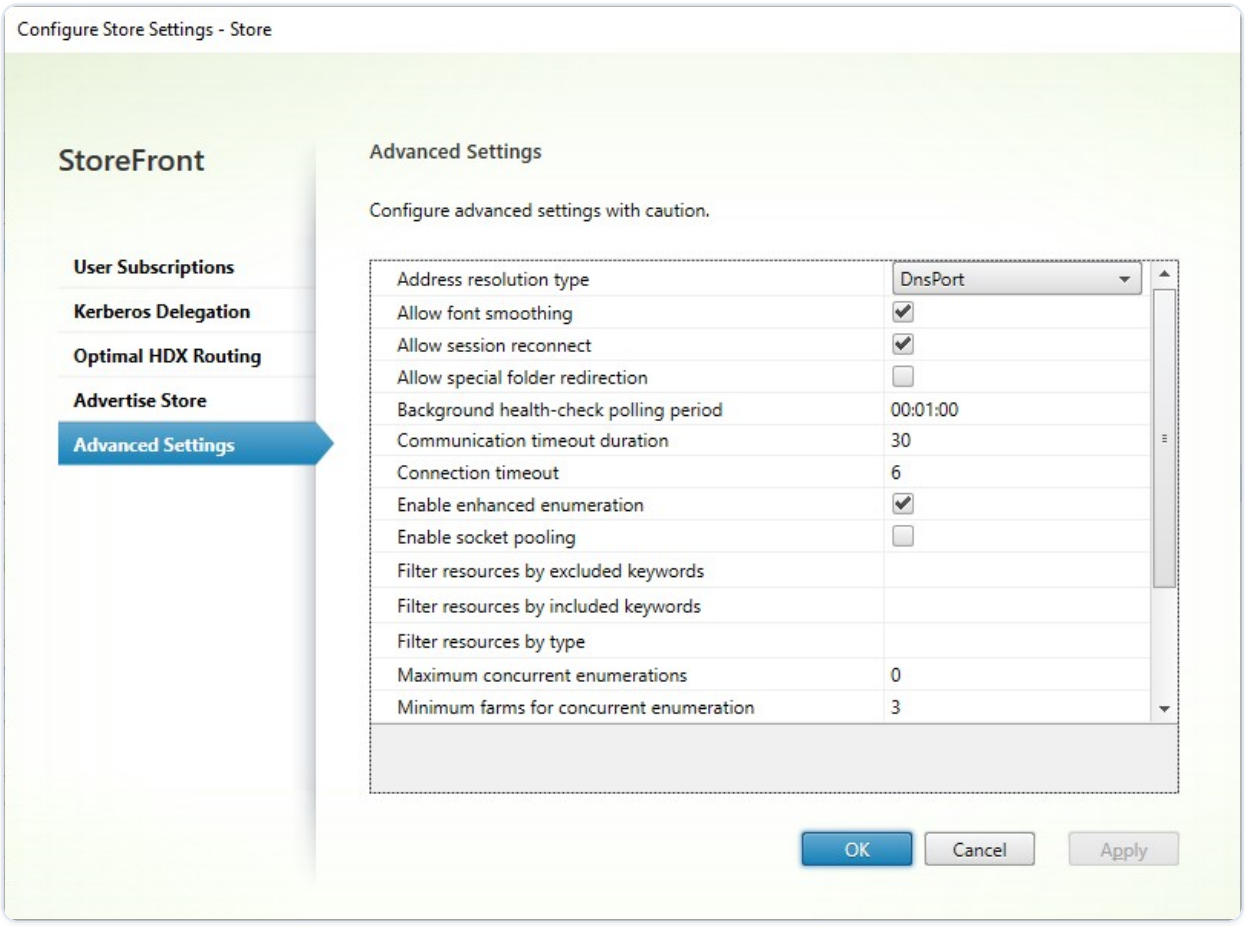


高级商店设置

您可以使用 配置商店设置 中的“高级设置”选项卡配置大多数高级商店属性。某些设置只能使用 PowerShell 修改。

> **重要提示：**
>
> 在多服务器部署中，一次只能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，将配置更改传播到服务器组，以便更新部署中的其他服务器。

1. 在 Citrix StoreFront 管理控制台的左窗格中选择“商店”节点，在中心窗格中选择一个商店，然后在“操作”窗格中选择 **配置商店设置**。
2. 在“**配置商店设置**”页面上，选择“**高级设置**”并进行所需的更改。



3. 单击“**确定**”以保存更改。

地址解析类型

您可以指定要从服务器请求的地址类型。默认值为 DnsPort。

在“**高级设置**”窗口中，从“**地址解析类型**”下拉列表中选择一个值。

- Dns
- DnsPort
- IPV4
- IPV4端口
- Dot
- DotPort
- Uri
- NoChange

允许字体平滑

您可以指定是否需要对 HDX™ 会话进行字体平滑处理。默认设置为“开”。

在“**高级设置**”窗口中，选择“**允许字体平滑**”选项，然后单击“**确定**”。

允许会话重新连接

您可以指定是否需要重新连接 HDX 会话。默认设置为“开”。

在“**高级设置**”窗口中，选择“**允许会话重新连接**”选项。

允许特殊文件夹重定向

配置特殊文件夹重定向后，用户可以将服务器的 Windows 特殊文件夹映射到其本地计算机上的文件夹。特殊文件夹是指标准 Windows 文件夹，例如 *\Documents* 和 *\Desktop*，无论操作系统如何，这些文件夹始终以相同的方式显示。

在“**高级设置**”窗口中，选中或清除“**允许特殊文件夹重定向**”选项以启用或禁用特殊文件夹重定向，然后单击“**确定**”。

高级运行状况检查

StoreFront 对每个 Citrix Virtual Apps and Desktops 交付控制器、Cloud Connector 和 Secure Private Access 服务器执行定期运行状况检查，以减少间歇性服务器可用性造成的影响。通过高级运行状况检查，StoreFront 执行更深入的检查，更有可能检测到任何问题。

通过 Cloud Connector 连接到 Citrix Desktops as a Service 时，高级运行状况检查的额外优势在于，它会检索有关哪些 VDA 与 Cloud Connector 位于同一位置的附加信息。如果 Cloud Connector 无法联系 Citrix Desktops as a Service，Cloud Connector 会使用其本地主机缓存来促进与共置 VDA 的连接。StoreFront 使用高级运行状况检查结果中的附加信息来联系最合适的在线连接器以启动应用程序和桌面。

为确保在中断期间资源可用，而无需在每个区域（资源位置）发布资源，请确保在所有 StoreFront 服务器上将站点配置为在服务器列表中包含所有资源位置中的所有云连接器，并启用高级健康检查功能。

高级健康检查默认启用。要启用或禁用高级健康检查，请使用 PowerShell cmdlet Set-STFStoreFarmConfiguration 和参数 `AdvancedHealthCheck`。不建议禁用高级健康检查，因为它会降低弹性。

后台健康检查轮询周期

StoreFront 会对每个 Citrix Virtual Apps and Desktops 交付控制器、Cloud Connector 和 Secure Private Access 服务器运行定期健康检查，以减少间歇性服务器可用性造成的影响。默认值为每分钟 (00:01:00)。在“**高级设置**”窗口中，为“**后台健康检查轮询周期**”指定时间，然后单击“**确定**”以控制健康

检查的频率。要禁用健康检查，请将轮询周期设置为 00:00:00，但不建议这样做。当高级健康检查启用时，不建议将轮询周期设置为较低值，因为它可能会影响性能。

通信超时持续时间

默认情况下，StoreFront 向为应用商店提供资源的服务器发出的请求会在 30 秒后超时。服务器在 1 次不成功的通信尝试后被视为不可用。在“**高级设置**”窗口中，更改默认时间，然后单击“**确定**”以更改这些设置。

连接超时

您可以指定与交付控制器建立初始连接时等待的秒数。默认值为 6。

在“**高级设置**”窗口中，指定建立初始连接时等待的秒数，然后单击“**确定**”

启用增强枚举

此选项控制 StoreFront 在跨多个 Citrix Virtual Apps and Desktops 站点枚举应用程序和桌面时是并发还是顺序查询交付控制器。并发枚举在聚合跨多个站点的资源时可为用户查询提供更快的响应。选中此选项（默认）后，StoreFront 会同时向所有交付控制器发送枚举请求，并在所有控制器都响应后聚合响应。您可以使用“**最大并发枚举数**”和“**并发枚举的最小场数**”选项来调整此行为。

在“**高级设置**”窗口中，选中（或清除）“**启用增强枚举**”选项，然后单击“**确定**”。

启用套接字池

套接字池在应用商店中默认禁用。启用套接字池后，StoreFront 会维护一个套接字池，而不是在每次需要时创建套接字并在连接关闭时将其返回给操作系统。启用套接字池可提高性能，尤其适用于安全套接字层 (SSL) 连接。要启用套接字池，请编辑应用商店配置文件。在“**高级设置**”窗口中选择“**启用套接字池**”选项，然后单击“**确定**”以启用套接字池。

文件类型关联

默认情况下，商店中启用了文件类型关联，以便在用户打开相应类型的本地文件时，内容可以无缝重定向到他们订阅的应用程序。要启用或禁用文件类型关联，请使用 PowerShell 命令 Set-STFStoreFarmConfiguration。例如：

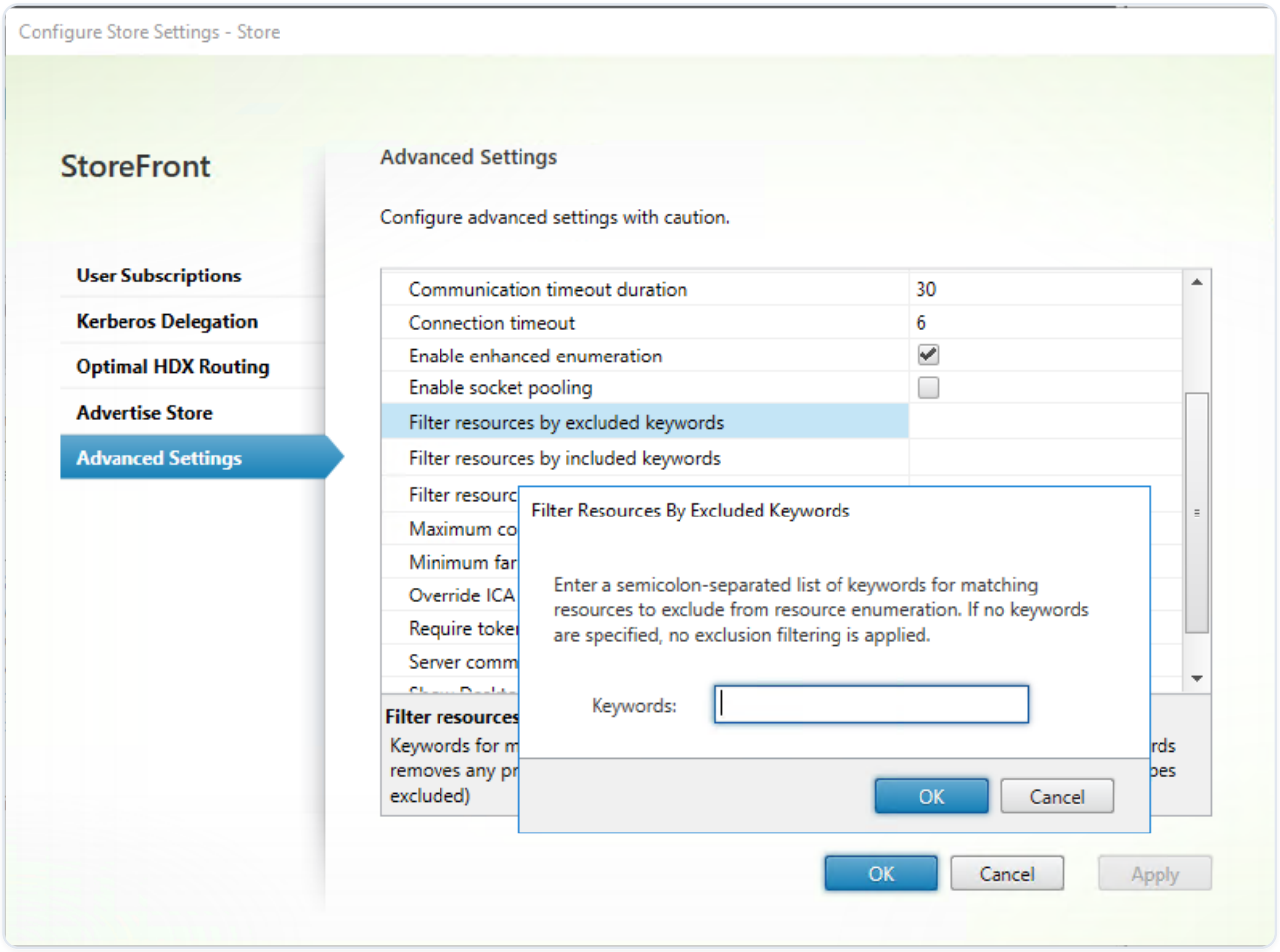
```
$storeService = Get-STFStoreService –VirtualPath '/Citrix/Store'

Set-STFStoreFarmConfiguration $storeService -EnableFileTypeAssociation
$false
```

按排除的关键字筛选资源

您可以按排除的关键字筛选匹配的资源。指定排除关键字会删除任何先前配置的包含关键字。默认情况下不进行筛选（不排除任何资源类型）。

1. 在“**高级设置**”窗口中，找到“**按排除的关键字筛选资源**”行。
2. 单击右侧列以调出“**按排除的关键字筛选资源**”窗口。
3. 在关键字输入框中输入以分号分隔的关键字列表
4. 单击“**确定**”。



要使用 PowerShell 更改设置，请使用 cmdlet Set-STFStoreEnumerationOptions 和参数 `-FilterByKeywordsExclude`。

以下关键字是保留的，不得用于筛选：

- 自动
- 强制性

按包含的关键字筛选资源

您可以按包含的关键字筛选匹配的资源。指定包含关键字会删除任何先前配置的排除关键字。默认情况下不进行筛选（不排除任何资源类型）。

1. 在“**高级设置**”窗口中，找到“**按包含的关键字筛选资源**”行。
2. 单击右侧列以调出“**按包含的关键字筛选资源**”窗口。
3. 在关键字输入框中输入以分号分隔的关键字列表
4. 单击“**确定**”。

要使用 PowerShell 更改设置，请使用 cmdlet Set-STFStoreEnumerationOptions 和参数 `-FilterByKeywordsInclude`。

以下关键字为保留字，不得用于筛选：

- 自动
- 强制性

按类型筛选资源

选择要包含在资源枚举中的资源类型。默认值为“不筛选”（包含所有资源类型）。

在“**高级设置**”窗口中，选择“**按类型筛选资源**”，单击其右侧，选择要包含在枚举中的资源类型，然后单击“**确定**”。

要使用 PowerShell 更改设置，请使用 cmdlet Set-STFStoreEnumerationOptions 和参数 `-FilterByTypesInclude`，并指定资源类型数组（应用程序、桌面或文档）。

最大并发枚举数

指定要发送到所有 Delivery Controller 的最大并发请求数。此选项在启用“**启用增强枚举**”选项时生效。默认值为 0（无限制）。

在“**高级设置**”窗口中，选择“**最大并发枚举数**”，输入一个数字，然后单击“**确定**”。

并发枚举的最小场数

指定触发并发枚举所需的 Delivery Controller 的最小数量。此选项在启用“**启用增强枚举**”选项时生效。默认值为 3。

在“**高级设置**”窗口中，选择“**并发枚举的最小场数**”，输入一个数字，然后单击“**确定**”。

覆盖 ICA® 客户端名称

使用 Web 浏览器生成的唯一 ID 覆盖 .ica 启动文件中的客户端名称设置。禁用时，Citrix Workspace 应用程序会指定客户端名称。默认值为“关”。

从“**高级设置**”窗口中，选择“**覆盖 ICA 客户端名称**”选项，然后单击“**确定**”。

要求令牌一致性

启用后，StoreFront 会强制执行用于身份验证的网关与用于访问应用商店的网关之间的一致性。如果值不一致，用户必须重新进行身份验证。必须为 Smart Access 启用此功能。如果用户通过禁用身份验证的网关访问应用商店，则必须禁用此功能。默认设置为“开”。

从“**高级设置**”窗口中，选择“**要求令牌一致性**”选项，然后单击“**确定**”。

服务器通信尝试次数

指定在将 Delivery Controller 标记为不可用之前尝试与其通信的次数。默认值为 1。

从“**高级设置**”窗口中，选择“**服务器通信尝试次数**”，输入一个数字，然后单击“**确定**”。

为旧版客户端显示 Desktop Viewer

指定当用户从旧版客户端访问其桌面时是否显示 Citrix Desktop Viewer 窗口和工具栏。默认设置为“关”。

从“**高级设置**”窗口中，选择“**为旧版客户端显示 Desktop Viewer**”选项，然后单击“**确定**”。

将桌面视为应用程序

指定访问应用商店时，桌面是显示在“应用程序”视图中还是“桌面”视图中。默认设置为“关”。

从“**高级设置**”窗口中，选择“**将桌面视为应用程序**”选项，然后单击“**确定**”。

联合身份验证服务配置

联合身份验证服务 (FAS) 使用证书身份验证为 VDA 提供单点登录。这在使用 SAML 等身份验证方法时非常有用，因为 StoreFront 无法访问 Active Directory 凭据。

为应用商店启用 FAS

在为应用商店启用 FAS 之前，您必须使用组策略配置 FAS 服务器列表。有关详细信息，请参阅 (/zh-cn/federated-authentication-service/current-release/install-configure#configure-group-policy)。

要为应用商店启用 FAS，您必须使用 PowerShell cmdlet Set-STFStoreLaunchOptions 将 VDA 登录数据登录提供程序设置为 `FASLogonDataProvider`。

例如，要为应用商店启用 FAS 并在登录时选择服务器：

```
$store = Get-STFStoreService -VirtualPath [VirtualPath]

Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider
"FASLogonDataProvider"
```

要禁用应用商店的 FAS：

```
$store = Get-STFStoreService -VirtualPath [VirtualPath]

Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider ""
```

将 `[VirtualPath]` 替换为相应的虚拟路径，例如 `/Citrix/Store`。

当在启用了 FAS 的应用商店中使用 (/zh-cn/storefront/2507-ltsr/stores/authentication/username-password.html) 时，StoreFront 始终使用 FAS 而不是提供的凭据进行单点登录。

在登录时选择 FAS 服务器

默认情况下，StoreFront 在启动时选择 FAS 服务器。您可以更改此设置，以便 StoreFront 在登录时选择 FAS 服务器。这通常不是必需的，但如果 FAS 选择速度较慢，为避免启动延迟，您可以启用此功能。要配置此行为，请运行 PowerShell cmdlet Set-STFClaimsFactoryNames，并使用参数 `ClaimsFactoryName`。要在登录时选择 FAS 服务器，请将其设置为 `FASClaimsFactory`。要恢复默认行为并在启动时选择 FAS 服务器，请将其设置为 `standardClaimsFactory`。

例如，要在登录时选择 FAS 服务器：

```
$store = Get-STFStoreService -VirtualPath [VirtualPath]

$auth = Get-STFAuthenticationService -StoreService $store

Set-STFClaimsFactoryNames -AuthenticationService $auth -ClaimsFactoryName
"FASClaimsFactory"
```

FAS 服务器不可用

如果 FAS 服务器不可用，则启动默认会失败。但是，您可以配置 StoreFront，以便在 FAS 服务器不可用时，用户可以通过输入其凭据登录到 VDA。要更改配置，请使用 PowerShell cmdlet Set-

STFStoreLaunchOptions 和参数 `FederatedAuthenticationServiceFailover`。例如，要为应用商店启用故障转移：

```
$storeService = Get-STFStoreService -VirtualPath [VirtualPath]

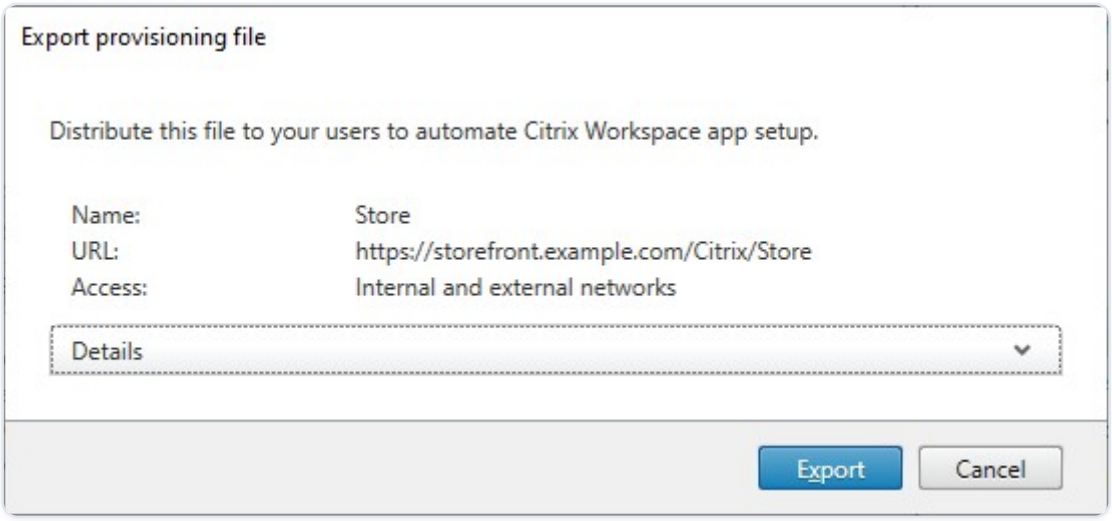
Set-STFStoreLaunchOptions $storeService
-FederatedAuthenticationServiceFailover $True
```

为用户导出应用商店预配文件

您可以生成包含应用商店连接详细信息的文件，包括为应用商店配置的任何 Citrix Gateway 部署和信标。将这些文件提供给用户，以便他们可以使用应用商店的详细信息自动配置 Citrix Workspace 应用程序。用户还可以通过 Web 浏览器访问应用商店网站时下载 Citrix Workspace 应用程序预配文件。

生成包含单个应用商店详细信息的预配文件

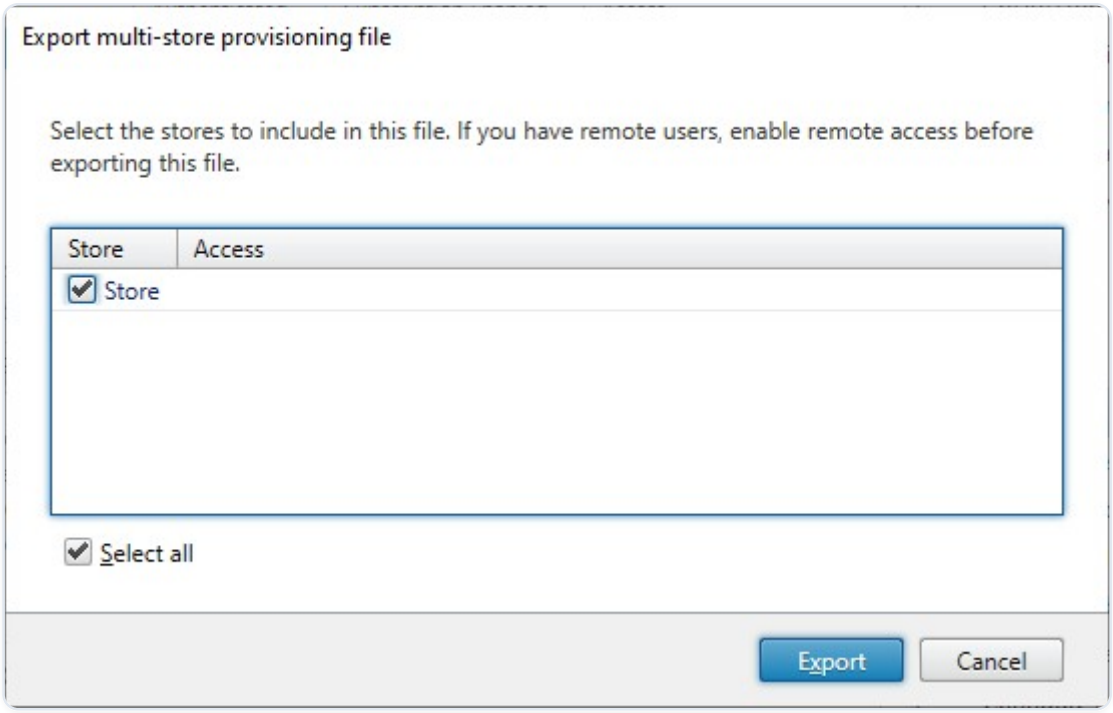
1. 在 StoreFront 管理控制台中，选择“**应用商店**”节点。
2. 选择要为其导出预配文件的应用商店。
3. 在“**操作**”窗格中，选择“**导出预配文件**”。
4. 选择“**导出**”。
5. 选择保存文件的位置，然后选择“**保存**”。



为多个应用商店生成预配文件：

1. 在 StoreFront 管理控制台中，选择“**应用商店**”节点。
2. 在“操作”窗格中，单击“**导出多应用商店预配文件**”。
3. 选择要包含在文件中的应用商店。

4. 选择“**导出**”。
5. 选择保存文件的位置，然后选择“**保存**”。



配置会话设置

当用户启动应用程序时，StoreFront 会生成一个文档（称为 ICA 文件），其中包含 Citrix Workspace 应用程序启动和配置该会话所需的所有设置。

在大多数情况下，建议使用 Citrix Virtual Apps and Desktops Policies 或 Citrix DaaS Policies 修改会话设置。但在某些情况下，为特定应用商店覆盖这些设置会很有用。如果应用商店聚合了来自多个站点的资源，并且您希望将相同的设置应用于该应用商店的所有资源，这会很有用。

要为应用商店定义会话设置，请执行以下操作之一：

- 使用全局应用程序配置服务。这是 Citrix Cloud 上的一项服务。有关更多详细信息，请参阅 使用全局应用程序配置服务配置 Citrix Workspace 应用程序。
- 在 StoreFront 服务器上，将设置添加到应用商店的 default.ica 文件中。

您可以在 StoreFront 服务器的 `\inetpub\wwwroot\Citrix\[StoreName]\App_Data` 目录中找到 default.ica。

有关可用设置的列表，请参阅 ICA 设置参考。某些设置全局适用。您还可以通过添加一个名称与 Studio 中配置的应用程序名称完全匹配的部分，来添加适用于特定应用程序的部分。

示例：在窗口模式下启动记事本

要在 default.ica 中配置应用程序以窗口模式启动，请为该应用程序添加一个包含以下设置的部分：

- TWIMode - 设置为 Off 以启用窗口模式。
- DesiredHRES - 可选的水平像素数。
- DesiredVRES - 可选的垂直像素数。

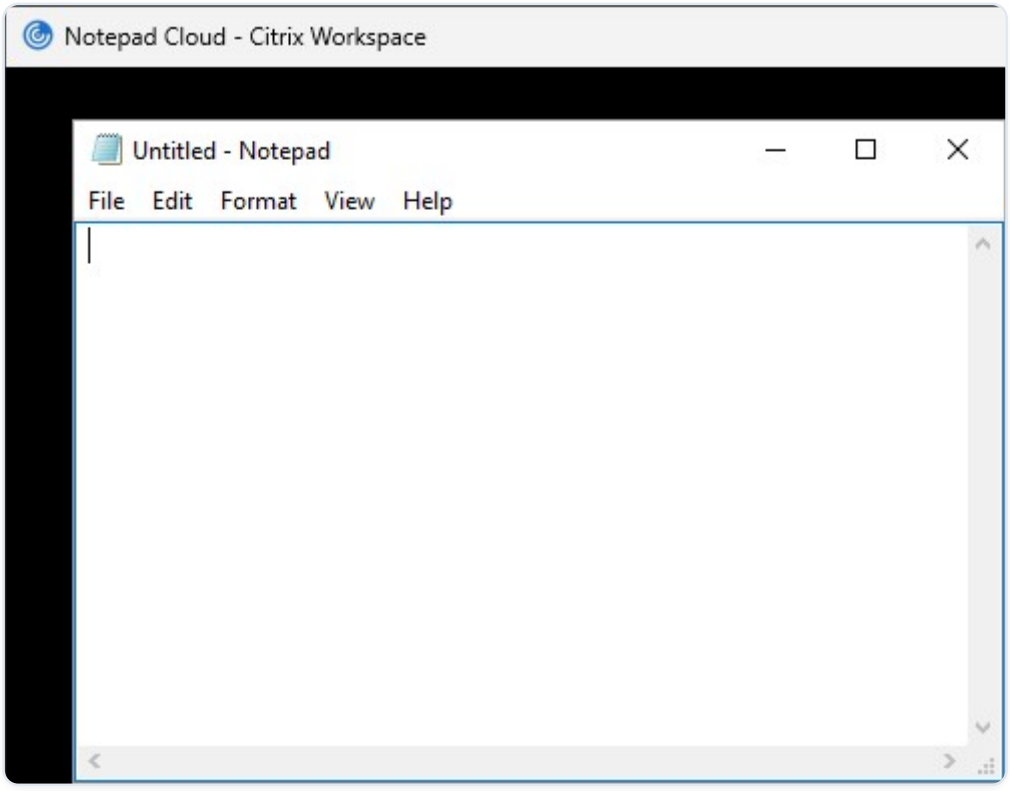
例如：

```
[Notepad]

TWIMode=Off

DesiredHRES=1024

DesiredVRES=768
```



Citrix Workspace™ 应用程序配置

全局应用程序配置服务

全局应用程序配置服务是一种用于管理 Citrix Workspace 应用程序配置的云服务。在您的 Citrix Cloud 帐户中，您可以声明您的应用商店 URL 并为每个应用商店定义配置。有关更多详细信息，请参阅配置本地应用商店的设置。

应用商店帐户设置

作为全局应用程序配置服务的替代方案，您可以通过应用商店帐户设置配置 Citrix Workspace 应用程序。当用户将应用商店添加到本地安装的 Citrix Workspace 应用程序时，它会检索应用商店帐户设置 StoreFront。这可以包括配置属性，例如告知适用于 Windows 的 Citrix Workspace 应用程序是否应为应用程序创建开始菜单快捷方式。有关属性的详细信息，请参阅 Workspace 应用程序文档，例如使用 StoreFront 帐户设置自定义应用程序快捷方式位置。

要修改这些设置：

1. 在 `C:\inetpub\wwwroot\Citrix\Roaming` 中打开 web.config 文件。
2. 在 `<Accounts>` 部分中，找到要更改的应用商店的元素 `<account ... name="Store" ...>`。
3. 在 `Account` 部分下，找到 `<annotatedServices>/<annotatedServiceRecord>/<metadata>/<properties>` 部分。
4. 在 `<clear/>` 元素之后，添加 `<property name="[name]" value="[value]"/>` 形式的属性。例如：

```
<properties>

    <clear/>

    <property name="PutShortcutsOnDesktop" value="true"/>

    <property name="DesktopDir" value="Citrix Applications"/>

</properties>
```

重要

> 在多服务器部署中，一次只能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，将您的配置更改传播到服务器组，以便更新部署中的其他服务器。

Workspace 应用程序网站

要配置本地安装的 Citrix Workspace 应用程序使用的网站配置，请参阅配置 Workspace 应用程序网站。

与 Citrix Gateway 和 NetScaler ADC 集成

将 Citrix Gateway 与 StoreFront 结合使用，为企业网络外部的用户提供安全的远程访问，并使用 NetScaler ADC 提供负载平衡。

任务	详细信息
导入 思杰网关	从 Citrix Gateway 导出配置并将其导入 StoreFront
管理 思杰网关	添加、删除和编辑 Citrix Gateway 连接设置
使用 NetScaler ADC 进行负载平衡	将 NetScaler ADC 配置为 StoreFront 服务器组前的负载平衡器
为委派表单身份验证 (DFA) 配置 NetScaler ADC 和 StoreFront	
使用不同域进行身份验证	配置 StoreFront 和 Citrix Gateway，以便用户首先在一个域上通过网关进行身份验证，然后在一个不同的域上向 StoreFront 进行身份验证。
配置信标点	配置信标 URL，Citrix Workspace 应用程序可以使用这些 URL 来确定它是在企业网络内部还是外部。
创建内部和外部使用的单个 FQDN	创建一个单一的完全限定域名 (FQDN)，该域名可以直接从企业网络内部访问应用商店，也可以通过 Citrix Gateway 远程访问。
通过网关连接时要求 Citrix Workspace 应用程序(/zh-cn/storefront/2507-ltsr/integrate-with-citrix-gateway-and-citrix-adc/require-app.html)	
通过 OIDC 进行 Entra ID 身份验证以及对 VDA 的单点登录(/zh-cn/storefront/2507-ltsr/integrate-with-citrix-gateway-and-citrix-adc/entra-id-oidc.html)	

配置 Citrix 网关

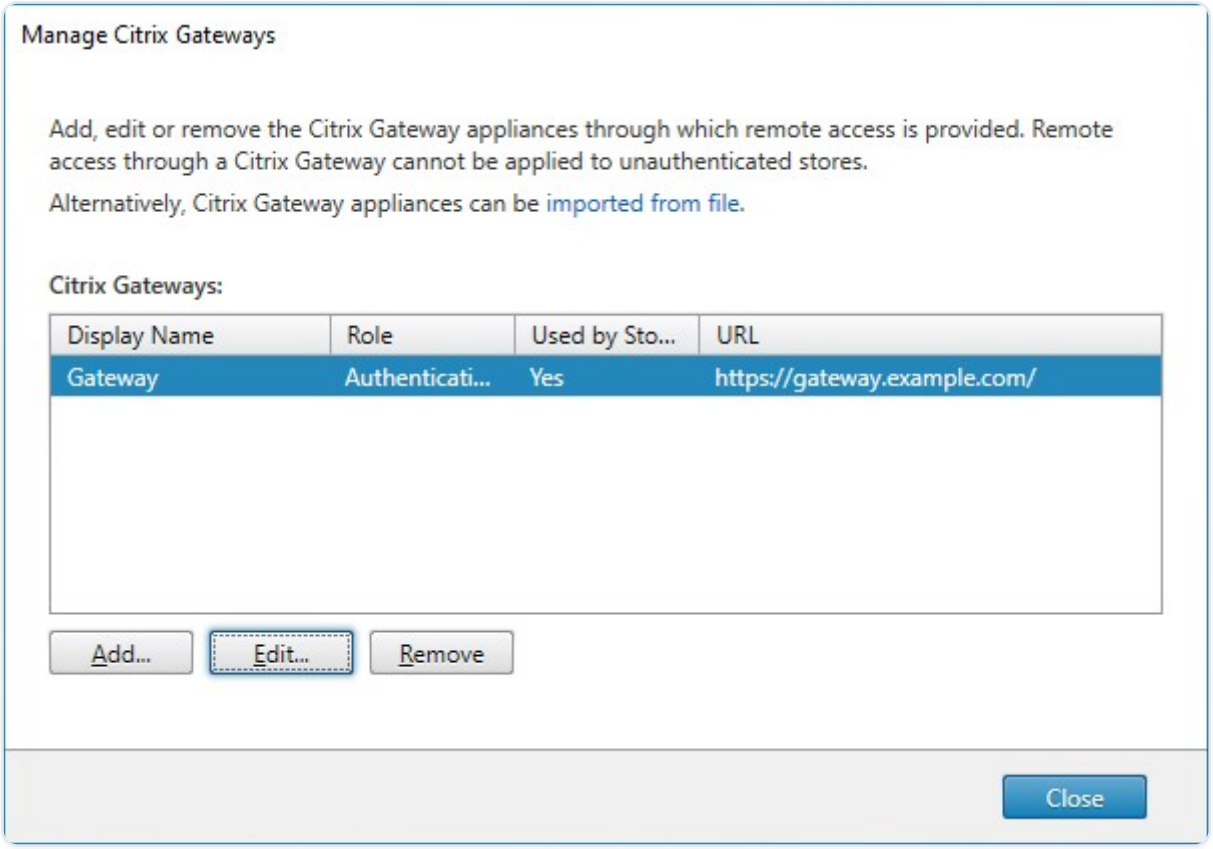
使用 Citrix Gateway 为 StoreFront 和您的虚拟投递代理 (VDA) 提供身份验证和远程访问。Citrix Gateway 在硬件或软件 NetScaler ADC 上运行。Citrix Gateway Service 由 Citrix 管理，可用于 HDX 路由，但不能用于 StoreFront 的身份验证或远程访问。

有关配置您的 Gateway 的详细信息，请参阅将 NetScaler Gateway 与 StoreFront 集成。

您必须在 StoreFront 中配置您的网关，然后 StoreFront 才能允许通过该网关进行访问。

查看网关

要查看在 StoreFront 中配置的网关，请在 Citrix StoreFront 管理控制台的左窗格中选择“应用商店”节点，然后单击“**管理 Citrix Gateway**”。这将显示“**管理 Citrix Gateway**”窗口。



PowerShell

要获取网关及其配置的列表，请调用 Get-STFRoamingGateway。

添加 Citrix Gateway 设备

1. 在“**管理 Citrix Gateway**”窗口中，单击“**添加**”。
2. 在“常规设置”选项卡上输入设置，然后按“**下一步**”。

- 为 Citrix Gateway 部署指定一个“**显示名称**”，以帮助用户识别它。

  用户在 Citrix Workspace 应用程序中会看到您指定的显示名称，因此请在名称中包含相关信息，以帮助用户决定是否使用该部署。例如，您可以在 Citrix Gateway 部署的显示名称中包含地理位置，以便用户可以轻松识别最适合其位置的部署。

- 将“**网关类型**”设置为“**Citrix Gateway 设备**”。
- 输入网关的 URL。

  您的 StoreFront 部署的完全限定域名 (FQDN) 必须是唯一的，并且不同于 Citrix Gateway 虚拟服务器的 FQDN。StoreFront 和 Citrix Gateway 虚拟服务器使用相同的 FQDN 是不受支持的。网关会将 URL 添加到 `X-Citrix-Via` HTTP 标头。StoreFront 使用此标头来确定正在使用哪个网关。

  使用 GUI 只能添加一个网关 URL。如果网关可以通过多个 URL 访问，则需要添加两次相同的网关，除了 URL 之外，配置完全相同。为了简化配置，您可以配置一个用于访问网关的辅助 URL。此选项无法通过 GUI 使用，因此您必须使用 PowerShell 进行配置。在运行任何 PowerShell 命令之前，您应该关闭管理控制台。例如，如果您在全球服务器负载均衡器后面有多个网关，通常，添加 GSLB URL 和可用于访问每个特定区域网关的 URL 都很有用，例如用于测试或故障排除目的。创建网关后，您可以使用 `Set-STFRoamingGateway` 添加一个额外的 URL，其中 `-GSLBurl` 参数用于辅助 URL。尽管该参数名为 `GSLBurl`，但它可用于任何您希望添加第二个 URL 的情况。例如：

  ```
  Set-STFRoamingGateway -Name "Europe Gateway" -GSLBurl
  "eugateway.example.com" -GatewayUrl "gslb.example.com"
  ```

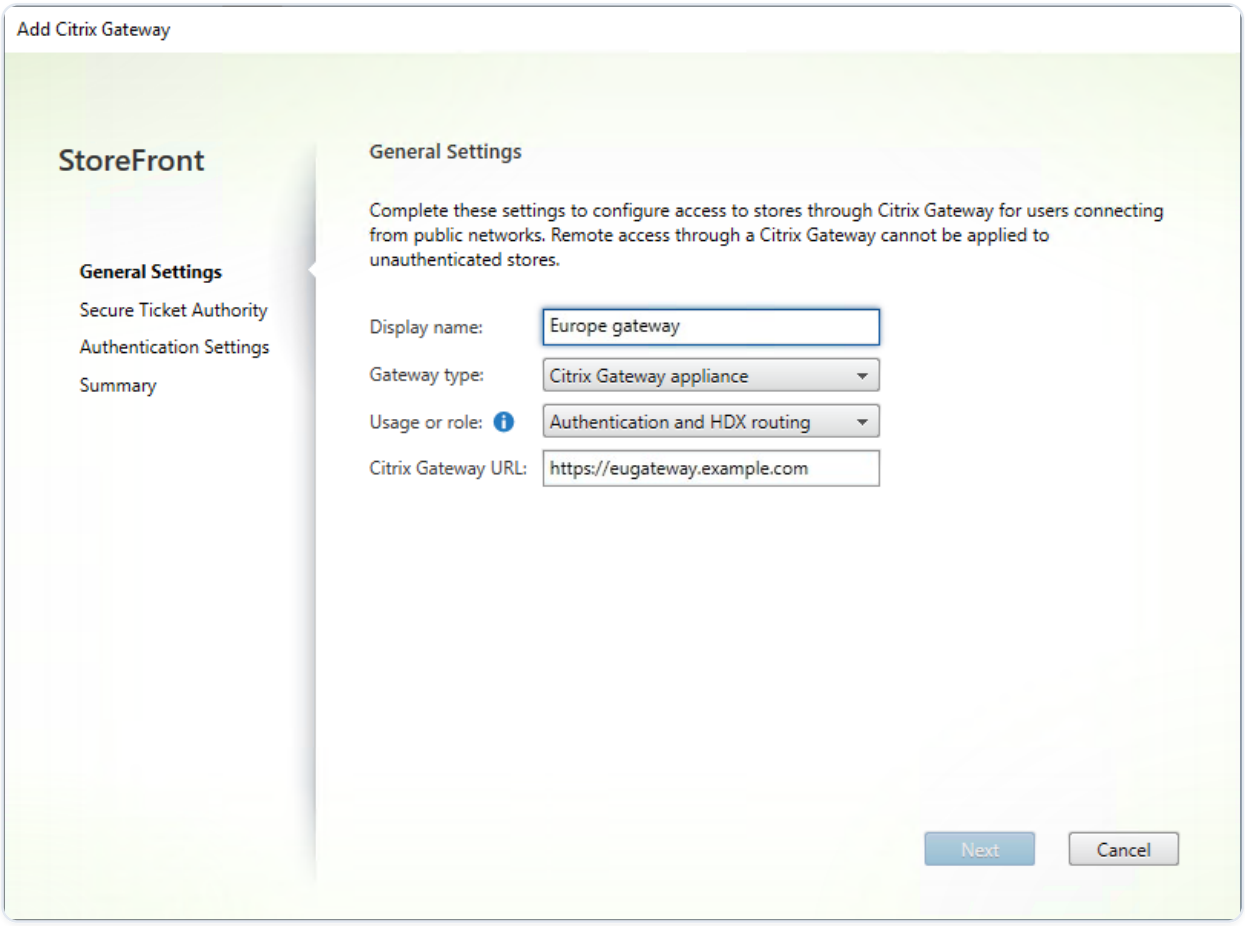
  注意：

  在此示例中，与直觉相反，`GSLBurl` 参数包含区域 URL，而 `GatewayUrl` 参数包含 GSLB URL。在大多数情况下，URL 被视为相同，如果商店仅通过 Web 浏览器访问，则可以以任何一种方式配置它们。但是，当通过 Citrix Workspace 应用程序访问 StoreFront 时，它会从 StoreFront 读取 `GatewayUrl` 并随后将其用于远程访问，并且最好将其配置为始终连接到 GSLB URL。

  如果您需要两个以上的 URL，则需要将其配置为单独的网关。

- 选择用途或角色：

用途或角色	描述
身份验证和 HDX 路由	使用网关同时提供对 StoreFront 的远程访问和对 VDA 的访问。
仅身份验证	如果网关仅用于对 StoreFront 的远程访问，请选择此项。此选项会阻止 Citrix Workspace 启动器 工作。因此，如果您需要使用混合启动，即使网关仅用于身份验证，也请选择 **身份验证和 HDX 路由**。
仅 HDX 路由	如果网关仅用于向 VDA 提供 HDX 访问，例如在没有 StoreFront 实例的站点，请选择此项。



3. 填写“**安全票证颁发机构**”选项卡上的设置。

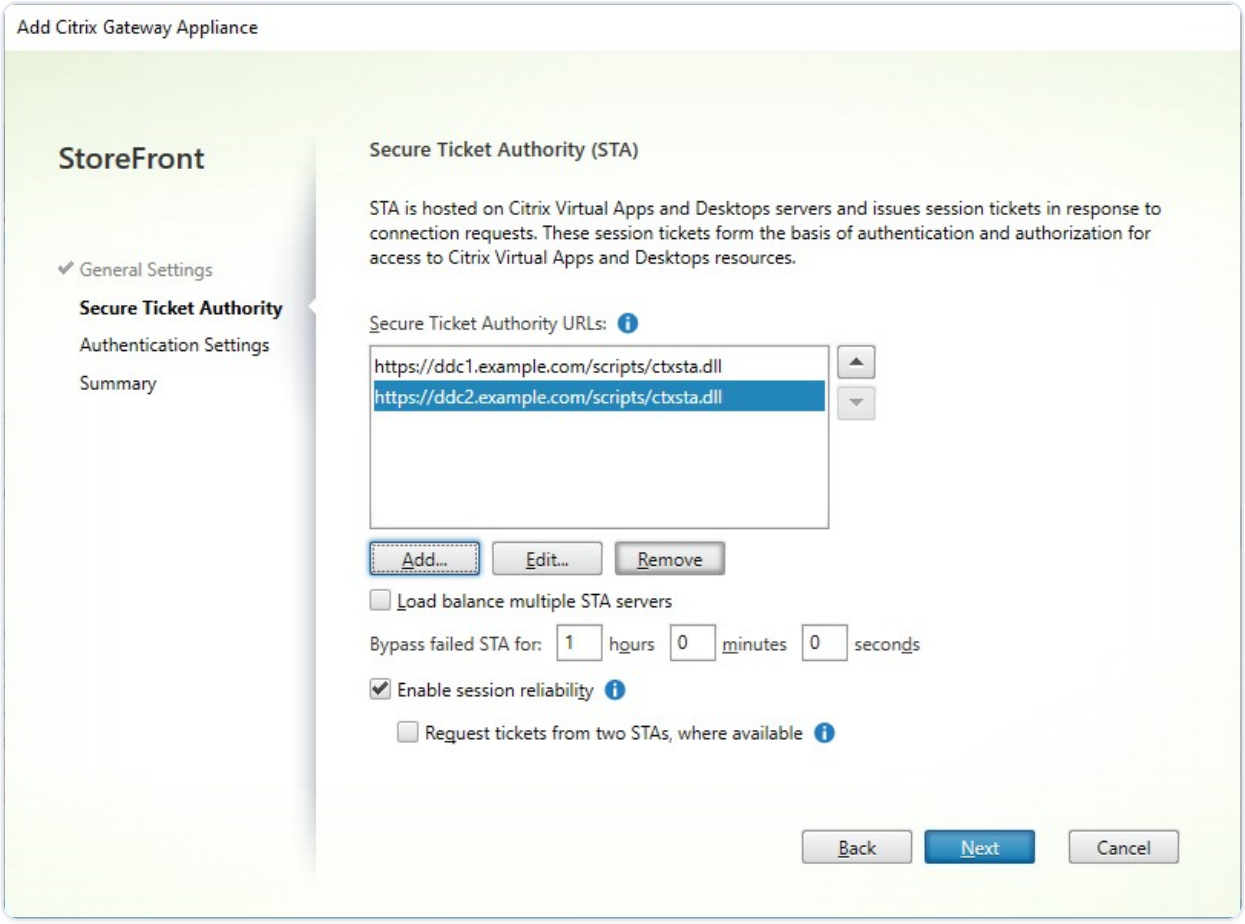
   安全票证颁发机构响应连接请求颁发会话票证。这些会话票证构成了 Citrix Workspace 应用程序检测和访问 VDA 的身份验证和授权基础。

   - 输入一个或多个安全票证颁发机构服务器 URL。

  - 如果您正在使用 Citrix Virtual Apps and Desktops™，则可以将交付控制器用作 STA 服务器。
  - 如果您正在使用 Citrix Desktop as a Service，则可以将云连接器用作 STA 服务器。这些服务器要么将请求代理到 Citrix Cloud™ 票证颁发机构，要么在 LHC 模式下生成自己的票证。将来，这将发生变化，以便它们始终生成自己的票证以提高弹性。
  - 建议您至少使用 2 个 STA 服务器以实现冗余。
  - 当使用云连接器作为 STA 服务器时，建议您在至少一个资源位置中包含所有云连接器。首先，在资源位置内，Citrix Cloud 确保一次只升级一个云连接器，因此包含所有连接器可确保始终至少有一个连接器未在升级。其次，如果资源位置进入 LHC 模式，则只有指定为“选定代理”的单个云连接器才能颁发 STA 票证。由于您无法提前知道这将是哪个连接器，因此请在资源位置中包含所有云连接器。
  - 确保 StoreFront 中列出的所有 STA 服务器也作为 STA 服务器列在 Citrix Gateway 虚拟服务器中。如果 Citrix Gateway 中缺少任何服务器，则可能导致启动失败。目前，当使用云连接器作为 STA 时，这在正常使用中可能不明显，因为任何连接器都可以用于从 Citrix Cloud 票证颁发机构兑换票证。但是，在本地主机缓存模式下，连接器会生成自己的票证，将来这将成为默认行为。
  - 交付控制器或云连接器可能已配置为 StoreFront 必须包含安全密钥。无法使用 GUI 添加安全密钥；有关使用 PowerShell 添加安全密钥的步骤，请参阅后面的步骤。

- 选择 **负载平衡多个 STA 服务器** 以在 STA 服务器之间分发请求。如果未选中，则 StoreFront 将按照列出的顺序尝试服务器。
- 如果 StoreFront 无法访问 STA 服务器，则它会在一段时间内避免使用该服务器。默认情况下，此时间为 1 小时，但您可以自定义此值。
- 如果您希望 Citrix Virtual Apps and Desktops 在 Citrix Workspace 应用程序尝试自动重新连接时保持断开连接的会话打开，请选择 **启用会话可靠性**。
- 如果您配置了多个 STA，可以选择 **从两个 STA 请求票证（如果可用）**。

  选中 **从两个 STA 请求票证（如果可用）** 后，StoreFront 会从两个不同的 STA 获取会话票证，这样即使一个 STA 在会话期间变得不可用，用户会话也不会中断。如果 StoreFront 因任何原因无法联系到两个 STA，它将回退到使用单个 STA。



填写完设置后，按 **下一步**

4. 填写 **身份验证设置** 选项卡上的设置。

   - 选择 NetScaler® **版本**。
   - 如果存在具有相同 URL 的多个网关（通常在使用全局服务器负载平衡器时），并且您已输入回调 URL，则必须输入网关的 VIP。这允许 StoreFront 确定请求来自哪个网关，从而确定使用回调 URL 联系哪个服务器。否则，您可以将其留空。
   - 从“**登录类型**”列表中选择您在设备上为 Citrix Workspace 应用程序用户配置的身份验证方法。

   您提供的有关 Citrix Gateway 设备配置的信息将添加到应用商店的预配文件中。这使得 Citrix Workspace 应用程序在首次联系设备时能够发送相应的连接请求。

   - 对于 LDAP 身份验证，请选择“**域**”。
   - 对于本机 OTP 身份验证，请选择“**安全令牌**”。
   - 对于 LDAP 加 OTP 身份验证，请选择“**域和安全令牌**”。
   - 对于通过短信进行的 OTP 身份验证，请选择“**短信身份验证**”。
   - 对于证书身份验证，请选择“**智能卡**”。
   - 对于 SAML 身份验证，请选择“**域**”。

- 对于 OIDC 身份验证，请选择“**域**”。

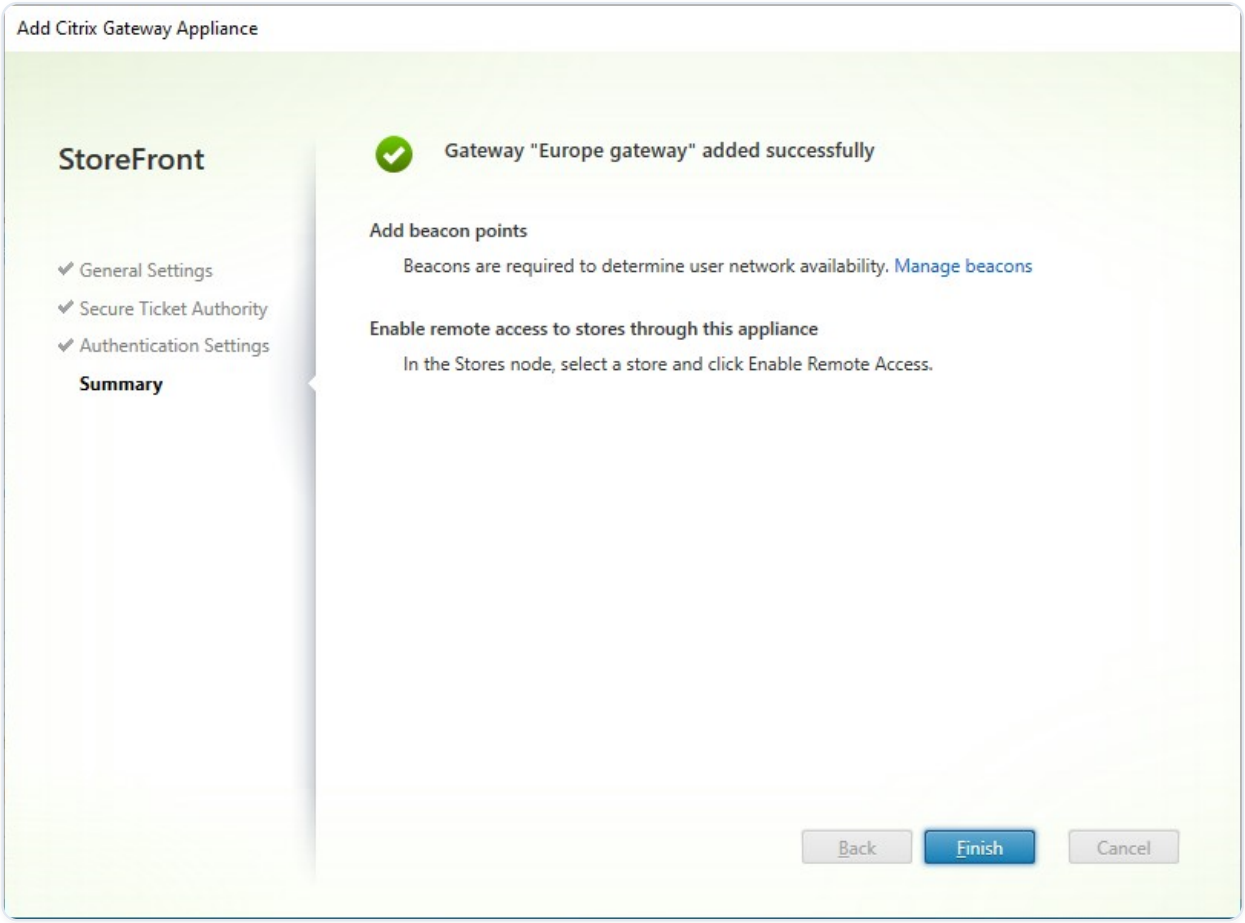
如果您配置了智能卡身份验证，并带有一个辅助身份验证方法，用户在智能卡出现任何问题时可以回退到该方法，请从“智能卡回退”列表中选择辅助身份验证方法。

- （可选）在“回调 URL”框中输入网关的内部可访问 URL。这允许 StoreFront 联系 Citrix Gateway 身份验证服务，以验证从 Citrix Gateway 收到的请求是否源自该设备。智能访问以及智能卡或 SAML 等无密码身份验证方案需要此项，否则可以将其留空。如果您有多个具有相同 URL 的 Citrix Gateway，则此 URL 必须用于特定的网关服务器。

添加网关设备屏幕身份验证设置选项卡的屏幕截图(/en-us/storefront/2507-ltsr/media/integrate-with-citrix-gateway-and-citrix-adc/gateway-authentication.png)

填写完设置后，按“**下一步**”

5. 单击“**创建**”以应用配置。



6. 应用部署后，单击“**完成**”。
7. 如果您已配置安全密钥（推荐），则必须关闭管理控制台并使用 PowerShell 配置它们。例如：

```
$gateway = Get-STFRoamingGateway -Name [Gateway name]

$sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

$sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs
$sta1,$sta2
```

8. 要让用户通过网关访问您的应用商店，请配置远程用户访问。
9. 默认情况下，StoreFront 使用对用户进行身份验证的网关进行 HDX 路由以访问其资源。您可以选择配置 StoreFront，以便在使用最佳 HDX 路由访问特定资源时使用该网关。

PowerShell

要使用 PowerShell 添加网关，请运行 cmdlet New-STFRoamingGateway。

添加 Citrix Gateway 服务

如果您已在 Citrix Cloud 中启用了适用于 StoreFront 的 Citrix Gateway Service，则必须将其配置为 StoreFront 中的网关。

