# Citrix Workspace 应用程序

# Contents



# Citrix Workspace 应用程序

April 25, 2024

## 关于 Citrix Workspace 应用程序

Citrix Workspace 应用程序提供对最终用户保持工作效率所需的所有资源的即时、安全和无缝访问。Citrix Workspace 应用程序包括访问虚拟桌面、虚拟应用程序、Web 和 SaaS 应用程序，以及嵌入式浏览和单点登录（从任何位置和任何设备）等功能。

Citrix Workspace 应用程序是一种客户端应用程序，可以在云端和本地环境的设备上部署。它建立在以前称为 Citrix Receiver 的功能之上，包括 HDX、Citrix Gateway 插件和 Secure Private Access 等 Citrix 客户端技术。

客户端应用程序已经过优化，可在所有客户端操作系统上运行，例如 Windows、macOS、Linux、iOS 和 Android。也可以通过浏览器进行访问。有关支持的浏览器的更多详细信息，请参阅 Workspace Browser 兼容性。

由 Citrix 协议和 HDX（高清体验）提供支持的 Citrix Workspace 应用程序提供高性能的虚拟应用程序和桌面会话。它经过增强，可提供安全的登录和 Internet 浏览体验、应用程序和桌面的轻松管理、高级搜索功能等。

> 注意：
>
> 应用程序用户界面可能因资源部署而异，即在云端（利用 Workspace 平台）还是在本地（利用 StoreFront 平台）。

有关 Citrix Workspace 应用程序中提供的功能的信息，请参阅 Citrix Workspace app feature matrix（Citrix Workspace 应用程序功能列表）。

有关 LTSR 与当前版本之间的差别的信息，请参阅 Lifecycle Milestones for Citrix Workspace app（Citrix Workspace 应用程序的生命周期里程碑）。

Citrix Workspace 应用程序适用于以下操作系统：

- 适用于 Android 的 Citrix Workspace 应用程序
- 适用于 ChromeOS 的 Citrix Workspace 应用程序
- 适用于 HTML5 的 Citrix Workspace 应用程序
- 适用于 iOS 的 Citrix Workspace 应用程序
- 适用于 Linux 的 Citrix Workspace 应用程序
- 适用于 Mac 的 Citrix Workspace 应用程序
- 适用于 Windows 的 Citrix Workspace 应用程序
- 适用于 Windows（应用商店版本）的 Citrix Workspace 应用程序

> 重要
>
> 为 **Citrix Workspace** 应用程序更新收集的数据：
>
> 对于连接到 Internet 的设备，Citrix Workspace 应用程序可能会在不另行通知的情况下检查是否有可供下载和安装到设备上的更新，并告知用户其可用性。发生这种情况时，除非在某些司法管辖区 IP 地址可能被视为个人身份信息，否则只会传输非个人身份信息。

## 使用 **Global App Configuration Service** 配置 **Citrix Workspace** 应用程序

Global App Configuration Service 提供了一个集中的界面，用于为最终用户配置 Citrix Workspace 应用程序设置。可以从单个界面为云应用商店和本地应用商店配置设置。这些设置同时适用于托管设备和非托管设备 (BYOD)。有关详细信息，请参阅 Global App Configuration Service。

### 语言支持

Citrix Workspace 应用程序已调整为在英语以外的其他语言中适用。本部分内容列出了最新版本的 Citrix Workspace 应用程序中支持的语言。

下表列出了各种操作系统或平台上的 Citrix Workspace 应用程序支持的语言。☑ 表示应用程序可在该特定语言中使用。

| 语言 | Android | ChromeOS | HTML5 | iOS | Linux | macOS | Windows | Windows 应用商店 |
|---|---|---|---|---|---|---|---|---|
| 英语 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 丹麦语 | ☑ | | | ☑ | | | | |
| 荷兰语 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 法语 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 德语 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 意大利语 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 日语 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 韩语 | ☑ | ☑ | ☑ | ☑ | ☑ | | ☑ | ☑ |
| 葡萄牙语 (巴西) | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 俄语 | | ☑ | ☑ | | ☑ | | ☑ | ☑ |
| 简体中文 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |
| 西班牙语 | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ | ☑ |

| 语言 | Android | ChromeOS HTML5 | iOS | Linux | macOS | Windows | Windows 应用商店 |
|---|---|---|---|---|---|---|---|
| 瑞典语 | ☑ | | ☑ | | | | |
| 繁体中文 | | ☑ | ☑ | | | ☑ | ☑ |

## 功能标志

本文讨论了功能标志管理以及支持功能标志的各种 Citrix Workspace 应用程序。

### 功能标志管理

如果生产环境中的 Citrix Workspace 应用程序出现问题，我们可以在 Citrix Workspace 应用程序中动态禁用受影响的功能，即使该功能已发布亦如此。为此，我们将使用功能标志以及名为 LaunchDarkly 的第三方服务。不需要做任何配置即可启用传输到 LaunchDarkly 的流量，但当您配置了阻止出站流量的防火墙或代理时除外。在这种情况下，您根据策略要求通过特定 URL 或 IP 地址启用传输到 LaunchDarkly 的流量。

下表列出了支持功能标志的各种应用程序以及在这些应用程序中引入了功能标志的发行版本。

| 应用程序 | 功能标志支持 | 版本 | 文档 |
|---|---|---|---|
| 适用于 Android 的 Citrix Workspace 应用程序 | 是 | 10.7.5 | 适用于 Android 的 Citrix Workspace 应用程序的功能标志管理 |
| 适用于 ChromeOS 的 Citrix Workspace 应用程序 | 是 | 1908 | 适用于 ChromeOS 的 Citrix Workspace 应用程序的功能标志管理 |
| 适用于 HTML5 的 Citrix Workspace 应用程序 | 是 | 1908 | 适用于 HTML5 的 Citrix Workspace 应用程序的功能标志管理 |
| 适用于 iOS 的 Citrix Workspace 应用程序 | 是 | 10.4.10 | 适用于 iOS 的 Citrix Workspace 应用程序的功能标志管理 |
| 适用于 Linux 的 Citrix Workspace 应用程序 | 是 | 2109 | 适用于 Linux 的 Citrix Workspace 应用程序的功能标志管理 |

| 应用程序 | 功能标志支持 | 版本 | 文档 |
| --- | --- | --- | --- |
| 适用于 Mac 的 Citrix Workspace 应用程序 | 是 | 2010 | 适用于 Mac 的 Citrix Workspace 应用程序的功能标志管理 |
| 适用于 Windows 的 Citrix Workspace 应用程序 | 是 | 2012 | 适用于 Windows 的 Citrix Workspace 应用程序的功能标志管理 |

### 关于 **Citrix Receiver** 的重要更新

自 2018 年 8 月起，Citrix Workspace 应用程序取代了 Citrix Receiver。虽然您仍然可以下载较旧版本的 Citrix Receiver，但已经发布了 Citrix Workspace 应用程序的新增功能和增强功能。

Citrix Workspace 应用程序是 Citrix 的新客户端，其工作方式与 Citrix Receiver 类似，并且完全向后兼容贵组织的 Citrix 基础结构。Citrix Workspace 应用程序具有 Citrix Receiver 的全部功能以及根据贵组织的 Citrix 部署新增的功能。

Citrix Workspace 应用程序构建于 Citrix Receiver 技术之上，并且完全向后兼容所有 Citrix 解决方案。

有关详细信息，请访问 Workspace 应用程序常见问题解答页面。

## **Citrix Workspace Web** 扩展程序

April 25, 2024

使用 Citrix Workspace Web 扩展，您无需 `.ica` 文件即可在任意位置启动 Workspace 应用程序，从而使您的体验更安全、更可靠。使用浏览器扩展程序打开应用程序可将您的所有应用程序和桌面保存在一个位置，这样您就能够轻松跟踪工作并使桌面摆脱混乱。Citrix Workspace Web 扩展还提供了屏幕截图 App Protection 和无缝服务连续性的好处。

### 安装 **Citrix Workspace Web** 扩展

要安装 Citrix Workspace Web 扩展，请执行以下步骤：

1. 导航到您的首选浏览器的 Web 应用商店：
    - Chrome 网上应用店
    - Microsoft Edge 加载项
    - Mac 应用商店

2. 通过您的首选浏览器应用商店添加并确认安装 Citrix Workspace Web 扩展。
3. 如果需要，请确认要添加 Web 扩展程序的弹出消息。
4. （可选）选择浏览器右上角的拼图块以固定浏览器以便于访问。
5. 选择 **Add extension**（添加扩展程序）。
6. 选择图钉图标以固定扩展程序。

Citrix Workspace Web 扩展现已安装。

有关 Citrix Workspace Web 扩展的详细信息，请参阅 Citrix Workspace web extension blog（Citrix Workspace Web 扩展博客）。

### 在 **Citrix Workspace** 实例中打开 **SaaS** 应用程序

如果您的 Workspace 实例中尚未启用 Citrix Workspace Web 扩展程序，请按照以下步骤进行操作：

1. 在 Workspace 窗口中选择您的帐户配置文件。
2. 从配置文件菜单中选择 **Advanced**（高级）。
3. 在 **Apps and Desktops Launch Preference**（应用程序和桌面启动首选项）窗口中选择 **Use Web Browser**（使用 Web 浏览器）。
4. 在弹出窗口中确认 **Open Citrix Workspace Launcher**（打开 Citrix Workspace 启动器）。

现在，您的 SaaS 应用程序将在 Citrix Workspace 应用程序窗口中打开。

### **Citrix Workspace** 应用程序功能列表

Citrix Workspace 应用程序提供跨不同平台或操作系统分布的许多功能。通过此功能列表，您可以清楚地了解这些功能在不同平台上的可用性。

具有支持的 Web 浏览器和 Internet 连接的任何计算机都可以访问 Citrix Workspace Web 扩展。为使用 Citrix Workspace Web 扩展的所有特性和功能，支持以下浏览器类型：

| 浏览器名称 | 版本 |
| --- | --- |
| Google Chrome | 最新版本 |
| Microsoft Edge | 最新版本 |
| Apple Safari | 最新版本 |

# App Protection

May 30, 2024

App Protection 是 Citrix Workspace 应用程序的一项功能，可在使用 Citrix Virtual Apps and Desktops 的已发布资源时提供增强的安全性。与 StoreFront 和 Workspace 结合使用的本地 Citrix Virtual Apps and Desktops 部署和 Citrix DaaS（以前称为 Citrix Virtual Apps and Desktops 服务）支持 App Protection 功能。这意味着所有云环境、本地环境和混合环境都支持 App Protection。当您通过 ADC Gateway 连接到 StoreFront 或 Workspace 时，还支持 App Protection。

两个策略为 Citrix HDX 会话提供了反键盘记录和防屏幕捕获功能。适用于 Windows 的 Citrix Workspace 应用程序 2203.1 LTSR、适用于 Mac 的 Citrix Workspace 应用程序 2001 或适用于 Linux 的 Citrix Workspace 应用程序 2108 的最低版本随附的策略可帮助保护数据免受键盘记录器和屏幕抓取工具的影响。

启用反键盘记录时：

- 键盘记录器看到加密的击键。
- 仅当受保护的窗口处于焦点时，此功能才处于活动状态。

启用了防屏幕捕获时：

- 在 Windows OS 和 macOS 上捕获屏幕时，只有受保护窗口的内容为空白。当受保护的窗口未最小化时，此功能处于活动状态。在 Linux 操作系统中，整个捕获内容是空白的。无论受保护的窗口是否已最小化，此功能均处于活动状态。
- 使用 Windows 操作系统中的 **Print Screen** 按钮创建屏幕截图时，数据不会复制到剪贴板。要使用 **Print Screen** 按钮创建屏幕截图，请最小化所有受保护的应用程序。

可以通过 PowerShell 和 Web Studio 配置策略。有关详细信息，请参阅为虚拟应用程序和桌面配置 App Protection。

购买此功能后，请确保启用 App Protection 许可证。

> 免责声明：
>
> App Protection 策略通过筛选对基础操作系统所需功能的访问（捕获屏幕或键盘按下所需的特定 API 调用）来运行。执行此操作意味着 App Protection 策略甚至可以针对自定义的专用黑客工具提供保护。但是，随着操作系统的发展，捕获屏幕和记录键盘的新方法可能会出现。虽然我们会继续识别和解决这些问题，但我们无法保证在特定配置和部署中提供充足的保护。
>
> Citrix App Protection 策略可与包括 ICA 文件在内的基本操作系统组件一起高效运行。如果检测到有意篡改或修改基本组件，Citrix 可能不会提供支持，以提供所应用策略的完整性。

### 检查是否已安装 **App Protection**

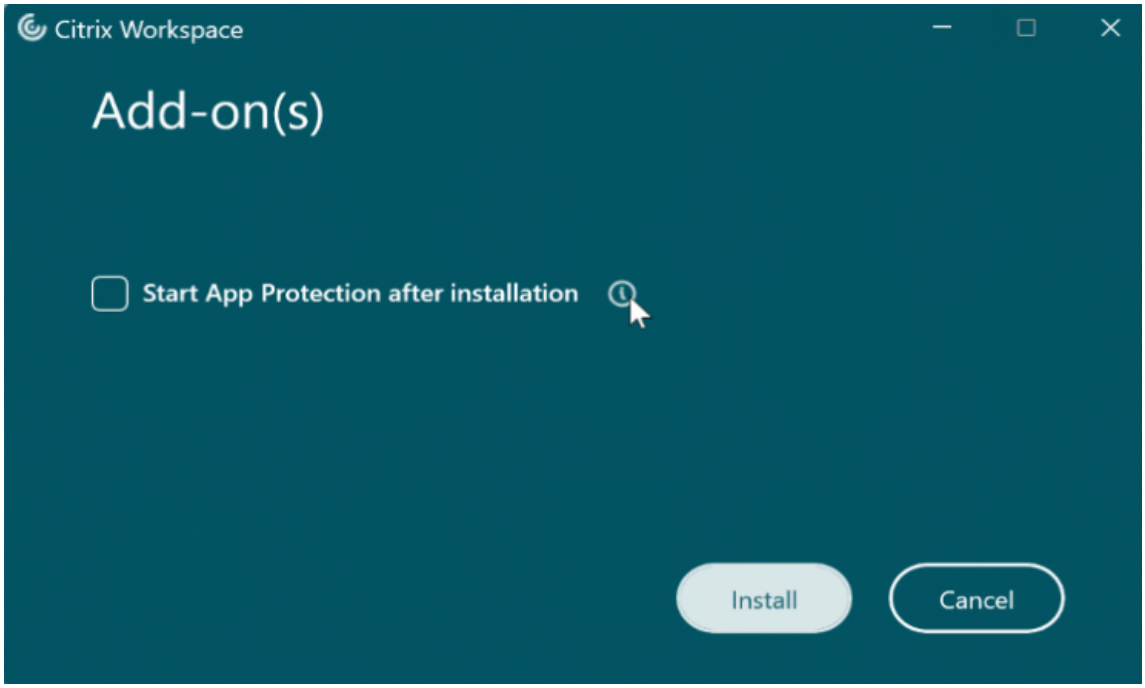
适用于 **Windows** 的 **Citrix Workspace** 应用程序

自 Citrix Workspace 应用程序版本 2212 起，默认安装 App Protection。但是，该组件可能处于活动状态，也可能处于休眠状态，具体取决于用户是否选择了安装后启动 **App Protection** 复选框。

- 对于 2311 之前的 Citrix Workspace 应用程序版本：

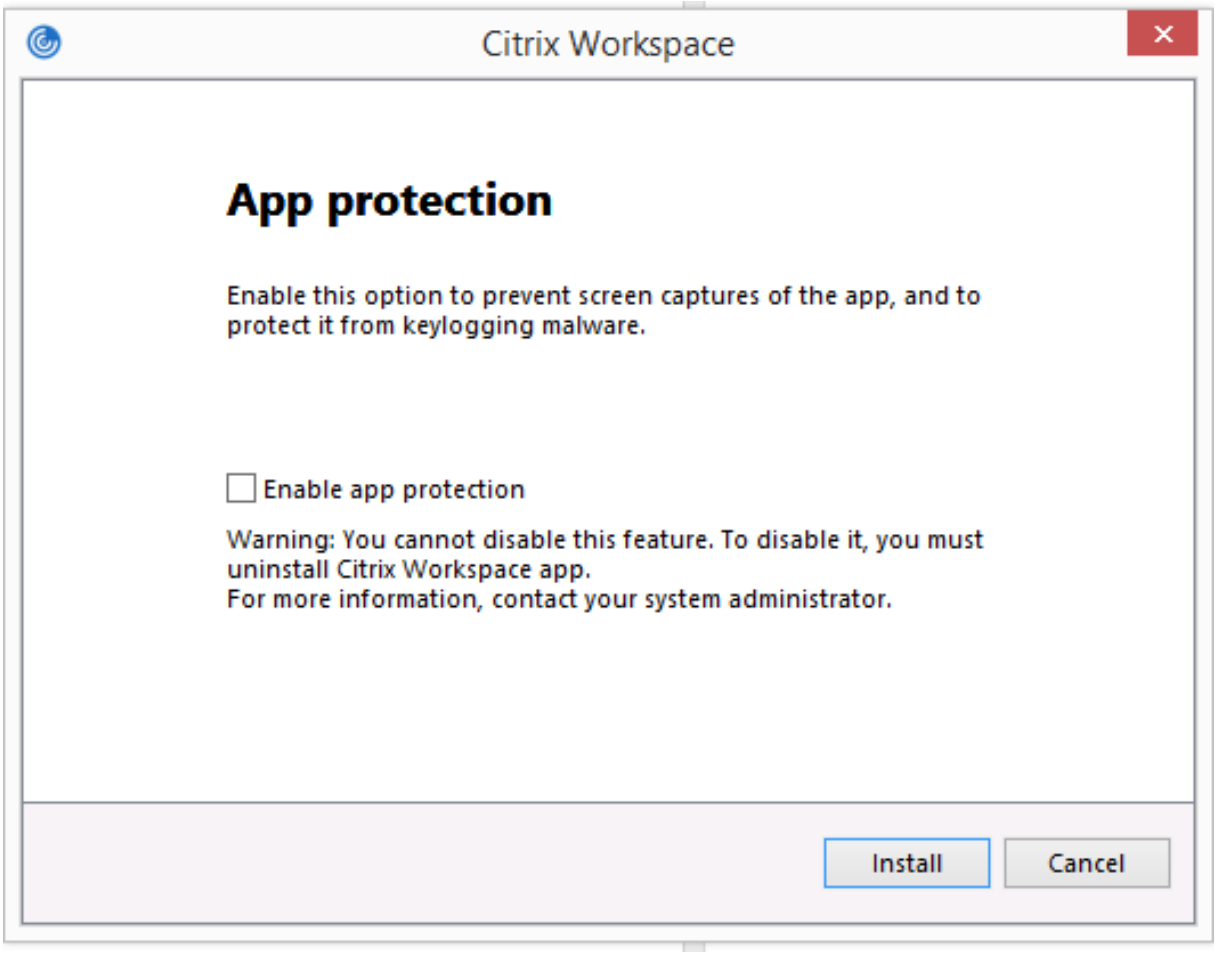

- 自 Citrix Workspace 应用程序版本 2311 起：




对于 2212 之前的 Citrix Workspace 应用程序版本，仅当安装 Citrix Workspace 应用程序时选中了启用 **App Protection** 复选框时，App Protection 才会安装并处于活动状态。



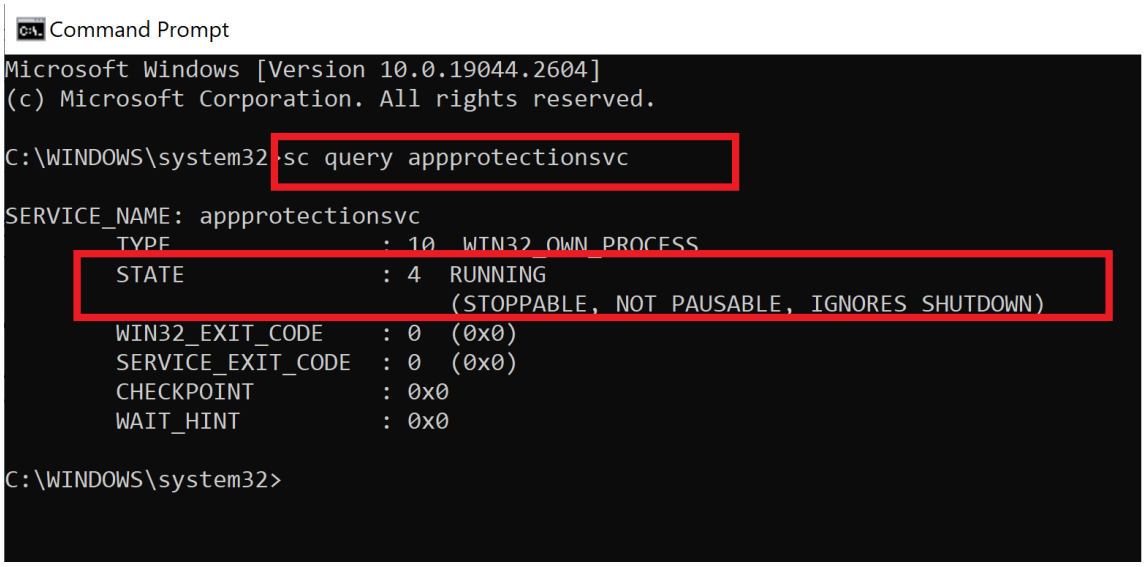

App Protection 可能会处于已停止状态或正在运行状态。

要检查服务的状态，请执行以下步骤之一：

- 对于 Citrix Workspace 应用程序版本 2206 或更高版本，请运行以下命令：

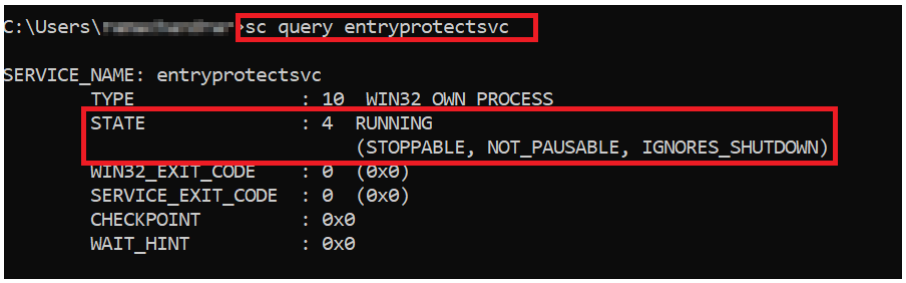
```
sc query appprotectionsvc
<!--NeedCopy-->
```

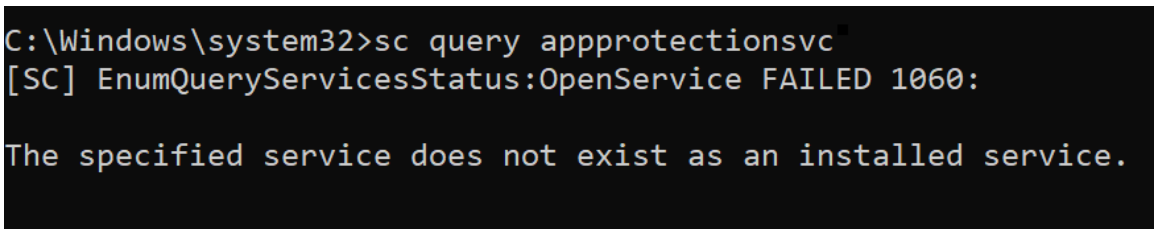
 




- 对于 2206 之前的 Citrix Workspace 应用程序版本，请运行以下命令：

```
sc query entryprotectsvc
<!--NeedCopy-->
```




> 注意：
>
> 在 2212 之前的 Citrix Workspace 应用程序版本中，如果您在安装 Citrix Workspace 应用程序时没有选中启用 **App Protection** 复选框，则当您运行前面的命令来检查状态时，会显示以下错误消息：
>
> 
> 

### **App Protection** 在不同环境中的行为

App Protection 的行为取决于您如何访问配置了 App Protection 策略的资源。这些资源包括 Virtual Apps and Desktops、内部 Web 应用程序和 SaaS 应用程序。可以使用受支持的原生 Citrix Workspace 应用程序客户端或 Web 浏览器访问这些资源。App Protection 在不同环境中的行为各异：

- 不受支持的 **Citrix Receivers** 或 **Citrix Workspace** 应用程序 - 配置了 App Protection 策略的资源不可用。
- 不受支持的 **Citrix Workspace** 应用程序版本 - 配置了 App Protection 策略的资源可用并正确启动。
- 使用 **Workspace** 应用程序 **URL** 的混合启动 - 配置了 App Protection 策略的资源始终可用。要使用 Workspace 应用商店 URL 在 Web 浏览器上成功启动资源，请参阅适用于 Workspace 混合启动的 App Protection。
- 使用 **StoreFront** 应用程序 **URL** 的混合启动 - 如果未部署 StoreFront 自定义，则配置了 App Protection 策略的资源不可用。要使用 StoreFront 应用商店 URL 在 Web 浏览器上成功启动资源，请参阅适用于 StoreFront 混合启动的 App Protection。

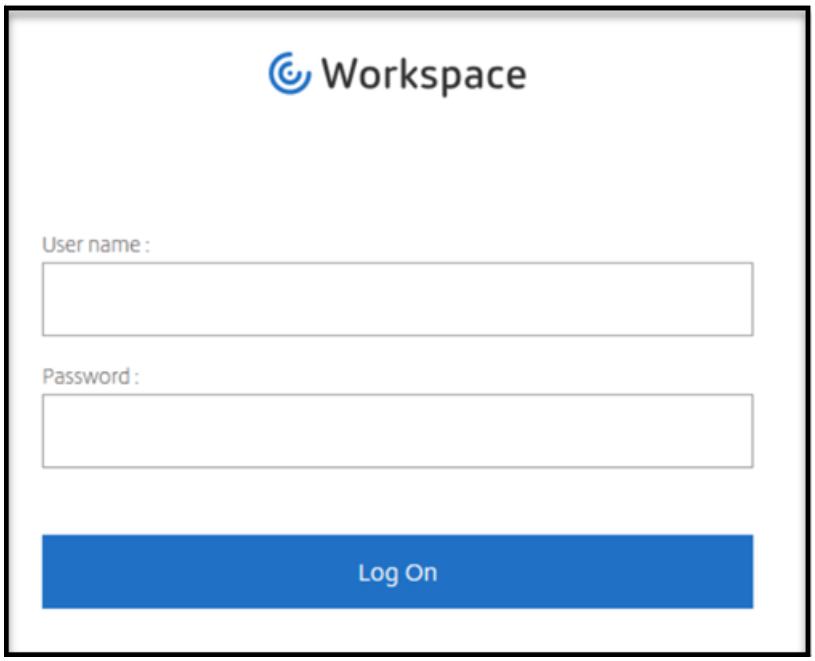
保护功能在以下条件下应用：

- 防屏幕捕获 - 对于适用于 Windows 的 Citrix Workspace 应用程序和适用于 Mac 的 Citrix Workspace 应用程序，如果屏幕上可见任何受保护的窗口，则启用此功能。要禁用保护功能，请最小化所有受保护的窗口。对于适用于 Linux 的 Citrix Workspace 应用程序，如果任何受保护的窗口都处于活动状态，则将启用该功能。要禁用保护功能，请关闭所有受保护的窗口。
- 反键盘记录 - 如果受保护的窗口处于焦点中，则启用此功能。要禁用保护功能，请将焦点更改为另一个窗口。

### App Protection 保护哪些项目?

App Protection 会保护以下 Citrix 窗口：

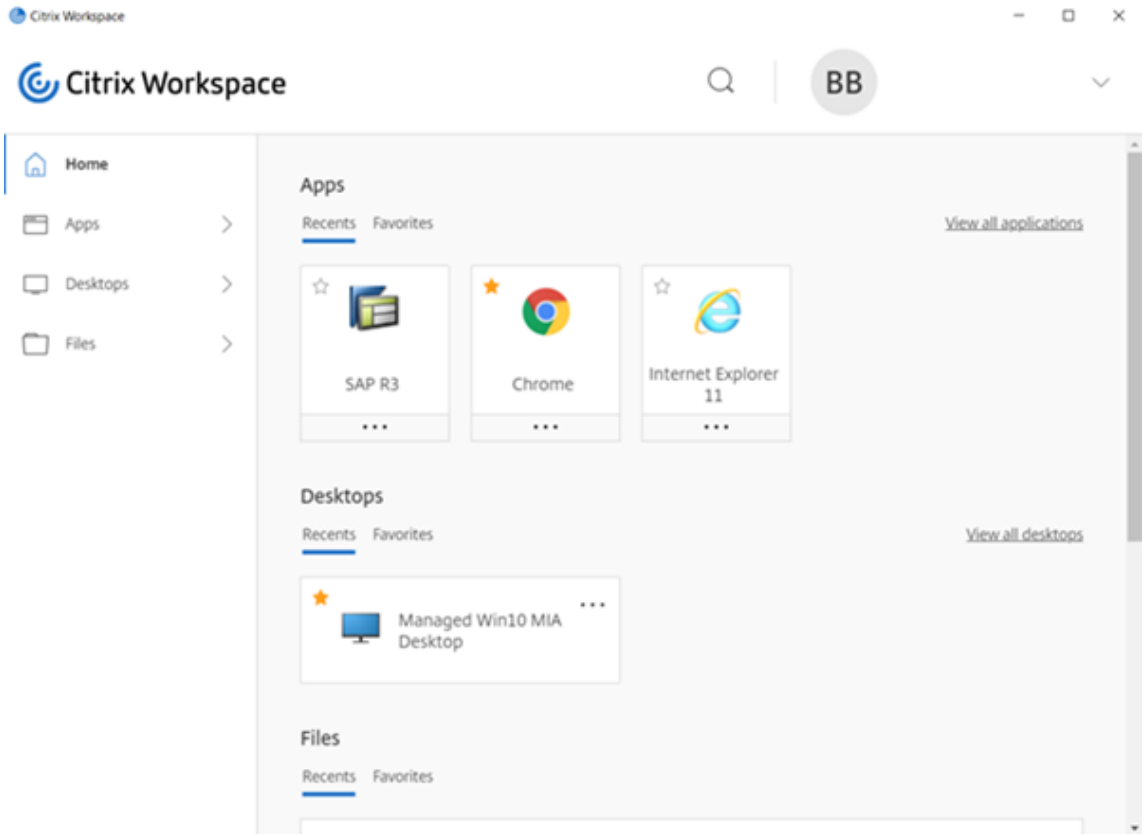
- Citrix 登录窗口




- Citrix Workspace 应用程序 HDX 会话窗口（例如，托管桌面）


- 自助服务（应用商店）窗口

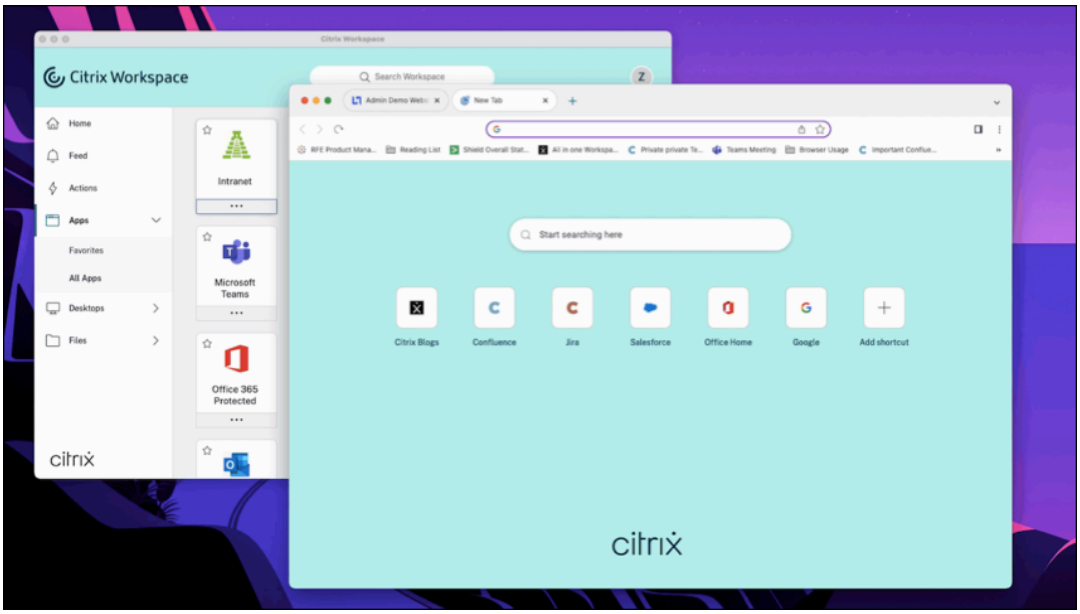



- Web 和 SaaS 应用程序

  – 适用于 Windows 的 Citrix Workspace 应用程序和适用于 Mac 的 Citrix Workspace 应用程序 - Web 和 SaaS 应用程序在 Citrix Enterprise Browser 中打开。如果将这些应用程序配置为通过 Citrix

Secure Private Access 使用 App Protection 策略，App Protection 将按选项卡应用。




- 适用于 Linux 的 Citrix Workspace 应用程序 - 不支持 Citrix Enterprise Browser。

## App Protection 不保护哪些项目?

- 导航栏中的 Citrix Workspace 应用程序图标下的以下项目：
  - 连接中心
  - “高级首选项”下的所有链接
  - 个性化
  - 检查更新
  - 注销
- 如果您选择使用防屏幕截图来保护虚拟桌面，用户仍然可以在虚拟桌面内的应用程序中共享屏幕。但是，对于虚拟桌面之外的应用程序，您将无法创建屏幕截图或者录制虚拟桌面。

限制

设计存在以下限制：

- 启用了 App Protection 的 Virtual Apps and Desktops 在 RDP 会话中访问时会被阻止启动。
- 在 RDP 会话中，使用 Citrix Enterprise Browser 打开的 Web 和 SaaS 应用程序不支持 App Protection。
- 双跃点和多跃点场景不支持 App Protection。
- 如果您使用的是不受支持的 Citrix Workspace 应用程序或 Citrix Receiver 版本，则不支持 App Protection。在这种情况下，资源是隐藏的。
- 将 App Protection 功能应用到虚拟应用程序和桌面时，如果使用优化，传出的屏幕共享可能会受到影响。

- 具有 App Protection 功能的 Citrix Workspace 应用程序可能与一些其他安全解决方案或使用类似底层技术的应用程序不兼容。
- 从 Citrix Secure Browser 中启动资源或者通过 Remote Browser Isolation 启动资源时，不支持 App Protection。
- 在适用于 Linux 的 Citrix Workspace 应用程序中，安装 App Protection 后，您无法使用快照应用程序。

### 上下文 **App Protection**

上下文 App Protection 提供了精细的灵活性，可以根据用户、其设备和网络状况，有条件地为一部分用户应用 App Protection 策略。有关详细信息，请参阅以下文章：

- 适用于 StoreFront 的上下文 App Protection
- 适用于 Workspace 的上下文 App Protection

### 面向混合启动的 **App Protection**

Citrix Virtual Apps and Desktops 的混合启动是指您通过浏览器登录 Citrix Workspace 应用程序（适用于 Web 的 Citrix Workspace），然后通过本机 Citrix Workspace 应用程序使用应用程序。“混合”一词是用户结合应用适用于 Web 的 Citrix Workspace 应用程序与本机 Citrix Workspace 应用程序来连接和使用资源的结果。App Protection 支持 Workspace 和 StoreFront 中的混合启动。有关详细信息，请参阅以下文章：

- 面向 Workspace 的混合启动的 App Protection
- 面向 StoreFront 的混合启动的 App Protection

## 系统要求和兼容性

April 29, 2024

### 系统要求

作为必备条件，请确保您已使用管理员权限安装了 Citrix Workspace 应用程序。

#### **Citrix** 组件的最低版本

- 适用于 Linux 的 Citrix Workspace 应用程序 2108
- 适用于 Windows 的 Citrix Workspace 应用程序 2203.1 LTSR
- 适用于 Windows 的 Citrix Workspace 应用程序 2002

- 适用于 Windows 的 Citrix Workspace 应用程序 2305.1（应用商店版本）
- 适用于 Mac 的 Citrix Workspace 应用程序 2001
- StoreFront 1912 LTSR
- Delivery Controller 1912
- 有效的 Citrix 许可证。有关详细信息，请联系您的 Citrix 销售代表或 Citrix Partner。

> 注意：
>
> 如果用户使用的设备或 Workspace 应用程序版本不支持 App Protection，他们将无法访问受保护的资源。受保护的资源包括 Virtual Apps and Desktops 以及 Web 和 SaaS 应用程序。

许可证

以下部分根据产品、平台和用例说明了可用于 App Protection 的不同类型的许可证。

**IT 管理的 VDI**　对于 IT 管理的 VDI 的所有版本，App Protection 均作为加载项提供。有关详细信息，请参阅 IT 管理的 VDI。

适用于超大规模企业的 **Citrix DaaS**

- Azure
- Google
- AWS

**Citrix DaaS**　在 Feature Matrix for Citrix DaaS（Citrix DaaS 的功能列表）一文中，导航到 **DaaS cloud Services**（**DaaS** 云服务）**> Security and Monitoring**（安全和监视）**> App Protection**。

**Citrix Secure Private Access**　App Protection 作为 Citrix Secure Private Access 的独立附件提供。有关详细信息，请导航到 Service descriptions for Citrix Services（Citrix Services 的服务说明）一文中的 **Citrix Cloud Services > Citrix Secure Private Access**。

**Citrix Universal** 订阅　App Protection 包含在以下服务中：

- Citrix Universal Premium
- Citrix Universal Premium Plus

它作为加载项提供，有以下版本：

- Citrix Universal Advanced
- Citrix Universal Advanced Plus

有关详细信息，请参阅这篇文章。

操作系统平台

App Protection 策略运行时安装在要从中进行连接的端点上，而非安装在要连接到的 VDA 上。因此，只有端点的操作系统版本很重要。（App Protection 可以连接到 Citrix Virtual Apps and Desktops 系统要求中所述的任何受支持的操作系统上托管的 VDA。）

运行以下操作系统的端点支持 App Protection 功能：

- **Windows**：
  - Windows 11（64 位版本）
  - Windows 10（32 位和 64 位版本）

    > 注意：
    >
    > 搭载 Arm64 版本的 Windows 操作系统的设备不支持 App Protection。

- **macOS**：
  - High Sierra (10.13) 及更高版本
- **Linux**：
  - 64 位 Ubuntu 22.04
  - 64 位 RHEL 9
  - ARM64 Raspberry Pi OS（基于 Debian 11 (bullseye)）

> 注意：
>
> 对于 App Protection，适用于 Linux 的 Citrix Workspace 应用程序需要 Gnome Display Manager 以及支持的操作系统。

兼容性列表

基于 **Citrix Cloud** 的产品的兼容性矩阵

与基于 Citrix Cloud 的产品兼容的 App Protection 功能如下：

| 功能 | Citrix Cloud | Citrix Cloud Japan |
| --- | --- | --- |
| 面向虚拟应用程序和桌面的反键盘记录和防屏幕捕获 | 是 | 是 |
| 面向 Web 或 SaaS 应用程序的反键盘记录和防屏幕捕获 | 是 | 否 |
| 适用于 Windows 的防 DLL 攻击 | 是 | 是，通过组策略对象 (GPO) |

| 功能 | Citrix Cloud | Citrix Cloud Japan |
| --- | --- | --- |
| 防 DLL 攻击允许列表 | 是 | 是的，通过 GPO |
| Global App Configuration Service (GACS) | 是 | 否 |
| 适用于 Linux 的身份验证或自助服务插件屏幕保护 | 是 | 是的，通过 AuthManConfig.xml |
| 适用于 Mac 的身份验证或自助服务插件屏幕保护 | 是的，通过 GACS | 是的，通过 GACS |
| 适用于 Windows 的身份验证或自助服务插件屏幕保护 | 是 | 是的，通过 GPO |
| CAS App Protection 屏幕截图事件 | 是 | 否 |
| 上下文 App Protection | 是 | 是，视用户而定 |
| 策略篡改检测 | 是 | 是 |
| App Protection 状态检查 | 是 | 是 |
| 本地应用程序允许列表或过滤器 - Windows | 是 | 是的，通过 GPO |
| 本地 App Protection - Windows | 是 | 是的，通过 GPO |

## App Protection 功能

June 19, 2024

本文重点介绍了适用于 Windows 的 Citrix Workspace 应用程序、适用于 Linux 的 Citrix Workspace 应用程序和适用于 Mac 的 Citrix Workspace 应用程序支持的 App Protection 功能。

### 反键盘记录

通过加密，App Protection 功能的的反键盘记录功能会对用户在物理键盘和屏幕键盘上键入的文本进行加密。在任何键盘记录工具可以从内核或操作系统级别访问文本之前，反键盘记录功能都会对文本进行加密。安装在客户端端点上从操作系统或驱动程序中读取数据的键盘记录器将捕获哈希文本，而非用户正在键入的按键。App Protection 策略不仅对已发布的应用程序和桌面有效，对 Citrix Workspace 身份验证对话框也是如此。从用户打开第一个身份验证对话框的那一刻起，您的 Citrix Workspace 就会受到保护。App Protection 会扰乱按键，将无法理解的文本返回给按键记录器。

管理员可以选择为以下类型的资源启用反键盘记录：

- Virtual Apps and Desktops
- 内部 Web 和 SaaS 应用程序
- 身份验证屏幕
- 自助服务插件 (SSP) 屏幕

### 防屏幕捕获

防屏幕捕获可防止应用程序尝试在虚拟应用程序或桌面会话中截取屏幕截图或录制屏幕。屏幕捕获软件无法检测捕获区域内的内容。应用程序选择的区域显示为灰色，或者应用程序除了要复制的屏幕部分外，不捕获任何对象。防屏幕捕获功能适用于 Windows 上的
截屏和草图、截图工具和 **Shift+Ctrl+Print Screen**。

防屏幕捕获的另一个用例是防止在 GoToMeeting、Microsoft Teams 或 Zoom 等虚拟会议或网络会议应用程序中共享敏感数据。当应用程序受到保护时，App Protection 功能会在 Web 会议中返回空白屏幕，从而防止意外共享。此功能可确保敏感数据不会意外从组织泄露。此功能有助于遵守受监管行业的合规性，因为在披露数据泄露时不考虑意图。

管理员可以选择为以下类型的资源启用防屏幕捕获：

- Virtual Apps and Desktops
- 内部 Web 和 SaaS 应用程序
- 身份验证屏幕
- 自助服务插件 (SSP) 屏幕

> 注意：
>
> 如果您启动了两个虚拟桌面，其中一个虚拟桌面启用了防屏幕捕获功能，而另一个虚拟桌面未启用防屏幕捕获功能，防屏幕捕获功能将同时应用到这两个虚拟桌面。您无法截取任何一个虚拟桌面的屏幕截图。
>
> 如果您已最小化启用了防屏幕捕获的虚拟桌面，则防屏幕捕获功能仍然应用于没有防屏幕捕获功能的虚拟桌面。

### 屏幕截图检测和通知

对于 Citrix Workspace 应用程序而言，当有人可能尝试对任何受保护的资源进行屏幕捕获时，您可以查看通知。有关 App Protection 保护的资源的信息，请参阅 App Protection 保护什么?