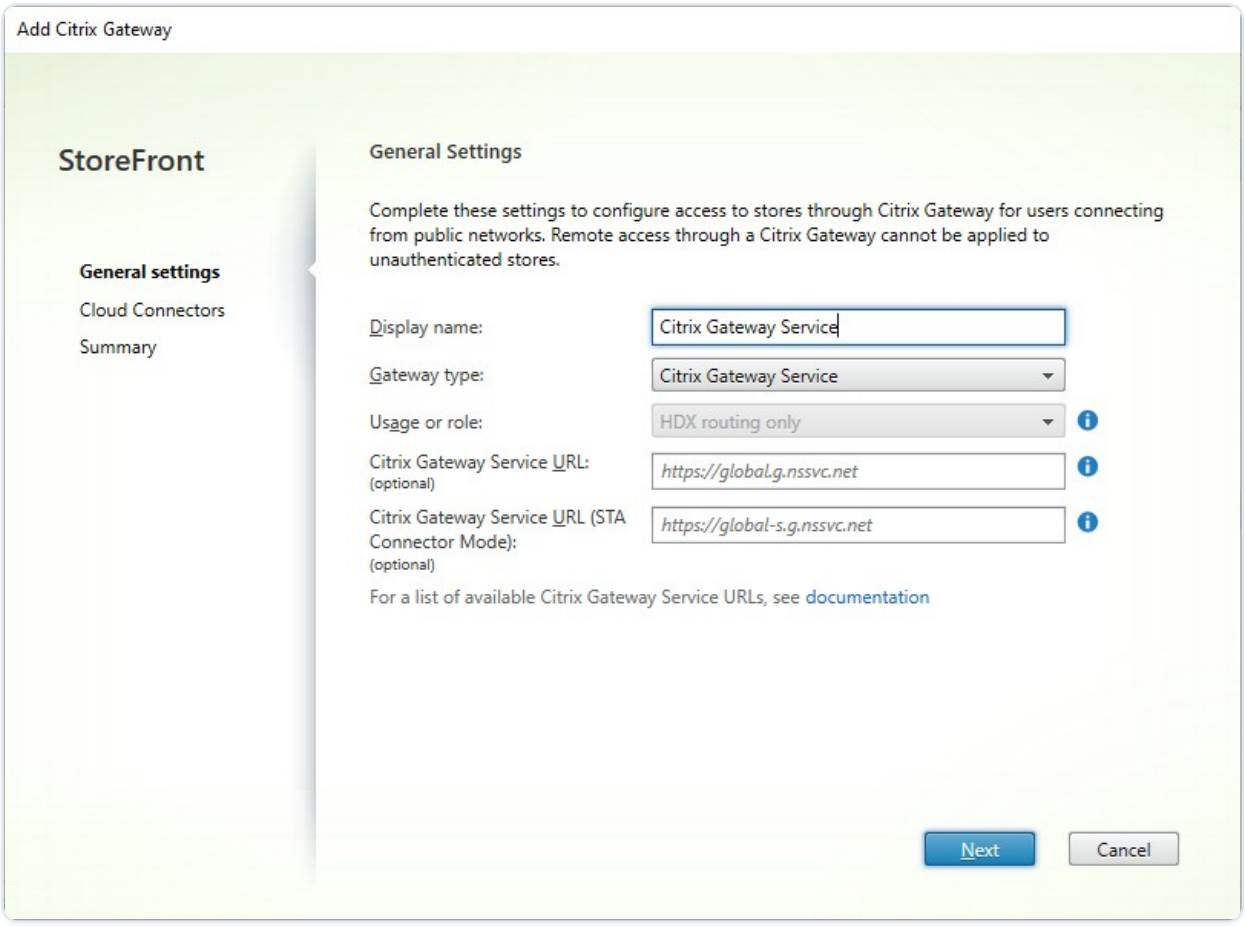
1. 在“**管理 Citrix 网关**”窗口中，单击“**添加**”。
2. 在“常规设置”选项卡上，输入设置，然后按“**下一步**”。

   - 为 Citrix Gateway 部署指定一个**显示名称**，以帮助用户识别它。

     用户会在 Citrix Workspace 应用程序中看到您指定的显示名称，因此请在名称中包含相关信息，以帮助用户决定是否使用该部署。例如，您可以在 Citrix Gateway 部署的显示名称中包含地理位置，以便用户可以轻松识别对其位置最方便的部署。

   - 将“**网关类型**”设置为“**Citrix Gateway Service**”。这将导致“**用法或角色**”设置为“**仅 HDX™ 路由**”并禁用“**Citrix Gateway URL**”。
   - （可选）输入一个**Citrix Gateway Service URL**。如果 URL 留空，则它将使用默认的商业 URL `https://global.g.nssvc.net`，该 URL 会为用户的位置选择最佳的接入点。如果您希望使用特定的网关区域，例如针对特定区域，则可以在此处输入其 URL。有关可用网关服务 URL 的列表，请参阅Citrix Gateway Service 文档。
   - 如果您已输入**Citrix Gateway 服务 URL**，则还必须输入相应的**Citrix Gateway 服务 URL (STA 连接器模式)**。这指定了当云连接器无法访问 Citrix Cloud 时要使用的网关服务 URL，

因此它会发出自己的 STA 票证。如果 URL 留空，则使用默认 URL `https://global-s.g.nssvc.net`。



3. 填写**云连接器**选项卡上的设置。

云连接器允许 StoreFront 访问 Citrix Cloud 以查找网关配置，并访问云票证颁发机构以请求会话票证。

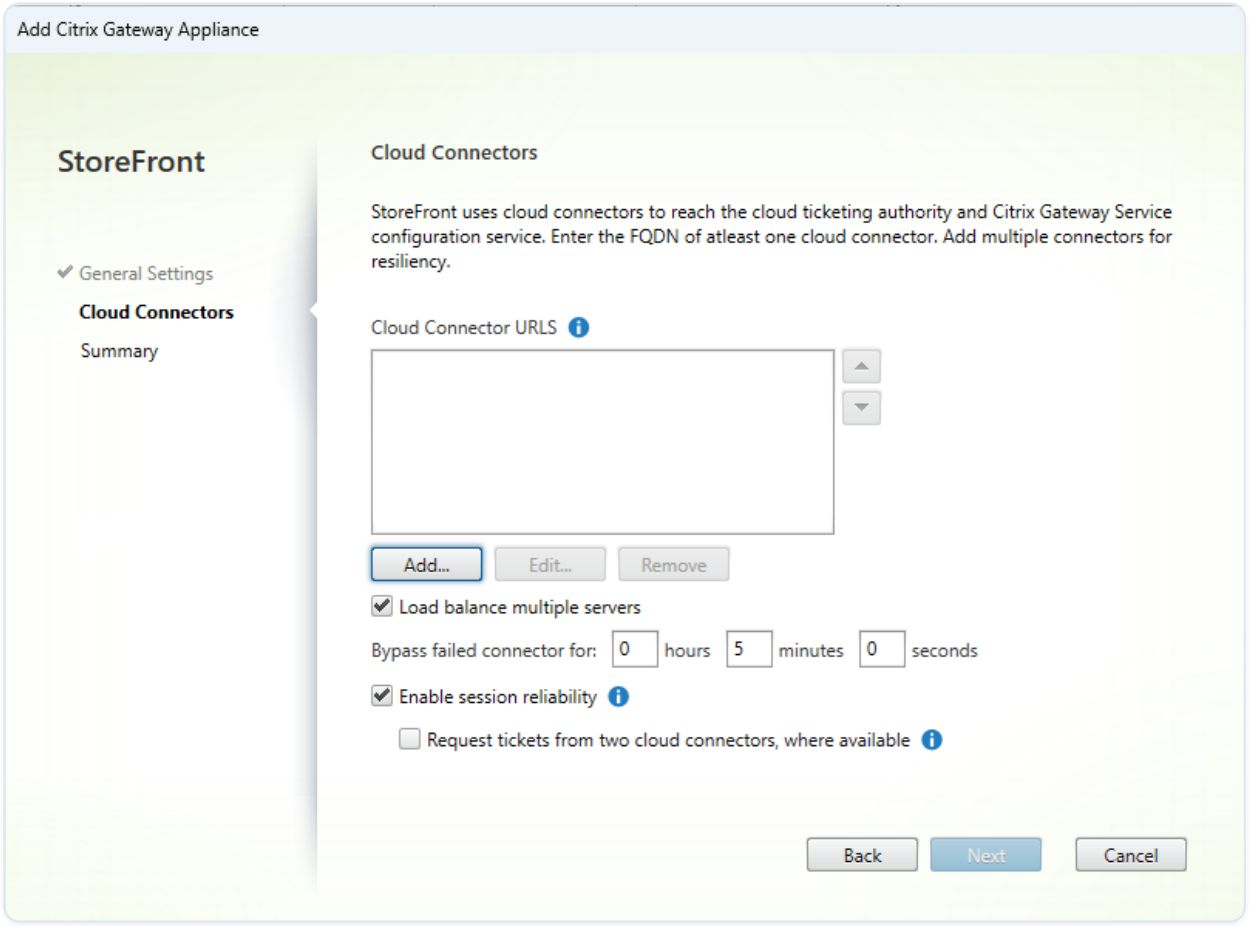
- 输入至少一个云连接器服务器 URL。

  StoreFront 调用这些云连接器以检索 STA 票证，Citrix Workspace 应用程序可以使用这些票证通过 Citrix Gateway 验证请求。在正常操作中，云连接器将请求代理到 Citrix Cloud 票证颁发机构，或者在 LHC 模式下生成自己的票证。将来，这将发生变化，以便它们始终生成自己的票证以提高弹性。

  - 建议您在同一资源位置中包含多个云连接器，因为每个资源位置中一次只升级一个云连接器，从而确保至少有一个云连接器始终可用。为了进一步提高冗余性，请在多个资源位置中添加云连接器。
  - 您可以添加一个负载平衡器，在某个位置的云连接器之间分配请求，而不是单独列出资源位置中的每个云连接器。但是，在 Citrix Gateway VServer 配置中，您必须单独列出每个连接器。

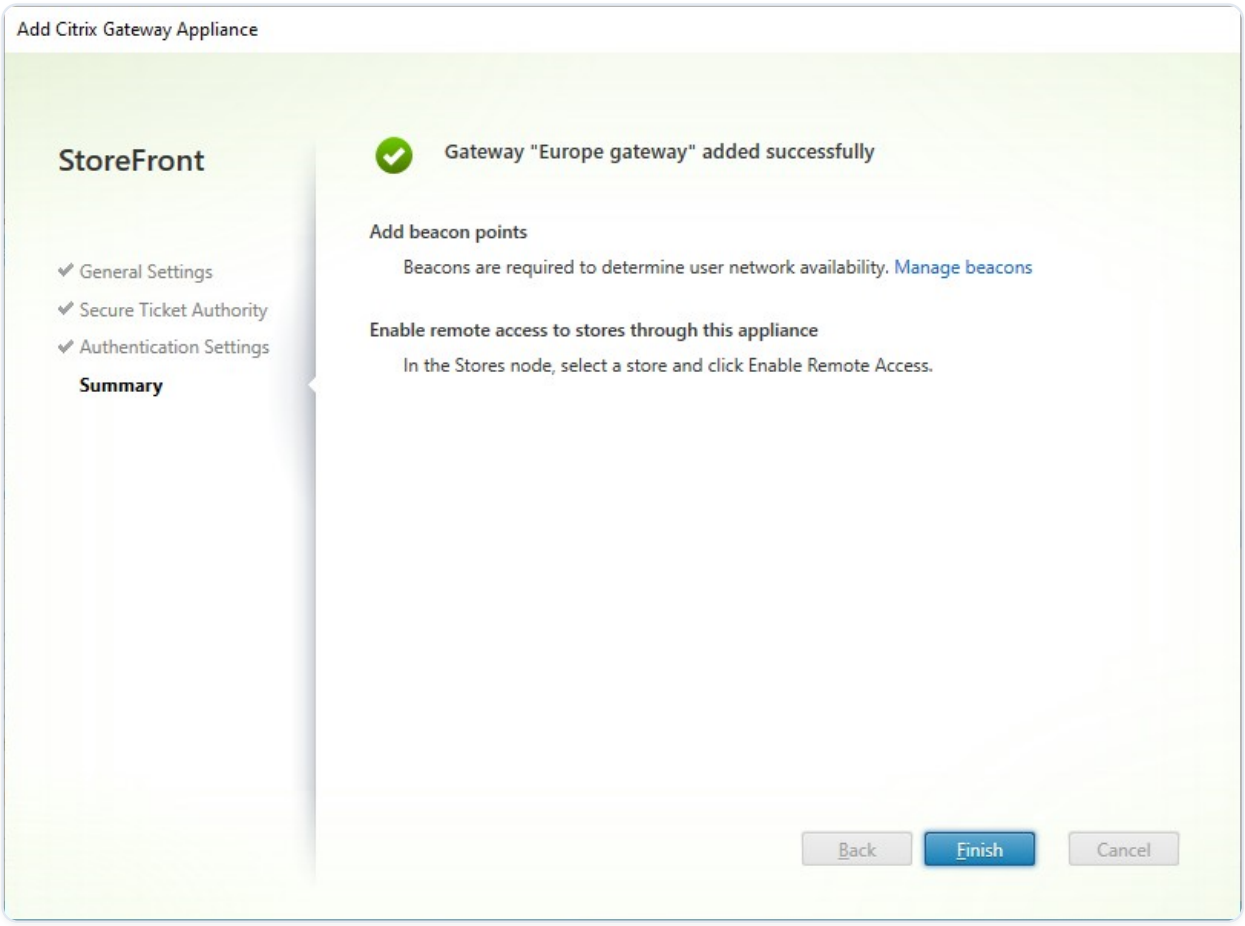
- Citrix DaaS 可以配置为 StoreFront 必须包含安全密钥。无法使用 GUI 添加安全密钥；有关使用 PowerShell 添加安全密钥的步骤，请参阅后面的步骤。

- 选择**负载平衡多个服务器**以在服务器之间分配请求。如果清除此选项，StoreFront 将按照列出的顺序尝试服务器。
- 如果 StoreFront 无法访问服务器，则会在一段时间内避免使用该服务器。默认情况下，此时间为 1 小时，但您可以自定义此值。
- 可选地选择**启用会话可靠性**。
- 可选地选择**从两个云连接器请求票证（如果可用）**。



填写完设置后，选择**下一步**

4. 选择 **创建** 以应用配置。



5. 部署应用后，选择 **完成**。
6. 如果您已配置 安全密钥（建议），则必须关闭管理控制台并使用 PowerShell 配置它们。例如：

```
$gateway = Get-STFRoamingGateway -Name [Gateway name]

$sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

$sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs
$sta1,$sta2
```

7. 默认情况下，StoreFront 使用与用于身份验证相同的网关来访问资源，因此从不使用 Citrix Gateway 服务。您必须使用 最佳 HDX 路由 来配置 StoreFront 何时应使用 Citrix Gateway 服务。

PowerShell

要使用 PowerShell 添加网关，请运行 cmdlet New-STFRoamingGateway，设置 `-IsCloudGateway $true`。

编辑 Citrix 网关

1. 在 **管理 Citrix Gateway** 窗口中，单击要更改的网关，然后按 **编辑**。

   有关参数的说明，请参阅 添加 Citrix Gateway 设备

2. 按 **保存** 以保存更改。

PowerShell

要使用 PowerShell 修改网关配置，请运行 cmdlet Set-STFRoamingGateway。

删除 Citrix 网关

1. 在 **管理 Citrix Gateway** 窗口中，单击要更改的网关，然后按 **删除**。
2. 在确认窗口中，按 **是**。

PowerShell

要使用 PowerShell 删除网关，请运行 cmdlet Remove-STFRoamingGateway。

导入一个 Citrix Gateway

在 Citrix Gateway 管理控制台中配置的远程访问设置必须与 StoreFront 中配置的设置相同。本文将向您展示如何导入 Citrix Gateway 虚拟服务器的详细信息，以便正确配置 Citrix Gateway 和 StoreFront 以协同工作。

要求

- 需要 NetScaler 11.1.51.21 或更高版本才能将多个网关 vServer 导出到 ZIP 文件。

  > **注意：**
  >
  > Citrix Gateway 只能导出使用 Citrix Virtual Apps and Desktops™ 向导创建的网关 vServer。

- DNS 必须能够解析，并且 StoreFront 必须能够联系 Citrix Gateway 生成的 ZIP 文件中 GatewayConfig.json 文件中的所有 STA（安全票证颁发机构）服务器 URL。

- Citrix Gateway 生成的 ZIP 文件中的 GatewayConfig.json 文件必须包含 StoreFront 服务器上现有 Citrix Receiver for Web 站点的 URL。Citrix Gateway 11.1 及更高版本通过联系 StoreFront 服务器并在生成用于导出的 ZIP 文件之前枚举所有现有存储和网站来处理此问题。
- StoreFront 必须能够在 DNS 中将回调 URL 解析为网关 VPN vServer IP 地址，以便使用导入的网关进行身份验证成功。

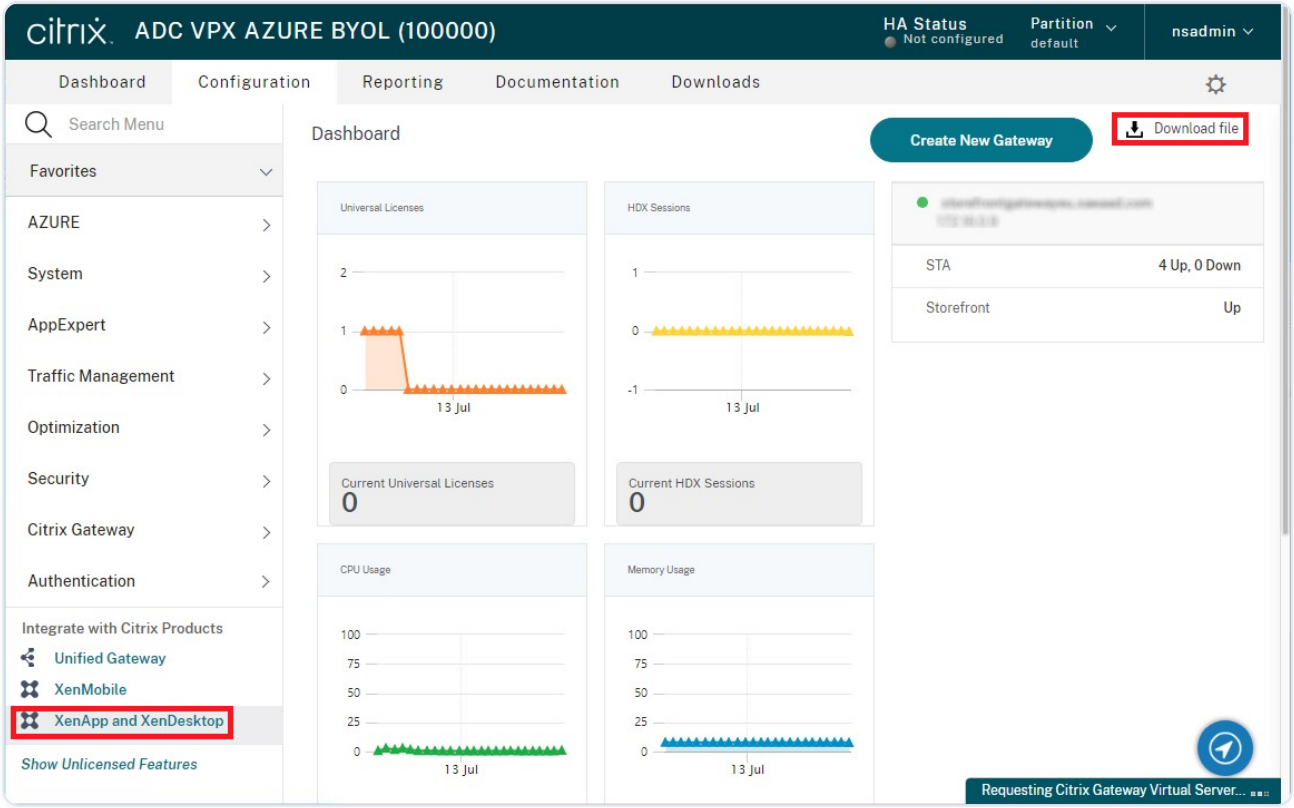
  只要 StoreFront 能够解析此 URL，您使用的回调 URL 和端口组合通常与网关 URL 和端口组合相同。

  或

  如果您在环境中使用了不同的外部和内部 DNS 命名空间，则回调 URL 和端口组合可能与网关 URL 和端口组合不同。如果您的网关位于 DMZ 中并使用 `<example.com>` URL，并且 StoreFront 位于您的私有公司网络中并使用 `<example.local>` URL，则您可以使用 `<example.local>` 回调 URL 指向 DMZ 中的网关 vServer。

从 Citrix Gateway 导出配置

1. 登录到 Citrix Gateway。
2. 转到“配置”选项卡
3. 在“与 Citrix 产品集成”下，单击 XenApp and XenDesktop®
4. 在右上角单击“下载文件”。



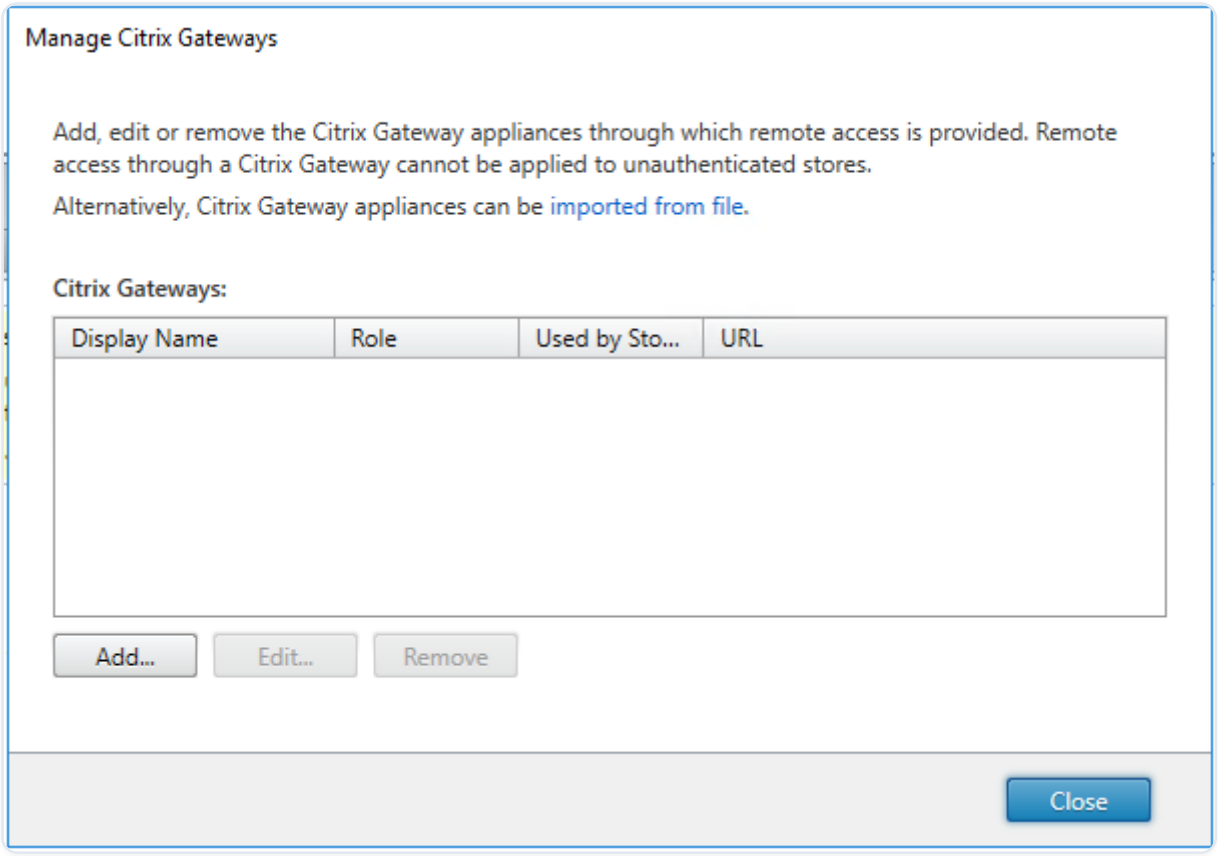
1. 选择您希望下载所有网关的配置还是特定网关的配置。

使用控制台导入 Citrix Gateway

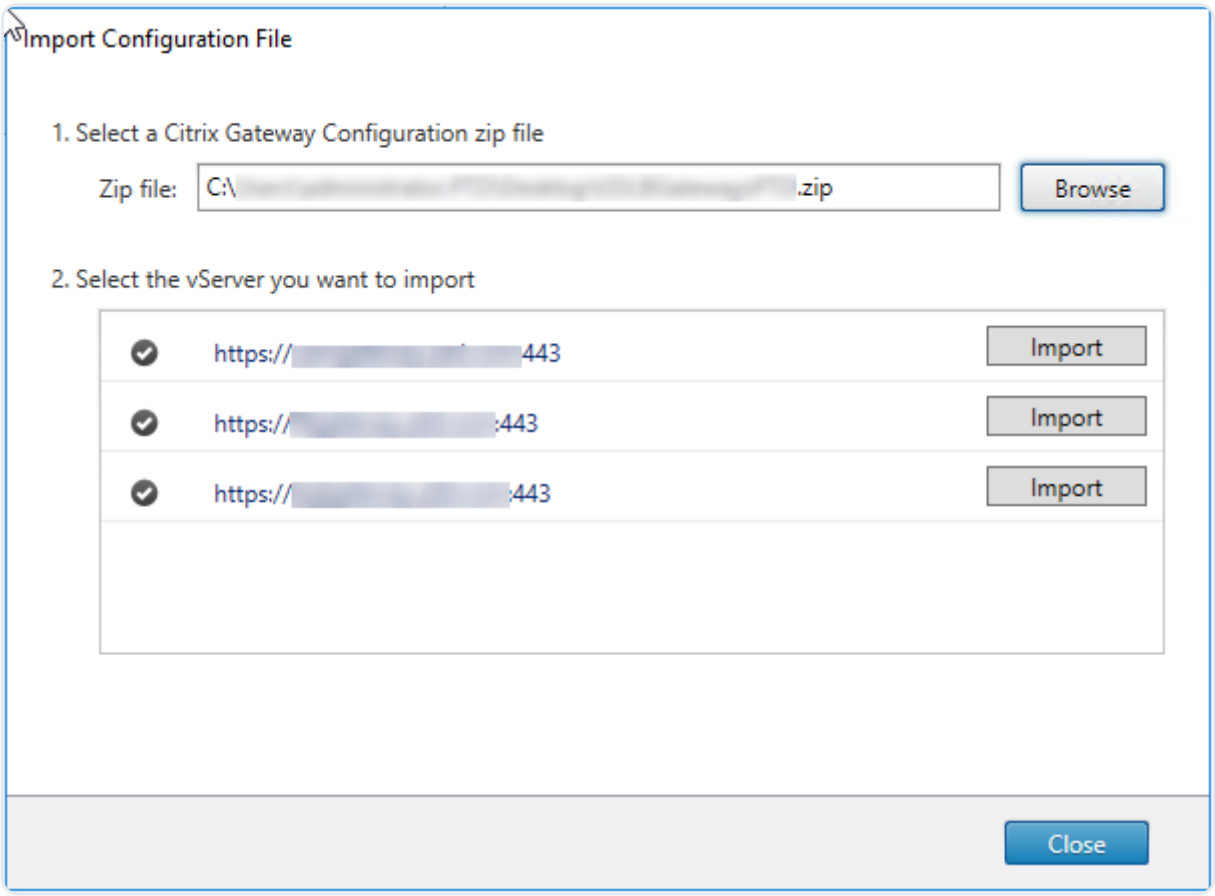
您可以使用同一个导入文件导入一个或多个 Citrix Gateway 虚拟服务器配置。如果您有来自不同 Citrix Gateway 的多个网关虚拟服务器，则必须使用多个导入文件。

> 重要提示：
>
> Citrix 不支持手动编辑从 Citrix Gateway 导出的配置文件。

1. 在 Citrix StoreFront 管理控制台的左窗格中选择**应用商店**，然后在**操作**窗格中，单击**管理 Citrix Gateway**。
2. 在“管理 Citrix Gateway”屏幕上，单击**从文件导入**链接。

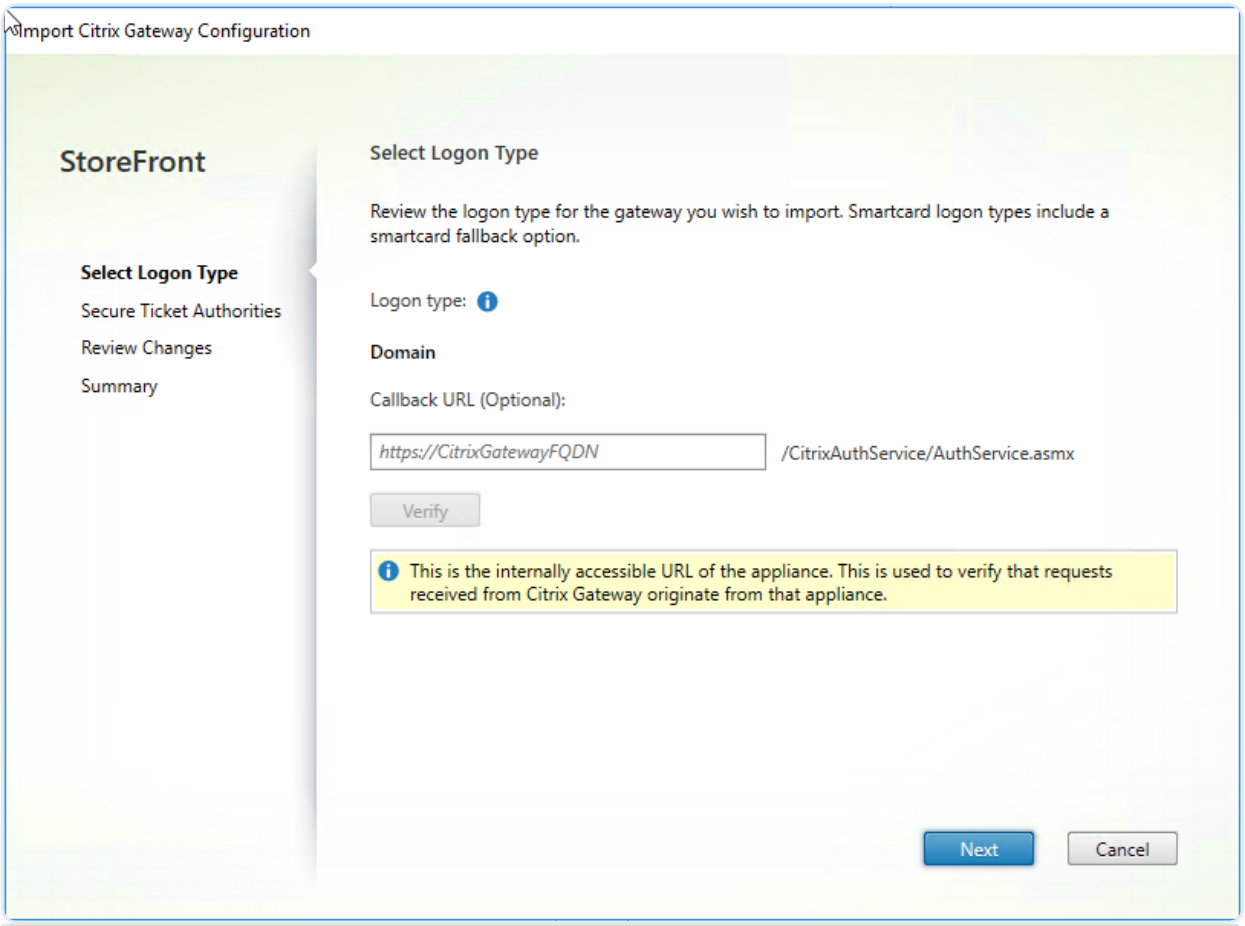


3. 浏览到 Citrix Gateway 虚拟服务器配置文件。
4. 将显示所选 ZIP 文件中的网关 vServer 列表。选择要导入的网关 vServer，然后单击**导入**。如果您重复导入 vServer，则“导入”按钮将显示为“更新”。如果选择**更新**，则稍后可以选择覆盖或创建新网关。



5. 查看所选网关的**登录类型**，并根据需要指定**回调 URL**。登录类型是您在 Citrix Gateway 上为 Citrix Workspace 应用程序用户配置的身份验证方法。某些登录类型需要回调 URL（请参阅表格）。

   - 单击**验证**以检查回调 URL 是否有效且可从 StoreFront 服务器访问。

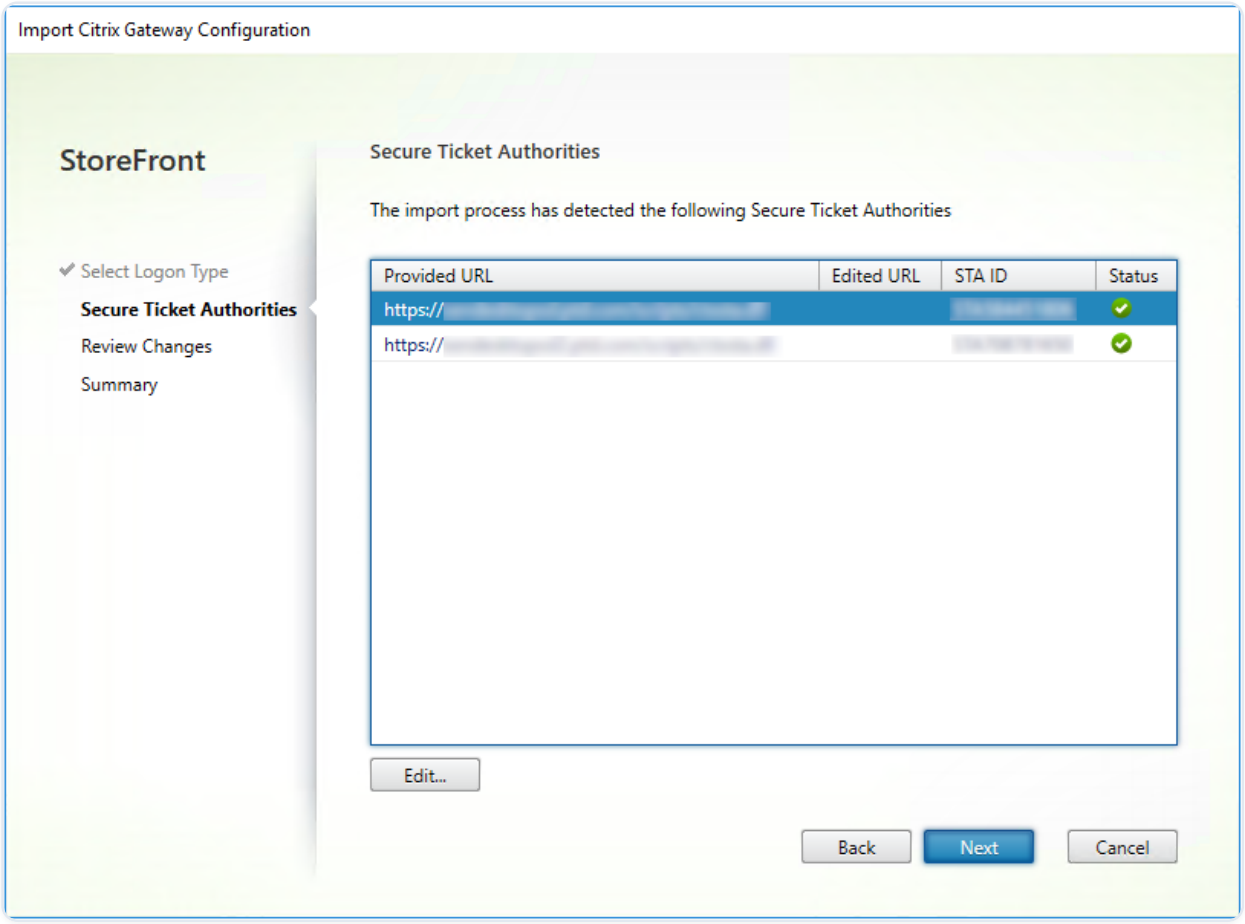


控制台中的登录类型	JSON 文件中的 LOGONTYPE	需要回调 URL
域	域	否
域和安全令牌	DomainAndRSA	否
安全令牌	RSA	是
智能卡 - 无回退	SmartCard	是
智能卡 - 域	SmartCardDomain	是
智能卡 - 域和安全令牌	SmartCardDomainAndRSA	是
智能卡 - 安全令牌	SmartCardRSA	是
智能卡 - 短信身份验证	SmartCardSMS	是
短信身份验证	SMS	是

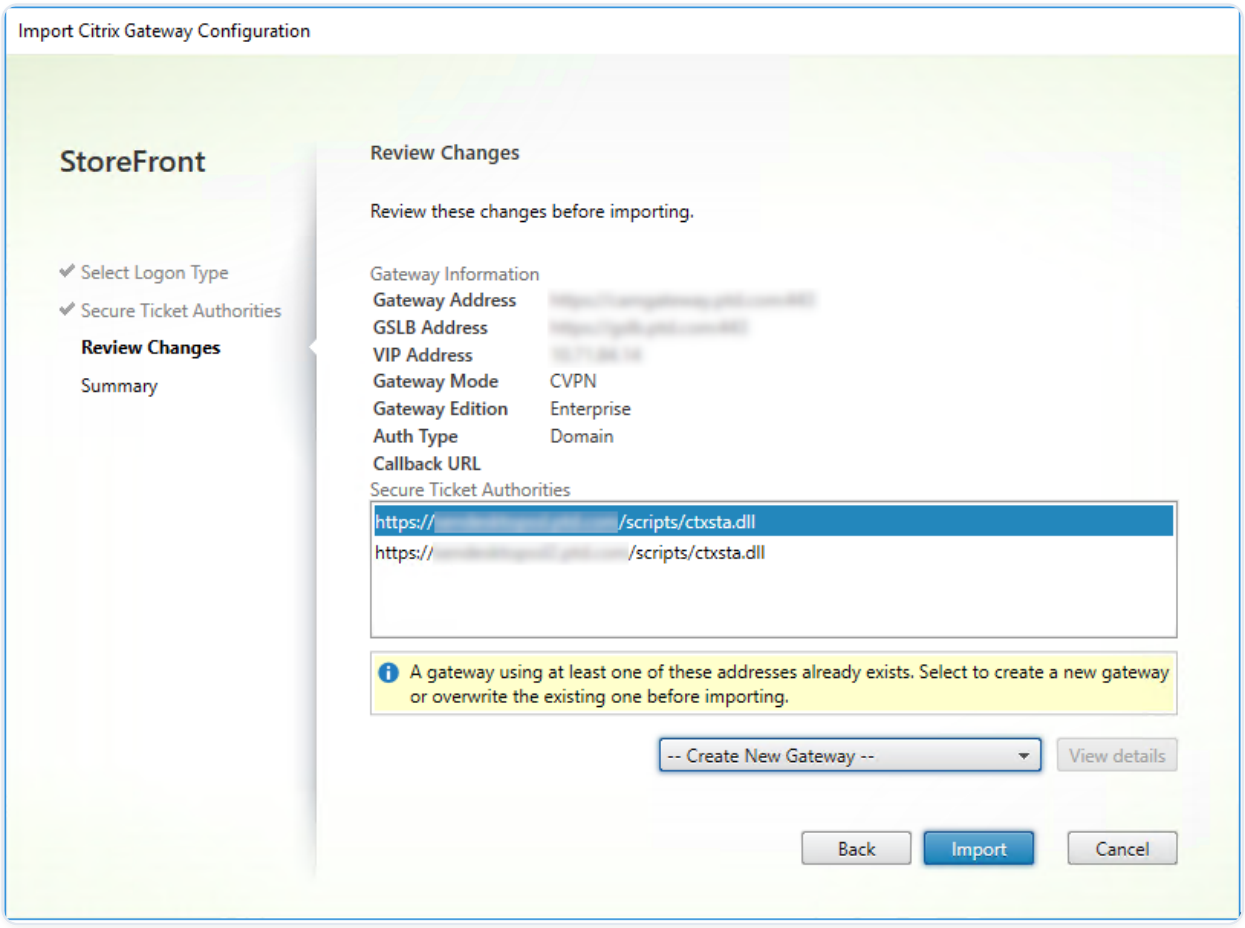
如果需要回调 URL，StoreFront 将根据 ZIP 文件中找到的网关 URL 自动填充回调 URL。您可以将其更改为指向正确的 Citrix Gateway VIP 的任何有效 URL。对于 GSLB 网关，您导入的每个网关都需要唯一的 Callback URL。

要使用智能访问或无密码身份验证，需要回调 URL。

6. 单击**下一步**。
7. StoreFront 使用 DNS 联系 ZIP 文件中列出的所有 STA（安全票证颁发机构）服务器 URL，并验证它们是否是功能正常的 STA 票证服务器。如果一个或多个 STA URL 无效，则导入将不会继续。



8. 单击**下一步**。
9. 查看导入的详细信息。如果已存在具有相同网关 URL 和端口组合 (GatewayURL:port) 的网关，请使用下拉列表选择要覆盖的网关，或创建新网关。



StoreFront 使用 GatewayURL:port 组合来确定您尝试导入的网关是否与您可能希望更新的现有网关匹配。如果网关具有不同的 GatewayURL:port 组合，则 StoreFront 会将其视为新网关。此网关设置表显示了您可以更新哪些设置。

网关设置	可更新
网关 URL:端口组合	否
GSLB URL	是
Netscaler® 信任证书和指纹	是
回调 URL	是
Web 版 Receiver 站点 URL	是
网关地址/VIP	是
STA URL 和 STA ID	是
所有登录类型	是

10. 单击**导入**。如果 StoreFront 服务器是服务器组的一部分，则会显示一条消息，提醒您将导入的网关设置传播到组中的其他服务器。
11. 单击“**完成**”。

要导入另一个 vServer 配置，请重复上述步骤。

> **注意：**
>
> 商店的默认网关是 Citrix Workspace™ 应用程序尝试连接的网关，除非它们配置为使用不同的网关。如果商店未配置任何网关，则从 ZIP 文件导入的第一个网关将成为 Citrix Workspace 应用程序使用的默认网关。导入后续网关不会更改已为商店设置的默认网关。

使用 PowerShell 导入多个 Citrix Gateway

读取 STFNetScaler 配置

- 将 ZIP 文件复制到当前登录的 StoreFront 管理员的桌面。
- 将 Citrix Gateway 虚拟服务器配置文件 ZIP 文件的内容读入内存，并使用其索引值查看其中包含的三个网关。

```
$ImportedGateways = Read-STFNetScalerConfiguration -path
"$env:USERPROFILE\desktop\GatewayConfig.zip"
```

使用 **Read-STFNetScalerConfiguration** cmdlet 查看从 Netscaler ZIP 导入包中读取的内存中的三个网关对象。

```
$ImportedGateways.Document.Gateways[0]

$ImportedGateways.Document.Gateways[1]

$ImportedGateways.Document.Gateways[2]



GatewayMode             : CVPN

CallbackUrl             :

GslbAddressUri          : https://gslb.example.com/
```

```
AddressUri              : https://emeagateway.example.com/

Address                 : https://emeagateway.example.com:443

GslbAddress             : https://gslb.example.com:443

VipAddress              : 10.0.0.1

Stas                    : {STA298854503, STA909374257}

StaLoadBalance          : True

CertificateThumbprints : {F549AFAA29EBF61E8709F2316B3981AD503AF387}

GatewayAuthType         : Domain

GatewayEdition          : Enterprise

ReceiverForWebSites     :
{Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.ReceiverForWebSite
}



GatewayMode             : CVPN

CallbackUrl             :

GslbAddressUri          : https://gslb.example.com/

AddressUri              : https://emeagateway.example.com/

Address                 : https://emeagateway.example.com:444

GslbAddress             : https://gslb.example.com:443

VipAddress              : 10.0.0.2

Stas                    : {STA298854503, STA909374257}

StaLoadBalance          : True

CertificateThumbprints : {F549AFAA29EBF61E8709F2316B3981AD503AF387}
```

```
GatewayAuthType         : DomainAndRSA

GatewayEdition          : Enterprise

ReceiverForWebSites     :
{Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.ReceiverForWebSite
}



GatewayMode             : CVPN

CallbackUrl             : https://emeagateway.example.com:445

GslbAddressUri          : https://gslb.example.com/

AddressUri              : https://emeagateway.example.com/

Address                 : https://emeagateway.example.com:445

GslbAddress             : https://gslb.example.com:443

VipAddress              : 10.0.0.2

Stas                    : {STA298854503, STA909374257}

StaLoadBalance          : True

CertificateThumbprints : {F549AFAA29EBF61E8709F2316B3981AD503AF387}

GatewayAuthType         :SmartCard

GatewayEdition          : Enterprise

ReceiverForWebSites     :
{Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.ReceiverForWebSite
}
```

不指定 CallbackURL 导入 Import-STFNetScalerConfiguration

将 ZIP 文件复制到当前登录的 StoreFront 管理员的桌面。将 Citrix Gateway 配置 ZIP 导入包读入内存，并使用其索引值查看其中包含的三个网关。

```
$ImportedGateways = Read-STFNetScalerConfiguration -path
"$env:USERPROFILE\desktop\GatewayConfig.zip"
```

使用 **Import-STFNetScalerConfiguration** cmdlet 并指定所需的网关索引，将三个新网关导入 StoreFront。使用 **-Confirm:$False** 参数可防止 PowerShell GUI 提示您允许导入每个网关。如果您希望一次仔细导入一个网关，请删除此参数。

```
Import-STFNetScalerConfiguration -Configuration $ImportedGateways
-GatewayIndex 0 -Confirm:$False

Import-STFNetScalerConfiguration -Configuration $ImportedGateways
-GatewayIndex 1 -Confirm:$False

Import-STFNetScalerConfiguration -Configuration $ImportedGateways
-GatewayIndex 2 -Confirm:$False
```

指定您自己的 CallbackURL 导入 Import-STFNetScalerConfiguration

使用 **Import-STFNetScalerConfiguration** cmdlet 并使用 -callbackURL 参数指定您选择的回调 URL，将三个新网关导入 StoreFront。

```
$ImportedGateways = Read-STFNetScalerConfiguration -path
"$env:USERPROFILE\desktop\GatewayConfig.zip"



Import-STFNetScalerConfiguration -Configuration $ImportedGateways
-GatewayIndex 0 -CallbackUrl "https://emeagatewaycb.example.com:443
-Confirm:$False



Import-STFNetScalerConfiguration -Configuration $ImportedGateways
-GatewayIndex 1 -CallbackUrl "https://emeagatewaycb.example.com:444
-Confirm:$False



Import-STFNetScalerConfiguration -Configuration $ImportedGateways
```

```
-GatewayIndex 2 -CallbackUrl "https://emeagatewaycb.example.com:445
-Confirm:$False
```

Import-STFNetScalerConfiguration 覆盖导入文件中存储的身份验证方法并指定您自己的 CallbackURL

使用 **Import-STFNetScalerConfiguration** cmdlet 并使用 -callbackURL 参数指定您选择的回调 URL，将三个新网关导入 StoreFront。

```
$ImportedGateways = Read-STFNetScalerConfiguration -path
"$env:USERPROFILE\desktop\GatewayConfig.zip"



Import-STFNetScalerConfiguration -Configuration $ImportedGateways
-GatewayIndex 0 -LogonType "SmartCard" -CallbackUrl "https://
emeagatewaycb.example.com:443" -Confirm:$False



Import-STFNetScalerConfiguration -Configuration $ImportedGateways
-GatewayIndex 1 -LogonType "SmartCard" -CallbackUrl "https://
emeagatewaycb.example.com:444" -Confirm:$False



Import-STFNetScalerConfiguration -Configuration $ImportedGateways
-GatewayIndex 2 -LogonType "SmartCard" -CallbackUrl "https://
emeagatewaycb.example.com:445" -Confirm:$False
```

使用 NetScaler® ADC 进行负载平衡

本文提供了关于如何在所有活动负载平衡配置中部署包含两个或更多 StoreFront 服务器的 StoreFront 服务器组的指导。本文详细介绍了如何配置 NetScaler ADC 设备，以在服务器组中的 StoreFront 服务器之间负载平衡来自 Citrix Workspace 应用程序和 Web 浏览器的传入请求。

为 StoreFront 服务器组负载平衡器创建 DNS 记录

为您选择的共享 FQDN 创建 DNS A 和 PTR 记录。您网络中的客户端使用此 FQDN 通过 NetScaler ADC 设备负载平衡器访问 StoreFront 服务器组。

示例：`storefront.example.com` 解析为负载平衡虚拟服务器的虚拟 IP (VIP)。

配置 StoreFront 服务器

您希望进行负载平衡的所有 StoreFront 服务器都应配置为 StoreFront 服务器组的一部分，该服务器组在服务器之间同步配置，以确保它们的配置相同。有关将服务器添加到服务器组的更多详细信息，请参阅加入现有服务器组。

每个服务器都应配置为使用 HTTPS，以便负载平衡器和 StoreFront 服务器之间的通信是加密的。请参阅使用 HTTPS 保护 StoreFront。证书必须包含负载平衡的 FQDN 作为通用名称 (CN) 或主题备用名称 (SAN)。

将服务器组基本 URL 设置为负载平衡器的 URL。要修改基本 URL，请在 Citrix StoreFront 管理控制台中，在左侧窗格中右键单击 **服务器组**，然后单击 **更改基本 URL**。输入负载平衡虚拟服务器的 URL。

可选配置 Citrix 服务监视器以使用 HTTPS

StoreFront 安装包含 **Citrix 服务监视器** Windows 服务。此服务没有其他服务依赖项，并监视关键 StoreFront 服务的运行状况。这允许 NetScaler ADC 和其他第三方应用程序监视 StoreFront 服务器部署的相对运行状况。

默认情况下，监视器使用端口 8000 上的 HTTP。您可以选择将其更改为使用端口 443 上的 HTTPS。

1. 在主 StoreFront 服务器上打开 PowerShell 集成脚本环境 (ISE) 并运行以下命令，以将默认监视器更改为 HTTPS 443：

   ```
   $ServiceUrl = "https://localhost:443/StorefrontMonitor"

   Set-STFServiceMonitor -ServiceUrl $ServiceUrl

   Get-STFServiceMonitor
   ```

2. 完成后，将更改传播到 StoreFront 服务器组中的所有其他服务器。
3. 要对监视器执行快速测试，请在 StoreFront 服务器或任何其他可网络访问 StoreFront 服务器的计算机上的浏览器中输入以下 URL。浏览器将返回每个 StoreFront 服务的状态 XML 摘要。

   `https://<loadbalancingFQDN>/StoreFrontMonitor/GetSFServicesStatus`

   ```
   <ArrayOfServiceStatus xmlns="http://schemas.datacontract.org/2004/07/
   Citrix.DeliveryServices.ServiceMonitor.Contract" xmlns:i="http://
   www.w3.org/2001/XMLSchema-instance">
   ```

```
<ServiceStatus>
    <name>Citrix Peer Resolution Service</name>
    <status>running</status>
</ServiceStatus>
<ServiceStatus>
    <name>CitrixConfigurationReplication</name>
    <status>running</status>
</ServiceStatus>
<ServiceStatus>
    <name>CitrixCredentialWallet</name>
    <status>running</status>
</ServiceStatus>
<ServiceStatus>
    <name>CitrixDefaultDomainService</name>
    <status>running</status>
</ServiceStatus>
<ServiceStatus>
    <name>CitrixSubscriptionsStore</name>
    <status>running</status>
</ServiceStatus>
<ServiceStatus>
    <name>NetTcpPortSharing</name>
```

```
    <status>running</status>
</ServiceStatus>
<ServiceStatus>
    <name>WAS</name>
    <status>running</status>
</ServiceStatus>
<ServiceStatus>
    <name>W3SVC</name>
    <status>running</status>
</ServiceStatus>
</ArrayOfServiceStatus>
```

配置 NetScaler 负载均衡器

安装根证书

如果您的 StoreFront 服务器使用内部颁发机构签名的证书，则必须在 NetScaler 上安装根证书。这是必需的，以便 NetScaler 信任 StoreFront 服务器的证书。

1. 登录到 NetScaler ADC 设备管理 GUI。
2. 选择 **流量管理** > **SSL** > **证书** > **CA 证书**。
3. 单击**安装**。
4. 在“**安装 CA 证书**”页面上，输入证书-密钥对名称，单击“**选择文件**”并浏览到证书文件。
5. 单击**安装**。

安装服务器证书

要启用 HTTPS，您需要一个证书，其主题备用名称包含负载均衡器的 FQDN。您可以使用企业或公共证书颁发机构对证书进行签名。

您必须拥有 PEM 格式的单独证书和密钥文件。如果您有包含 PKCS12 格式私钥的证书，则可以使用 `openssl` 转换文件。例如：

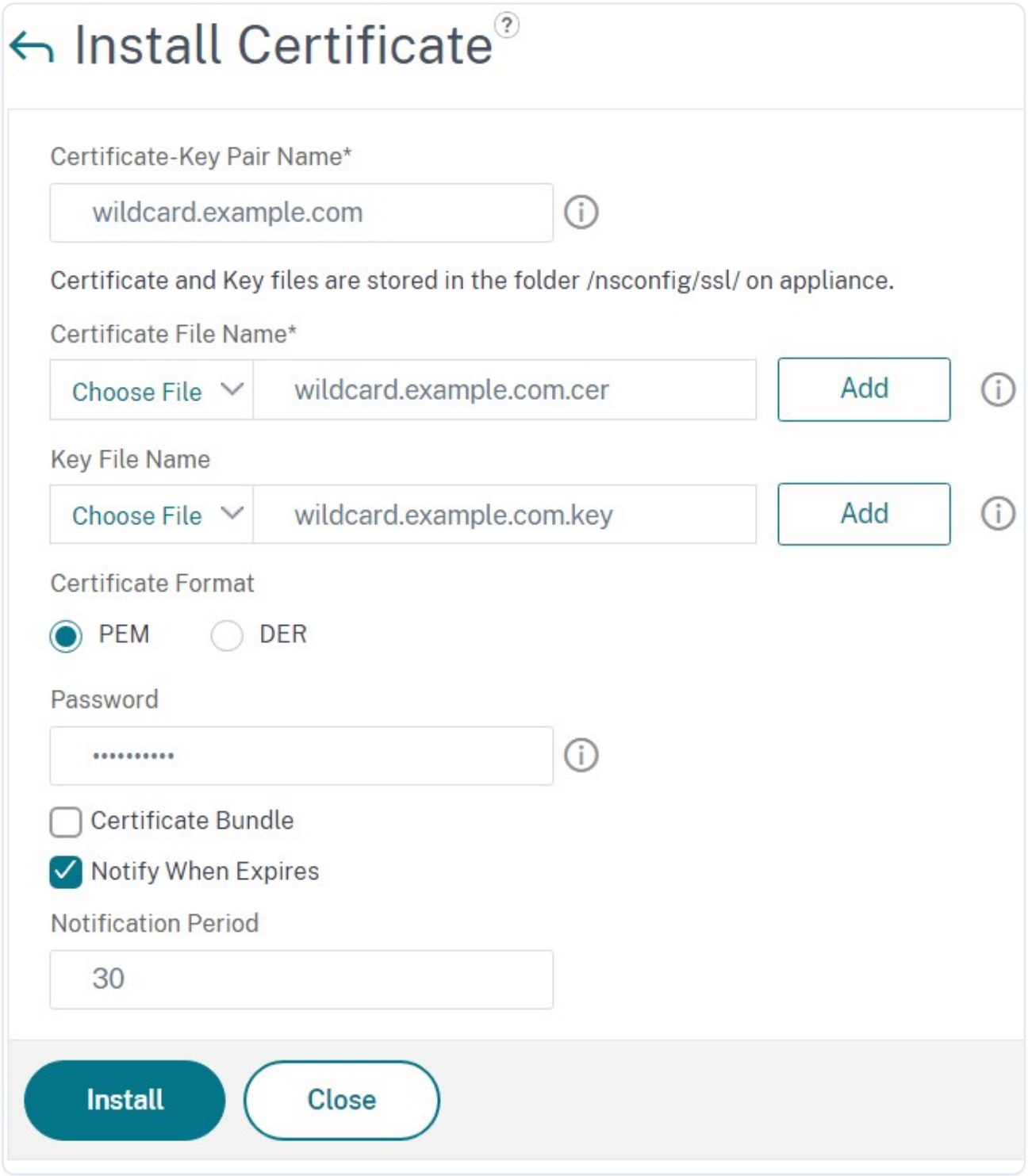
```
openssl pkcs12 -in cert.pfx -clcerts -nokeys -out cert.cer

openssl pkcs12 -in cert.pfx -nocerts -out storefrontlbeu.key
```

将出现提示以输入现有密码和新的 PEM 密码短语。

要安装证书：

1. 登录到 NetScaler ADC 设备管理 GUI。
2. 选择 **流量管理** > **SSL** > **证书** > **CA 证书**。
3. 单击**安装**。
4. 在“**安装 CA 证书**”页面上：
    a. 输入“**证书-密钥对名称**”。
    b. 在“**证书文件名**”下，单击“**选择文件**”并浏览证书文件。
    c. 在“**密钥文件名**”下，单击“**选择文件**”并浏览密钥文件。
    d. 在“**密码**”下输入密码短语。
    e. 单击**安装**。
5. 单击“**链接**”将证书链接到根证书。

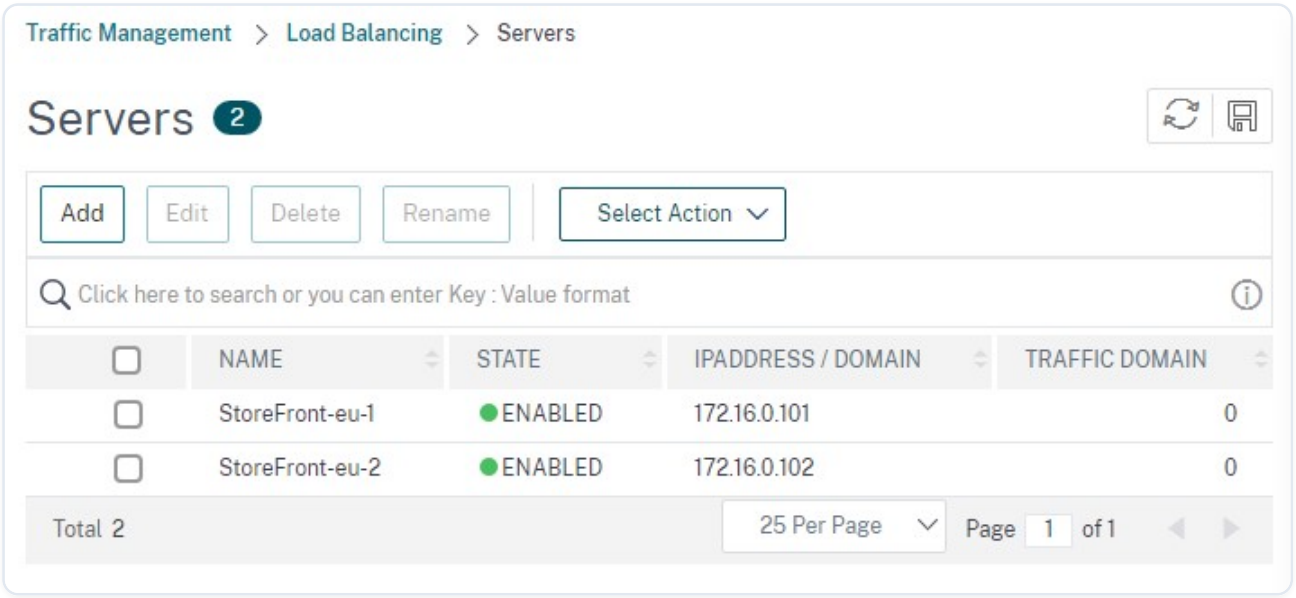


将各个 StoreFront 服务器节点添加到 NetScaler ADC 设备负载平衡器

1. 导航到“**流量管理 > 负载平衡 > 服务器**”。单击“**添加**”并添加每个要进行负载平衡的 StoreFront 服务器。

   示例 = 2 个 StoreFront 服务器，名为 StoreFront-eu-1 和 StoreFront-eu-2

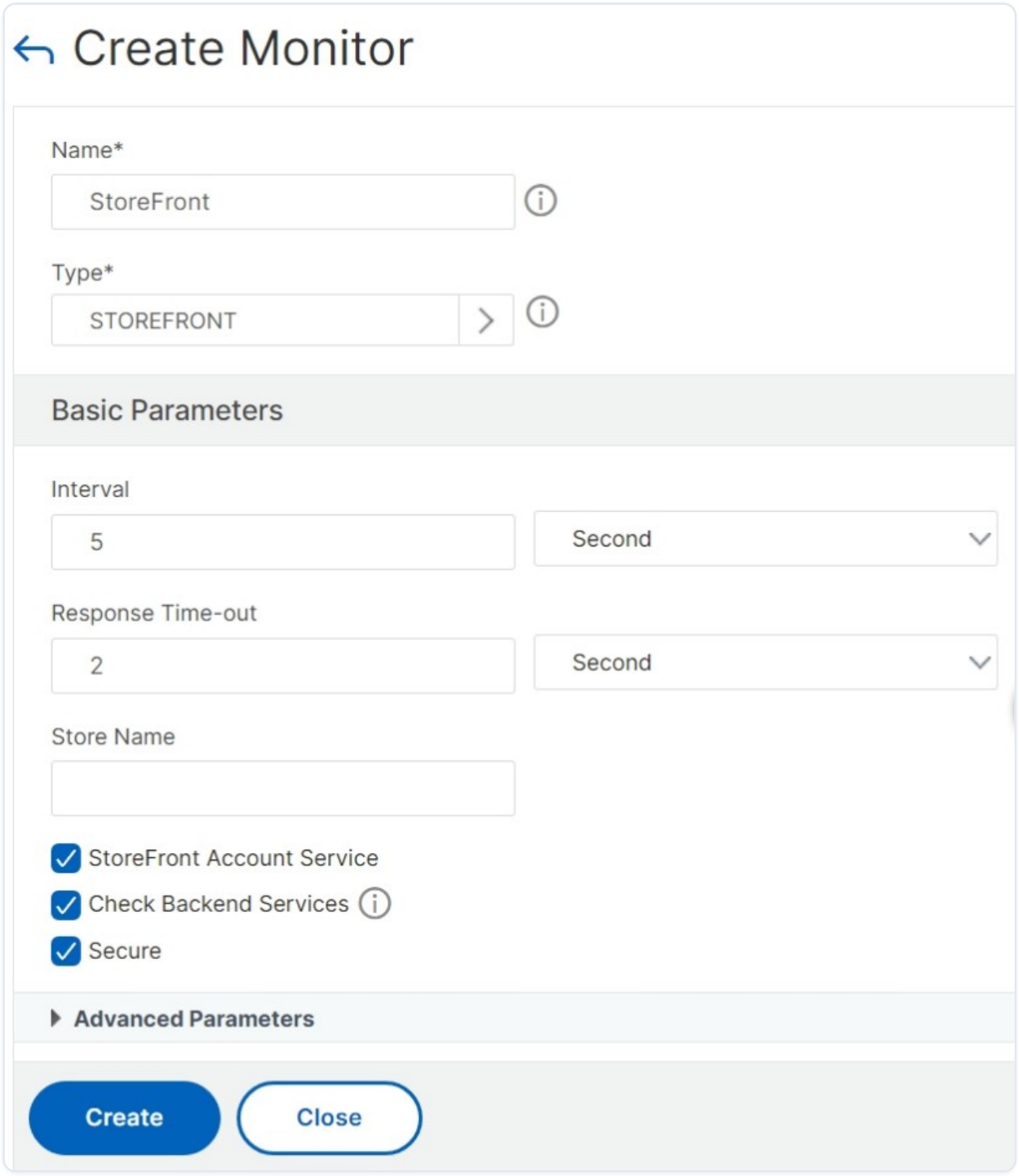
2. 使用基于 IP 的服务器配置，并输入每个 StoreFront 节点的服务器 IP 地址。



定义 StoreFront 监视器以检查服务器组中所有 StoreFront 节点的状态

1. 登录到 NetScaler ADC 管理 GUI。
2. 选择“**流量管理 > 负载平衡 > 监视器 > 添加**”并添加一个名为 *StoreFront* 的新监视器，然后接受所有默认设置。
3. 从“**类型**”下拉菜单中，选择“**StoreFront**”。
4. 如果您已将 StoreFront 监视器配置为使用 HTTPS，则确保选中“**安全**”选项。否则，请取消选中此选项并输入端口 8000。
5. 选择 **检查后端服务** 选项。此选项可启用对 StoreFront 服务器上运行的服务的监控。StoreFront 服务通过探测在 StoreFront 服务器上运行的 Windows 服务进行监控，该服务返回以下服务的状态：

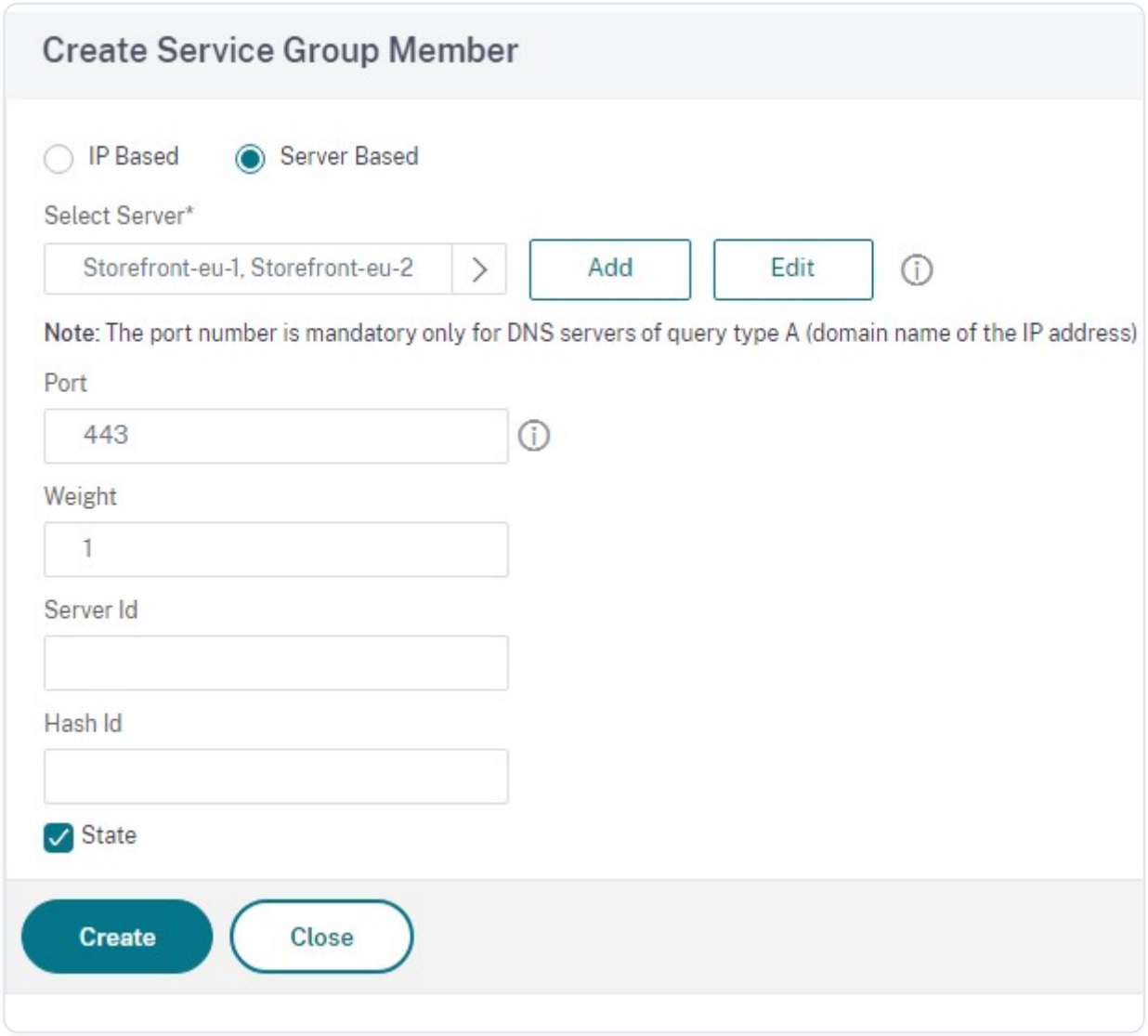
   - W3SVC (IIS)
   - WAS (Windows 进程激活服务)
   - CitrixCredentialWallet
   - CitrixDefaultDomainService



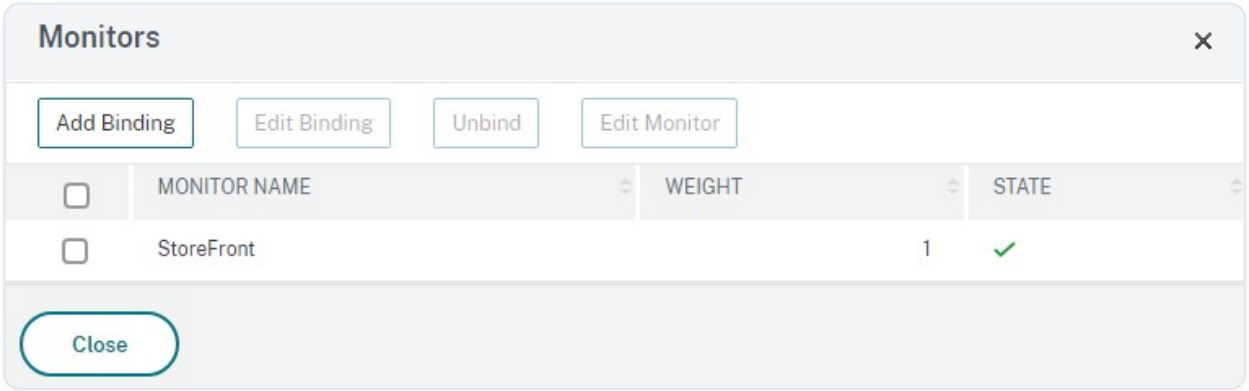
创建包含所有 StoreFront 服务器的服务组

1. 导航到 **流量管理 > 负载平衡 > 服务组**。按 **添加**。要通过 HTTPS 连接到 StoreFront 服务器，请选择 SSL 协议。将其他设置保留为默认值。按 **确定**。
2. 在您的服务组中，在 **服务组成员** 下，单击 **无服务组成员**。
   a. 单击 **基于服务**。
   b. 选择您之前定义的所有服务器。

c. 要在负载平衡器和 StoreFront 服务器之间使用 SSL，请输入端口 443。否则，请输入端口 80。



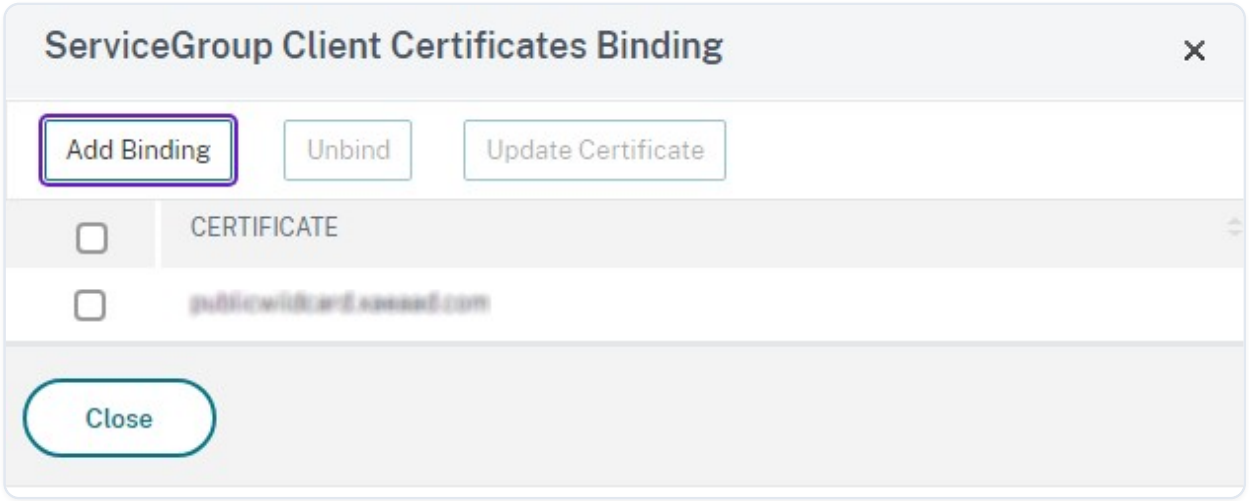
3. 添加 **监视器** 部分并选择您之前创建的 StoreFront 监视器。



4. 添加**证书**部分。

a. 绑定客户端证书。

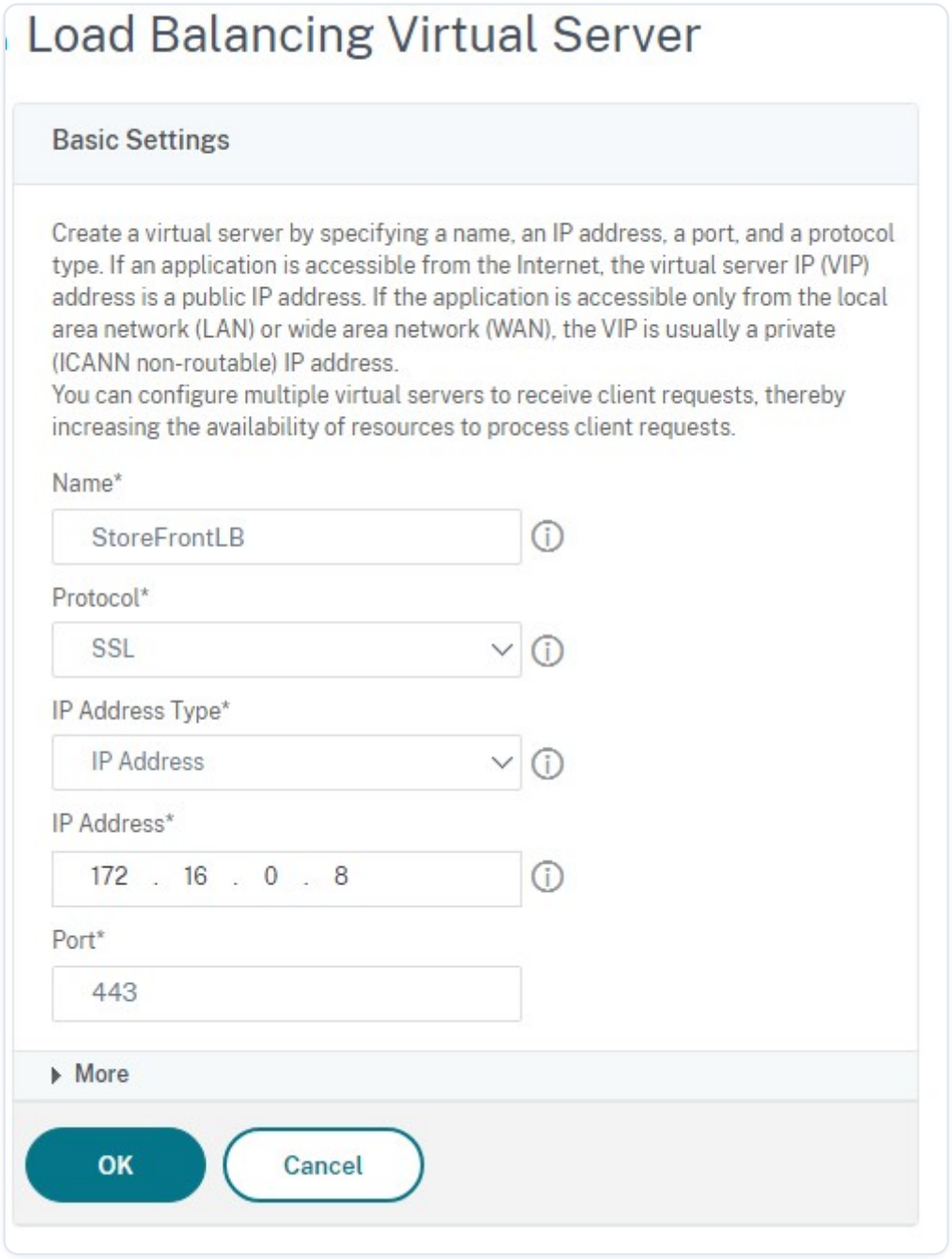
b. 绑定用于签署您之前导入的服务器证书的 CA 证书，以及可能属于 PKI 信任链的任何其他 CA。



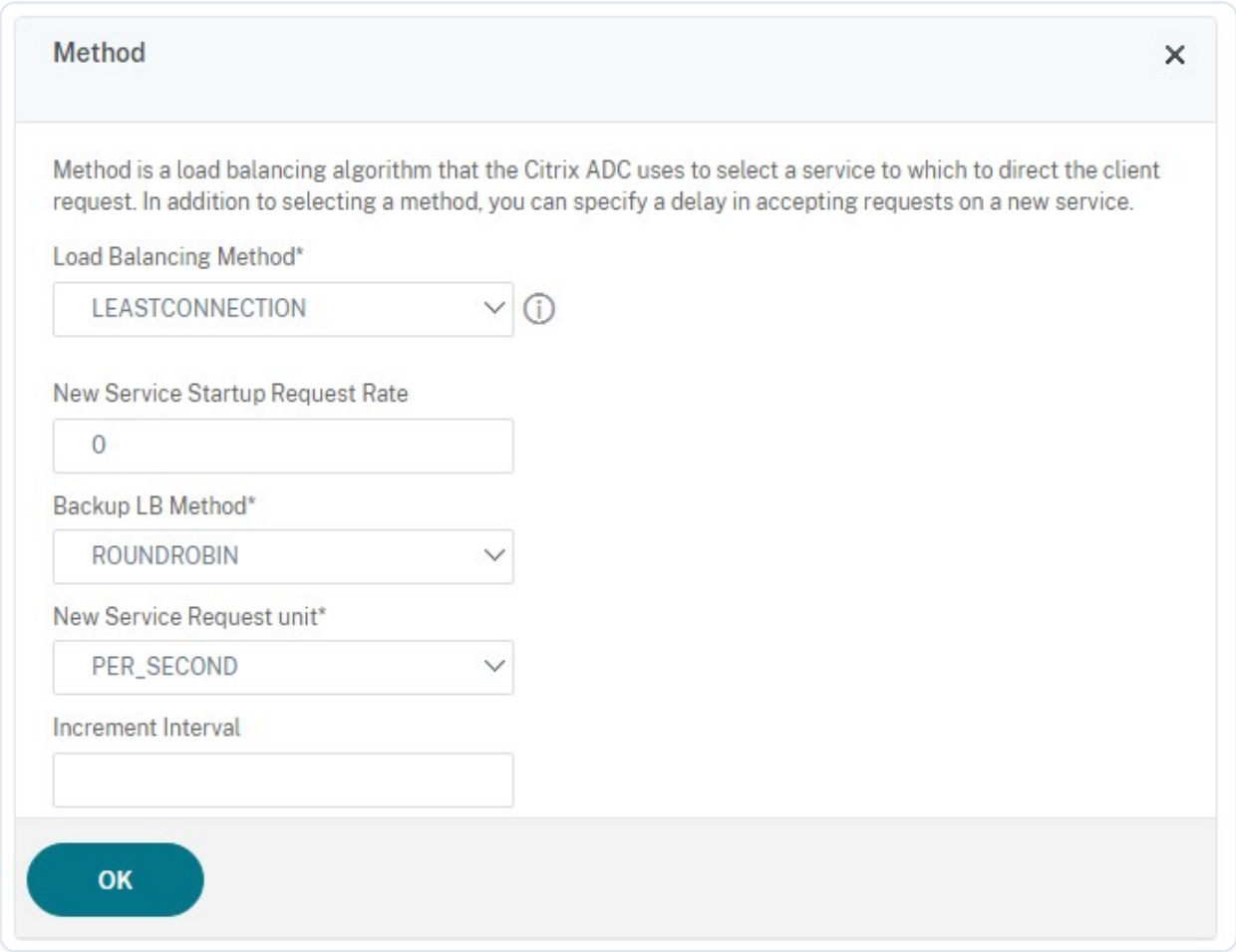
5. 添加**设置**部分。选择**插入客户端 IP 标头**并输入标头名称**X-Forwarded-For**。这允许在Citrix Virtual Apps and Desktops Policies中使用客户端 IP 地址。

为用户流量创建负载平衡虚拟服务器

1. 登录到 NetScaler ADC 设备管理 GUI。
2. 选择**流量管理 > 负载平衡 > 虚拟服务器 > 添加**以创建新的虚拟服务器。
3. 输入名称，选择 SSL 协议并输入**端口**。单击“确定”创建虚拟服务器。



4. 将您之前创建的**服务组**绑定到负载平衡虚拟服务器。
5. 绑定您之前绑定到服务组的相同服务器和 CA 证书。
6. 添加**方法**部分并选择负载平衡方法。StoreFront 负载平衡的常见选择是**轮询**或**最少连接**。



7. 添加**持久性**部分。

   a. 将持久性方法设置为 **COOKIEINSERT**。

   b. 将超时设置为与 StoreFront 中的会话超时相同，默认情况下为 20 分钟。

   c. 命名 Cookie。例如，**NSC_SFPersistence**，因为这有助于在调试期间轻松识别。

   d. 将备份持久性设置为 **NONE**。

> **注意：**
>
> 如果客户端不允许存储 HTTP cookie，则后续请求将不包含 HTTP cookie，并且不使用持久性。

持久性部分屏幕截图(/en-us/storefront/2507-ltsr/media/integrate-with-citrix-gateway-and-citrix-adc/persistence.png)

配置 StoreFront 环回

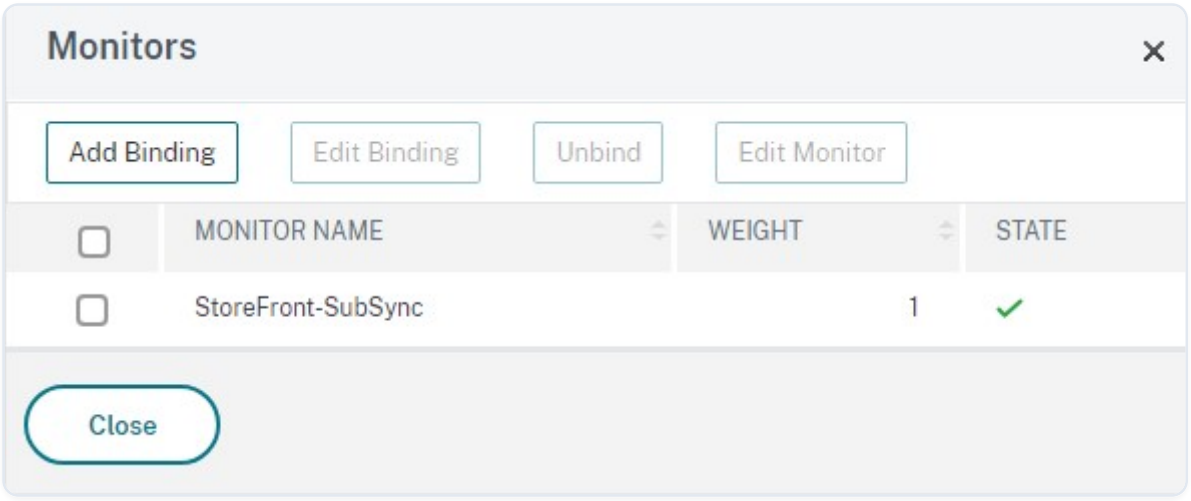
当基本地址是负载均衡器时，对于 StoreFront 服务之间的内部通信，它可能导致流量路由到负载均衡器，并可能路由到另一个服务器。这会导致性能不佳和意外行为。使用 StoreFront 设置 启用环回通信 来避免此问题。默认情况下，此设置设为 **On**，这意味着它会将服务地址的主机部分替换为环回 IP 地址 127.0.0.1，同时保持方案（HTTP 或 HTTPS）不变。这适用于单服务器部署和使用非 SSL 终止负载均衡器的部署。如果负载均衡器是 SSL 终止的，并且通过 HTTP（不推荐）与 StoreFront 通信，则需要将 StoreFront 环回通信配置为 **OnUsingHttp**，这意味着 StoreFront 也会将方案从 HTTPS 更改为 HTTP。

配置 NetScaler ADC 负载均衡器以实现服务器组之间的订阅同步

如果您有一个由两个或更多 StoreFront 服务器组组成的多站点部署，则可以使用重复计划上的拉取策略在它们之间复制订阅数据。StoreFront 订阅复制使用 TCP 端口 808，因此使用 HTTP 端口 80 或 HTTPS 443 上的现有负载均衡虚拟服务器会失败。为了为此服务提供高可用性，请在部署中的每个 NetScaler ADC 设备上创建第二个虚拟服务器，以对每个 StoreFront 服务器组的 TCP 端口 808 进行负载均衡。

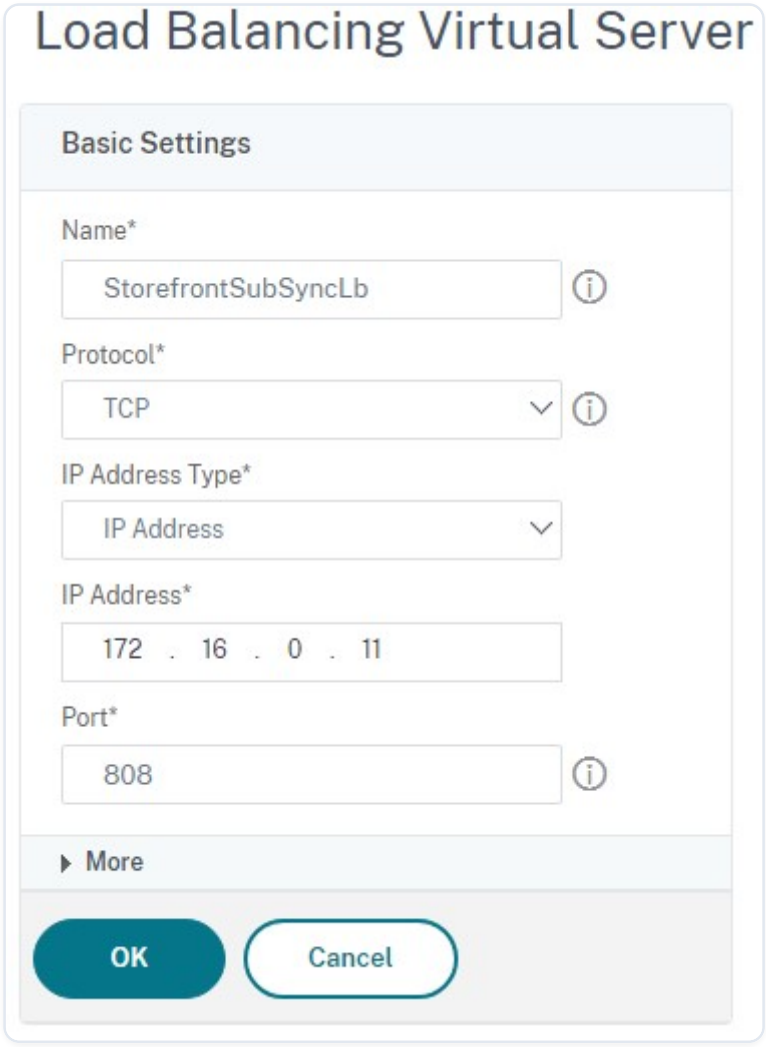
配置用于订阅同步的服务组

1. 登录到 NetScaler ADC 设备管理 GUI。
2. 选择 **流量管理 > 负载均衡 > 服务组 > 添加**。
3. 输入服务组名称，将协议更改为 **TCP**，然后单击 **确定** 保存。
4. 在**服务组成员**部分中，添加您之前在“服务器”部分中定义的所有 StoreFront 服务器节点，并将**端口**指定为 **808**。
5. 添加**监视器**部分。
    a. 单击“**无服务组可监视绑定**”所在的位置。
    b. 单击“添加”。输入监视器**名称**，并将其**类型**设置为 **TCP**。单击“**创建**”。
    c. 单击“**绑定**”。



创建用于订阅同步的负载平衡虚拟服务器

1. 登录到 NetScaler ADC 设备管理 GUI。
2. 选择 **流量管理> 负载平衡 > 虚拟服务器 > 添加** 并添加新的服务组。
3. 输入**名称**
4. 将协议更改为 **TCP**。
5. 输入 IP 地址。
6. 输入 **端口** 为 **808**。



7. 单击“**确定**”。
8. 单击“**无负载平衡虚拟服务器服务组绑定**”，选择之前创建的服务组，然后单击“**绑定**”。
9. 添加“**方法**”部分，并将**负载平衡方法**设置为 **ROUNDROBIN**
10. 单击“**完成**”以完成更改。

配置 StoreFront 以通过负载均衡器拉取订阅数据

请参阅 配置订阅同步。

配置复制计划时，请指定与订阅同步虚拟服务器虚拟负载均衡器 IP 地址匹配的服务器组地址。

配置 Citrix Gateway 和 StoreFront 用于委派表单身份验证 (DFA)

可扩展身份验证为扩展 Citrix Gateway 和 StoreFront 的基于表单的身份验证提供了一个单一的自定义点。要使用可扩展身份验证 SDK 实现身份验证解决方案，您必须在 Citrix Gateway 和 StoreFront 之间配置委派表单身份验证 (DFA)。委派表单身份验证协议允许将身份验证表单的生成和处理（包

括凭据验证）委派给另一个组件。例如，Citrix Gateway 将其身份验证委派给 StoreFront，然后 StoreFront 与第三方身份验证服务器或服务进行交互。

在 Citrix Gateway 上配置委派表单身份验证，具体描述请参阅 CTX200383。

安装建议

- 为确保 Citrix Gateway 和 StoreFront 之间的通信受到保护，请使用 HTTPS 而非 HTTP 协议。
- 对于群集部署，请确保在配置步骤之前，所有节点都安装了相同的服务器证书并在 IIS HTTPS 绑定中进行了配置。
- 确保当 StoreFront 中配置了 HTTPS 时，Citrix Gateway 将 StoreFront 服务器证书的颁发者作为受信任的证书颁发机构。

StoreFront 群集安装注意事项

- 在将所有节点连接在一起之前，请在所有节点上安装第三方身份验证插件。
- 在一个节点上配置所有与委派表单身份验证相关的设置，并将更改传播到其他节点。请参阅“启用委派表单身份验证”。

启用委派表单身份验证

由于 StoreFront 中没有用于设置 Citrix 预共享密钥的 GUI，请使用 PowerShell 控制台安装委派表单身份验证。

1. 安装委派表单身份验证。默认情况下未安装，您需要使用 PowerShell 控制台进行安装。

```
PS C:\Users\administrator.PTD.000> cd 'C:\Program Files\Citrix\Receiver
StoreFront\Scripts'

PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> & .
\ImportModules.ps1

Adding snapins

Importing modules

Loading 'C:\Program Files\Citrix\Receiver
StoreFront\Admin\Citrix.DeliveryServices.ConfigurationProvider.dll'

Loading 'C:\Program Files\Citrix\Receiver
StoreFront\Admin\Citrix.DeliveryServices.ConfigurationProvider.dll'
```

```
PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Install-
DSDFAServer

Id                              : bf694fbc-ae0a-4d56-8749-c945559e897a

ClassType                       : e1eb3668-9c1c-4ad8-bbae-c08b2682c1bc

FrameworkController             :
Citrix.DeliveryServices.Framework.FileBased.FrameworkController

ParentInstance                  : 8dd182c7-f970-466c-ad4c-27a5980f716c

RootInstance                    : 5d0cdc75-1dee-4df7-8069-7375d79634b3

TenantId                        : 860e9401-39c8-4f2c-928d-34251102b840

Data                            : {}

ReadOnlyData                    : {[Name, DelegatedFormsServer],
[Cmdlet, Add-DSWebFeature], [Snapin, Citrix.DeliverySer

                                  vices.Web.Commands], [Tenant,
860e9401-39c8-4f2c-928d-34251102b840]}

ParameterData                   : {[FeatureClassId, e1eb3668-9c1c-4ad8-
bbae-c08b2682c1bc], [ParentInstanceId, 8dd182c7-f

                                  970-466c-ad4c-27a5980f716c],
[TenantId, 860e9401-39c8-4f2c-928d-34251102b840]}

AdditionalInstanceDependencies : {b1e48ef0-b9e5-4697-af9b-0910062aa2a3}

IsDeployed                      : True

FeatureClass                    :
Citrix.DeliveryServices.Framework.Feature.FeatureClass
```

2. 添加 Citrix 受信任客户端。配置 StoreFront 和 Citrix Gateway 之间的共享密钥（密码）。您的密码和客户端 ID 必须与您在 Citrix Gateway 上配置的相同。

```
PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Add-
DSCitrixPSKTrustedClient -clientId netscaler.fqdn.com -passphrase
secret
```

3. 将委派表单身份验证对话工厂设置为将所有流量路由到自定义表单。要查找对话工厂，请在 C:\inetpub\wwwroot\Citrix\Authentication\web.config 中查找 ConversationFactory。以下是您可能会看到的一个示例。

```
<example connectorURL="http://Example.connector.url:8080/adapters-sf-
aaconnector-webapp">

      <routeTable order="1000">

        <routes>

          <route name="StartExampleAuthentication" url="Example-Bridge-
Forms/Start">

            <defaults>

              <add param="controller"
value="ExplicitFormsAuthentication" />

              <add param="action" value="AuthenticateStart" />

              <add param="postbackAction" value="Authenticate" />

              <add param="cancelAction" value="CancelAuthenticate" />

              <add param="conversationFactory"
value="ExampleBridgeAuthentication" />

              <add param="changePasswordAction"
value="StartChangePassword" />

              <add param="changePasswordController"
value="ChangePassword" />

              <add param="protocol" value="CustomForms" />

            </defaults>
```

```
        </route>
```

4. 在 PowerShell 中，设置委派表单身份验证对话工厂。在此示例中，设置为 ExampleBridgeAuthentication。

```
PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Set-
DSDFAProperty -ConversationFactory ExampleBridgeAuthentication
```

PowerShell 参数不区分大小写：**-ConversationFactory** 与 **-conversationfactory** 相同。

卸载 StoreFront

在卸载 StoreFront 之前，请卸载任何第三方身份验证插件，因为它会影响 StoreFront 的功能。

使用不同的域进行身份验证

某些组织制定了不允许第三方开发人员或承包商访问生产环境中已发布资源的策略。本文介绍如何通过使用一个域通过 Citrix Gateway 进行身份验证，从而在测试环境中授予对已发布资源的访问权限。然后，您可以使用不同的域向 StoreFront 和 Receiver for Web 站点进行身份验证。本文所述的通过 Citrix Gateway 进行身份验证支持通过 Receiver for Web 站点登录的用户。此身份验证方法不支持本机桌面或移动 Citrix Receiver 或 Citrix Workspace 应用程序的用户。

设置测试环境

本示例使用名为 production.com 的生产域和名为 development.com 的测试域。

`production.com` 域

本示例中的 `production.com` 域设置如下：

- 配置了 `production.com` LDAP 身份验证策略的 Citrix Gateway。
- 通过网关的身份验证使用 production\testuser1 帐户和密码进行。

`development.com` 域

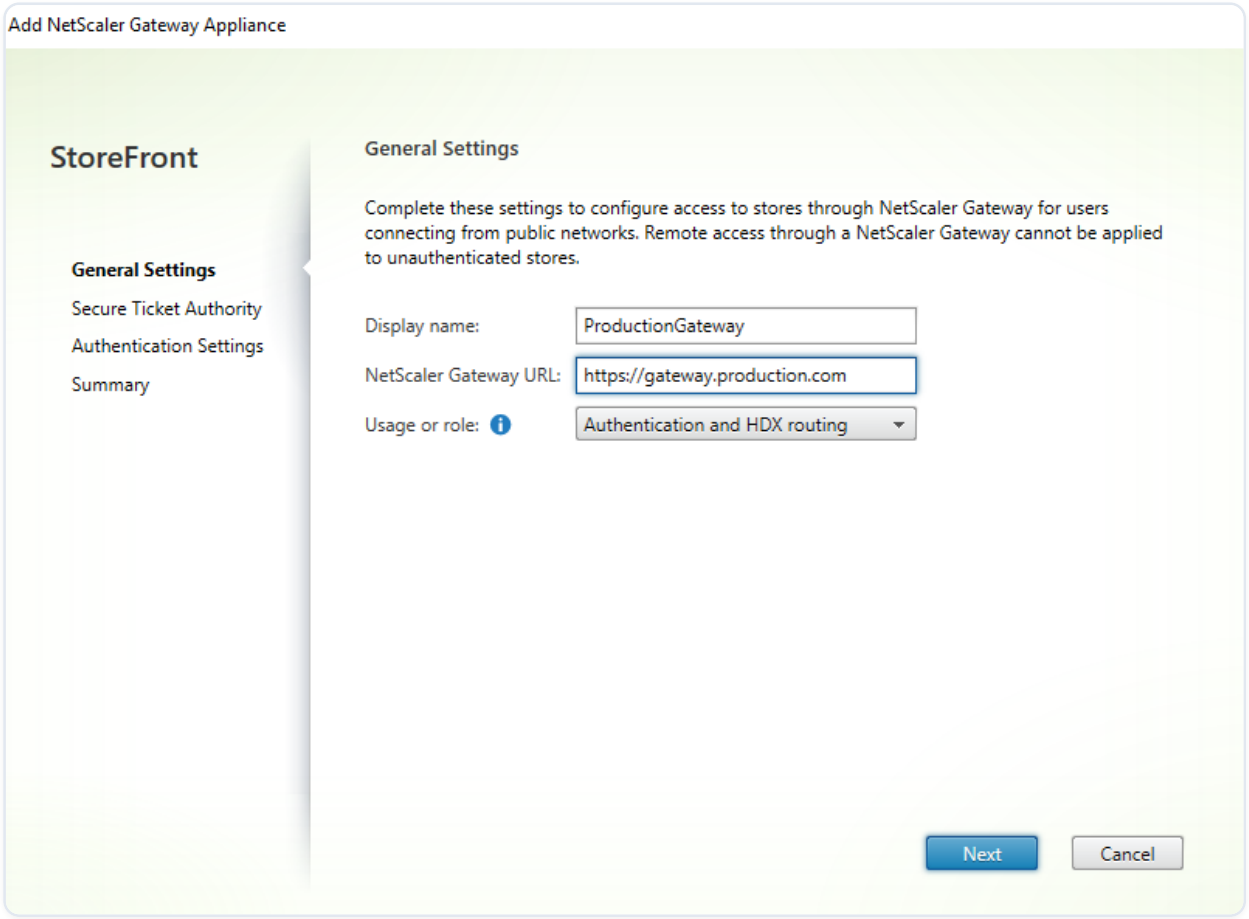
本示例中的 `development.com` 域设置如下：

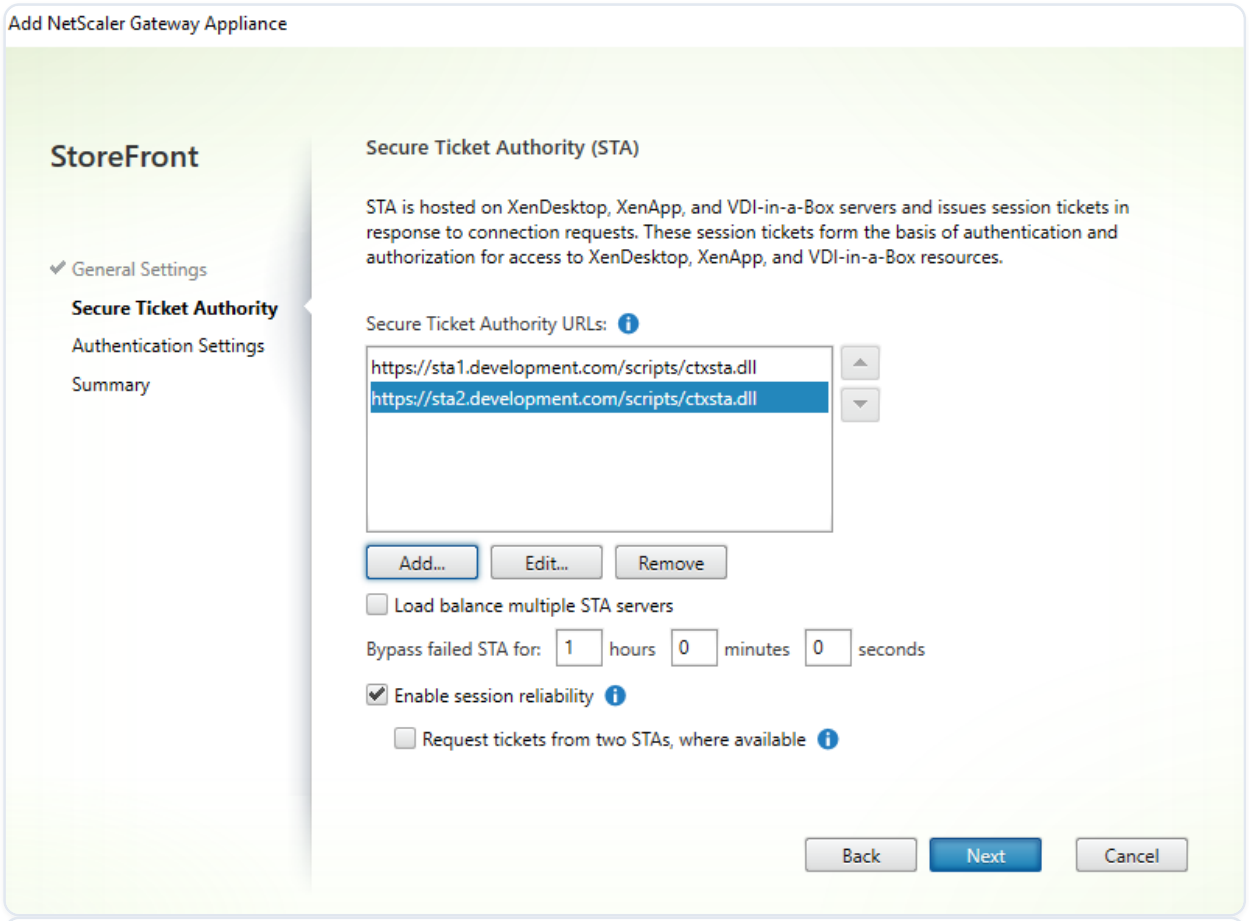
- StoreFront、Citrix Virtual Apps and Desktops 和 VDA 都位于 `development.com` 域中。
- 对 Citrix Receiver for Web 站点的身份验证使用 development\testuser1 帐户和密码进行。
- 这两个域之间没有信任关系。

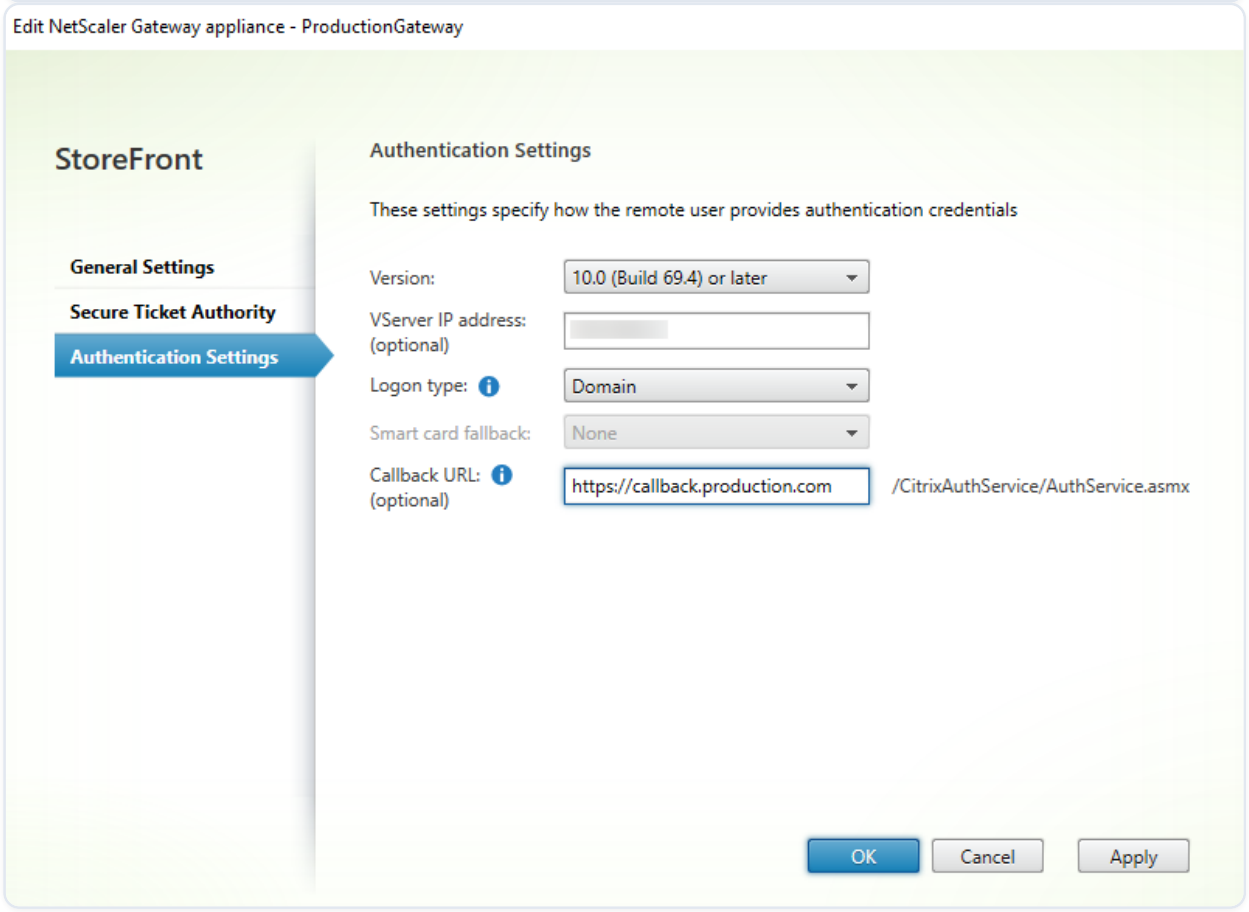
为应用商店配置 Citrix Gateway

要为应用商店配置 Citrix Gateway：

1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择**存储**，然后在**操作**窗格中单击**管理 Citrix Gateway**。
2. 在“管理 Citrix Gateway”屏幕上，单击**添加**。
3. 完成“常规设置”、“安全票证颁发机构”和“身份验证”步骤。




Add NetScaler Gateway Appliance
StoreFront
General Settings
Secure Ticket Authority
Authentication Settings
Summary
Secure Ticket Authority (STA)
STA is hosted on XenDesktop, XenApp, and VDI-in-a-Box servers and issues session tickets in response to connection requests. These session tickets form the basis of authentication and authorization for access to XenDesktop, XenApp, and VDI-in-a-Box resources.
Secure Ticket Authority URLs:
https://sta1.development.com/scripts/ctxsta.dll
https://sta2.development.com/scripts/ctxsta.dll
Add...
Edit...
Remove
Load balance multiple STA servers
Bypass failed STA for: 1 hours 0 minutes 0 seconds
Enable session reliability
Request tickets from two STAs, where available
Back
Next
Cancel

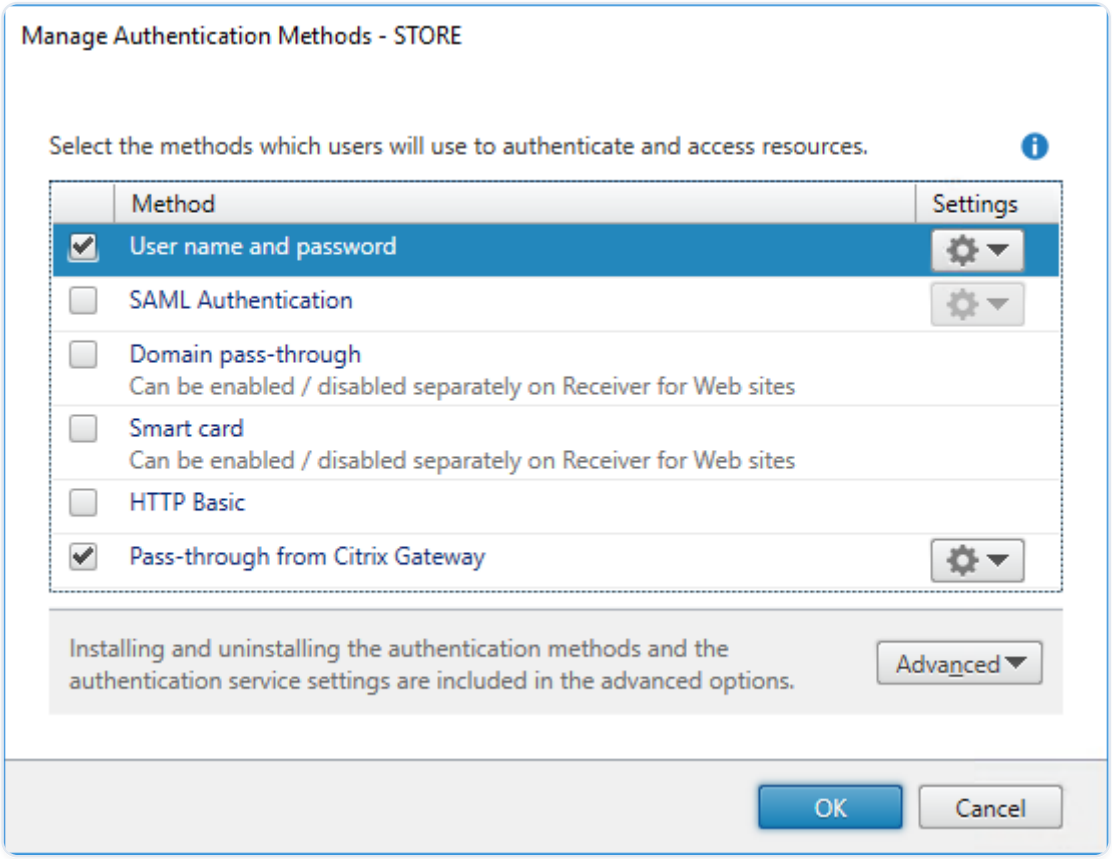

Edit NetScaler Gateway appliance - ProductionGateway
StoreFront
General Settings
Secure Ticket Authority
Authentication Settings
Authentication Settings
These settings specify how the remote user provides authentication credentials
Version:
10.0 (Build 69.4) or later
VServer IP address: (optional)
Logon type:
Domain
Smart card fallback:
None
Callback URL: (optional)
https://callback.production.com
/CitrixAuthService/AuthService.asmx
OK
Cancel
Apply

注意：

可能需要添加 DNS 条件转发器，以便两个域中使用的 DNS 服务器可以解析另一个域上的 FQDN。Citrix Gateway 必须能够使用其 `production.com` DNS 服务器解析 `development.com` 域上的 STA 服务器 FQDN。StoreFront 还应能够使用其 `development.com` DNS 服务器解析 `production.com` 域上的回调 URL。或者，可以使用解析为 Citrix Gateway 虚拟服务器虚拟 IP (VIP) 的 `development.com` FQDN。

启用 Citrix Gateway 直通

1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择**存储**，然后在**操作**窗格中单击**管理身份验证方法**。
2. 在“管理身份验证方法”屏幕上，选择**从 Citrix Gateway 直通**。
3. 单击“**确定**”。



使用 Gateway 配置商店以进行远程访问

1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择**存储**节点，然后在结果窗格中选择一个存储。在**操作**窗格中，单击**配置远程访问设置**。
2. 选择**启用远程访问**。
3. 确保已将 Citrix Gateway 注册到您的商店。如果未注册 Citrix Gateway，STA 票证将无法工作。

配置远程访问设置窗口的屏幕截图(/en-us/storefront/2507-ltsr/media/stores/configure-remote-access-settings.png)

禁用令牌一致性

1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择**存储**节点，并在结果窗格中选择一个存储。在**操作**窗格中，单击**配置存储设置**。
2. 在“配置存储设置”页面上，选择**高级设置**。
3. 清除**要求令牌一致性**复选框。有关详细信息，请参阅高级存储设置。

   高级设置要求令牌一致性设置的屏幕截图(/en-us/storefront/2507-ltsr/media/stores/store-advanced-settings-token-consistency.png)
4. 单击“**确定**”。

> 注意：
>
> 默认情况下，已选择（启用）“要求令牌一致性”设置。如果禁用此设置，用于 Citrix Gateway 端点分析 (EPA) 的 SmartAccess 功能将停止工作。

禁用 Citrix Gateway 对网站的直通

> **重要提示：**
>
> 禁用 Citrix Gateway 直通可防止网站尝试使用从 Citrix Gateway 传递的 `production.com` 域中的不正确凭据。禁用 Citrix Gateway 直通会导致网站提示用户输入凭据。这些凭据与通过 Citrix Gateway 登录时使用的凭据不同。

1. 在 Citrix StoreFront 管理控制台的左侧窗格中选择**存储**节点。
2. 选择要修改的**存储**。
3. 在**操作**窗格中，单击**管理网站**。
4. 在“身份验证方法”中，清除**从 Citrix Gateway 直通**。
5. 单击“**确定**”。

编辑 Web 版 Receiver 站点窗口的“身份验证方法”部分的屏幕截图(/en-us/storefront/2507-ltsr/media/integrate-with-citrix-gateway-and-citrix-adc/recr-for-web-site-authentication-methods.png)

使用 `production.com` 用户和凭据登录到 Gateway

要测试，请使用 `production.com` 用户和凭据登录到 Gateway。

登录屏幕截图(/en-us/storefront/2507-ltsr/media/integrate-with-citrix-gateway-and-citrix-adc/log-on-to-gateway-production.png)

登录后，系统会提示用户输入 `development.com` 凭据。

第二个登录屏幕截图(/en-us/storefront/2507-ltsr/media/integrate-with-citrix-gateway-and-citrix-adc/recr-for-web-logon.png)

在 StoreFront 中添加受信任域下拉列表（可选）

此设置是可选的，但它可能有助于防止用户意外输入错误的域以通过 Citrix Gateway 进行身份验证。

如果两个域的用户名相同，则更有可能输入错误的域。新用户也可能习惯于通过 Citrix Gateway 登录时省略域。然后，当系统提示用户登录到 Receiver for Web 站点时，用户可能会忘记为第二个域输入 domain\username。

1. 在 Citrix StoreFront 管理控制台的左窗格中选择“**应用商店**”，然后在“**操作**”窗格中，单击“**管理身份验证方法**”。
2. 选择“**用户名和密码**”旁边的下拉箭头。
3. 单击“**添加**”以将 `development.com` 添加为受信任域，然后选中“**在登录页面中显示域列表**”复选框。
4. 单击“**确定**”。

配置受信任域窗口的屏幕截图(/en-us/storefront/2507-ltsr/media/integrate-with-citrix-gateway-and-citrix-adc/configure-trusted-domains.png)

带有域下拉列表的登录屏幕截图(/en-us/storefront/2507-ltsr/media/integrate-with-citrix-gateway-and-citrix-adc/logon-with-trusted-domain.png)

> **注意：**

> 在此身份验证方案中，不建议使用浏览器密码缓存。如果用户为两个不同的域帐户设置了不同的密码，密码缓存可能会导致糟糕的体验。

NetScaler® 会话操作策略

- 如果在 Citrix Gateway 会话策略中启用了 Web 应用程序的单点登录，则 Citrix Gateway 发送到网站的错误凭据将被忽略，因为您已在网站上禁用了“**从 Citrix Gateway 直通**”身份验证方法。无论此选项设置为如何，网站都会提示输入凭据。
- 在 Citrix Gateway 的“客户端体验”和“已发布应用程序”选项卡中填充单点登录条目不会改变本文所述的行为。