出现以下情况时会显示通知：

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

> 注意：
>
> - 屏幕捕获工具的每个运行实例仅显示一次。如果您重新启动该工具并尝试捕获屏幕，则会再次显示通知。
> - 在适用于 Windows 的 Citrix Workspace 应用程序 2212 及更高版本中，默认情况下，登录窗口和自助

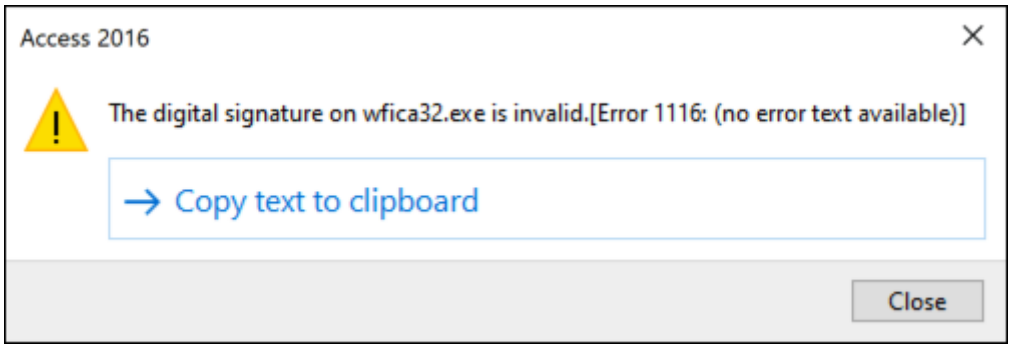
> 服务（应用商店）窗口不受保护。

### 反 **DLL** 注入

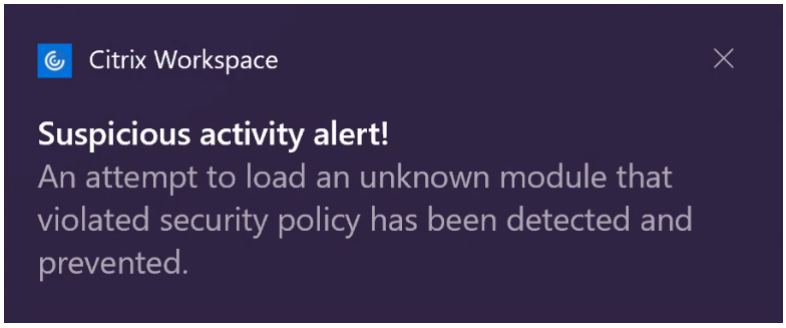
反 DLL 注入安全增强功能有助于保护 Citrix Workspace 应用程序免受某些未经授权的动态链接库 (DLL) 或不可信模块的侵害。如果注入了此类不可信模块，Citrix Workspace 应用程序会检测到这些干预措施并停止加载这些模块。此外，如果在会话启动之前检测到任何不受信任或恶意的 DLL，App Protection 会阻止会话启动并显示错误消息。关闭错误消息将退出虚拟应用程序和桌面会话。

此功能适用于所有受保护的虚拟应用程序和桌面以及 Citrix Workspace 应用程序身份验证窗口（本地部署/StoreFront）。

当受保护的组件上存在某些不可信或恶意 DLL 时，此增强功能将立即退出会话。




当不可信或恶意 DLL 被阻止时，此增强功能将显示通知。关闭消息将退出虚拟应用程序和桌面会话。




免责声明：此功能通过筛选对底层操作系统所需功能（加载 DLL 所需的特定 API 调用）的访问来发挥作用。这样做意味着它甚至可以提供保护，使其免受某些自定义和专门构建的黑客工具的侵害。但是，随着操作系统的发展，加载 DLL 的新方法可能会出现。虽然我们会继续识别和解决这些问题，但我们无法保证在特定配置和部署中提供充足的保护。

此功能支持适用于 Windows 的 Citrix Workspace 应用程序版本 2206 及更高版本。

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

### 与 **Microsoft Teams** 的 **HDX** 优化的兼容性

仅当在 Desktop Viewer 模式下为 Citrix Workspace 应用程序启用了 App Protection 时，优化的 Microsoft Teams 才支持屏幕共享。当您在 Microsoft Teams 中单击共享内容时，屏幕选取器会提供以下选项：

- 用于共享任何打开的应用程序的窗口选项 - 仅当 VDA 版本为 2109 或更高版本时才会显示此选项。
- 用于共享您的 VDA 桌面上的内容的桌面选项 - 此选项仅对 Citrix Workspace 应用程序的以下版本显示：
  - 适用于 Linux 的 Citrix Workspace 应用程序 2311 或更高版本
  - 适用于 Mac 的 Citrix Workspace 应用程序 2308 或更高版本
  - 适用于 Windows 的 Citrix Workspace 应用程序 2309 或更高版本

> 注意：
>
> 对于适用于 Linux 的 Citrix Workspace 应用程序，“桌面共享”选项默认处于禁用状态。要将其启用，请在您的 *config.json* 文件中添加 `UseGbufferScreenSharing` 参数，如下所示：

```
mkdir -p /var/.config/citrix/hdx_rtc_engine
vim /var/.config/citrix/hdx_rtc_engine/config.json
{

      "UseGbufferScreenSharing":1
 }

<!--NeedCopy-->
```

启用了 App Protection 的优化的 Microsoft Teams 还支持 Citrix 虚拟显示器布局，这允许您分别共享每个虚拟显示器。

> 限制：
>
> - 优化后的启用了 App Protection 的 Microsoft Teams 不支持在启用了本地应用程序访问 (LAA) 的已发布桌面上共享屏幕。
> - 无法捕获或共享客户端呈现的内容，例如使用 BCR 的浏览器内容。如果您尝试截屏，屏幕会显示为黑屏。
>
> 注意：
>
> 对于适用于 Linux 的 Citrix Workspace 应用程序，此功能为技术预览版。

### 本地 **App Protection**（预览版）

App Protection 提供增强的安全性，保护客户免受键盘记录器以及意外和恶意屏幕截图的侵害。目前，App Protection 功能仅针对 Workspace 资源提供。借助此功能，App Protection 功能可以扩展到端点上的本地应用程序。自适用于 Windows 的 Citrix Workspace 应用程序 2210 起，App Protection 可以应用到 Windows 设备上的本地应用程序。

使用 Podio 表单注册获取此功能的预览版。

#### 策略篡改检测

如果 App Protection 的防屏幕捕获和反键盘记录策略被篡改，策略篡改检测功能可防止用户访问虚拟应用程序或桌面会话。如果检测到策略篡改，虚拟应用程序或桌面会话将终止。

> 注意：
>
> 策略篡改检测功能在将来的版本中默认处于启用状态。

要配置策略篡改检测，请参阅配置策略篡改检测。

#### 状态检查

要检测和阻止启动不支持策略篡改检测功能的 Citrix Workspace 应用程序版本中启用了 App Protection 策略的虚拟应用程序和桌面，请启用 App Protection 状态检查。

> 注意：
>
> 如果启用了状态检查，并且您使用的是不支持状态检查的 Citrix Workspace 应用程序版本，启用了 App Protection 策略的会话将终止。

要配置状态检查，请参阅配置状态检查。

> 限制：
>
> 将 Microsoft Azure 上托管的 Windows 工作站 VDA 与 VDA 2308 结合使用时，状态检查会间歇性地停止工作。此限制已在 VDA 版本 2311 及更高版本中得到解决。

### 在 **DoubleHop** 场景中使用 **App Protection**

双跃点场景中不支持 App Protection 功能。双跃点是指在 Citrix Virtual Desktops 会话中运行的 Citrix Virtual Apps 或 Virtual Desktops 会话。在双跃点场景中，您可以启动启用了 App Protection 策略的虚拟应用程序和桌面，但不会应用 App Protection 功能。

自适用于 Windows 的 Citrix Workspace 应用程序 2309 版本起，引入了一个 Windows 组策略来允许您在双跃点场景中阻止启动启用了 App Protection 策略的虚拟应用程序和桌面。有关启用阻止 **DoubleHop** 启动设置的详细信息，请参阅启用“阻止 DoubleHop 启动”设置。

### 适用于 **App Protection** 的 **Citrix Analytics Service**

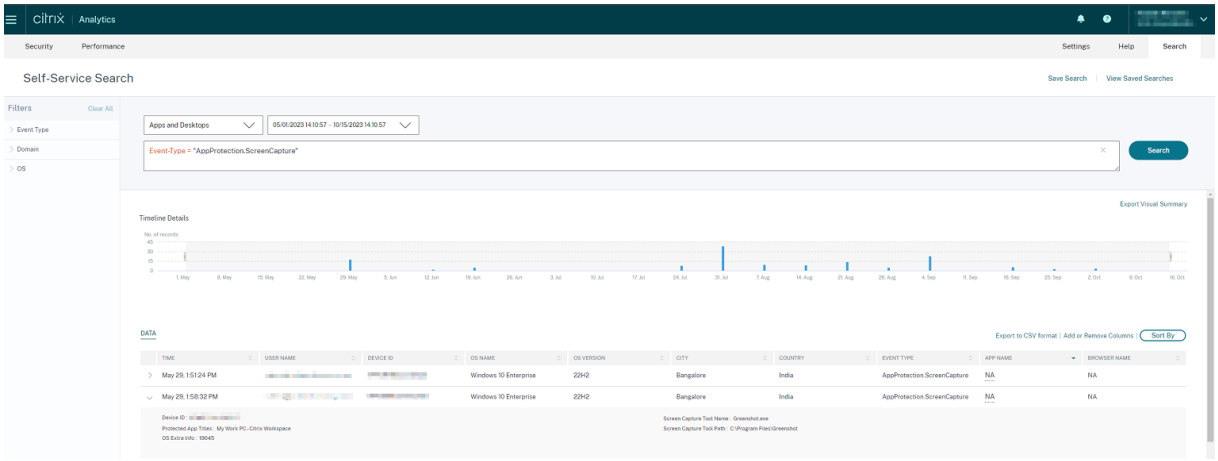
当您使用 Citrix Virtual Apps and Desktops 时，会生成与其活动和操作相对应的用户事件。Citrix Analytics for Security 具有一项名为自助搜索的功能，该功能将记录这些用户事件并为您提供有关这些事件的见解。通过自助搜索，您可以查找、筛选和浏览这些用户事件，以便您能够了解完成了哪些用户事件并根据事件的严重性执行操作。有关自助搜索的详细信息，请参阅自助搜索。

面向应用程序和桌面的自助搜索具有事件类型 `AppProtection.ScreenCapture`，允许您确定是否有人尝试创建启用了 App Protection 策略的虚拟应用程序或桌面的屏幕截图。有关如何搜索用户事件的详细信息，请参阅指定搜索查询以筛选事件。

此服务提供以下信息：

- 设备 ID
- 受保护的应用程序标题
- 操作系统的额外信息
- 屏幕截图工具名称
- 屏幕截图工具路径




## 屏幕捕获允许列表

如果 Citrix Workspace 应用程序、Virtual Apps and Desktops 或 SaaS 应用程序启用了 App Protection 防屏幕捕获策略，您将无法使用任何屏幕捕获工具捕获其屏幕。

但是，从适用于 Windows 的 Citrix Workspace 应用程序 2402 版本起，“屏幕捕获允许列表”功能允许您向屏幕捕获允许列表中添加应用程序。通过此功能，您可以使用允许列出的应用程序并捕获通过 App Protection 防屏幕捕获策略启用的资源的屏幕。要将应用程序添加到屏幕捕获允许列表中，请参阅配置屏幕捕获允许列表。

> 重要：
>
> 建议不要在设备上长时间运行列出的允许运行的应用程序，因为这会降低安全状况。在故障排除等场景中，可以使用列出的允许运行的应用程序临时共享您的屏幕。建议遵守以下条件：
>
> - 在短时间内运行列出的允许运行的应用程序以及启用了 App Protection 防屏幕捕获功能的资源。
> - 完成所需任务后，请立即终止列出的允许运行的应用程序。
> - 请在共享屏幕时添加水印，同时使用启用了 App Protection 防屏幕捕获功能的资源，以提高安全性。

进程排除列表

当您在设备上启动任何进程或应用程序时，如果启用了 App Protection，App Protection DLL 会注入到每个进程中。有时，由于 DLL 的兼容性问题，这可能会导致进程或应用程序无法运行。

自适用于 Windows 的 Citrix Workspace 应用程序 2402 版本起，您可以将任何进程添加到进程排除列表中，以避免将 App Protection DLL 注入到该特定进程中，并从 App Protection DLL 的存在导致的任何兼容性问题中恢复。要配置进程排除列表，请参阅配置进程排除列表。

> 重要：
>
> 不建议排除进程，因为这会降低安全状况。可以用它来暂时解除对应用程序的使用限制，并提出支持票据以供进一步调查。

**USB** 过滤器驱动程序排除列表

有时，当您在 Citrix Workspace 应用程序中使用游戏键盘等专用外部键盘时，App Protection USB 过滤器驱动程序可能会导致出现兼容性问题并阻止您使用该键盘。

自适用于 Windows 的 Citrix Workspace 应用程序 2402 版本起，USB 过滤器驱动程序排除列表功能允许您使用设备供应商 ID 和产品 ID 排除与 Citrix Workspace 应用程序存在兼容性问题的任何 USB 设备。要将任何设备添加到 USB 过滤器驱动程序排除列表中，请参阅配置 USB 过滤器驱动程序排除列表。

> 注意：
>
> 不建议永久排除设备。使用此功能可以暂时解除对用户使用设备的限制，并提出支持票据以进一步调查兼容性问题。

# 配置 **App Protection**

April 10, 2024

App Protection 可以在您使用 Citrix Workspace 应用程序时提供增强的安全性。该功能限制了客户端被键盘记录和屏幕捕获恶意软件入侵的能力。App Protection 可防止泄露屏幕上显示的用户凭据和敏感信息等机密信息。该功能可防止用户和攻击者截取屏幕截图以及使用键盘记录器收集和利用敏感信息。

本文介绍如何在不同平台上的 Citrix Workspace 应用程序中配置 App Protection。

App Protection 在 Citrix Workspace 应用程序上可用，适用于以下平台：

- 适用于 Windows 的 Citrix Workspace 应用程序
- 适用于 Linux 的 Citrix Workspace 应用程序
- 适用于 Mac 的 Citrix Workspace 应用程序

> 免责声明
>
> App Protection 策略筛选对基础操作系统所需功能的访问权限。需要特定的 API 调用才能捕获屏幕或按下键盘。App Protection 策略甚至能够针对自定义的专用黑客工具提供保护。但是，随着操作系统的发展，捕获屏幕和记录键盘的新方法可能会出现。虽然我们会继续识别和解决这些问题，但我们无法保证在特定配置和部署中提供充足的保护。

### 适用于 **Windows** 的 **Citrix Workspace** 应用程序

必备条件

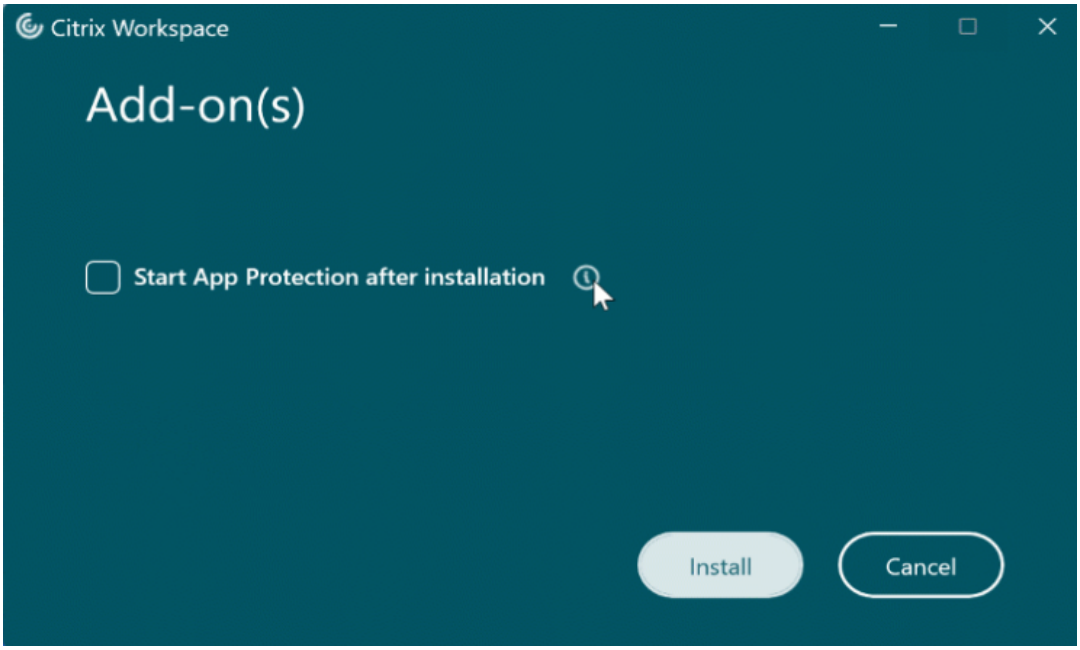
- Citrix Virtual Apps and Desktops 版本 1912 LTSR 或更高版本。
- StoreFront 1912 LTSR 或 Workspace。
- Citrix Workspace 应用程序 2203.1 LTSR 或更高版本。
- 有效的 App Protection 许可证
- 自 Citrix Workspace 应用程序版本 2212 起，App Protection 组件是在安装 Citrix Workspace 应用程序期间默认安装的。

  安装期间出现的启用 **App Protection** 复选框将被替换为安装后启动 **App Protection**。

  - 对于 2311 之前的 Citrix Workspace 应用程序版本：

- 自 Citrix Workspace 应用程序版本 2311 起：




选中此复选框后，App Protection 将在安装后立即启动。

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

配置

为适用于 Windows 的 Citrix Workspace 应用程序配置以下 App Protection 功能：

- 反键盘记录和防屏幕捕获：
  - 对于 Virtual Apps and Desktops，请参阅为 Virtual Apps and Desktops 配置反键盘记录和防屏幕捕获。
  - 对于 Web 和 SaaS 应用程序，请参阅为 Web 和 SaaS 应用程序配置反键盘记录和防屏幕捕获。
  - 对于身份验证和自助服务插件：
    - 使用 Global App Configuration Service 用户界面，请参阅使用 Global App Configuration Service 用户界面为身份验证和自助服务插件配置反键盘记录和防屏幕捕获
    - 使用组策略对象，请参阅使用组策略对象为身份验证和自助服务插件配置反键盘记录和防屏幕捕获
    - 使用 API，请参阅使用 GACS API 为身份验证和自助服务插件配置反键盘记录和防屏幕捕获
- 要配置反 DLL 注入功能，请参阅配置反 DLL 注入功能。
- 要配置 App Protection 策略篡改，请参阅配置 App Protection 策略篡改。
- 要配置 App Protection 状态检查，请参阅配置 App Protection 状态检查。
- 要启用“阻止 DoubleHop 启动”设置，请参阅阻止 DoubleHop 启动。

限制

- 此功能仅在 Windows 11 和 Windows 10 等桌面操作系统中受支持。
- 自版本 2006.1 起，Windows 7 不支持 Citrix Workspace 应用程序。因此，App Protection 在 Windows 7 中不起作用。有关详细信息，请参阅弃用。
- 远程桌面协议 (RDP) 不支持此功能。

命令行接口

可以使用 `/startappprotection` 命令行参数启动 App Protection 组件。但是，先前的 `/includeappprotection` 开关已弃用。

下表提供了有关受保护的屏幕的信息，具体取决于部署：

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

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

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

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

**App Protection** 增强功能：

在适用于 Windows 的 Citrix Workspace 应用程序 2305 及更高版本中，如果满足以下条件之一，则会在身份验证和自助服务插件屏幕上启用反键盘记录：

- 您已使用以下任一方式启用了 App Protection：
  - 在安装过程中选中启动 **App Protection** 复选框。
  - 使用 **/startappprotection** 命令行参数启动 App Protection 组件。

- 如果您尚未在安装过程中选中启动 **App Protection** 复选框或者尚未使用 **/startappprotection** 命令行参数，则在启动第一个受保护的资源后将启用反键盘记录保护。

> 注意：
>
> Global App Configuration Service 和组策略对象设置会覆盖上述行为。例如，如果您对这些屏幕禁用了 GACS 或 GPO 策略，则在身份验证和 SSP 屏幕上未启用反键盘记录。

### 适用于 **Linux** 的 **Citrix Workspace** 应用程序

自版本 2108 起，App Protection 功能现已完全起作用。此功能支持 Virtual Apps and Desktops，并且默认处于启用状态。但是，您必须在 `AuthManConfig.xml` 文件中配置 App Protection 功能，才能对身份验证管理器和自助服务插件界面启用该功能。

#### 必备条件

App Protection 功能最适合以下操作系统以及 Gnome Display Manager：

- 64 位 Ubuntu 22.04、Ubuntu 20.04 和 Ubuntu 18.04
- 64 位 Debian 10 和 Debian 9
- 64 位 CentOS 7
- 64 位 RHEL 7
- ARMHF 32 位 Raspberry Pi OS（基于 Debian 10 (buster)）
- ARM64 Raspberry Pi OS（基于 Debian 11 (bullseye)）

> 注意：
>
> 如果您使用的 Citrix Workspace 应用程序早于 2204 版，App Protection 功能将不支持使用 `glibc` 2.34 或更高版本的操作系统。
>
> 如果在使用 `glibc` 2.34 或更高版本的操作系统中安装启用了 App Protection 功能的 Citrix Workspace 应用程序，操作系统引导在重新启动系统时可能会失败。要从操作系统引导失败进行恢复，请执行以下任一操作：
>
> - 重新安装操作系统。
> - 转至操作系统恢复模式，然后使用终端卸载 Citrix Workspace 应用程序。
> - 通过实时操作系统进行引导，并从现有操作系统中删除 `rm -rf /etc/ld.so.preload` 文件。

#### 安装 **App Protection** 组件

1. 使用 tarball 软件包安装 Citrix Workspace 应用程序时，将显示以下消息：是否要安装 **App Protection** 组件**?** 警告**:** 不能禁用此功能。必须卸载 **Citrix Workspace** 应用程序，才能将其禁用。有关详细信息，请与系统管理员联系。**[default $INSTALLER_N]:**

2. 输入 **Y** 以安装 App Protection 组件。默认不安装 App Protection 组件。
3. 重新启动您的计算机以使更改反映出来。只有在您重新启动计算机后，App Protection 功能才能按预期运行。

安装 **RPM** 软件包中的 **App Protection** 组件　自版本 2104 起，Citrix Workspace 应用程序的 RPM 版本支持 App Protection 功能。

要安装 App Protection 组件，请执行以下操作：

1. 安装 Citrix Workspace 应用程序。
2. 从 Citrix Workspace 应用程序安装程序中安装 App Protection `ctxappprotection<version>.rpm` 软件包。
3. 重新启动系统以使更改反映出来。

安装 **Debian** 软件包中的 **App Protection** 组件　自版本 2101 起，Citrix Workspace 应用程序的 Debian 版本支持 App Protection 功能。

要安装 App Protection 组件，请在安装 Citrix Workspace 应用程序之前从终端运行以下命令：

```
export DEBIAN_FRONTEND="noninteractive"
sudo debconf-set-selections <<< "icaclient app_protection/
   install_app_protection select yes"

sudo debconf-show icaclient
* app_protection/install_app_protection: yes

sudo apt install -f ./icaclient_<version>._amd64.deb
<!--NeedCopy-->
```

自版本 2106 起，Citrix Workspace 应用程序引入了一个选项，用于同时为身份验证管理器和自助服务插件界面分别配置反键盘记录和防屏幕捕获功能。

### 配置

为适用于 Linux 的 Citrix Workspace 应用程序配置以下 App Protection 功能：

- 要为“身份验证”屏幕配置反键盘记录和防屏幕捕获，请参阅配置对身份验证管理器使用 AuthManConfig.xml。
- 要为“自助服务插件”屏幕配置反键盘记录和防屏幕捕获，请参阅配置对自助服务插件界面使用 AuthManConfig.xml。
- 要为 Virtual Apps and Desktops 配置反键盘记录和防屏幕捕获，请参阅为 Virtual Apps and Desktops 配置反键盘记录和防屏幕捕获。
- 要配置 App Protection 策略篡改，请参阅配置 App Protection 策略篡改。
- 要配置 App Protection 状态检查，请参阅配置 App Protection 状态检查。

### 适用于 **Mac** 的 **Citrix Workspace** 应用程序

为适用于 Mac 的 Citrix Workspace 应用程序配置以下 App Protection 功能：

- 要使用 Global App Configuration Service 用户界面为身份验证和自助服务插件配置反键盘记录和防屏幕捕获，请参阅使用 Global App Configuration Service 用户界面为身份验证和自助服务插件配置反键盘记录和防屏幕捕获。
- 要使用 API 为身份验证和自助服务插件配置反键盘记录和防屏幕捕获，请参阅使用 GACS API 为身份验证和自助服务插件配置反键盘记录和防屏幕捕获。
- 要为 Virtual Apps and Desktops 配置反键盘记录和防屏幕捕获，请参阅为 Virtual Apps and Desktops 配置反键盘记录和防屏幕捕获。
- 要为 Web 和 SaaS 应用程序配置反键盘记录和防屏幕捕获，请参阅为 Web 和 SaaS 应用程序配置反键盘记录和防屏幕捕获。
- 要配置 App Protection 策略篡改，请参阅配置 App Protection 策略篡改。
- 要配置 App Protection 状态检查，请参阅配置 App Protection 状态检查。

### 建议

App Protection 策略主要侧重于增强端点的安全性和保护。查看针对您的环境的所有其他安全建议和策略。可以在风险容忍度低的环境中使用安全性与控制策略模板设置建议的配置。有关详细信息，请参阅策略模板。

## 配置反键盘记录和防屏幕捕获

April 10, 2024

可以为以下对象配置反键盘记录和防屏幕捕获：

- 身份验证和自助服务插件
- Virtual Apps and Desktops
- Web 和 SaaS 应用程序

### 为身份验证和自助服务插件配置反键盘记录和防屏幕捕获

可以使用以下方法为身份验证和自助服务插件配置反键盘记录和防屏幕捕获：

| 配置方法 | 适用于 Linux 的 Citrix Workspace 应用程序 | 适用于 Mac 的 Citrix Workspace 应用程序 | 适用于 Windows 的 Citrix Workspace 应用程序 |
| --- | --- | --- | --- |
| 使用组策略对象 | 否 | 否 | 是 |
| 使用 Global App Configuration Service | 否 | 是 | 是 |
| 使用 AuthManConfig.xml | 是 | 否 | 否 |

使用组策略对象

1. 通过运行 `gpedit.msc` 打开 Citrix Workspace 应用程序组策略对象管理模板。
2. 在计算机配置节点下，转至管理模板 > **Citrix** 组件 > **Citrix Workspace**。
3. 请使用以下步骤之一，具体取决于您是为身份验证管理器还是为自助服务插件配置 App Protection 功能：
   - 身份验证管理器

     要为身份验证管理器配置反键盘记录和防屏幕捕获，请选择用户身份验证 > 管理 **App Protection** 策略。
   - 自助服务插件界面

     要为自助服务插件界面配置反键盘记录和防屏幕捕获，请选择自助服务 > 管理 **App Protection** 策略。
4. 选择以下选项之一或同时选中二者：
   - 反键盘记录：防止键盘记录器捕获按键。
   - 防屏幕捕获：防止用户创建屏幕截图和共享其屏幕。
5. 单击应用和确定。

预期行为：

预期行为取决于您访问具有受保护的资源的 StoreFront 的方法。

#### 使用 **Global App Configuration Service** 用户界面

自适用于 Windows 的 Citrix Workspace 应用程序 2302 或适用于 Windows 的 Citrix Workspace 应用程序 2301 版本起，Citrix Workspace 应用程序允许您使用 Global App Configuration Service (GACS) 为身份验证屏幕和自助服务插件配置 App Protection。

如果您使用 GACS 启用反键盘记录和防屏幕捕获功能，这两项功能将同时适用于身份验证和自助服务插件屏幕。

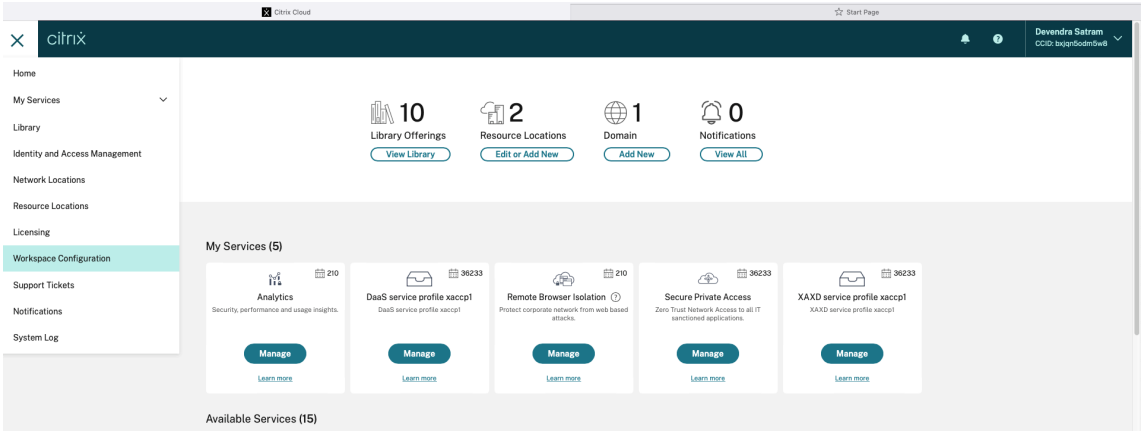
> 注意：
>
> - 使用 GACS 为身份验证和自助服务插件配置反键盘记录或防屏幕捕获适用于 Windows 的 Citrix

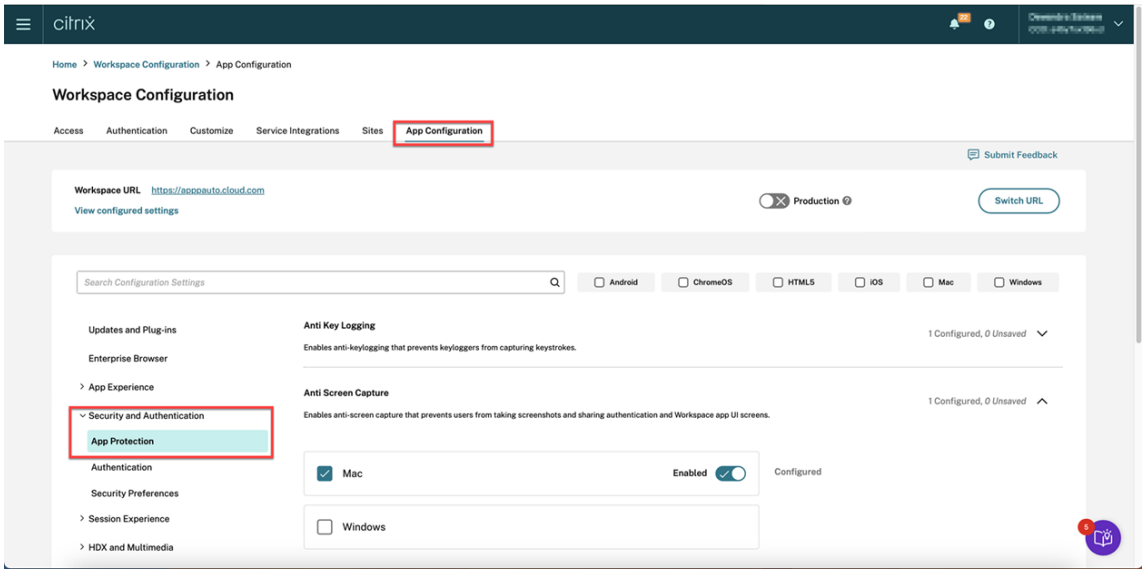
> Workspace 应用程序和适用于 Mac 的 Citrix Workspace 应用程序。此功能不适用于适用于 Linux 的 Citrix Workspace 应用程序。
> - GACS 配置不适用于 Virtual Apps and Desktops 以及 Web 和 SaaS 应用程序。这些资源将继续使用 Delivery Controller 和 Citrix Secure Private Access 进行控制。
> - 自适用于 Mac 的 Citrix Workspace 应用程序 2311 版本起，对于云应用商店和本地应用商店，您都可以使用 Global App Configuration Service 用户界面为身份验证和自助服务插件配置 App Protection。但是，如果您使用的是早于 2311 版本的适用于 Mac 的 Citrix Workspace 应用程序，则只能为云应用商店配置该功能。

管理员可以使用 Workspace 配置用户界面配置 App Protection：

1. 登录到您的 Citrix Cloud 帐户并选择 **Workspace** 配置。

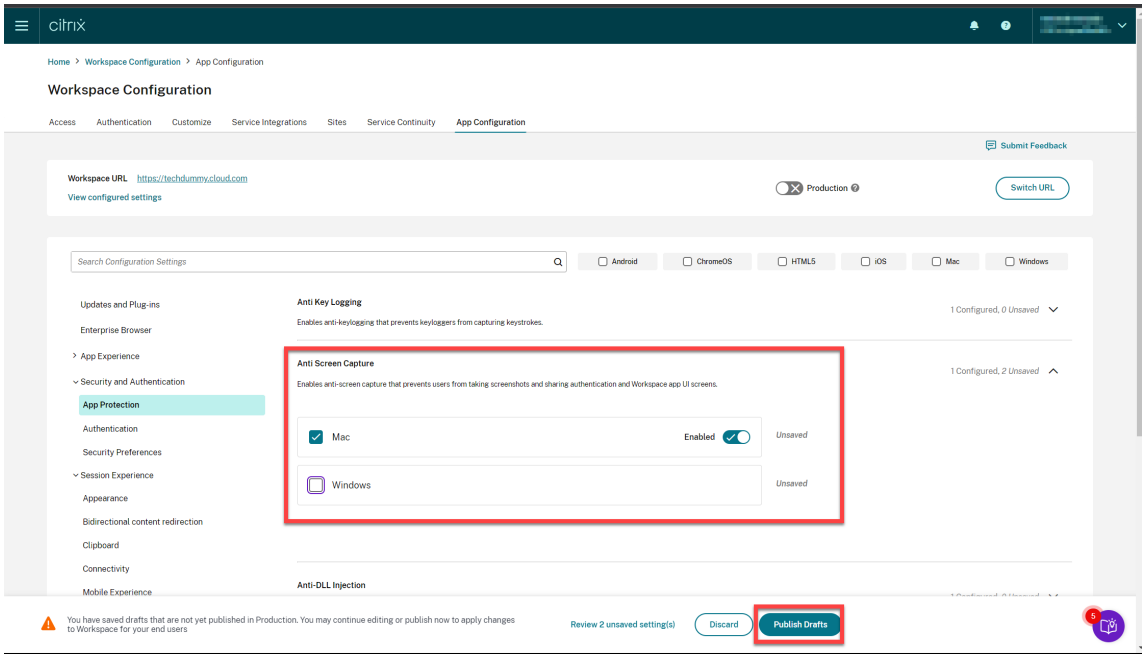



2. 选择 **App Configuration**（应用程序配置）> **Security and Authentication**（安全性和身份验证）> **App Protection**。

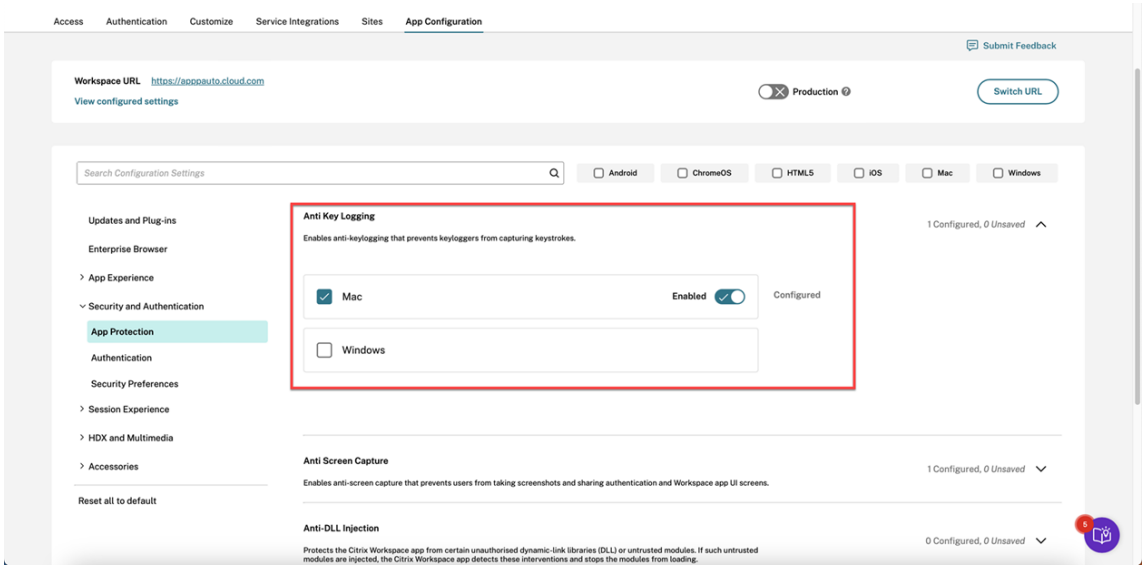



3. 单击 **Anti Screen Capture**（防屏幕捕获），然后选择相关的操作系统（Windows 或 Mac）。
4. 单击 **Enabled**（已启用）切换按钮，然后单击 **Publish Drafts**（发布草稿）。

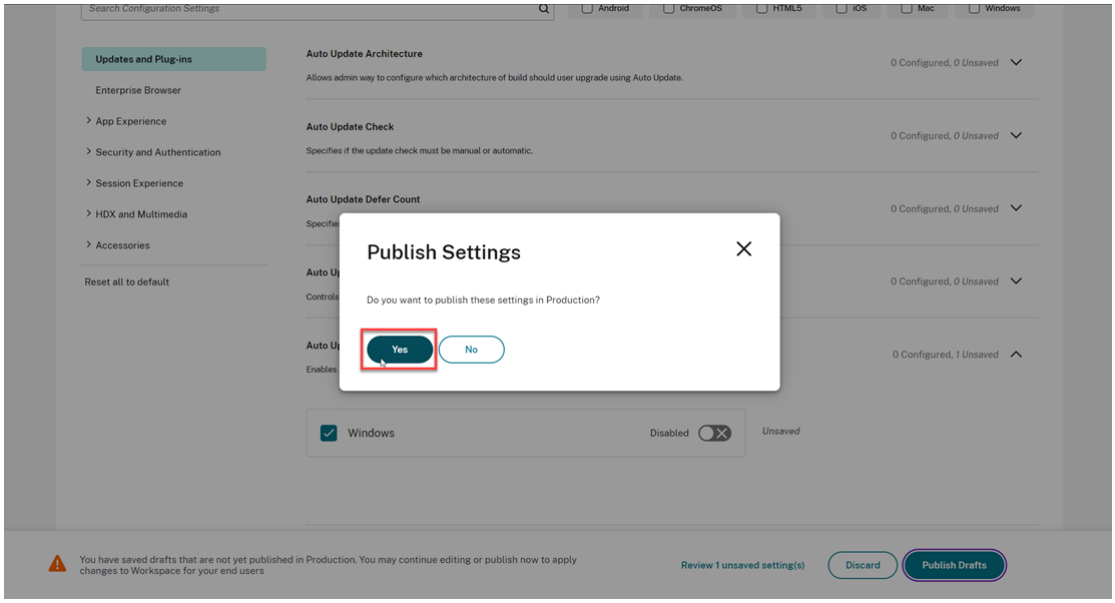



5. 单击 **Anti Key Logging**（反键盘记录），然后选择相关的操作系统（Windows 或 Mac）。
6. 单击 **Enabled**（已启用）切换按钮，然后单击 **Publish Drafts**（发布草稿）。




7. 在发布设置对话框中，单击是。




### 使用 **Global App Configuration Service API**

管理员可以使用 API 配置这些 App Protection 功能。设置如下所示：

- 用于启用或禁用防屏幕捕获的设置：

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

- 用于启用或禁用反键盘记录的设置：

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

示例：下面是在 GACS 中为 Citrix Workspace 应用程序启用防屏幕捕获和反键盘记录功能的示例 JSON 文件：

```
{

        "category": "App Protection",

        "userOverride": true,

        "assignedTo": [

          "AllUsersNoAuthentication"

        ],

        "settings": [

          {
```

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

对身份验证管理器使用 **AuthManConfig.xml**

请按如下所示导航到 $ICAROOT/config/AuthManConfig.xml 并编辑该文件：

```
1  /opt/Citrix/ICAClient/config$ cat AuthManConfig.xml | grep -i
       authmananti -A 1
2      <key>AuthManAntiScreenCaptureEnabled</key>
3      <value>true</value>
4      <key>AuthManAntiKeyLoggingEnabled</key>
5      <value>true </value>
6
7  <!--NeedCopy-->
```

对自助服务插件界面使用 **AuthManConfig.xml**

请按如下所示导航到 $ICAROOT/config/AuthManConfig.xml 并编辑该文件：

```
1  /opt/Citrix/ICAClient/config$ cat AuthManConfig.xml | grep -i
       protection -A 4
2  <!-- Selfservice App Protection configuration -->
3      <Selfservice>
4        <AntiScreenCaptureEnabled>true</AntiScreenCaptureEnabled>
5        <AntiKeyLoggingEnabled>true</AntiKeyLoggingEnabled>
6      </Selfservice>
7
8  <!--NeedCopy-->
```

### 为 **Virtual Apps and Desktops** 配置反键盘记录和防屏幕捕获

两个策略在会话中提供了反键盘记录和防屏幕捕获功能。可以按如下所示为 Virtual Apps and Desktops 配置反键盘记录和防屏幕捕获：

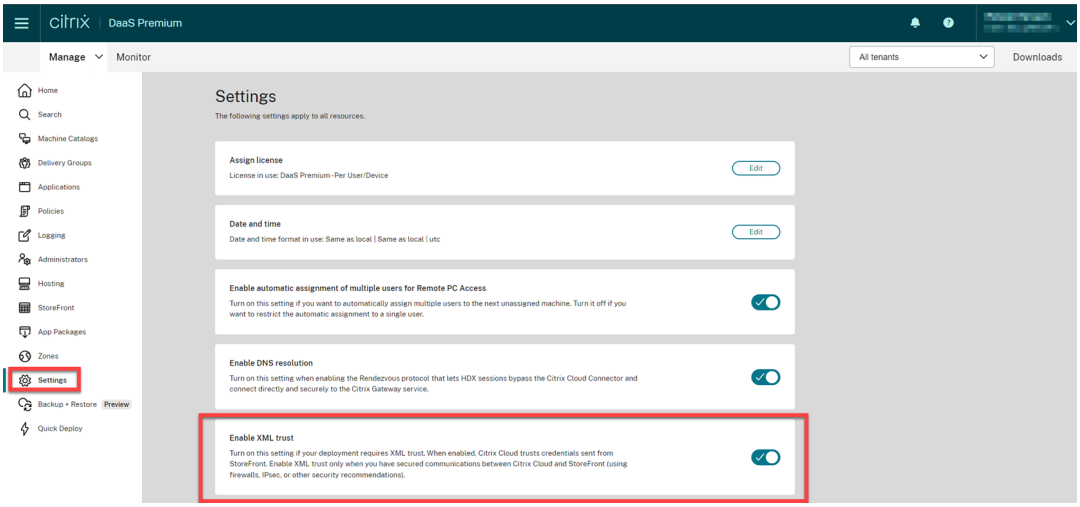
> 注意：
>
> 自版本 2103 起，Citrix DaaS 支持对 StoreFront 和 Workspace 使用 App Protection。

#### 使用 **Web Studio**

要通过 Web Studio 为 Citrix Virtual Apps 或 Citrix Virtual Desktops 配置反键盘记录和防屏幕捕获，请执行以下步骤：

1. App Protection 需要 XML 信任。要启用 XML 信任，请执行以下步骤：

   a) 登录您的 Citrix DaaS 帐户，然后转至管理 > 设置 > 启用 **XML** 信任。



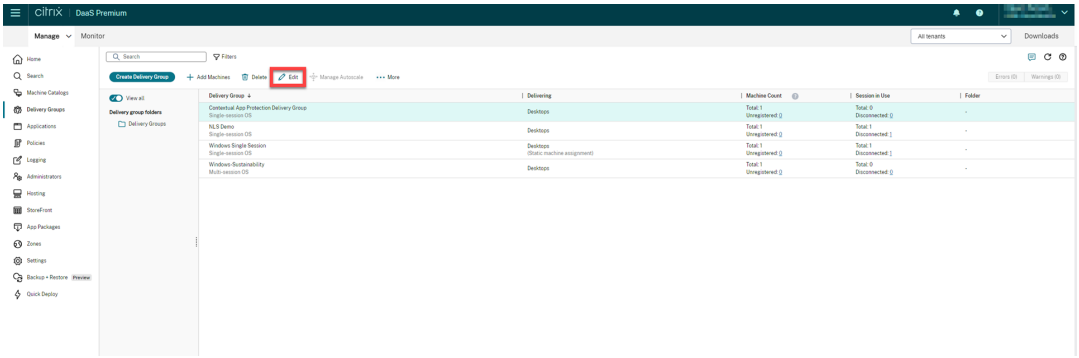

   b) 打开启用 **XML** 信任开关。

2. 要为交付组选择一种 App Protection 方法，请执行以下步骤：

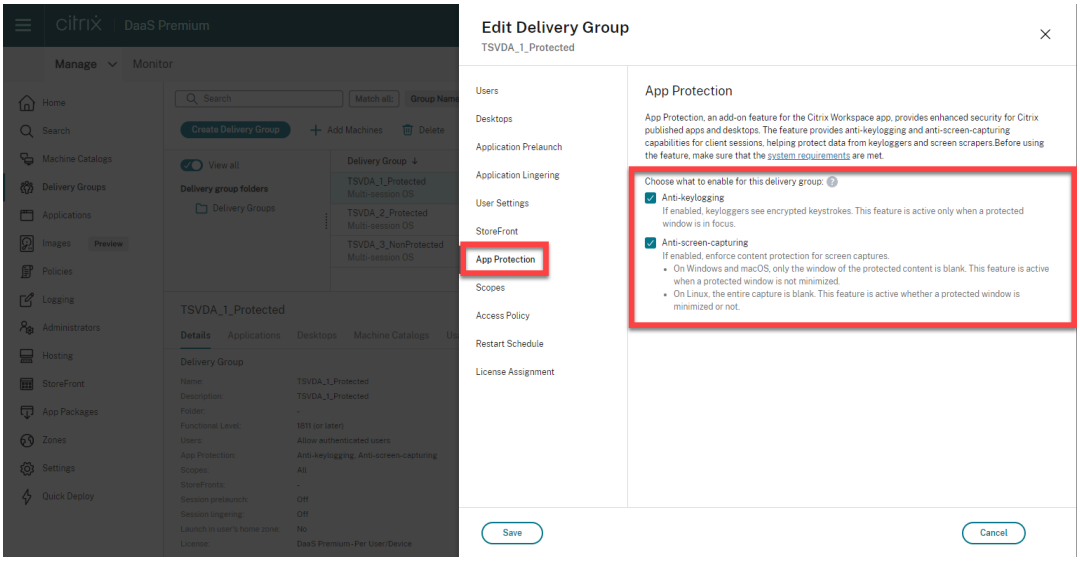
   a) 在 Citrix DaaS 中，转至管理 > 交付组。

   b) 选择一个交付组，然后在操作栏中单击编辑。



c) 单击 **App Protection**，然后选择反键盘记录和防屏幕捕获复选框。




d) 单击保存。

### 使用 **PowerShell**

> 注意：
>
> 在 Citrix DaaS 环境中，请在任何计算机（Citrix Cloud Connector 计算机除外）上使用 Citrix Virtual Apps and Desktops 远程 PowerShell SDK 中的 cmdlet 执行此部分中的命令。

在任何安装了 Delivery Controller 的计算机上或安装了独立 Studio 以及 FMA PowerShell 管理单元的计算机上，使用 Citrix Virtual Apps and Desktops SDK 为 App Protection 交付组启用以下属性。

- `AppProtectionKeyLoggingRequired`: `True`
- `AppProtectionScreenCaptureRequired`: `True`

可以为每个交付组单独启用其中的每个策略。例如，可以仅为 DG1 配置键盘记录保护，仅为 DG2 配置屏幕捕获保护。可以为 DG3 启用这两个策略。

示例：

要为名为 **DG3** 的交付组启用这两个策略，请在站点中的任何 Delivery Controller 上运行以下命令：

```
Set-BrokerDesktopGroup -Name DG3 -AppProtectionKeyLoggingRequired
$true -AppProtectionScreenCaptureRequired $true
```

要验证设置，请运行以下 cmdlet：

```
Get-BrokerDesktopGroup -Property Name, AppProtectionKeyLoggingRequired
, AppProtectionScreenCaptureRequired | Format-Table -AutoSize
```

此外，请启用 XML 信任：

```
Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
```

请务必保护 StoreFront 与 Broker 之间的网络安全。有关详细信息，请参阅知识中心文章 CTX236929 和保护 XenApp 和 XenDesktop XML Service 的安全。

#### 为 **Web** 和 **SaaS** 应用程序配置反键盘记录和防屏幕捕获

对于适用于 Windows 的 Citrix Workspace 应用程序和适用于 Mac 的 Citrix Workspace 应用程序，Web 和 SaaS 应用程序在 Citrix Enterprise Browser 中打开。如果将这些应用程序配置为通过 Citrix Secure Private Access 使用 App Protection 策略，App Protection 将按选项卡应用。

请使用以下方法为 Web 和 SaaS 应用程序配置 App Protection：

- 要为适用于 Workspace 的 Web 和 SaaS 应用程序配置 App Protection，请参阅适用于 Citrix Workspace 的 Citrix Secure Private Access。
- 要为适用于 StoreFront 的 Web 和 SaaS 应用程序配置 App Protection，请参阅 StoreFront 支持 Citrix Secure Private Access。

## 配置反 **DLL** 注入

March 10, 2024

默认情况下，反 DLL 注入功能处于禁用状态。可以使用以下方法启用此功能：

- 组策略对象 (GPO)
- Global App Configuration Service (GACS)

#### 使用组策略对象进行配置

添加了以下策略来配置反 DLL 注入功能：

- 反 DLL 注入
- 反 DLL 注入模块允许列表

使用“反 **DLL** 注入”策略

使用此策略可启用或禁用反 DLL 注入功能。如果未配置此策略，反 DLL 注入功能将处于禁用状态。可能的值如下：

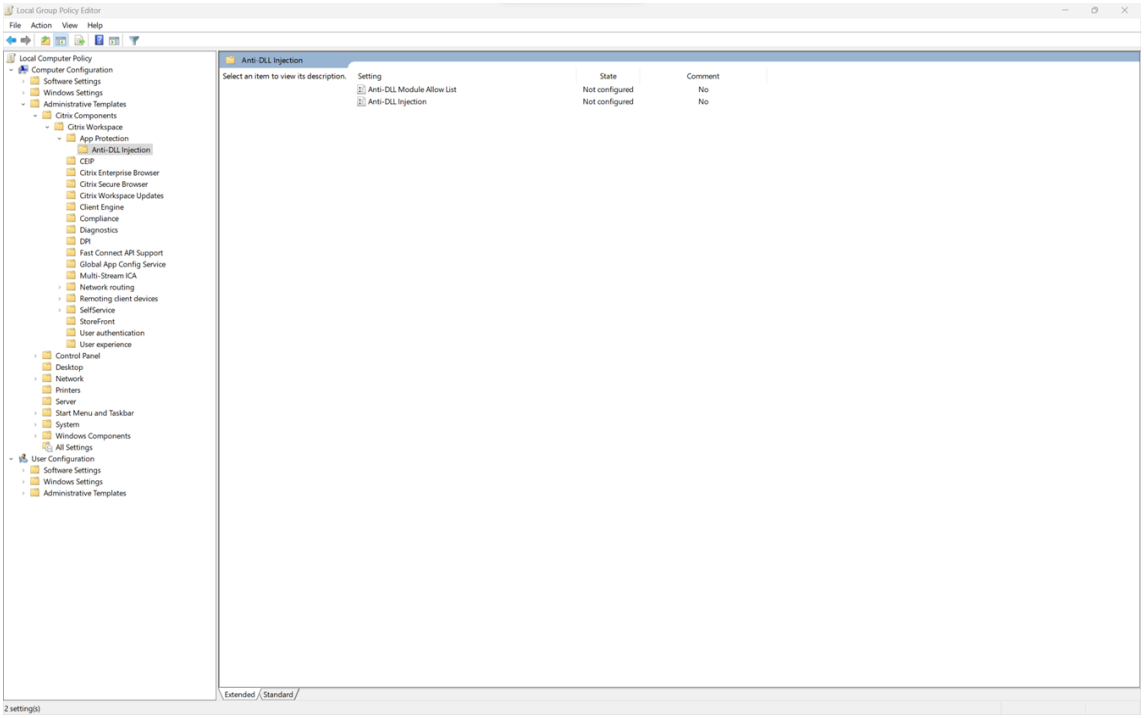
- 已启用 - 已为 Citrix Authentication Manager、Citrix Workspace 应用程序用户界面和 Citrix Virtual Apps and Desktops 启用反 DLL 注入功能。管理员可以选择所需的组件来启用反 DLL 注入功能。
- 已禁用 - 已为 Citrix Authentication Manager、Citrix Workspace 应用程序用户界面和 Citrix Virtual Apps and Desktops 禁用反 DLL 注入功能。

要启用反 DLL 注入策略，请执行以下步骤：

1. 请通过运行以下命令打开 Citrix Workspace 应用程序组策略对象管理模板：

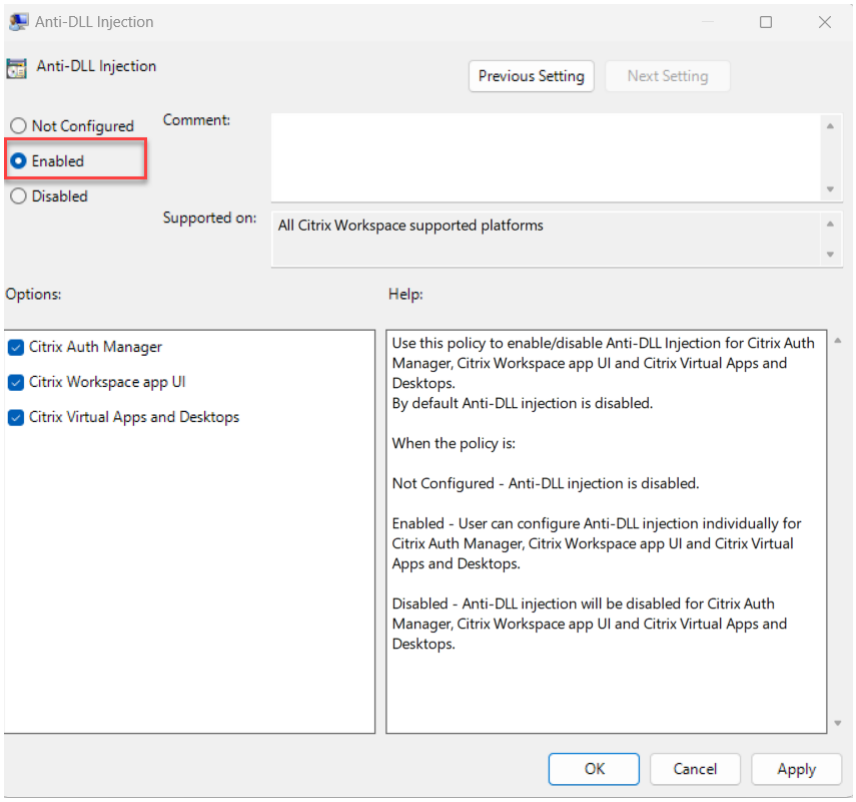
   ```
   gpedit.msc
   ```

2. 在计算机配置节点下，转到管理模板 > **Citrix** 组件 > **Citrix Workspace** > **App Protection** > **Anti-DLL Injection**（反 DLL 注入）。




3. 单击 **Anti-DLL Injection**（反 DLL 注入）策略并选择 **Enabled**（已启用）。所有组件均已选中。但是，您可以从 Options（选项）部分修改组件的选择。




4. 单击确定。

使用“反 **DLL** 注入模块允许列表”策略

作为管理员，您可以使用此策略将任何 DLL 排除在反 DLL 注入功能之外。Citrix 建议您仅使用此策略来处理任何异常情况。如果未配置此策略，则任何 DLL 都不是允许列表的一部分。所有 DLL 都包含在内，以提供反 DLL 保护。可能的值如下：

- 已启用 - 从反 DLL 保护中排除在允许列表中添加的 DLL。
- 已禁用 - 清除添加到允许列表中的 DLL 列表。

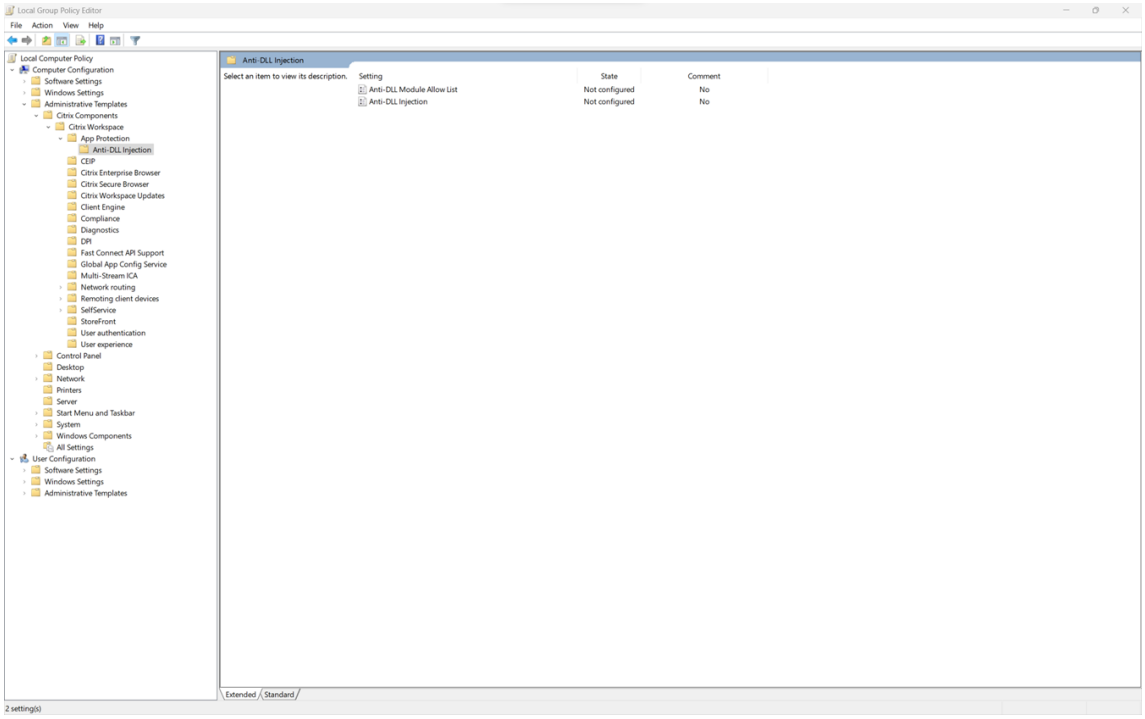
要启用“反 DLL 注入模块允许列表”策略，请执行以下步骤：

1. 请通过运行以下命令打开 Citrix Workspace 应用程序组策略对象管理模板：

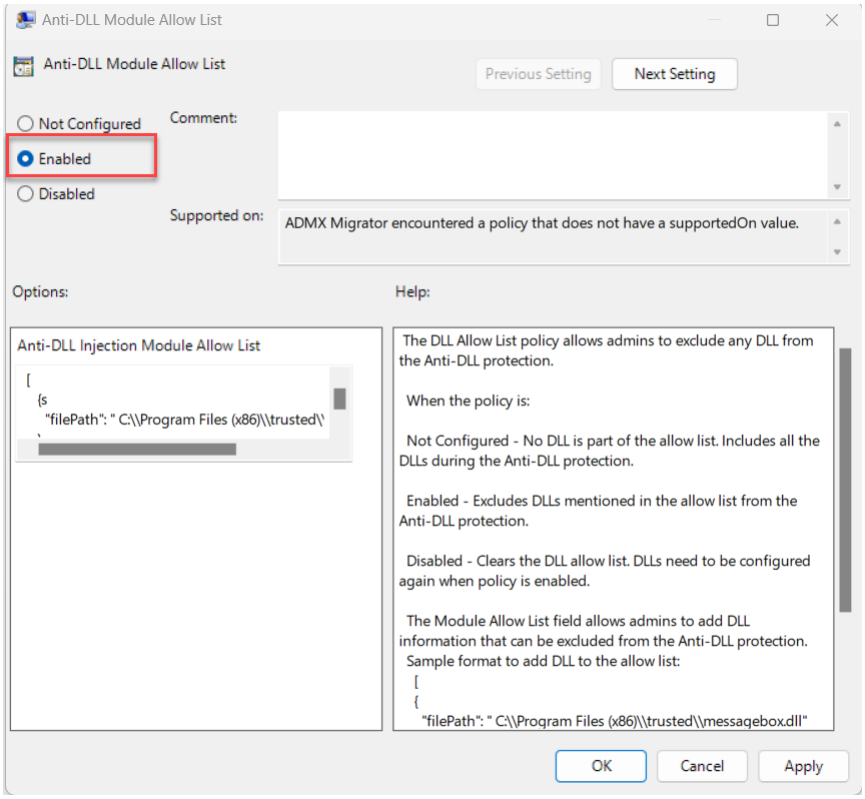
   ```
   gpedit.msc
   ```

2. 在计算机配置节点下，转到管理模板 > **Citrix** 组件 > **Citrix Workspace** > **App Protection** > **Anti-DLL Module Allow List**（反 DLL 模块允许列表）。




3. 单击 **Anti-DLL Module Allow List**（反 DLL 模块允许列表）策略并选择 **Enabled**（已启用）。




4. 在 **Anti-DLL Injection Module Allow List**（反 DLL 注入模块允许列表）字段中添加要从反 DLL 保护中排除的模块列表。

将 DLL 添加到允许列表的示例格式：

```
[
    {

        "filePath":"C:\Program Files (x86)\trusted\messagebox.dll"
     }
  ,
    {

        "filePath":"%PROGRAMFILES%\trusted\logging.dll"
     }

]
<!--NeedCopy-->
```

5. 单击确定。

### 使用 **Global App Configuration Service** 进行配置

管理员可以使用 GACS 配置反 DLL 注入功能。设置如下所示：

- 反 DLL 注入 - 添加您想要启用反 DLL 注入功能的必需模块
- 反 DLL 模块允许列表 - 添加要从反 DLL 保护中排除的必需 DLL

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

下面是在 GACS 中为适用于 Windows 的 Citrix Workspace 应用程序启用反 **dll** 注入和反 **dll** 模块允许列表的示例 JSON 文件：

```
{

  "serviceURL": {

    "url": "https://tuleshtest.cloudburrito.com:443"
   }
 ,
  "settings": {

    "appSettings": {

      "windows": [
        {

          "category": "App Protection",
          "userOverride": false,
          "assignedTo": [
            "AllUsersNoAuthentication"
          ],
          "assignmentPriority": 0,
          "settings": [
```

```
22              {
23
24                "name": "anti dll injection",
25                "value": [
26                  "Citrix Auth Manager",
27                  "Citrix Virtual Apps And Desktops",
28                  "Citrix Workspace app UI"
29                ]
30               }
31  ,
32              {
33
34                "name": "anti dll module allow list",
35                "value": [
36                  {
37
38                    "filePath": "C:\Program Files (x86)\Citrix\ICA Client
                        \wfica32.exe"
39                   }
40  ,
41                  {
42
43                    "filePath": "C:\Program Files (x86)\Citrix\ICA Client
                        \AuthManager\AuthManSvr.exe"
44                   }
45
46                ]
47               }
48
49            ]
50           }
51
52        ]
53       }
54  ,
55     "name": "name",
56     "description": "desc",
57     "useForAppConfig": true
58    }
59
60  }
61
62  <!--NeedCopy-->
```

配置策略篡改检测

March 10, 2024

必备条件

要配置策略篡改检测功能，请确保您具备以下条件：

- 适用于云部署 - Cloud Desktop Delivery Controller 版本 115 或更高版本
- 适用于本地部署 - Citrix Virtual Apps and Desktops 版本 2308 或更高版本
- Windows Virtual Delivery Agent 安装程序版本 2308 或更高版本
- 对于 Windows - 适用于 Windows 的 Citrix Workspace 应用程序 2309 或更高版本
- 对于 Mac - 适用于 Mac 的 Citrix Workspace 应用程序 2308 或更高版本
- 对于 Linux - 适用于 Linux 的 Citrix Workspace 应用程序 2308 或更高版本

要启用策略篡改检测，管理员必须在托管配置了 App Protection 的虚拟应用程序和桌面的 TS/WS VDA 上启动 **Citrix AppProtection Service**。

请执行以下步骤之一以启用策略篡改检测：

- 使用命令提示符：
  1. 在任务栏的最左边，单击搜索 图标。键入 **cmd**，然后单击以管理员身份运行。此时将出现命令提示符屏幕。
  2. 运行以下命令：

```
sc config ctxappprotectionsvc start=auto
sc start ctxappprotectionsvc

<!--NeedCopy-->
```

- 使用用户界面：
  1. 在任务栏的最左边，单击搜索 图标。键入 **services.msc**，然后按 **Enter** 键。此时将出现服务屏幕。
  2. 选择 **Citrix AppProtection Service**，然后单击启动。
  3. 右键单击 **Citrix AppProtection Service**，然后选择属性。
  4. 选择常规 > 启动类型 > 自动，然后单击确定，以确保该服务在系统启动时自动启动。

策略篡改检测功能已成功启用。

要检测和阻止不支持策略篡改检测的 Citrix Workspace 应用程序的早期版本，请配置 App Protection 状态检查。有关 App Protection 状态检查的详细信息，请参阅 App Protection 状态检查。

## 配置 App Protection 状态检查

March 10, 2024

要启用 App Protection 状态检查，请配置与此功能相关的新 VDA Citrix 策略。

### 必备条件

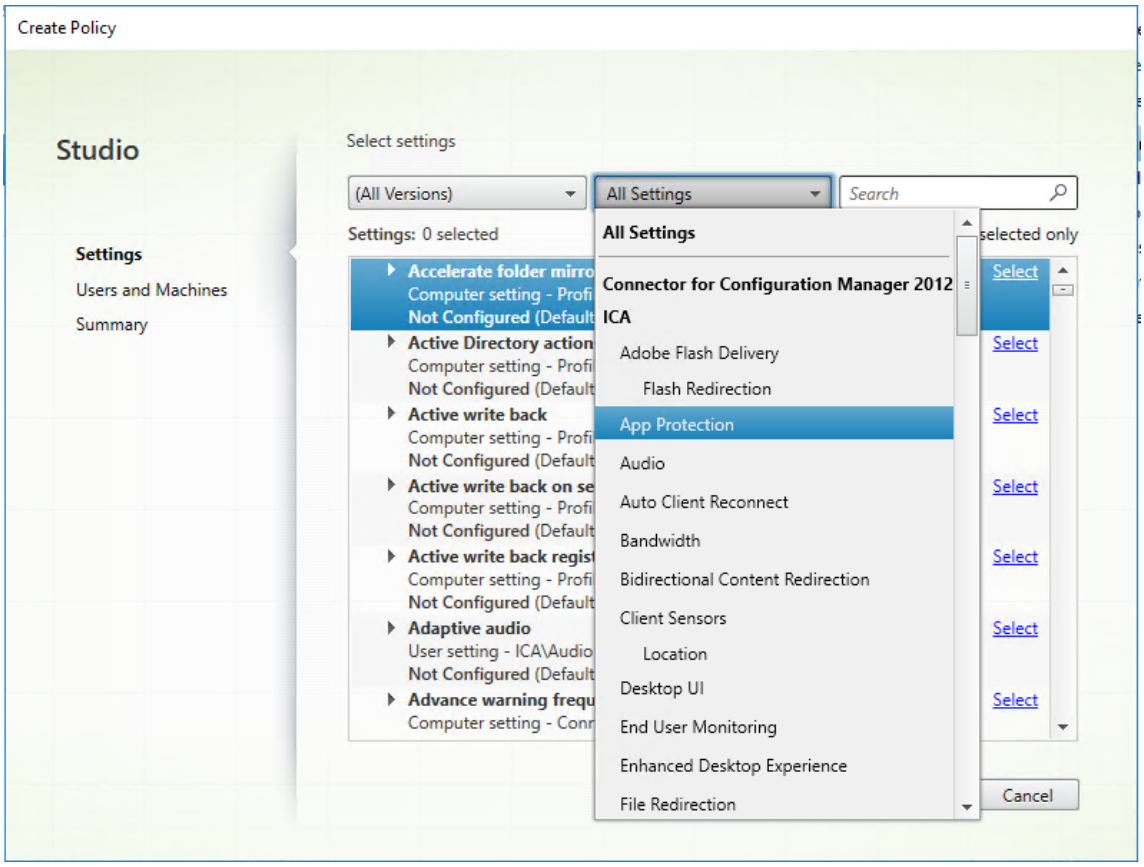
请确保您具备以下项：

- 适用于云部署 - Cloud Desktop Delivery Controller 版本 115 或更高版本
- 适用于本地部署 - Citrix Virtual Apps and Desktops 版本 2308 或更高版本
- Windows Virtual Delivery Agent 安装程序版本 2308 或更高版本
- 对于 Windows - 适用于 Windows 的 Citrix Workspace 应用程序 2309 或更高版本
- 对于 Mac - 适用于 Mac 的 Citrix Workspace 应用程序 2308 或更高版本
- 对于 Linux - 适用于 Linux 的 Citrix Workspace 应用程序 2308 或更高版本

请按如下所示配置适用于状态检查的新 VDA Citrix 策略：

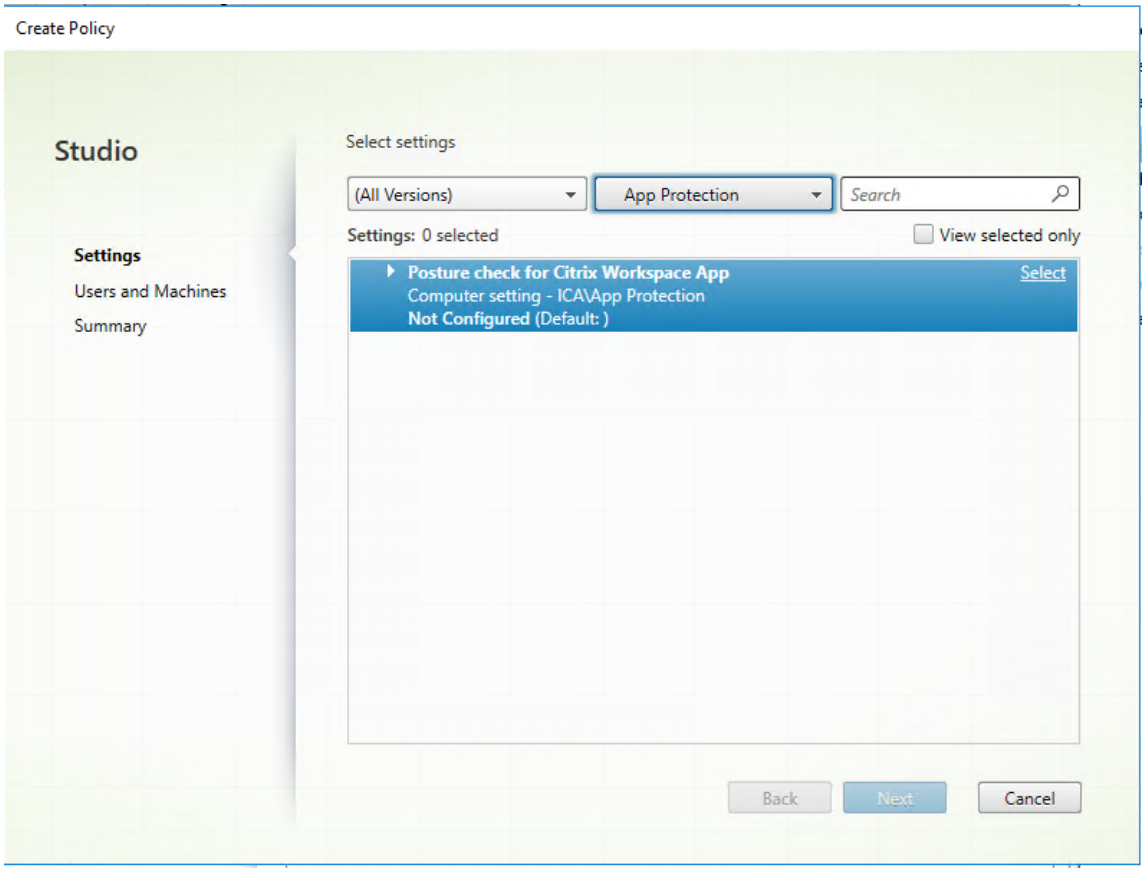
> 注意：
>
> 这项新的 VDA Citrix 策略可以同时使用 Citrix Studio 和 Web Studio 进行部署。以下过程是通过 Citrix Studio 部署的，您也可以对 Web Studio 使用相同的过程。

1. 在本地部署的 Desktop Delivery Controller (DDC) 上打开 Citrix Studio 应用程序，或者在云部署的 Web Studio 上打开 Citrix Studio 应用程序，然后选择策略。
2. 在操作下，选择策略 > 创建策略。
3. 单击所有设置下拉菜单，然后在 **ICA** 下选择 **App Protection**。



4. 选择 **Citrix Workspace** 应用程序的状态检查，然后单击选择。



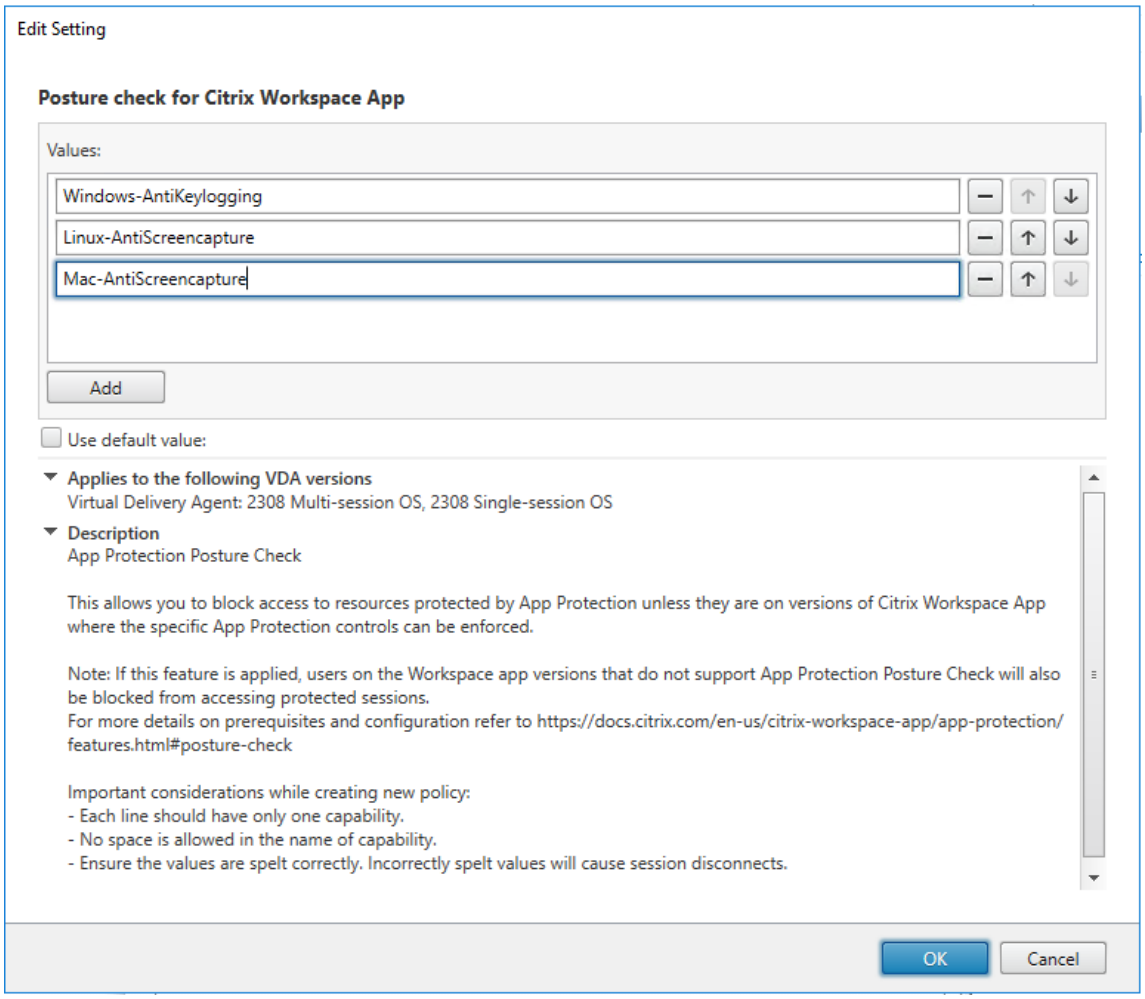

此时将显示编辑设置窗口。

5. 清除使用默认值复选框。
6. 单击添加并输入以下对象中的相关值：

   - Windows-AntiScreencapture
   - Windows-AntiKeylogging
   - Linux-AntiScreencapture
   - Linux-AntiKeylogging
   - Mac-AntiScreencapture
   - Mac-AntiKeylogging

   例如，如果您添加了“Windows-AntiScreencapture”和“Windows-AntiKeylogging”，则允许支持状态检查并且具有这些功能的适用于 Windows 的 Citrix Workspace 应用程序连接到 VDA。

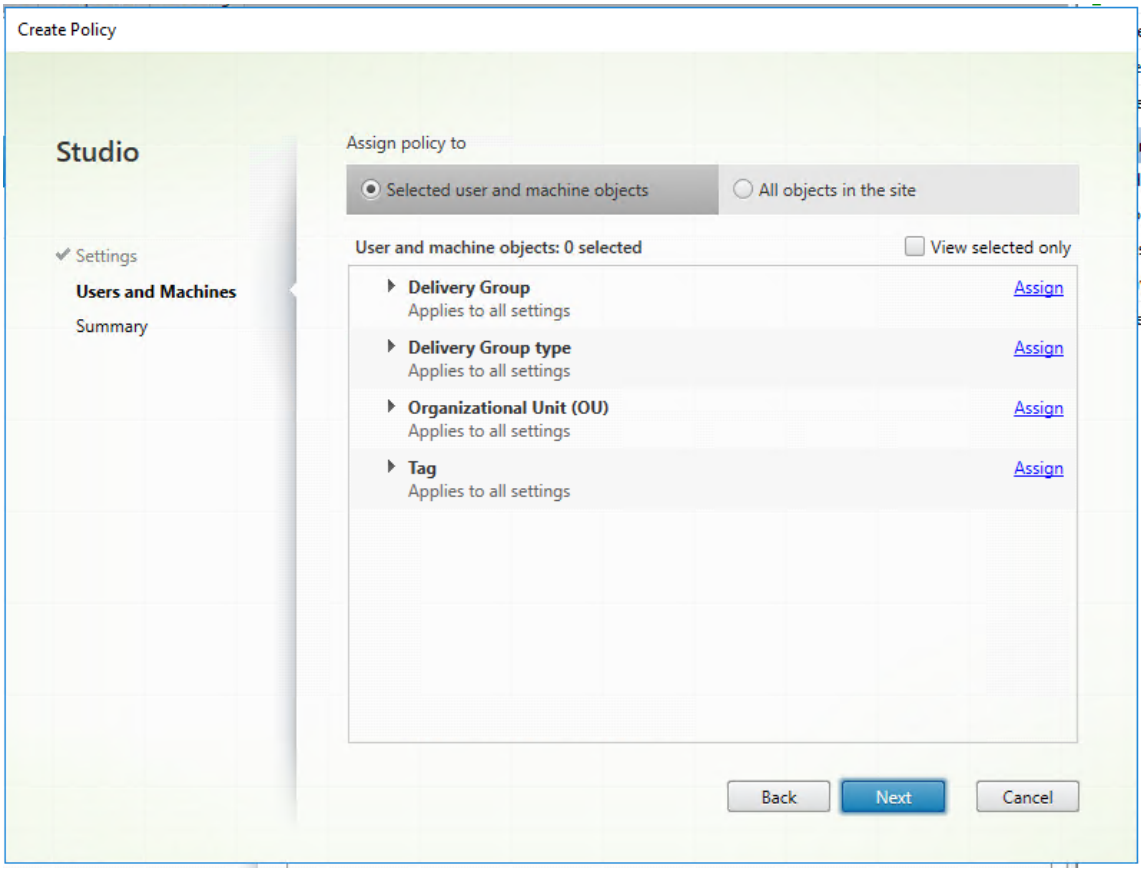
 




> 注意：
>
> - 每个条目只能有一个功能。
> - 不允许在功能名称中使用空格。
> - 请确保值拼写正确。拼写值不正确会导致会话终止。
> - 没有前缀 Windows-、Linux- 或 Mac- 的值将被忽略。

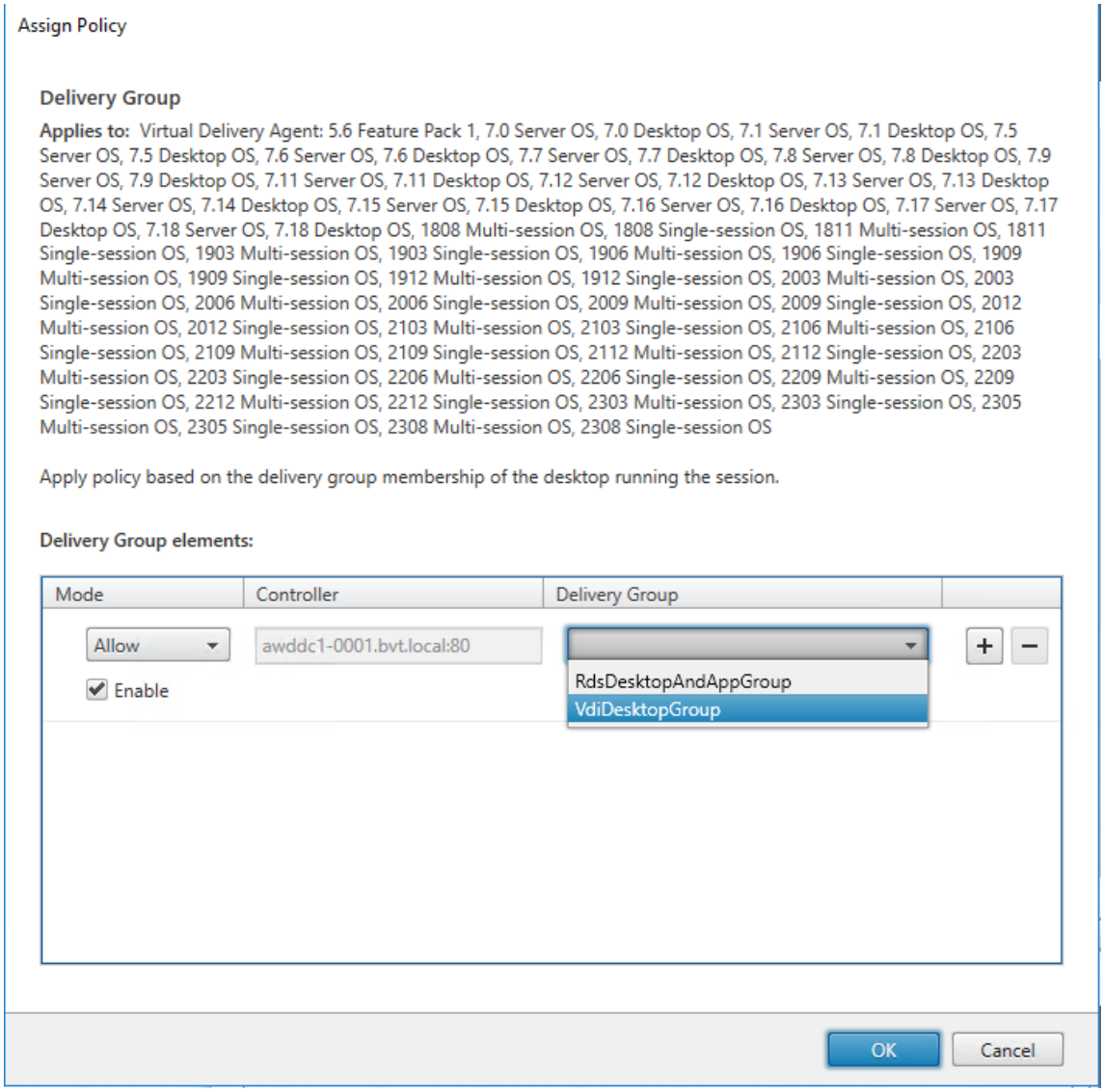
7. 添加所有必需值后，单击确定。
8. 单击下一步。
9. 选择将策略分配给 > 所选用户和计算机对象。