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration | **Client Experience** | Security | Published Applications

Accounting Policy

Override Global

Display Home Page

Home Page

https://sf.development.com/Citrix/S

URL for Web-Based Email

Split Tunnel*

OFF

Session Time-out (mins)

60

Client Idle Time-out (mins)

Clientless Access*

On

Clientless Access URL Encoding*

Clear

Clientless Access Persistent Cookie*

ALLOW

Plug-in Type*

Windows/MAC OS X

Windows Plugin Upgrade

Always

Linux Plugin Upgrade

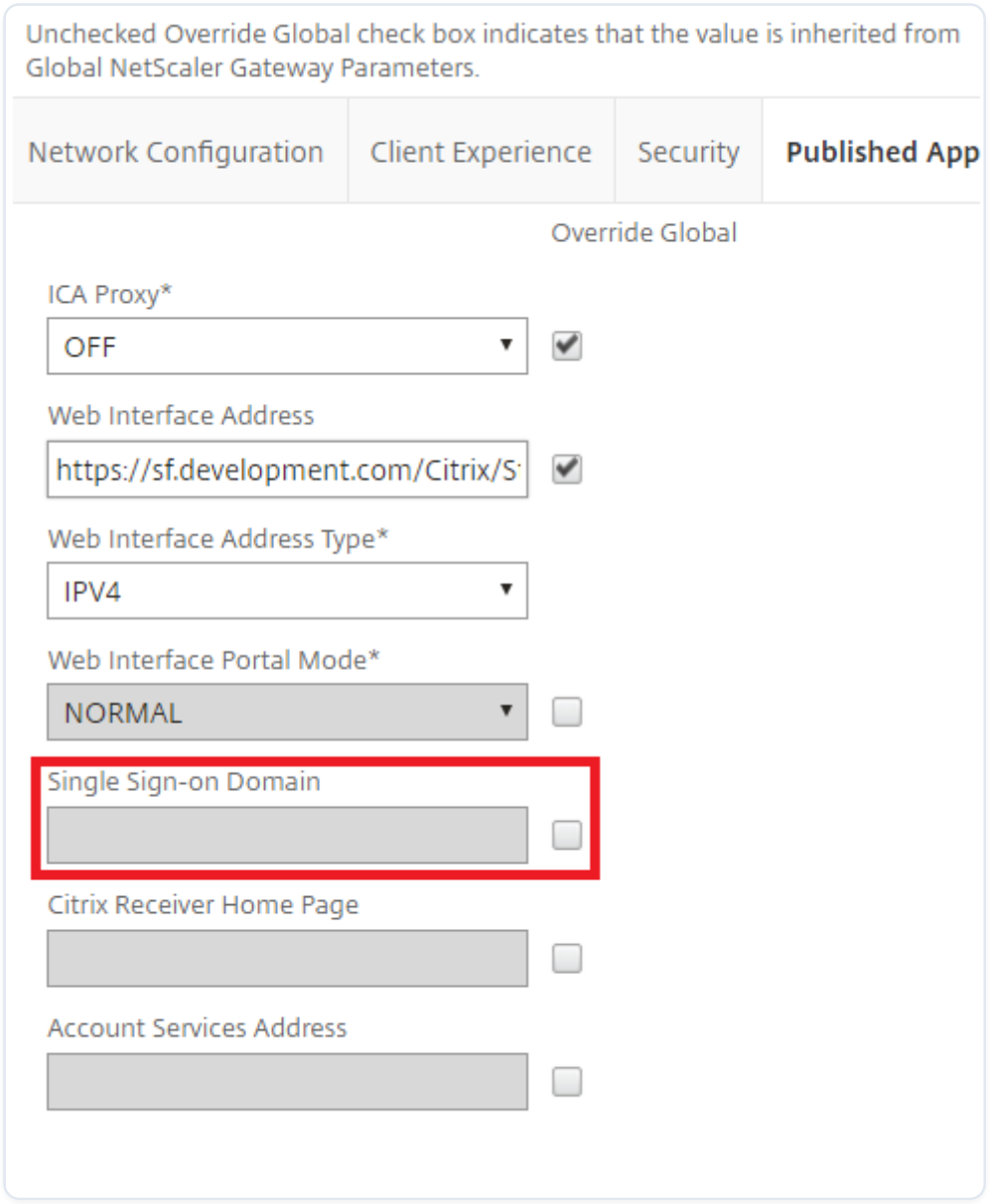
Always

MAC Plugin Upgrade

Always

AlwaysON Profile Name

Single Sign-on to Web Applications

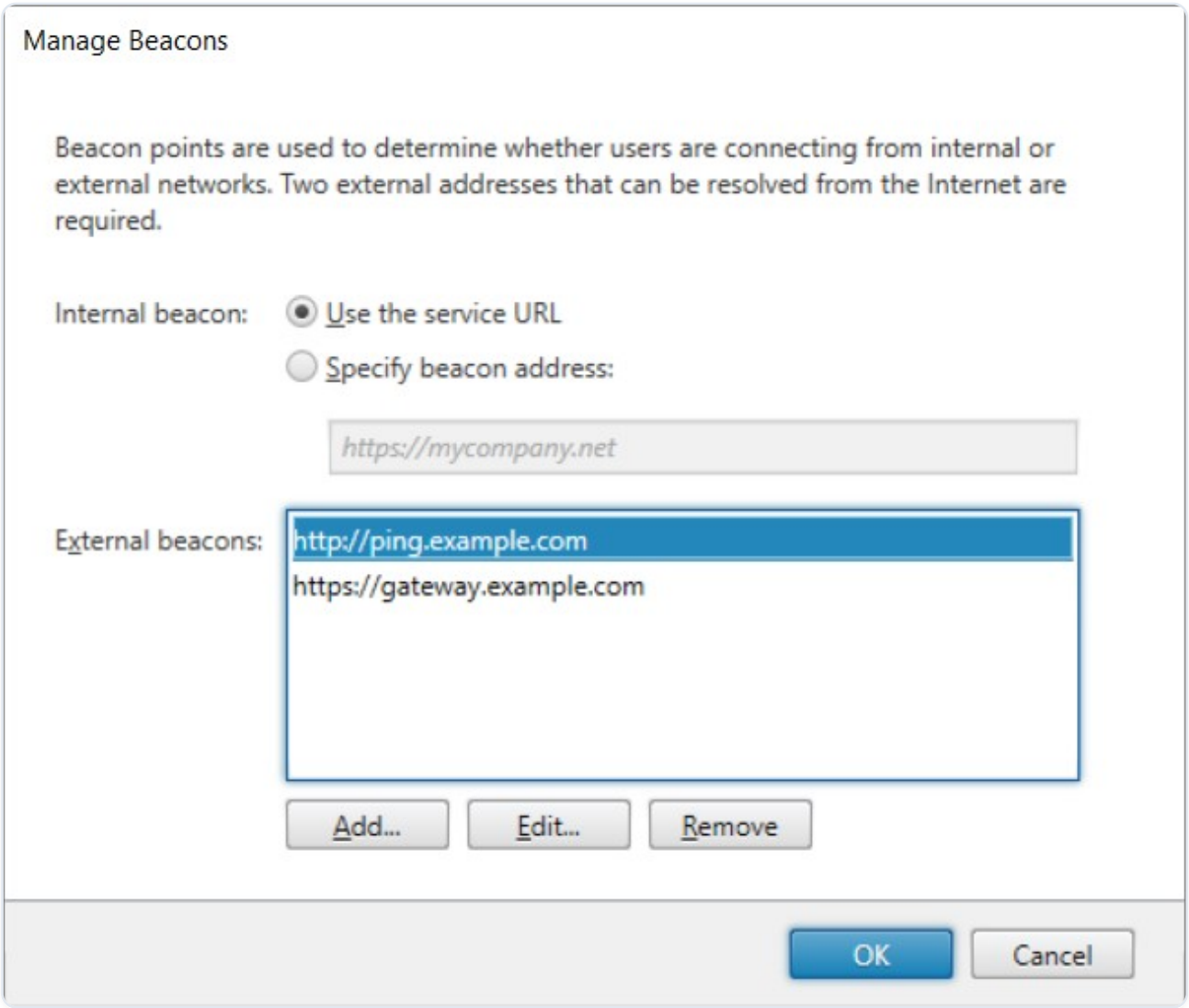


配置信标点

重要提示：

- `http://ping.citrix.com` 已不再可用，不应使用。
- 请勿使用您不拥有的第三方网站作为外部信标。请改用由您的组织控制的网站。
- 内部和外部信标 URL 应为完全限定域名 (FQDN)，例如 (`http://example.com`)，而不是缩写的 NetBIOS 名称 (`http://example`)。

> 在“管理信标”屏幕中，指定内部网络内外用作信标点的 URL。本地安装的 Citrix Workspace 应用程序会尝试联系信标点，并使用响应来确定用户是连接到本地网络还是公共网络。当用户访问桌面或应用程序时，位置信息会传递给提供资源的服务器，以便将适当的连接详细信息返回给 Citrix Workspace 应用程序。这可确保用户在访问桌面或应用程序时不会再次被要求登录。基于浏览器的 HDX 客户端不使用信标。适用于 Windows 2503 及更高版本的 Citrix Workspace 应用程序仅使用内部信标，不使用外部信标。旧版本和在其他平台上运行的 Citrix Workspace 应用程序同时使用内部和外部信标。



例如，如果内部信标点可访问，则表示用户已连接到本地网络。但是，如果 Citrix Workspace 应用程序无法联系内部信标点并从两个外部信标点接收到响应，则表示用户具有 Internet 连接，但位于公司网络外部。因此，用户必须通过 Citrix Gateway 连接到桌面和应用程序。当用户访问桌面或应用程序时，提供资源的服务器会收到通知，以提供必须通过其路由连接的 Citrix Gateway 设备详细信息。这意味着用户在访问桌面或应用程序时无需登录设备。

默认情况下，StoreFront 设置：

- 内部信标为部署的基本 URL。

- 外部信标为：
  - `http://ping.citrix.com`。此项已不再可用，必须替换为您自己的信标。
  - 您添加的第一个 Citrix Gateway 部署的 URL。

要配置信标点：

1. 在 Citrix StoreFront 管理控制台的左窗格中选择“**应用商店**”节点，然后在“操作”窗格中单击“**管理信标**”。
2. 指定用作内部信标点的 URL。
   - 要使用 StoreFront 部署的服务器 URL 或负载均衡 URL，请选择 **使用服务 URL**。
   - 要使用备用 URL，请选择 **指定信标地址** 并输入内部网络中高可用的 URL。
3. 单击 **添加** 以输入外部信标点的 URL。要修改信标点，请在“外部信标”列表中选择该 URL，然后单击 **编辑**。在列表中选择一个 URL，然后单击 **删除** 以停止将该地址用作信标点。

   您必须指定至少两个可从 Internet 解析的高可用外部信标点。这些信标点必须响应 HTTP HEAD 请求。您应该使用由您的组织控制的 URL，而不是第三方网站。

如果更改任何信标点，请确保用户使用修改后的信标信息更新 Citrix Workspace 应用程序。用户可以通过使用 Web 浏览器登录并转到帐户设置来获取更新的 Citrix Workspace 应用程序预配文件。否则，您可以为应用商店导出预配文件，并将其提供给您的用户。

PowerShell

要获取当前信标，请使用 Get-STFRoamingBeacon。

要添加信标，请使用 Set-STFRoamingBeacon。

要将信标设置为默认值，请使用 Clear-STFRoamingBeacon。

创建一个内部和外部都使用的单个 FQDN

您可以创建一个单独的完全限定域名 (FQDN)，该域名可以直接从公司网络内部访问应用商店，也可以通过 Citrix Gateway 远程访问。

例如，您可以使用以下 URL：

- `https://storefront.example.com` 作为用户访问 StoreFront 的单个 URL。在网络内部时，它解析为 StoreFront 服务器或负载均衡器。在网络外部时，它解析为网关。

- `https://storefrontcb.example.com` 作为回调 URL。在您的网络内部时，它解析为网关。这仅适用于智能访问或无密码身份验证。您必须确保网关上的证书包含此地址作为 SAN，或者使用通配符证书。

服务器组基本 URL

将基本 URL 更改为单个 URL。请参阅更改部署的基本 URL。

本地安装的 Citrix Workspace 应用程序的 StoreFront 信标

本地安装的 Citrix Workspace™ 应用程序会尝试联系信标点，并使用响应来确定用户是连接到本地网络还是公共网络。

默认情况下，StoreFront 使用服务器组基本 URL 作为内部信标 URL。在此配置中，相同的 URL 在内部和外部都有效，因此不能用作信标。因此，您必须将内部信标设置为您知道只能在内部访问的 URL。

请参阅配置信标。

外部 DNS

- storefront.example.com 解析为 Citrix Gateway 虚拟服务器的外部 IP。

内部 DNS

- storefront.example.com 解析为 StoreFront 负载均衡器或单个 StoreFront 服务器 IP。
- storefrontcb.example.com 解析为网关 vServer VIP。如果 DMZ 和企业本地网络之间存在防火墙，请允许此访问。

当通过网关连接时要求使用 Citrix Workspace™ app

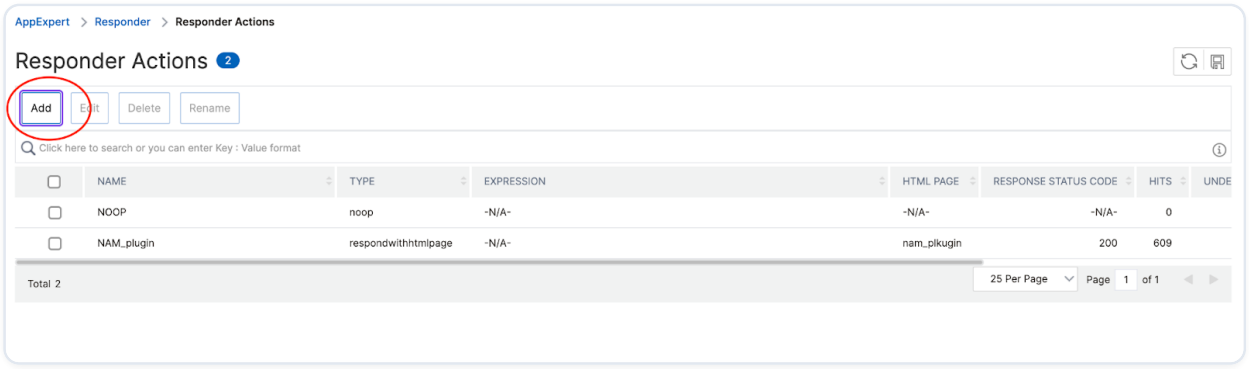
您可以通过使用插件，要求用户在通过网关连接时使用 Citrix Workspace app。

要将插件部署到您的网关：

1. 从 Citrix 下载 下载插件。
2. 解压 zip 文件和 citrix-gateway-plugin.tar.gz。它包含一个 HTML 文件和一个 JavaScript 文件。
3. 将文件复制到 NetScaler 网关的 `/var/netscaler/gui/vpn/init` 下
4. 使用管理 GUI 配置 或 使用 CLI 配置

使用管理 GUI 配置

1. 登录 Netscaler® 管理 GUI。
2. 创建响应程序操作并单击“添加”。

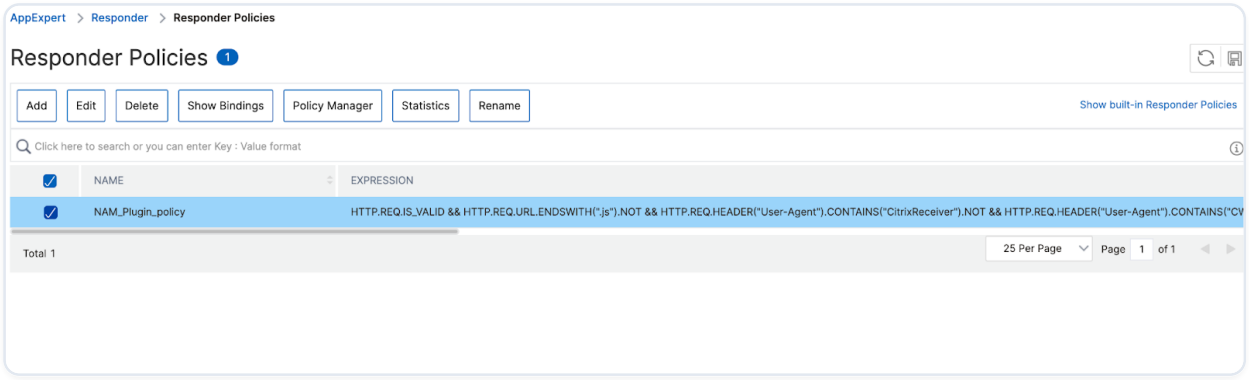


3. 配置响应程序操作：

   类型：使用 HTML 页面响应

   添加：输入路径 `/vpn/init/native-app-mandate.html`

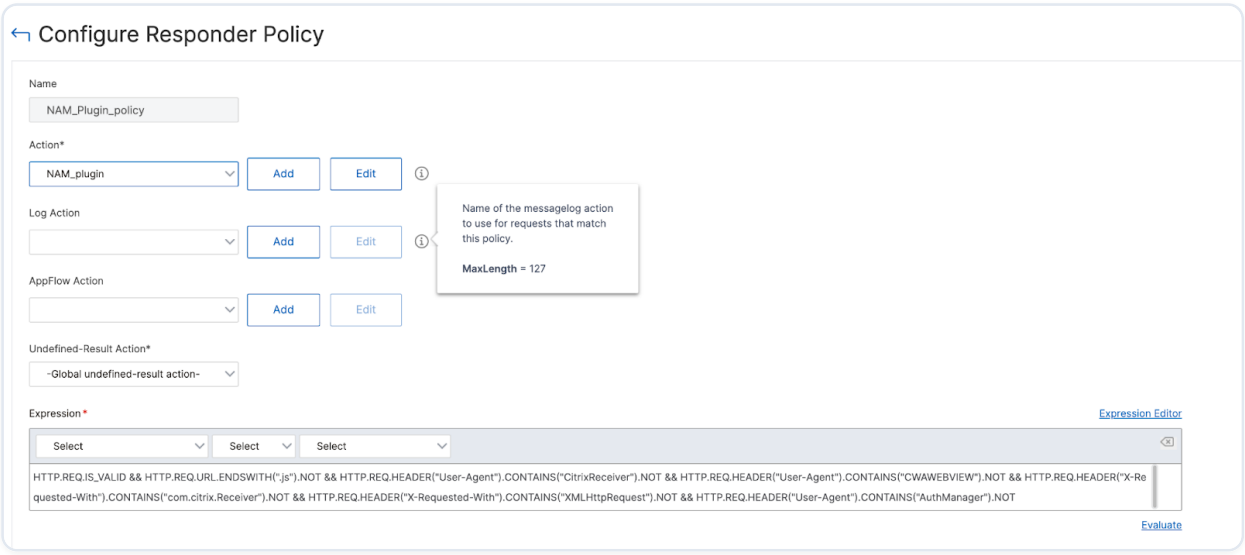
4. 创建响应程序策略。



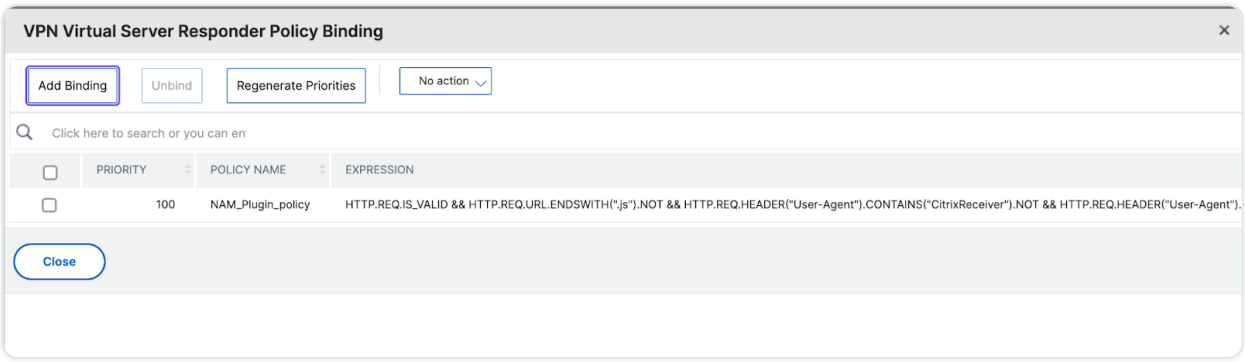
5. 配置响应程序策略：

   操作：您在上面创建的操作的名称。

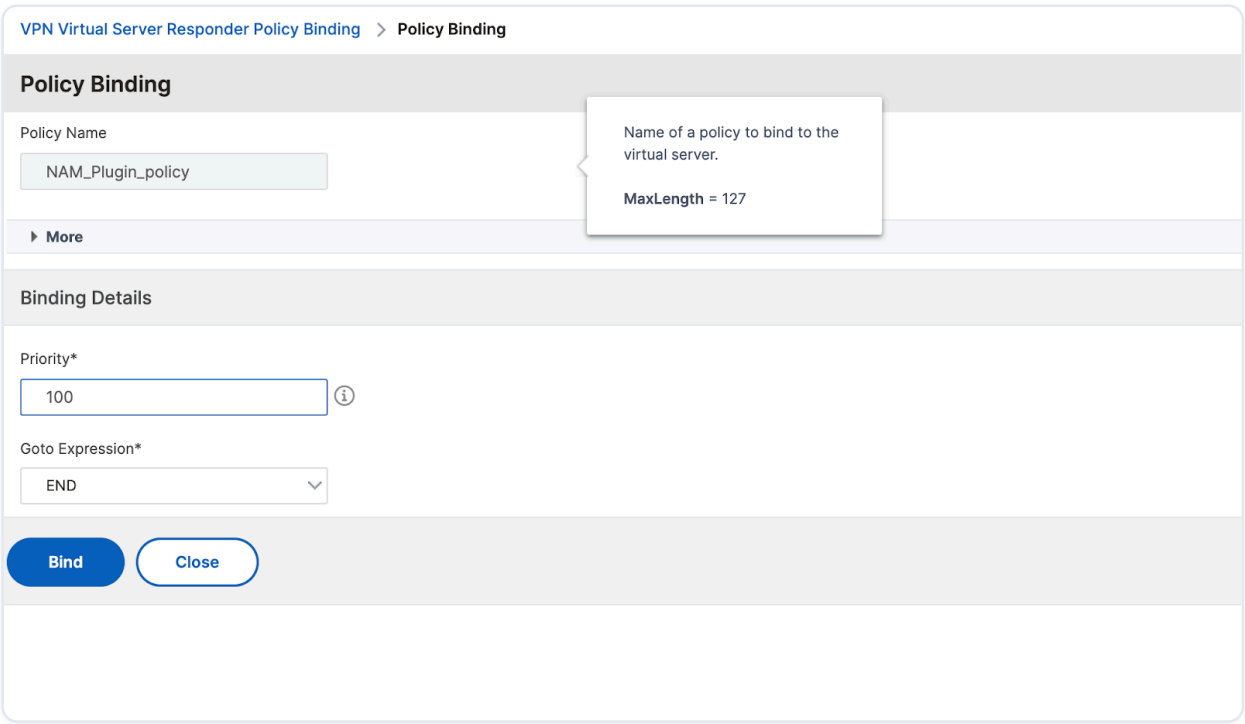
   表达式：`HTTP.REQ.IS_VALID && HTTP.REQ.URL.ENDSWITH(".js").NOT && HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT && HTTP.REQ.HEADER("User-Agent").CONTAINS("CWAWEBVIEW").NOT && HTTP.REQ.HEADER("X-Requested-With").CONTAINS("com.citrix.Receiver").NOT && HTTP.REQ.HEADER("X-Requested-With").CONTAINS("XMLHttpRequest").NOT && HTTP.REQ.HEADER("User-Agent").CONTAINS("AuthManager").NOT`



6. 导航到要绑定响应程序策略的虚拟服务器。



7. 绑定您创建的策略。



8. 要验证其配置是否正确，请打开网关 URL 以确认其显示“**需要 Citrix Workspace 应用程序**”屏幕。将 Netscaler URL 添加到 Citrix Workspace 应用程序，并确认其不显示“**需要 Citrix Workspace 应用程序**”屏幕。

使用 CLI 进行配置

要使用 CLI 配置“需要 Citrix Workspace 应用程序”功能，请执行以下操作：

1. 创建包含 HTML 文件的响应程序操作（您可以在 GUI 中编辑配置）

```
add responder action respond_with_html_act respondwithhtmlpage
sample_page -responseStatusCode 200
```

2. 创建响应程序策略以处理来自 Web 浏览器而非 Citrix Workspace 应用程序的请求。

```
add responder policy respond_with_html_pol "HTTP.REQ.IS_VALID &&
HTTP.REQ.URL.ENDSWITH(".js").NOT && HTTP.REQ.HEADER("User-
Agent").CONTAINS("CitrixReceiver").NOT && HTTP.REQ.HEADER("User-
Agent").CONTAINS("CWAWEBVIEW").NOT && HTTP.REQ.HEADER("X-Requested-
With").CONTAINS("com.citrix.Receiver").NOT && HTTP.REQ.HEADER("X-
Requested-With").CONTAINS("XMLHttpRequest").NOT &&
HTTP.REQ.HEADER("User-Agent").CONTAINS("AuthManager").NOT"
respond_with_html_act
```

3. 将策略绑定到 VPN 虚拟服务器

```
bind vpn vserver vpn_vs -policy respond_with_html_pol -priority 100
-gotoPriorityExpression END -type AAA_REQUEST
```

通过 OIDC 进行 Entra ID 身份验证以及到 VDA 的单点登录

本文介绍了如何配置 StoreFront 和 NetScaler ADC，以允许用户通过 OIDC 使用 Entra ID 进行身份验证，然后单点登录到已加入 Entra 的 VDA。

重要提示：

通过 OIDC 进行 Entra ID 身份验证以及到 VDA 的单点登录目前处于预览阶段。此功能不提供支持，并且尚不建议在生产环境中使用。

先决条件

- NetScaler ADC
- StoreFront 2507 LTSR CU1 或更高版本
- 现代体验
- Microsoft Entra ID 以及具有以下权限之一的帐户：
  - 云应用程序管理员
  - 应用程序管理员
  - 全局管理员
- 带有连接器的 DaaS 订阅。CVAD 不提供此功能。
- 已发布的桌面和/或应用程序
- 对于从 Web 浏览器启动到 Citrix Workspace 应用程序的情况，为了启用对 VDA 的 SSO，需要 Citrix Web 扩展。

已知问题和限制

- 在通过 Entra ID 身份验证的 Store 上启用联合身份验证服务不受支持，并且可能导致启动失败。
- 如果 Store 包含 Citrix Virtual Apps and Desktops 站点，并且用户通过 OIDC 使用 Entra ID 进行身份验证，则 StoreFront 不会枚举该站点的任何资源。
- Entra ID 单点登录到 VDA 仅在使用基于 OIDC 的身份验证时受支持。SAML 不支持此功能。
- 当用户属于许多 Entra 组时，StoreFront 会占用大量 RAM。

使用 OIDC 进行 Entra ID 身份验证

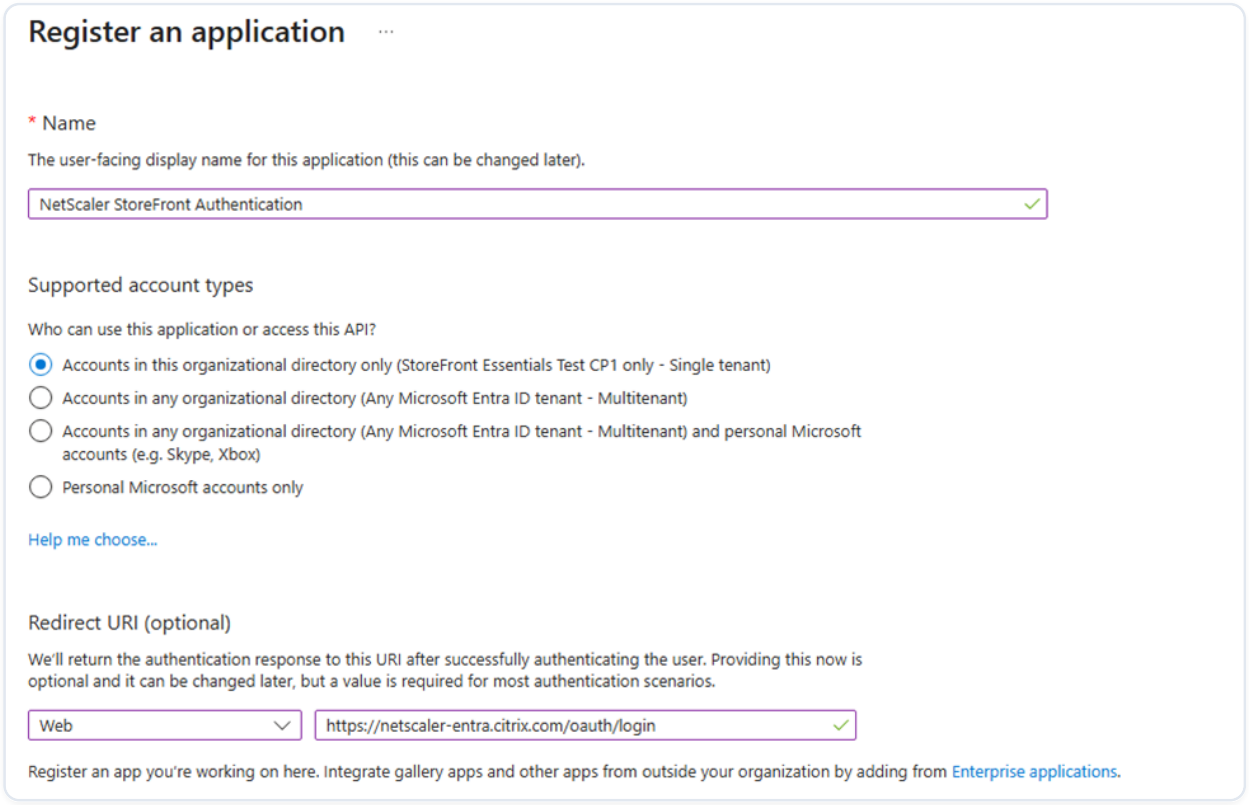
本节介绍如何配置 NetScaler 和 StoreFront，以便用户可以使用 Entra ID 进行身份验证。在此配置中，用户可以拥有混合身份，也可以拥有不带 Active Directory 帐户的纯 Entra 身份。

创建 Microsoft Azure Entra ID 应用程序

Microsoft Entra ID 中的应用程序注册定义了您的应用程序，以便 Entra ID 能够识别它——在本例中为 NetScaler OIDC。此注册还管理应用程序的身份验证和授权请求。由于 OAuth 需要受信任的身份提供程序 (IdP) 来对用户进行身份验证并颁发令牌，因此注册您的应用程序会告知 Entra ID：“此应用程序使用您作为其 OAuth 流的 IdP。”

1. 登录到 Azure 门户，以获取用于 NetScaler 或 StoreFront 身份验证的 Entra ID 租户。
2. 转到**Microsoft Entra ID 资源** > **管理** > **应用注册**，然后选择**新建注册**。
3. 命名应用程序，例如 NetScaler StoreFront 身份验证。

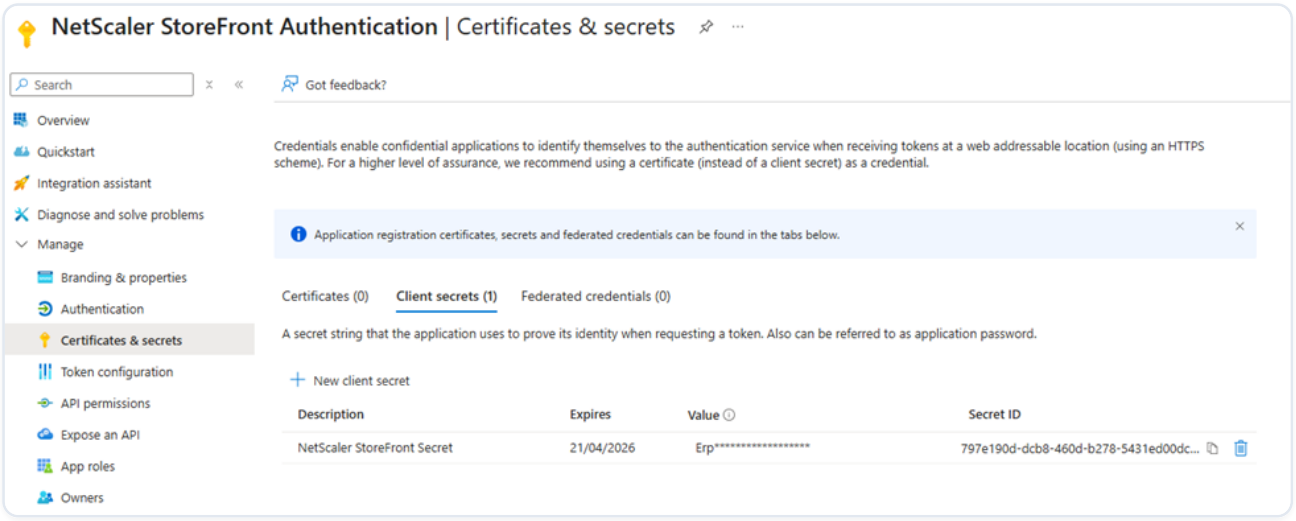
4. 在**支持的帐户类型**下，选择**仅此组织目录中的帐户**。
5. 在**重定向 URI** 下，选择**Web**作为要创建的应用程序类型。输入发送访问令牌的 URI。使用格式 \<NetScaler 虚拟服务器 URL>/oauth/login，例如 `https://netscalerentra.customer.com/oauth/login`。



创建客户端密钥

要创建客户端密钥：

1. 注册应用程序后，转到**管理** > **证书和密钥**。
2. 选择 **客户端密码**，然后选择 **新建客户端密码**。 您的应用程序使用这些凭据与 IdP 安全通信并请求令牌。
3. 提供密码的描述和持续时间。
4. 创建密码后，记录密码值，因为您在设置过程中稍后会用到它，并且它只在此创建阶段可见。

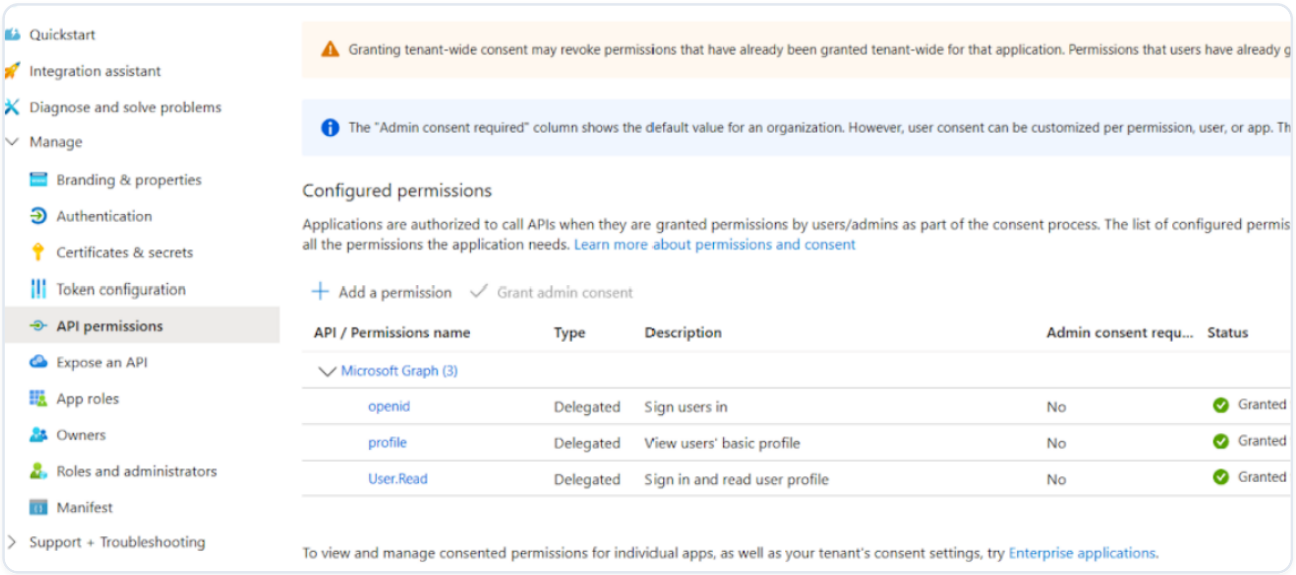


配置应用程序权限

配置应用程序权限：

1. 转到 **管理** > **应用注册**，然后选择您的应用程序。
2. 选择 **管理** > **API 权限**。
3. **User.Read** 权限默认已添加。
4. 添加 **openid** 和 **profile**。
5. 选择 **授予管理员同意以用于 \<租户名称>** 并接受。

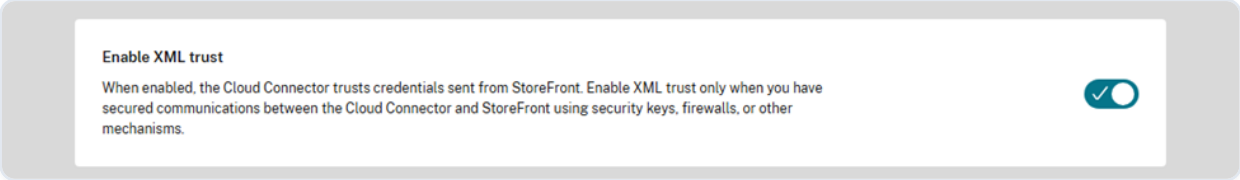
Microsoft Entra ID 中 API 权限中的“授予管理员同意”意味着管理员代表组织中的所有用户批准应用程序使用请求的权限访问特定资源或 API。



配置 Citrix DaaS 以启用 XML 信任

默认情况下，Citrix DaaS 使用用户的 Active Directory 凭据对请求进行身份验证。使用 Entra ID 身份验证时，StoreFront 没有凭据。因此，您必须配置 DaaS 以信任 StoreFront，而无需使用身份验证。强烈建议您启用安全密钥以提供服务级别身份验证。

1. 登录 Citrix Cloud 并前往 DaaS 控制台。
2. 转到“**设置**”。
3. 启用“**XML 信任**”。



4. （可选步骤）为了增强安全性，您可以在 DaaS 和 StoreFront 之间启用安全密钥。有关详细信息，请参阅 Citrix DaaS™ 文档中的管理安全密钥。

配置 NetScaler 身份验证配置文件

本节介绍如何配置可绑定到网关 VPN 虚拟服务器的 NetScaler 身份验证配置文件。此配置告知 ADC 如何将用户重定向到外部 OAuth IdP（例如 Microsoft Entra ID）进行登录，以及如何处理身份验证后收到的 OAuth 令牌。它指定了端点、客户端凭据、范围以及 ADC 如何从令牌中提取用户信息。

您需要前面步骤中的客户端密钥和 Microsoft Entra ID 身份验证端点。您可以通过转到 Azure 门户中的“应用注册概述”并单击“**终结点**”选项卡来查找身份验证端点。

创建身份验证虚拟服务器

身份验证虚拟服务器处理用户身份验证。

```
add authentication vserver EntraId_Authentication_VirtualServer SSL
0.0.0.0 443 \

  -state ENABLED \

  -authentication ON \

  -td 0 -appflowLog ENABLED \

  -noDefaultBindings NO

bind ssl vserver EntraId_Authentication_VirtualServer \
```

```
  -certkeyName <Certificate Key Name>
```

创建 OAuth 策略和操作

OAuth 操作指定 NetScaler ADC 如何与 OAuth IdP（例如 Microsoft Entra ID）交互。此操作允许 Citrix Gateway 将用户重定向到 IdP 进行登录并处理返回的 OAuth 令牌。它将 `userNameField` 设置为 `oid`，这会导致网关在向 StoreFront 进行身份验证时将 OID 作为用户名传递。StoreFront 会验证 OID 是否与通过查找 Entra ID 访问令牌获得的信息匹配，否则身份验证将失败。

您需要前面步骤中的客户端 ID 和客户端密钥。

```
add authentication OAuthAction EntraId_Oauth_Server \

  -authorizationEndpoint "https://login.microsoftonline.com/<TenantId>/
oauth2/v2.0/authorize\?prompt=login" \

  -tokenEndpoint "https://login.microsoftonline.com/<TenantId>/oauth2/
v2.0/token" \

  -clientID <ClientId> \

  -clientSecret <ClientSecret> \

  -Attribute1 email \

  -Attribute2 family_name \

  -Attribute3 given_name \

  -Attribute4 upn \

  -CertEndpoint "https://login.microsoftonline.com/<TenantId>/discovery/
v2.0/keys" \

  -userNameField oid \

  -allowedAlgorithms HS256 RS256 RS512 \

  -PKCE ENABLED \

  -tokenEndpointAuthMethod client_secret_post \
```

```
  -OAuthType GENERIC \

  -grantType CODE \

  -refreshInterval 1440

add authentication Policy EntraId_Authentication_Policy \

  -rule true \

  -action EntraId_Oauth_Server
```

`authorizationEndpoint` 包含查询字符串参数 `prompt=login`，以便用户在尝试通过 NetScaler 访问 StoreFront 时被迫重新进行身份验证。

将身份验证策略绑定到虚拟服务器

```
bind authentication vserver EntraId_Authentication_VirtualServer \

  -policy EntraId_Authentication_Policy \

  -priority 100 \

  -gotoPriorityExpression END
```

创建身份验证配置文件

```
add authentication authnProfile EntraId_Auth_Profile \

  -authnVsName EntraId_Authentication_VirtualServer \

  -AuthenticationLevel 0
```

创建 VPN 虚拟服务器并绑定身份验证配置文件

使用前面步骤中创建的身份验证配置文件，完成 将 NetScaler Gateway 与 StoreFront 集成 中的步骤 1、2 和 4。

或者，如果您已有合适的 Citrix Gateway，则可以将其绑定到新的身份验证配置文件。运行此命令将替换现有身份验证配置文件。

```
set vpn vserver <StoreFront ICA Proxy vServer> \

  -authentication ON \

  -authnProfile EntraId_Auth_Profile
```

用于 StoreFront 单点登录的 Entra ID 令牌注入配置

Citrix Gateway 对用户进行身份验证后，必须将足够的信息传递给 StoreFront，以便 StoreFront 能够验证用户是否已通过身份验证并查找组成员身份。默认情况下，Citrix Gateway 仅发送 Active Directory 用户名和密码。在 Entra ID 身份验证的情况下，它必须传递 Entra ID 访问令牌，以便 StoreFront 可以使用 Microsoft Graph API 查找用户信息。为此，您必须添加一个重写策略，将 Entra ID 令牌添加到其用于向 StoreFront 验证用户的调用中。如果重写 Entra ID 访问令牌策略未生效，则登录将失败。如果重写策略功能默认未启用，则必须先启用它。

```
enable ns feature Rewrite

add rewrite action EntraId_Oauth_Insert_AccessToken_Header
insert_http_header X-Citrix-OIDC-Access-Token
"AAA.USER.ATTRIBUTE(\"accesstoken\")" \

  -comment "A rewrite policy to add the OAUTH access_token to subsequent
user authentication requests"

add rewrite policy EntraId_Oauth_Insert_AccessToken_Policy
"HTTP.REQ.URL.TO_LOWER.ENDSWITH(\"gatewayauth/login\") ||
HTTP.REQ.URL.TO_LOWER.ENDSWITH(\"citrixagbasic/authenticate\")"
EntraId_Oauth_Insert_AccessToken_Header \

  -comment "A rewrite policy to add the OAUTH access_token to subsequent
user authentication requests"

bind vpn vserver <StoreFront ICA Proxy vServer> \

  -policy EntraId_Oauth_Insert_AccessToken_Policy \

  -priority 100 \

  -gotoPriorityExpression END \
```

```
-type REQUEST
```

在 StoreFront 中配置 Citrix Gateway

1. 在 StoreFront 上添加 NetScaler Gateway 实例.
2. 配置 Citrix 网关。
   - 将登录类型设置为 **Domain**。
   - 指定一个有效的回调 URL。StoreFront 使用 Entra ID 身份验证时需要此项。
3. 为聚合 Citrix DaaS 资源的 Store (/zh-cn/storefront/2507-ltsr/stores/remote-access.html)配置网关以进行远程访问。
4. 从 NetScaler Gateway 启用并配置 Entra ID 身份验证。运行以下 PowerShell，将租户 ID 替换为您的 Entra ID 租户中的 ID，并将 `/Citrix/EntraStore` 替换为存储路径。

```
$store = Get-STFStoreService /Citrix/EntraStore

$authenticationService = Get-STFAuthenticationService -Store $store

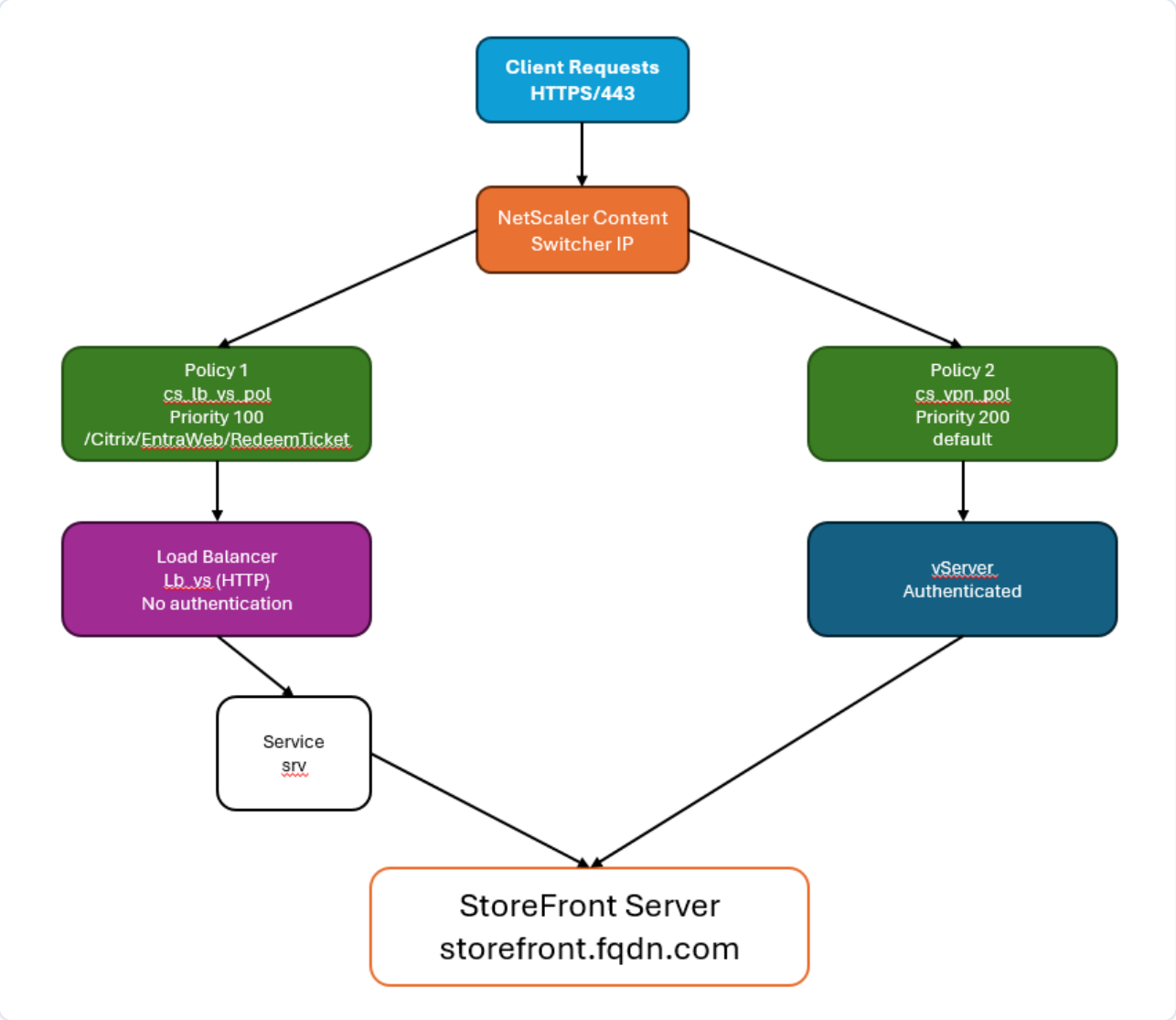
Set-STFEntraIdSettings -AuthenticationService $authenticationService
-TenantId "<Your tenant id>" -Enabled $true
```

配置 Entra ID 单点登录到 VDA

在您配置 StoreFront 和 Citrix Gateway 以使用 Entra ID 验证用户后，您可以启用 Entra ID 单点登录到 VDA，而无需 FAS。仅在完成 DaaS 配置后才启用此功能。有关详细信息，请参阅 (/zh-cn/citrix-daas/install-configure/session-authentication/entra-sso.html)。这需要为 StoreFront 和 NetScaler ADC 进行以下额外配置。

配置 NetScaler ADC 内容切换

通常，所有对 StoreFront 的请求都通过网关 VServer，因此需要身份验证。当用户启动已加入 Entra ID 的 VDA 时，Citrix Workspace 应用程序必须再次向 Azure 进行身份验证（如果 Entra ID 会话仍然有效，则进行 SSO）并检索访问令牌。作为此流程的一部分，StoreFront 会生成一个令牌，该令牌必须由在 Citrix Cloud 中运行的服务进行验证。此服务必须能够回调到 StoreFront 端点 `/Citrix/<StoreWeb>/Tickets/RedeemStoreTicket` 以验证令牌。由于此服务无法访问 NetScaler 会话，因此有必要绕过 VPN 虚拟服务来处理兑换票证的调用。为此，您可以使用内容切换器。



对 `/Citrix/<StoreWeb>/Tickets/RedeemStoreTicket` 的调用将定向到负载均衡器，该负载均衡器将请求转发到 StoreFront，从而绕过网关。请注意，需要负载均衡器，因为内容切换器无法配置为直接将流量定向到 URL，并且需要一个虚拟服务器作为目标。负载均衡器不执行任何负载均衡，仅将流量转发到 StoreFront。如果您在同一台计算机上已有合适的 StoreFront 负载均衡器，则可以使用它。

所有其他调用都定向到网关的 VPN 虚拟服务器。

创建负载均衡器以从内容切换器传递到 StoreFront

如果您已经有一个负载均衡器虚拟服务器，它位于您的 StoreFront 服务器组之前并与网关在同一台计算机上运行，那么您可以跳过此步骤，并将内容切换器配置为直接将流量发送到该虚拟服务器。否则，您必须创建一个负载均衡器以将流量传递到 StoreFront 服务器。这是因为内容切换器操作必须引用一个虚拟服务器。

这些步骤略有不同，具体取决于 StoreFront 是配置为 HTTPS（推荐）还是 HTTP。

STOREFRONT 配置为 HTTPS

创建一个服务 `stf_srv`，使用其 IP 地址表示 StoreFront，并将其绑定到没有持久性的 SSL 负载均衡器。

```
add service stf_srv <StoreFront Ip Address> SSL 443

add lb vserver lb_vs SSL <lb_vs Ip Address> 443 -persistenceType NONE
-cltTimeout 180

bind lb vserver lb_vs stf_srv
```

STOREFRONT 配置为 HTTP

创建一个服务 `stf_srv`，使用其 FQDN 表示 StoreFront，并将其绑定到没有持久性的 HTTP 负载均衡器。

```
add server storefront1 <storefront fqdn>

add service stf_srv storefront1 HTTP 80

add lb vserver lb_vs HTTP 0.0.0.0 0 -persistenceType NONE -cltTimeout 180

bind lb vserver lb_vs stf_srv
```

创建 SSL 内容切换虚拟服务器

创建一个 SSL 内容切换虚拟服务器来处理客户端请求。此内容切换虚拟服务器侦听端口 443 上的 HTTPS 流量，并将请求路由到网关 VPN 虚拟服务器，或通过负载均衡器传递到 StoreFront。

默认情况下，内容切换处于禁用状态，因此如果您之前未启用，则必须启用它。

```
enable feature CS

add cs vserver cs_vs SSL <cs_vs Ip Address> 443 -cltTimeout 180
-persistenceType NONE

bind ssl vserver cs_vs -certkeyName <Certificate Name>
```

创建用于票证兑换的内容切换策略

创建基于包含 StoreFront 票证兑换路径的 URL 的负载平衡内容切换策略。

当 URL 包含 `/Citrix/<StoreWeb>/Tickets/RedeemStoreTicket` 时，此策略会匹配请求，并将其路由到负载均衡器，而无需通过 VPN 虚拟服务器。

将 `StoreEntraWeb` 替换为 StoreFront 虚拟服务器 Web 策略中的 StoreFront 网站名称。您可以使用上一步中创建的负载均衡器 `lb_vs`，也可以使用现有负载均衡器虚拟服务器作为 StoreFront 服务器的前端。

```
add cs action cs_lb_vs -targetLBVserver lb_vs

add cs policy cs_lb_vs_pol -rule "HTTP.REQ.URL.CONTAINS(\"/Citrix/
<StoreWeb>/Tickets/RedeemStoreTicket\")" -action cs_lb_vs

bind cs vserver cs_vs -policyName cs_lb_vs_pol -priority 100
```

创建用于所有其他流量的内容切换策略

创建包罗万象的内容切换策略，通过 VPN 虚拟服务器发送所有其他 StoreFront 流量以进行身份验证。

```
add cs action cs_vpn_vs -targetVserver <VPN vServer>

add cs policy cs_vpn_pol -rule TRUE -action cs_vpn_vs

bind cs vserver cs_vs -policyName cs_vpn_pol -priority 110
```

配置 VDA Entra ID 单点登录

单点登录使用户在登录 Citrix Gateway 时只需进行一次身份验证，然后即可访问其虚拟桌面和应用程序，而无需重新向 VDA 输入凭据。

```
$store = Get-STFStoreService /Citrix/EntraStore

Set-STFStoreLaunchOptions -StoreService $store -EntraIdSsoEnabled $true
```

启用或禁用 Entra ID SSO 的注意事项

1. 仅在完成 Microsoft Entra single sign-on 中描述的所有配置后，才启用 Entra ID 单点登录。否则，单点登录将失败，用户可能会遇到启动延迟或错误。

最终用户体验

最终用户可以在 Web 浏览器或 Citrix Workspace 应用程序中查看应用商店。请参阅最终用户访问。

StoreFront 提供以下用户体验：

现代体验

现代用户体验与 Citrix Workspace 保持一致。它集成了 Activity Manager，用于管理您的会话并改进搜索功能。

现代体验具有以下限制：

- 无法创建可直接引导您访问应用程序或桌面的嵌入式 URL 快捷方式。
- 无法使用 StoreFront™ Client UI Customization API 通过 JavaScript 和 CSS 进行深度自定义。但是，可以使用管理控制台完成许多自定义，从而避免了对 JavaScript 或 CSS 的需求。

有关详细信息，请参阅现代体验

经典体验

这是与 StoreFront 早期版本一致的默认用户体验。您可以使用 JavaScript 和 CSS 自定义用户界面。

有关详细信息，请参阅经典体验

思杰网关 cVPN

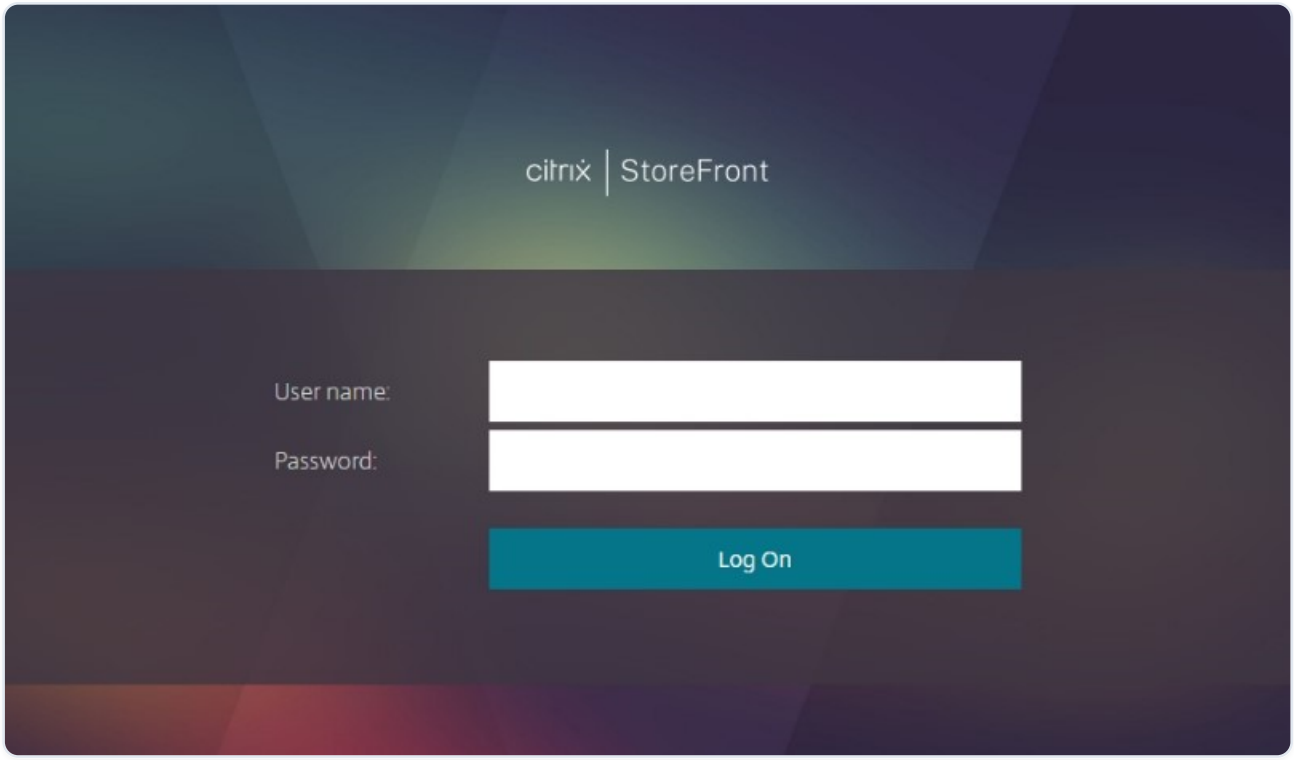
如果用户通过配置为无客户端 VPN (CVPN)的 Citrix Gateway 访问 StoreFront，则它会提供自己的用户界面，而不是显示 StoreFront 的界面。在这种情况下，StoreFront 中的某些 UI 配置设置不适用。