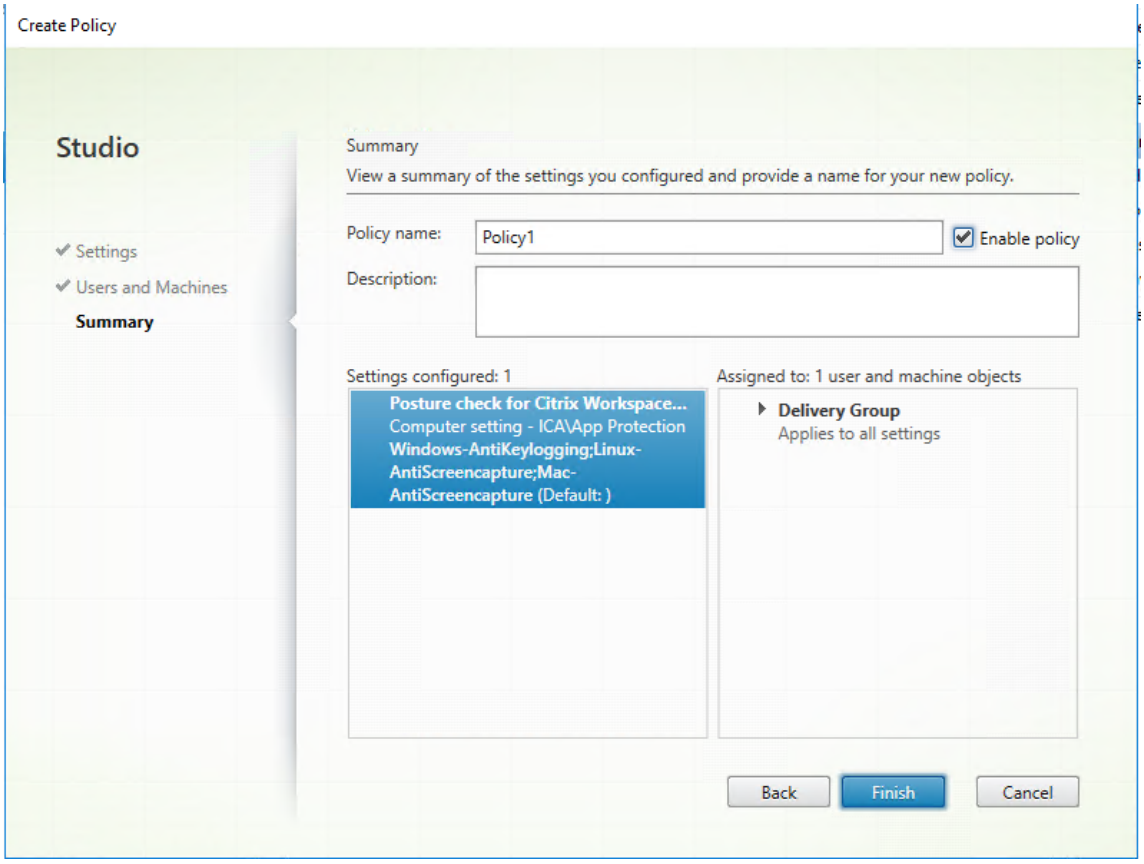

10. 选择必须部署此策略的所需交付组，然后单击确定。




11. 单击下一步。
12. 在策略名称字段中输入策略名称，然后选中启用策略复选框。

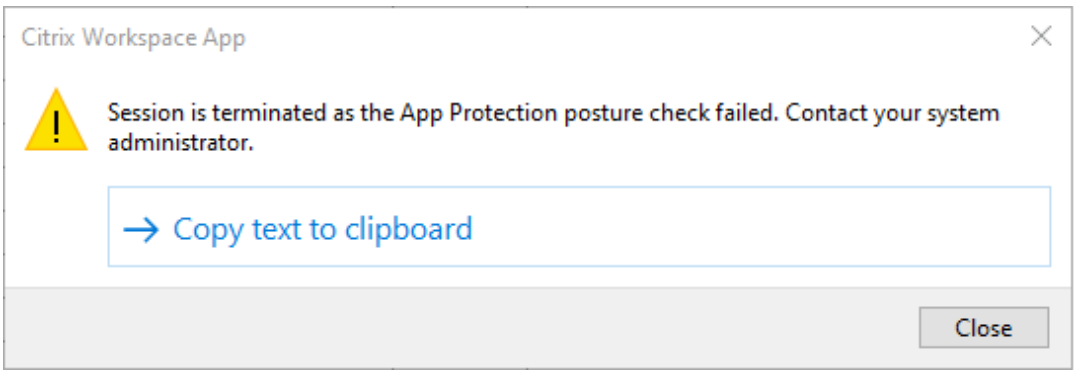



13. 单击完成。

状态检查策略已创建。

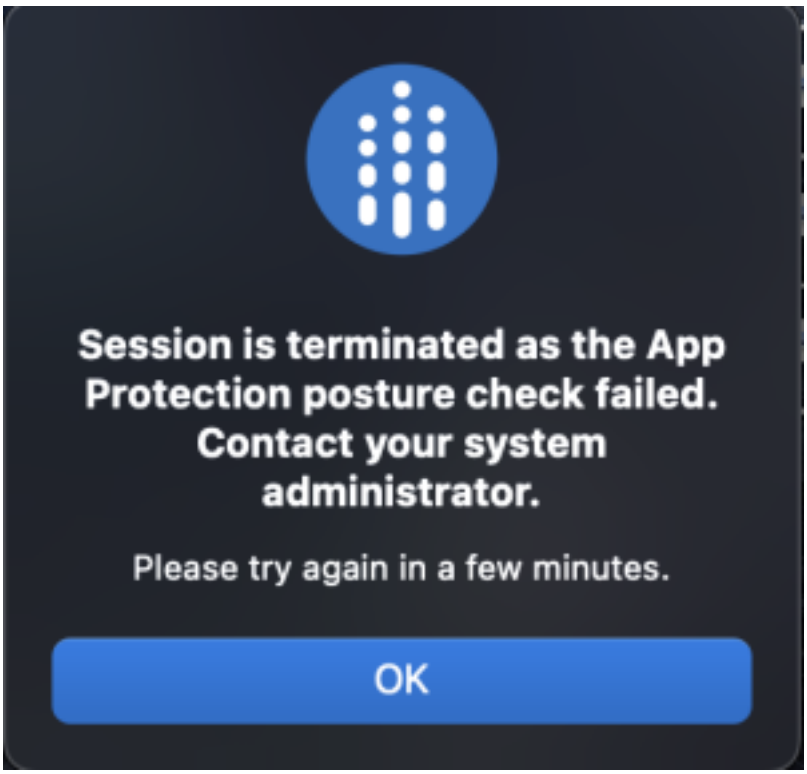
### App Protection 状态检查失败时的预期行为

- 如果启用了状态检查 VDA Citrix 策略，并且您使用的是不支持状态检查功能的 Citrix Workspace 应用程序版本，会话将终止，而不会显示任何错误消息。
- 如果您使用的是支持状态检查功能的 Citrix Workspace 应用程序版本，会话将终止并分别显示以下错误消息：
  - Windows：

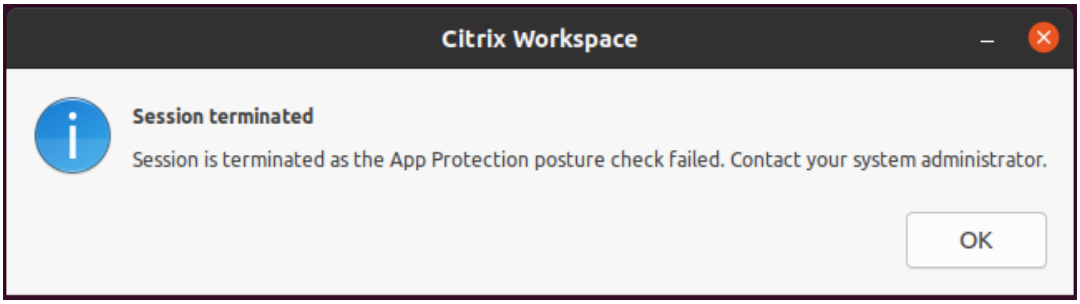


- Mac




- Linux




## 阻止 **DoubleHop** 启动

March 10, 2024

要阻止双跃点启动，请确保您在第一个跃点上运行适用于 Windows 的 Citrix Workspace 应用程序 2309 或更高版本。

请在第一个跃点上将以下配置部署到所有 VDA：

1. 更新最新的 GPO 策略。有关详细信息，请参阅更新最新的 GPO 策略。

2. 启动组策略编辑器，然后转到计算机配置 > 管理模板 > **Citrix** 组件 > **Citrix Workspace** > **App Protection** > 阻止 **DoubleHop** 启动。
3. 选择已启用，然后单击确定。

   阻止 **DoubleHop** 启动设置已启用，如果您尝试执行双跃点启动，您将被阻止。

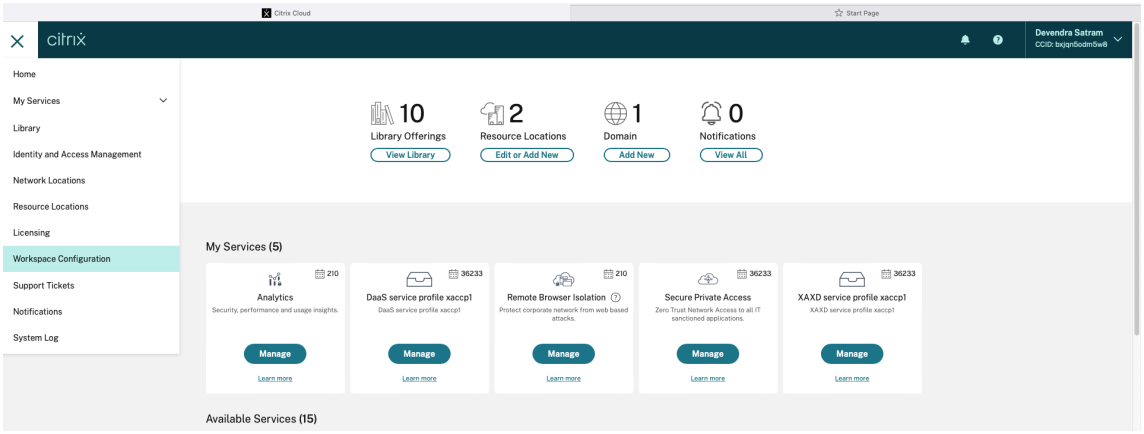
> 注意：
>
> Windows Server 操作系统不支持 App Protection。因此，如果您在第一个跃点上运行 Windows Server 操作系统，则不会显示启用了 App Protection 的 Virtual Apps and Desktops。

## 配置屏幕捕获允许列表

April 25, 2024

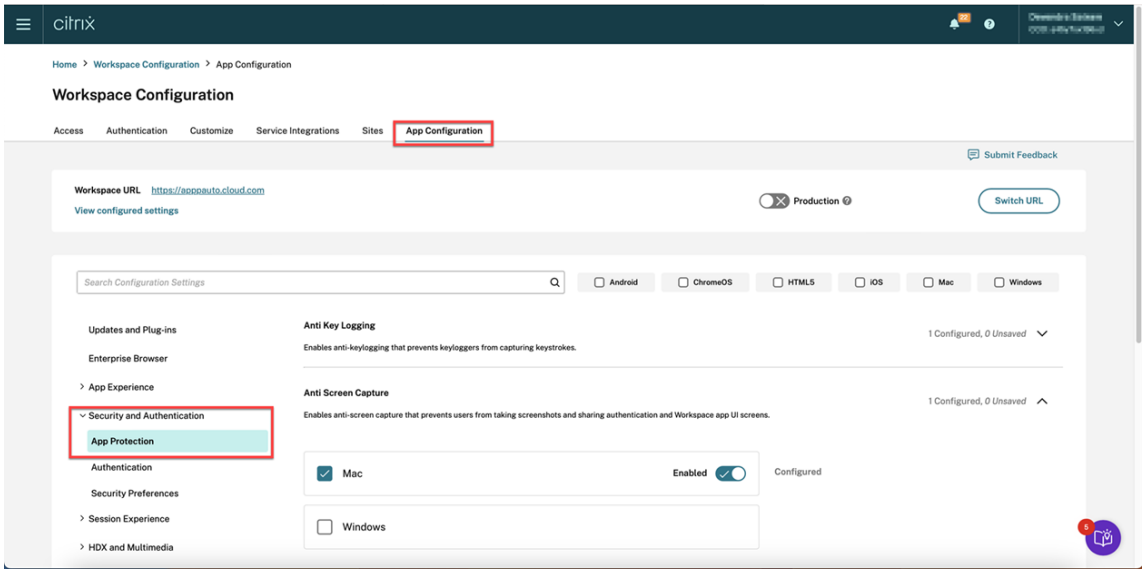
要将应用程序添加到屏幕捕获允许列表中，请执行以下步骤：

1. 登录到您的 Citrix Cloud 帐户并选择 **Workspace** 配置。

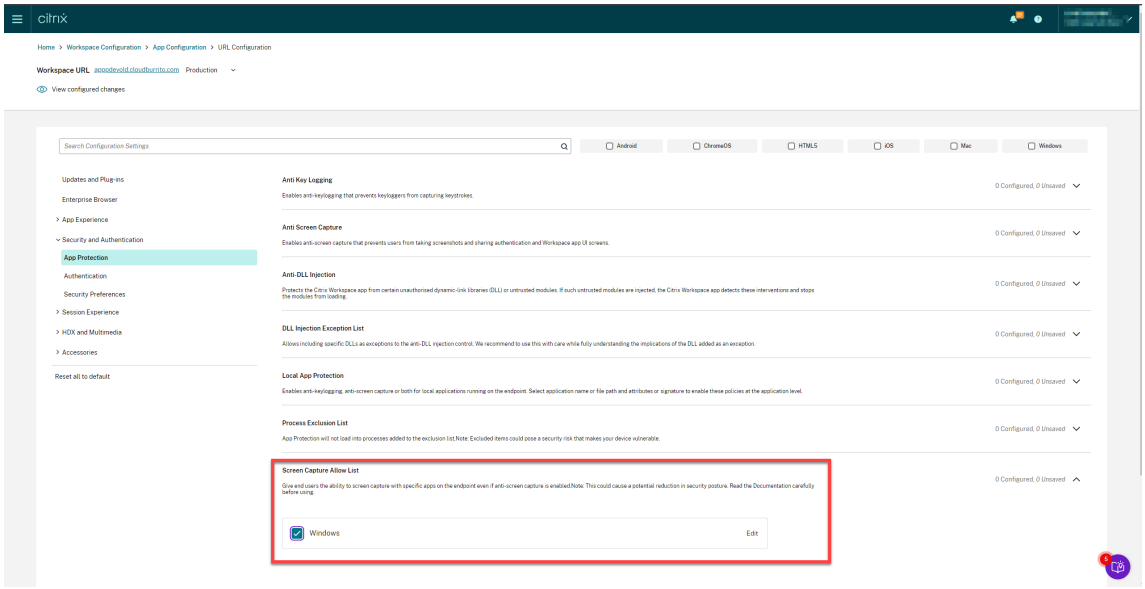



2. 选择 **App Configuration**（应用程序配置）> **Security and Authentication**（安全性和身份验证）**Configure**（配置）> **App Protection**。




3. 单击 **Screen Capture Allow List**（屏幕捕获允许列表），然后选中 **Windows** 复选框。




4. 单击 **Edit**（编辑）选项。

   此时将出现 **Manage settings for Windows**（管理 Windows 设置）屏幕。

5. 将要添加的应用程序的相关信息添加到屏幕捕获允许列表中。

   例如，

```
[
 {

 "name": "ScreenshotTool_1.exe",
 "signature": "ScreenshotTool_1 Signature",
 "publisher": "ScreenshotTool_1 Publisher"
  }
```

```
  ,
  {

   "name": "Screenshottool_2.exe",
   "signature": "",
   "publisher": ""
   }

]
<!--NeedCopy-->
```

## Manage settings for Windows


Save draft Cancel

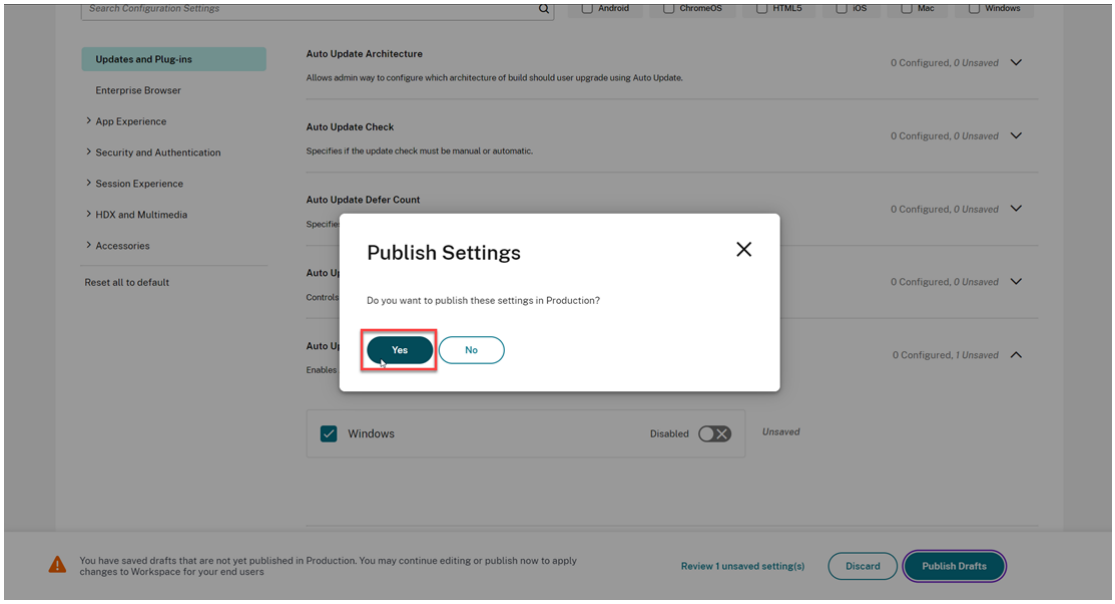
注意：

- name 为必填字段。同时，publisher 和 signature 不是必填字段。但是，建议添加相关的 publisher 和 signature 以确保只有允许列出的应用程序才能创建屏幕截图。
- 如果未设置 publisher 和 signature 值，同名的恶意应用程序可以捕获屏幕截图。
- 此外，您可以通过在此块中添加多个条目将多个应用程序添加到“屏幕截图允许列表”中。

要获取 publisher 和 signature 信息，请参阅获取 publisher 和 signature 信息。

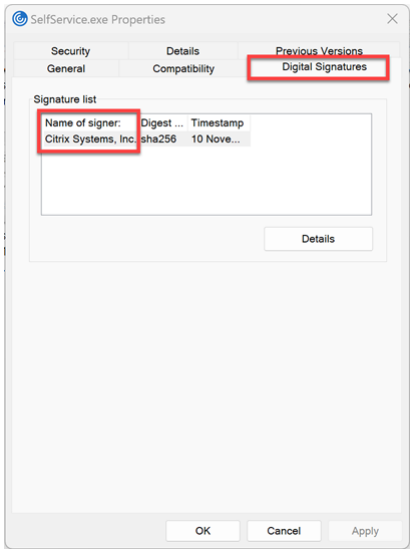
6. 单击 **Save draft**（保存草稿），然后单击 **Publish Drafts**（发布草稿）。
7. 在 **Publish Settings**（发布设置）对话框中，单击 **Yes**（是）。




## 获取 `publisher` 和 `signature` 信息

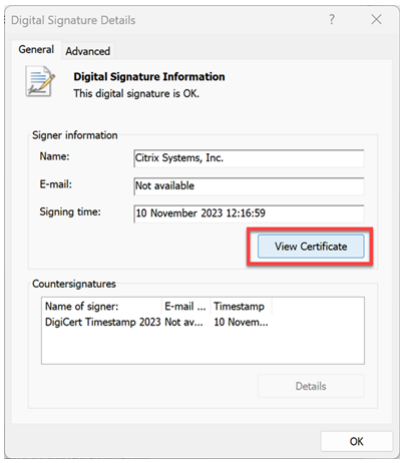
要获取 `publisher` 和 `signature` 信息，请执行以下步骤：

1. 打开保存应用程序的相关 `.exe` 文件的文件位置。
2. 右键单击 `.exe` 文件，然后单击属性。此时将出现一个属性弹出屏幕。
3. 单击 **Digital Signatures**（数字签名）。**Name of signer**（签名者姓名）为 `publisher` 值。

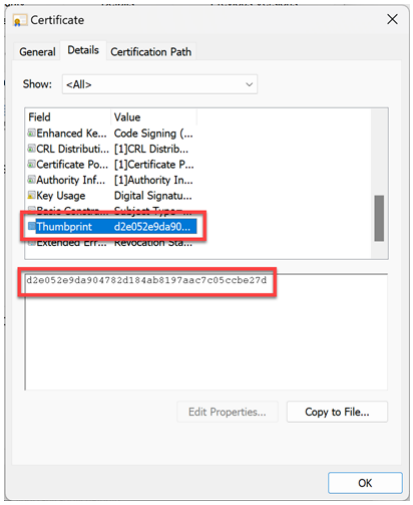


4. 单击 **Name of signer**（签名者姓名）中的第一个条目，然后单击 **Details**（详细信息）> **View Certificate**（查看证书）。




5. 单击 **Details**（详细信息）> **Thumbprint**（指纹）。文本框中显示的内容为 `signature`。



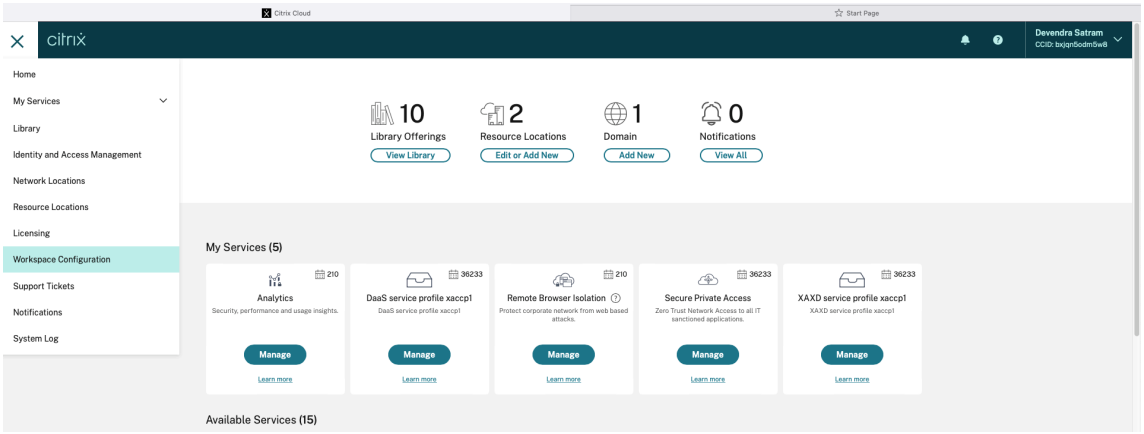

## 配置进程排除列表

April 29, 2024

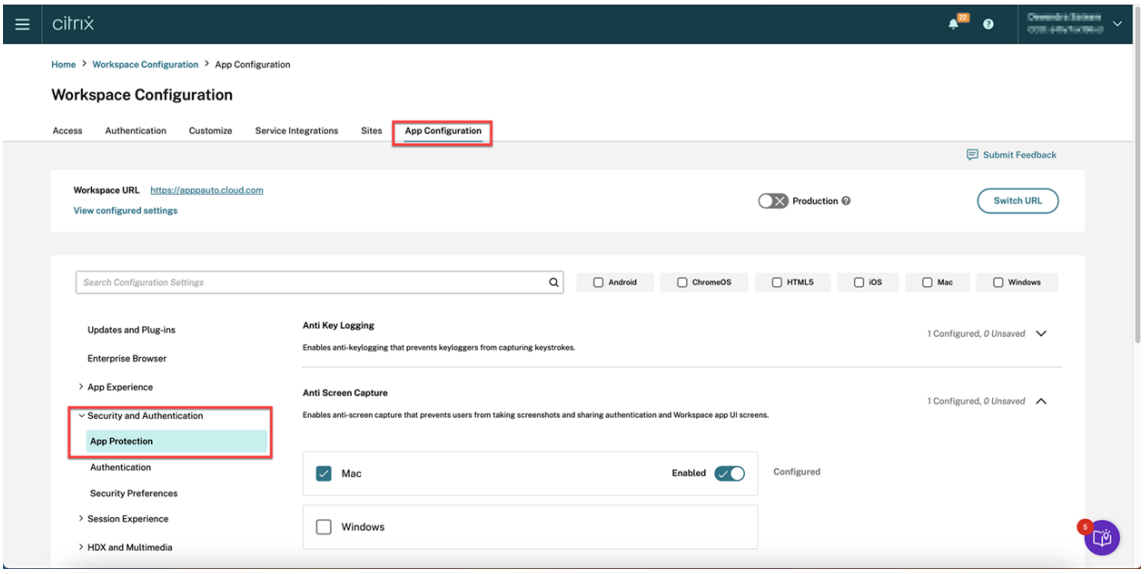
要将流程添加到进程排除列表中，请执行以下步骤：

1. 登录到您的 Citrix Cloud 帐户并选择 **Workspace** 配置。

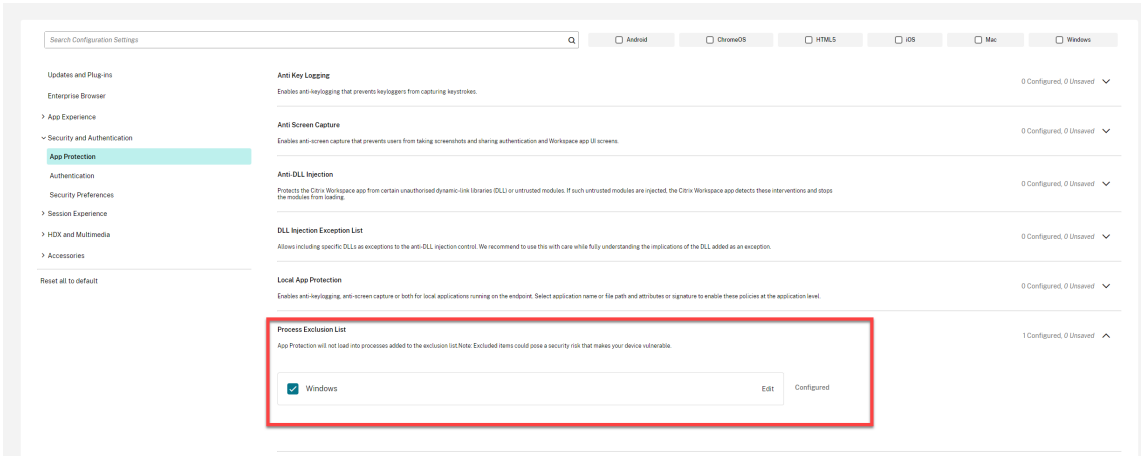
 




2. 选择 **App Configuration**（应用程序配置）> **Security and Authentication**（安全性和身份验证）**Configure**（配置）> **App Protection**。




3. 单击 **Process Exclusion List**（进程排除列表），然后选中 **Windows** 复选框。




4. 单击 **Edit**（编辑）选项。

此时将出现 **Manage settings for Windows**（管理 Windows 设置）屏幕。

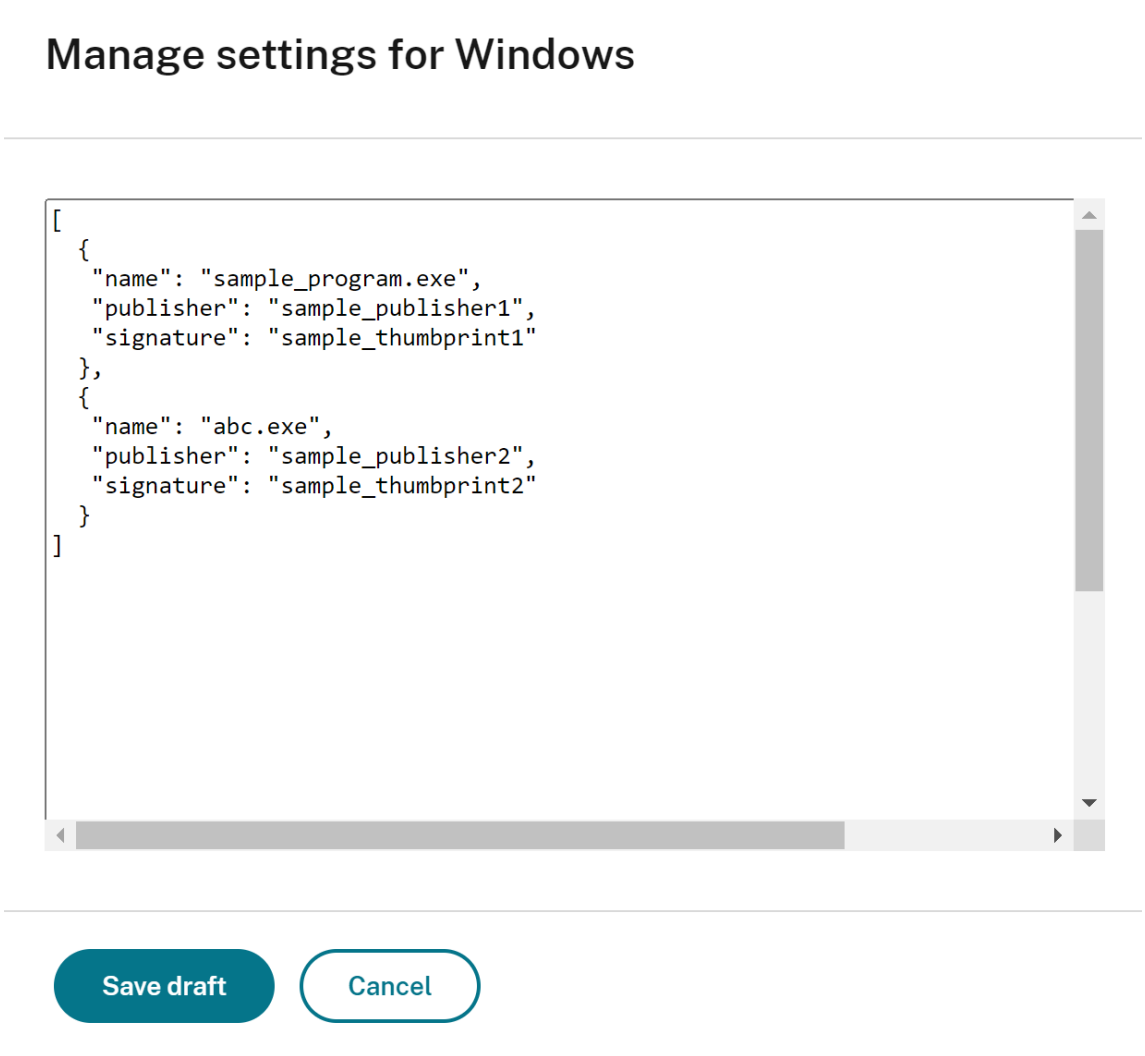
5. 将要添加的进程的相关信息添加到进程排除列表中。

例如，

```
[
 {

  "name": "sample_program.exe",
  "publisher": "sample_publisher1",
  "signature": "sample_thumbprint1"
  }

]
<!--NeedCopy-->
```



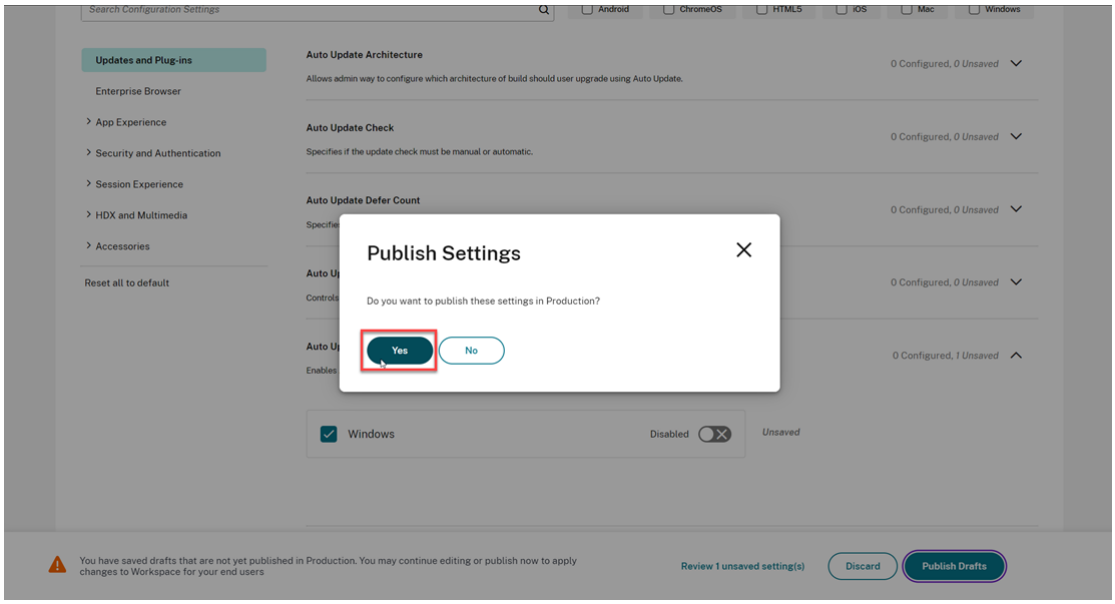

> 注意：
>
> - `name` 为必填字段。同时，`publisher` 和 `signature` 不是必填字段。但是，建议添加

> `publisher` 和 `signature` 以确保将正确的流程添加到该列表中。
> - 此外，您可以通过在此块中添加多个条目来将多个进程添加到进程排除列表中。

要获取 `publisher` 和 `signature` 信息，请参阅获取 `publisher` 和 `signature` 信息。

6. 单击 **Save draft**（保存草稿），然后单击 **Publish Drafts**（发布草稿）。
7. 在 **Publish Settings**（发布设置）对话框中，单击 **Yes**（是）。




8. 重新启动 Citrix Workspace 应用程序。

## 配置 USB 过滤器驱动程序排除列表

April 29, 2024

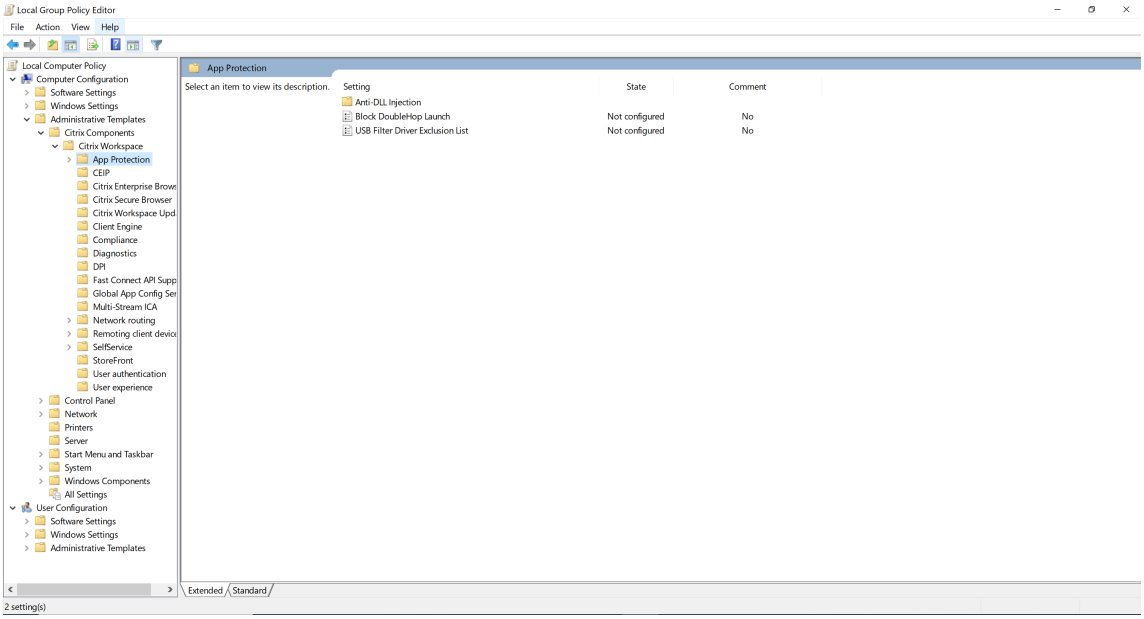
可以使用以下方法之一将 USB 设备添加到 USB 过滤器驱动程序排除列表中：

- 使用组策略对象
- 使用 Global App Configuration Service 用户界面

### 使用组策略对象

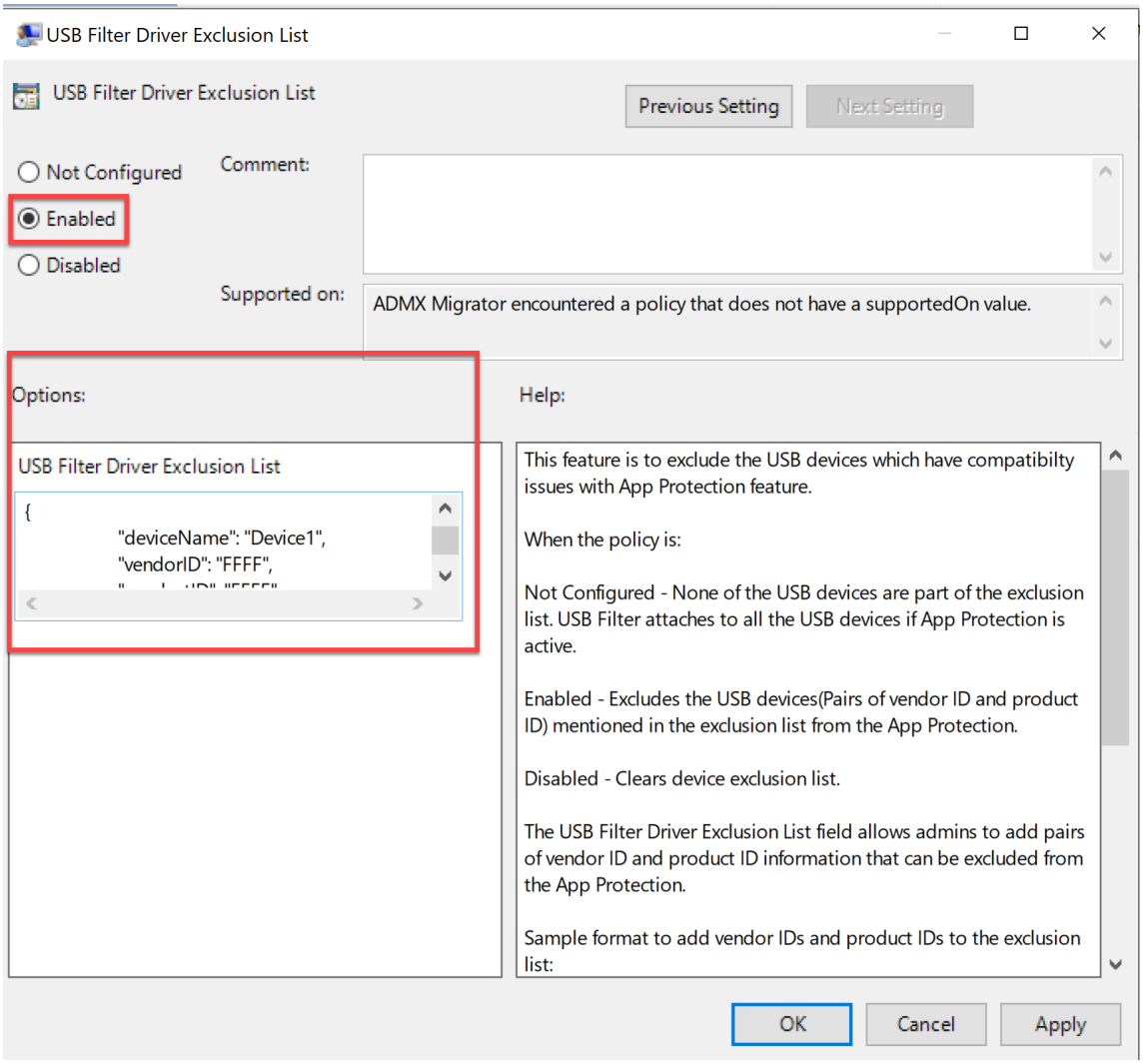
1. 通过运行 `gpedit.msc` 打开 Citrix Workspace 应用程序组策略对象管理模板。有关详细信息，请参阅组策略对象。
2. 在计算机配置节点下，转到管理模板 > **Citrix Components**（Citrix 组件）> **Citrix Workspace** > **App Protection** > **USB Filter Driver Exclusion List**（USB 过滤器驱动程序排除列表）。




3. 选择 **Enabled**（已启用），然后在 **Options**（选项）文本框中输入要排除的 USB 设备的 **Vendor ID**（供应商 ID）和 **Product ID**（产品 ID）。




> 注意：
>
> - `productID` 和 `vendorID` 为必填字段。同时，`deviceName` 不是必填字段。
> - 此外，您可以通过在此块中添加多个条目将多个 USB 设备添加到排除列表中。

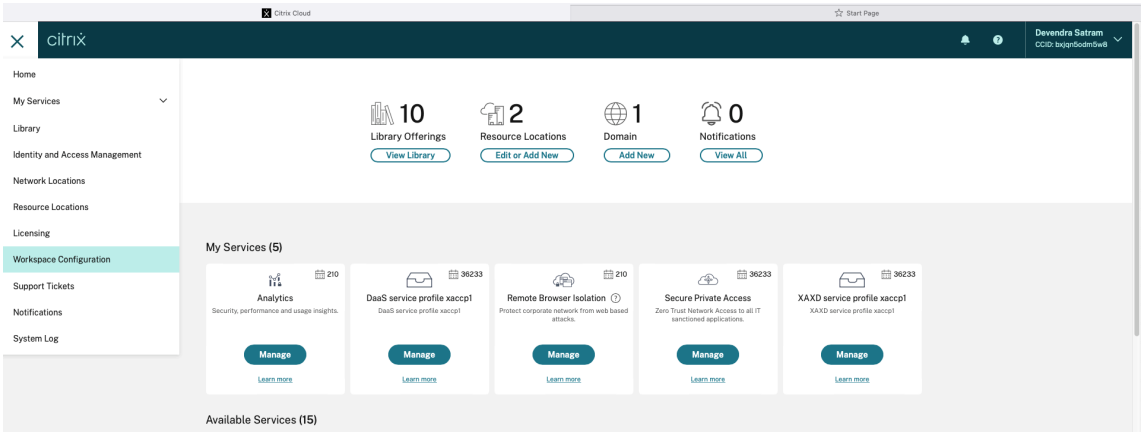
要获取 `productID` 和 `vendorID`，请参阅获取 `productID` 和 `vendorID`。

4. 单击确定。

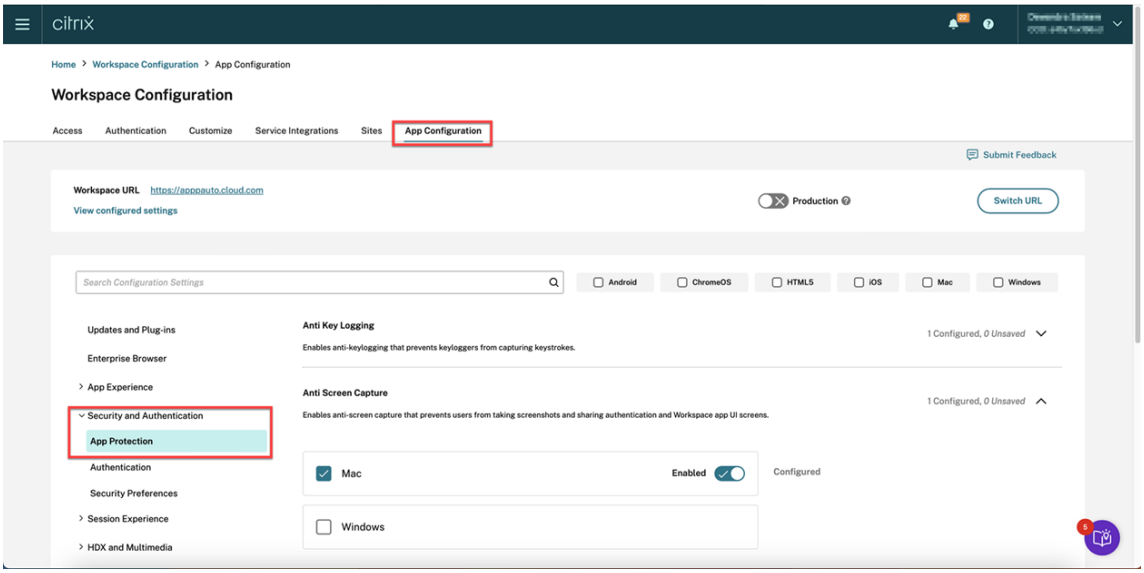
### 使用 **Global App Configuration Service** 用户界面

1. 登录到您的 Citrix Cloud 帐户并选择 **Workspace** 配置。

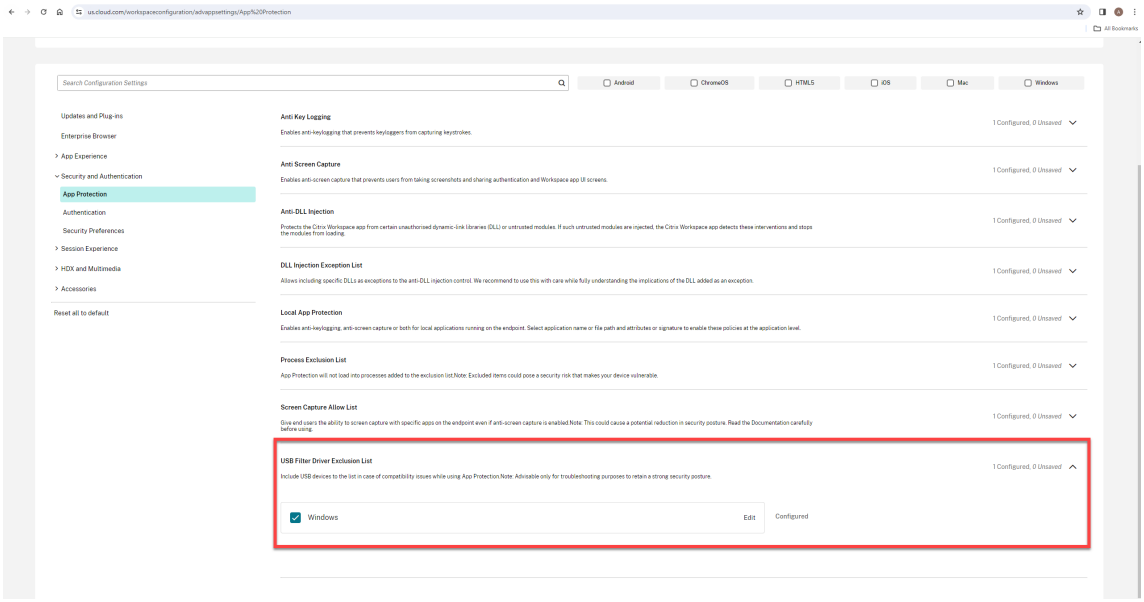



2. 选择 **App Configuration**（应用程序配置）> **Security and Authentication**（安全性和身份验证）**Configure**（配置）> **App Protection**。




3. 单击 **USB Filter Driver Exclusion List**（USB 过滤器驱动程序排除列表），然后选中 **Windows** 复选框。




4. 单击 **Edit**（编辑）选项。

   此时将出现 **Manage settings for Windows**（管理 Windows 设置）屏幕。

5. 将有关要添加的进程或应用程序的信息添加到“USB 过滤器驱动程序排除列表”中。

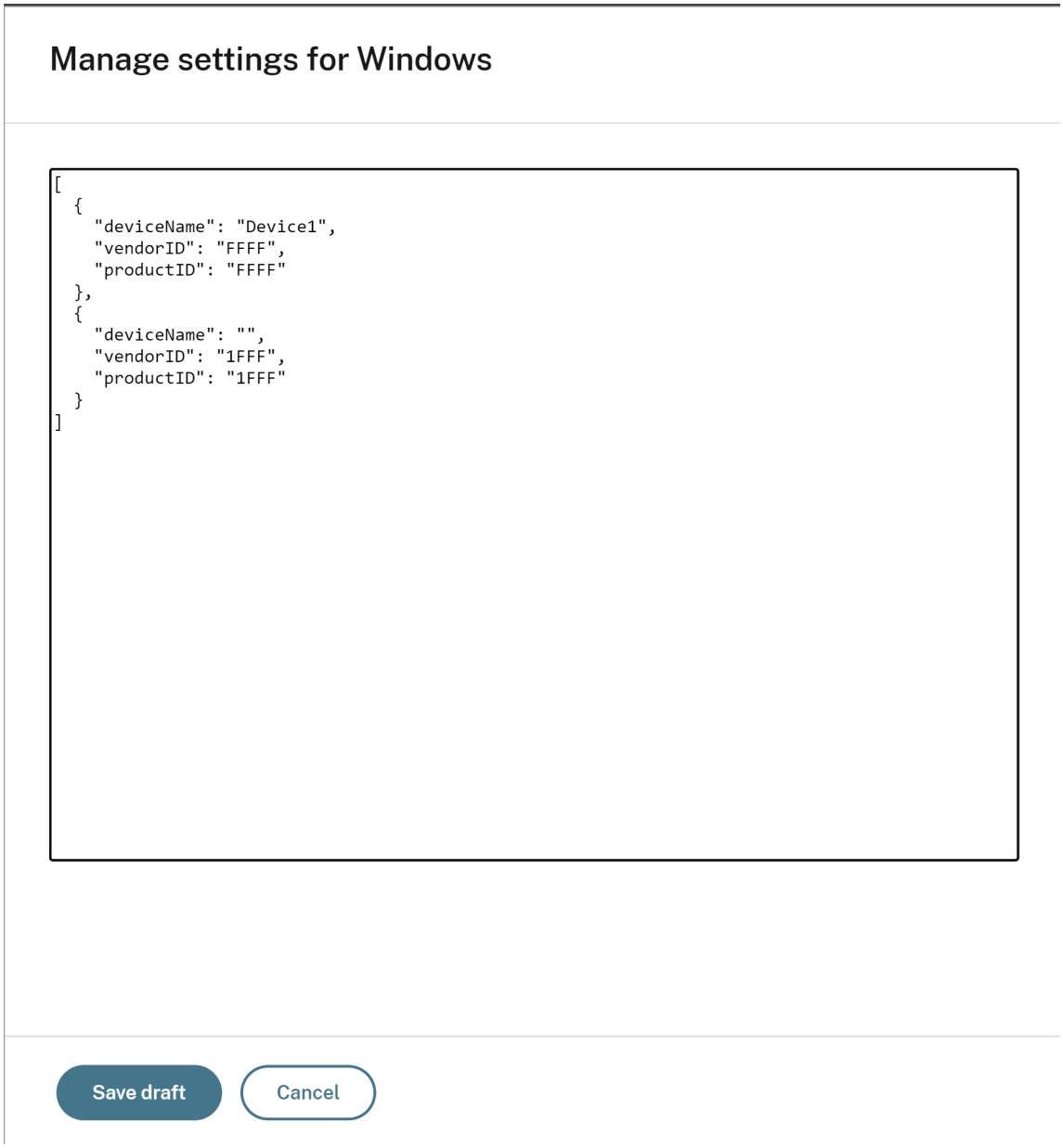
   例如，

```
[
 {

  "deviceName": "Device1",
  "vendorID": "FFFF",
  "productID": "FFFF"
  }

]
<!--NeedCopy-->
```

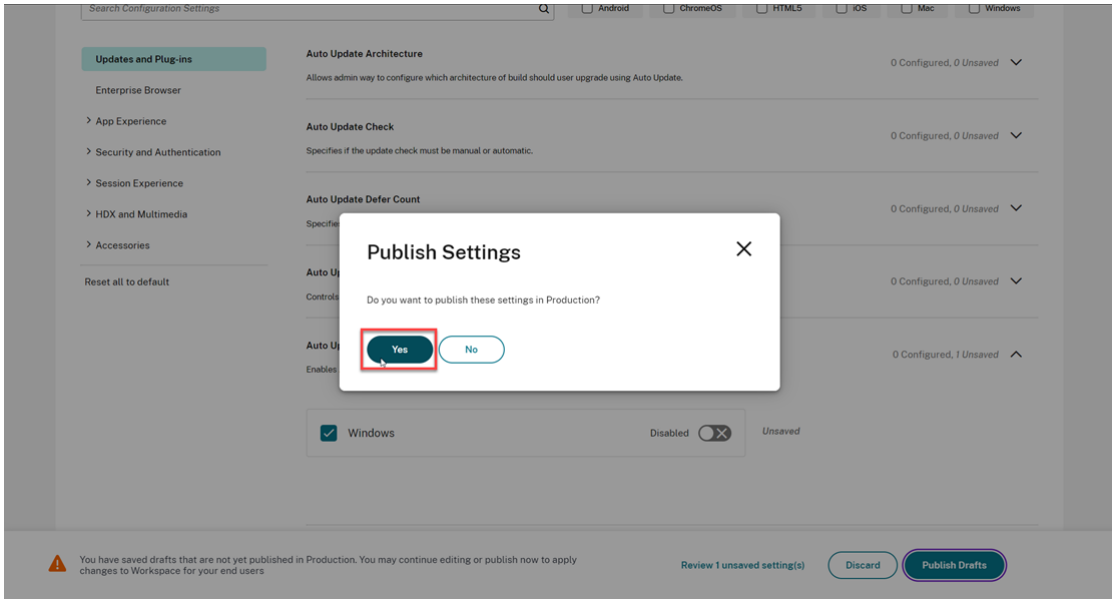



> 注意：
>
> - `productID` 和 `vendorID` 为必填字段。同时，`deviceName` 不是必填字段。
> - 此外，您可以通过在此块中添加多个条目将多个 USB 设备添加到排除列表中。

要获取 `productID` 和 `vendorID`，请参阅获取 `productID` 和 `vendorID`。

6. 单击 **Save draft**（保存草稿），然后单击 **Publish Drafts**（发布草稿）。
7. 在 **Publish Settings**（发布设置）对话框中，单击 **Yes**（是）。



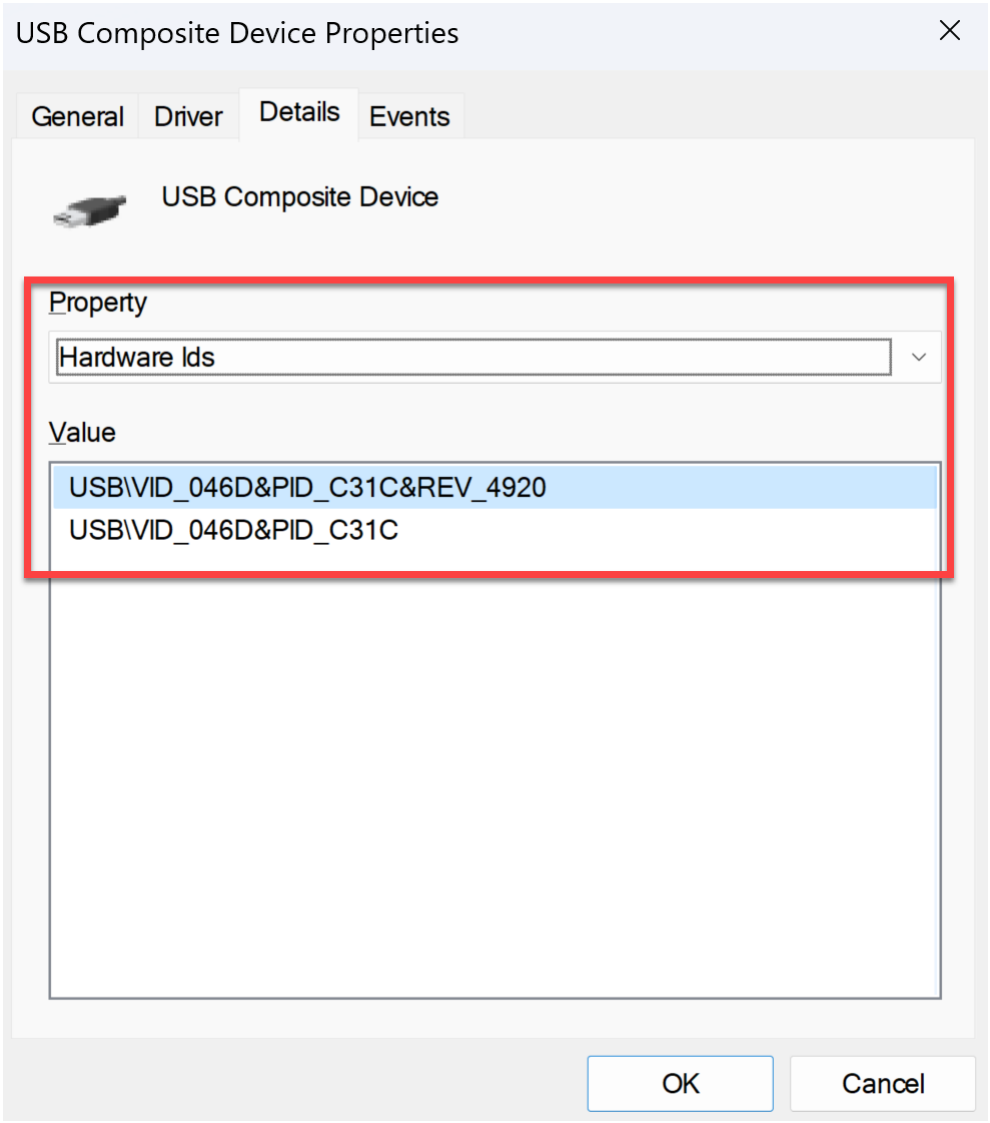

8. 重新启动 Citrix Workspace 应用程序。

### 获取 **productID** 和 **vendorID**

要获取 productID 和 vendorID，请执行以下步骤：

1. 打开设备管理器，找到要添加到排除列表的设备。
2. 右键单击设备名称，然后单击属性。此时将出现一个属性弹出屏幕。
3. 单击 **Details**（详细信息），然后从 **Property**（属性）列表中选择 **Hardware Ids**（硬件 ID）选项。
4. 在 **Value**（值）字段中，前缀 VID_ 为 vendorID 的值和前缀为 PID_ 的值为 productID。




## 故障排除

March 10, 2024

本文介绍了如何对不同平台上的 Citrix Workspace 应用程序的 App Protection 功能进行故障排除。

有关故障排除场景，请参阅以下内容：

- 通用故障排除场景
- 策略篡改检测
- App Protection 状态检查

### 适用于 **Windows** 的 **Citrix Workspace** 应用程序

1. 按照日志收集中的说明收集日志。
2. 按 **Win + R** 打开“运行”框 > 键入 `cmd` > 选择 **Enter**。
3. 运行以下命令：
    - 如果您使用的是 2311 之前的适用于 Windows 的 Citrix Workspace 应用程序版本，请运行以下命令：
        - `sc query appprotectionsvc`
        - `sc query entryprotectdrv`
        - `sc query epinject6`
        - `sc query epusbfilter`
    - 如果您使用的是适用于 Windows 的 Citrix Workspace 应用程序 2311 或更高版本，请运行以下命令：
        - `sc query appprotectionsvc`
        - `sc query ctxapdriver`
        - `sc query ctxapinject`
        - `sc query ctxapusbfilter`

提供结果以及从日志收集工具收集的跟踪记录。

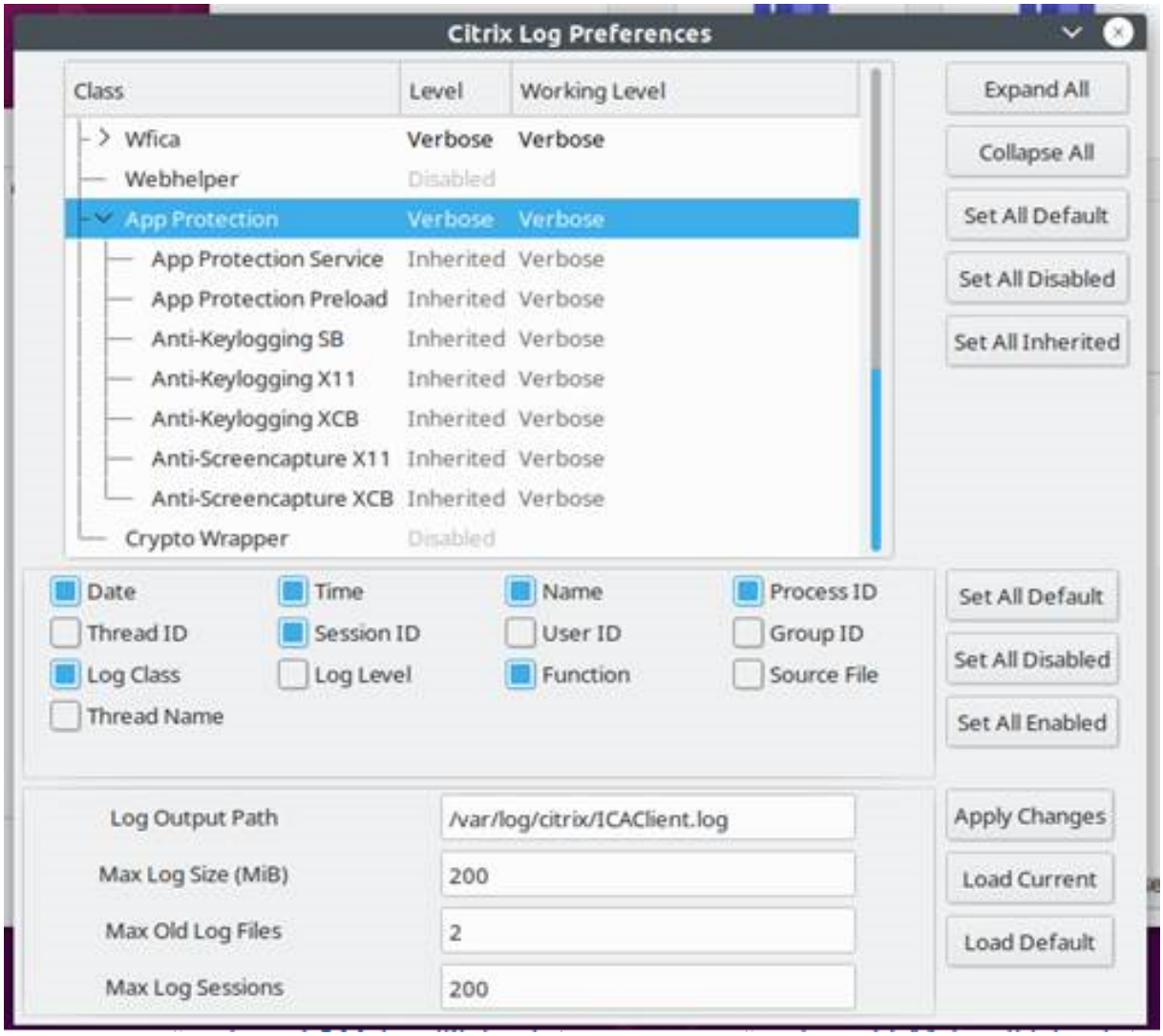
### 适用于 **Mac** 的 **Citrix Workspace** 应用程序

按照日志收集中的说明通过收集日志来提供日志。

### 适用于 **Linux** 的 **Citrix Workspace** 应用程序

1. 运行在安装的 *util* 文件夹中找到的 setlog 可执行文件。例如，`/opt/Citrix/ICAClient/util/setlog`。
2. 单击全部设置为已禁用（此步骤是可选步骤，并确保仅收集所需的日志）。
3. 转到“App Protection logging”（App Protection 日志记录）。
4. 单击鼠标右键并选择“Verbose”（详细）（仅记录警告和错误），将“App Protection log level”（App Protection 日志级别）设置为“Verbose”（详细）。
5. 展开 App Protection 类并右键单击其子元素。选择 **Group**（组）**> Inherited**（已继承）。
6. 为 **wfica** 启用日志。右键单击 **wfica** 并选择 **Verbose**（详细）。如果未安装 App Protection 或者 **wfica** 检测不到 App Protection，则日志为 **[NCS] < P3563 > citrix-wfica: App Protection is not installed**。
7. 启动会话时，日志将记录在 setlog 的日志输出路径中提到的文件中。




## 通用故障排除

March 10, 2024

### 启用了 **App Protection** 策略的资源不会显示在本机应用程序中

如果启用了 App Protection 策略的资源未显示在本机应用程序中，请执行以下步骤：

1. 如果您的 Citrix Workspace 应用程序版本早于以下版本，请将其更新到更高的任意版本：
    - 适用于 Linux 的 Citrix Workspace 应用程序 2108
    - 适用于 Windows 的 Citrix Workspace 应用程序 2203.1 LTSR

- 适用于 Windows 的 Citrix Workspace 应用程序 2002
- 适用于 Windows 的 Citrix Workspace 应用程序 2305.1（应用商店版本）
- 适用于 Mac 的 Citrix Workspace 应用程序 2001

2. 确保您未在 Windows 多会话操作系统（例如 Windows 2K16 或 Windows 2K22）中安装 Citrix Workspace 应用程序。
3. 如果满足上述条件但仍未显示资源，请收集日志并联系 Citrix 技术支持。有关收集日志的详细信息，请参阅日志收集。

### 使用本地应用商店时，启用了 **App Protection** 策略的资源不会显示在浏览器中

如果在使用本地应用商店时未在浏览器中显示启用了 App Protection 策略的资源，请执行以下步骤：

1. 请确保您的 Delivery Controller 版本不早于 1912 版。

   > 注意：
   >
   > 如果您使用的是 1912 版之前的 Delivery Controller，则不支持 App Protection。

2. 如果您使用的是介于 1912 到 2203 之间的 StoreFront 版本，请验证您是否启用了 StoreFront 自定义。有关启用 StoreFront 自定义功能的详细信息，请参阅启用 StoreFront 自定义。
3. 如果您使用的是 StoreFront 版本 2308 或更高版本，则无需启用 StoreFront 自定义。使用 StoreFront 版本 2308 或更高版本中的混合启动功能，验证您是否已在 StoreFront 上正确启用了 App Protection 以进行混合启动。
4. 验证您是否已为交付组正确启用 App Protection 功能。
5. 如果满足上述条件但仍未显示资源，请收集日志并联系 Citrix 技术支持。有关收集日志的详细信息，请参阅收集 Citrix Workspace 应用程序的日志和收集 StoreFront 的日志。

### 启动启用了 **App Protection** 的资源时无法建立安全的环境

对于适用于 Windows 的 Citrix Workspace 应用程序，必须在安装过程中启用安装后启动 **App Protection** 复选框，以确保 App Protection 服务已启动并建立安全环境。如果您在安装过程中未启用安装后启动 **App Protection** 复选框，则当您启动启用了 App Protection 策略的资源时，App Protection 服务会自动启动。App Protection 可能需要一段时间才能启动，具体取决于系统负载。有时，App Protection 可能会启动或超时。因此，建议在安装过程中选中安装后启动 **App Protection** 复选框。通常情况下，请重新启动启用了 App Protection 的资源，并且必须建立安全连接。但是，如果您仍然无法启动启用了 App Protection 的资源，请执行以下步骤：

1. 以管理员身份打开命令提示符并运行以下命令，检查 App Protection 服务是否正在运行：

```
sc query AppProtectionSvc
<!--NeedCopy-->
```

2. 如果 App Protection 服务未运行，则请通过运行以下命令启动该服务：

```
sc start AppProtectionSvc
<!--NeedCopy-->
```

3. 如果仍然出现错误，请收集日志并联系 Citrix 技术支持。有关收集日志的详细信息，请参阅日志收集。

### 无法启用或禁用 **App Protection**

如果您无法使用 Web Studio 或 PowerShell 为本地或云端交付组启用或禁用 App Protection，请执行以下步骤：

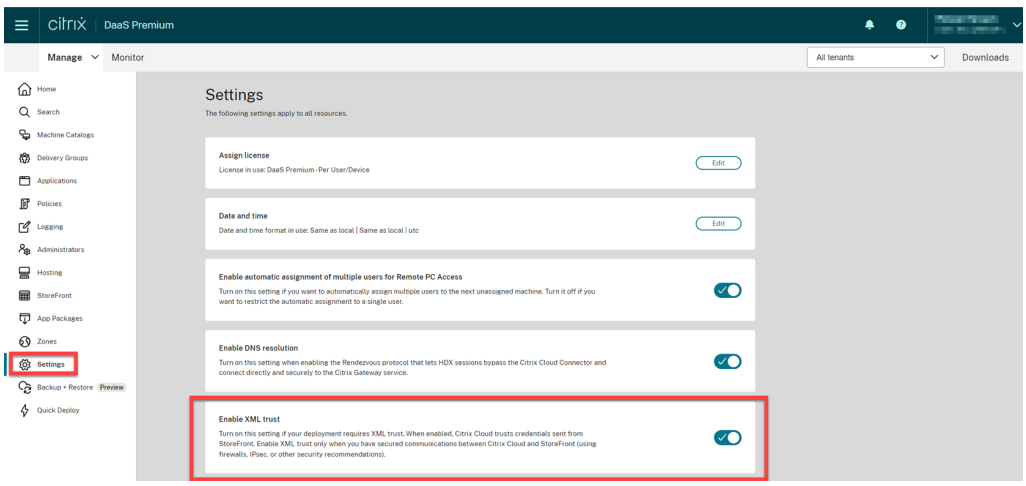
1. 检查您是否具有所需的许可证。如果所需的许可证不可用，则无法启用 App Protection。
2. 如果没有必要的许可证，则请获取所需的许可证并添加许可证。
3. 添加许可证后，请重新启动许可证服务器并尝试再次启用 App Protection。
4. 如果有有效的许可证可用，但您仍然无法启用或禁用 App Protection，则请运行以下命令检查是否已启用 `TrustRequestsSentToTheXmlServicePort`：

```
Get-BrokerSite | Select-Object
    TrustRequestsSentToTheXmlServicePort
<!--NeedCopy-->
```

5. 如果未启用 `TrustRequestsSentToTheXmlServicePort`，则请使用以下方法之一启用 XML 信任：

   - 使用 **Web Studio**：

     a) 登录您的 Citrix DaaS 帐户，然后转至管理 > 设置 > 启用 **XML** 信任。




     b) 打开启用 **XML** 信任开关。

   - 使用 **PowerShell**：运行以下命令以启用 XML 信任：

```
Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
<!--NeedCopy-->
```

6. 启用 `TrustRequestsSentToTheXmlServicePort` 后，再次启用 App Protection。
7. 如果满足上述条件，但仍无法启用或禁用 App Protection，请联系 Citrix 技术支持。

### App Protection 策略未正确应用

1. 请确保满足以下条件：
   - 您使用的是支持的 Citrix Workspace 应用程序版本。
   - 交付组启用了适当的功能。
   - 该功能已安装在端点上。
   - 安装了 Citrix Workspace 应用程序并启用了 `/includeappprotection` 开关。
2. 如果满足上述条件，但仍未正确应用 App Protection 策略，请收集日志并联系 Citrix 技术支持。有关收集日志的详细信息，请参阅收集 Citrix Workspace 应用程序的日志

屏幕截图不适用于非 **Citrix** 窗口：

- 最小化或关闭受保护的 Citrix 窗口，包括 Citrix Workspace 应用程序。

## 策略篡改检测故障排除

March 10, 2024

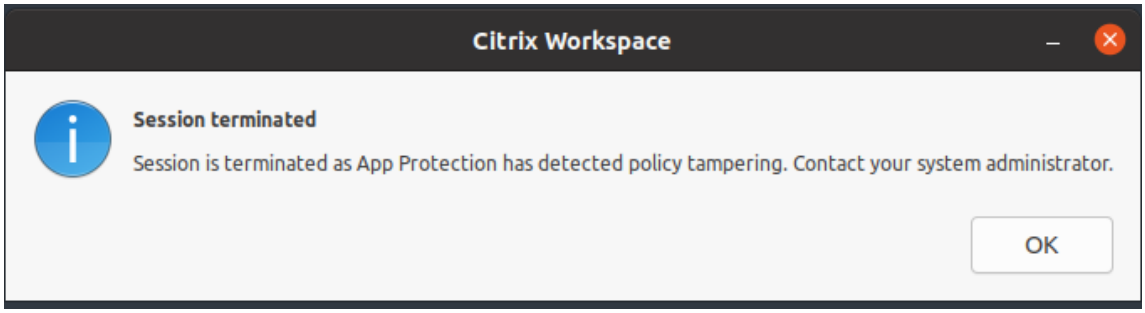
以下部分介绍了您可能会面临的一些问题以及如何解决这些问题：

### ICA 文件被篡改，会话仍在运行

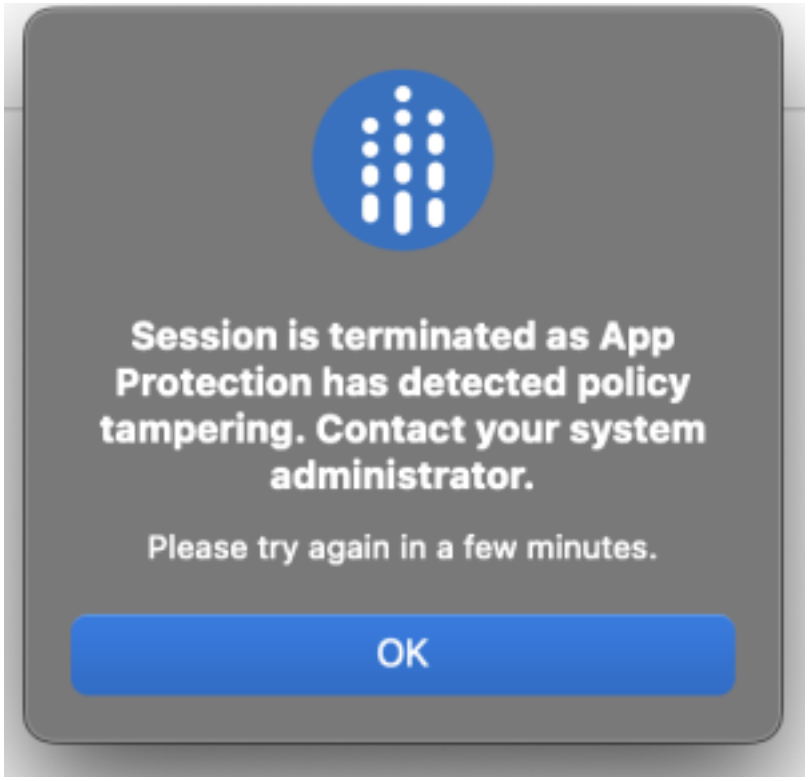
如果启用了“App Protection 策略篡改检测”功能的虚拟应用程序或桌面会话的 ICA 文件被篡改，会话将被终止并显示以下错误消息之一：

- 适用于 Linux 的 Citrix Workspace 应用程序

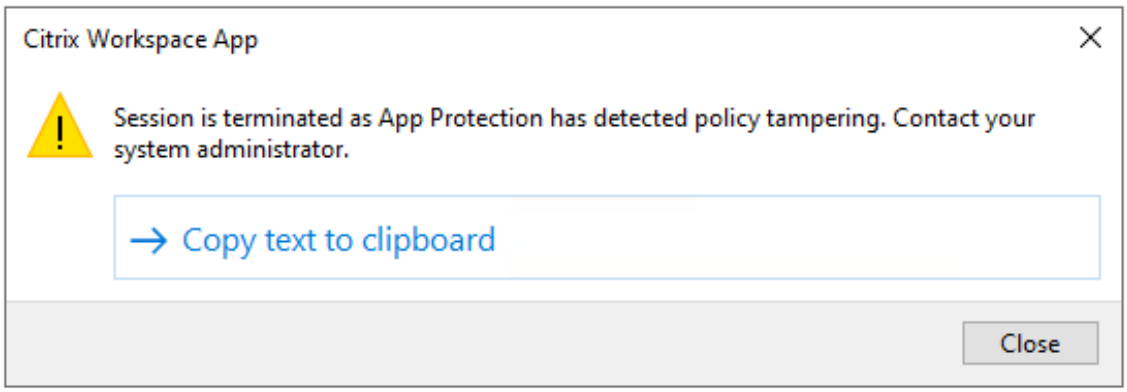
 




- 适用于 Mac 的 Citrix Workspace 应用程序




- 适用于 Windows 的 Citrix Workspace 应用程序




但是，如果即使 ICA 文件被篡改且启用了“策略篡改检测”功能，会话仍在运行，则请执行以下步骤：

1. 在 Virtual Delivery Agent 中，执行以下操作：

   a) 运行以下命令并检查 `ctxappprotectionsv` 服务是否正在运行：

   ```
   sc query ctxappprotectionsvc
   ```

   b) 如果 `ctxappprotectionsvc` 服务未运行，请执行以下步骤以启动该服务：

      i. 请通过运行以下命令将 `ctxappprotectionsvc` 服务的启动类型更改为 automatic：

      ```
      sc config ctxappprotectionsvc start=auto
      ```

      ii. 请通过运行以下命令启动该服务：

      ```
      sc start ctxappprotectionsvc
      ```

2. 在客户端中，执行以下操作：

   a) 检查 *vdappp.dll* 文件是否位于 Citrix Workspace 应用程序的安装位置。Citrix Workspace 应用程序的默认安装位置如下：

   - Windows - C:\Program Files (x86)\Citrix\ICA Client
   - Linux - /opt/Citrix/ICAClient
   - Mac - 不适用

   b) 对于适用于 Windows 的 Citrix Workspace 应用程序，请使用 *procexp.exe* 并检查 *vdappp.dll* 文件是否已加载到 *wfica32.exe* 中。

   c) 对于适用于 Linux 的 Citrix Workspace 应用程序，请检查 *vdappp.dll* 文件是否已加载到 *wfica.exe* 中。

3. 如果会话仍在运行，则请收集日志并联系 Citrix 技术支持部门。有关收集日志的详细信息，请参阅日志收集。

### 重新启动 **Virtual Delivery Agent** 后，“策略篡改检测”功能将停止运行

如果您重新启动了 Virtual Delivery Agent，而“策略篡改检测”功能停止运行，则可能是因为重新启动后 App Protection 服务未运行。请在 Virtual Delivery Agent 上执行以下步骤：

1. 运行以下命令并检查 `ctxappprotectionsvc` 服务是否正在运行并设置为 **automatic**：

   ```
   sc query ctxappprotectionsvc
   ```

2. 如果 `ctxappprotectionsvc` 服务未运行，请执行以下步骤以启动该服务：

   a) 请通过运行以下命令将 `ctxappprotectionsvc` 服务的启动类型更改为 **automatic**：

   ```
   sc config ctxappprotectionsvc start=auto
   ```

   b) 请通过运行以下命令启动该服务：

   ```
   sc start ctxappprotectionsvc
   ```

3. 如果“策略篡改检测”功能仍然无法运行，请收集日志并联系 Citrix 技术支持部门。有关收集日志的详细信息，请参阅日志收集。

## App Protection 状态检查故障排除

March 10, 2024

以下部分介绍了您可能会面临的一些问题以及如何解决这些问题：

### 会话已终止但未显示任何错误消息

如果您的虚拟应用程序或桌面会话突然终止但未显示任何错误消息，请执行以下步骤：

1. 检查您的 Citrix Workspace 应用程序版本是否早于以下版本之一：
   - 适用于 Windows 的 Citrix Workspace 应用程序 2309
   - 适用于 Mac 的 Citrix Workspace 应用程序 2308
   - 适用于 Linux 的 Citrix Workspace 应用程序 2308

   > 注意：
   >
   > 如果 Citrix Workspace 应用程序版本早于步骤 1 中列出的版本，并且启用了 App Protection 状态检查功能，虚拟应用程序或桌面会话将终止但不显示任何错误消息。但是，如果 Citrix Workspace 应用程序版本高于或等于步骤 1 中列出的版本，并且启用了 App Protection 状态检查功能，虚拟应用程序或桌面会话将终止并显示错误消息。

2. 检查 App Protection 状态检查功能是否已启用。
3. 如果 Citrix Workspace 应用程序版本高于或等于之前的版本，并且状态检查功能也处于活动状态，则请收集日志并联系 Citrix 技术支持部门。有关收集日志的详细信息，请参阅日志收集。

### App Protection 状态检查已启用，但较旧版本的会话未终止

通常情况下，如果启用了 App Protection 状态检查功能，并且您正在通过较旧版本的 Citrix Workspace 应用程序进行连接，则必须终止会话。

但是，如果会话未终止，则请执行以下步骤：

1. 在 Virtual Delivery Agent 中，执行以下操作：
   a) 运行以下命令并检查 `ctxappprotectionsvc` 服务是否正在运行：

   ```
   sc query ctxappprotectionsvc
   ```

b) 如果 `ctxappprotectionsvc` 服务未运行，请执行以下步骤以启动该服务：

i. 请通过运行以下命令将 `ctxappprotectionsvc service` 的启动类型更改为 **automatic**：

```
sc config ctxappprotectionsvc start=auto
```

ii. 请通过运行以下命令启动该服务：

```
sc start ctxappprotectionsvc
```

2. 检查您输入的状态检查值是否具有以下前缀之一：

- 对于适用于 Windows 的 Citrix Workspace 应用程序，前缀为 `windows-`
- 对于适用于 Linux 的 Citrix Workspace 应用程序，前缀为 `linux-`
- 对于适用于 Mac 的 Citrix Workspace 应用程序，`mac-`

3. 检查状态检查值是否根据相关平台正确添加，因为这些值是平台特有的值。
4. 检查 `reg` 位置 (`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\AppProtectionPolicies`) 以验证状态检查是否已与 Virtual Delivery Agent 同步。
5. 如果满足上述所有条件，并且较旧版本的 Citrix Workspace 应用程序的会话仍处于连接状态，请收集日志并联系 Citrix 技术支持部门。有关收集日志的详细信息，请参阅日志收集。

### App Protection 状态检查在一个平台上运行，但在另一个平台上无法运行

有时，App Protection 状态检查功能可能在一个平台上运行，但在另一个平台上无法运行。例如，App Protection 状态检查功能在适用于 Windows 的 Citrix Workspace 应用程序中运行，但在适用于 Linux 的 Citrix Workspace 应用程序中无法运行。

在此类场景中，请执行以下步骤：

1. 检查您输入的状态检查值是否具有以下前缀之一：

- 对于适用于 Windows 的 Citrix Workspace 应用程序，前缀为 `windows-`
- 对于适用于 Linux 的 Citrix Workspace 应用程序，前缀为 `linux-`
- 对于适用于 Mac 的 Citrix Workspace 应用程序，`mac-`

2. 检查状态检查值是否根据相关平台正确添加，因为这些值是平台特有的值。
3. 检查 Virtual Delivery Agent 上的 `reg` 位置 (`Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Citrix\AppProtectionPolicies`) 以验证状态检查是否已与 Virtual Delivery Agent 同步。它们必须与 Studio 上的配置相匹配。
4. 如果满足上述所有条件，并且较旧版本的 Citrix Workspace 应用程序的会话仍处于连接状态，请收集日志并联系 Citrix 技术支持部门。有关收集日志的详细信息，请参阅日志收集。

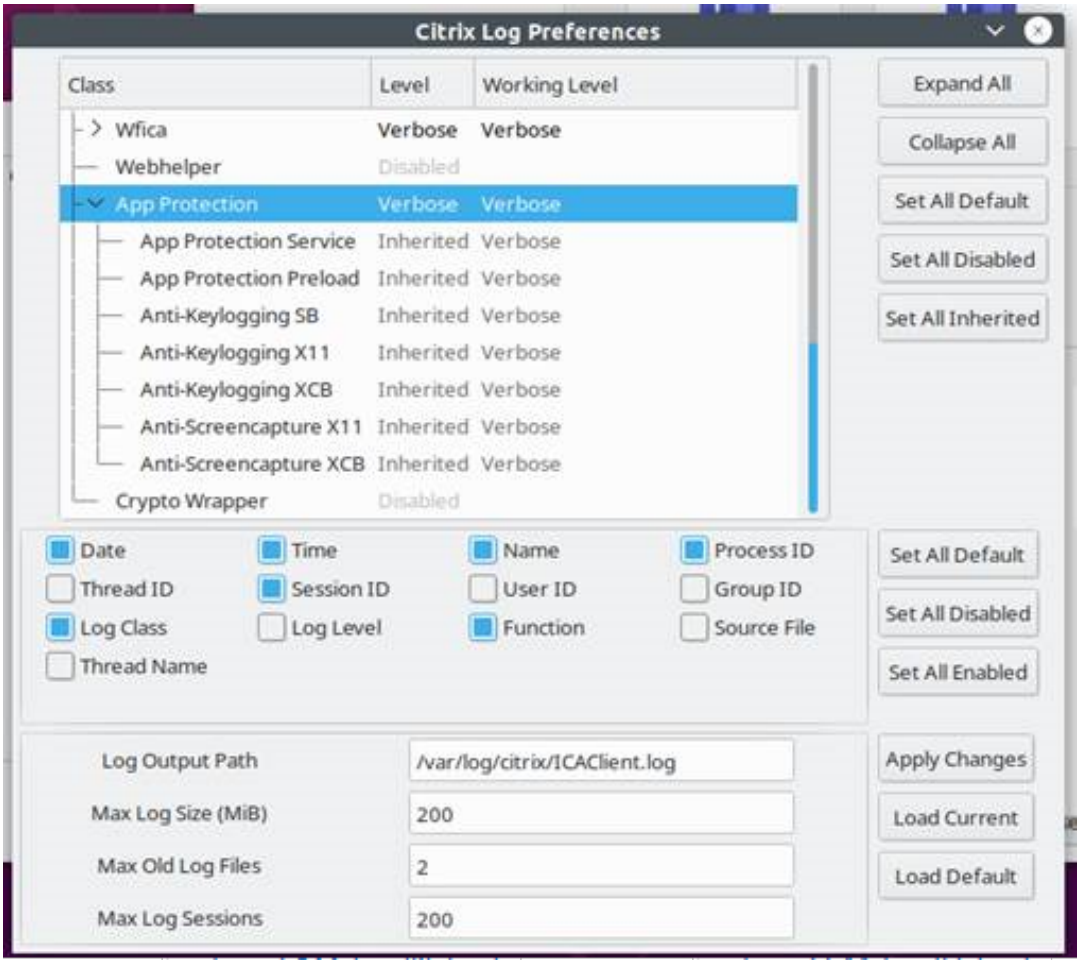
# 日志收集

March 10, 2024

- 要收集适用于 Windows 的 Citrix Workspace 应用程序的日志，请参阅面向 Windows 的日志收集。
- 要收集适用于 Mac 的 Citrix Workspace 应用程序的日志，请参阅面向 Mac 的日志收集。
- 要收集适用于 Linux 的 Citrix Workspace 应用程序的日志，请执行以下步骤：

  1. 运行在安装的 *util* 目录中找到的 setlog 可执行文件。例如，*/opt/Citrix/ICAClient/util/setlog*。
  2. （可选）单击全部设置为已禁用，并确保仅收集所需的日志。
  3. 转到“App Protection logging”（App Protection 日志记录）。
  4. 单击鼠标右键并选择 **Verbose**（详细）（仅记录警告和错误），将“App Protection log level”（App Protection 日志级别）设置为“Verbose”（详细）。
  5. 展开 App Protection 类并右键单击其子元素。选择 **Group**（组）> **Inherited**（已继承）。
  6. 使用 linux 日志记录实用程序（从 *install dir* 中启动 *util/setlog*），并将虚拟通道的日志记录级别更改为“Verbose”（详细）。
  7. 为 **wfica** 启用日志。右键单击 **wfica** 并选择 **Verbose**（详细）。如果未安装 App Protection 或者 **wfica** 检测不到 App Protection，则日志为 **[NCS] < P3563 > citrix-wfica: App Protection is not installed**。
  8. 单击 **wfica** 并将 **winstation** 驱动程序的日志记录级别更改为 **Verbose**（详细）。
  9. 启动会话时，日志将记录在 setlog 的日志输出路径中提到的文件中。

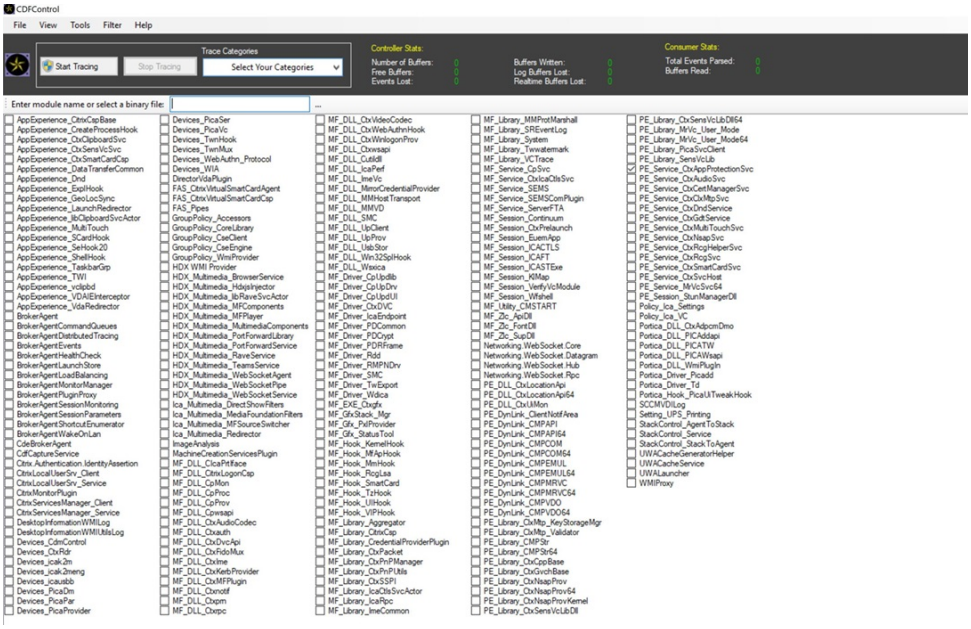
 




- 要收集 Virtual Delivery Agent 的日志，请执行以下步骤：

  1. 要通过 CDF 控制功能从 App Protection 服务获取跟踪信息，请选择所有模块。




2. 在某些情况下，我们可能必需从另一台计算机捕获 CDF 跟踪信息。要收集 CDF 跟踪信息，请参阅 CTX237216。

## 适用于 **Workspace** 的上下文 **App Protection**

March 10, 2024

上下文 App Protection 提供了精细的灵活性，可以根据用户、其设备和网络状况，有条件地为一部分用户应用 App Protection 策略。

### 实施上下文 **App Protection**

您可以使用 Broker 访问策略规则中定义的连接过滤器来实施上下文 App Protection。Broker 访问策略定义的规则用于控制用户能否访问交付组。该策略由一组规则组成。每条规则都关联到单个交付组，并且包含一组连接过滤器和访问权限控件。