经典体验

本节介绍用户如何使用经典体验访问和与其应用商店进行交互。

登录

根据配置的 身份验证方法 以及是否启用了单点登录，用户可能需要登录。



如果有多种身份验证方法可用，用户可以选择切换到不同的身份验证方法。

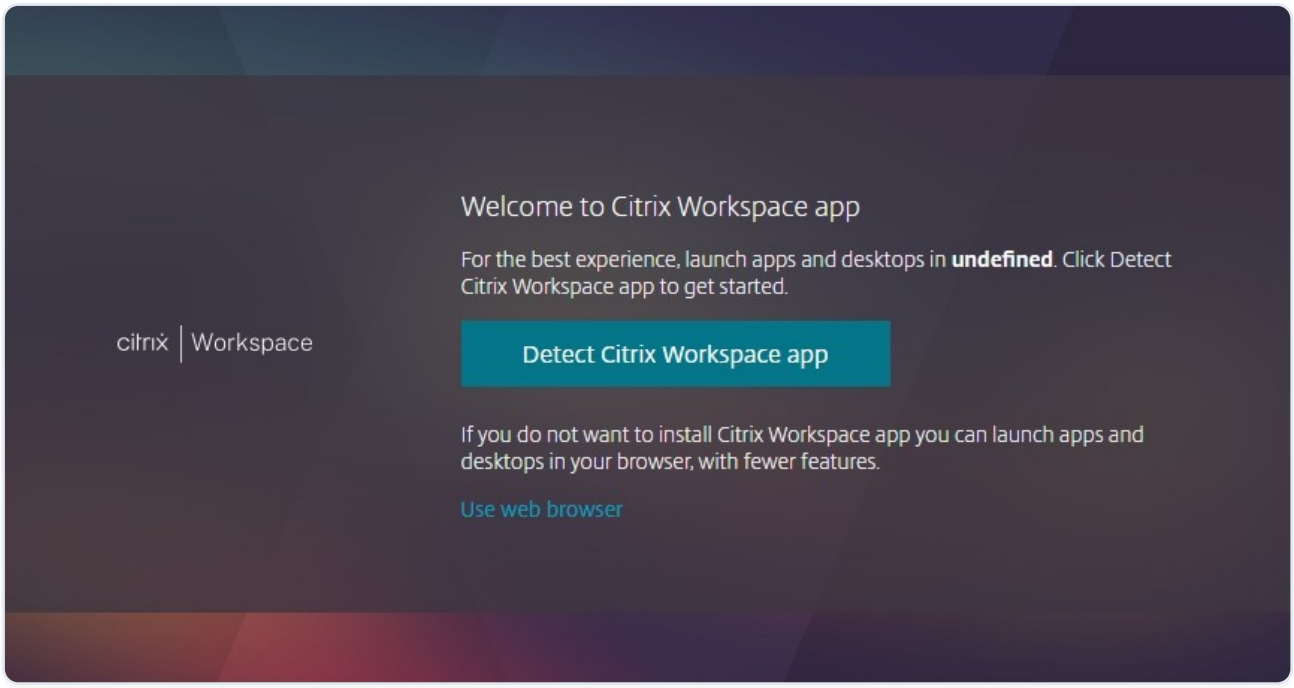
Citrix Workspace 应用程序检测

> **注意：**

> 本节仅适用于通过 Web 浏览器访问应用商店，并且 启动选项 设置为 **Open in Citrix Workspace app** 或 **Let the user choose** 的情况。此步骤可能在登录之前或之后发生，具体取决于配置。

> 如果已安装 Citrix Web Extension 并检测到 Citrix Workspace 应用程序，或者 Citrix Workspace 启动器 已禁用，则会跳过此步骤。用户可以改为从 高级设置 更改启动首选项。

> 当用户首次通过 Web 浏览器访问应用商店或清除其 Cookie 后，会看到 **Welcome to Citrix Workspace app** 屏幕。



他们可以：

- 选择 **Detect Citrix Workspace app** 以在本地安装的 Citrix Workspace 应用程序中启动资源。建议使用此选项以获得最佳体验。
- 选择 **Use web browser** 以始终在浏览器中启动资源。此选项仅在 启动选项 设置为 **Let the user choose** 时可用。

当用户选择 **Detect Citrix Workspace app** 时，它会尝试打开 **Citrix Workspace Launcher**，这是 Citrix Workspace 应用程序的一个组件。如果已安装 Citrix Workspace 应用程序，则其浏览器会弹出一个窗口，要求运行 **Citrix Workspace Launcher**。他们应选择 **Open Citrix Workspace Launcher**、**Open link**、**Open** 或 **Always open**（取决于浏览器）。建议他们还选择 **Always allow *domain* to open links of this type in the associated app**（或类似选项，取决于浏览器），以避免每次启动资源时都出现此窗口。

客户端检测权限弹出窗口截图(/en-us/storefront/2507-ltsr/media/end-user-experience/unified-ui-client-detection.png)

如果检测到本地安装的 Citrix Workspace 应用程序，几秒钟后它会继续显示下一个屏幕。当用户随后启动资源时，它会根据检测到的情况，使用 Citrix Web 扩展或 Citrix Workspace 启动器，在本地安装的 Citrix Workspace 应用程序中打开资源。

如果未安装 Citrix Workspace 应用程序，或者用户取消了启动器，则根据配置，他们有以下选项：

- **下载** - 从 Citrix 网站或 StoreFront 服务器下载 Citrix Workspace 应用程序。要隐藏此选项，请参阅 允许用户下载 Citrix Workspace 应用程序。
- **再次检测** - 尝试再次检测本地安装的 Citrix Workspace 应用程序。

- **使用 Web 浏览器** - 跳过 Workspace 应用程序检测，始终在 Web 浏览器中打开资源。要显示此选项，请将 启动选项 设置为 **让用户选择**。
- **跳过检测** - 如果用户安装了不支持 Citrix Workspace 启动器或 Citrix Web 扩展的旧版 Citrix Receiver，则可以使用此选项。如果他们选择此选项，当他们启动虚拟应用程序或桌面时，其浏览器会下载一个 **launch.ica** 文件，他们可以使用 Citrix Receiver 打开该文件。此选项会导致功能和安全性降低，因此建议管理员 禁用此选项。

主页选项卡

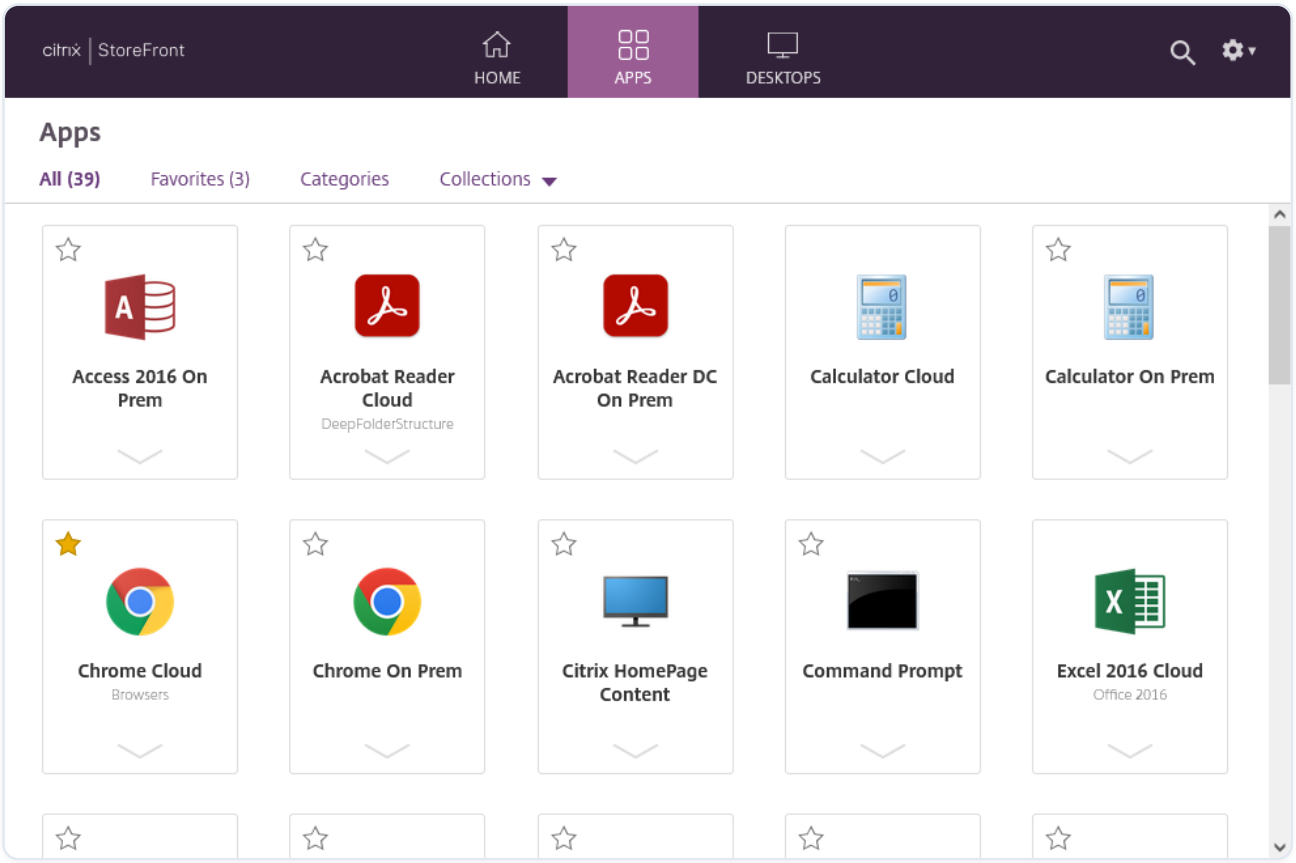
主页 选项卡显示所有特色应用程序组以及任何收藏或强制应用程序和桌面。仅当为应用商店启用了收藏夹时，才会显示 **主页** 选项卡。

主页选项卡截图(/en-us/storefront/2507-ltsr/media/end-user-experience/unified-ui-home.png)

应用选项卡

应用 选项卡包含多个子视图：

- **全部** - 显示所有应用程序。
- **收藏夹** - 显示所有收藏的应用程序。
- **类别** - 显示类别以及这些类别中的应用程序。类别的显示方式取决于 类别设置。
- **集合** 显示 特色应用程序组。



。

桌面选项卡

桌面选项卡有两个子视图：

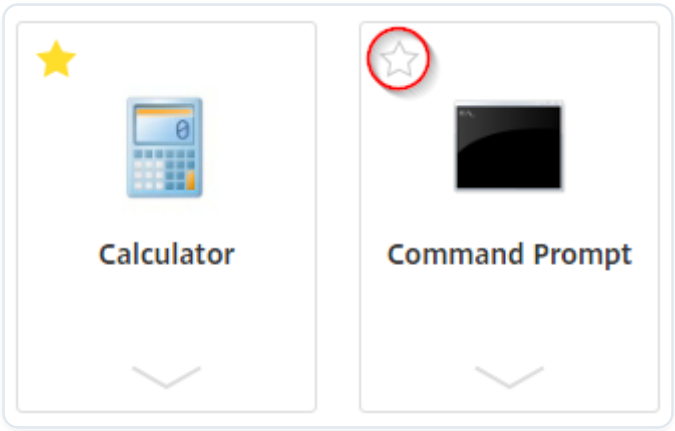
- **所有** - 显示所有桌面。
- **收藏夹** - 显示用户的收藏桌面。

应用程序和桌面磁贴

单击图标以启动应用程序或桌面。

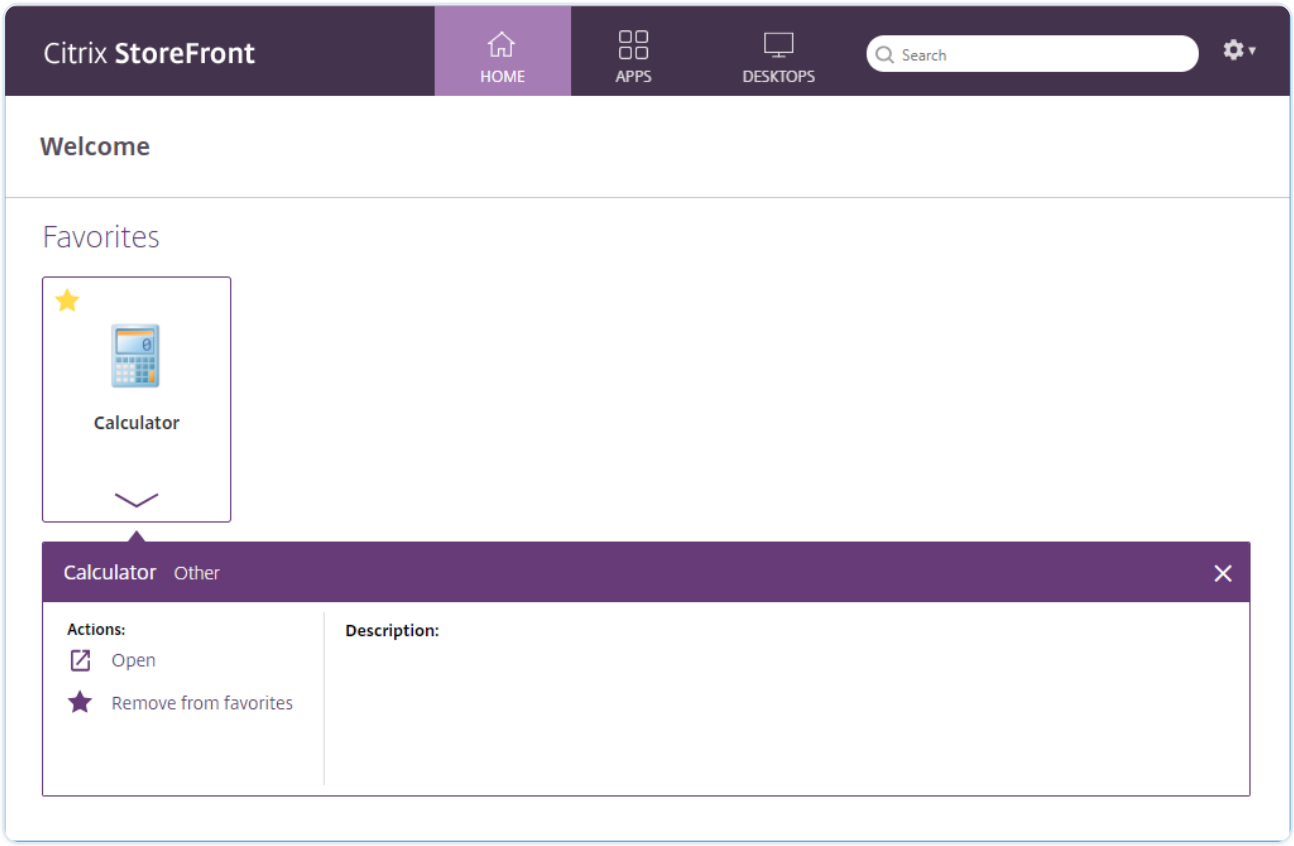
收藏夹

如果收藏夹已启用，则用户可以在资源的磁贴上选择星形图标以将其设为收藏：



查看详细信息和操作

用户可以展开每个图标下方的面板以显示应用程序说明和操作。



可能提供以下操作：

- **打开** - 启动或重新连接到应用程序或桌面。
- **添加到收藏夹** - 如果项目不是收藏夹、不是强制性的，并且商店已启用收藏夹功能，则将应用程序或桌面设为收藏夹。
- **从收藏夹中删除** - 如果项目是收藏夹、不是强制性的，并且商店已启用收藏夹功能，则将应用程序或桌面从收藏夹中删除。
- **重新启动** - 对于可重新启动的已分配桌面，此操作将重新启动桌面。

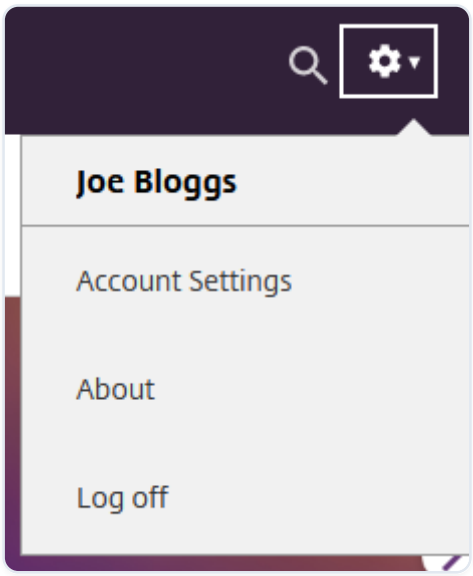
搜索

用户可以选择放大镜图标以调出搜索框。搜索所有应用程序、桌面和类别：



设置菜单

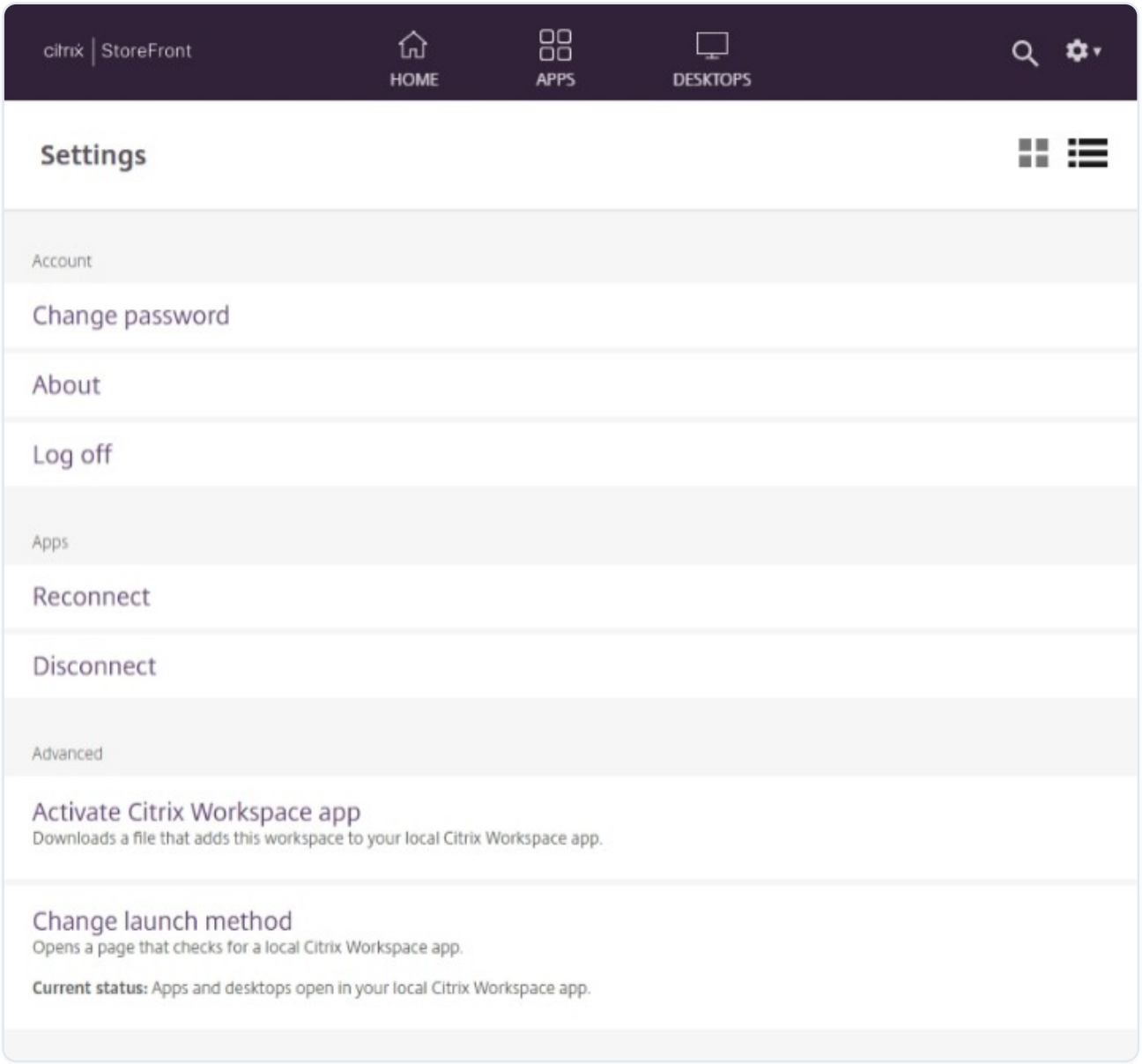
设置菜单仅在通过 Web 浏览器访问商店时可用。



设置菜单包含以下选项：

- **帐户设置** - 打开设置页面。
- **关于** - 显示有关应用程序的信息。
- **注销** - 注销网站。

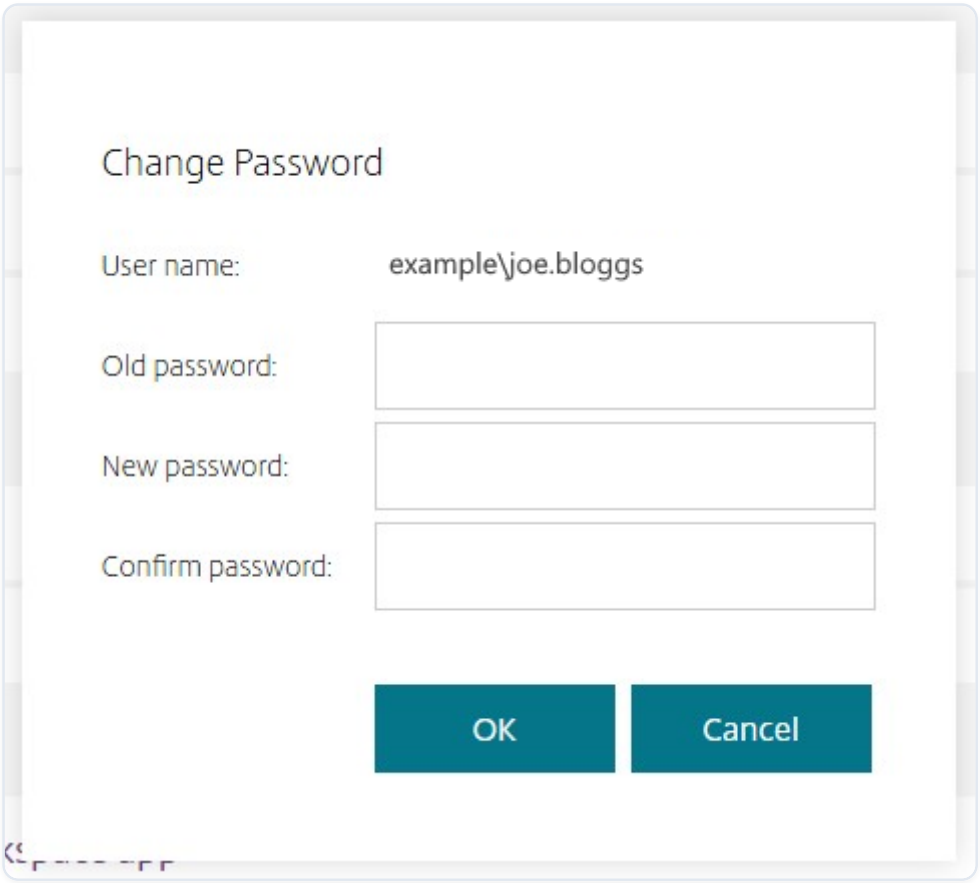
设置



帐户设置页面可能包含以下部分。

帐户

更改密码。仅在使用用户名和密码身份验证时。要配置是否显示此选项，请参阅用户名和密码。



关于。提供第三方通知的链接。

注销。注销用户。

应用程序

连接。恢复所有已断开连接的会话。要配置是否显示此选项，请参阅工作区控制。

断开连接。断开所有当前会话并注销。要配置是否显示此选项，请参阅工作区控制。

高级

激活 Citrix Workspace 应用程序。下载一个文件，将此应用商店添加到本地 Citrix Workspace 应用程序。要配置是否显示此选项，请参阅用户界面设置。

更改启动方法。打开一个页面，检查本地安装的 Citrix Workspace 应用程序。这还允许用户在通过本地安装的 Citrix Workspace 应用程序启动资源和在 Web 浏览器中启动资源之间进行切换。

注销

要注销，请打开设置菜单并单击**注销**。这会将用户从应用商店注销。如果他们连接到任何资源，则根据配置，它将执行以下操作之一：

- 终止资源。

- 断开与资源的连接
- 保持资源连接。

作为渐进式 Web 应用程序 (PWA) 安装（预览版）

如果管理员已启用渐进式 Web 应用程序，则用户可以将应用商店网站安装为渐进式 Web 应用程序。

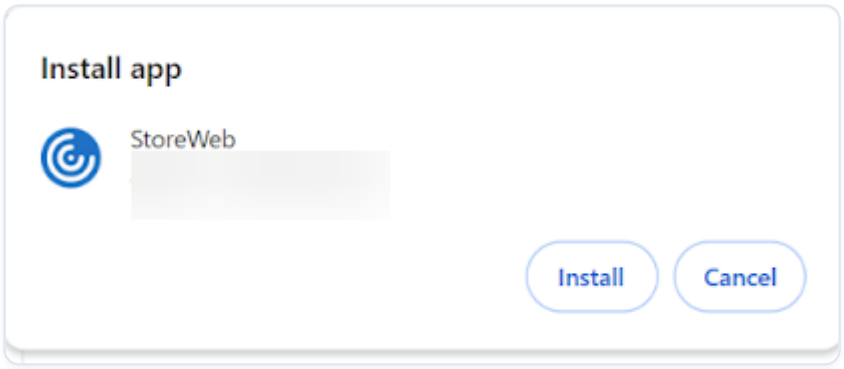
使用 Google Chrome 安装渐进式 Web 应用程序

用户可以按如下方式安装商店网站：

1. 在 Google Chrome 浏览器中打开商店。
2. 在工具栏中选择以下图标：

   出现安装 PWA 的选项。

3. 选择 **安装** 将商店添加到桌面和“开始”菜单：

   如果用户有多个 StoreFront™ 商店，他们可以单独安装每个商店网站。每次安装都会生成一个名为 `<Store website name>` 的快捷方式，可以根据需要重命名。

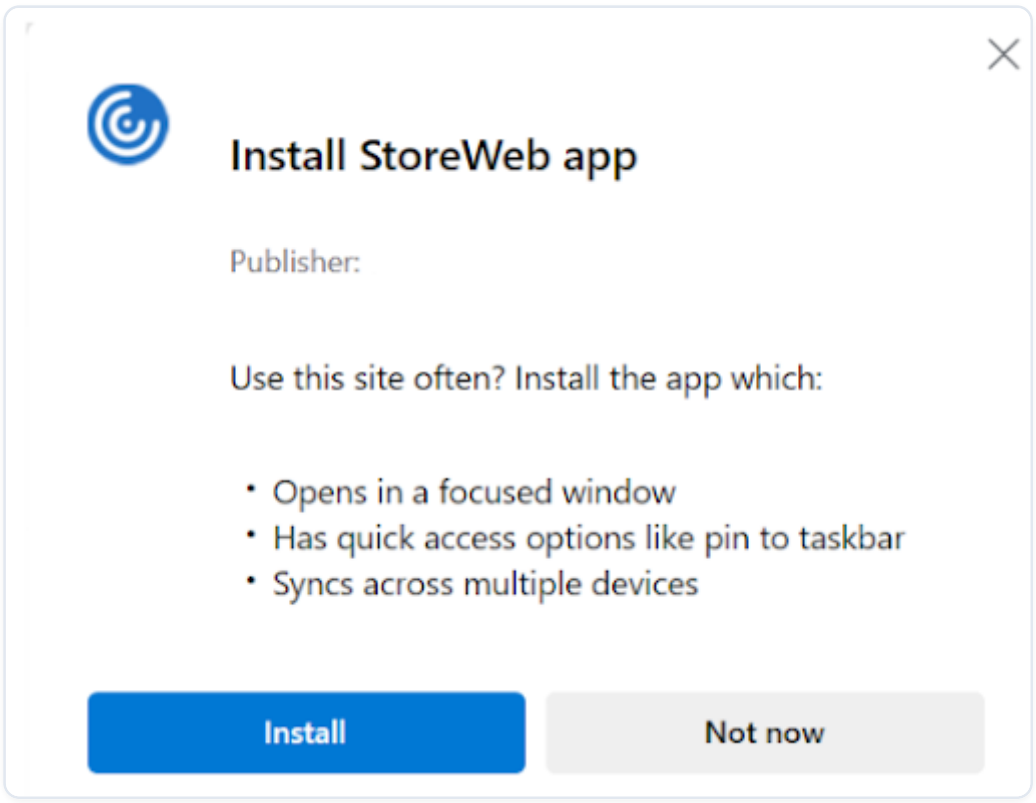
使用 Microsoft Edge 安装渐进式 Web 应用

用户可以按如下方式安装商店网站：

1. 在 Microsoft Edge 浏览器中打开商店。
2. 在工具栏中选择以下图标：



出现安装选项。



3. 选择 **安装** 将商店添加到桌面和“开始”菜单：



如果用户有多个 StoreFront 商店，他们可以单独安装每个商店网站。每次安装都会生成一个名为 `<Store website name>` 的快捷方式，可以根据需要重命名。

现代体验

本节介绍用户如何使用现代体验访问其应用商店并与之交互。默认情况下，现代体验未启用。要启用它，请参阅UI 体验。

需要 Citrix Workspace 应用程序屏幕

如果用户在 Web 浏览器中打开应用商店，但应用商店配置为需要 Citrix Workspace 应用程序，则会引导用户安装和配置 Citrix Workspace 应用程序。有关详细信息，请参阅要求使用 Citrix Workspace 应用程序。

Citrix Workspace 应用程序检测

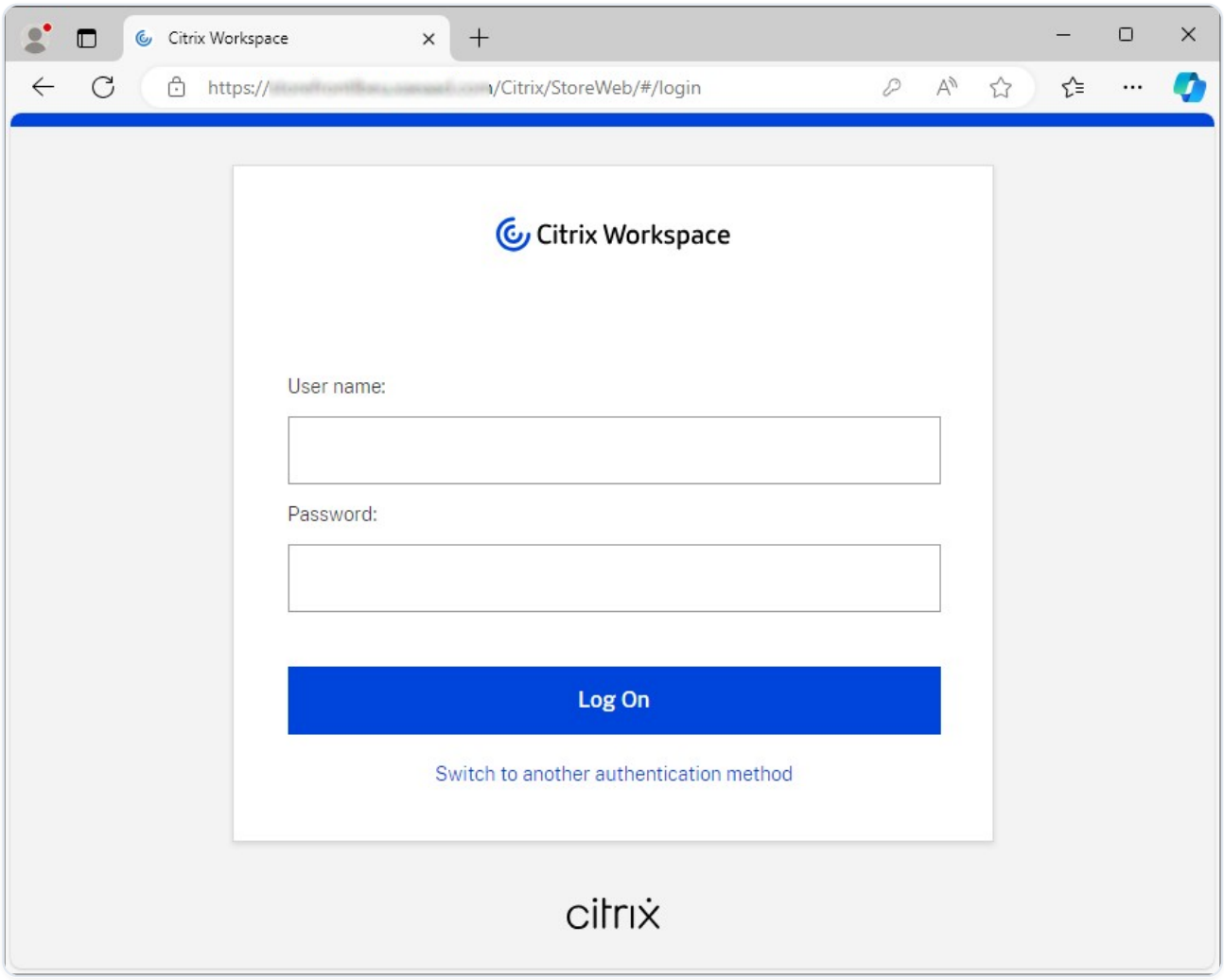
用户首次在 Web 浏览器中打开应用商店，或清除 Cookie 后，网页可能会显示“**欢迎使用 Citrix Workspace 应用程序**”屏幕，提示用户检测 Citrix Workspace 应用程序。此步骤可能在登录之前或之后发生，具体取决于配置。有关详细信息，请参阅Citrix Workspace 应用程序检测屏幕。

当用户在 NetScaler Gateway 进行身份验证时，此屏幕会在身份验证后显示。当用户直接向 StoreFront 进行身份验证时，此屏幕通常会在身份验证之前显示，除非您已配置登录后提示安装 Citrix Workspace 应用程序。

如果已安装 Citrix Web Extension 并检测到 Citrix Workspace 应用程序，则会跳过此步骤，并默认在 Citrix Workspace 应用程序中启动。用户可以从设置页面更改启动方法。

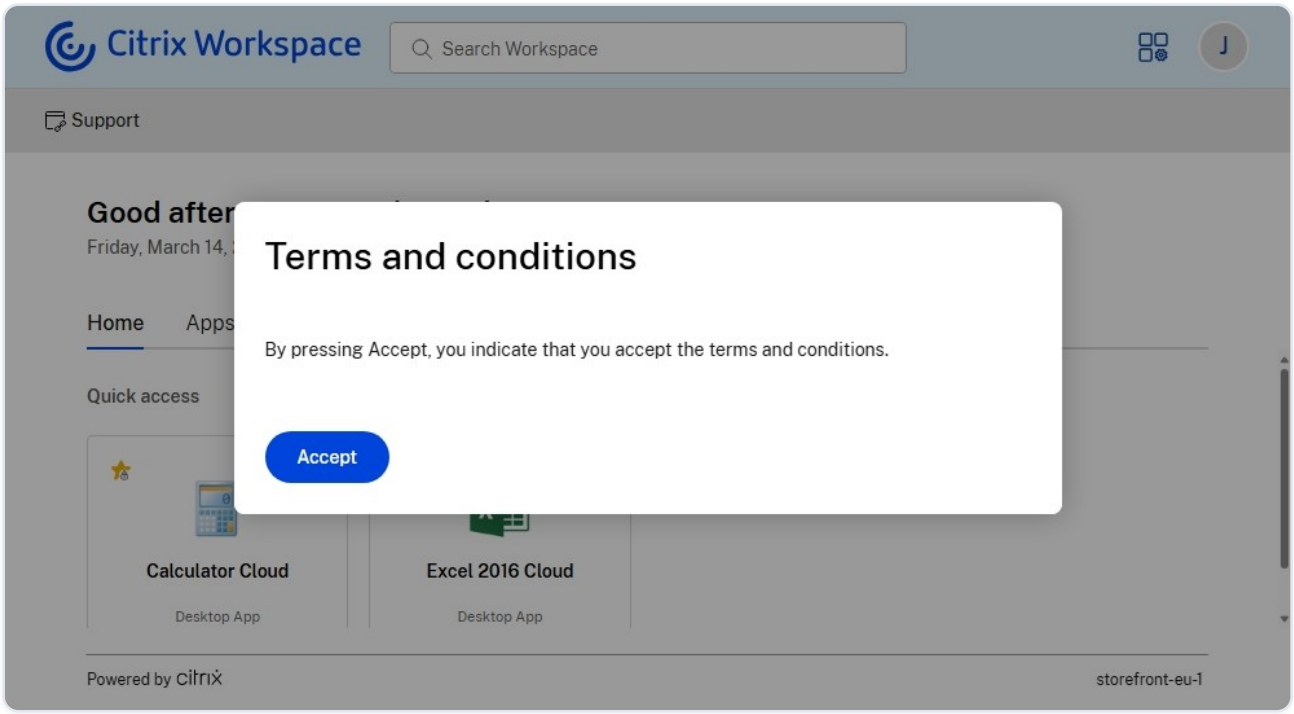
身份验证

根据配置的身份验证方法以及是否启用了单点登录，用户可能需要登录。



如果提供了多种身份验证方法，则用户可以选择切换到其他身份验证方法。

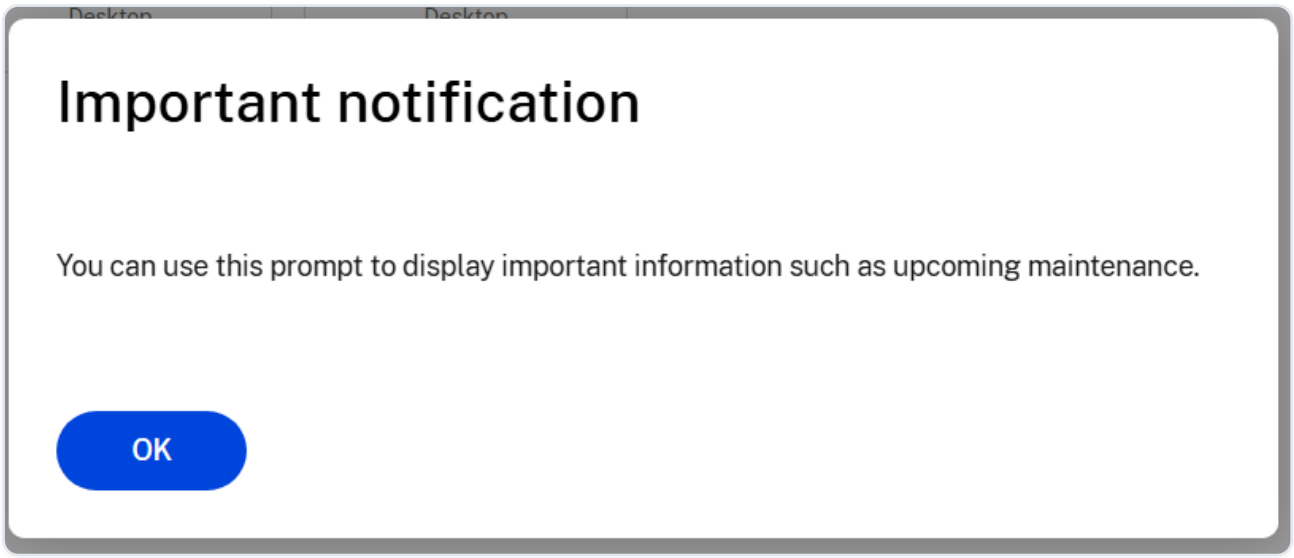
登录后，如果已配置，用户可能会看到一条消息，必须接受才能继续。



有关如何配置此项的详细信息，请参阅登录后对话框。

登录后对话框

可能会向用户显示一个对话框。有关详细信息，请参阅 (/zh-cn/storefront/2507-ltsr/stores/websites/dialog-after-login.html)。



用户必须在访问其资源之前接受该消息。您可以配置消息的显示频率。

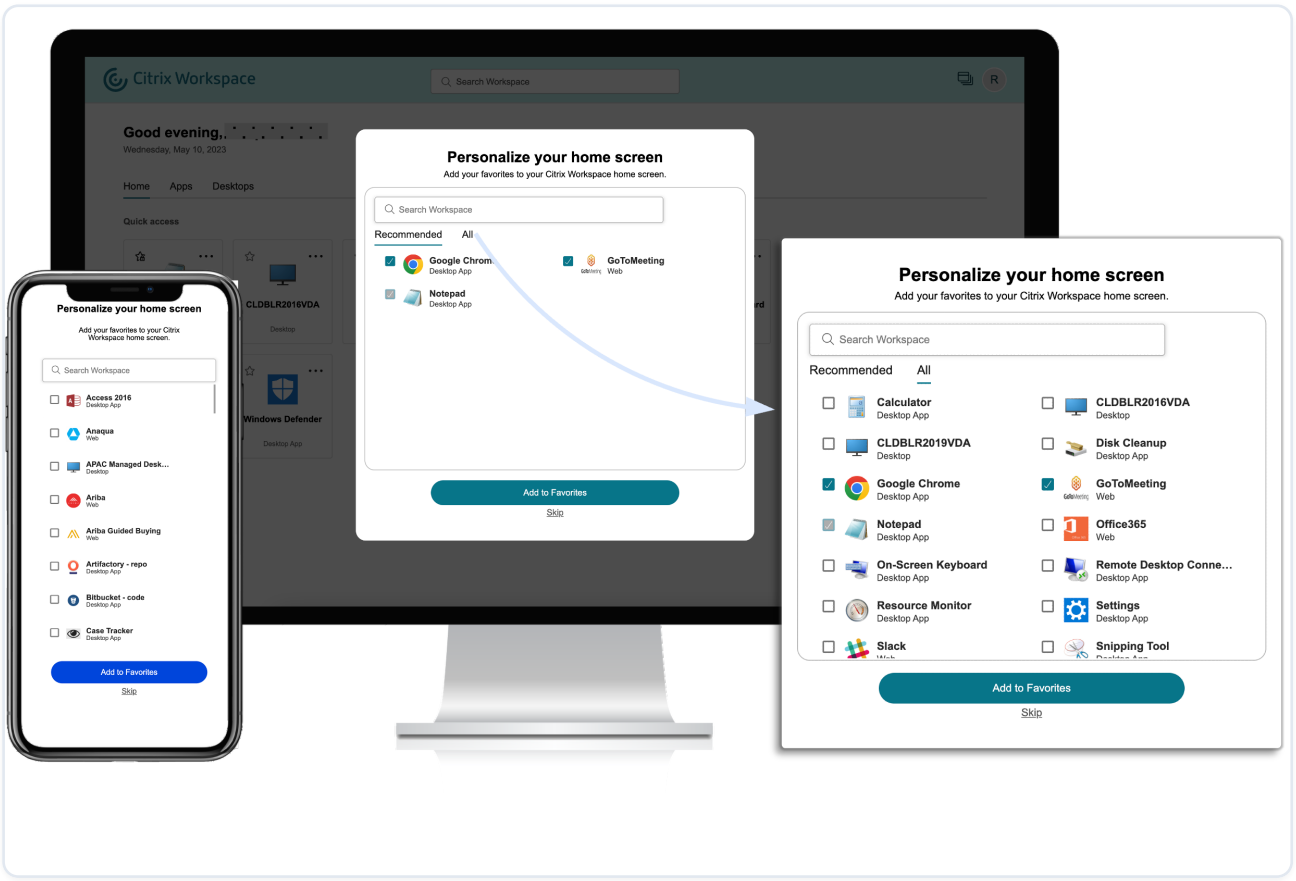
首次用户体验

首次访问 UI 时，系统会向用户显示一个弹出窗口，他们可以在其中轻松一步收藏多个应用程序。

当用户拥有 20 多个应用程序且尚未将任何应用程序添加到“收藏夹”时，将激活首次用户体验。此体验支持所有浏览器和本机客户端（Mac、Windows、Linux 和 ChromeOS）以及移动设备（iOS 和

Android）。要配置此窗口是否显示，请参阅 (/zh-cn/storefront/2507-ltsr/stores/websites/client-interface-settings.html#display-personalize-your-home-screen-for-first-time-users)。

推荐或强制应用程序显示在首次用户屏幕的“**推荐**”选项卡上，由管理员在 Citrix Virtual Apps and Desktops™ 的 DaaS 控制台以及 Web 和 SaaS 应用程序的安全专用访问控制台上设置。强制应用程序默认选中且禁用复选框。**推荐**和自动收藏的应用程序默认选中且为用户启用复选框。最终用户还可以选择其他应用程序添加到“收藏夹”。所有选定的应用程序都会自动添加到“收藏夹”并反映在主页上。



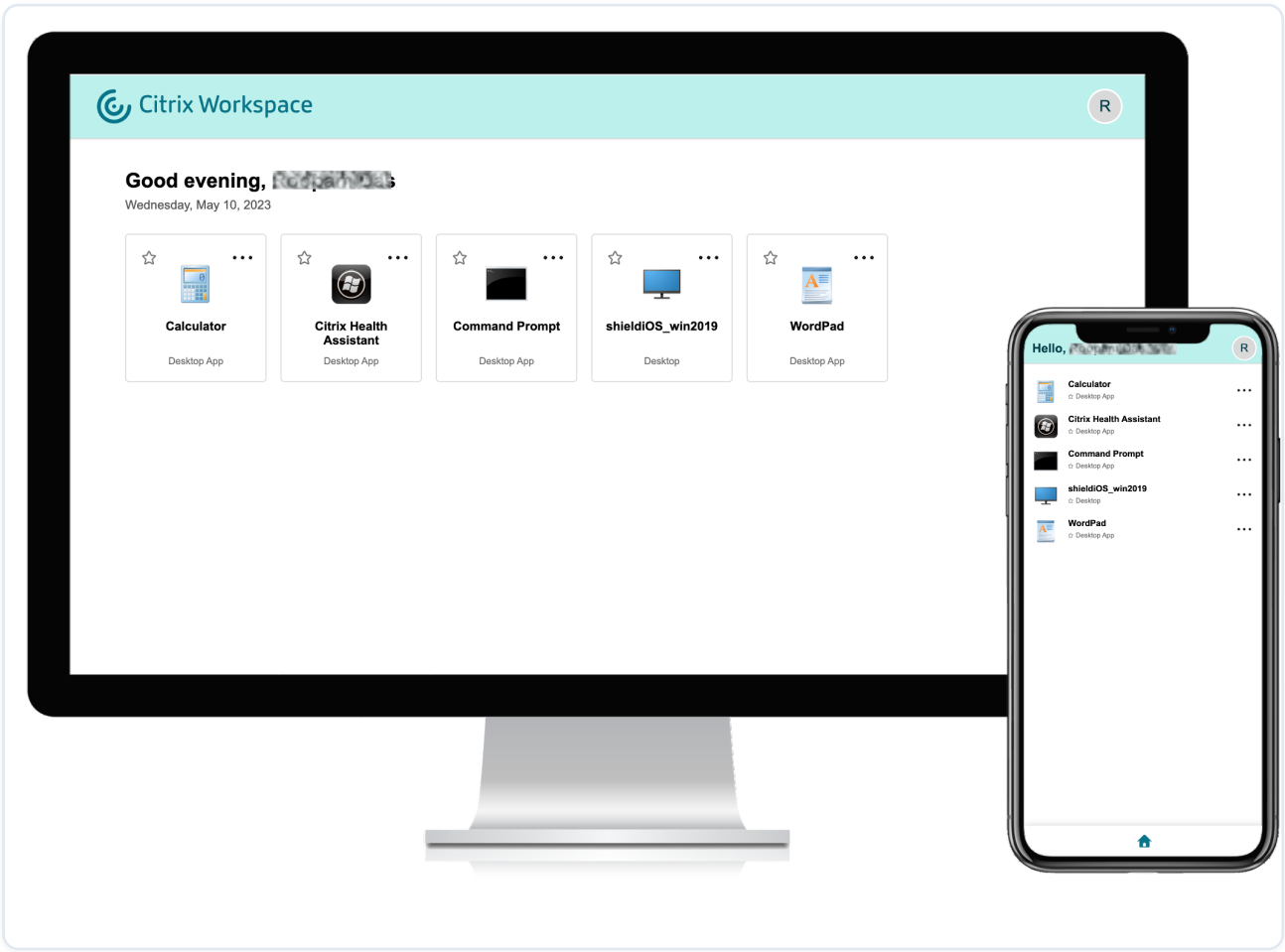
限制

- “**个性化**”屏幕在每个设备和浏览器上显示一次，在隐身模式下每次都会显示，除非用户标记了收藏夹。
- 如果管理员从应用程序中删除强制或推荐标签，则“**收藏夹**”中的应用程序将不受影响。
- 如果最终用户尚未将任何应用程序添加到“**收藏夹**”，则每次打开工作区应用程序时都会显示“**个性化**”屏幕。 为避免这种情况：
  - 最终用户可以将一个或多个应用程序添加到“**收藏夹**”。这可以防止每次启动应用程序时都显示个性化屏幕。
  - 管理员可以将一个或多个应用程序添加到“收藏夹”。有关详细信息，请参阅 (/zh-cn/storefront/2507-ltsr/get-started/configure-resources.html)。

导航选项卡

简单视图

如果用户拥有的资源少于 20 个，则默认情况下，他们会进入不带任何选项卡或类别的“简单视图”屏幕。所有应用程序和桌面都显示在同一页面上。在此屏幕上，收藏夹首先显示，然后是所有其他应用程序，按字母顺序排列。



您可以将应用商店配置为始终显示导航选项卡，这将禁用简单视图。

完整视图

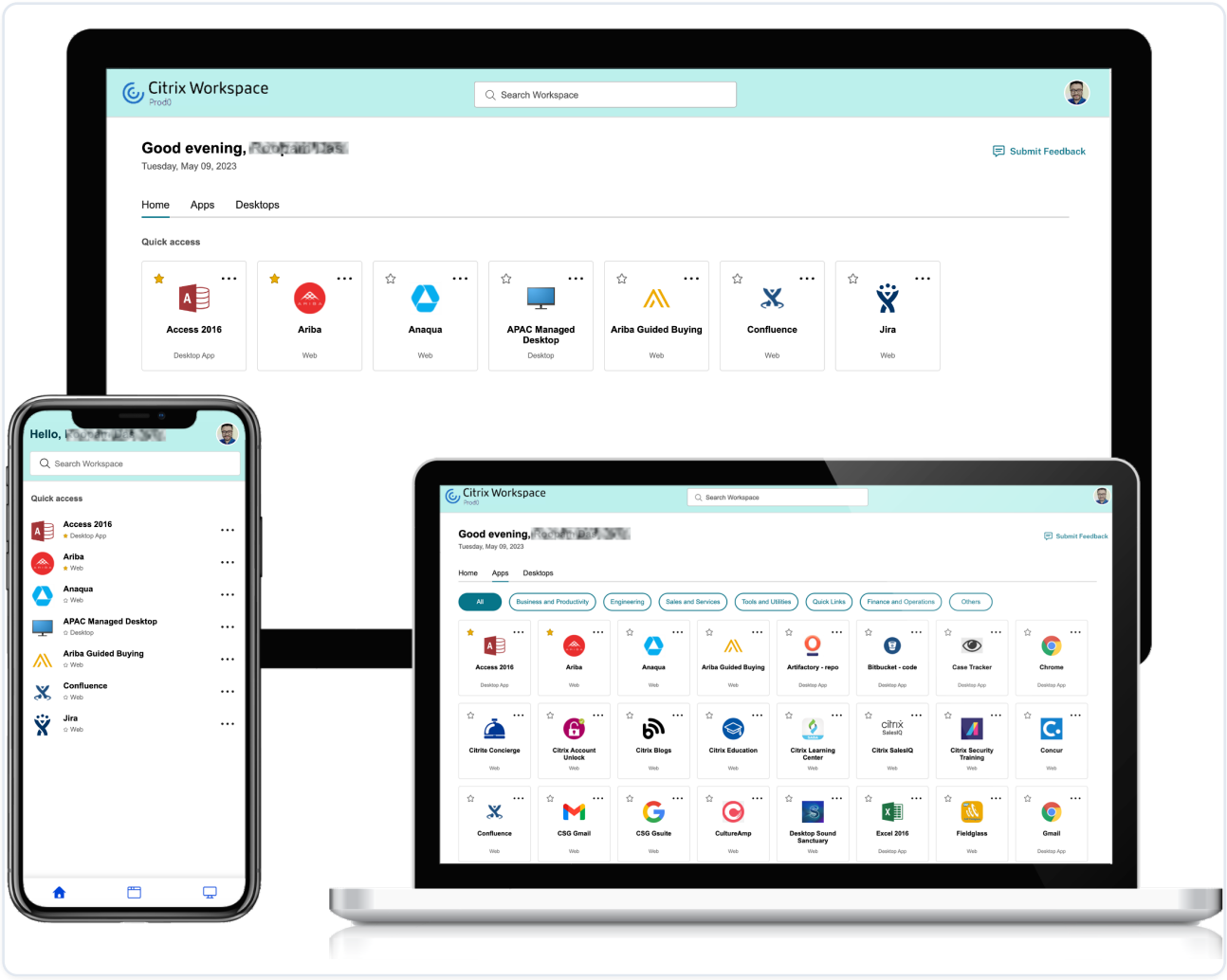
如果用户拥有的资源超过 20 个，或者应用商店网站配置为“始终显示导航选项卡”，则最多显示三个选项卡 - **主页**、**应用程序**和**桌面**。默认情况下，用户登录时会进入**主页**选项卡（如果存在），否则进入**应用程序**选项卡。您可以配置主页选项卡是否显示以及默认选项卡。

主页选项卡

在主页选项卡上，强制和收藏的应用程序首先显示，然后是五个最近使用的应用程序。**强制**应用程序的星形图标已锁定，用户无法将其从收藏夹中删除。

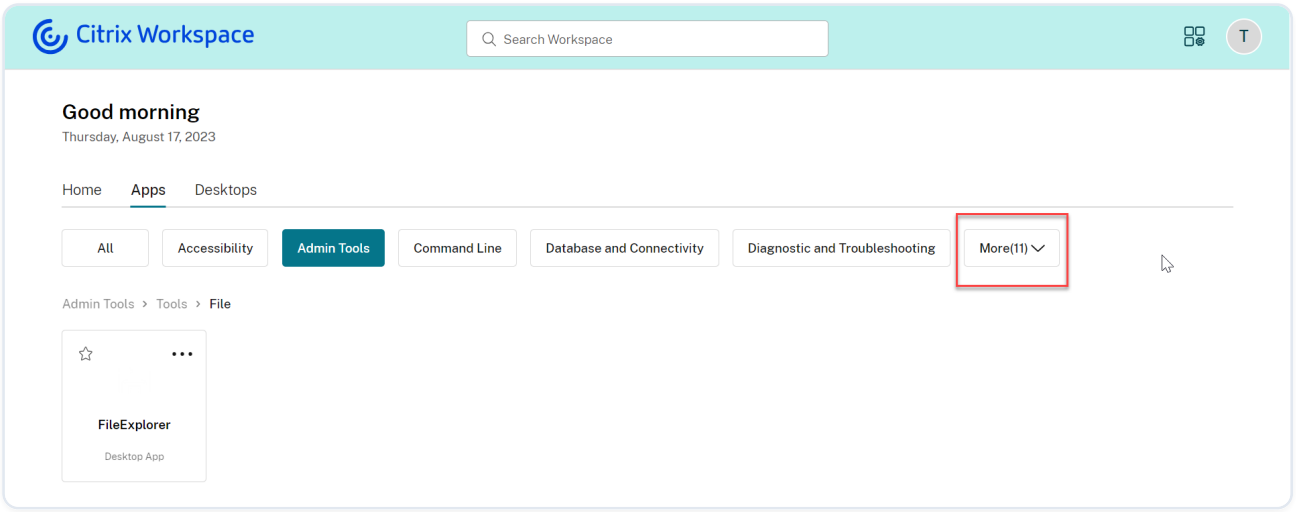
应用程序选项卡

在**应用程序**选项卡上，收藏夹首先显示，然后是所有其他应用程序，按字母顺序排列。如果管理员已创建类别并将应用程序附加到这些类别，则会显示各种类别，用户可以选择他们想要查看的应用程序类别。