当用户的连接详细信息与 Broker 访问策略中的一个或多个规则的连接过滤器匹配时，用户将获得对交付组的访问权限。默认情况下，用户无权访问站点中的任何交付组。您可以根据要求创建更多 Broker 访问策略。多个规则可以应用于同一个交付组。有关详细信息，请参阅 New-BrokerAccessPolicyRule。

如果用户的连接与访问策略规则中定义的连接过滤器匹配，则 Broker 访问策略规则中的以下参数能够灵活根据上下文启用 App Protection：

- `AppProtectionKeyLoggingRequired`
- `AppProtectionScreenCaptureRequired`

使用 Broker 访问策略规则中引用的智能访问策略可进一步优化连接过滤器。请参阅本文中解释说明的场景，了解如何使用智能访问策略设置上下文 App Protection。

### 上下文 **App Protection** 场景

下面是有关如何启用上下文 App Protection 的一些场景：

- 为通过 Access Gateway 进入的外部用户启用 App Protection
- 为不可信设备启用 App Protection
- 根据设备状态结果启用 App Protection
- 为特定用户组启用 App Protection

## 必备条件

March 10, 2024

请确保您具备以下项：

- 网络位置服务 (NLS)，适用于基于用户的网络位置的场景
- 许可要求 -
  - 适用于 DaaS 的 App Protection
  - 配置了智能访问策略的场景的自适应身份验证授权。

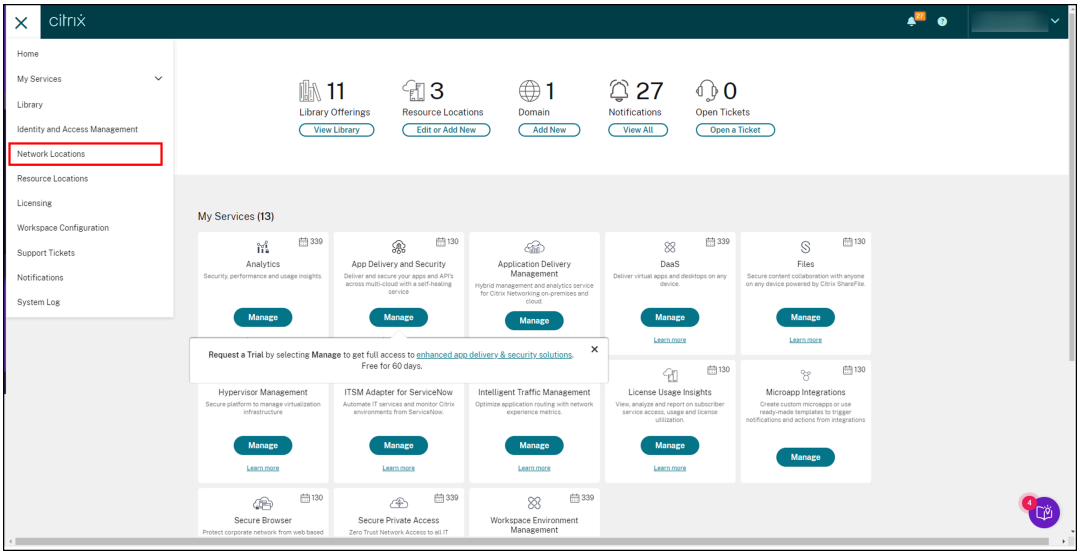
## 场景 **1**

April 10, 2024

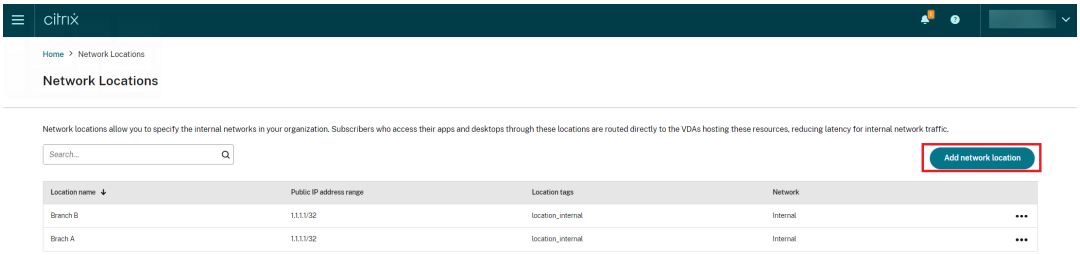
此场景介绍了如何为通过 **Access Gateway** 进入的外部用户启用 **App Protection**。

1. 配置自适应身份验证。
2. 根据您的网络位置配置自适应访问。
   a) 登录 Citrix Cloud 并导航到 **Network Locations**（网络位置）。




b) 单击 **Add Network location**（添加网络位置）。




此时将显示 **Add a Network Location**（添加网络位置）屏幕。

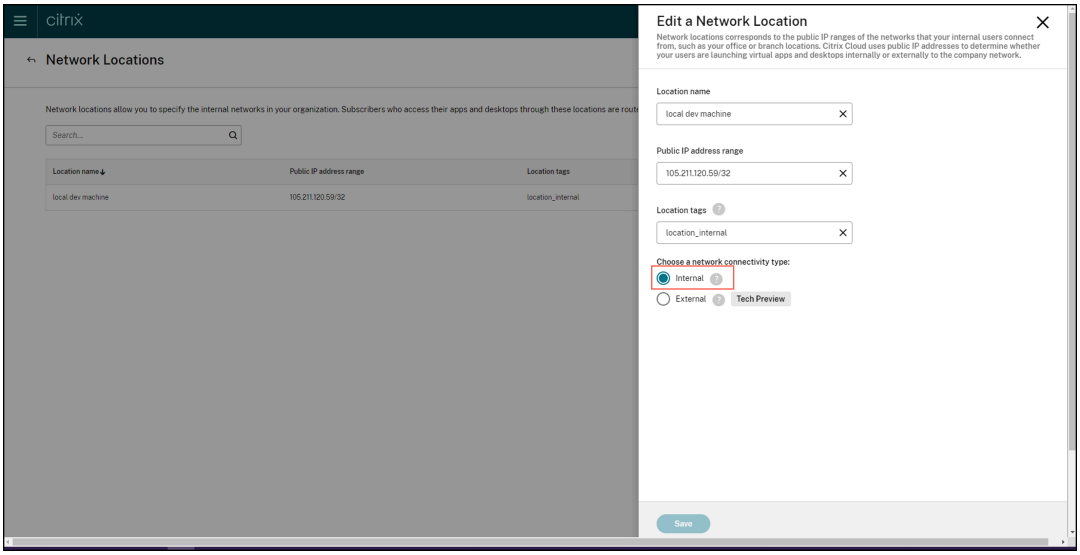
c) 在 **Location name** （位置名称）字段中，输入相关的位置名称。

d) 在 **Public IP address range**（公用 IP 地址范围）字段中，输入您要视为内部网络的网络 IP 地址或子网。

e) 在 **Location tags**（位置标记）字段中，输入 **location_internal**。有关位置标记的详细信息，请参阅位置标记。

f) 在 **Choose a network connectivity type**（选择网络连接类型）下，选择 *Internal*（内部）。




如果您登录到云应用商店时使用的设备的 IP 地址在 **Choose a network connectivity type**（选择网络连接类型）设置下被配置为 *Internal*（内部），则该连接被视为一个内部连接。

3. 配置 Broker 访问策略规则

   默认情况下，为每个交付组创建两个 Broker 访问策略。一个策略适用于通过 Access Gateway 建立的连接，另一个策略适用于直接连接。您只能为通过 Access Gateway 建立的连接（即外部连接）启用 App Protection。请使用以下步骤配置 Broker 访问策略规则：

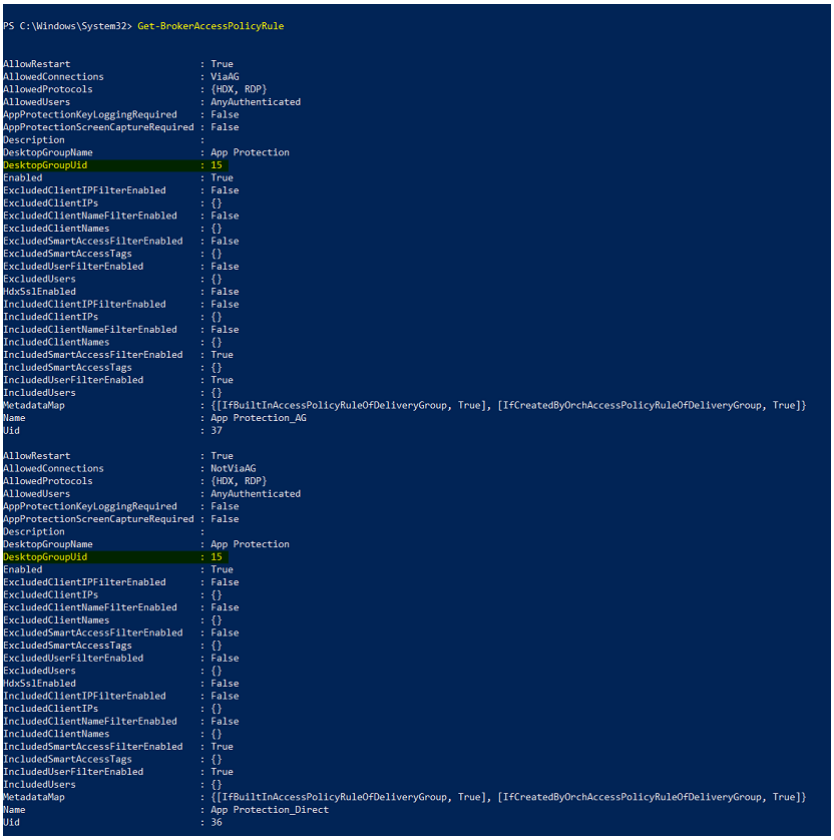
   a) 按照 Citrix 博客 Getting started with PowerShell automation for Citrix Cloud（Citrix Cloud 的 PowerShell 自动化入门）中的说明，安装 Citrix PowerShell SDK 并连接到 Citrix Cloud API。

   b) 运行命令 `Get-BrokerAccessPolicyRule`。

      显示存在的所有交付组的所有 Broker 访问策略的列表。

   c) 找到要更改的交付组的 **DesktopGroupUid**。

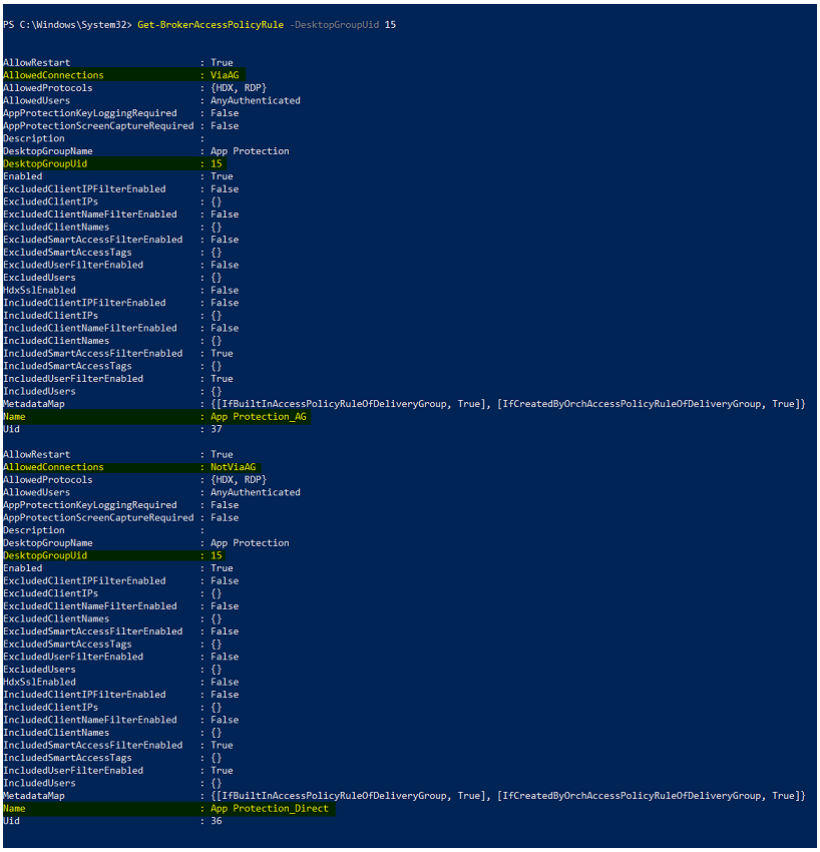
 




d) 使用 **DesktopGroupUid** 运行以下命令以获取适用于交付组的策略。至少存在两个策略，其中一个策略中的 *AllowedConnections* 设置了 *ViaAG*，另一个设置了 *NotViaAG*。

```
Get-BrokerAccessPolicyRule -DesktopGroupUid 15
```




在屏幕截图中，您可以看到两个策略：

- App Protection_AG - 设置了 *ViaAG* 的 *AllowedConnections*，这是适用于通过 Access Gateway 建立的连接的策略
- App Protection_Direct –设置了 *NotViaAG* 的 *AllowedConnections*，这是适用于非通过 Access Gateway 建立的连接的策略

4. 请使用以下命令仅为外部连接启用 App Protection 策略，为内部连接禁用 App Protection 策略：

   - `Set-BrokerAccessPolicyRule "App Protection_AG"-IncludedSmartAccessFilt $true -IncludedSmartAccessTags Workspace:LOCATION_internal -AppProtectionScreenCaptureRequired $false -AppProtectionKeyLoggingRequ $false`
   - `New-BrokerAccessPolicyRule "App Protection_AG_Exclude"-ExcludedsmartAc $true -ExcludedSmartAccessTags Workspace:LOCATION_internal -AppProtectionScreenCaptureRequired $true -AppProtectionKeyLoggingRequi $true -DesktopGroupUid 15 -AllowedConnections ViaAG -AllowedProtocols HDX, RDP`
   - `Remove-BrokerAccessPolicyRule "App Protection_Direct”`

5. 验证：

注销 Citrix Workspace 应用程序并重新登录。从外部连接启动受保护的资源。您会看到 App Protection 策略已应用。请从内部连接启动相同的资源，即在第一步中配置的 IP 地址范围内的设备。您会看到 App Protection 策略已禁用。

## 场景 2

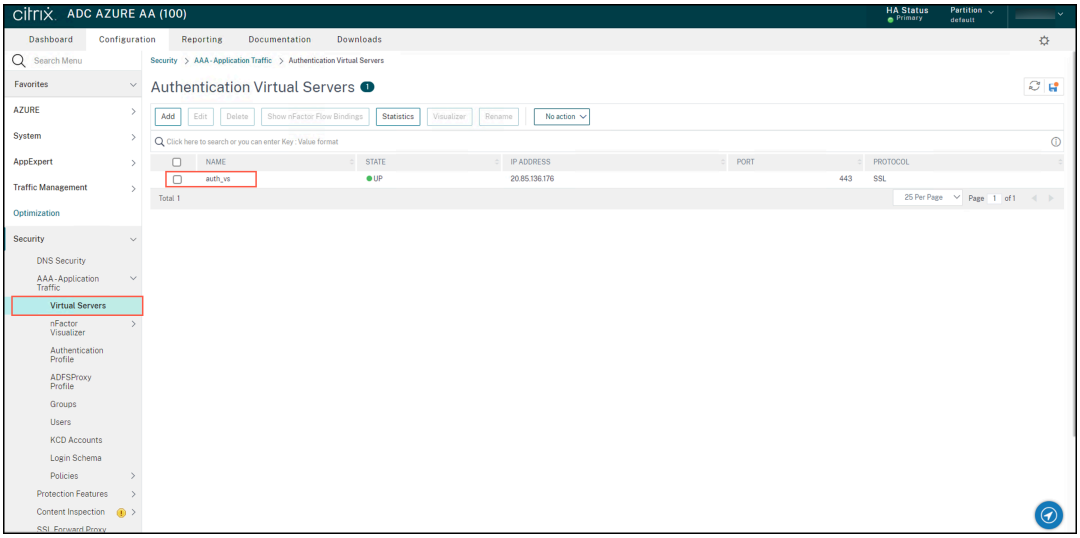
April 10, 2024

此场景介绍了如何为不受信任的设备启用 **App Protection**。

可信设备和不可信设备有许多定义。在这种情况下，假设端点分析 (EPA) 扫描成功后设备是可信的。所有其他设备均被视为不可信设备。

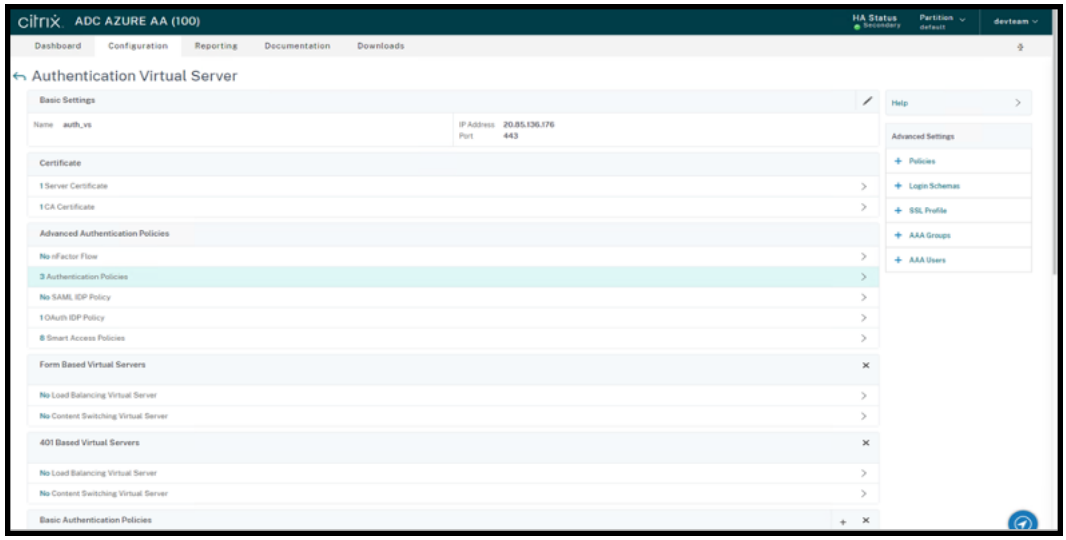
1. 配置自适应身份验证。
2. 请使用以下步骤通过 EPA 扫描创建身份验证策略：

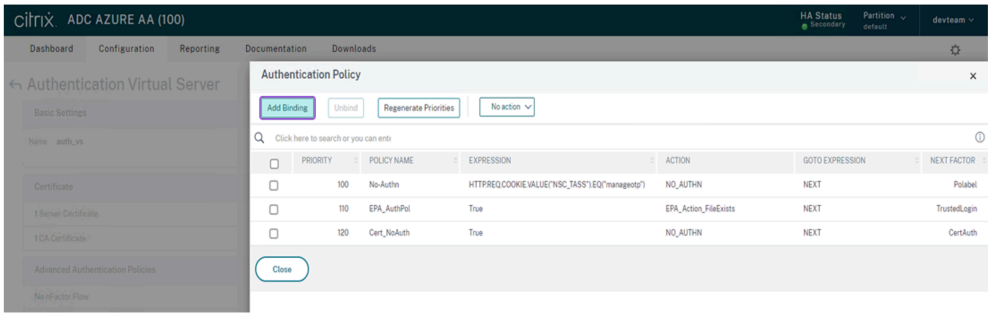
   a) 登录 Citrix ADC 管理 UI。在 **Configuration**（配置）选项卡中，导航到 **Security**（安全）**> AAA-Application Traffic**（**AAA-**应用程序流量）**-> Virtual Servers**（虚拟服务器）。单击要使用的虚拟服务器，在本例中为 *auth_vs*。



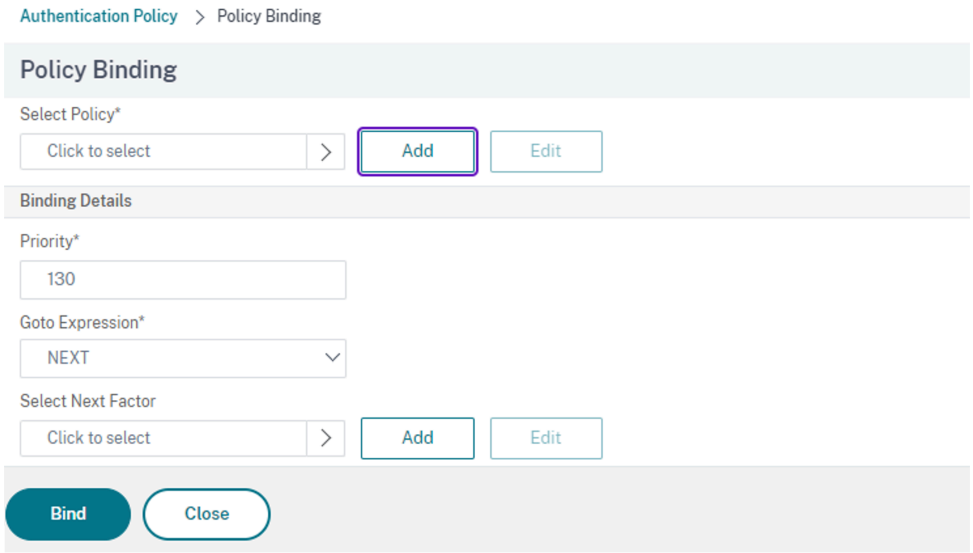

   b) 导航到 **Authentication Policies**（身份验证策略）**> Add Binding**（添加绑定）。



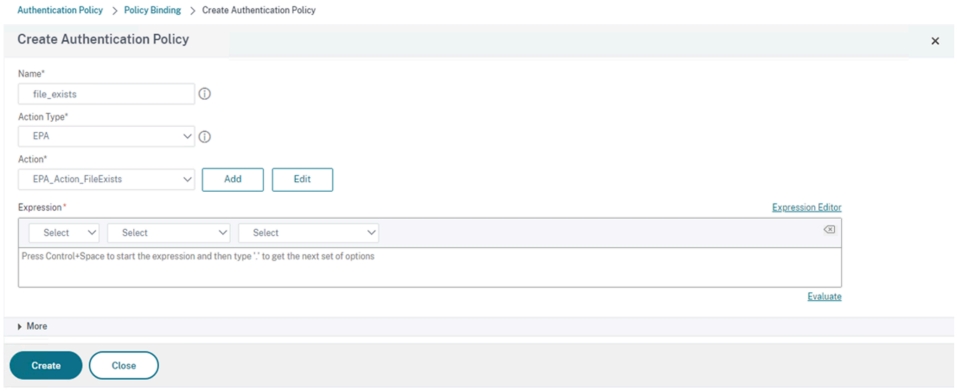




c) 单击添加以创建策略。

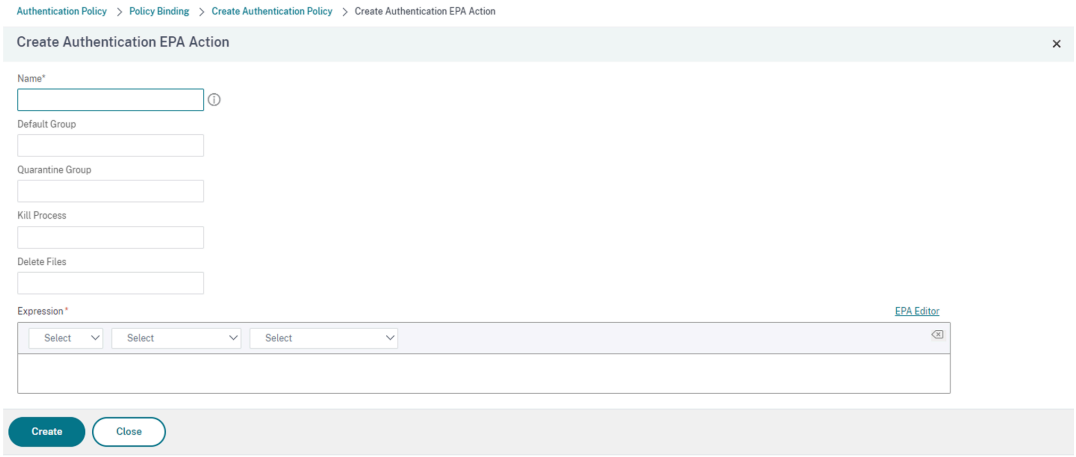



d) 根据 EPA 扫描创建身份验证策略。请输入策略的名称。选择操作类型为 *EPA*。单击添加创建操作。




此时将显示 **Create Authentication EPA Action**（创建身份验证 EPA 操作）屏幕。



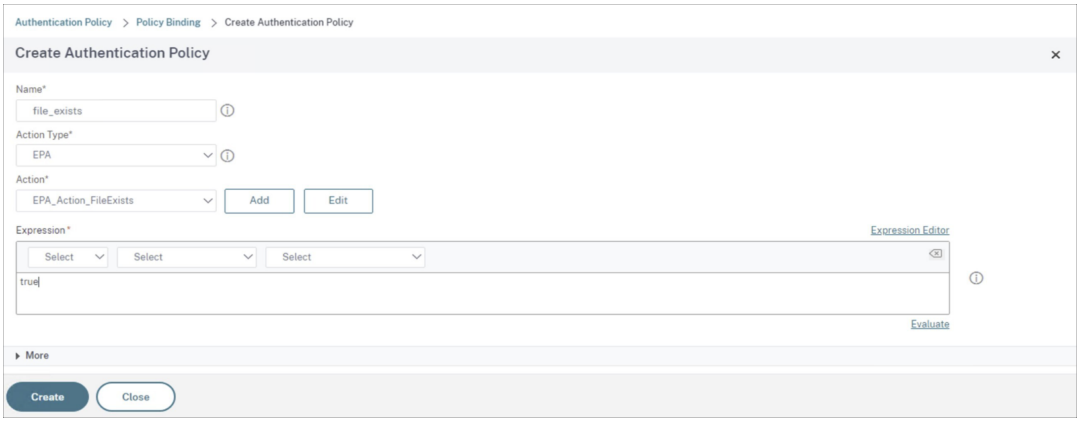

e) 在 **Create Authentication EPA Action**（创建身份验证 EPA 操作）屏幕上，输入以下详细信息，然后单击 **Create**（创建）以创建操作：

- **Name**（名称）：EPA 操作的名称。在这种情况下为 *EPA_Action_FileExists*。
- **Default Group**（默认组）：输入默认组的名称。如果 EPA 表达式为 *True*，则将用户添加到默认组中。本例中的默认组为 *FileExists*。
- **Quarantine Group**（隔离组）：输入隔离组的名称。如果 EPA 表达式为 *False*，则将用户添加到隔离组中。
- **Expression**（表达式）：添加要扫描的 EPA 表达式。在本示例中，如果存在特定文件，我们认为 EPA 扫描是成功的：`sys.client_expr("file_0_C:\\\\\epa\\\\\avinstalled.txt")`

您将返回到 **Create Authentication Policy**（创建身份验证策略）屏幕。

f) 在表达式编辑器中输入 **true**，然后单击创建。



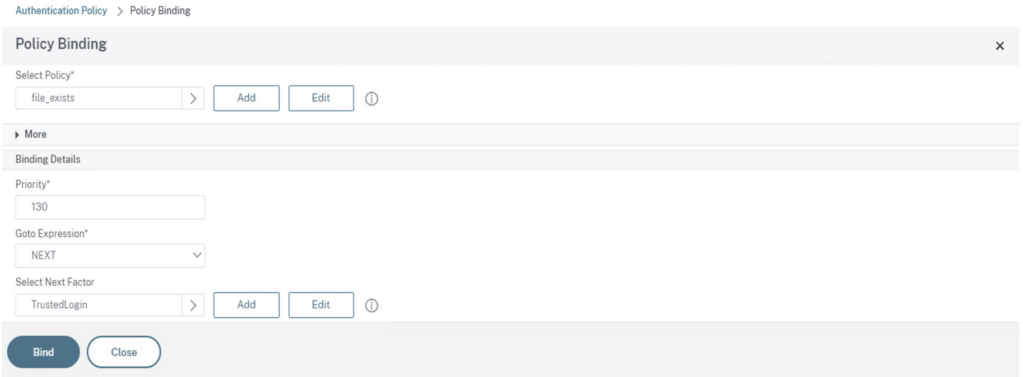

您将返回到策略绑定屏幕。

g) 在 **Policy Binding**（策略绑定）屏幕上，执行以下操作：

i. 选择 **Goto** 表达式为 **NEXT**。

ii. 在 **Select Next Factor**（选择下一个因素）部分中，选择您在 Application Delivery Controller (ADC) 中为身份验证配置的 LDAP 策略。

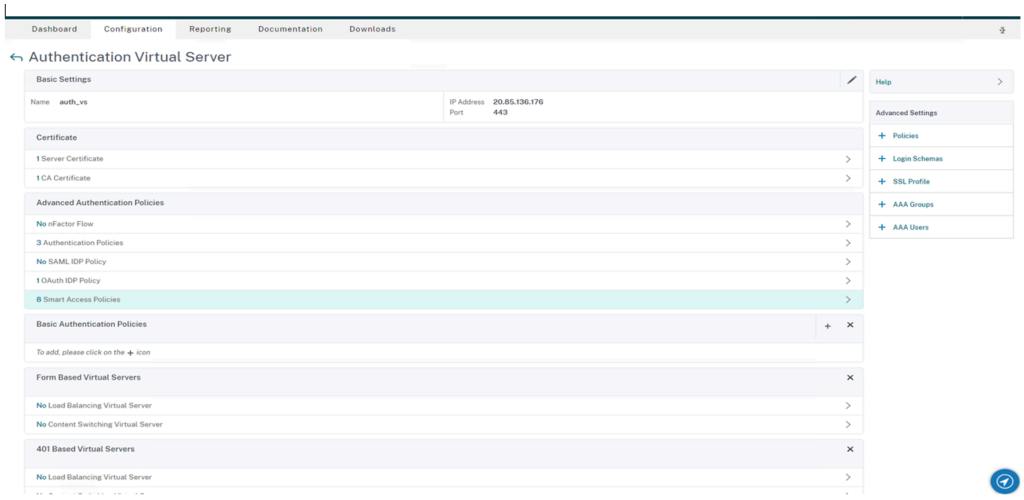
iii. 单击绑定。



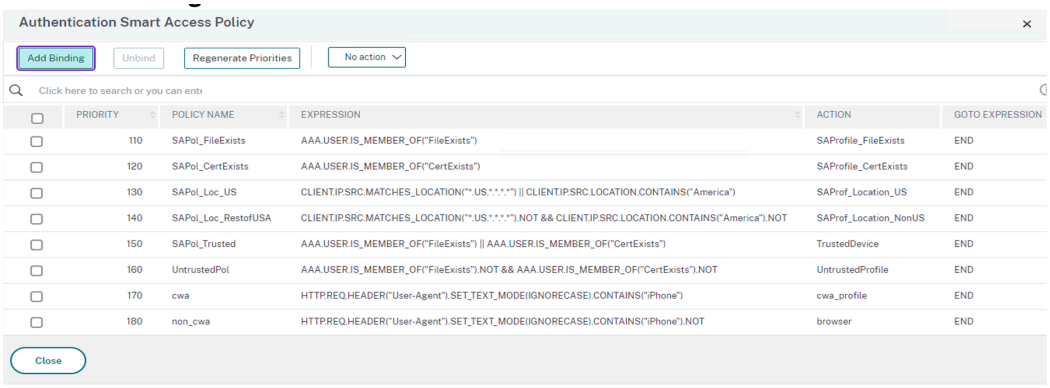

3. 为可信设备创建智能访问策略：

a) 在 *auth_vs* 服务器的 **Authentication Virtual Server**（身份验证虚拟服务器）页面上选择 **Smart Access Policies**（智能访问策略）。



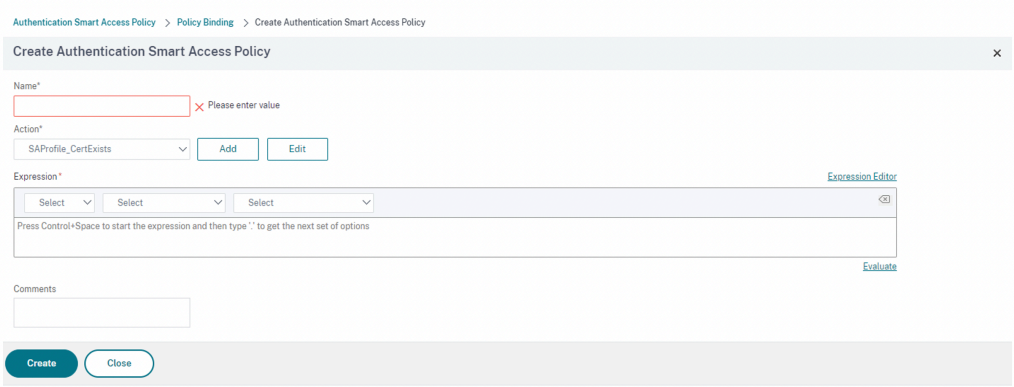

b) 单击 **Add Binding**（添加绑定）。




c) 在 **Policy Binding**（策略绑定）屏幕上，单击 **Select Policy**（选择策略）部分中的添加。


此时将显示 **Create Authentication Smart Access Policy**（创建身份验证智能访问策略）屏幕。

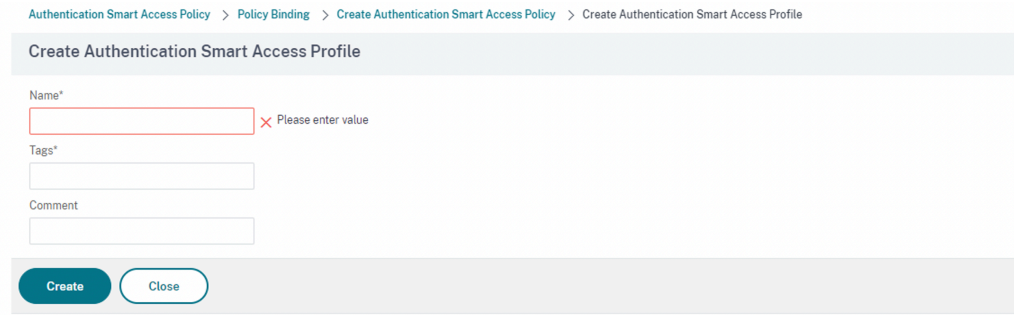
 




d) 在 **Create Authentication Smart Access Policy**（创建身份验证智能访问策略）屏幕上，输入智能访问策略的名称，然后单击添加以创建智能访问配置文件。

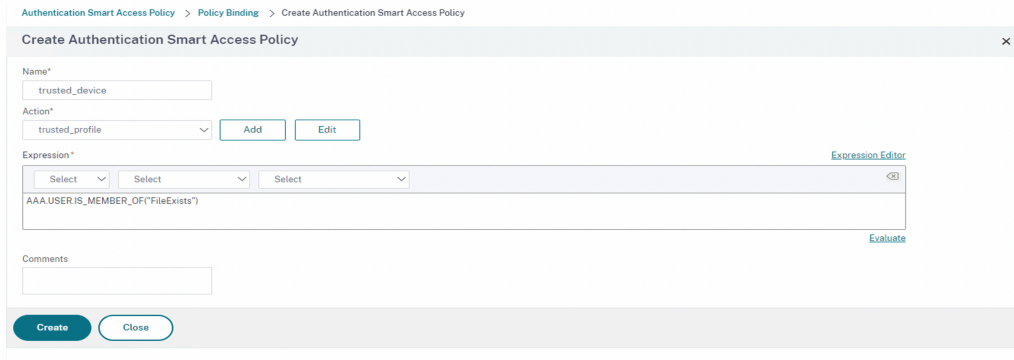
此时将显示 **Create Authentication Smart Access Profile**（创建身份验证智能访问配置文件）屏幕。

e) 为操作添加名称。在 **Tags**（标记）中输入 *trusted*（可信）。稍后将在 Broker 访问策略规则中引用该标记进行配置。单击创建。




您将返回到 **Create Authentication Smart Access Policy**（创建身份验证智能访问策略）屏幕。

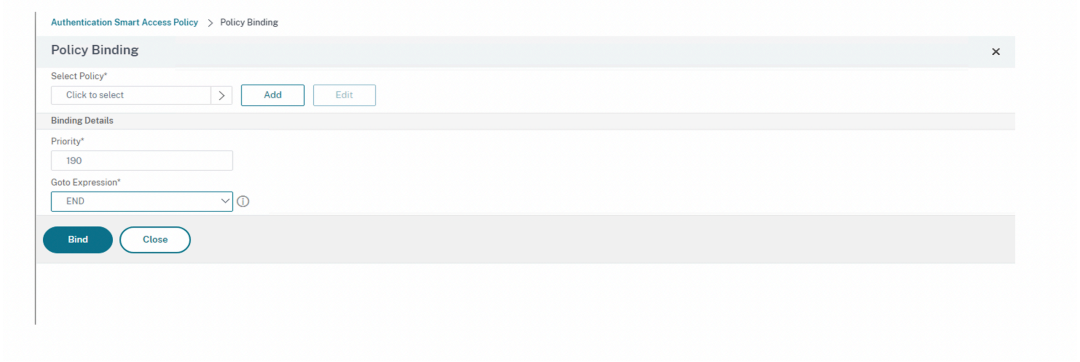
f) 在 **Expression**（表达式）部分中，输入您要为其推送标记的表达式。在本例中，因为要为可信设备推送标记，所以请输入 `AAA.USER.IS_MEMBER_OF("FileExists")`。单击创建。




您将返回到策略绑定屏幕。

g) 选择 *End*（结尾）作为 **Goto Expression**（Goto 表达式），然后单击 **Bind**（绑定）。




4. 为不可信设备创建智能访问策略：

   a) 按照上一步的说明进行操作，子步骤 **v** 和 **vi** 除外。

   b) 对于子步骤 **v**，请在 **Create Authentication Smart Access Profile**（创建身份验证智能访问配置文件）屏幕上，为操作添加名称。在 **Tags**（标记）中输入 *untrusted*（不可信）。稍后将在 Broker 访问策略规则中引用该标记进行配置。单击创建。

   c) 对于子步骤 **vi**，请在 **Create Authentication Smart Access Policy**（创建身份验证智能访问策略）屏幕的 **Expression**（表达式）部分中，输入要推送标记的表达式。在本例中，因为要为不可信设备推送标记，所以请输入 `AAA.USER.IS_MEMBER_OF("FileExists").NOT`。

5. 配置 Broker 访问策略规则：

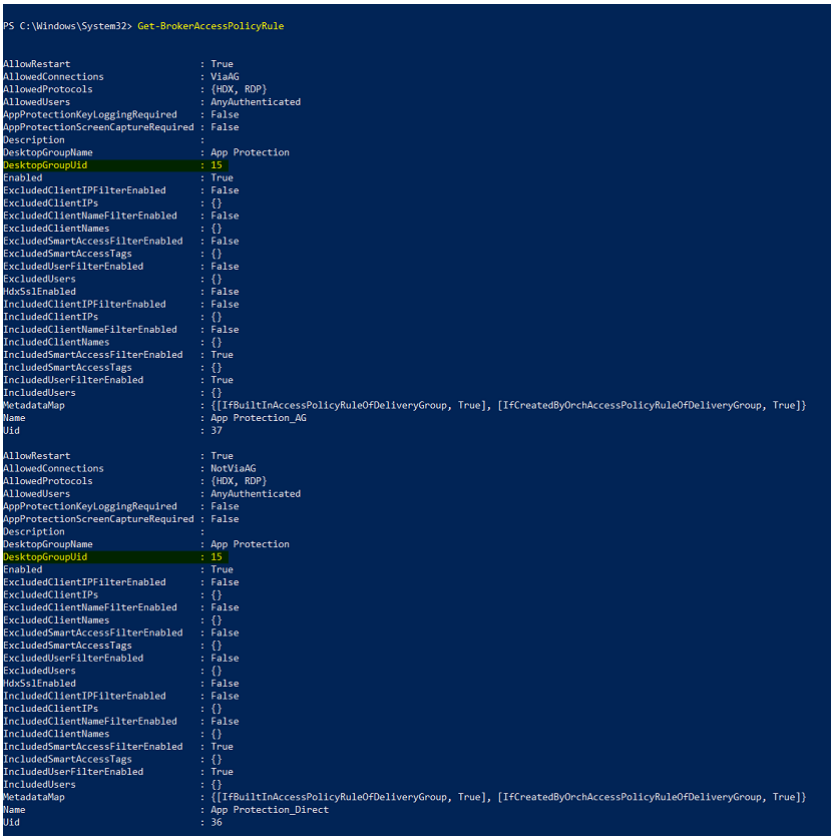
   a) 按照 Citrix 博客 Getting started with PowerShell automation for Citrix Cloud（Citrix Cloud 的 PowerShell 自动化入门）中的说明，安装 Citrix PowerShell SDK 并连接到 Citrix Cloud API。

   b) 运行命令 `Get-BrokerAccessPolicyRule`。

      显示存在的所有交付组的所有 Broker 访问策略的列表。

   c) 找到要更改的交付组的 **DesktopGroupUid**。




d) 使用以下命令获取仅应用于特定交付组的策略：

```
Get-BrokerAccessPolicyRule -DesktopGroupUid 7
```

e) 要过滤使用可信设备的用户，请使用以下命令创建另一个 Broker 访问策略：

```
New-BrokerAccessPolicyRule -Name CAP_Desktops_AG_Trusted-
DesktopGroupUid 7 - AllowedConnections ViaAG -AllowedProtocols
 HDX, RDP -AllowedUsers AnyAuthenticated - AllowRestart $true
 -Enabled $true-IncludedSmartAccessFilterEnabled $true
```

f) 要为可信设备禁用 App Protection，为不可信设备启用 App Protection，请使用以下命令：

```
Set-BrokerAccessPolicyRule CAP_Desktops_AG_trusted -IncludedSmartAcces
 Workspace:trusted -AppProtectionKeyLoggingRequired $false -
AppProtectionScreenCaptureRequired $false

Set-BrokerAccessPolicyRule CAP_Desktops_AG -IncludedSmartAccessTags
 Workspace:untrusted -AppProtectionKeyLoggingRequired $true -
AppProtectionScreenCaptureRequired $true
```

6. 验证：

注销 Citrix Workspace 应用程序并重新登录。从满足 EPA 扫描条件的可信设备启动受保护的资源。您会看到 App Protection 策略未应用。从不受信任的设备启动相同的资源。您会看到 App Protection 策略已应用。

## 场景 3

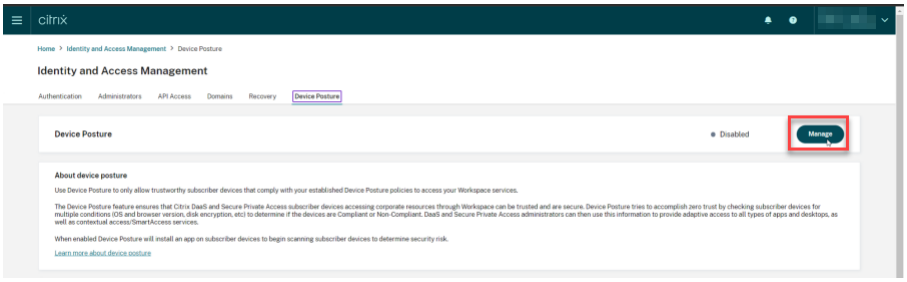
March 10, 2024

此场景介绍了如何根据设备状态结果启用 **App Protection**。

1. 配置设备状态服务：

   a) 登录 Citrix Cloud。

   b) 导航到 **Identity and Access Management**（标识和访问管理）> **Device Posture**（设备状态）并单击 **Manage**（管理）。

   c) 单击 **Create device policy**（创建设备策略）。

   此时将显示 **Create device policy**（创建设备策略）页面。

   d) 在 **Policy rules**（策略规则）下，单击 **Select Rule**（选择规则）下拉菜单，然后选择 *Citrix Workspace App Version*（Citrix Workspace 应用程序版本）。

   e) 单击 **Select a rule**（选择规则）下拉菜单，并选择 *Greater or equal to* >=（大于或等于 >=）。

   f) 输入要设置为条件的 Citrix Workspace 应用程序版本。在此示例中，它是 *23.7.0.19*。

   g) 在 **Policy result**（策略结果）下，选择 **Compliant**（符合标准）。

   h) 在 **Name**（名称）字段中，输入策略的名称。

   i) 在 **Priority**（优先级）字段中，输入策略的优先级。

   j) 选中 **Enable when created**（创建后启用）复选框以在创建策略后将其启用。

   k) 单击创建。

2. 配置 Broker 访问策略规则：

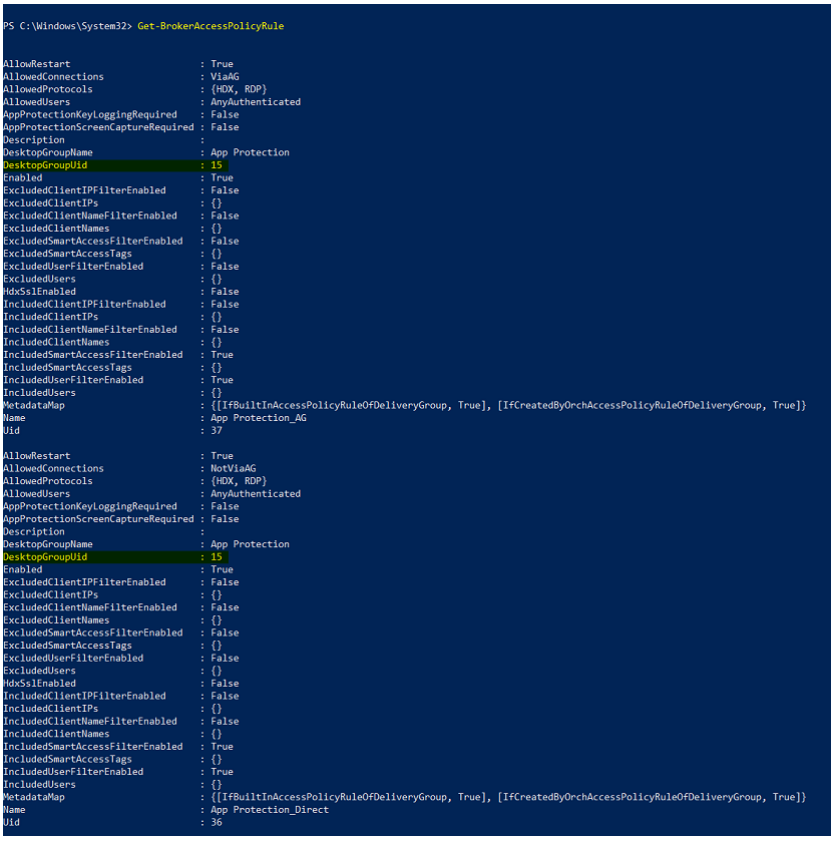
   a) 按照 Citrix 博客 Getting started with PowerShell automation for Citrix Cloud（Citrix Cloud 的 PowerShell 自动化入门）中的说明，安装 Citrix PowerShell SDK 并连接到 Citrix Cloud API。

   b) 运行命令 `Get-BrokerAccessPolicyRule`。

   显示存在的所有交付组的所有 Broker 访问策略的列表。

c) 找到要更改的交付组的 **DesktopGroupUid**。




d) 使用以下命令获取仅应用于特定交付组的策略：

```
Get-BrokerAccessPolicyRule -DesktopGroupUid 7
```

e) 要将 App Protection 应用于符合标准的设备，请运行以下命令：

```
Set-BrokerAccessPolicyRule "Contextual App Protection Delivery
 Group_AG"-IncludedSmartAccessFilterEnabled $true -IncludedSmartAccess
 Workspace:COMPLIANT
```

f) 要将 App Protection 应用于不符合标准的设备，请运行以下命令：

```
New-BrokerAccessPolicyRule "Contextual App Protection Delivery
 Group_AG_NonCompliant"-DesktopGroupUid 7 -AllowedConnections
 ViaAG -AllowedProtocols HDX, RDP -Enabled $true -AllowRestart
 $true -ExcludedSmartAccessFilterEnabled $true -ExcludedSmartAccessTag
 Workspace:COMPLIANT-IncludedSmartAccessFilterEnabled $true
```

3. 验证：

注销 Citrix Workspace 应用程序。从符合设备策略的 Citrix Workspace 应用程序版本登录。您会看到 App Protection 策略未应用。同样，从 Citrix Workspace 应用程序中注销，然后使用不符合设备策略的 Citrix Workspace 应用程序版本登录。您会看到 App Protection 策略已应用。

## 场景 4

March 10, 2024

此场景介绍了如何为特定用户组启用 **App Protection**。

以下步骤允许您为特定组的用户启用 App Protection：

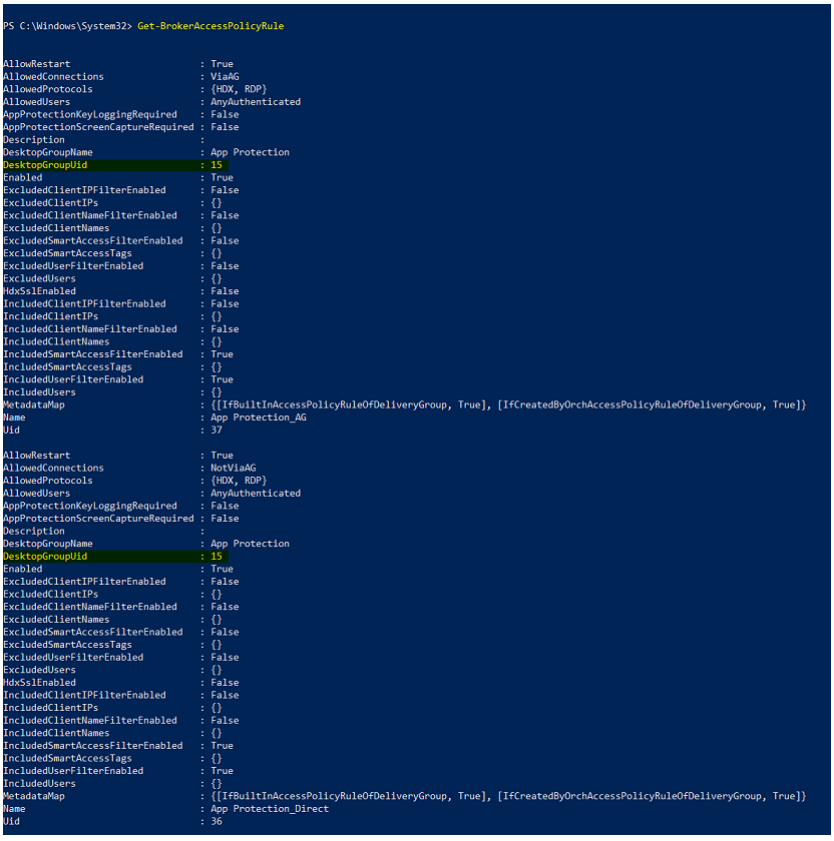
1. 选择要为其中的用户启用 App Protection 策略的 Active Directory 用户组。在此示例中，Active Directory 用户组是 **ProductManagers**。
2. 配置 Broker 访问策略规则：

   a) 按照 Citrix 博客 Getting started with PowerShell automation for Citrix Cloud（Citrix Cloud 的 PowerShell 自动化入门）中的说明，安装 Citrix PowerShell SDK 并连接到 Citrix Cloud API。

   b) 运行命令 `Get-BrokerAccessPolicyRule`。

   显示存在的所有交付组的所有 Broker 访问策略的列表。

   c) 找到要更改的交付组的 **DesktopGroupUid**。




   d) 使用以下命令获取仅应用于特定交付组的策略：

```
Get-BrokerAccessPolicyRule -DesktopGroupUid 7
```

e) 要为 **ProductManagers** 用户组中的用户启用 App Protection 策略，请运行以下命令：

```
New-BrokerAccessPolicyRule "Example Rule Name_1"-DesktopGroupUid
 7 -AllowedConnections AnyViaAG -AllowedProtocols HDX -AllowedUsers
 Filtered -AppProtectionScreenCaptureRequired $true -IncludedUserFilte
 $true -IncludedUsers domain.com\ProductManagers
```

f) 要为不属于 **ProductManagers** 用户组的用户禁用 App Protection 策略，请运行以下命令：

```
New-BrokerAccessPolicyRule "Example Rule Name_2"-DesktopGroupUid
 7 -AllowedConnections AnyViaAG -AllowedProtocols HDX -AllowedUsers
 Filtered -AppProtectionScreenCaptureRequired $false-ExcludedUserFilte
 $true -ExcludedUsers domain.com\ProductManagers
```

3. 验证：

   如果已打开 Citrix Workspace 应用程序，则将其注销。以 **ProductManagers** Active Directory 用户组中某个用户的身份登录 Citrix Workspace 应用程序。启动受保护的资源，您会看到 App Protection 已被禁用。注销 Citrix Workspace 应用程序，然后以不属于 **ProductManagers** Active Directory 用户组的某个用户的身份重新登录。启动受保护的资源，您将看到 App Protection 已启用。

## 适用于 **StoreFront** 的上下文 **App Protection**

March 10, 2024

上下文 App Protection 提供了精细的灵活性，可以根据用户、其设备和网络状况，有条件地为一部分用户应用 App Protection 策略。

### 实施上下文 **App Protection**

您可以使用 Broker 访问策略规则中定义的连接过滤器来实施上下文 App Protection。Broker 访问策略定义的规则用于控制用户能否访问交付组。该策略由一组规则组成。每条规则都关联到单个交付组，并且包含一组连接过滤器和访问权限控件。

当用户的连接详细信息与 Broker 访问策略中的一个或多个规则的连接过滤器匹配时，用户将获得对交付组的访问权限。默认情况下，用户无权访问站点中的任何桌面组。您可以根据要求创建更多 Broker 访问策略。多个规则可以应用于同一个交付组。有关详细信息，请参阅 New-BrokerAccessPolicyRule。

如果用户的连接与访问策略规则中定义的连接过滤器匹配，则 Broker 访问策略规则中的以下参数能够灵活根据上下文启用 App Protection：

- `AppProtectionKeyLoggingRequired`
- `AppProtectionScreenCaptureRequired`

使用 Broker 访问策略中引用的智能访问过滤器来优化连接过滤器。有关配置智能访问过滤器的信息，请参阅 CTX227055。请参考以下场景，了解如何使用智能访问策略设置上下文 App Protection。

> 注意：
>
> 如果在交付组上启用了 App Protection，则默认情况下无法应用上下文 App Protection。使用以下命令在交付组上禁用 App Protection：
>
> ```
> Set-BrokerDesktopGroup -Name "Admin Desktop" -
>    AppProtectionKeyLoggingRequired $false -
>    AppProtectionScreenCaptureRequired $false
> <!--NeedCopy-->
> ```

### 必备条件

要为 StoreFront 启用上下文 App Protection，请确保满足必备条件部分中提到的要求。

### 启用上下文 **App Protection**

1. 从 Citrix 下载页面下载适用于 Citrix Virtual Apps and Desktops 版本的上下文 App Protection 策略（功能表）。
2. 在 Delivery Controller 上运行以下 PowerShell 命令：

   ```
   asnp Citrix*
   Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true
   <!--NeedCopy-->
   ```

3. 运行以下命令以在 Delivery Controller 中启用上下文 App Protection：

   ```
   Import-ConfigFeatureTable <path to the downloaded feature table>
   <!--NeedCopy-->
   ```

   例如，

   ```
   Import-ConfigFeatureTable\Downloads\FeatureTable.OnPrem.
      AppProtContextualAccess.xml
   <!--NeedCopy-->
   ```

### 上下文 **App Protection** 场景

下面是有关如何启用或禁用上下文 App Protection 的一些场景：

- 为某些设备类型禁用 App Protection
- 为从基于浏览器的访问启动的连接禁用 App Protection，并为来自 Citrix Workspace 应用程序的连接启用 App Protection

- 为特定 Active Directory 组中的用户禁用 App Protection
- 根据 EPA 扫描结果为设备启用 App Protection
- 为特定用户组启用 App Protection

## 必备条件

March 10, 2024

请确保您具备以下项：

- Citrix Virtual Apps and Desktops 版本 2109 或更高版本
- Delivery Controller 版本 2109 或更高版本
- StoreFront 版本 1912 LTSR 或更高版本
- VPN 虚拟服务器或网关以及身份验证虚拟服务器配置
- NetScaler 与 StoreFront 之间的成功连接。有关详细信息，请参阅将 NetScaler Gateway 与 StoreFront 集成
- 在 Citrix Virtual Apps and Desktops 2006 版本发布之前，需要导入 XML 表
- 在 Citrix Virtual Apps and Desktops 版本 2209 发布之前，需要导入上下文 App Protection 功能表
- 对于需要智能访问标记的场景，请在 NetScaler Gateway 上启用智能访问。有关详细信息，请参阅此支持文章。
- 许可要求 -
  - App Protection 本地许可证
  - Citrix Gateway 通用许可证适用于使用智能访问标记的场景

## 场景 **1**

March 10, 2024

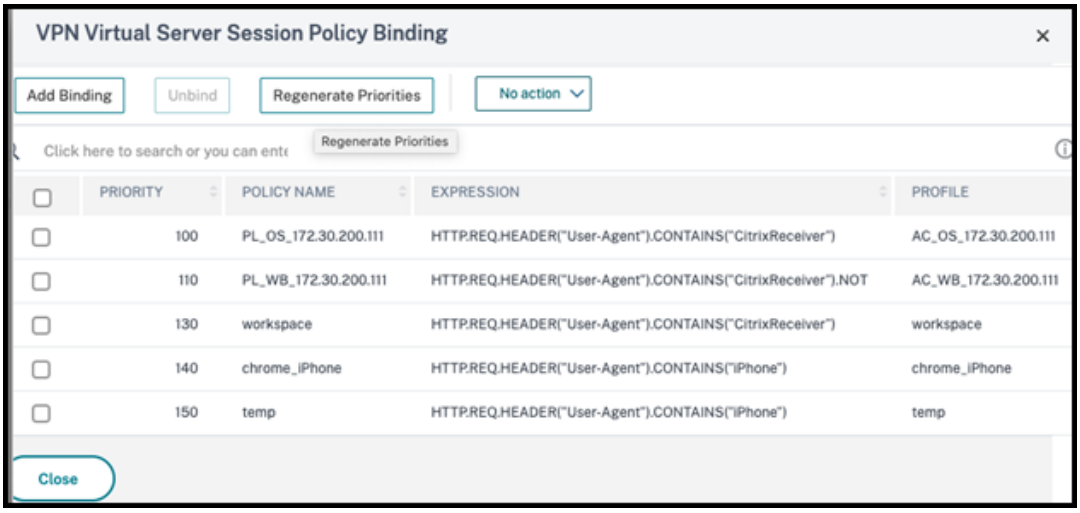
此场景介绍了如何为某些设备类型禁用 **App Protection**。

下面是在名为 `Win10Desktop` 的交付组上为 iPhone 用户禁用 App Protection 的步骤：

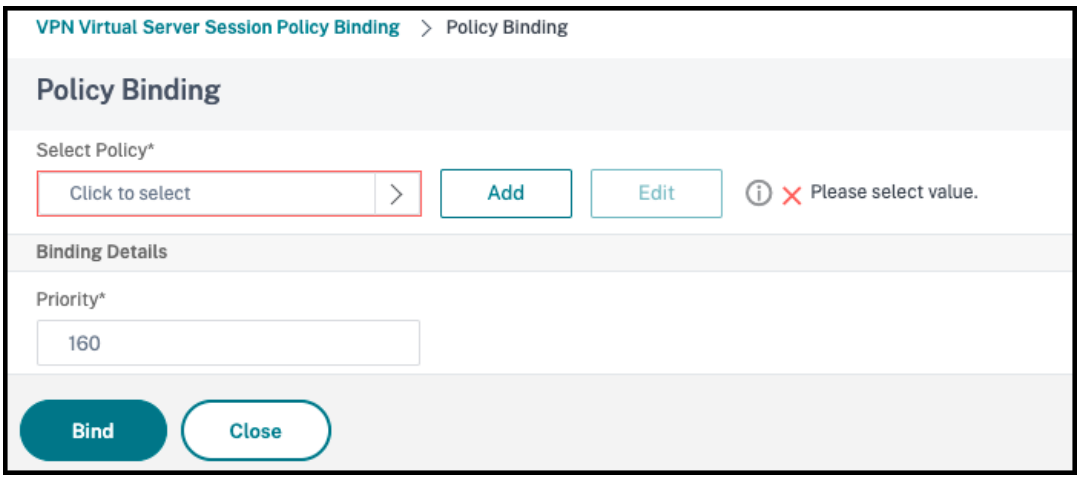
1. 创建一个智能访问策略：
   a) 登录 Citrix ADC 管理 UI。
   b) 在左侧导航菜单中，转到 **Citrix Gateway** > 虚拟服务器。
      记下 VPN 虚拟服务器名称，这是稍后配置 Broker 访问策略所必需的。
   c) 单击 **VPN** 虚拟服务器。滚动到页面底部，然后单击会话策略。此时将显示会话策略列表。

d) 单击 **Add Binding**（添加绑定）。

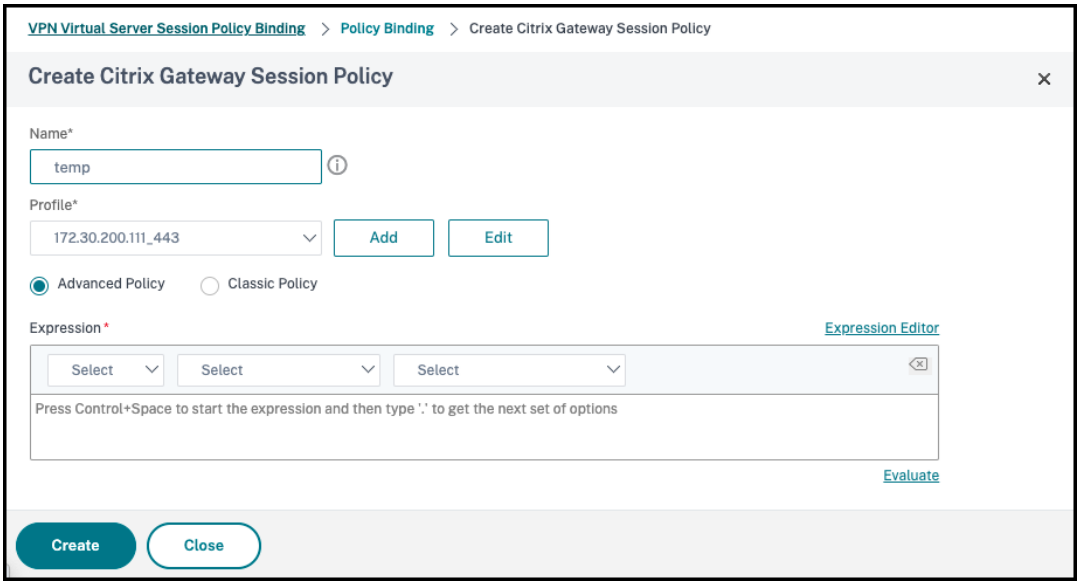



e) 单击添加以创建会话策略。

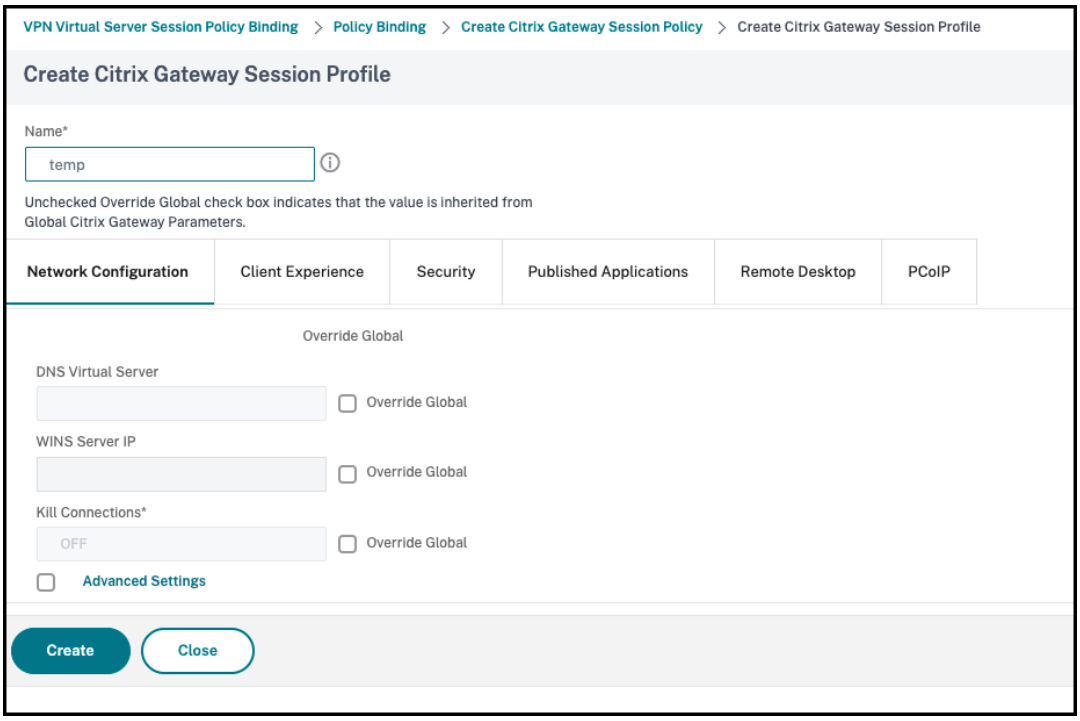



f) 输入会话策略的名称。在此场景中，它是 *temp*。




g) 单击“配置文件”旁边的添加以指定配置文件名称。单击创建。




h) 从“会话策略”窗口中单击表达式编辑器。

i) 创建以下表达式以用于检查用户代理字符串中是否有 *iPhone*：

```
1 HTTP.REQ.HEADER("User-Agent").CONTAINS("iPhone")
2 <!--NeedCopy-->
```


j) 单击绑定以创建会话策略。

2. 创建 Broker 访问策略规则：

要为通过 Access Gateway 访问 `Win10Desktop` 的 iPhone 用户应用该策略，请执行以下步骤：

a) 在 Delivery Controller (DDC) 中运行以下命令：

```
Get-BrokerAccessPolicyRule
<!--NeedCopy-->
```

其中列出了 DDC 中定义的所有 Broker 访问策略。在这种情况下，交付组 `Win10Desktop` 的 Broker 访问策略为 `Win10Desktop_AG` 和 `Win10Desktop_Direct`。为下一个步骤记下交付组的桌面组 UID。

b) 请使用以下命令为 `Win10Desktop` 创建 Broker 访问策略规则，以筛选通过 Access Gateway 访问的 iPhone 用户：

```
New-BrokerAccessPolicyRule -Name Win10Desktop_AG_iPhone -
    DesktopGroupUid <Uid_of_desktopGroup> -AllowedConnections
    ViaAG -AllowedProtocols HDX, RDP -AllowedUsers
    AnyAuthenticated -AllowRestart $true -
    AppProtectionKeyLoggingRequired $false -
    AppProtectionScreenCaptureRequired $false -Enabled $true -
    IncludedSmartAccessFilterEnabled $true
<!--NeedCopy-->
```

**Uid_of_desktopGroup** 是通过在步骤 1 中运行 GetBrokerAccessPolicy 规则所获得的交付组的 DesktopGroupUID。

c) 要为通过 Access Gateway 访问的 `Win10Desktop` iPhone 用户禁用 App Protection，请引用在步骤 1 中创建的智能访问标记 *temp*。使用以下命令创建智能访问策略：

```
Set-BrokerAccessPolicyRule Win10Desktop_AG_iPhone -
    IncludedSmartAccessTags Primary_HDX_Proxy:temp -
    AppProtectionScreenCaptureRequired $false -
    AppProtectionKeyLoggingRequired $false
<!--NeedCopy-->
```

Primary_HDX_Proxy 是在前面步骤 1“创建智能访问策略”中的 VPN 虚拟服务器名称。

d) 要为其余的 `Win10desktop` 用户启用 App Protection 策略，请使用以下命令：

```
Set-BrokerAccessPolicyRule Win10Desktop_AG -
    AppProtectionScreenCaptureRequired $true -
    AppProtectionKeyLoggingRequired $true
<!--NeedCopy-->
```

3. **Verification**（验证）

对于 iPhone：如果已在 iPhone 上打开 Citrix Workspace 应用程序，则将其注销。通过 Access Gateway 连接从外部登录到 Citrix Workspace 应用程序。您可以在 StoreFront 中看到所需的资源，并且必须禁用 App Protection。

对于 iPhone 以外的设备：如果已在设备上打开 Citrix Workspace 应用程序，则将其注销。通过 Access Gateway 连接从外部登录到 Citrix Workspace 应用程序。您可以在 StoreFront 中看到所需的资源，并且必须禁用 App Protection。

## 场景 2

March 10, 2024

此场景介绍了如何为从基于浏览器的访问启动的连接禁用 **App Protection**，以及如何为从 **Citrix Workspace** 应用程序启动的连接启用 **App Protection**。

以下步骤用于在从浏览器启动连接时为名为 `Win10Desktop` 的交付组禁用 App Protection，并为来自 Citrix Workspace 应用程序的连接启用 App Protection：

1. 创建智能访问策略：

a) 创建一个智能访问策略来过滤从 Citrix Workspace 应用程序启动的连接，如前面的场景为某些设备类型禁用 **App Protection** 中所定义。创建以下表达式，用以检查用户代理字符串中是否有 **CitrixReceiver**：

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver")
<!--NeedCopy-->
```

在此场景中，智能访问策略为 `cwa`。

b) 创建另一个智能访问策略 `HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT` 来筛选不是从 Citrix Workspace 应用程序启动的连接。在此案例中，此智能访问策略是 *browser*。


2. 创建 Broker 访问策略规则：

a) 运行 `GetBrokerAccessPolicyRule` 以查看 `Win10Desktop` 的两个 Broker 访问策略。对于交付组 `Win10Desktop`，Broker 访问策略为 `Win10Desktop_AG` 和 `Win10Desktop_Direct`。记下 `Win10Desktop` 的桌面组 UID。

b) 使用以下命令，为 `Win10Desktop` 创建 Broker 访问策略以筛选从 Citrix Workspace 启动的连接。

```
New-BrokerAccessPolicyRule -Name Win10Desktop_AG_CWA -
    DesktopGroupUid <Uid_of_desktopGroup> -AllowedConnections
    ViaAG -AllowedProtocols HDX, RDP -AllowedUsers
    AnyAuthenticated -AllowRestart $true -Enabled $true -
    IncludedSmartAccessFilterEnabled $true
<!--NeedCopy-->
```

**Uid_of_desktopGroup** 是通过在步骤 1 中运行 GetBrokerAccessPolicy 规则所获得的交付组的 DesktopGroupUID。

c) 通过引用智能访问标记 `cwa`，使用以下命令仅为通过 CWA 建立的连接启用 App Protection 策略。

```
Set-BrokerAccessPolicyRule Win10Desktop_AG_CWA -
    IncludedSmartAccessTags Primary_HDX_Proxy:cwa -
    AppProtectionScreenCaptureRequired $true -
    AppProtectionKeyLoggingRequired $true
<!--NeedCopy-->
```

Primary_HDX_Proxy 是在前面步骤 1“创建智能访问策略”中记下的 VPN 虚拟服务器名称。

d) 使用以下命令为通过浏览器建立的其他连接禁用 App Protection 策略：

```
Set-BrokerAccessPolicyRule Win10Desktop_AG -
    IncludedSmartAccessTags Primary_HDX_Proxy:browser -
    AppProtectionScreenCaptureRequired $false -
    AppProtectionKeyLoggingRequired $false
<!--NeedCopy-->
```

3. **Verification**（验证）

如果已打开 Citrix Workspace 应用程序，则将其注销。重新登录 Citrix Workspace 应用程序，然后通过

Access Gateway 从外部连接启动所需的资源。您会看到已为该资源启用 App Protection 策略。通过外部连接从浏览器启动相同的资源，您会看到 App Protection 策略已被禁用。

## 场景 3

March 10, 2024

此场景介绍了如何为特定 **Active Directory** 组中的用户禁用 **App Protection**。

以下步骤用于为属于 Active Directory 组 **xd.local\sales** 的 `Win10Desktop` 用户禁用 App Protection。

1. 运行 `Get-BrokerAccessPolicyRule` 以查看 `Win10Desktop` 的两个 Broker 访问策略。对于交付组 `Win10Desktop`，有两种 Broker 访问策略 `Win10Desktop_AG` 和 `Win10Desktop_Direct`。记下 `Win10Desktop` 的桌面组 UID。
2. 为 `Win10Desktop` 创建 Broker 访问策略规则，以筛选 Active Directory 组 `xd.local\sales` 中的用户建立的连接。

```
1 New-BrokerAccessPolicyRule -Name Win10Desktop_AG_Sales_Group -
      DesktopGroupUid <Uid_of_desktopGroup> -AllowedConnections ViaAG
       -AllowedProtocols HDX, RDP -AllowedUsers Filtered -
      AllowRestart $true -Enabled $true
2 <!--NeedCopy-->
```

   **Uid_of_desktopGroup** 是通过在步骤 1 中运行 GetBrokerAccessPolicy 规则所获得的交付组的 DesktopGroupUID。

3. 使用以下命令禁用 Windows 10 桌面用户（属于 AD 组 **xd.local\sales**）的 App Protection 策略：

```
1 Set-BrokerAccessPolicyRule Win10Desktop_AG_Sales_Group -
      AllowedUsers Filtered -IncludedUsers xd.local\sales -
      IncludedUserFilterEnabled $true -
      AppProtectionScreenCaptureRequired $false -
      AppProtectionKeyLoggingRequired $false
2 <!--NeedCopy-->
```

4. 使用以下命令为除 **xd.local\sales** 中的用户之外的其余网关连接启用 App Protection 策略：

```
1 Set-BrokerAccessPolicyRule Win10Desktop_AG -AllowedUsers
      Anyauthenticated -ExcludedUserFilterEnabled $true -
      ExcludedUsers xd.local\sales -
      AppProtectionScreenCaptureRequired $true -
      AppProtectionKeyLoggingRequired $true
2 <!--NeedCopy-->
```

5. **Verification**（验证）

如果已打开 Citrix Workspace 应用程序，则将其注销。以 **xd.local\sales** Active Directory 组中的用户身份登录 Citrix Workspace 应用程序。启动受保护的资源，您会看到 App Protection 已被禁用。

注销 Citrix Workspace 应用程序，然后以不属于 **xd.local\sales** 的用户的身份重新登录。启动受保护的资源，您将看到 App Protection 已启用。

## 场景 4

March 10, 2024

此场景介绍了如何根据 **EPA** 扫描结果为设备启用 **App Protection**。

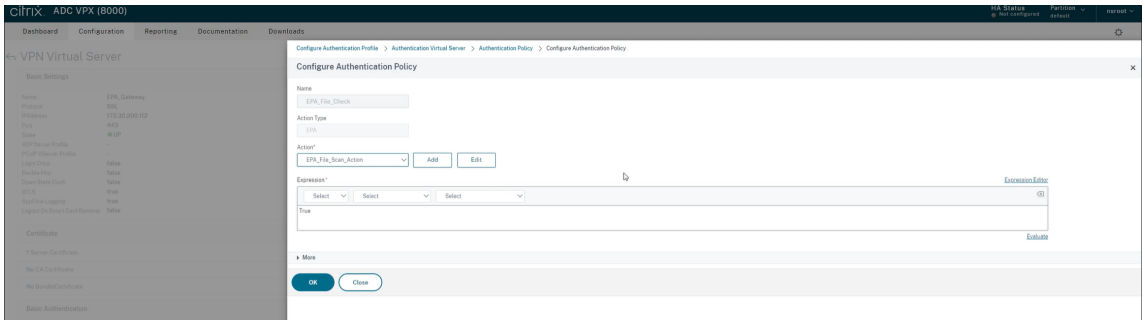
以下步骤用于为通过了 EPA 扫描的设备启用 App Protection：

必备条件：

请确保您具备以下项：

- 身份验证、授权和审核用户组（适用于默认用户组和隔离用户组）及关联的策略
- LDAP 服务器配置和关联的策略

1. 登录到 Citrix ADC 并转到 **Configuration**（配置）> **Citrix Gateway** > **Virtual Servers**（虚拟服务器）。
2. 选择相关的虚拟服务器，然后单击 **Edit**（编辑）。
3. 编辑现有的身份验证配置文件。
4. 选择相关的虚拟服务器，然后单击 **Edit**（编辑）。
5. 单击 **Authentication Policies**（身份验证策略）> **Add Binding**（添加绑定）。
6. 在 **Select Policy**（选择策略）下，单击 **Add**（添加）。
7. 在 **Name**（名称）字段中，输入身份验证策略的名称。
8. 在 **Action Type**（操作类型）下拉列表中，选择 **EPA**。
9. 在 **Expression**（表达式）字段中，输入 `True`。

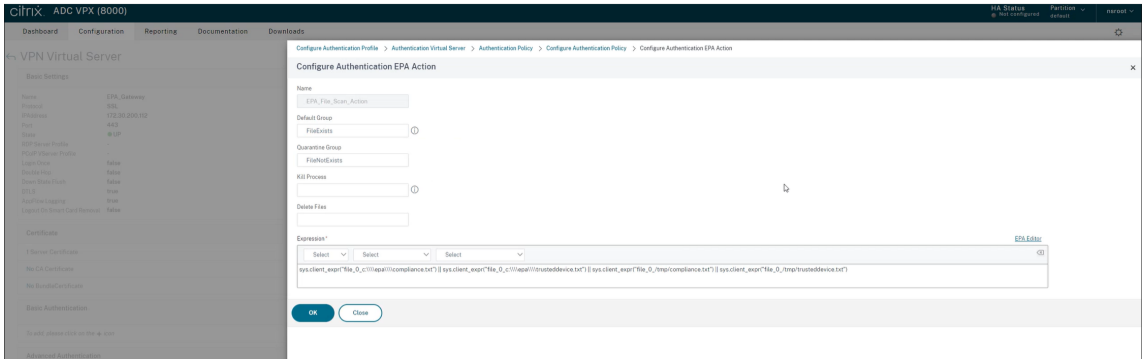



10. 在 **Action**（操作）下，单击 **Add**（添加）。

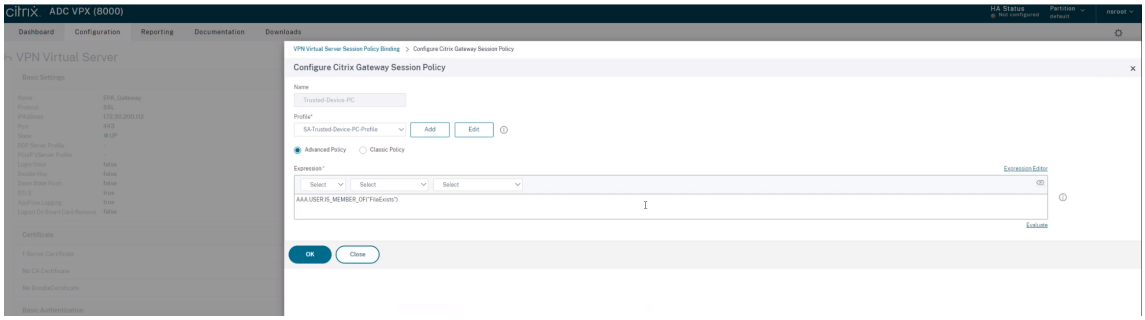
11. 在 **Name**（名称）字段中，输入 EPA 操作的名称。
12. 输入默认组和隔离组的名称。在此场景中，默认组名称为 **FileExists**，隔离组名称为 **FileNotExists**。
13. 在 **Expression**（表达式）字段中，输入以下值：

```
sys.client_expr("file_0_c:\\epa\\compliance.txt") || sys.
    client_expr("file_0_c:\\epa\\trusteddevice.txt") || sys.
    client_expr("file_0_/tmp/compliance.txt") || sys.client_expr("
    file_0_/tmp/trusteddevice.txt")
<!--NeedCopy-->
```




14. 单击 **Create**（创建），然后单击 **Bind**（绑定）。
15. 单击 **Session Policies**（会话策略）> **Add Binding**（添加绑定）。
16. 在 **Select Policy**（选择策略）下，单击 **Add**（添加）。
17. 在 **Name**（名称）字段中，输入会话策略的名称。
18. 在 **Expression**（表达式）字段中，输入以下值：

```
AAA.USER.IS_MEMBER_OF("FileExists")
<!--NeedCopy-->
```




19. 单击 **Create**（创建），然后单击 **Bind**（绑定）。
20. 在任务栏的最左边，单击搜索 图标。
21. 键入 **Powershell** 并打开 **Windows Powershell**。
22. 使用以下命令通过引用智能访问标记“**EPA_GW:Trusted-Device-PC**”为已通过 EPA 扫描的设备禁用 App Protection 策略：

```
Set-BrokerAccessPolicyRule "Contextual App Protection Delivery
    Group_AG" -IncludedSmartAccessFilterEnabled $true -
    IncludedSmartAccessTags EPA_GW:Trusted-Device-PC -
    AppProtectionScreenCaptureRequired $false
<!--NeedCopy-->
```

其中，*EPA_GW* 是 VPN 虚拟服务器的名称。

23. 使用以下命令通过引用智能访问标记“**EPA_GW:Trusted-Device-PC**”为未能通过 EPA 扫描的设备启用 App Protection 策略：