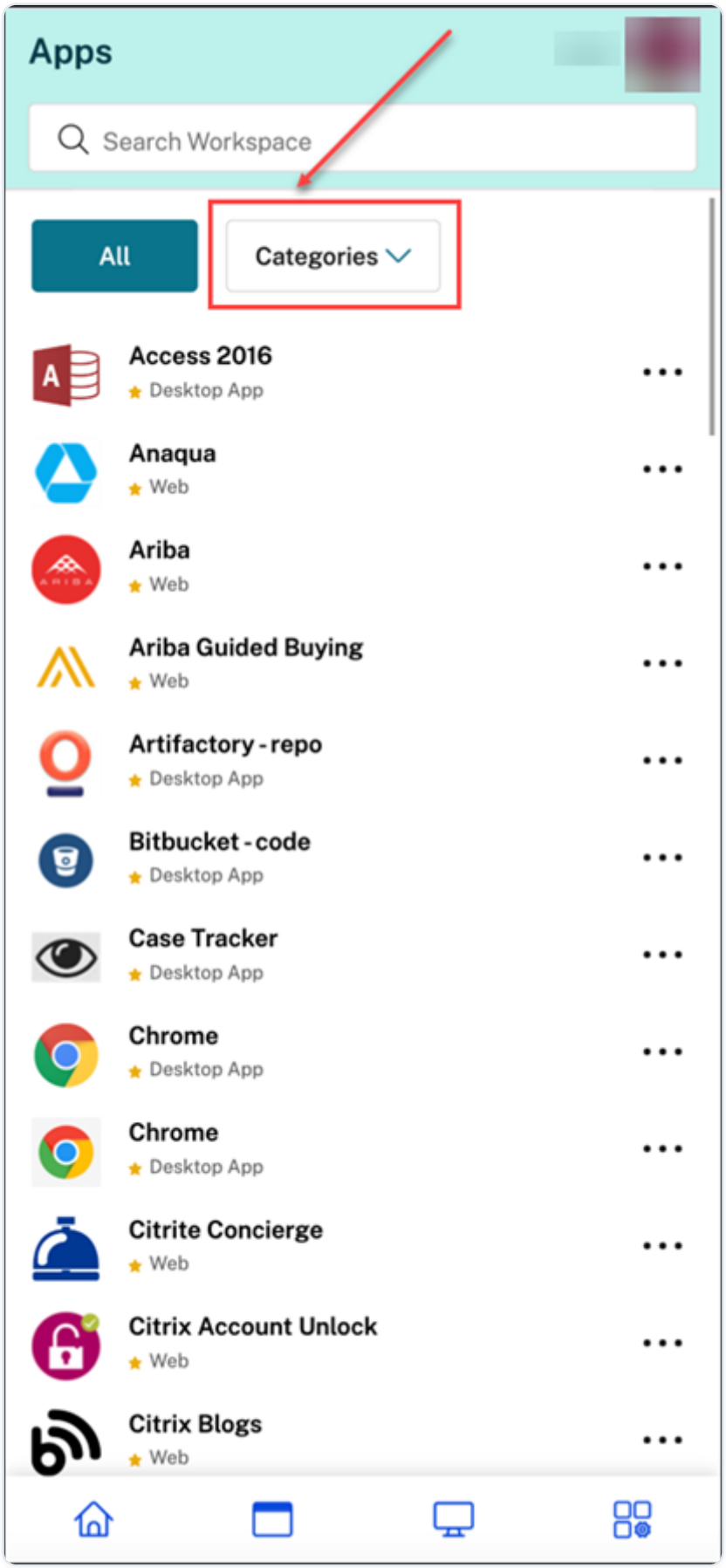


您可以为每个应用程序定义一个类别。该类别表示在最终用户屏幕上显示的文件夹结构。例如，考虑一个文件夹定义为 `Optimisation tools/Cleaning` 的应用程序。现在，要访问此应用程序，最终用户必须转到“优化工具”>“清理”，其中“优化工具”是一个类别，“清理”是其子类别。有关配置类别的更多信息，请参阅应用程序。

当管理员创建的主类别数量超出用户屏幕上的可用空间时，用户界面会根据屏幕大小进行调整，并将类别动态移动到“**更多**”下拉菜单下。 导航面包屑也会显示给用户。



在移动平台上，导航到“应用程序”选项卡并单击“**类别**”下拉菜单以查看可用类别列表。子类别显示为文件夹，根据管理员配置，这些文件夹可能包含更多子文件夹或应用程序。



选择相关类别后，将根据管理员所做的配置显示可用子类别和应用程序的列表。

移动设备上的子类别(/en-us/storefront/2507-ltsr/media/end-user-experience/wsui-mobile-subcategory-with-app-resized.png)

桌面选项卡

桌面选项卡显示所有可用的虚拟桌面。

收藏和强制应用程序

默认情况下，用户可以通过选择磁贴上的星形图标来创建和删除收藏夹。

管理员还可以使用关键字 关键字 配置以下内容：

- **auto** - 应用程序会自动创建为收藏夹，但用户可以将其删除。
- **mandatory** - 应用程序始终是收藏夹，用户无法将其删除。

要禁用收藏夹，请参阅 启用或禁用收藏夹。如果禁用收藏夹，所有应用程序将显示在**主页**选项卡上。

搜索应用程序和桌面

用户可以输入搜索词来按名称和类别搜索应用程序和桌面。收藏夹显示在列表顶部。

搜索结果(/en-us/storefront/2507-ltsr/media/end-user-experience/enhanced-search.png)

活动管理器

用户可以使用 活动管理器 管理其会话。

应用程序和桌面磁贴

磁贴显示在 Studio 中配置的应用程序名称。用户可以单击磁贴以启动应用程序。

对于分配的桌面，还会显示电源状态。有关详细信息，请参阅 电源状态。

磁贴操作

磁贴上的“**更多**”选项菜单（省略号图标）为用户提供了相关操作的访问权限。显示的选项是上下文相关的。

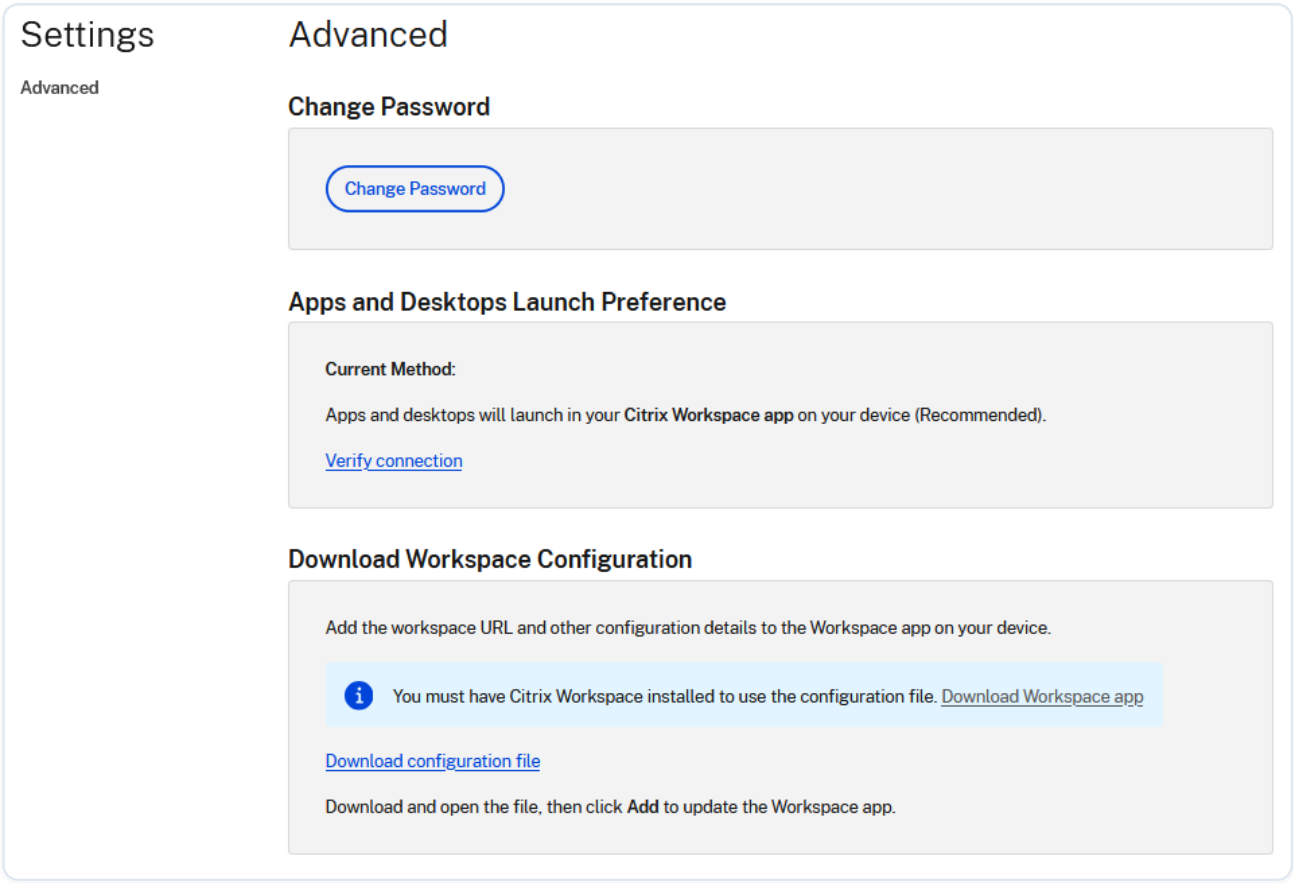
这些操作可能包括：

- **打开桌面**或**打开应用程序** - 启动或重新连接到应用程序或桌面。如果桌面已关机或处于休眠状态，则会先打开桌面电源，然后再启动会话。

- **添加到收藏夹** - 添加到收藏夹，使其显示在“**主页**”选项卡上。这与单击“**星形**”具有相同的效果。仅当收藏夹已启用时才启用。
- **显示详细信息** - 打开一个弹出窗口，其中包含应用程序或桌面的描述。
- 对于分配的桌面，可能提供额外的电源管理操作。有关详细信息，请参阅 电源操作。

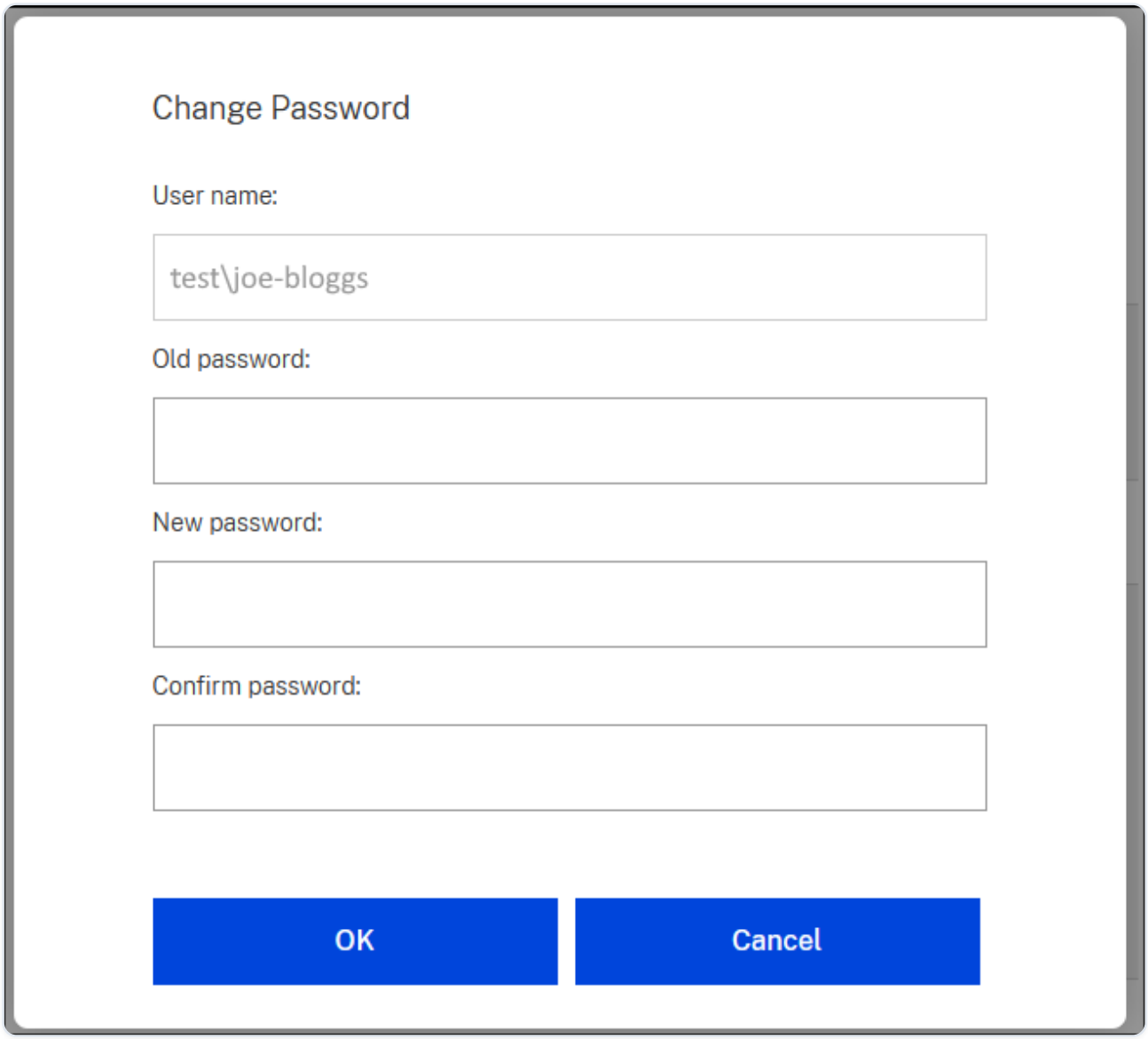
设置

用户通过选择 UI 右上角的个人资料图标时出现的菜单访问“**帐户设置**”。



更改密码

如果用户使用用户名和密码身份验证登录，并且 StoreFront 配置为 允许用户随时更改密码，则用户会看到“**更改密码**”选项。如果用户选择此屏幕，则会出现一个窗口，他们可以在其中输入旧密码和新密码：



应用程序和桌面启动首选项

当使用网络浏览器时，这会显示应用程序是在网络浏览器中启动，还是在 Citrix Workspace 应用程序中启动，或者通过下载用户可以在 Citrix Workspace 应用程序中打开的 ICA 文件来启动。

用户可以选择 **验证连接** 以打开 Citrix Workspace 应用程序检测屏幕。

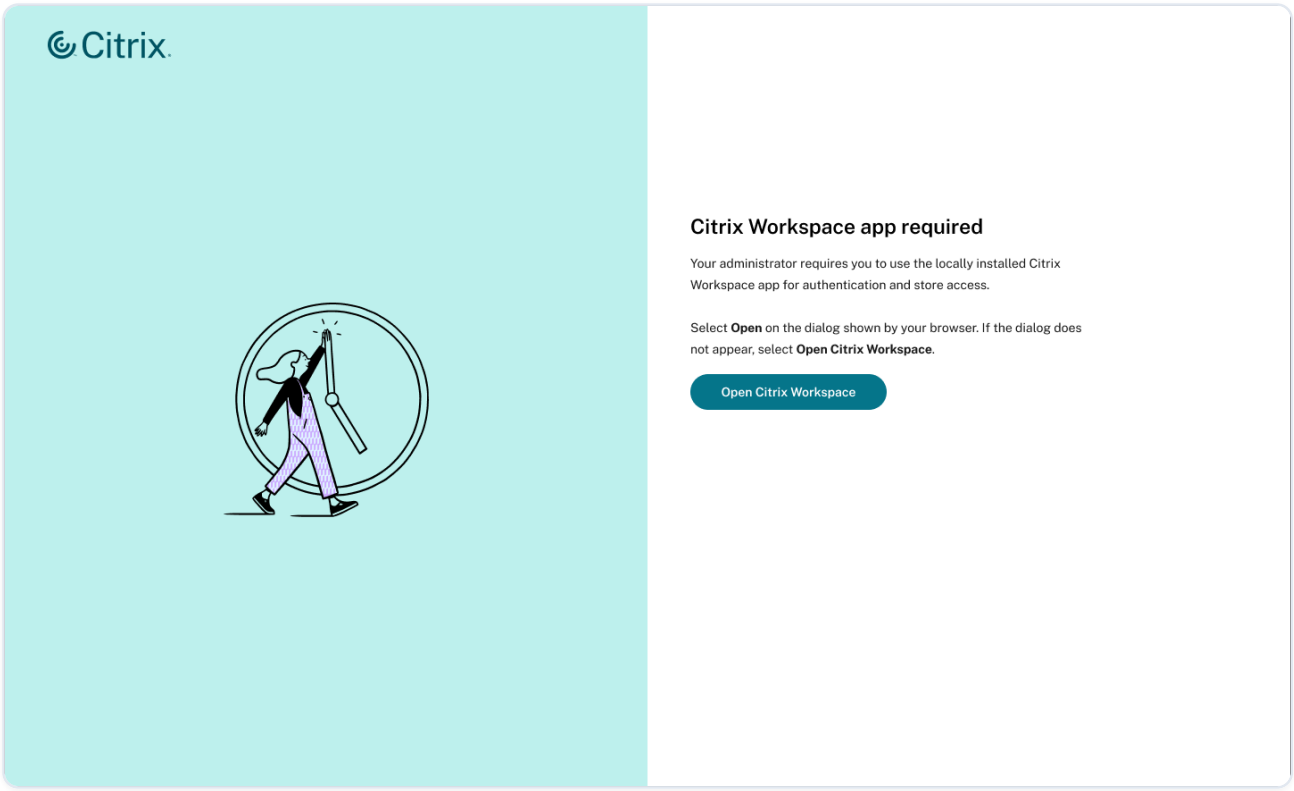
下载 Workspace 配置

当使用网络浏览器时，用户可以下载一个文件，该文件用于配置 Citrix Workspace 应用程序以连接到应用商店。要启用此功能，请参阅 允许最终用户下载 Citrix Workspace 应用程序配置文件

要求 Citrix Workspace 应用程序

一旦管理员启用了 要求 Citrix Workspace 应用程序，最终用户就无法在浏览器中使用 Citrix Workspace Web 客户端。

当用户尝试通过在浏览器中输入应用商店 URL 来访问 Web 客户端时，他们会看到以下网页，提示打开本机应用程序。



1. 单击 **打开 Citrix Workspace**。

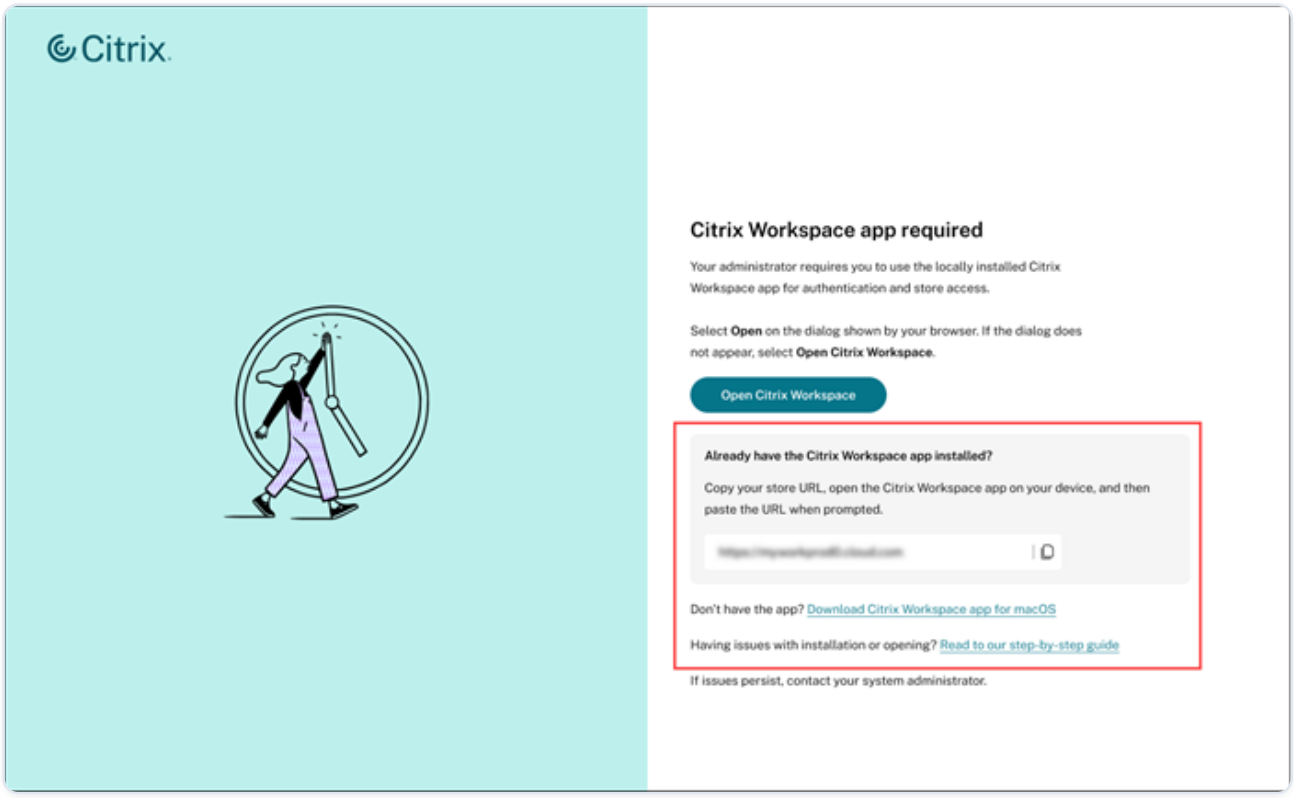
   客户端检测过程开始，检查 Citrix Workspace 应用程序是否已本地安装在用户设备上。

   出现 **打开 Citrix Workspace 启动器** 提示，要求用户打开本机应用程序。

2. 单击 **打开 Citrix Workspace 应用程序**。

如果用户在 5 秒内没有看到提示或没有单击提示中的 **打开 Citrix Workspace 应用程序**，网页会提供以下额外选项以继续：

- 可在本地 Citrix Workspace 应用程序中手动复制和添加的应用商店 URL。
- 用于安装 Citrix Workspace 应用程序的下载链接。要配置下载链接，请参阅 Citrix Workspace 应用程序部署。
- 指向最终用户指南的链接，该指南提供了安装和打开 Citrix Workspace 应用程序的分步说明。



注意：

如果用户在 iPad 上使用 Safari 浏览器，浏览器无法将其与 Mac 桌面区分开来。因此，用户必须单击 **我正在使用 iPad** 链接才能继续自动添加应用商店。

Linux 和 ChromeOS 不支持自动添加应用商店。因此，这些设备上不会出现 **打开 Citrix Workspace 启动器** 提示。在这种情况下，用户需要手动在本地应用程序中添加应用商店 URL。有关详细信息，请参阅 手动添加应用商店。

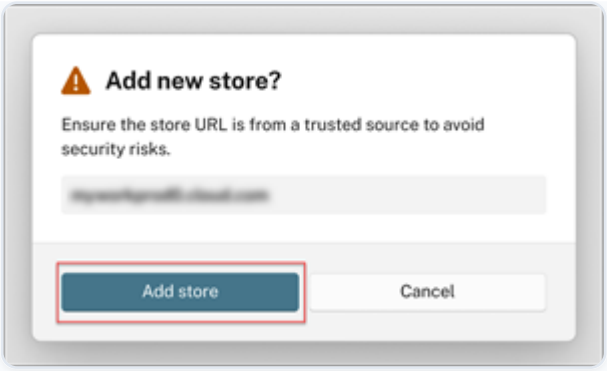
自动添加应用商店

在支持的 Citrix Workspace 应用程序版本上，它会自动添加应用商店。最低版本如下：

操作系统	兼容版本
视窗	24.9.0 或更高版本
Mac	24.5.0 或更高版本
安卓和 iOS	24.9.0 或更高版本

注意：

Linux 和 ChromeOS 平台不支持自动添加应用商店，并且在 Windows 和 Mac 平台上具有版本要求。在这种情况下，用户需要在本机应用程序中手动添加应用商店 URL。有关详细信息，请参阅手动添加应用商店。

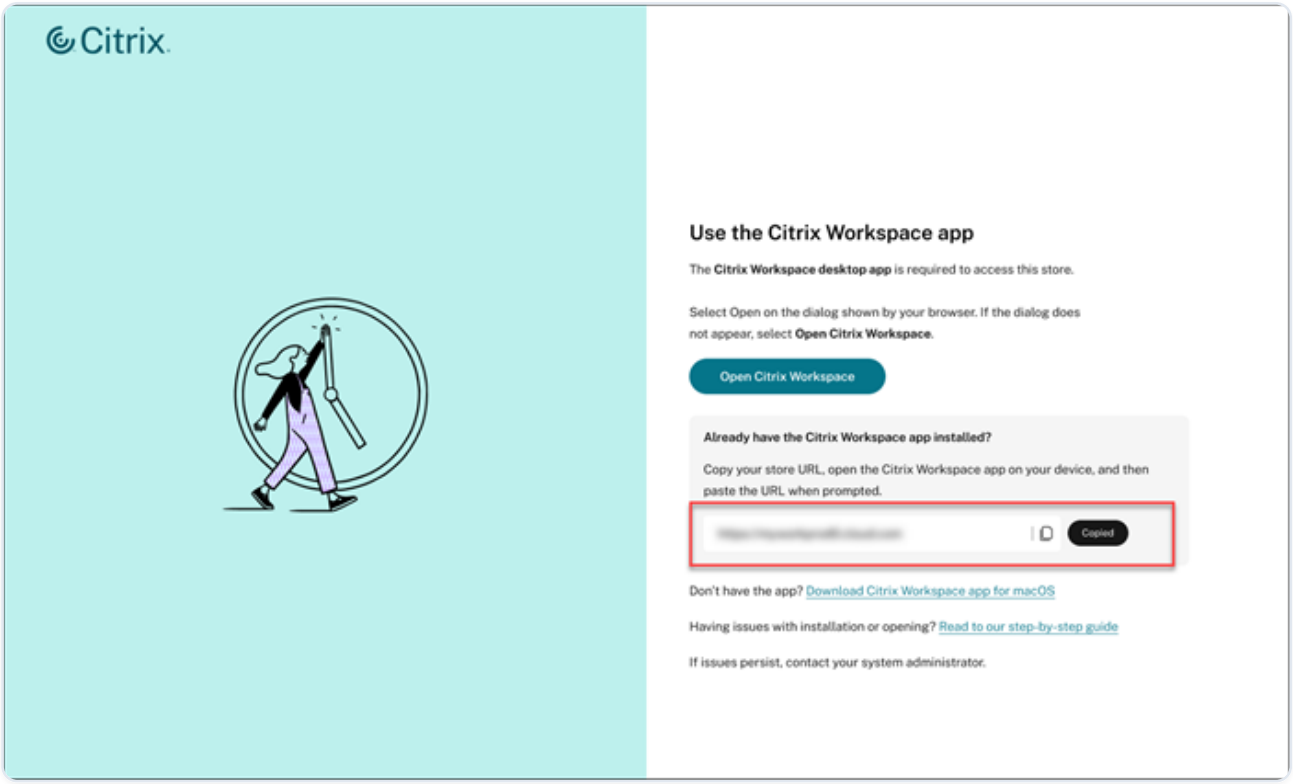


单击 **添加应用商店**。

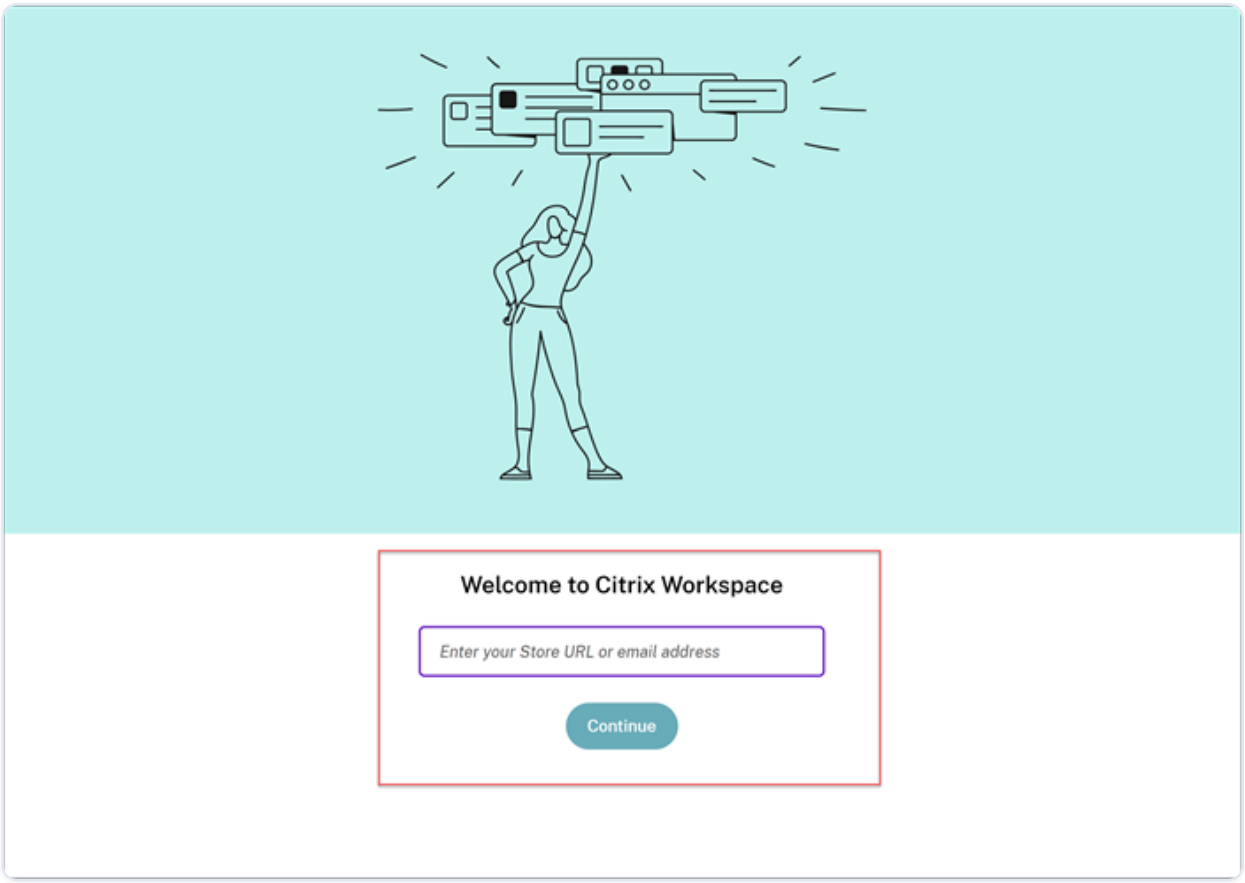
单击后，本机应用程序会自动捕获在浏览器中输入的应用商店 URL，并显示身份验证页面供用户登录。成功进行身份验证后，用户可以看到本机 Citrix Workspace 应用程序的主页。

手动添加应用商店

如果本机应用程序在用户单击**添加应用商店**选项时未自动捕获应用商店 URL，则用户可以手动将应用商店添加到 Citrix Workspace 应用程序。



1. 从本机强制网页复制应用商店 URL，并将其粘贴到 **欢迎使用 Citrix Workspace** 页面。



2. 单击“**继续**”。

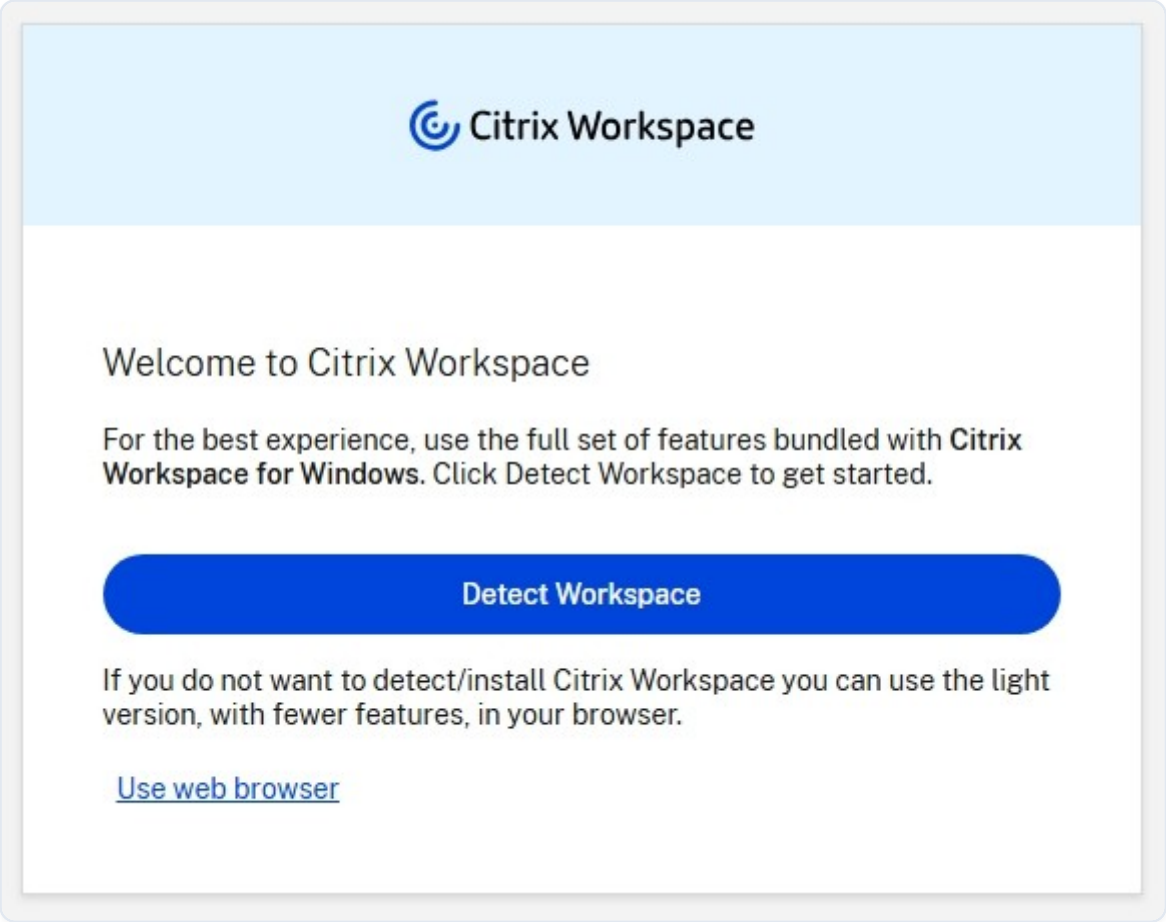
提交有效的商店 URL 后，Citrix Workspace 应用程序会显示身份验证页面供用户登录。成功进行身份验证后，用户可以看到本机 Citrix Workspace 应用程序的主页。

Citrix Workspace 应用程序检测

欢迎使用 Citrix Workspace 屏幕

通过 Web 浏览器访问应用商店时，网站可能会显示“**欢迎使用 Citrix Workspace**”屏幕。这适用于以下情况：

- 用户首次在其 Web 浏览器中打开应用商店，或在清除 Web 浏览器中的站点数据后打开应用商店。
- 启动首选项 设置为“**在 Citrix Workspace 应用程序中打开**”或“**让用户选择**”。
- 如果未安装 Citrix Web Extension，或者未检测到 Citrix Workspace 应用程序。如果 Citrix Web Extension 检测到 Citrix Workspace 应用程序，则会跳过此步骤并默认在 Citrix Workspace 应用程序中启动。
- 设备的操作系统支持 Citrix Workspace 启动器。

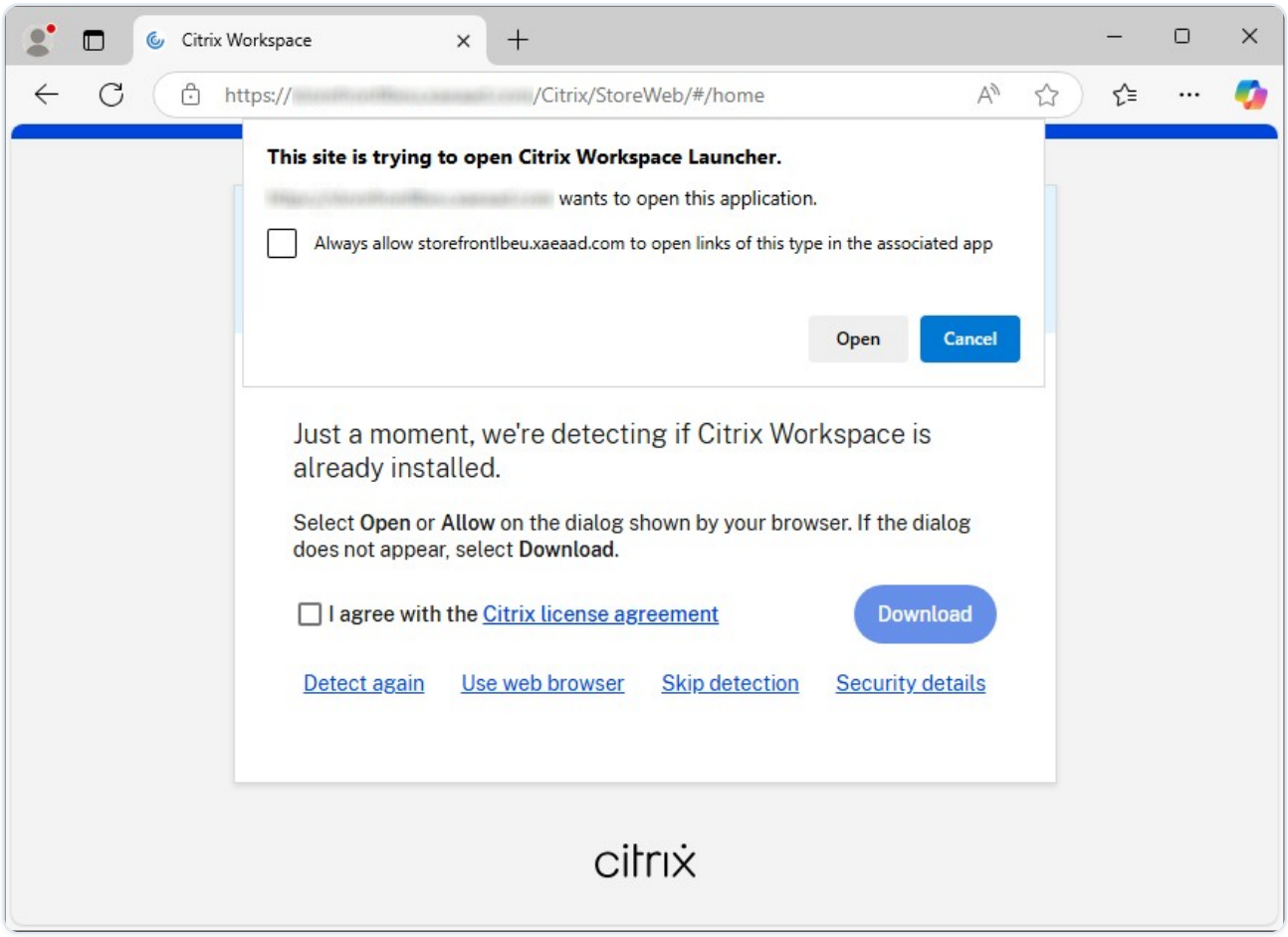


用户可以执行以下任一操作：

- 如果希望在本地安装的 Citrix Workspace 应用程序中启动资源，请选择“**检测 Citrix Workspace 应用程序**”。建议选择此项以获得最佳体验。
- 选择“**使用 Web 浏览器**”以始终在浏览器中启动资源。此选项仅在 启动首选项 设置为“**让用户选择**”时可用。

Citrix Workspace 应用程序检测屏幕

当用户选择“**检测 Citrix Workspace 应用程序**”时，网站会显示 Citrix Workspace 应用程序检测屏幕。此操作会尝试打开 **Citrix Workspace Launcher**，它是 Citrix Workspace 应用程序的一个组件。如果已安装 Citrix Workspace 应用程序，则浏览器会显示一条消息，要求运行 **Citrix Workspace Launcher**。单击“**打开 Citrix Workspace Launcher**”或“**打开链接**”（具体取决于浏览器）。建议他们同时选择“**始终允许 *domain* 在关联的应用程序中打开此类链接**”（或类似选项，具体取决于浏览器），以避免每次启动资源时都出现此消息。



用户也可以从 设置屏幕 访问此功能。

如果检测到本地安装的 Citrix Workspace 应用程序，则几秒钟后会继续到下一个屏幕。当用户随后启动资源时，它会使用 Citrix Workspace Launcher 在本地安装的 Citrix Workspace 应用程序中打开资源。

如果未安装 Citrix Workspace 应用程序，或者用户取消了 Citrix Workspace 启动器，那么他们可能会有以下选项：

- **下载** - 从 Citrix 网站下载 Citrix Workspace 应用程序。要配置此选项，请参阅 Citrix Workspace 应用程序部署。
- **再次检测** - 尝试再次检测本地安装的 Citrix Workspace 应用程序。
- **使用 Web 浏览器** - 跳过 Workspace 应用程序检测，并始终在 Web 浏览器中打开资源。仅当 启动首选项 设置为 **让用户选择** 时，此选项才可用。
- **跳过检测** - 如果用户安装了不支持 Citrix Workspace Launcher 或 Citrix Web 扩展的旧版 Citrix Receiver，则可以使用此选项。如果他们选择此选项，当他们启动虚拟应用程序或桌面时，浏览器会下载一个 `.ica` 文件，他们可以使用 Citrix Workspace 应用程序打开该文件。此选项会导致功能和安全性降低，因此建议管理员 禁用此选项。

活动管理器

活动管理器是一个简单而强大的功能，可帮助用户有效管理其资源。通过在任何设备上对活动应用程序和桌面执行快速操作，它提高了工作效率。用户可以无缝地与其会话交互，结束或断开不再需要的会话，从而释放资源并随时随地优化性能。

活动管理器面板显示应用程序和桌面的整合列表，这些应用程序和桌面不仅在当前设备上处于活动状态，而且在任何具有活动会话的远程设备上也是如此。用户可以通过单击活动管理器图标来查看此列表，该图标位于桌面上的配置文件图标旁边，以及移动设备屏幕的底部。

> **注意：**
>
> 如果您在较暗的横幅主题中无法看到活动管理器图标，请考虑更改并测试“**横幅文本和图标颜色**”设置中选择的颜色。由于横幅与活动管理器图标之间的对比度较低，该图标可能无法清晰显示。有关详细信息，请参阅外观。

先决条件

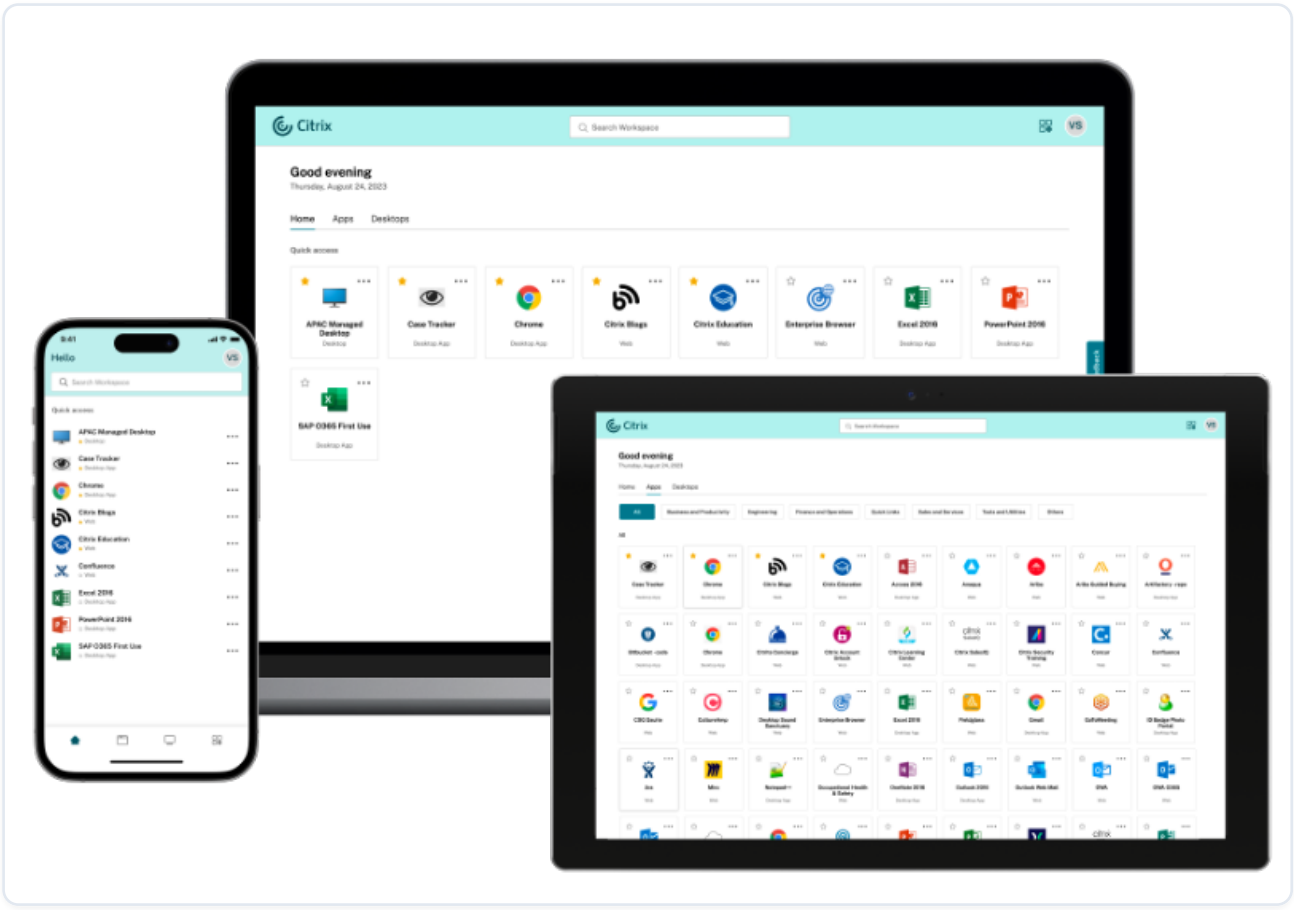
活动管理器功能需要 Citrix Desktops as a Service 或 Citrix Virtual Apps™ and Desktop 2311 及更高版本。如果您使用的是早期版本的 Citrix Virtual Apps and Desktops，则活动管理器不会显示任何会话，因此建议隐藏活动管理器。

要控制是否显示“**活动管理器**”按钮，请参阅显示活动管理器。

使用活动管理器

活动管理器上的活动应用程序和桌面按以下方式分组。

- 在当前设备上处于活动状态的应用程序和桌面列表分组在“**在此设备上**”下。
- 在其他设备上处于活动状态的应用程序和桌面列表分组在“**远程运行**”下。



用户可以通过单击相应的省略号 (...) 按钮对应用程序或桌面执行以下操作。

- **断开连接**：远程会话已断开连接，但应用程序和桌面仍在后台运行。
- **注销**：从当前会话注销。会话中的所有应用程序都将关闭，并且任何未保存的文件都将丢失。
- **关机**：关闭已断开连接的桌面。
- **强制关机**：在出现技术问题时强制关闭桌面电源。
- **重新启动**：关闭桌面并重新启动。
- **休眠**：保存当前状态并关闭计算机电源。
- **恢复**：启动并恢复处于休眠状态的计算机。

断开连接的应用程序和桌面

活动管理器使最终用户能够查看在本地或远程以断开连接模式运行的应用程序和桌面，并对其执行操作。会话可以通过移动设备或桌面设备进行管理，使最终用户能够随时随地执行操作。对断开连接的会话（例如注销或关机）执行操作有助于优化资源使用并降低能耗。

断开连接的会话(/en-us/storefront/2507-ltsr/media/end-user-experience/activity-manager-disconnected-icon.png)

- 断开连接的应用程序和桌面显示在活动管理器面板上，并由断开连接图标指示。

- 断开连接的应用程序按各自的会话分组，并且这些会话由断开连接图标指示。

断开连接的会话(/en-us/storefront/2507-ltsr/media/end-user-experience/wsui-disconnected-options.png)

最终用户可以通过单击省略号按钮对其断开连接的桌面执行以下操作：

- **注销**：使用此选项可从断开连接的桌面注销。会话中的所有应用程序都将关闭，并且任何未保存的文件都将丢失。
- **关机**：使用此选项可关闭断开连接的桌面。
- **强制关机**：如果出现技术问题，请使用此选项强制关闭断开连接的桌面电源。
- **重新启动**：使用此选项可关闭并重新启动断开连接的桌面。

活动管理器上断开连接的会话的行为差异如下。

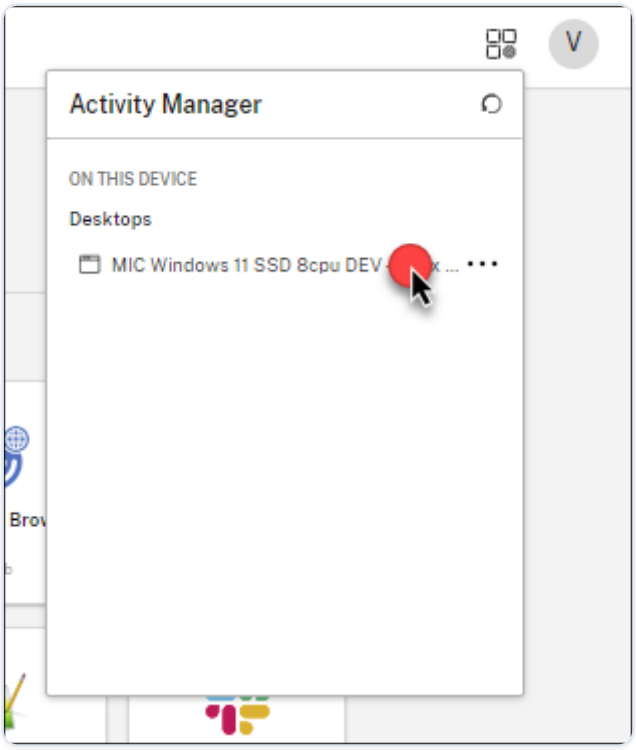
- 如果用户通过浏览器登录到 Citrix® Workspace，并断开本地会话，则该会话首先显示在“**此设备上**”下。但是，一旦用户关闭并重新打开活动管理器，断开的会话将移至“远程运行”下。
- 如果用户登录到 Citrix Workspace 应用程序并断开本地会话，则断开的会话将从列表中消失。但是，一旦用户再次关闭并重新打开活动管理器，断开的会话将移至“**远程运行**”下。

重新连接到已断开连接的应用程序和桌面

重新连接功能允许最终用户轻松地重新打开其已断开连接的应用程序和桌面会话，确保设备之间平稳过渡而不会丢失进度。此功能无缝恢复对以前工作环境的访问，无需搜索和重新打开应用程序和桌面。

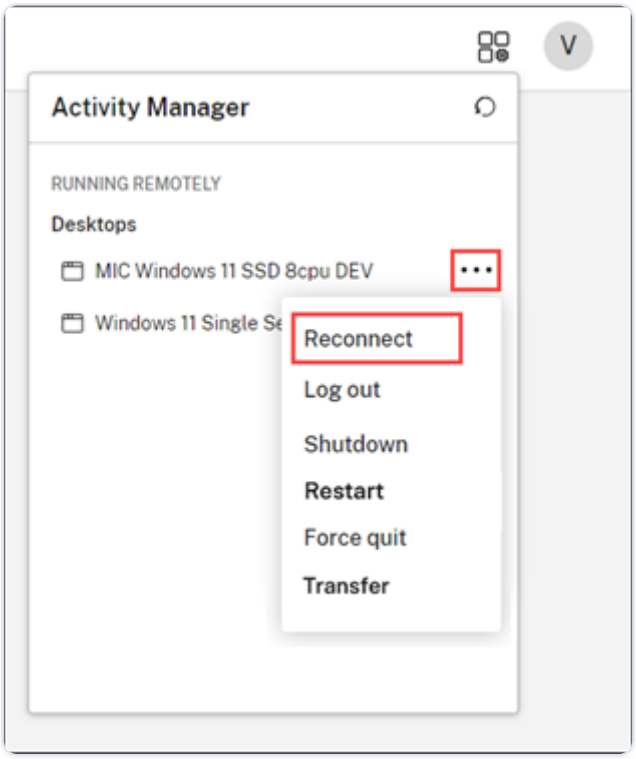
要重新连接到已断开连接的应用程序或桌面：

- 打开活动管理器，然后单击资源项。



或

- 单击省略号按钮 (...)，然后单击“**重新连接**”。

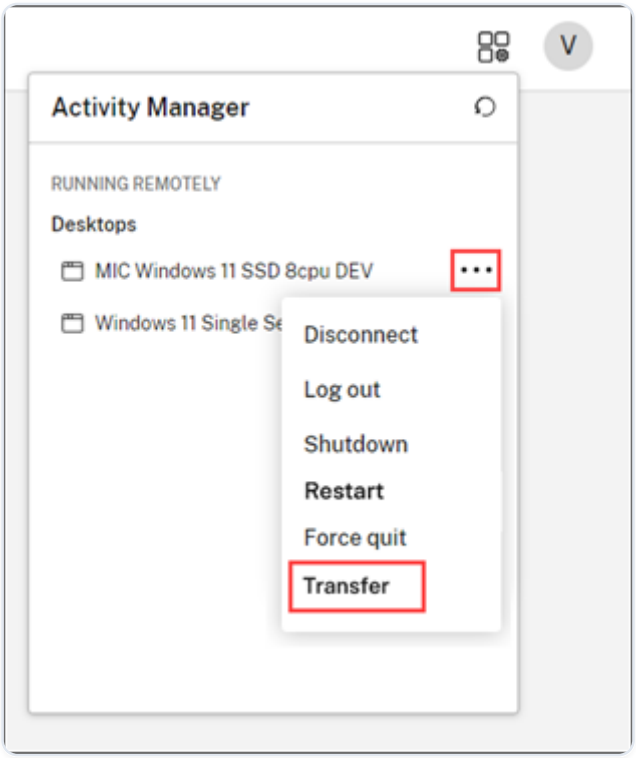


单击“**重新连接**”将从您上次离开的位置重新打开已断开连接的资源。

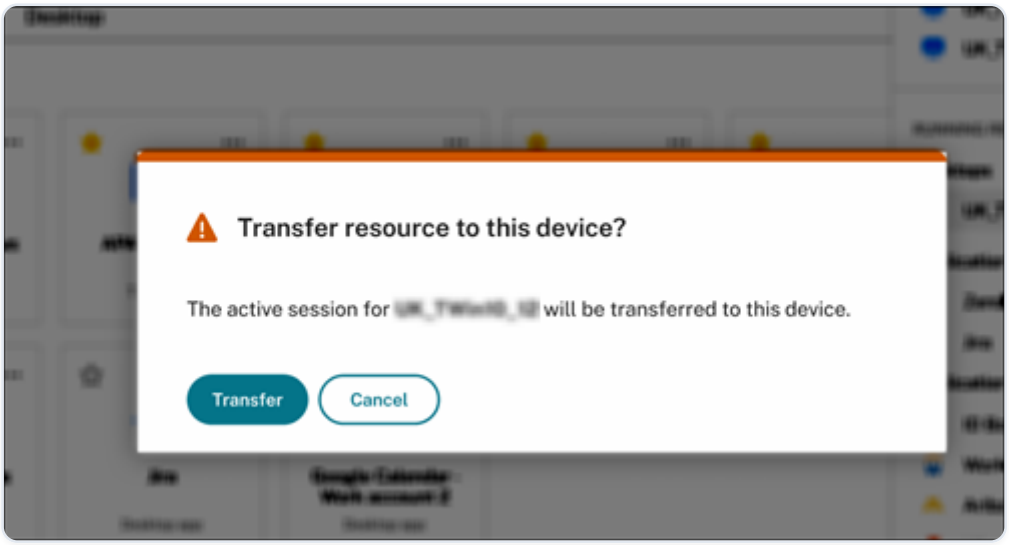
传输您的应用程序和桌面

传输功能允许最终用户将其活动应用程序和桌面从其他设备传输到当前设备。要传输应用程序和桌面，请按照以下步骤操作：

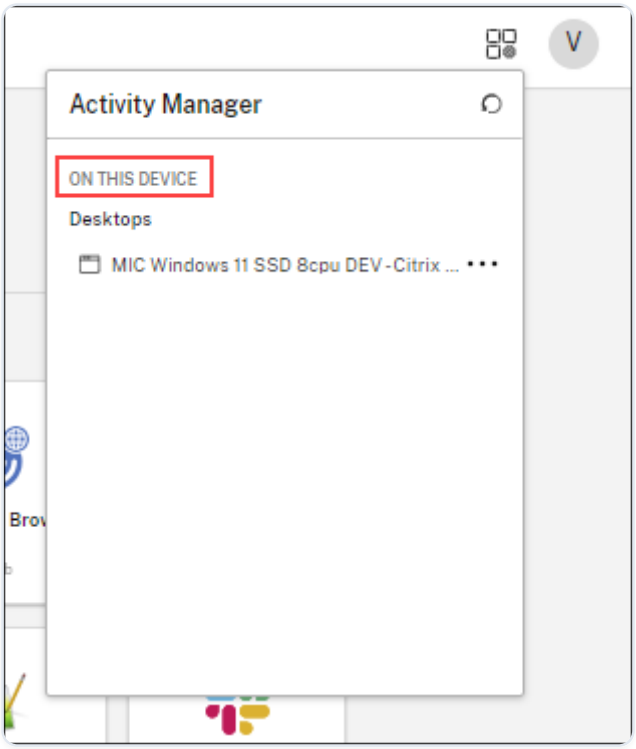
1. 单击省略号按钮 (...)，然后单击“**传输**”。



2. 在确认对话框中单击“**传输**”。



资源传输到当前设备后，您可以在活动管理器中的“**在此设备上**”部分下看到它们。



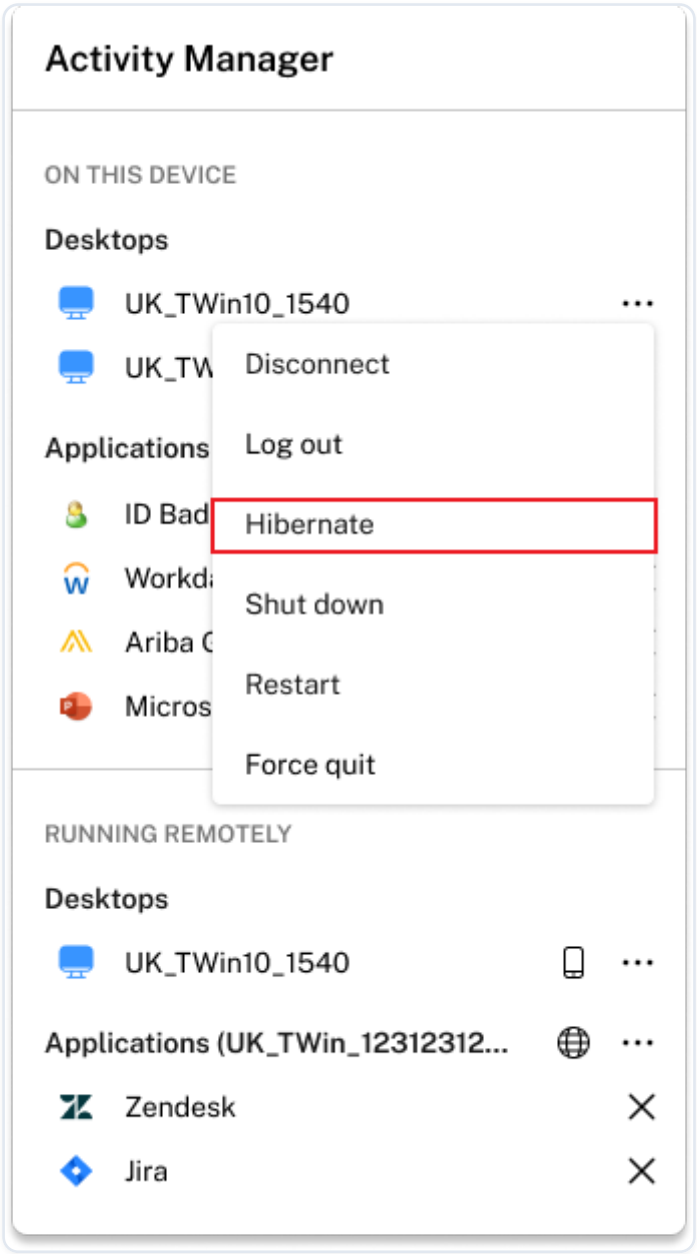
休眠和恢复虚拟桌面会话

休眠和恢复功能允许用户在不使用时休眠虚拟桌面，并在需要时无缝恢复它们，从而优化资源利用率。这不仅节省了成本和能源，还通过更快的会话恢复时间增强了用户工作流程。

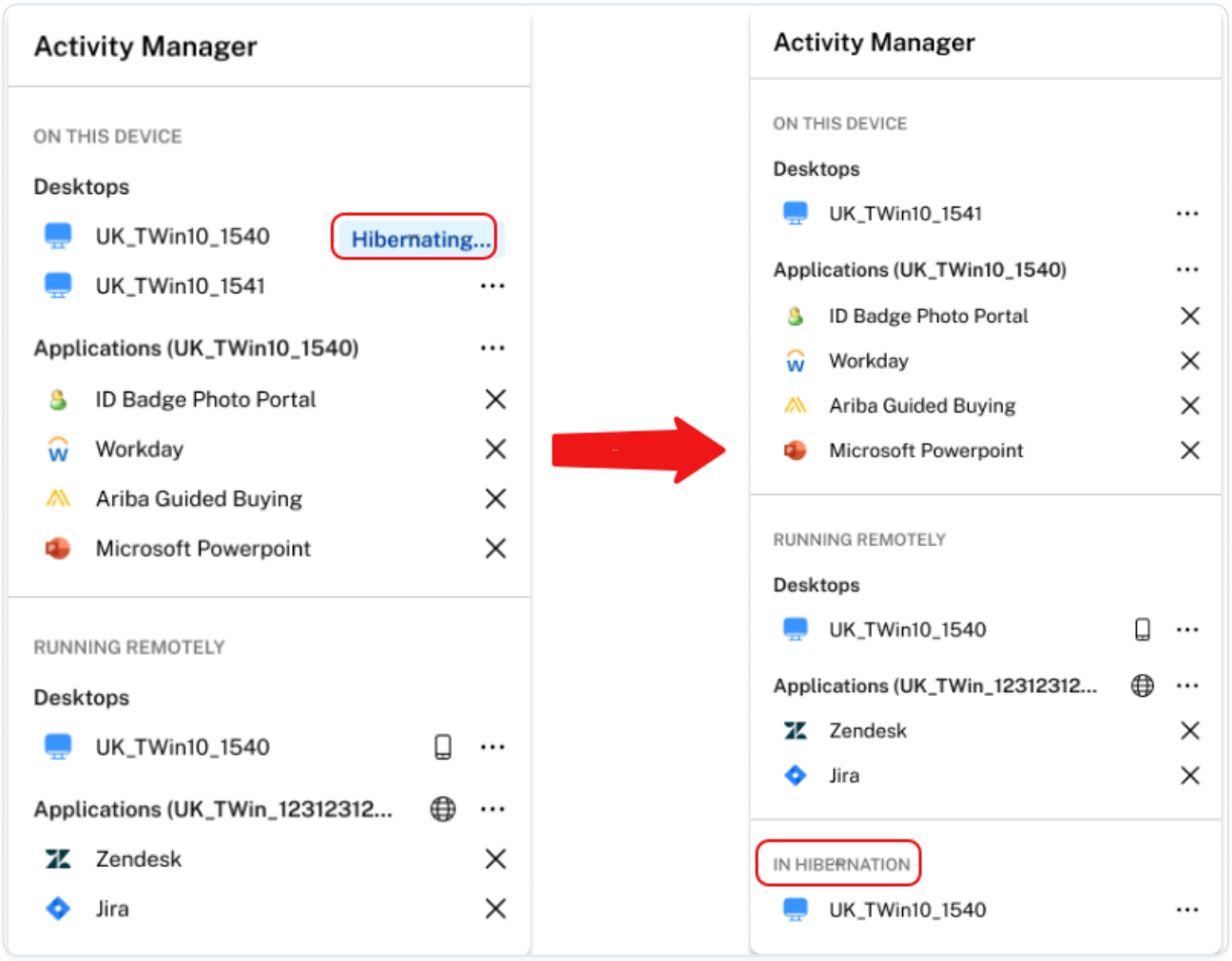
启动休眠时，管理程序会与客户操作系统通信，触发磁盘挂起操作。在此过程中，虚拟桌面的内存 (RAM) 内容会保存在操作系统磁盘上，而虚拟桌面本身则被解除分配。在随后的启动时，虚拟桌面的 RAM 内容会从操作系统磁盘恢复，确保应用程序和进程从其上次状态无缝恢复。

休眠功能适用于支持的管理程序上的分配的电源管理桌面。要启用休眠功能，管理员需要遵循特定指南并在 Azure 和 Citrix DaaS 中启用预览功能。有关更多信息，请参阅创建可休眠的 VM（预览版）。

休眠桌面会话：

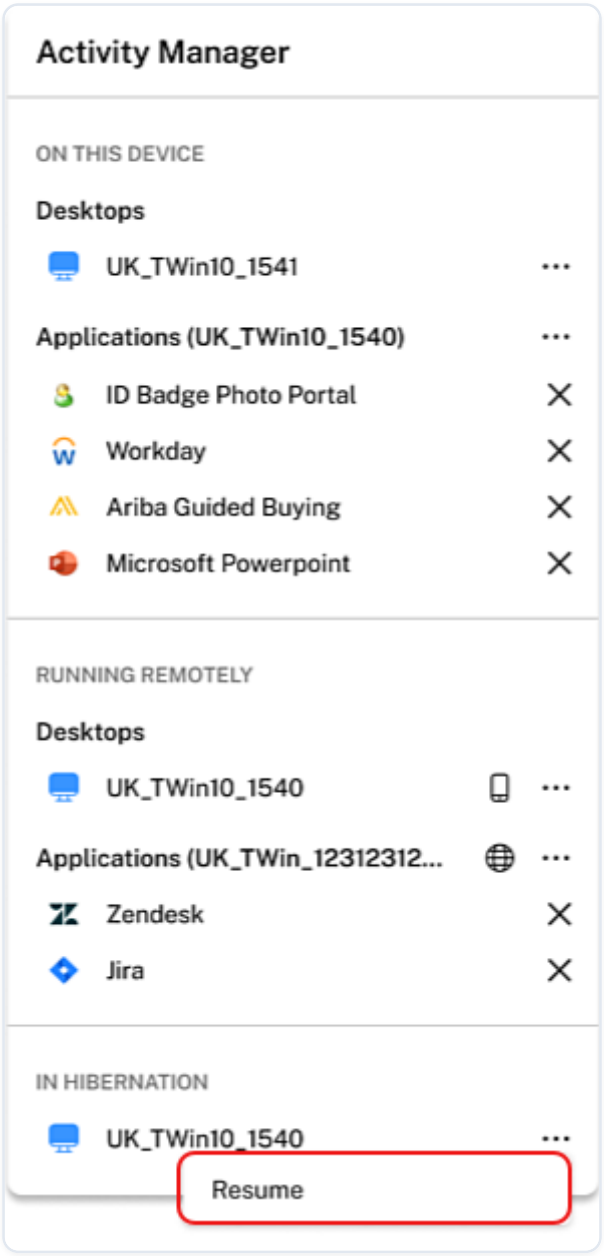


要休眠桌面会话，用户可以单击三点按钮 (...)，然后单击“**休眠**”选项。用户单击“**休眠**”选项后，桌面将启动休眠。桌面休眠后，桌面资源将移至“**活动管理器**”中的“**休眠中**”部分。

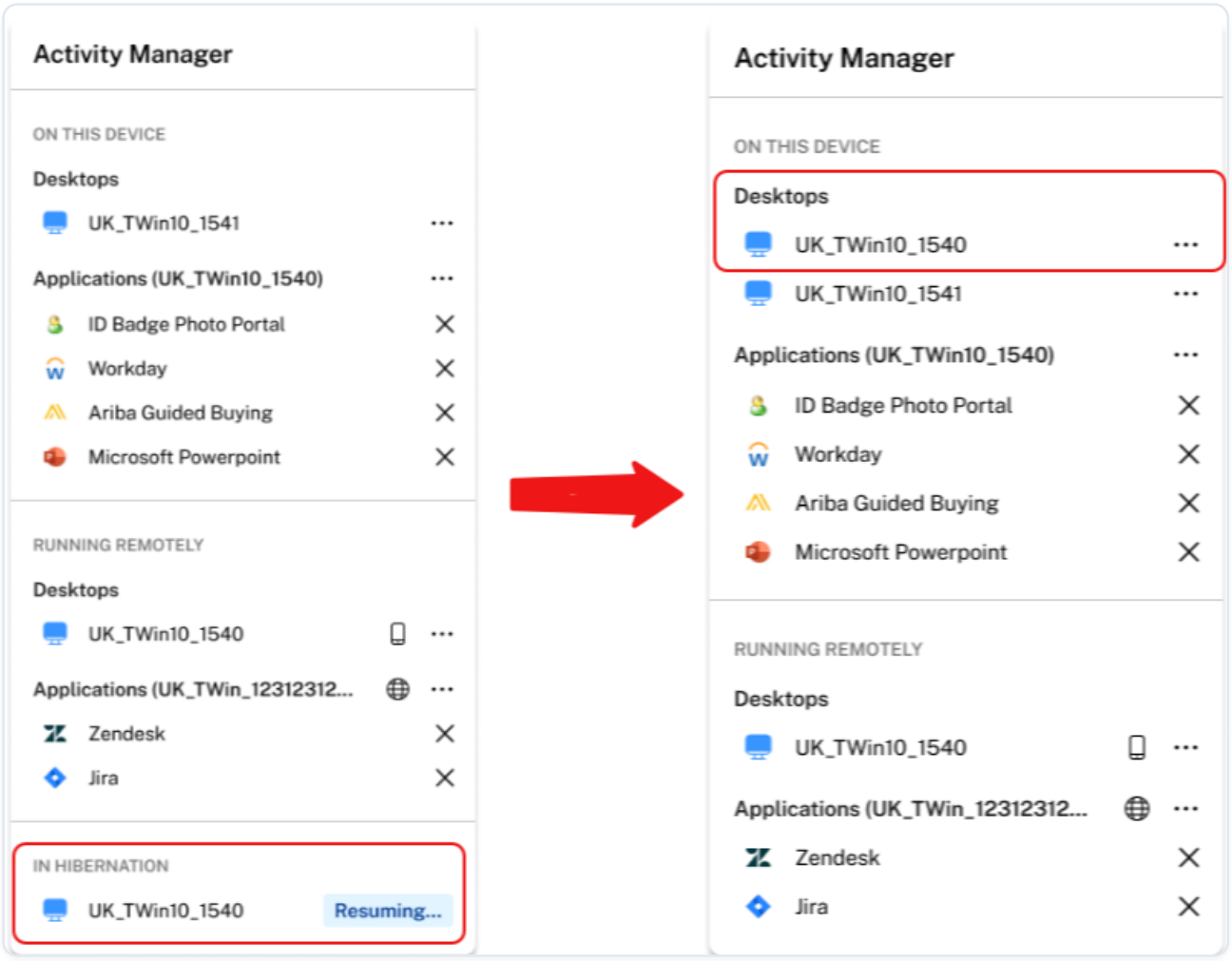


恢复休眠的桌面会话：

休眠的桌面会话可在“**活动管理器**”中的“**休眠中**”部分下找到。要恢复休眠的桌面会话，用户可以单击三点按钮 (...)，然后单击“**恢复**”选项。



用户单击“**恢复**”选项后，桌面将恢复。

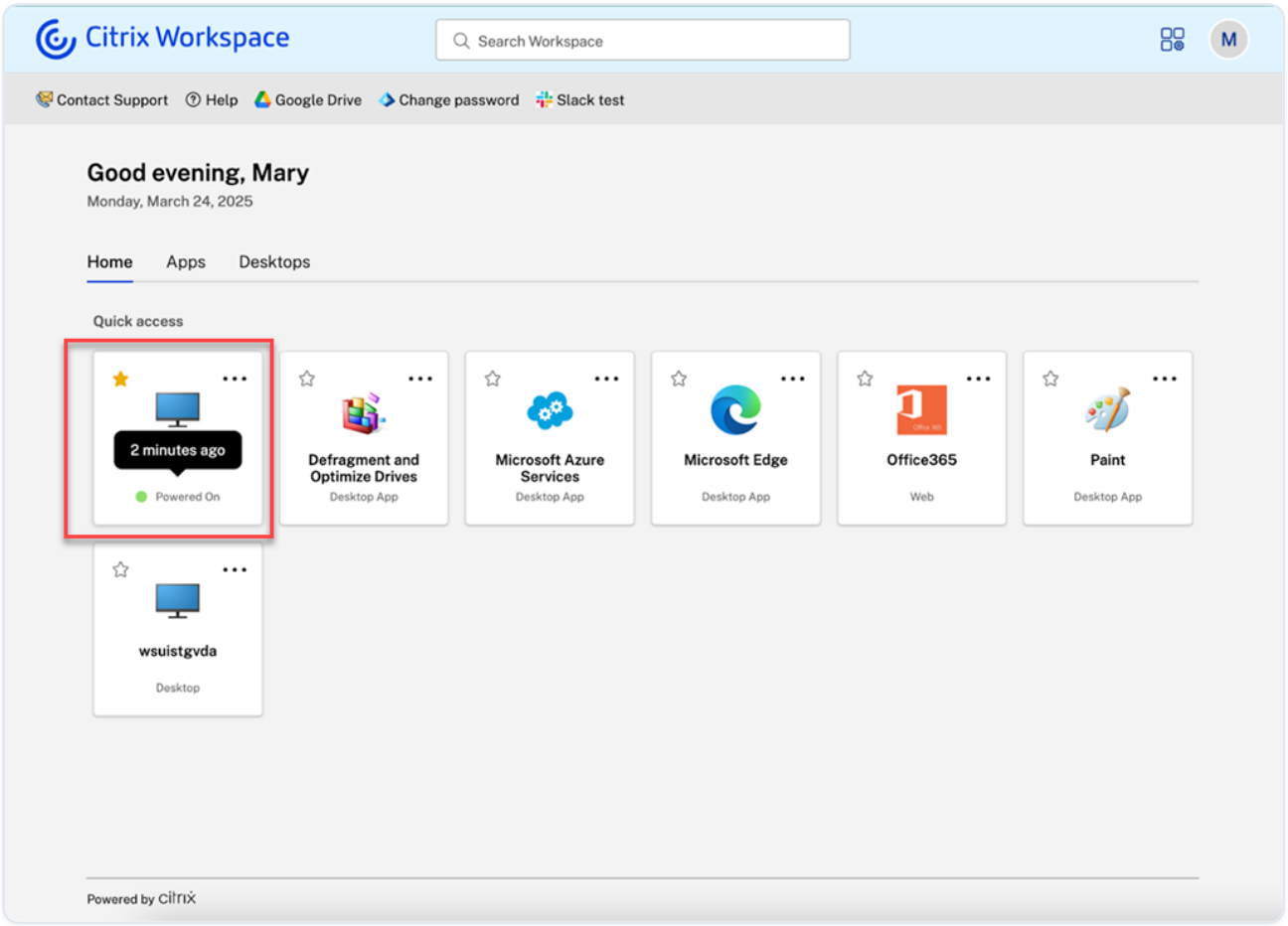


分配的桌面电源管理

电源状态

桌面磁贴可能会显示电源状态，如果满足以下条件：

- 计算机目录具有单会话操作系统，其中 桌面体验 设置为 **每次用户登录时连接到相同的（静态）桌面。**。
- 计算机目录必须配置为 电源管理。
- 计算机由 Citrix DaaS 或 Citrix Virtual Apps™ and Desktops 2511 或更高版本发布。



可能会显示以下电源状态：

- **已关机：** 计算机已关闭且当前未运行。
- **休眠中：** 计算机处于休眠状态，其当前会话已保存到磁盘，并且计算机正在使用最少的电量。
- **正在开机：** 处于 **已关机** 或 **休眠中** 状态的计算机最近已启动，但尚未准备好使用。
- **已开机：** 桌面处于活动状态并正在运行。对于专用资源，即使用户断开其会话，电源状态通常也保持“已开机”状态。
- **正在关机：** 用户已启动关机。

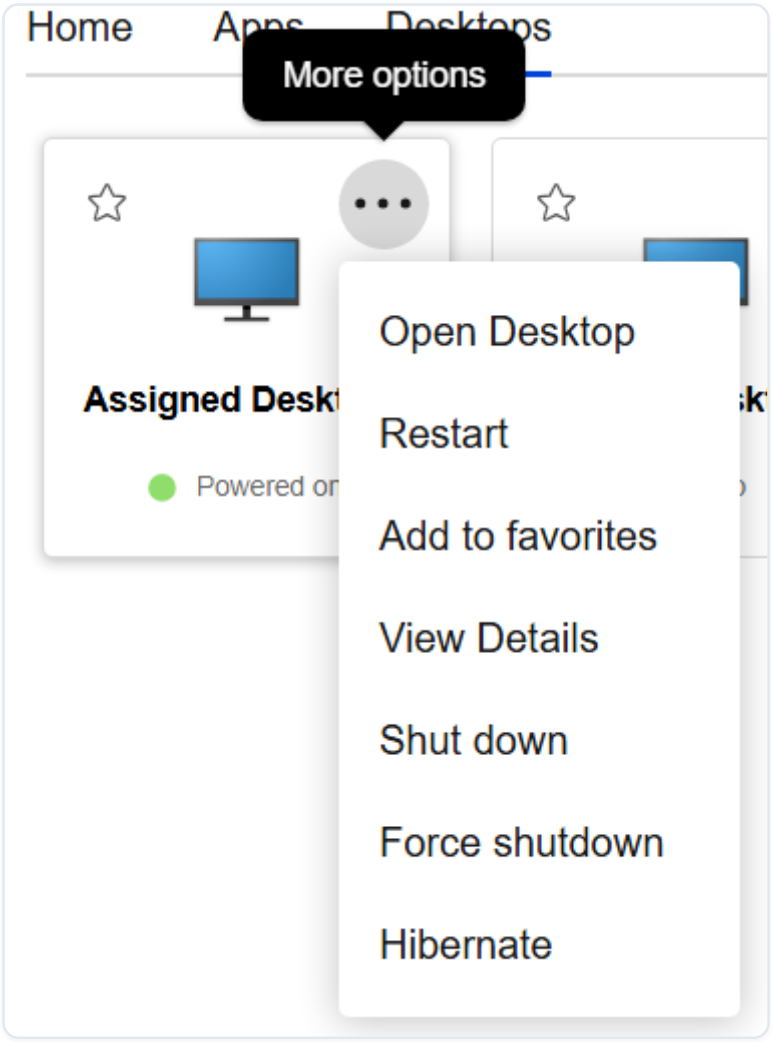
状态每两分钟刷新一次，或者在用户单击桌面磁贴上的省略号菜单时刷新。当用户将鼠标悬停在电源状态上时，会显示上次刷新的时间。

已知问题

- 当您启动多个电源管理的桌面之一时，应用商店可能会显示其他桌面不一致的电源状态，直到第一个桌面完成启动。

电源操作

磁贴上的**更多**选项菜单（省略号图标）为用户提供相关操作的访问权限。对于电源管理的分配计算机，还有其他操作，具体取决于资源的当前电源状态。



这些操作可能包括：

- **打开应用** - 启动或重新连接到应用。
- **重新启动** - 启动强制重新启动。仅适用于已分配的电源管理桌面。
- **关机** - 启动正常关机。仅适用于已分配的电源管理桌面。
- **强制关机** - 强制关闭计算机电源。仅适用于已分配的电源管理桌面。
- **休眠** - 将专用桌面置于休眠状态。仅适用于已启用休眠功能的已分配电源管理桌面。
- **恢复** - 将专用桌面从休眠状态唤醒。仅适用于已启用休眠功能的已分配电源管理桌面。

保护您的 StoreFront 部署

本文重点介绍了在部署和配置 StoreFront 时可能影响系统安全性的方面。

最终用户身份验证

通常，最终用户必须直接向 StoreFront 进行身份验证，或者向 StoreFront 前面的 Citrix Gateway 进行身份验证。有关可用身份验证方法的详细信息，请参阅身份验证。

与最终用户的通信

Citrix 建议使用 HTTPS 保护用户设备与 StoreFront 之间的通信。这可确保客户端与 StoreFront 之间发送的密码和其他数据经过加密。此外，纯 HTTP 连接可能会受到各种攻击的威胁，例如中间人攻击，尤其是在从公共 Wi-Fi 热点等不安全位置建立连接时。在没有适当的 IIS 配置的情况下，StoreFront 使用 HTTP 进行通信。

根据您的配置，用户可以通过网关或负载平衡器访问 StoreFront。您可以在网关或负载平衡器处终止 HTTPS 连接。但是，在这种情况下，Citrix 仍然建议您使用 HTTPS 保护网关或负载平衡器与 StoreFront 之间的连接。

要启用 HTTPS、禁用 HTTP 并启用 HSTS，请参阅使用 HTTPS 保护 StoreFront。

在您的 NetScaler Gateway 或负载平衡器虚拟服务器上，您可以配置启用的 TLS 版本。建议您禁用早于 1.2 的旧版 TLS 版本。

在 StoreFront 服务器上，Windows 和 IIS 决定允许哪些 TLS 版本用于传入连接。建议您禁用早于 1.2 的旧版 TLS 版本。在 Windows Server 2025 上，TLS 1.0 和 1.1 默认禁用。在 Windows Server 2022 上，您可以配置 IIS 以禁用客户端连接的 TLS 1.0 和 1.1，请参阅使用 HTTPS 保护 StoreFront。在所有 Windows 服务器版本上，您可以使用组策略或 Windows 注册表设置禁用 TLS 1.0 和 1.1，请参阅Microsoft 文档。

旧版 Citrix Receiver 无法使用 TLS 1.2 连接，有关详细信息，请参阅CTX232266。

与 Delivery Controller 的通信

Citrix 建议使用 HTTPS 协议来保护 StoreFront 与您的 Citrix Virtual Apps and Desktops Delivery Controller 之间传输的数据。有关详细信息，请参阅在 Delivery Controller 上启用 HTTPS。要配置 StoreFront 以使用 HTTPS，请参阅添加 Citrix Virtual Apps and Desktops 站点和添加 Citrix Gateway 设备。如果证书遭到泄露，您可以使用证书吊销列表 (CRL) 检查。StoreFront 使用 TLS 1.2 或更高版本与 Delivery Controller 进行通信。

建议您配置 Delivery Controller 和 StoreFront，以确保只有受信任的 StoreFront 服务器才能与 Delivery Controller 通信，请参阅管理安全密钥。

与 Cloud Connector 的通信

Citrix 建议使用 HTTPS 协议来保护 StoreFront 与 Cloud Connector 之间传输的数据。请参阅 (/zh-cn/citrix-cloud/citrix-cloud-resource-locations/citrix-cloud-connector/installation.html#https-configuration)。要配置 StoreFront，请参阅 (/zh-cn/storefront/2507-ltsr/stores/sites.html#add-sites-for-citrix-desktops-as-a-service) 和 (/zh-cn/storefront/2507-ltsr/integrate-with-citrix-gateway-and-citrix-adc/configure-citrix-gateway.html#add-citrix-gateway-appliance)。如果证书遭到泄露，可以使用 (/zh-cn/storefront/2507-ltsr/secure/certificate-revocation-list-checking.html)。StoreFront 使用 TLS 1.2 或更高版本与 Cloud Connector 通信。

建议您配置 DaaS 和 StoreFront，以确保只有受信任的 StoreFront 服务器才能与 Cloud Connector 通信。有关详细信息，请参阅 (/zh-cn/citrix-daas/manage-deployment/security-keys.html)。

与联合身份验证服务通信

有关 StoreFront 与联合身份验证服务 (FAS) 服务器之间通信的信息，请参阅 (/zh-cn/federated-authentication-service/current-release/config-manage/security.html)。

远程访问

Citrix 不建议将 StoreFront 服务器直接暴露在 Internet 上。Citrix 建议使用 Citrix Gateway 为远程用户提供身份验证和访问。

微软 Internet 信息服务 (IIS) 强化

您可以使用受限的 IIS 配置来配置 StoreFront。请注意，这不是默认的 IIS 配置。

文件名扩展名

您可以使用请求筛选来配置允许的文件扩展名列表，并禁止未列出的文件名扩展名。请参阅 IIS 文档。

StoreFront 需要以下文件扩展名：

- .（空白扩展名）
- .appcache 文件
- .aspx 扩展名
- .cr
- .css 扩展名
- .dtd 文件
- .gif 文件
- HTML 文件
- .html 文件
- ICA 文件
- .ico 文件
- JPEG 文件
- .js
- ．png
- .svg 文件
- 文本文件
- XML 文件

如果为商店网站启用了 Citrix Workspace 应用程序的下载或升级，StoreFront 还需要以下文件扩展名：

- DMG 文件
- 可执行文件

如果启用了适用于 HTML5 的 Citrix Workspace 应用程序，StoreFront 还需要以下文件扩展名：

- ．eot
- “.ttf”
- 点woff

- WebAssembly 文件

动词

您可以使用请求筛选来配置允许的动词列表，并禁止未列出的动词。请参阅 IIS 文档。

- GET
- POST
- HEAD

URL 中的非 ASCII 字符

如果您确保商店名称和网站名称仅使用 ASCII 字符，则 StoreFront URL 不会包含非 ASCII 字符。您可以使用请求筛选来禁止非 ASCII 字符。请参阅 IIS 文档。

MIME 类型

您可以删除与以下文件扩展名对应的操作系统 shell MIME 类型：

- .exe 文件
- .dll 文件
- .com 文件
- .bat 文件
- 点csh

请参阅 IIS 文档。

删除 X-Powered-By 标头

默认情况下，IIS 在服务器级别包含一个值为 `ASP.NET` 的标头 `X-Powered-By`。StoreFront 会删除所有 StoreFront 网站上的此标头。您也可以在服务器级别删除此标头，这适用于服务器上的所有网站，请参阅 IIS 自定义标头文档。

删除包含 IIS 版本的 Server 标头

默认情况下，IIS 通过添加 `Server` 标头来报告 IIS 版本。您可以配置 IIS 以删除此标头。请参阅 IIS 请求筛选文档。

将 StoreFront 网站移动到单独的分区

您可以将 StoreFront 网站托管在与系统文件分开的单独分区上。在 IIS 中，您必须在创建 StoreFront 部署之前，将 **默认网站** 移动到或在适当的分区上创建单独的站点。

IIS 功能

有关 StoreFront 安装和使用的 IIS 功能列表，请参阅 系统要求。您可以删除其他 IIS 功能。

尽管 StoreFront 不直接使用 ISAPI 筛选器，但 ASP.NET 需要此功能，因此无法卸载。

处理程序映射

StoreFront 需要以下处理程序映射。您可以删除其他处理程序映射。

- 无扩展名URL处理程序-集成-4.0
- 页面处理程序工厂-集成-4.0
- StaticFile

请参阅 IIS 处理程序文档。

ISAPI 筛选器

StoreFront 不需要任何 ISAPI 筛选器。您可以删除所有 ISAPI 筛选器。但是，ASP.NET 需要 ISAPI Windows 功能。请参阅 IIS ISAPI 筛选器文档。

.NET 授权规则

默认情况下，IIS 服务器将“.NET 授权规则”设置为“允许所有用户”。默认情况下，StoreFront 使用的网站继承此配置。

如果您在服务器级别删除或更改 .NET 授权规则，则必须覆盖 StoreFront 使用的网站上的规则，以添加“所有用户”的允许规则并删除任何其他规则。

零售模式

您可以启用零售模式，请参阅 IIS 文档。

应用程序池

StoreFront 创建以下应用程序池：

- Citrix 配置 API
- Citrix 交付服务身份验证
- Citrix 交付服务资源
- 和 Citrix Receiver™ 网页版

请勿更改每个 IIS 应用程序使用的应用程序池或每个池的标识。如果您使用多个站点，则无法将每个站点配置为使用单独的应用程序池。

在“回收”设置下，您可以设置应用程序池空闲超时和虚拟内存限制。请注意，当“Citrix Receiver for Web”应用程序池回收时，会导致通过 Web 浏览器登录的用户注销，因此默认设置为每天 02:00 回收，以最大程度地减少中断。如果您更改任何回收设置，可能会导致用户在一天中的其他时间注销。

默认 IIS 登录页面

您可以从 `c:\inetpub\wwwroot` 删除文件 `iisstart.htm`、`welcome.png`。

所需设置

- 请勿更改 IIS 身份验证设置。StoreFront 管理身份验证并使用适当的身份验证设置配置 StoreFront 站点的目录。
- 对于 StoreFront 服务器，在 **SSL 设置**下，请勿选择 **客户端证书: 要求**。StoreFront 安装会使用此设置配置 StoreFront 站点的相应页面。
- StoreFront 需要 Cookie 来实现会话状态和其他功能。在某些目录中，在 **会话状态**、**Cookie 设置**下，**模式**必须设置为 **使用 Cookie**。
- StoreFront 要求将 **.NET 信任级别**设置为 **完全信任**。请勿将 .NET 信任级别设置为任何其他值。

服务

StoreFront 安装会创建以下 Windows 服务：

- Citrix 配置复制 (NT SERVICE\CitrixConfigurationReplication)
- Citrix 群集加入 (NT SERVICE\CitrixClusterService)
- 思杰对等解析 (NT SERVICE\Citrix Peer Resolution Service)
- Citrix 凭据钱包 (NT SERVICE\CitrixCredentialWallet)
- Citrix 订阅存储 (NT SERVICE\CitrixSubscriptionsStore)
- Citrix 默认域服务 (NT SERVICE\CitrixDefaultDomainService)

这些帐户以 `Network Service` 身份登录。请勿更改此配置。

如果您为 XenApp 6.5 配置 StoreFront Kerberos 约束委派，这还会额外创建 Citrix StoreFront 协议转换服务 (NT SERVICE\CitrixStoreFrontProtocolTransition)。此服务以 `NT AUTHORITY\SYSTEM` 身份运行。请勿更改此配置。

用户权限分配

修改偏离默认设置的用户权限分配可能会导致 StoreFront 出现问题。具体而言：

- Microsoft IIS 作为 StoreFront 安装的一部分启用。Microsoft IIS 授予内置组 IIS_IUSRS 登录权限 **作为批处理作业登录** 和特权 **在身份验证后模拟客户端**。这是正常的 Microsoft IIS 安装行为。请勿更改这些用户权限。有关详细信息，请参阅 Microsoft 文档。
- 安装 StoreFront 时，它会创建 应用程序池，IIS 会向其授予用户权限 **作为服务登录**、**调整进程的内存配额**、**生成安全审核** 和 **替换进程级别令牌**。
- 要创建或更改部署，管理员必须拥有权限 **还原文件和目录**。
- 要使服务器加入服务器组，Administrators 组必须拥有权限 **还原文件和目录**、**从网络访问此计算机** 和 **管理审核和安全日志**。
- 要使用用户名和密码身份验证（直接或通过网关）登录的用户，必须拥有权限 **允许本地登录**，除非您已将 StoreFront 配置为通过交付控制器验证密码。

这不是一个全面的列表，可能还需要其他用户访问权限。

配置组成员身份

配置 StoreFront 服务器组时，以下服务将添加到 Administrators 安全组中：

- Citrix 配置复制 (NT SERVICE\CitrixConfigurationReplication)
- Citrix 群集加入 (NT SERVICE\CitrixClusterService)。此服务仅在属于某个组的服务器上可见，并且仅在加入过程中运行。

StoreFront 正常运行需要这些组成员身份，以便：

- 创建、导出、导入和删除证书，并设置其访问权限
- 读取和写入 Windows 注册表
- 在全局程序集缓存 (GAC) 中添加和删除 Microsoft .NET Framework 程序集
- 访问文件夹 **Program Files\\Citrix**<*StoreFrontLocation*>
- 添加、修改和删除 IIS 应用程序池标识和 IIS Web 应用程序
- 添加、修改和删除本地安全组和防火墙规则
- 添加和删除 Windows 服务和 PowerShell 管理单元
- 注册 微软 Windows 通信框架 (WCF) 终结点

在 StoreFront 的更新中，此操作列表可能会在不另行通知的情况下发生更改。

StoreFront 安装还会创建以下本地安全组：

- CitrixClusterMembers
- CitrixCWServiceReadUsers
- CitrixCWServiceWriteUsers
- CitrixDelegatedAuthenticatorUsers
- CitrixDelegatedDirectoryClaimFactoryUsers
- CitrixPNRSReplicators
- CitrixPNRSUsers
- CitrixStoreFrontAdministrators
- CitrixSubscriptionServerUsers
- CitrixSubscriptionsStoreServiceUsers
- CitrixSubscriptionsSyncUsers

StoreFront 维护这些安全组的成员资格。它们用于 StoreFront 内部的访问控制，不适用于文件和文件夹等 Windows 资源。请勿修改这些组成员资格。

NTLM

如果使用本地 ESENT 数据库启用了收藏夹，则 StoreFront 在服务器组中同步收藏夹时可能会使用 NTLM。如果禁用 NTLM，则收藏夹可能无法同步。作为替代方案，您可以使用 SQL Server 数据库。

如果用户使用 (/zh-cn/storefront/current-release/stores/authentication/domain-pass-through.html) 进行身份验证，则 IIS 默认情况下会尽可能使用 Kerberos，否则会回退到 NTLM。如果 StoreFront 前面有负载均衡器，则它总是回退到 NTLM。

您可以将服务器配置为仅使用 NTLMv2 并拒绝 NTLMv1，请参阅 Microsoft 文档。在 Windows Server 2025 及更高版本中，NTLMv1 已被移除，因此始终使用 NTLMv2。

StoreFront 中的证书

服务器证书

服务器证书用于 StoreFront 中的计算机识别和传输层安全 (TLS) 传输安全。如果您决定启用 ICA 文件签名，StoreFront 还可以使用证书对 ICA 文件进行数字签名。

有关详细信息，请参阅 (#communication-with-end-users) 和 (#ica-file-signing)。

令牌管理证书

身份验证服务和存储都需要用于令牌管理的证书。当创建身份验证服务或存储时，StoreFront 会生成一个自签名证书。StoreFront 生成的自签名证书不应用于任何其他目的。

思杰交付服务证书

StoreFront 在自定义 Windows 证书存储 (Citrix Delivery Services) 中保存了多个证书。Citrix Configuration Replication 服务、Citrix Credential Wallet 服务和 Citrix Subscriptions Store 服务使用这些证书。群集中的每个 StoreFront 服务器都有一份这些证书的副本。这些服务不依赖 TLS 进行安全通信，并且这些证书不作为 TLS 服务器证书使用。这些证书在创建 StoreFront 存储或安装 StoreFront 时创建。请勿修改此 Windows 证书存储的内容。

代码签名证书

StoreFront 在 <*InstallDirectory*>\Scripts 文件夹中包含多个 PowerShell 脚本 (.ps1)。默认的 StoreFront 安装不使用这些脚本。它们简化了特定和不常见任务的配置步骤。这些脚本已签名，允许 StoreFront 支持 PowerShell 执行策略。我们建议使用 **AllSigned** 策略。（不支持 **Restricted** 策略，因为它会阻止 PowerShell 脚本执行。）StoreFront 不会更改 PowerShell 执行策略。

尽管 StoreFront 不会在“受信任的发布者”存储中安装代码签名证书，但 Windows 可以自动将代码签名证书添加到其中。当 PowerShell 脚本以“**始终运行**”选项执行时，就会发生这种情况。（如果您选择“**从不运行**”选项，则证书会添加到“不受信任的证书”存储中，并且 StoreFront PowerShell 脚本将无法执行。）一旦代码签名证书已添加到“受信任的发布者”存储中，Windows 将不再检查其有效期。在 StoreFront 任务完成后，您可以从“受信任的发布者”存储中删除此证书。

StoreFront 安全隔离

如果您在与 StoreFront 相同的 Web 域（域名和端口）中部署任何 Web 应用程序，则这些 Web 应用程序中的任何安全风险都可能降低 StoreFront 部署的安全性。如果需要更高程度的安全隔离，Citrix 建议您将 StoreFront 部署在单独的 Web 域中。

ICA 下载

ICA 文件包含连接到 VDA 的信息，并且通常无需进一步身份验证即可单点登录到这些 VDA。因此，请确保 ICA 文件受到保护。对于混合启动，根据配置，ICA 文件可能会下载到用户设备。建议您禁用 ICA 下载。有关详细信息，请参阅 启动首选项。

ICA 文件签名

StoreFront 提供了使用服务器上指定证书对 ICA 文件进行数字签名的选项，以便支持此功能的 Citrix Workspace 应用程序版本可以验证文件是否源自受信任的来源。ICA 文件可以使用 StoreFront 服务器上运行的操作系统支持的任何哈希算法进行签名，包括 SHA-1 和 SHA-256。有关详细信息，请参阅 启用 ICA 文件签名。

应用程序保护

您可以使用 应用程序保护 来防止屏幕捕获和屏幕记录器。对于混合启动，应用程序保护默认处于禁用状态。要启用它，请参阅 应用程序保护。

用户更改密码

您可以允许通过 Web 浏览器使用 Active Directory 域凭据登录的用户更改其密码，无论是在任何时候还是仅在密码过期时。但是，这会将敏感的安全功能暴露给任何可以访问使用身份验证服务的任何应用商店的人。如果您的组织有安全策略规定用户密码更改功能仅供内部使用，请确保任何应用商店都无法从公司网络外部访问。创建身份验证服务时，默认配置会阻止用户更改其密码，即使密码已过期。有关详细信息，请参阅 允许用户更改其密码。

自定义项

为了加强安全性，内容安全策略会阻止来自其他服务器的脚本。编写自定义项时，请将脚本放在网站 `custom` 文件夹中。如果 StoreFront 配置为 HTTPS 连接，请确保指向自定义内容或脚本的任何链接也使用 HTTPS。

安全标头

通过 Web 浏览器查看应用商店网站时，StoreFront 会返回以下与安全相关的标头，这些标头对 Web 浏览器施加了限制。

标头名称	值	描述
`content-security-policy`	`frame-ancestors 'none'`	这可以防止其他站点在框架中嵌入 StoreFront 网站，从而避免点击劫持攻击。此外，HTML 页面包含一个 `meta` 标签，其中包含一个 `content-security-policy`

标头名称	值	描述
		，用于限制脚本源以减轻 XSS 攻击。
`X-Content-Type-Options`	`nosniff`	这可以避免 MIME 类型嗅探。
`X-Frame-Options`	`deny`	这可以防止其他网站在框架内嵌入 StoreFront 网站，从而避免点击劫持攻击。它已被 `content-security-policy` 到 `frame-ancestors 'none'` 淘汰，但仍受某些不支持 `content-security-policy` 的旧版浏览器支持。
`X-XSS-Protection`	`1; mode=block`	某些浏览器使用此功能来缓解 XSS（跨站点脚本）攻击。

默认情况下未设置 `Strict-Transport-Security`，但可以对其进行配置。有关详细信息，请参阅 HSTS。

Cookie 文件

StoreFront 使用多个 Cookie。网站运行中使用的部分 Cookie 如下：

COOKIE 文件	描述
`ASP.NET_SessionId`	跟踪用户会话，包括身份验证状态。已设置 `HttpOnly`。
`CtxsAuthId`	为防止会话固定攻击，StoreFront 还会使用此 Cookie 跟踪用户是否已通过身份验证。它已设置 `HttpOnly`。
`CsrfToken`	用于通过标准 Cookie-to-header token 模式防止跨站点请求伪造。服务器在 Cookie 中设置一个令牌。客户端从 Cookie 中读取令牌，并在后续请求中将令牌包含在查询字符串或标头中。此 Cookie 要求不设置 `HttpOnly`，以便客户端 JavaScript 可以读取它。

COOKIE 文件	描述
`CtxsDeviceId`	识别设备。已设置 `HttpOnly`。

StoreFront 设置了许多其他 Cookie 来跟踪用户状态，其中一些需要由 JavaScript 读取，因此未设置 `HttpOnly`。这些 Cookie 不包含任何与身份验证或其他机密信息相关的信息。

如果客户端通过 HTTPS 连接，则在创建或更新 Cookie 时会设置 `secure` 属性。

其他安全信息

> **注意：**
>
> 此信息可能随时更改，恕不另行通知。

> 您的组织可能出于法规原因希望对 StoreFront 执行安全扫描。上述配置选项有助于消除安全扫描报告中的一些发现。

如果安全扫描器和 StoreFront 之间存在网关，则某些发现可能与网关相关，而不是与 StoreFront 本身相关。安全扫描报告通常不会区分这些发现（例如，TLS 配置）。因此，安全扫描报告中的技术描述可能会产生误导。

使用 HTTPS 保护 StoreFront

Citrix 强烈建议使用 HTTPS 保护 StoreFront 与用户设备之间的通信。这可确保客户端与 StoreFront 之间发送的密码和其他数据经过加密。此外，纯 HTTP 连接容易受到各种攻击的威胁，例如中间人攻击，尤其是在从公共 Wi-Fi 热点等不安全的场所建立连接时。如果没有适当的 IIS 配置，StoreFront 将使用 HTTP 进行通信。

根据您的配置，用户可能通过网关或负载均衡器访问 StoreFront。您可以在网关或负载均衡器处终止 HTTPS 连接。但是，在这种情况下，Citrix 仍然建议您在网关、负载均衡器和 StoreFront 之间使用 HTTPS 建立安全连接。使用 NetScaler 负载均衡器时，有关证书要求，请参阅 ADC 设备上的服务器证书支持矩阵。

如果 StoreFront 未配置 HTTPS，它将显示以下警告：



创建或导入证书

- 确保 StoreFront (/zh-cn/storefront/2507-ltsr/manage-deployment/base-url.html) 作为通用名称或主题备用名称 (SAN) 包含在 DNS 字段中。在 StoreFront 服务器前面使用负载均衡器时，建议将服务器 FQDN 和负载均衡器 FQDN 都作为 SAN 包含在内。这允许您直接连接到特定的 StoreFront 服务器进行故障排除。
- 使用适用于您的组织的企业根 CA 或公共 CA 对证书进行签名。
- 如果用户通过负载均衡器或网关访问 StoreFront，则证书只需由负载均衡器或网关信任。如果用户直接连接到 StoreFront 服务器，则客户端必须信任该证书。

您必须在 Windows 中创建或导入证书到“**个人**”证书存储区。要查看已安装的证书：

1. 打开 **IIS 信息服务 (IIS) 管理器**。
2. 在“**连接**”窗格中，选择服务器。
3. 打开“**服务器证书**”。

有关管理证书的更多信息，请参阅 管理证书。

为 HTTPS 配置 IIS

要在 StoreFront 服务器上为 HTTPS 配置 Microsoft Internet Information Services (IIS)：

1. 在左侧的树状视图中选择 **Default Web Site**（或相应的网站）
2. 在“操作”窗格中单击 **Bindings...**

   IIS 管理服务器默认网站主屏幕突出显示绑定链接的屏幕截图(/en-us/storefront/2507-ltsr/media/secure/iis-default-web-site-highlight-bindings.png)
3. 在“绑定”窗口中单击 **Add...**
4. 在“**类型**”下拉列表中选择 **https**
5. 在 Windows Server 2022 或更高版本上，单击 **Disable Legacy TLS** 以禁用早于 1.2 的 TLS 版本。

   在较旧的 Windows Server 版本上，您可以使用 Windows 注册表设置禁用旧版 TLS 版本，请参阅 Windows Server Documentation。
6. 选择之前导入的证书。按“确定”

   “添加站点绑定”窗口的屏幕截图(/en-us/storefront/2507-ltsr/media/secure/iis-add-site-binding.png)
7. 要删除 HTTP 访问，请选择 HTTP，然后单击 **Remove**。

“站点绑定”窗口的屏幕截图(/en-us/storefront/2507-ltsr/media/secure/iis-site-bindings.png)

8. 更新 base url 以使用 https 协议。

HSTS

即使在服务器端启用了 HTTPS，用户的客户端设备仍然容易受到攻击。例如，中间人攻击者可能会欺骗 StoreFront 服务器，诱使用户通过纯 HTTP 连接到欺骗服务器。然后，他们可以访问敏感信息，例如用户的凭据。解决方案是确保用户的浏览器不会尝试通过 HTTP 访问服务器。您可以通过 HTTP Strict Transport Security (HSTS) 实现此目的。

启用 HSTS 后，服务器会向 Web 浏览器指示，对网站的请求应始终通过 HTTPS 进行。如果用户尝试使用 HTTP 访问 URL，浏览器将自动切换为使用 HTTPS。这可确保安全连接的客户端验证以及 IIS 中的服务器端验证。Web 浏览器会在配置的期限内保持此验证。

> **注意：**

> 启用 HSTS 会影响同一域上的所有网站。例如，如果网站可通过 `https://www.company.com/Citrix/StoreWeb` 访问，则 HSTS 策略将应用于 `https://www.company.com` 下的所有网站，这可能不是您希望的结果。

> 有多种启用 HSTS 的选项。您应仅选择一个选项，以避免多次设置相同的标头。

选项 1 - IIS

在 Windows Server 2019 及更高版本上，您可以在 IIS 中配置 HSTS。

1. 打开 **Internet 信息服务 (IIS) 管理器**。
2. 选择 **Default Web Site**（或相应的网站）。
3. 在右侧的“操作”窗格中，单击 **HSTS...**。
4. 选择 **启用**。
5. 输入最大使用期限，例如，一年为 31536000。
6. （可选）选择 **将 HTTP 重定向到 HTTPS**。
7. 按 **确定**

HSTS 设置的屏幕截图(/en-us/storefront/2507-ltsr/media/secure/iis-hsts.png)

选项 2 - StoreFront™ 管理控制台

对于每个应用商店网站：

1. 选择应用商店，然后单击 **管理网站**。
2. 选择网站，然后单击 **配置...**
3. 转到 **高级设置** 选项卡
4. 选择 **启用严格传输安全**。
5. 将 **严格传输安全策略持续时间** 更新为所需的值。
6. 单击“**确定**”。

选项 3 - NetScaler® 负载均衡器

如果您在 StoreFront 服务器前面使用 NetScaler 负载均衡器，则可以在虚拟服务器上配置 HSTS。有关详细信息，请参阅 NetScaler 文档。

选项 4 - NetScaler Gateway

如果用户通过 NetScaler Gateway 连接到 StoreFront，则可以在 VPN 虚拟服务器上配置 HSTS。这样做的好处是，它也适用于 NetScaler 登录表单以及 StoreFront 托管的页面。

证书吊销列表 (CRL) 检查

简介

您可以将 StoreFront 配置为使用已发布的证书吊销列表 (CRL) 检查 CVAD 交付控制器使用的 TLS 证书的状态。如果出现以下情况，您可能需要吊销对证书的访问权限：

- 您认为私钥已泄露
- CA 已泄露
- 关联关系已更改
- 证书已被取代

> **注意：**

> 仅当 StoreFront 与 Citrix Virtual Apps and Desktops 交付控制器之间使用 HTTPS 连接时，本主题才相关。与交付控制器的 HTTP 连接不需要证书，因此，此处描述的 Store 的 -CertRevocationPolicy 设置无效。

> StoreFront 支持使用 CRL 分发 点 (CDP) 证书扩展和本地安装的证书吊销 列表 (CRL)。StoreFront 仅支持完整 CRL：不支持增量 CRL。

CRL 分发点 (CDP) 扩展

StoreFront 不会枚举来自 Citrix Virtual Apps and Desktops 交付控制器的资源，这些控制器正在使用其序列号列在已发布 CRL 中的已吊销证书。为了检测哪些证书已被吊销，StoreFront 必须能够使用 CDP 证书扩展中定义的 URL 之一访问已发布的 CRL。

带有 CLR 扩展点扩展的证书屏幕截图(/en-us/storefront/2507-ltsr/media/stores/clr-distribution-point-extensions-blur.png)

CRL 发布间隔

为了使 StoreFront 更快地检测到交付控制器上的已吊销证书，请缩短 CA 上的 CRL 发布间隔。编辑 CLR 分发点扩展的属性，以设置适合您的公钥基础结构的较低 CLR 发布间隔值。

已吊销证书属性(/en-us/storefront/2507-ltsr/media/stores/revoked-certificate-properties.png)

客户端 CRL 缓存

Windows 公钥基础设施客户端在本地缓存 CRL。只有当本地缓存的 CRL 过期后，才会下载更新的 CRL。

StoreFront 对证书吊销列表 (CRL) 的访问

证书吊销检查依赖于 StoreFront 访问 CRL 的能力。请仔细考虑 StoreFront 如何联系发布 CRL 的 Web 服务器或证书颁发机构 (CA)，以及 StoreFront 如何接收 CRL 更新。

交付控制器上的内部企业 CA 和私有证书

要使用私有 CA 和证书，StoreFront 需要一个正确配置的企业 CA 和一个已发布的 CRL，StoreFront 可以在您的组织和内部网络中访问该 CRL。有关配置企业 CA 以发布 CDP 扩展的信息，请参阅 Microsoft 文档。在配置 CA 以包含 CDP 扩展之前存在的交付控制器上的任何证书可能需要重新颁发。

StoreFront 和 Citrix Virtual Apps and Desktops 服务器通常位于无法访问 Internet 的隔离私有网络中。在这种情况下，应使用私有 CA。

交付控制器上的外部公共 CA 和公共证书

StoreFront 服务器和 Citrix Virtual Apps and Desktops 交付控制器可以使用公共 CA 颁发的证书。StoreFront 必须能够通过 Internet 联系公共 CA 的 Web 服务器，使用 CDP 扩展中引用的 URL。如果公共证书被吊销后，StoreFront 无法使用 CDP URL 下载 CRL 副本，则 StoreFront 无法执行 CRL 检查。

查看证书吊销策略

要使用 PowerShell 查看策略设置，请运行 cmdlet `Get-STFStoreFarmConfiguration` 并在结果对象中查看属性 `CertRevocationPolicy`。例如：

```
$store=Get-STFStoreService -VirtualPath '/Citrix/Store'

(Get-STFStoreFarmConfiguration -StoreService $store).CertRevocationPolicy
```

配置证书吊销策略

要使用 PowerShell 为存储设置证书吊销策略，请运行带参数 `-CertRevocationPolicy` 的 cmdlet `Set-STFStoreFarmConfiguration`。

`CertRevocationPolicy` 选项可以设置为以下值：

设置	描述
NoCheck	StoreFront 不检查交付控制器上证书的吊销状态。StoreFront 仍会从使用已吊销证书的交付控制器枚举资源。这是默认设置。
必须检查	这是最安全的选项。StoreFront 尝试通过联系交付控制器上证书的 CDP 扩展中引用的 URL 来获取 CRL。如果 CRL 不可用，或者交付控制器上使用的证书已被吊销，StoreFront 将无法从交付控制器枚举。如果证书是私有的，URL 可以指向内部 Web 服务器；如果证书是由公共 CA 颁发的，则可以指向公共 Internet Web 服务器。
完整检查	StoreFront 尝试联系交付控制器证书的 CDP 扩展中发布的 URL。如果 StoreFront 无法从这些 URL 获取 CRL 副本，它仍然允许从交付控制器枚举资源。如果 StoreFront 成功获取 CRL 并且交付控制器的证书已被吊销，则 StoreFront 不会枚举资源。如果证书是私有的，URL 可以指向内部 Web 服务器；如果证书是由公共 CA 颁发的，则可以指向公共 Internet Web 服务器。
无网络访问	仅检查已本地导入到 StoreFront 服务器上的 Citrix Delivery Servers 证书存储中的 CRL。StoreFront 不会尝试联系 CDP 扩展中指定的任

设置	描述
	何 URL。如果 StoreFront 无法获取 CRL 的本地副本，它仍然允许从交付控制器枚举资源。如果 StoreFront 成功从 Citrix Delivery Servers 证书存储中获取 CRL 的本地副本，并且交付控制器的证书已被吊销，则 StoreFront 不会枚举资源。

例如：

```
$StoreVirtualPath = "/Citrix/Store"

$StoreObject = Get-STFStoreService -VirtualPath $StoreVirtualPath

Set-STFStoreFarmConfiguration -StoreService $StoreObject
-CertRevocationPolicy "MustCheck"
```

如果您有多个应用商店，请在所有应用商店上重复此过程。-CertRevocationPolicy 是一个应用商店级别的设置，它会影响为 $StoreVirtualPath 中指定的应用商店配置的所有交付控制器。

在 StoreFront 服务器上使用本地导入的 CRL

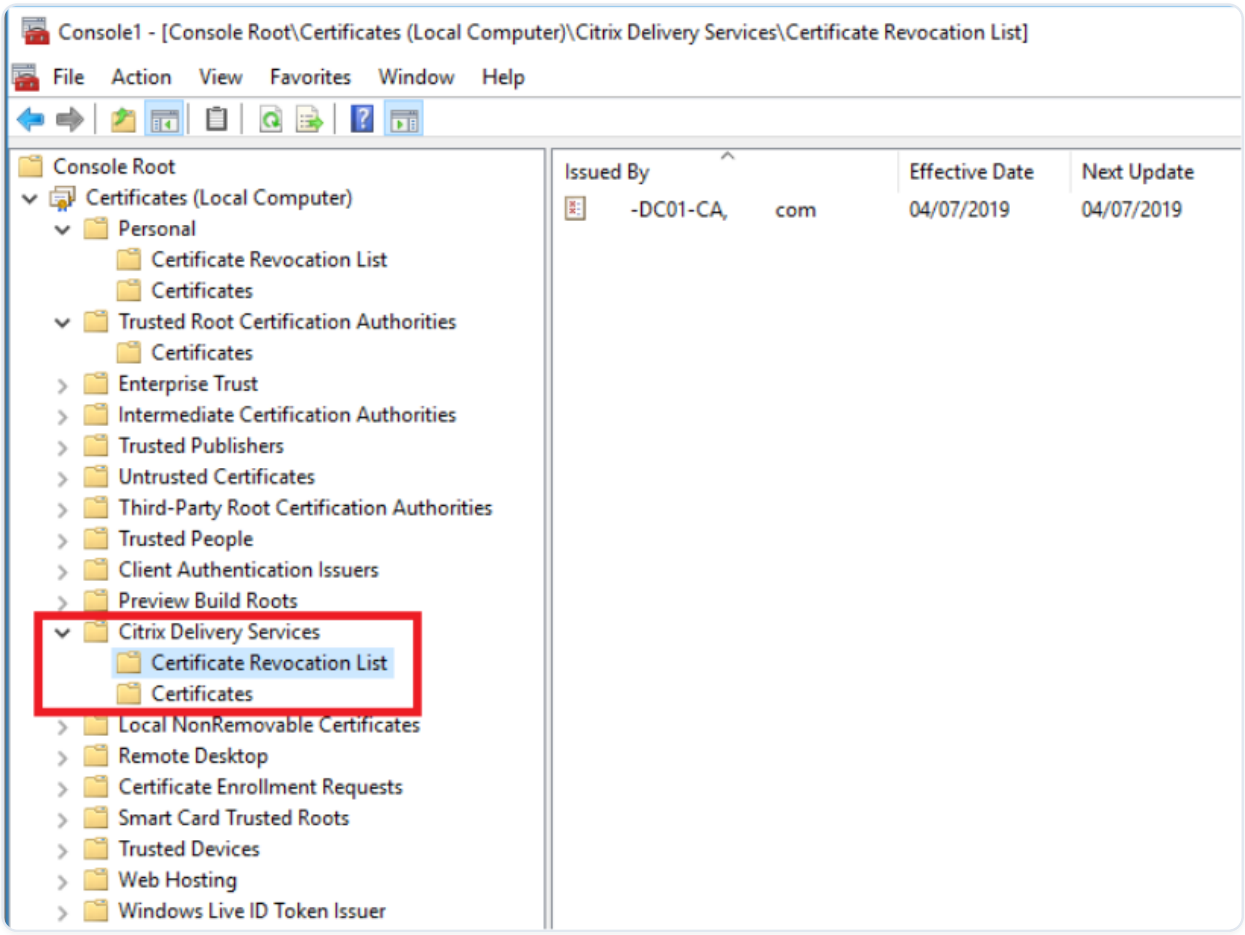
支持使用本地导入的 CRL，但 Citrix® 不建议这样做 因为：

- 在涉及多个 StoreFront 服务器组的大型企业部署中，它们难以管理和更新。
- 每次吊销证书时，在每个 StoreFront 服务器上手动更新 CRL，效率远低于在整个 Active Directory 域中使用 CDP 扩展和已发布的 CRL。

如果 -CertRevocationPolicy 设置为“NoNetworkAccess”，并且您有办法将 CRL 有效地分发到所有 StoreFront 服务器，则可以使用本地安装或更新的 CRL。

使用本地导入的 CLR

1. 将 CRL 复制到 StoreFront 服务器的桌面。如果 StoreFront 服务器是服务器组的一部分，请将其复制到组中的所有 StoreFront 服务器。
2. 打开 MMC 管理单元，并选择 **文件 > 添加/删除管理单元 > 证书 > 计算机帐户 > Citrix Delivery Services 证书存储**。
3. 右键单击并选择 **所有任务 > 导入**，然后浏览到 .CRL 文件并选择 **选择所有文件 > 打开 > 将所有证书放入以下存储 > Citrix 交付服务**。



通过 PowerShell 或命令行将 CRL 添加到 Citrix 交付服务证书存储

1. 登录 StoreFront 并将 .CRL 文件复制到当前 用户的桌面。
2. 打开 PowerShell ISE 并选择 **以管理员身份运行**。
3. 运行以下命令：

```
certutil -addstore "Citrix Delivery Services"
"$env:UserProfile\Desktop\Example-DC01-CA.crl"
```

如果成功，将返回以下内容：

```
Citrix Delivery Services

CRL "CN=Example-DC01-CA, DC=example, DC=com" added to store.

CertUtil: -addstore command completed successfully.

```
```
```

您可以使用此命令作为示例，通过脚本自动将 CRL 分发到部署中的所有 StoreFront 服务器。

使用交付控制器的 XML 身份验证

您可以配置 StoreFront 将用户身份验证委托给 Citrix Virtual Apps and Desktops 交付控制器。如果交付控制器上的证书已被吊销，用户将无法登录 StoreFront。这种行为是可取的，因为如果负责对 Active Directory 用户进行身份验证的 Citrix Virtual Apps and Desktops 交付控制器上的证书已被吊销，他们就不应该能够登录 StoreFront。

将用户身份验证委托给交付控制器

1. 按照上一节 配置存储以进行证书吊销检查 中所述，配置存储以进行证书吊销。
2. 按照 基于 XML 服务的身份验证 中所述的步骤，配置交付控制器以使用 HTTPS。

配置用于证书吊销检查的 XML 身份验证服务

仅当您在部署中使用 XML 身份验证时才需要这些步骤。

> **注意：**
>
> StoreFront 支持两种将存储映射到身份验证服务的模型。推荐的方法是存储与身份验证服务之间的一对一映射。在这种情况下，您必须对本节中的所有存储及其各自的身份验证服务执行这些步骤。
>
> 确保证书吊销模式在商店和身份验证服务中设置为相同的值。或者，如果所有商店的身份验证配置都相同，则可以将多个商店配置为共享单个身份验证服务。
>
> 身份验证服务 PowerShell cmdlet 没有与 **Set-STFStoreFarmConfiguration** 等效的 cmdlet，因此需要稍微不同的 PowerShell 方法。使用前面部分中描述的相同 (/zh-cn/storefront/2507-ltsr/secure/certificate-revocation-list-checking.html#certificate-revocation-policy-settings)。

1. 打开 PowerShell ISE 并选择 **以管理员身份运行**。

```
$SiteID = 1

$StoreVirtualPath = "/Citrix/Store"

$AuthVirtualPath = "/Citrix/StoreAuth"
```

2. 选择用于 XML 身份验证的商店服务、身份验证服务和交付控制器™。确保交付控制器已为商店配置。

```
$StoreObject = Get-STFStoreService -SiteId $SiteID -VirtualPath
$StoreVirtualPath

$FarmObject = Get-STFStoreFarm -StoreService $StoreObject -FarmName
"CVAD"

$AuthObject = Get-STFAuthenticationService -SiteID $SiteID -VirtualPath
$AuthVirtualPath
```

3. 修改身份验证服务的 CertRevocationPolicy 属性 直接。

```
$AuthObject.FarmsConfiguration.CertRevocationPolicy = "FullCheck"

$AuthObject.Save()

Enable-STFXmlServiceAuthentication -AuthenticationService $AuthObject
-Farm $FarmObject
```

4. 确认您已设置正确的证书吊销模式。

```
$AuthObject = Get-STFAuthenticationService -SiteID 1 -VirtualPath
$AuthVirtualPath

$AuthObject.FarmsConfiguration.CertRevocationPolicy
```

预期出现的 Windows 事件查看器错误

启用 CRL 检查时，错误会在 StoreFront 服务器上的 Windows 事件查看器中报告。

要打开事件查看器：

- 在 StoreFront 服务器上键入 **运行**。
- 键入 **eventvwr**，然后按 Enter。
- 在“应用程序和服务”中查找 Citrix Delivery Services 事件。

错误示例：商店无法联系具有已吊销证书的交付控制器

```
An SSL connection could not be established: An error occurred during SSL
crytography: Access is denied.



This message was reported from the Citrix XML Service at address https://
deliverycontrollerTLS.domain.com/scripts/wpnbr.dll.



The specified Citrix XML Service could not be contacted and has been
temporarily removed from the list of active services.
```

错误示例：如果用户因 XML 身份验证失败而无法登录，则来自 Web 版 Receiver 的错误

```
An unexpected response was received during the authentication process.



Citrix.DeliveryServicesClients.Authentication.Exceptions.ExplicitAuthentic
ationFailure,

Citrix.DeliveryServicesClients.Authentication, Version=3.20.0.0,

Culture=neutral, PublicKeyToken=null



General Authentication Failure



ExplicitResult.State: 5



AuthenticationControllerRequestUrl:

https://storefront.example.com/Citrix/StoreWeb/ExplicitAuth/LoginAttempt
```

```
ActionType: LoginAttempt



at

Citrix.Web.AuthControllers.Controllers.ExplicitAuthController.GetExplicitA
uthResult(ActionType

type, Dictionary`2 postParams)
```

ICA® 文件签名

StoreFront 提供数字签名 ICA 文件的选项，以便支持此功能的 Citrix Workspace 应用程序版本可以验证文件是否来自受信任的源。当 StoreFront 中启用文件签名时，用户启动应用程序时生成的 ICA 文件将使用 StoreFront 服务器个人证书存储中的证书进行签名。ICA 文件可以使用 StoreFront 服务器上运行的操作系统支持的任何哈希算法进行签名。不支持该功能或未配置 ICA 文件签名的客户端将忽略数字签名。如果签名过程失败，ICA 文件将在没有数字签名的情况下生成并发送到 Citrix Workspace 应用程序，其配置将决定是否接受未签名的文件。

要用于 StoreFront 的 ICA 文件签名，证书必须包含私钥并在允许的有效期内。如果证书包含密钥用法扩展，则必须允许该密钥用于数字签名。如果包含扩展密钥用法扩展，则必须将其设置为代码签名或服务器身份验证。

对于 ICA 文件签名，Citrix® 建议使用从公共证书颁发机构或您组织的私有证书颁发机构获取的代码签名证书或 SSL 签名证书。如果您无法从证书颁发机构获取合适的证书，您可以使用现有 SSL 证书（例如服务器证书），或者创建新的根证书颁发机构证书并将其分发给用户设备。

ICA 文件签名默认禁用。要启用 ICA 文件签名，您必须安装证书并配置存储以使用该证书。除非您还将适用于 Windows 的 Citrix Workspace 应用程序配置为需要证书，否则签名 ICA 文件无效，有关详细信息，请参阅 (/zh-cn/citrix-workspace-app-for-windows/security#ica-file-signing)。

> 注意：

> StoreFront 和 PowerShell 控制台不能同时打开。在使用 PowerShell 控制台管理 StoreFront 配置之前，请务必关闭 StoreFront 管理控制台。同样，在打开 StoreFront 控制台之前，请关闭所有 PowerShell 实例。

1. 在 StoreFront 服务器上，打开**管理计算机证书**。
2. 将您的证书添加到 **Citrix Delivery Services** 证书存储。
3. 打开证书，转到**详细信息**选项卡并记录指纹。
4. 使用 Set-STFStoreService PowerShell cmdlet 为存储启用签名：

```
$storeService = Get-STFStoreService

Set-STFStoreService $storeService -IcaFileSigning $true
-IcaFileSigningCertificateThumbprint [certificatethumbprint]
```

其中 是哈希算法生成的证书数据的摘要（或指纹）。

如果您想使用 SHA-1 以外的哈希算法，请根据需要添加参数 **-IcaFileSigningHashAlgorithm** 并将其设置为 sha256、sha384 或 sha512。

日志和分析

StoreFront 会生成许多日志文件和遥测数据。请参阅以下主题。

主题	描述
日志文件	StoreFront 会创建各种不同的日志文件，用于诊断目的。
事件日志	StoreFront 会将重要事件和错误写入 Windows 事件日志。
性能计数器	StoreFront 会记录性能计数器，您可以使用性能监视器查看这些计数器。
遥测	StoreFront 会将您的配置信息发送到 Citrix Cloud。
Citrix Workspace 应用程序分析	配置 Citrix Workspace 应用程序以将数据发送到 Citrix Analytics
Citrix 侦察兵	运行 Citrix Scout 以收集日志文件和其他系统信息，以便发送给支持部门

日志文件

安装日志

安装或卸载 StoreFront 时，StoreFront 安装程序会在 *C:\Windows\Temp\StoreFront* 目录中创建以下日志文件。文件名反映了创建它们的组件并包含时间戳。

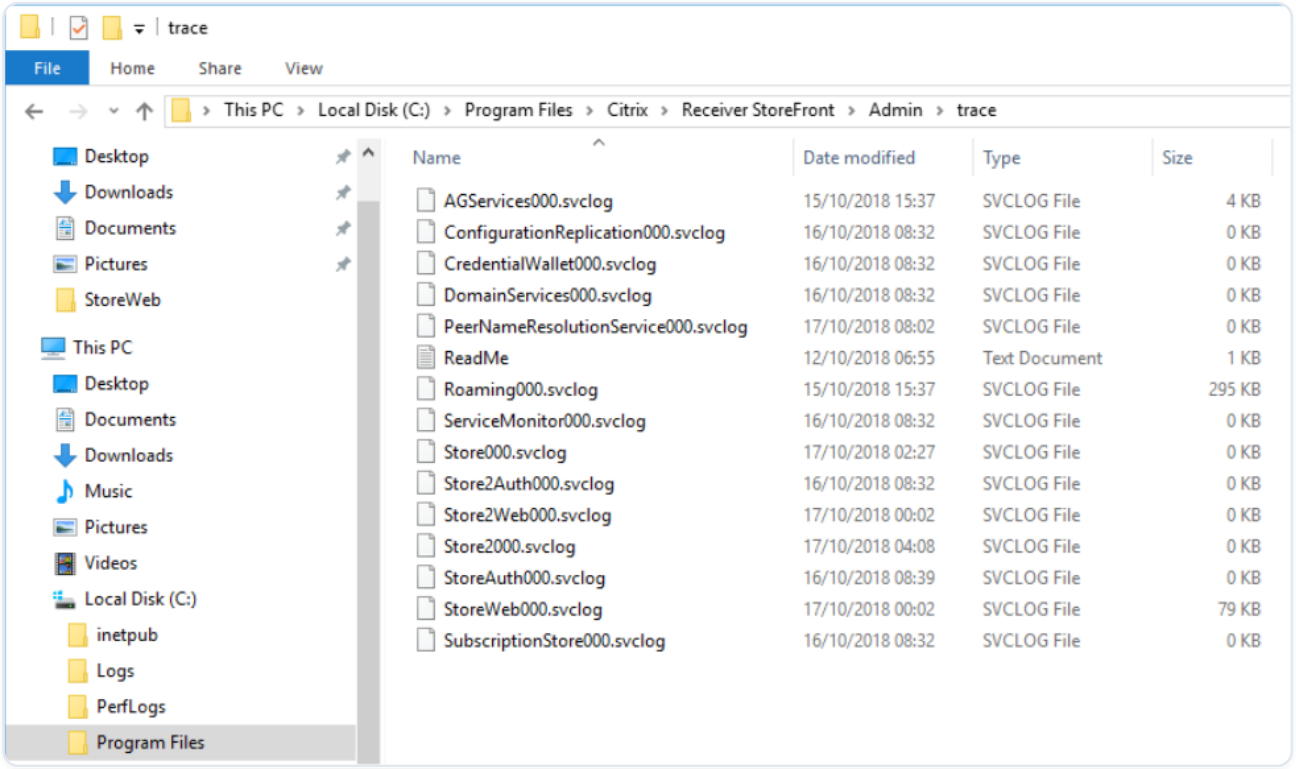
- Citrix-DeliveryServicesRoleManager-*.log—在交互式安装 StoreFront 时创建。
- Citrix-DeliveryServicesSetupConsole-*.log—在静默安装 StoreFront 以及以交互方式或静默方式卸载 StoreFront 时创建。
- CitrixMsi-CitrixStoreFront-x64-*.log—在以交互方式或静默方式安装和卸载 StoreFront 时创建。

PowerShell 和管理控制台日志

通过 PowerShell 或管理控制台进行的配置更改会记录在 `C:\Program Files\Citrix\Receiver StoreFront\Admin\logs` 中。日志文件名包含命令操作和主题，以及可用于区分命令序列的时间戳。

诊断日志记录

StoreFront 将诊断日志写入 `c:\Program Files\Citrix\Receiver StoreFront\admin\trace`



默认情况下，会记录 **Error**、**Warning** 和 **Info** 级别的消息。在大多数情况下，这包括足够的信息来诊断任何问题。

要使用 PowerShell 自定义日志记录，请运行 cmdlet `Set-STFDiagnostics`。

- StoreFront 为每个服务写入一个单独的日志文件。默认情况下，每个日志文件最大为 200MB，并且 StoreFront 在清除旧日志文件之前为每个服务写入最多五个日志文件。如果需要自定义写入的日志大小或数量，可以使用 `-FileSizeKb` 和 `-FileCount` 参数进行此操作。
- 要更改记录的详细信息级别，请使用参数 `-TraceLevel`。允许的值为 `Off`、`Error`、`Warning`、`Info` 或 `Verbose`。
- 要为所有服务设置日志记录参数，请使用参数 `-All`。您可以使用 `-Service [Service name]` 为单个服务自定义日志记录

详细日志记录

您可以启用额外的详细日志记录以用于故障排除。仅当 Citrix® 支持要求时才需要这样做。这可能会影响性能，因此故障排除完成后，您应将 `TraceLevel` 恢复为 `Info`。

要启用详细日志记录：

1. 使用具有本地管理员权限的帐户启动 Windows PowerShell
2. 输入命令：

   ```
   Set-STFDiagnostics -All -TraceLevel "Verbose" -confirm:$False
   ```

   这将为所有服务启用“详细”日志记录，而无需提示确认。输入此命令后，它会重新启动 StoreFront 服务。等待 PowerShell 提示符返回以验证服务是否已完成重新启动。在这些服务重新启动期间，用户将无法访问 StoreFront 服务器。
3. 重现问题以生成日志。
4. 将所有服务的日志记录级别设置回默认级别

   ```
   Set-STFDiagnostics -All -TraceLevel "Info" -confirm:$False
   ```

IIS 日志文件

默认情况下，IIS 会将每个请求的日志写入 `%SystemDrive%\inetpub\logs\LogFiles`。有关详细信息，请参阅 Microsoft 文档。

事件日志

StoreFront 支持对身份验证服务、应用商店和网站进行 Windows 事件日志记录。生成的任何事件都会写入 StoreFront 应用程序日志，可以使用事件查看器在 **应用程序和服务日志 > Citrix Delivery Services** 或 **Windows 日志 > 应用程序** 下查看。您可以通过编辑身份验证服务、应用商店和网站的配置文件来控制单个事件的重复日志条目数量。

日志限制

1. 使用文本编辑器打开身份验证服务、应用商店或 Receiver for Web 站点的 *web.config* 文件，这些文件通常分别位于 `C:\inetpub\wwwroot\Citrix\Authentication\`、`C:\inetpub\wwwroot\Citrix\storename\` 和 `C:\inetpub\wwwroot\Citrix\storenameWeb\` 目录中，其中 storename 是创建应用商店时指定的名称。

2. 在文件中找到以下元素。

   ```
   <logger duplicateInterval="00:01:00" duplicateLimit="10">
   ```

   默认情况下，StoreFront 配置为将重复日志条目的数量限制为每分钟 10 个。

3. 更改 duplicateInterval 属性的值，以设置监控重复日志条目的时间段（以小时、分钟和秒为单位）。使用 duplicateLimit 属性设置在指定时间间隔内必须记录的重复条目数量，以触发日志限制。

当触发日志限制时，会记录一条警告消息，指示后续相同的日志条目将被抑制。时间限制到期后，正常日志记录恢复，并记录一条信息性消息，指示重复日志条目不再被抑制。

性能计数器

StoreFront 写入多个性能计数器。要查看计数器值：

1. 从**开始**菜单中，打开**性能监视器**。这可以在**Windows 管理工具**文件夹下找到。
2. 在树状视图中，选择**监视工具** > **性能监视器**。
3. 在工具栏上选择 + 按钮 (**添加**)。
4. 选择您希望查看的计数器。它们可以在以 **Citrix®** 开头的类别下找到。

遥测

StoreFront 会将您的 StoreFront 配置和登录事件的遥测数据发送到 Citrix Cloud。这些数据通过本地内部部署 DDC 和许可证服务器或通过云连接器发送到 DaaS。有关详细信息，请参阅 Citrix Virtual Apps and Desktops 文档。

StoreFront™ 配置

用法

标头

字段	描述	示例
版本	许可证使用事件的版本	1.0
id	使用事件的唯一标识符	d4ce7919-5d80-44de-a8fa-102923fe0ead

字段	描述	示例
类型	CAS 用于识别云使用事件的事件类型	配置
st	在 Broker 中生成事件时的时间戳	2011-08-12T20:17:46.384Z
生产	使用事件的源产品和部署	OnPrem.StoreFront
prodVer	StoreFront 版本	3.30.0.0

负载

字段	描述	示例
serverName	StoreFront 运行所在服务的主机名	storefront-01.storefront.local
deploymentId	StoreFront 部署的唯一标识符	f47ac10b-58cc-4372-a567-0e02b2c3d479
installedWithCVAD	指示 StoreFront 是否与 CVAD 一同安装	否
cpuCores	CPU 核心的总数	4
cpuModel	运行 StoreFront 的 CPU	第12代 英特尔(R) 酷睿(TM) i7-1255U 1.70 GHz
ramGb	以 GB 为单位的 RAM 总量	16
numServersInGroup	服务器组中的服务器数量	3
商店	StoreFront Store 配置 JSON blob。Store 对象的数组。**某些值已打乱**	示例
rfWebSites	StoreFront 网站配置 JSON blob。RFWeb Config 对象的数组	示例

字段	描述	示例
网关	作为 JSON blob 的网关配置对象。网关对象的数组	示例
authServices	Auth 服务配置对象，以 JSON blob 形式。一个 Auth 服务对象数组。	示例
IsPiiScrambled	是	

字段 stores 的示例

```
[{
            "BaseUrl": "baseUrl",
            "StorePath": "/",
            "EnabledFeatures": 21 bit bitmap,
            "ResourceTypeFilteringEnabled": "disabled|
Citrix.MPS.Application;Citrix.MPS.Desktop",
            "DefaultRfWebSite": "/Citrix/StoreWeb",
            "GatewaysUsed": [
                "gatewayId"
            ],
            "VdaLogonDataProvider": "",
            "ResourceFeeds": [
                {
                    "FeedName": "<resourceFeedName>|scrambled",
                    "Type": "CVAD",
                    "LoadBalancingEnabled": true,
```

```
                }
            ],
            "AdvancedAggregation": {
                 "Enabled": true,
                 "GroupingCount": 1,
                 "ControllersPushIdenticalResources": true,
                 "LoadBalanced": true,
                 "AnyPrimaryFarms": true,
                 "AnyBackupFarms": true,
            }
}]
```

如果未找到 Stores，则它是一个空数组 。

字段 rfWebSites 的示例

```
[{
    "SiteId": "siteId",
    "BaseUrl": "baseUrl",
    "StorePath": "storePath",
    "UiExperienced": 0,
    "EnabledFeatures": 9 bit,
    "AuthMethodsEnabled": [
        "ad"
```

```
    ],
    "CanUsersDownloadApps": {
        "Enabled": true,
        "Windows": "exe",
        "MacOS": "dmg"
    },
    "WorkspaceControl": {
        "Enabled": true,
        "LogoffAction": 0,
        "AutoReconnectAtLogon": true,
        "ShowReconnectButton": true,
        "ShowDisconnectButton": true
    },
    "MultiClickTimeout": 1,
    "UiViews": [
        "apps",
        "desktops"
    ],
    "DefaultTab": 0,
}]
```

如果未找到 rfWebSites，则它是一个空数组 。

字段 gateways 的示例

```
[{

            "GatewayId": "gatewayId",

            "IsCloudGateway": true,

            "LoadBalancingSTAEnabled": true,

            "SessionReliabilityEnabled": true,

            "RequestTicketsFromTwoSTA": true,

            "Version": "1234",

            "LogonType": "domain",

            "SmartCardFallbackEnabled": true

}]
```

如果未找到 gateways，则它是一个空数组 。

字段 authServices 的示例

```
[{

    "SiteId": "SiteId",

    "Store": "StoreAuth",

    "AuthMethodsEnabled": [

        "ad"

    ],

    "PasswordChangeWhenExpired": 0,

    "PasswordRemindersForm": 1,

    "DelegateCredentialValidationToCitrix": true,
```

```
    "ValidatePasswordsOnDeliveryControllers": true

}]
```

如果未找到 auth 服务，则它是一个空数组 。

店面登录

用法

标头

字段	描述	示例
版本	许可证使用事件的版本	1.0
id	使用事件的唯一标识符	d4ce7919-5d80-44de-a8fa-102923fe0ead
类型	CAS 用于识别云使用事件的事件类型	登录
st	事件在 Broker 中生成时的时间戳	2011-08-12T20:17:46.384Z
生产	使用事件的原始产品和部署	OnPrem.StoreFront
prodVer	StoreFront 版本	3.30.0.0

有效负载

字段	描述	示例
用户	发起启动的用户。**该值已混淆**	fullName: C648FE671A44B3F7 **（始终混淆）** samName:C758LH671A44B3F7 **（始终混淆）**

字段	描述	示例
		upn: C7948FE671A44B3F7 **（始终混淆）** userLicenseId:C265FE671A44B3F7 **（始终混淆）** userSid: C097FE671A44B3F7 **（始终混淆）**
服务器名称	StoreFront 运行所在服务的主机名	storefront-01.storefront.local
loginMethodRfWeb	未使用	
loginMethodAuth	用户登录 StoreFront 所使用的方法	0
网关 URL	登录期间使用的 Netscaler Gateway 的 URL	netscaler-gateway.com
enabledFeatures	已启用功能的位掩码	12
userAgent	用于登录的客户端的 UserAgent	CitrixReceiver/ 22.11.0.19 Linux/ 5.17.15 X1Class CWACapable CWA/ 22.11.0.19
baseUrl	用户登录的商店的基本 URL	storefront-dev.storefront.dev
storePath	用户登录的商店路径	/Citrix/StoreWeb
apiUsed	指示客户端是否正在使用 Store API、Web API 或 PNAgent API	0

字段	描述	示例
deviceId	用于登录 StoreFront 的设备名称。**值已打乱**	john-doe
transactionId	用于对相关事件进行分组的标识符	773aba9e-5b91-4ef9-8782-c4afb75698e7

Citrix Workspace 应用程序分析

如果您有 Citrix Analytics，您可以配置 StoreFront，以便 Citrix Workspace app 将用户事件发送到 Citrix Analytics 进行处理。Citrix Analytics 聚合有关用户、应用程序、端点、网络和数据的指标，以提供对用户行为的全面洞察。要在 Citrix Analytics 文档中阅读有关此功能的信息，请参阅 使用 StoreFront 载入虚拟应用和桌面站点。

要配置此行为，请执行以下操作：

- 从 Citrix Analytics 下载配置文件。
- 使用 PowerShell 将 Citrix Analytics 数据导入到您的本地 StoreFront 部署中。

配置 StoreFront 后，当 Citrix Analytics 服务请求时，Citrix Workspace app 可以从 StoreFront 存储发送数据。

> **重要提示：**

> 您的 StoreFront 部署必须能够联系 Citrix API Services。请参阅 Analytics 网络要求。

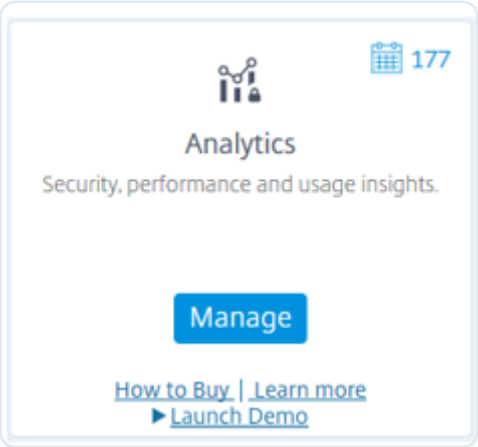
从 Citrix Analytics 下载配置文件

> **重要提示：**

> 初始配置需要包含敏感信息的配置文件。下载后请妥善保管该文件。请勿与组织外部的任何人共享此文件。配置完成后，您可以删除此文件。如果您需要在另一台计算机上再次重新应用配置，可以从 Citrix Analytics 服务管理控制台再次下载该文件。

1. 使用管理员帐户登录到监视器 (`https://citrix.cloud.com/`)。

2. 选择一个监视器客户。
3. 通过单击 **Manage** 打开 Citrix Analytics 服务管理控制台。



4. 在 Citrix Analytics 服务管理控制台中，选择 **Settings > Data Sources**。
5. 在 Virtual App and Desktops 卡中，选择 (⋮) 菜单图标，然后选择 **Connect StoreFront deployment**。
6. 在“连接 StoreFront 部署”页面上，选择“**下载文件**”以下载 *StoreFrontConfigurationFile.json* 文件。

示例配置文件

```
{

  "customerId": "<yourcloudcustomer>",

  "enablementService": " https://api.analytics.cloud.com /casvc/
<yourcloudcustomer>/ctxana/v1/cas/<yourcloudcustomer>/XenDesktop/
<deviceid>/dsconfigdata",

  "cwsServiceKey": "PFJTPn…….. T4=",

  "enablementServiceStatus": " https://api.analytics.cloud.com /casvc/
<yourcloudcustomer>/ctxana/v1/cas/storefront/config",

  "instanceId": "d98f21d0-56e0-11e9-ba52-5136d90862fe",

  "name": "CASSingleTenant"

}
```

其中

customerId 是当前监视客户的唯一 ID。

cwsServiceKey 是标识当前监视客户帐户的唯一密钥。

instanceID 是一个生成的 ID，用于签署（保护）从 Citrix Workspace 应用程序到 Citrix Analytics 的请求。如果您向监视器注册多个 StoreFront 服务器或服务器组，则每个服务器或服务器组都有一个唯一的 instanceID。

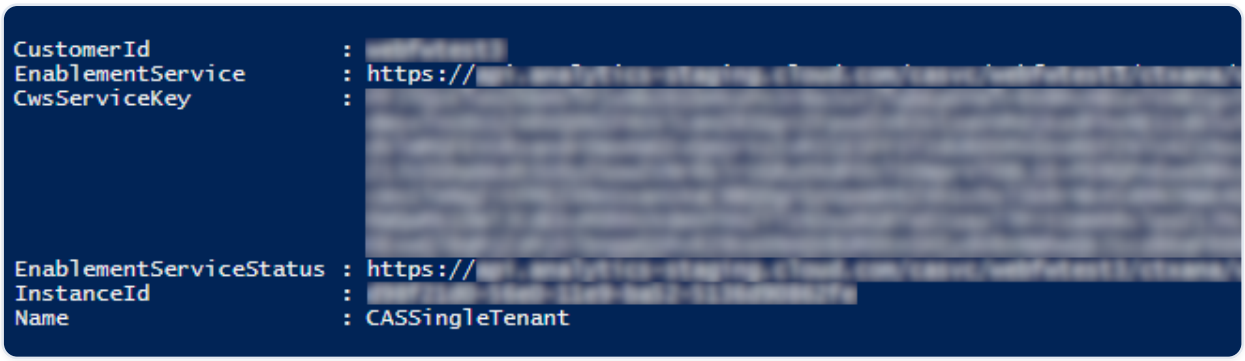
将 Citrix Analytics 数据导入您的 StoreFront™ 部署

1. 将 *StoreFrontConfigurationFile.json* 文件复制到本地 StoreFront 服务器（或 StoreFront 服务器组中的一台服务器）上的合适文件夹中。以下命令假定文件已保存到桌面。
2. 打开 PowerShell ISE 并选择“**以管理员身份运行**”。
3. 运行以下命令：

```
Import-STFCasConfiguration -Path
"$Env:UserProfile\Desktop\StoreFrontConfigurationFile.json"

Get-STFCasConfiguration
```

4. 此命令返回导入数据的副本，并在 PowerShell 控制台中显示。



注意：

安装在 Windows Server 2012 R2 上的本地 StoreFront 服务器可能需要手动安装 C++ 运行时软件组件，以便它们可以向 CAS 注册。如果在安装 Citrix Virtual Apps and Desktops 期间安装 StoreFront，则不需要此步骤，因为 CVAD 元安装程序已安装 C++ 运行时组件。如果仅使用 CitrixStoreFront-x64.exe 元安装程序安装 StoreFront 而没有 C++ 运行时，则在导入 CAS 配置文件后，它可能无法向监视器注册。

将 Citrix Analytics 数据传播到 StoreFront 服务器组

如果您正在 StoreFront 服务器组上执行这些操作，则必须将导入的 Citrix Analytics 数据传播到服务器组的所有成员。在单个 StoreFront 服务器部署中，此步骤不是必需的。

要传播数据，请使用以下方法之一：

- 使用 StoreFront 管理控制台。
- 使用 PowerShell 命令程序 **Publish-STFServerGroupConfiguration**。

检查 StoreFront 服务器组 ID

要检查您的部署是否已成功注册到 Citrix Analytics 服务，您可以使用 PowerShell 发现部署的 ServerGroupID。

1. 登录到您的 StoreFront 服务器，或服务器组中的一个 StoreFront 服务器。
2. 打开 PowerShell ISE 并选择**以管理员身份运行**。
3. 运行以下命令：

```
$WebConfigPath = "C:\Program Files\Citrix\Receiver
StoreFront\Framework\FrameworkData\Framework.xml"

$XMLObject = (Get-Content $WebConfigPath) -as [Xml]

$XMLObject.framework.properties.property
```

例如，这些命令会生成如下所示的输出：

```
name value

---- -----

ClusterId 8b8ff5c8-44ba-46e4-87f0-2df8cff31432

HostBaseUrl https://storefront.example.com/

SelectedIISWebSiteId 1

AdminConsoleOperationMode Full
```

停止从 StoreFront 向 Citrix Analytics 发送数据

1. 打开 PowerShell ISE 并选择**以管理员身份运行**。
2. 运行以下命令：

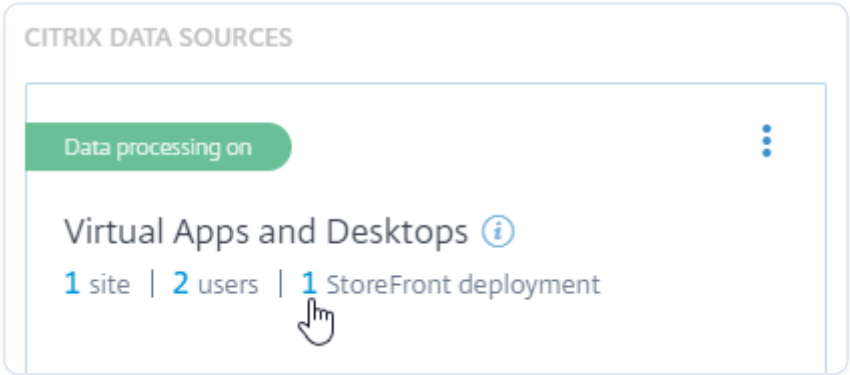
   ```
   Remove-STFCasConfiguration
   ```

   ```
   Get-STFCasConfiguration
   ```

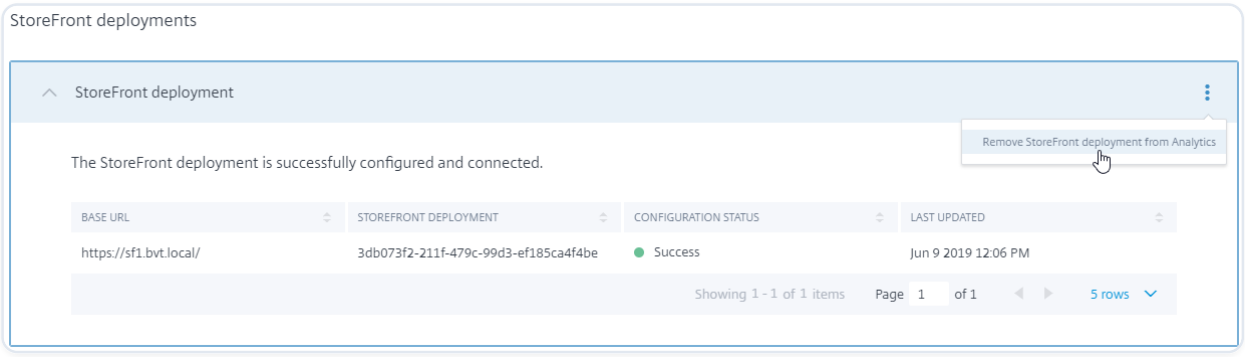
   如果以前导入的 Citrix Analytics 数据已成功删除，则 **Get-STFCasConfiguration** 不返回任何内容。
3. 如果您正在 StoreFront 服务器组上执行这些操作，请传播更改并从服务器组的所有成员中删除导入的 Citrix Analytics 数据。在服务器组中的一台服务器上，运行以下命令：

   ```
   Publish-STFServerGroupConfiguration
   ```
4. 在任何其他服务器组成员上，运行以下命令以确认 Citrix Analytics 配置已从组中的所有服务器成功删除：

   ```
   Get-STFCasConfiguration
   ```
5. 使用管理员帐户登录到监视器 (`https://citrix.cloud.com/`)。
6. 选择一个监视器客户。
7. 通过单击**管理**打开 Citrix Analytics 服务管理控制台。
8. 在 Citrix Analytics 服务管理控制台中，选择 **设置 > 数据源**。
9. 在“虚拟应用和桌面”卡中，选择 StoreFront 部署计数：



10. 通过引用其主机基本 URL 和 ServerGroupID 来识别要删除的 StoreFront 部署。
11. 在 (⋮) 菜单中，选择 **从 Analytics 中删除 StoreFront 部署**。



注意：

如果从服务器端而不是从 Citrix Analytics 中删除配置，则 StoreFront 部署条目将保留在 Citrix Analytics 中，但不会从 StoreFront 接收数据。如果仅从 Citrix Analytics 中删除配置，则 StoreFront 部署条目将在下一次应用程序池回收（通过 IIS 重置或每 24 小时自动执行）时重新添加。

配置 StoreFront 以使用 Web 代理联系监视器并向 Citrix Analytics 注册

如果 StoreFront 放置在 Web 代理后面的主机 Web 服务器上，则向 Citrix Analytics 注册将失败。如果 StoreFront 管理员在其 Citrix 部署中使用 HTTP 代理，则发往 Internet 的 StoreFront 流量必须先通过 Web 代理，然后才能到达云中的 Citrix Analytics。StoreFront 不会自动使用托管操作系统的代理设置；需要额外配置才能指示应用商店通过 Web 代理发送出站流量。您可以通过向应用商店 web.config 文件添加新部分来配置 `<system.net>` 代理配置。对 StoreFront 服务器上将用于向 Citrix Analytics 发送数据的每个应用商店执行此操作。

方法 1：通过 PowerShell 为一个或多个应用商店设置应用商店代理配置（推荐）

运行 PowerShell 脚本 Config-StoreProxy.ps1 可自动为一项或多项应用商店执行此过程，并自动插入有效的 XML 以配置 `<system.net>`。该脚本还会将应用商店 web.config 文件备份到当前用户的桌面，以便在必要时恢复未修改的 web.config 文件。

注意：

多次运行脚本可能会导致添加多个 `<system.net>` XML 副本。每个应用商店应只有一个 `<system.net>` 条目。添加多个副本会阻止应用商店代理配置正常工作。

1. 打开 PowerShell ISE 并选择 **以管理员身份运行**。
2. 设置 `$Stores = @("Store","Store2")` 以包含您希望使用 Web 代理配置的应用商店。

3. 指定以下任一选项：
   - 一个 IP 地址，或
   - 用于 Web 代理的 FQDN
4. 运行以下 PowerShell：

```
$Stores = @("Store","Store2")

$ProxyIP = "10.0.0.1"

$ProxyFQDN = "proxyserver.example.com"

$ProxyPort = 8888



# Set this for every Store using Stores array

function Set-StoreProxyServer() # Tested with both IP and FQDN

{

    [CmdletBinding()]

    param([Parameter(Mandatory=$true,ParameterSetName="ProxyIP")]
[Parameter(Mandatory=$true,ParameterSetName="ProxyFQDN")][array]
$Stores,

        [Parameter(Mandatory=$true,ParameterSetName="ProxyIP")][string]
$ProxyIP,

        [Parameter(Mandatory=$true,ParameterSetName="ProxyFQDN")]
[string]$ProxyFQDN,

        [Parameter(Mandatory=$true,ParameterSetName="ProxyIP")]
[Parameter(Mandatory=$true,ParameterSetName="ProxyFQDN")][int]
$ProxyPort)



    foreach($Store in $Stores)
```

```
    {

        Write-Host "Backing up the Store web.config file for store
$Store before making changes..." -ForegroundColor "Yellow"

        Write-Host "`n"



        if(!(Test-Path "$env:UserProfile\desktop\$Store\"))

        {

            Write-Host "Creating $env:UserProfile\desktop\$Store\
directory for backup..." -ForegroundColor "Yellow"

            New-Item -Path "$env:UserProfile\desktop\$Store\" -ItemType
"Directory" | Out-Null

            Write-Host "`n"

        }



        Write-Host "Copying c:\inetpub\wwwroot\Citrix\$Store\web.config
to $env:UserProfile\desktop\$Store\..." -ForegroundColor "Yellow"

        Copy-Item -Path "c:\inetpub\wwwroot\Citrix\$Store\web.config"
-Destination "$env:UserProfile\desktop\$Store\" -Force | Out-Null



        if(Test-Path "$env:UserProfile\desktop\$Store\web.config")

        {

            Write-Host "$env:UserProfile\desktop\$Store\web.config file
backed up" -ForegroundColor "Green"

        }

        else
```

```
        {

            Write-Host "$env:UserProfile\desktop\$Store\web.config file
NOT found!" -ForegroundColor "Red"

        }

        Write-Host "`n"



        Write-Host "Setting the proxy server to $ProxyAddress for Store
$Store..." -ForegroundColor "Yellow"

        Write-Host "`n"



        $StoreConfigPath = "c:\inetpub\wwwroot\Citrix\
$Store\web.config"

        $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]



        if([string]::IsNullOrEmpty($ProxyFQDN))

        {

            $ProxyServer = ("HTTP://$ProxyIP"+":"+$ProxyPort)

        }

        else

        {

            $ProxyServer = ("HTTP://$ProxyFQDN"+":"+$ProxyPort)

        }
```

```
        $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]



        # Create 3 elements

        $SystemNet = $XMLObject.CreateNode("element","system.net","")

        $DefaultProxy =
$XMLObject.CreateNode("element","defaultProxy","")

        $Proxy = $XMLObject.CreateNode("element","proxy","")

        $Proxy.SetAttribute("proxyaddress","$ProxyServer")

        $Proxy.SetAttribute("bypassonlocal","true")



        # Move back up the XML tree appending new child items in
reverse order

        $DefaultProxy.AppendChild($Proxy)

        $SystemNet.AppendChild($DefaultProxy)

        $XMLObject.configuration.AppendChild($SystemNet)



        # Save the modified XML document to disk

        $XMLObject.Save($StoreConfigPath)



        Write-Host "Getting the proxy configuration for c:
\inetpub\wwwroot\Citrix\$Store..." -ForegroundColor "Yellow"

        $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]

        $ConfiguredProxyServer =
$XMLObject.configuration.'system.net'.defaultProxy.proxy.proxyaddress |
```

```
Out-Null

        Write-Host ("Configured proxy server for Store $Store"+": "+
$ConfiguredProxyServer) -ForegroundColor "Green"

        Write-Host "`n"

    }

    Write-Host "Restarting IIS..." -ForegroundColor "Yellow"

    IISReset /RESTART

}



Set-StoreProxyServer -Stores $Stores -ProxyFQDN $ProxyFQDN -ProxyPort
$ProxyPort

# OR

Set-StoreProxyServer -Stores $Stores -ProxyIP $ProxyIP -ProxyPort
$ProxyPort
```

5. 检查 `C:\inetpub\wwwroot\Citrix\<Store>\web.config` 现在是否在文件末尾包含一个 `<system.net>` 部分。

```
        </dependentAssembly>

    </assemblyBinding>

</runtime>

<system.net>

    <defaultProxy>

    <proxy proxyaddress="HTTP://proxyserver.example.com:8888"
bypassonlocal="true" />

    </defaultProxy>
```

```
</system.net>

</configuration>
```

6. 按照 将 Citrix Analytics 数据导入您的 StoreFront 部署 中所述导入 Citrix Analytics 数据。

方法 2：手动将 `<system.net>` 部分添加到 Store 的 web.config 文件

这必须针对 StoreFront 服务器上将用于向 Citrix Analytics 发送数据的每个 Store 完成。

1. 备份 Store 的 web.config 文件并将其复制到 `C:\inetpub\wwwroot\Citrix\<Store>\web.config` 之外的另一个位置。
2. 使用您的代理设置修改以下 XML，可以使用 FQDN 和端口组合，也可以使用 IP 和端口组合。

   例如，使用 FQDN 和端口组合时，请使用以下 `<system.net>` 元素：

   ```
   <system.net>

       <defaultProxy>

       <proxy proxyaddress="HTTP://proxyserver.example.com:8888"
   bypassonlocal="true" />

       </defaultProxy>

   </system.net>
   ```

   例如，使用 IP 和端口组合时，请使用以下 `<system.net>` 元素：

   ```
   <system.net>

       <defaultProxy>

       <proxy proxyaddress="HTTP://10.0.0.1:8888" bypassonlocal="true" />

       </defaultProxy>

   </system.net>
   ```

3. 在 Store 的 web.config 文件末尾，在此处指示的位置插入相应的 `<system.net>` 元素：

```
<runtime>

<gcServer enabled="true" />

<assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">

    <dependentAssembly>

    <assemblyIdentity name="System.Web.MVC"
publicKeyToken="31BF3856AD364E35" culture="neutral" />

    <bindingRedirect oldVersion="0.0.0.0-5.0.0.0"
newVersion="5.0.0.0" />

    </dependentAssembly>

    <dependentAssembly>

    <assemblyIdentity name="Newtonsoft.Json"
publicKeyToken="30ad4fe6b2a6aeed" culture="neutral" />

    <bindingRedirect oldVersion="0.0.0.0-9.0.0.0"
newVersion="9.0.0.0" />

    </dependentAssembly>

</assemblyBinding>

</runtime>



Insert the <system.net> element here



</configuration>
```

4. 按照 将 Citrix Analytics 数据导入您的 StoreFront 部署 中所述导入 Citrix Analytics 数据。

弃用通知

本文中的公告旨在提前通知您即将淘汰的平台、Citrix 产品和功能，以便您能够及时做出业务决策。Citrix 会监控客户使用情况和反馈，以确定何时撤回这些产品和功能。公告可能会在后续版本中发生变化，并且可能不包括所有已弃用的功能。有关产品生命周期支持的详细信息，请参阅 Product Lifecycle Support Policy 文章。有关长期服务版本 (LTSR) 服务选项的信息，请参阅 < `<https://support.citrix.com/article/CTX205549>` >。

弃用

已弃用的项目不会立即移除。Citrix® 将继续支持它们，但它们将在未来的版本中移除。

项目	弃用版本	替代方案
XenApp® 服务（也称为 PNAgent）	2308	在 Workspace 应用程序中，使用应用商店 URL 而不是 XenApp 服务 URL 连接到应用商店

移除

已移除的项目要么已移除，要么不再受支持。

项目	弃用版本	删除版本	替代方案
Citrix 客户体验改善计划	2507	2507	
Windows 服务器 2016	2402	2407	在 Windows Server 2019 或更高版本上安装 StoreFront
对低于 4.8.0 版本的 Microsoft .NET Framework 的支持。	2407	2407	升级到 .NET Framework 4.8.0 或更高版本。（如果尚未安装，安装程序会自动安装 .NET

项目	弃用版本	删除版本	替代方案
			Framework 4.8.0。）
Internet Explorer 11 用于使用适用于 HTML5 的 Workspace 应用程序连接资源	2308	2308	要么使用受支持的 Web 浏览器，要么安装适用于 Windows 的 Citrix Workspace™ 应用程序。仍然可以使用 Internet Explorer 11 访问您的应用商店，但要启动资源，必须安装适用于 Windows 的 Citrix Workspace 应用程序。
XenApp 6.5 站点。	2308	2308	升级到最新版本的 Citrix Virtual Apps and Desktops。
对自助密码重置 (SSPR) 的支持	2203	2203	-
对 Citrix Virtual Apps and Desktops 与 Citrix Workspace 应用程序之间的 TLS 1.0 和 TLS 1.1 协议的支持。	3.14	2203	将 Citrix Receiver 升级到支持 TLS 1.2 的 Citrix Workspace 应用程序
在 Windows Server 2012 R2 上安装 StoreFront	2203	2203	在受支持的操作系统上安装 StoreFront。
支持低于 4.7.2 版本的 Microsoft .NET Framework。	2203	2203	升级到 .NET Framework 4.7.2 或更高版本。（如果尚未安装，安装程序会自动安装 .NET Framework 4.7.2。）

项目	弃用版本	删除版本	替代方案
移除以下已终止生命周期产品的 Delivery Controller 选项：VDI-in-a-Box 和 XenMobile（9.0 及更早版本）。	1903	1903	---
IE浏览器 9 和 10	1903	1903	---
支持用户访问桌面设备站点上的桌面	1811	1912	对于未加入域的用例，请使用 Desktop Lock。
Citrix 经典体验（“绿色气泡”用户界面）	3.12	1903	使用统一 UI
在 Windows Server 2012 和 Windows Server 2008 R2（包括 Service Pack）上安装 StoreFront。	3.12 LTSR	3.15	在受支持的操作系统上安装组件。
Citrix Online 集成 (Goto 产品) 集成	3.11	3.12	---
从 StoreFront 2.0、2.1、2.5 和 2.5.2 进行就地升级	3.9	1818	从这些版本之一升级到 3.12，然后再升级到更近的最新版本
在 32 位 (x86) 计算机上安装 StoreFront。	3.8	3.13	安装在受支持的 x64 操作系统上。

有关适用于 HTML5 的 Citrix Workspace 应用程序中的弃用信息，请参阅弃用页面。

第三方通知

StoreFront 可能包含根据以下条款获得许可的第三方软件组件。此列表是使用第三方软件于所列日期生成的。此列表可能随产品的特定版本而更改，并且可能不完整；它按“原样”提供。在适用法律允许的范围内，CITRIX 及其供应商对本列表或其准确性或完整性，或对使用或分发本列表所获得的任何结果，不作任何明示或暗示、法定或其他形式的陈述或保证。通过使用或分发本列表，您同意在任何情况下，CITRIX 均不对因使用或分发本列表而导致的任何特殊、直接、间接或后果性损害或任何其他损害承担责任。

卡斯尔温莎 3.3.0

版权所有 2004-2013 Castle Project - `<http://www.castleproject.org/>`

根据 Apache 许可证 2.0 版授权

Microsoft Unity 应用程序块 (Unity) 2.1

版权所有 © 2011 Microsoft Corporation。

根据 Microsoft 公共许可证 (MS-PL) 授权 `<https://msdn.microsoft.com/zh-cn/library/hh237493.aspx>`

Microsoft 模式与实践：Prism 2.2

版权所有 © 2010 Microsoft Corporation。

根据 Microsoft 公共许可证 (MS-PL) 授权。

Microsoft 模式与实践：通用服务定位器 1.0

版权所有 © Microsoft Corporation。

根据 Microsoft 公共许可证 (MS-PL) 授权

Microsoft .Net 参考源

版权所有 © Microsoft Corporation。根据 MIT 许可证授权。

Microsoft.IdentityModel.JsonWebTokens

版权所有 © Microsoft Corporation。根据 MIT 许可证授权。

Microsoft.IdentityModel.Logging

版权所有 © Microsoft Corporation。根据 MIT 许可证授权。

Microsoft.IdentityModel.Tokens

版权所有 © Microsoft Corporation。根据 MIT 许可证授权。

ManagedEsent 版本 1.9.4

版权所有 © Microsoft Corporation。

根据 Microsoft 公共许可证 (MS-PL) 授权。

jQuery UI - v1.10.4 - 2014-03-12

`<http://jqueryui.com/>`

版权所有 2014 jQuery Foundation 及其他贡献者；MIT 授权

jQuery JavaScript 库 v1.12.4

`<http://jquery.com/>`

包含 Sizzle.js

`<http://sizzlejs.com/>`

版权所有 jQuery Foundation 及其他贡献者

在 MIT 许可下发布

`<http://jquery.org/license>`

日期：2016-05-20T17:17Z

jQuery jScrollPane v2.0.0beta11

jScrollPane - v2.0.0beta11 - 2011-07-04

版权所有 (c) 2010 Kelvin Luck

在 MIT 和 GPL 许可下双重授权。

jquery.contextmenu.js

用于上下文菜单的 jQuery 插件

版权所有 (c) 2008 Matt Kruse (javascripttoolbox.com)

在 MIT 和 GPL 许可下双重授权。

Hammer.JS 的 jQuery 插件 - v1.0.0 - 2014-01-02

`<http://eightmedia.github.com/hammer.js>`

版权所有 (c) 2014 Jorik Tangelder <j.tangelder@gmail.com>；

在 MIT 许可下授权

jQuery MouseWheel

版权所有 (c) 2011 Brandon Aaron (http://brandonaaron.net)

根据 MIT 许可证 (LICENSE.txt) 授权。

WPF 工具包 3.5

WPF Toolkit 版权所有 (c) 2006-2014 Microsoft

MS-PL 许可证

扩展 WPF 工具包 3.0

版权所有 (C) 2007-2013 Xceed Software Inc.

本程序根据 Microsoft 公共许可证 (Ms-PL) 的条款提供给您。

如需更多功能、控件和快速专业支持，请在 `<http://xceed.com/wpf_toolkit>` 获取 Plus Edition。

保持关注：在 Twitter 上关注 @datagrid。

WiX 工具集

版权所有 (c) .NET Foundation 和贡献者。Microsoft 互惠许可证 (Ms-RL)

CLR 安全

版权所有 (c) Microsoft Corporation。Microsoft 有限许可许可证 (MS-LPL)

堆栈交换 Redis 1.1

StackExchange.Redis.StrongName 1.1 `<https://stackexchange.github.io/StackExchange.Redis>` 版权所有 (c) 2014 Stack Exchange

根据 MIT 许可证授权

牛顿软件 JSON

版权所有 (c) 2007 James Newton-King

根据 MIT 许可证授权。

jQuery JavaScript 库 v3.7.1

(c) OpenJS Foundation 和其他贡献者

根据 MIT 许可证发布

`<https://jquery.org/license>`

jQuery UI - v1.13.2 - 2022-07-14

`<http://jqueryui.com>`

版权所有 jQuery Foundation 和其他贡献者；根据 MIT 授权

Hammer.JS - v2.0.4 - 2014-09-28

Hammer.JS - v2.0.8 - 2016-04-23

`<http://hammerjs.github.io/>`

版权所有 (c) 2016 Jorik Tangelder;

根据 MIT 许可证授权

VelocityJS.org (1.5.0)

velocity-animate 著作权归 Julian Shapiro 所有，2014-2017。

根据 MIT 许可证授权。有关详细信息，请参阅项目根目录中的 LICENSE 文件。

slick.js - 1.8.0

MIT 许可证 (MIT)

版权所有 (c) 2013-2016

jQuery UI 触控潘趣 0.2.3

版权所有 2011–2014, Dave Furfero

根据 MIT 或 GPL 版本 2 许可证双重授权。

Microsoft.WebApi.Collection

MIT 许可证 (MIT)

版权所有 (c) Microsoft Corporation

波利

版权所有 (c) 2015-2024, App vNext

根据 BSD 3 条款许可证授权

Polly.Core

版权所有 (c) 2015-2024, App vNext

采用 BSD 3-Clause 许可证授权

Microsoft.Security.Crypto

MIT 许可证 (MIT)

版权所有 (c) Microsoft Corporation

微软 .NET 8

MIT 许可证 (MIT)

版权所有 (c) .NET Foundation 和贡献者

附录：引用的许可证

MIT 许可证


```
Permission is hereby granted, free of charge, to any person obtaining a
copy

of this software and associated documentation files (the "Software"), to
deal

in the Software without restriction, including without limitation the
rights

to use, copy, modify, merge, publish, distribute, sublicense, and/or sell

copies of the Software, and to permit persons to whom the Software is

furnished to do so, subject to the following conditions:



The above copyright notice and this permission notice shall be included in

all copies or substantial portions of the Software.



THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR

IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,

FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL
THE
```

```
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER

LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING
FROM,

OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN

THE SOFTWARE.
```

Apache 许可证，版本 2.0

```
                                 Apache License

                           Version 2.0, January 2004

                        http://www.apache.org/licenses/



TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION


1. Definitions.


   "License" shall mean the terms and conditions for use, reproduction,

   and distribution as defined by Sections 1 through 9 of this document.


   "Licensor" shall mean the copyright owner or entity authorized by

   the copyright owner that is granting the License.


   "Legal Entity" shall mean the union of the acting entity and all
```

other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work

(an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise

designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You

institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of

the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or

for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions

of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only

on Your own behalf and on Your sole responsibility, not on behalf

of any other Contributor, and only if You agree to indemnify,

defend, and hold each Contributor harmless for any liability

incurred by, or claims asserted against, such Contributor by reason

of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

Microsoft 公共许可证 (MS-PL)

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions

The terms “reproduce,” “reproduction,” “derivative works,” and “distribution” have the

same meaning here as under U.S. copyright law.

A “contribution” is the original software, or any additions or changes to the software.

A “contributor” is any person that distributes its contribution under this license.

“Licensed patents” are a contributor’s patent claims that read directly

on its contribution.

2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations

(A) No Trademark License- This license does not grant you rights to use any contributors’ name, logo, or trademarks.

(B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

(C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

(E) The software is licensed “as-is.” You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

BSD 3-Clause 许可证

Redistribution and use in source and binary forms, with or without

modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this

list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice,

this list of conditions and the following disclaimer in the documentation

and/or other materials provided with the distribution.

3. Neither the name of the copyright holder nor the names of its

```
   contributors may be used to endorse or promote products derived from

   this software without specific prior written permission.



THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS
IS"

AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE

IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE

DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE
LIABLE

FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL

DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR

SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER

CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY,

OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
USE

OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

Microsoft 互惠许可证 (Ms-RL)

```
This license governs use of the accompanying software. If you use the
software, you accept this license. If you do not accept the license, do
not use the software.



1. Definitions

The terms "reproduce," "reproduction," "derivative works," and
```

"distribution" have the same meaning here as under U.S. copyright law.

A "contribution" is the original software, or any additions or changes to the software.

A "contributor" is any person that distributes its contribution under this license.

"Licensed patents" are a contributor's patent claims that read directly on its contribution.

2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations

(A) Reciprocal Grants- For any file you distribute that contains code from the software (in source code or binary format), you must provide recipients the source code to that file along with a copy of this license, which license will govern that file. You may license other files that are entirely your own work and do not contain code from the software under any terms you choose.

(B) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

(C) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

(D) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(E) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

(F) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees, or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.