```
New-BrokerAccessPolicyRule "Contextual App Protection Delivery
    Group_AG_NonCompliant"-DesktopGroupUid 17 -AllowedConnections
    ViaAG -AllowedProtocols HDX, RDP -Enabled $true -AllowRestart
    $true -ExcludedSmartAccessFilterEnabled $true -
    ExcludedSmartAccessTags EPA_GW:Trusted-Device-PC -
    IncludedSmartAccessFilterEnabled $true -
    AppProtectionScreenCaptureRequired $true
<!--NeedCopy-->
```

24. **Verification**（验证）

    如果已打开 Citrix Workspace 应用程序，则将其注销。从可信设备登录 Citrix Workspace 应用程序。启动受保护的资源，您会看到 App Protection 已被禁用。

    注销 Citrix Workspace 应用程序，然后从不受信任的设备重新登录。启动受保护的资源，您将看到 App Protection 已启用。

## 场景 **5**

November 21, 2023

此场景介绍了如何为特定用户组启用 **App Protection**。

要为特定组的用户启用 App Protection，请参阅为特定用户组启用 App Protection

## 对通过 **Workspace** 进行的混合启动提供的 **App Protection** 支持

March 10, 2024

Citrix Virtual Apps and Desktops 的混合启动是指您登录适用于 Web 的 Citrix Workspace，方法是在本机浏览器中键入应用商店 URL，然后通过本机 Citrix Workspace 应用程序及其 HDX 引擎启动虚拟应用程序和桌面。“混合”一词是结合使用适用于 Web 的 Citrix Workspace 应用程序与本机 Citrix Workspace 应用程序来连接和使用资源的结果。

> 注意：
>
> 如果没有在端点上安装本机 Citrix Workspace 应用程序组件，则为零安装配置，其中 Citrix Workspace 应用商店和 HDX 引擎都位于浏览器中。此场景称为适用于 HTML5 的 Citrix Workspace 应用程序，托管在 Citrix Workspace 或 Citrix StoreFront 上。本文档未涉及这种情况。

### 必备条件

- 确保您正在使用的浏览器支持 Citrix Workspace Web 扩展程序。
- 确保您的 Workspace URL 的 DNS 后缀为 cloud.com。当前不支持自定义域。
- 请确保您使用的是下面其中一个 Citrix Workspace 应用程序版本：
  - 适用于 Windows 的 Citrix Workspace 应用程序 2106 或更高版本
  - 适用于 macOS 的 Citrix Workspace 应用程序 2106 或更高版本

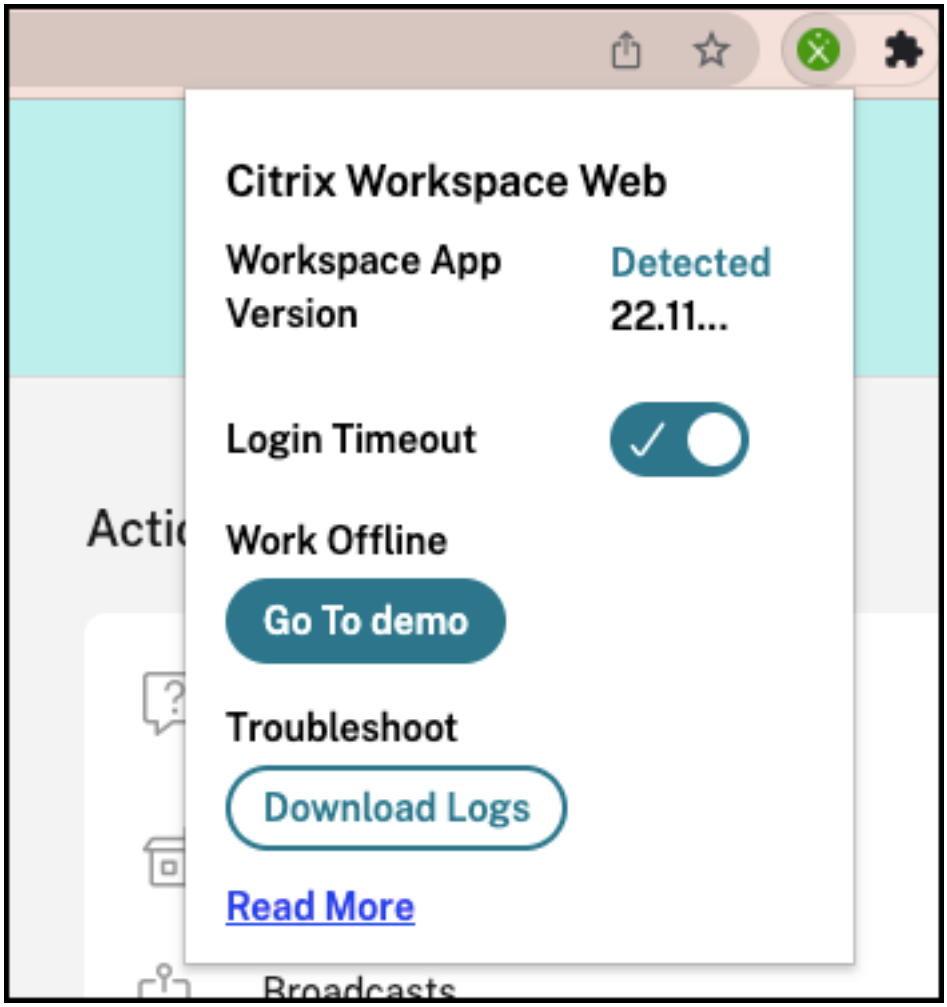
### 为混合启动启用 **App Protection**

1. 在添加应用商店之前，请为浏览器安装 Citrix Workspace Web 扩展程序。请根据您的浏览器使用以下链接之一：

   - Chrome
   - Edge Chromium

   安装该扩展程序后，您将在浏览器的扩展程序部分看到该扩展程序。

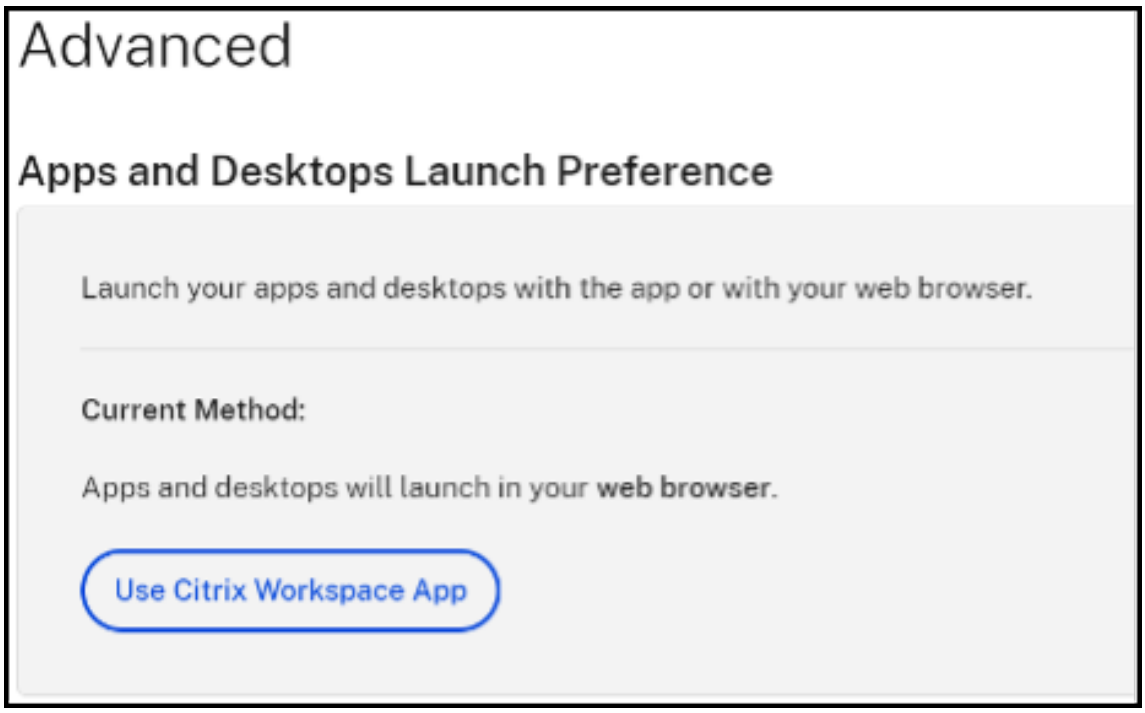
 



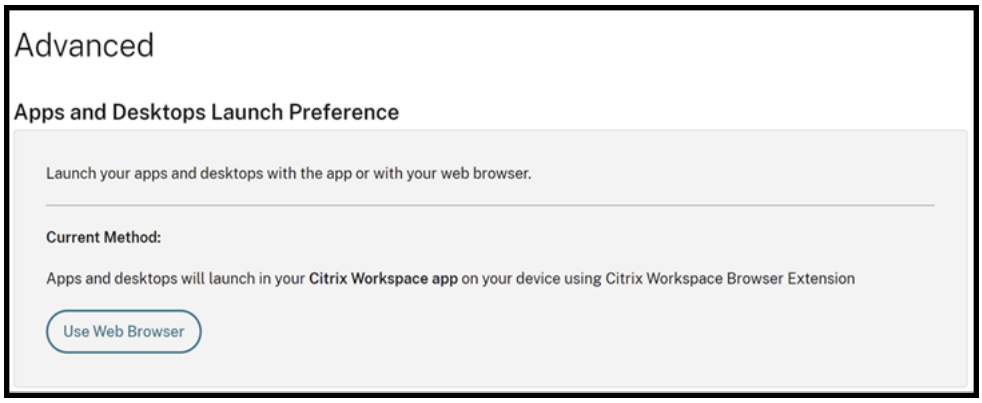

2. 从您的本机浏览器登录应用商店。
3. 导航到您的个人资料 **>** 帐户设置 **>** 高级。

   在应用程序和桌面启动首选项部分中，可以看到应用程序和桌面当前在您的 Web 浏览器中启动的当前方法。单击 **Use Citrix Workspace app**（使用 Citrix Workspace 应用程序）。




如果您使用 Citrix Workspace 应用程序启动资源，则会看到以下选项。在这种情况下，无需进行任何更改。



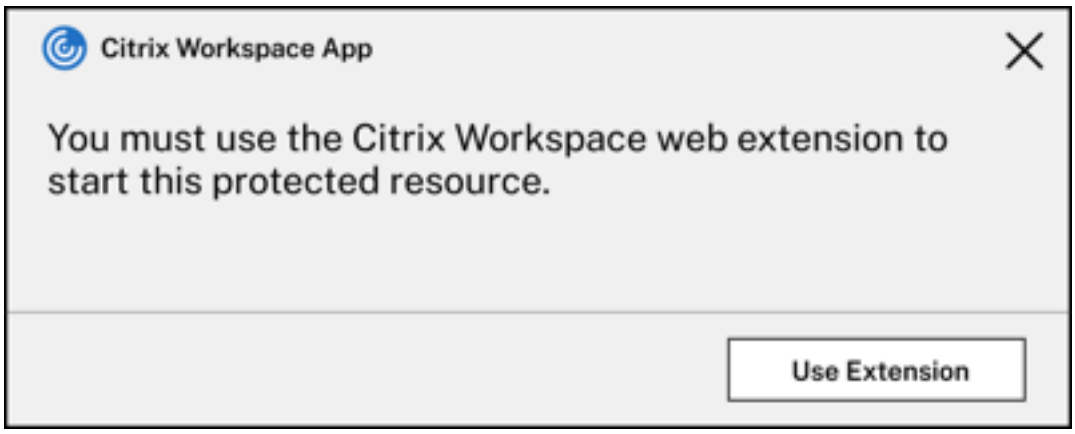

4. 现在，您可以启动受保护的虚拟应用程序或桌面。

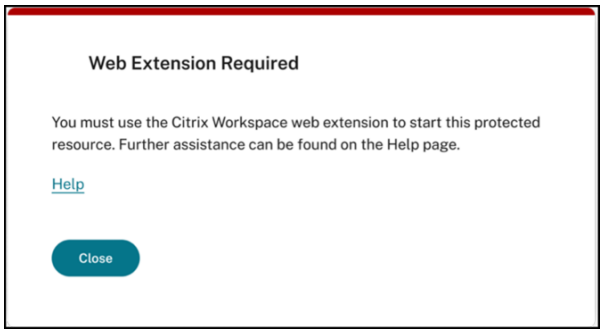
## 常见的故障场景

下面是一些场景，演示了启动失败以及如何修复这些故障。

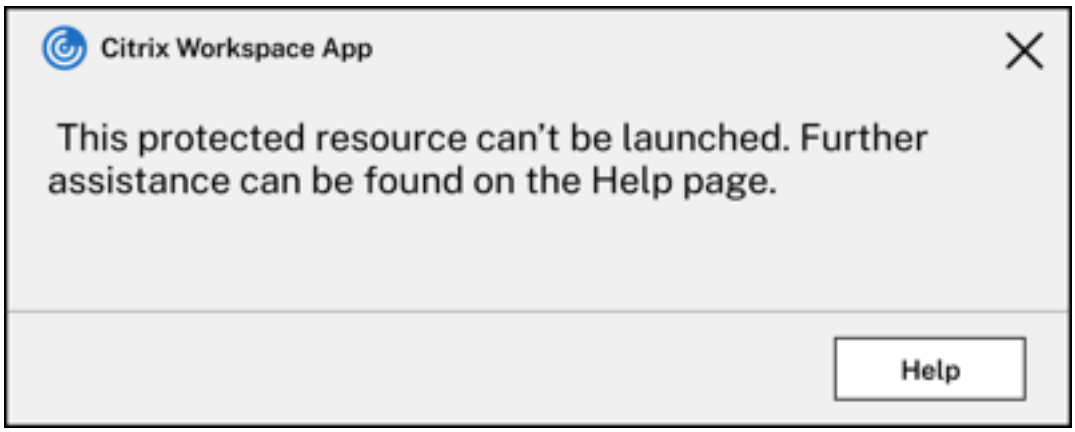
- 在启动受保护的应用程序之前禁用或卸载 Citrix Workspace Web 扩展程序时，会出现以下错误之一。为避免出现这种情况，请在登录适用于 Web 的 Citrix Workspace 之前安装扩展程序。

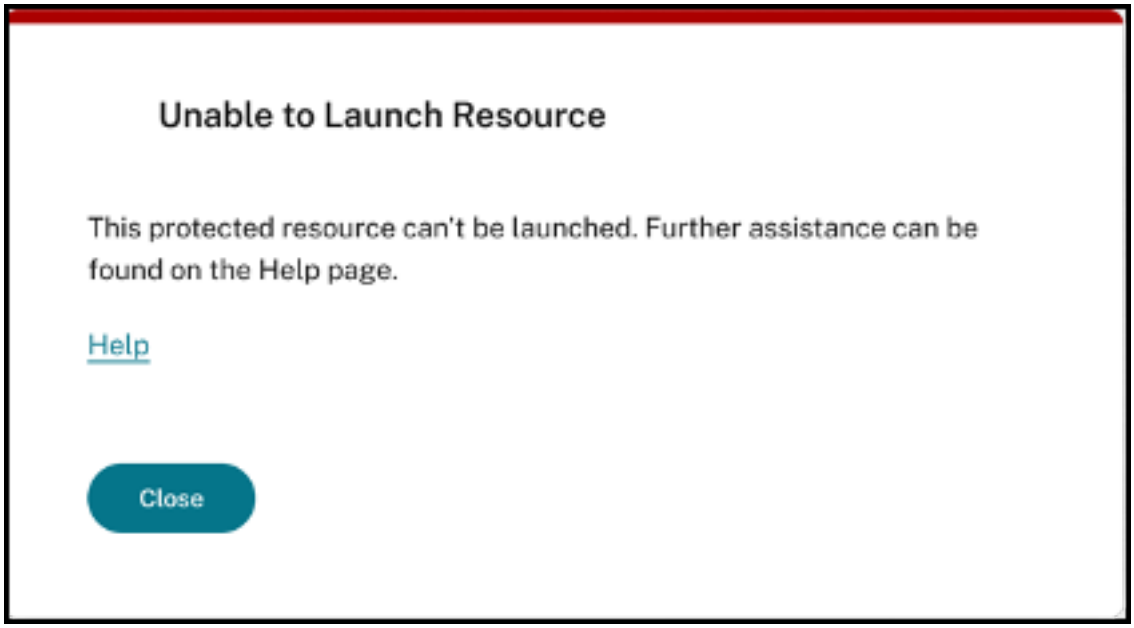



- 如果启动首选项设置为 **Web** 浏览器，则会出现以下错误之一。请将启动首选项更改为使用 **Citrix Workspace** 应用程序以解决此错误。有关详细信息，请参阅此支持文章。






## 对通过 **StoreFront** 进行的混合启动提供的 **App Protection** 支持

March 10, 2024

Citrix Virtual Apps and Desktops 的混合启动是指您通过在本机浏览器中键入应用商店 URL 登录到适用于 Web 的 StoreFront 并通过本机 Citrix Workspace 应用程序及其 HDX 引擎启动虚拟应用程序和桌面。“混合”一词是结合使用适用于 Web 的 StoreFront 与本机 Citrix Workspace 应用程序来连接和使用资源的结果。

> 注意：
>
> 如果没有在端点上安装本机 Citrix Workspace 应用程序组件，则为零安装配置，其中 Citrix Workspace 应用商店和 HDX 引擎都位于浏览器中。这称为适用于 HTML5 的 Citrix Workspace 应用程序，托管在 Citrix Workspace 或 Citrix StoreFront 上。本文档未涉及这种情况。

对通过 StoreFront 进行的混合启动提供的 App Protection 支持提供从浏览器显示和启动启用了 App Protection 的资源的能力。

> 注意：
>
> 如果您选择 **Use light version**（使用简易版）（这将使用 HTML5 客户端）或 **Already installed**（已安装）选项，则启用了 App Protection 的会话将被阻止，因为在浏览器中未成功检测到 Citrix Workspace 应用程序。

如果您使用的是 StoreFront 2308 或更高版本，则可以使用 Web 浏览器访问启用了 App Protection 策略的应用程序和桌面，前提是正确配置了 StoreFront，并且浏览器成功检测到本机 Citrix Workspace 应用程序。如果您使用的是介于 StoreFront 1912 到 2203 之间的版本，则必须按照如何部署部分中所述应用自定义。

> 限制：
>
> 当您首次登录 Web 站点时，StoreFront 会确定 Citrix Workspace 应用程序的版本。如果您之后安装了其他版本的 Citrix Workspace 应用程序，StoreFront 不会知晓这一变化。因此，它可能会错误地允许或禁止启动启用了 App Protection 策略的虚拟应用程序和桌面。Citrix 建议配置 App Protection 状态检查，以阻止从不支持 App Protection 的早期版本的 Citrix Workspace 应用程序启动虚拟应用程序和桌面。有关状态检查的更多信息，请参阅 App Protection 状态检查。

#### 通过 **StoreFront** 版本 **2308** 或更高版本进行的混合启动

StoreFront 版本 2308 及更高版本自动支持启用了 App Protection 策略的虚拟应用程序和桌面的混合启动。有关在 StoreFront 2308 或更高版本中为混合启动启用 App Protection 的更多信息，请参阅面向通过 StoreFront 进行的混合启动的 App Protection。

#### 通过 **StoreFront** 版本 **1912** 到 **2203** 进行的混合启动

StoreFront 版本 1912 到 2203 支持使用自定义设置为启用了 App Protection 策略的虚拟应用程序和桌面启用混合启动，如下所述：

Citrix 建议在升级到 StoreFront 2308 或更高版本时删除此自定义设置。

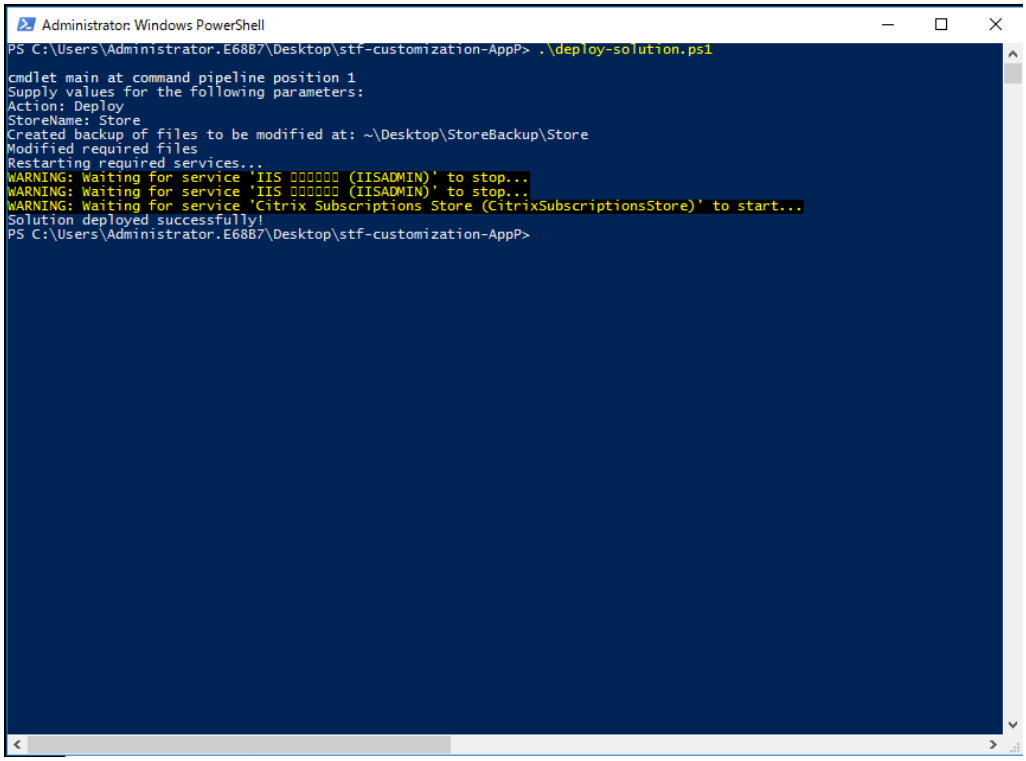
##### 必备条件

有关 App Protection 所需的 Citrix 组件版本的信息，请参阅系统要求。

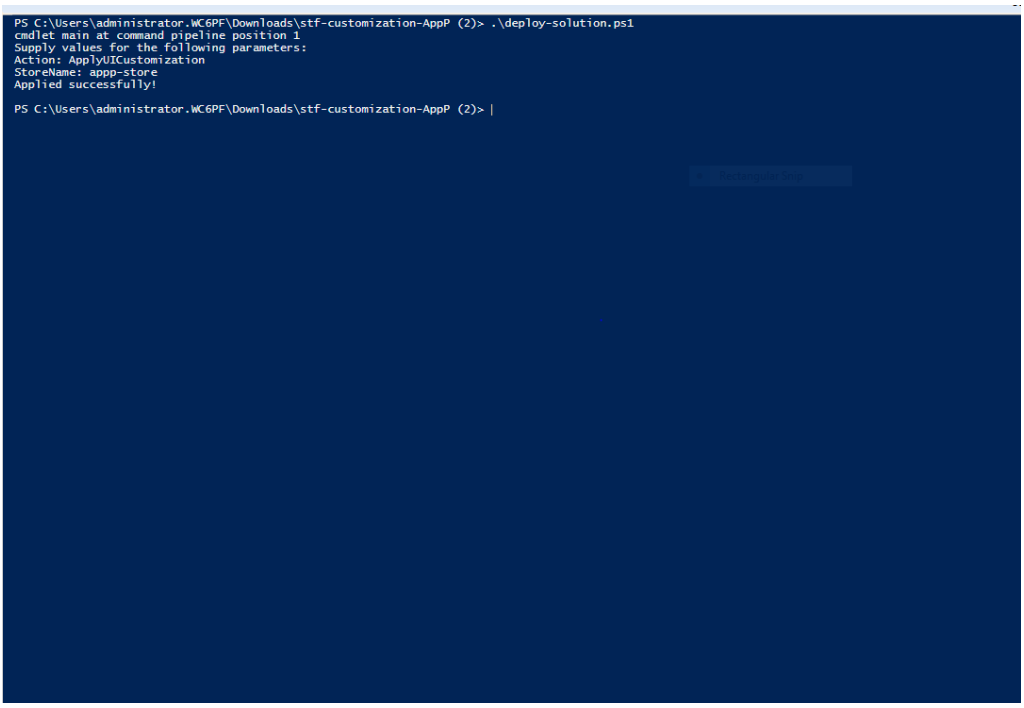
##### 部署方法

1. 下载名为 *stf-customization-AppP.zip* 的 Zip 文件，其中包含必须部署到 StoreFront 服务器计算机的所有必需文件。从 Citrix 下载中下载该文件。该文件包括以下内容：
   - 必须复制到应用商店的 bin 文件夹的 DLL
   - 解决方案正常运行所需的 JavaScript 文件和其他文件
   - *deploy-solution.ps1* PowerShell 脚本，StoreFront 管理员使用该脚本来部署解决方案
2. 解压缩 *stf-customization-AppP.zip* 文件并打开一个新的管理员 PowerShell，在该位置解压相关文件。运行 `deploy-solution.ps1` 命令，该命令采用以下参数：
   - `-Action`：脚本采取的操作。允许使用的值如下：
     - `Deploy` 操作以无缝方式部署解决方案。它会创建此解决方案变更的文件的备份，复制解决方案文件，然后重新启动服务。以下屏幕截图描述了在 StoreFront 服务器上部署解决方案的命令：




- `ApplyUICustomization` 操作对应用商店 UI 应用自定义设置，因此您看不到 **Already installed**（已安装）和 **Use light version**（使用简易版本）选项。此操作强制在浏览器中检测本机 Citrix Workspace 应用程序，并确保您绕过被阻止或不受支持的场景。




- `RemoveUICustomization` 操作会撤消 `ApplyUICustomization` 操作，并再次显示 **Already Installed**（已安装）和 **Use light version**（使用简易版本）选项。

- `-StoreName`：必须对其采取操作的应用商店的名称。此参数是强制性的，必须随 `Deploy` 操作一起传递。
- `-BackupDir`：可以在所需目录下创建备份的 `Deploy` 操作中传递的参数。如果未通过，则在桌面上创建备份。此参数是可选参数。

> 注意：
>
> 如果 *StoreCustomization_Input.dll* 或 *StoreCustomization_Launch.dll* 中有任何现有的自定义设置，则部署此解决方案会覆盖这些自定义设置。

只有在部署自定义设置后，启用了 App Protection 的应用程序和桌面才会显示。如果不进行该部署，则这类应用程序和桌面将无法显示。

#### 如何还原 **StoreFront** 自定义设置

请执行以下步骤以还原之前的 StoreFront 自定义设置：

1. 转到 *\Desktop\StoreBackup< 应用商店名称 >* 目录并将以下文件复制到相应的目录中：应用商店名称 >
   - *StoreCustomization_Input.dll* 和 *StoreCustomization_Launch.dll* 文件到 *IISINETPub\Citrix< 应用商店名称 >\bin* 目录应用商店名称 >
   - *web.config* 文件到 *IISINETPub\Citrix\StoreWeb* 目录
   - **.js* 和 *style.css* 文件到 *IISINETPub\Citrix\StoreWeb\Custom* 目录

     > 注意：
     >
     > 如果 \Desktop\StoreBackup< 应用商店名称 > 目录中除了上述文件之外还有其他自定义设置文件，请根据需要将这些文件和目录复制到相关目录中。应用商店名称 >
2. 打开 PowerShell。
3. 请运行以下命令停止 **IISADMIN** 和 **CitrixSubscriptionsStore** 服务：

```
sc stop IISADMIN
sc stop CitrixSubscriptionsStore
<!--NeedCopy-->
```

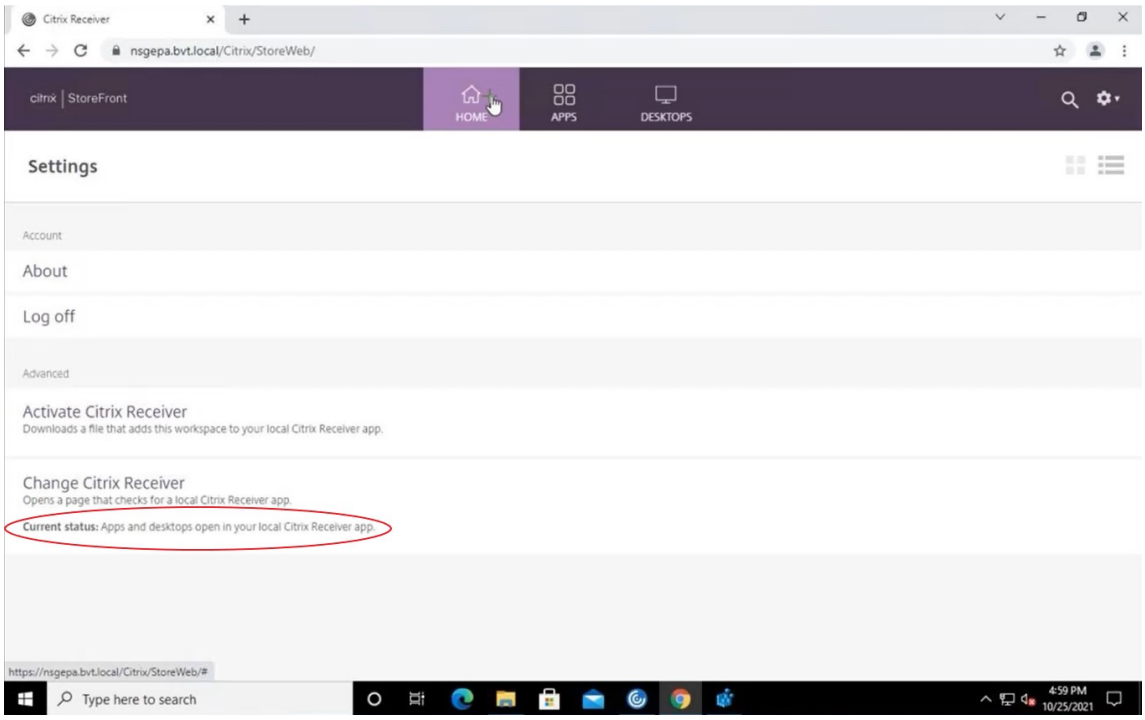
4. 请通过运行以下命令重新启动 **IISADMIN** 和 **CitrixSubscriptionsStore** 服务：

```
sc start IISADMIN
sc start CitrixSubscriptionsStore
<!--NeedCopy-->
```

受保护的资源的混合启动的最终用户体验

1. 在管理员在 StoreFront 服务器上部署解决方案后，在客户端登录您的应用商店，然后在 Web 浏览器中使用 URL 访问 StoreFront。
2. 要查看在浏览器中是否成功检测到 Citrix Workspace 应用程序，请检查您的帐户设置中的当前状态。




检测到 Citrix Workspace 应用程序后，您可以查看并启动所有启用了 App Protection 的虚拟应用程序和桌面。

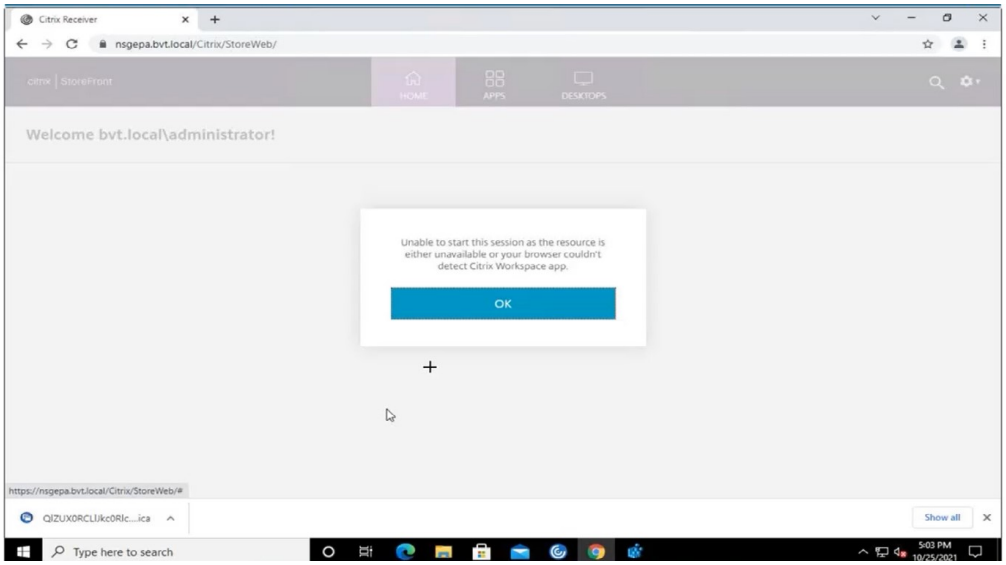
## 在 **StoreFront** 上启用跟踪

要在 StoreFront 中启用跟踪功能，请参阅 StoreFront 文档。此跟踪可用于验证配置的 NetScaler Gateway 会话策略标签是否已正确传递到应用商店。

## 故障排除

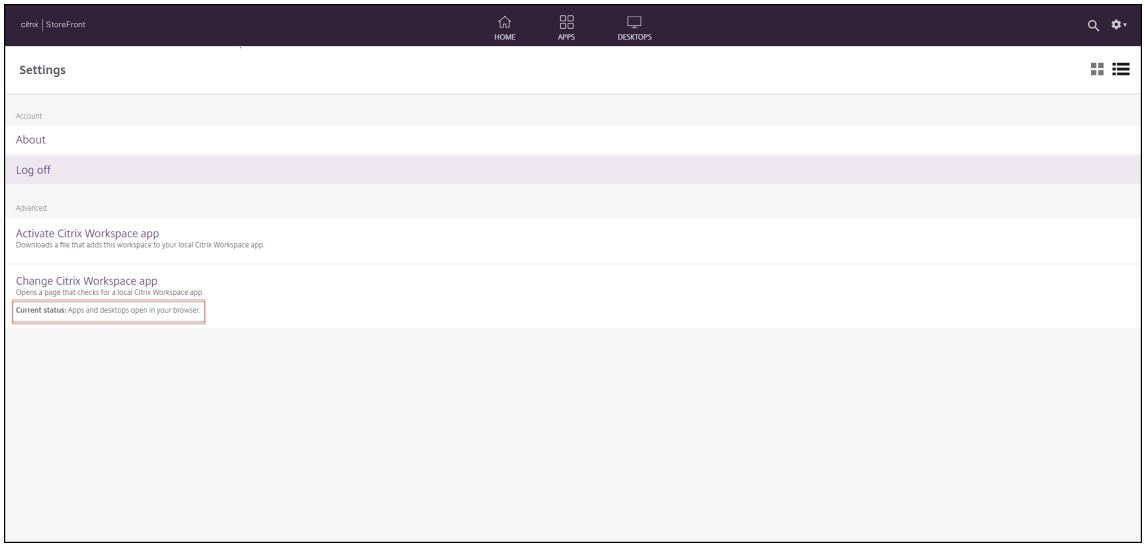
启动启用了 App Protection 的会话时，您有时候可能会遇到以下错误：



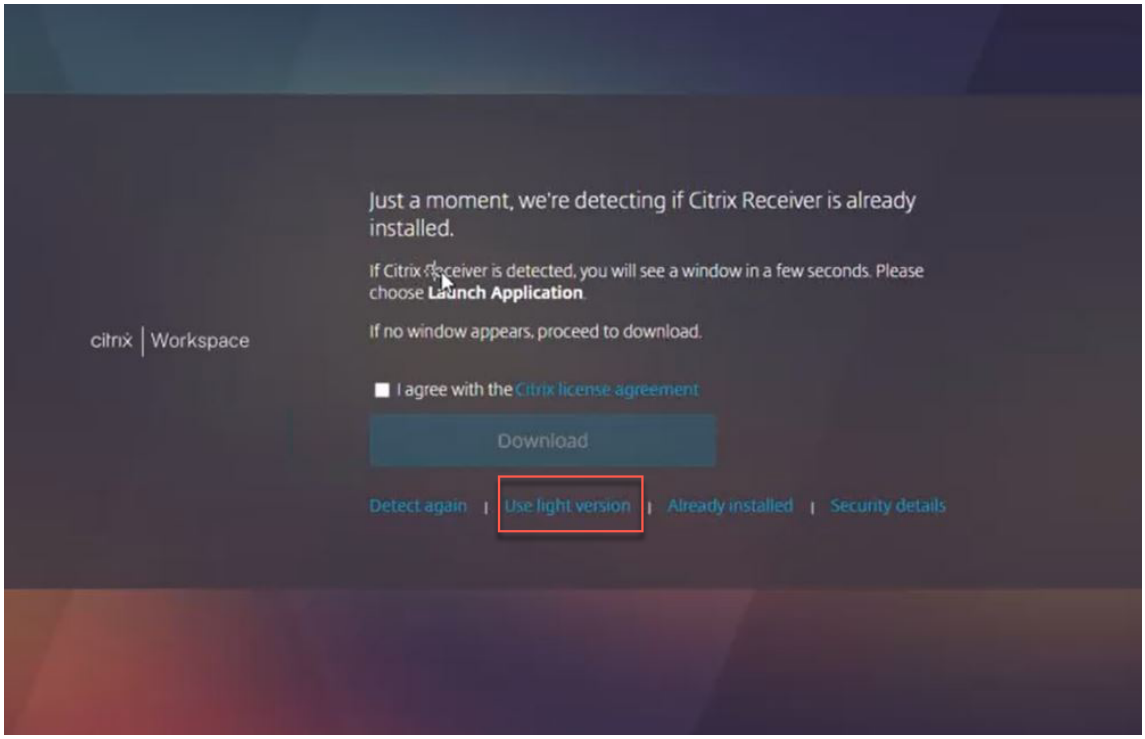

此错误的可能原因如下：

- 应用程序和桌面配置为在浏览器中打开。

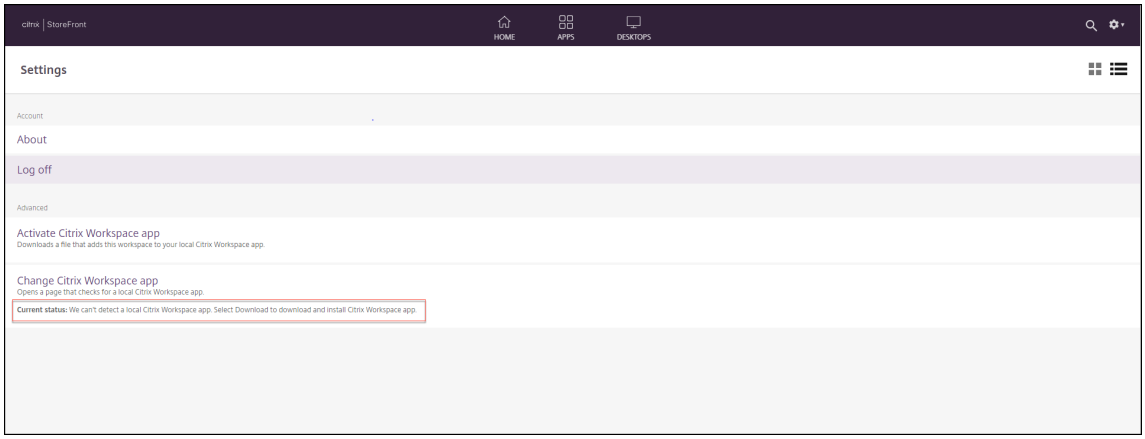



如果您在 Citrix Workspace 应用程序检测期间单击了 **Use light version**（使用简易版），则会遇到这种情况，如以下屏幕所示：

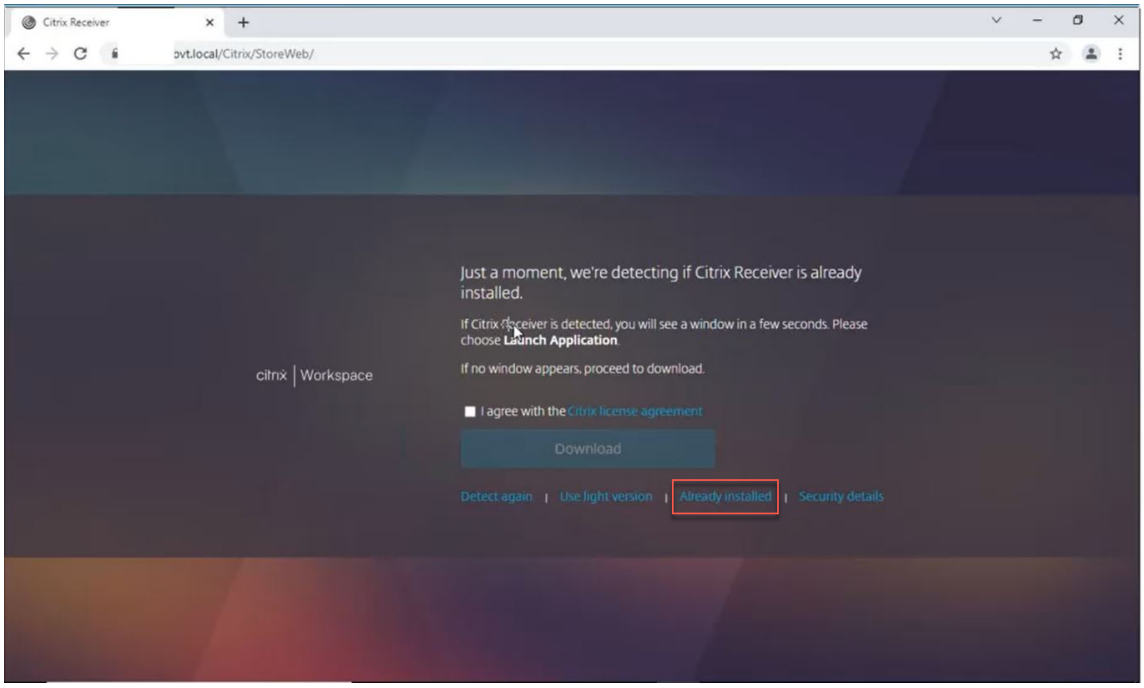



- 浏览器不检测 Citrix Workspace 应用程序。




如果您在 Citrix Workspace 应用程序检测期间单击了 **Already installed**（已安装），则会遇到这种情况，如以下屏幕所示：




解决方案：要更正上述情况并启动启用了 App Protection 的会话，请在帐户设置中单击更改 **Citrix Workspace** 应用程序，然后等待检测到 Citrix Workspace 应用程序。

优化

必须检测 Citrix Workspace 应用程序才能启动启用了 App Protection 的会话。为避免在混合启动受保护的会话时失败，StoreFront 管理员可以使用 `deploy-solution.ps1` 命令的 `ApplyUICustomization` 操作并隐藏 **Use light version**（使用简易版本）和 **Already installed**（已安装）选项。

## Citrix Workspace 应用程序发布时间表

May 30, 2024

此发布时间表说明了 Citrix Workspace 应用程序各版本的目标发布节奏和日期。尽管准确的日期可能会发生变化，我们仍希望提前帮助您制定计划。我们还希望帮助您更加轻松地管理 Citrix Workspace 应用程序部署。

可以从 Citrix Workspace 应用程序下载页面下载新版本。适用于 Android 的 Citrix Workspace 应用程序、适用于 iOS 的 Citrix Workspace 应用程序和适用于 Windows 的 Citrix Workspace 应用程序（应用商店版本）也可以从其各自的应用商店中下载。如果您为适用于 Mac 或 Windows 的 Citrix Workspace 应用程序启用了 Citrix Workspace 应用程序更新，系统将通知您接受下载并安装更新。请考虑订阅我们的 RSS 源，以便在新版本可用时接收警报。

有关每个 Citrix Workspace 应用程序中提供的功能的详细信息，请参阅 Citrix Workspace app feature matrix (Citrix Workspace 应用程序功能列表)。

有关生命周期的信息，请参阅 Citrix Workspace 应用程序的生命周期。

### 目标发布节奏

以下 Citrix Workspace 应用程序平台遵循每季度发布一次的节奏：

- Linux
- Mac
- Windows

以下 Citrix Workspace 应用程序平台遵循每六周发布一次的节奏：

- ChromeOS
- HTML5

以下 Citrix Workspace 应用程序平台遵循每月发布一次的节奏：

- Android
- iOS

> 注意：
>
> 将来，适用于 Windows 的 Citrix Workspace 应用程序、适用于 Mac 的 Citrix Workspace 应用程序、适用于 Android 的 Citrix Workspace 应用程序和适用于 iOS 的 Citrix Workspace 应用程序将在一个季度内发布主要版本和次要版本。次要版本将标记为“.10”，这些版本将包括有关质量和性能改进的细微改进。次要“.10”版本预计没有任何主要功能。

### 桌面应用程序的目标发布日期

| Citrix Workspace 应用程序 | 2024 年 2 月 | 2024 年 3 月 | 2024 年 4 月 | 2024 年 5 月 | 2024 年 6 月 | 2024 年 7 月 | 2024 年 8 月 | 2024 年 9 月 | 2024 年 10 月 | 2024 年 11 月 | 2024 年 12 月 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Windows | - | ☑ | ☑ | ☒ | - | ☑ | ☒ | - | ☑ | - | |
| Windows LTSR | ☒ | - | ☑ | - | ☒ | - | - | ☒ | - | - | ☒ |
| Mac | - | - | ☑ | ☒ | ☑ | - | ☑ | ☒ | - | ☑ | - |

| Citrix Workspace 应用程序 | 2024 年 2 月 | 2024 年 3 月 | 2024 年 4 月 | 2024 年 5 月 | 2024 年 6 月 | 2024 年 7 月 | 2024 年 8 月 | 2024 年 9 月 | 2024 年 10 月 | 2024 年 11 月 | 2024 年 12 月 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Chrome OS 和 HTML5 | ☑ | - | ☑ | ☑ | ☑ | - | ☑ | ☑ | ☑ | - | ☑ |
| Linux | - | ☑ | - | ☑ | - | - | ☑ | - | - | ☑ | - |

注意：

☑ 符号表示主要版本，☒ 符号表示次要版本。

☒ 符号表示累积更新 (CU)。

手机和平板电脑应用程序的目标发布日期

适用于 Android 的 Citrix Workspace 应用程序和适用于 iOS 的 Citrix Workspace 应用程序遵循每月发布一次的节奏。

| Citrix Workspace 应用程序 | 2024 年 3 月 | 2024 年 4 月 | 2024 年 5 月 | 2024 年 6 月 | 2024 年 7 月 | 2024 年 8 月 | 2024 年 9 月 | 2024 年 10 月 | 2024 年 11 月 | 2024 年 12 月 |
|---|---|---|---|---|---|---|---|---|---|---|
| Android 和 iOS | ☑ | ☒ | ☑ | ☒ | ☑ | ☒ | ☑ | ☒ | ☑ | ☒ |

| Citrix Workspace 应用程序 | 2024 年 3 月 | 2024 年 4 月 | 2024 年 5 月 | 2024 年 6 月 | 2024 年 7 月 | 2024 年 8 月 | 2024 年 9 月 | 2024 年 10 月 | 2024 年 11 月 | 2024 年 12 月 |
|---|---|---|---|---|---|---|---|---|---|---|

注意：

☑ 符号表示主要版本，☒ 符号表示次要版本。次要版本是指为满足特定要求或改进功能而量身定制的可选版本。

> 免责声明：
>
> 我们的产品的开发、发布和执行时间仍由我们自行决定，如有变更，恕不另行通知或协商。所提供的数据仅供参考，并不是提供任何资料、代码或功能的保证、承诺或法律义务，并且不应依赖于制定购买决策或纳入任何合同。

## Citrix Workspace 应用程序功能列表

June 19, 2024

Citrix Workspace 应用程序提供跨不同平台或操作系统分布的许多功能。通过此功能列表，您可以清楚地了解这些功能在不同平台上的可用性。在每个部分中，除了功能列表外，您还可以找到简要描述每项功能的功能定义表。

### Citrix Workspace

| 功能 | Windows 2403.1 和 Windows 应用商店 2403.1 | Windows 2402 LTSR | Linux 2405 | Mac 2402.10 | iOS 24.5.0 | Android 24.5.0 | HTML5 2404.1 | ChromeOS 2405 |
|---|---|---|---|---|---|---|---|---|
| Citrix Virtual Apps | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| Citrix Virtual Desktops | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| Citrix Secure Private Access | 是 | 是 | 否 | 是 | 是 | 是 | 否 | 否 |
| Citrix Enterprise Browser（以前称为 Citrix Workspace Browser） | 是 | 否 | 是 | 是 | 否 | 否 | 否 | 否 |
| 具有 SSO 功能的 Web/SaaS 应用程序 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| Citrix 移动应用程序 | 否 | 否 | 否 | 否 | 是 | 是 | 否 | 否 |
| 应用程序个性化服务 | 是 | 否 | 否 | 是 | 是 | 是 | 否 | 否 |

| 功能 | 定义 |
| --- | --- |
| Citrix Virtual Apps | 通过 Citrix DaaS 或 Citrix Virtual Apps and Desktops 授权访问 Citrix Virtual Apps。 |
| Citrix Virtual Desktops | 通过 Citrix DaaS 或 Citrix Virtual Apps and Desktops 授权访问 Citrix Virtual Desktops。 |
| Citrix Secure Private Access | 借助 Citrix Secure Private Access，IT 管理员可以管理对已审批的 SaaS 应用程序的访问权限。此外，借助简化的单点登录体验，管理员可以通过过滤对特定 Web 站点和 Web 站点类别的访问来保护组织的网络和最终用户设备免受恶意软件和数据泄露的侵害。 |
| Citrix Enterprise Browser | Citrix Workspace 应用程序随附的浏览器，用于安全访问 SaaS 和 Web 应用程序。 |
| 具有 SSO 功能的 Web/SaaS 应用程序 | 访问使用带 SSO 的 Secure Workspace Access 配置的 SaaS/Web 应用程序。 |
| Citrix 移动应用程序 | 访问由 Citrix Endpoint Management（以前称为 XenMobile）聚合的 Citrix 移动应用程序。 |
| Citrix 移动应用程序升级 | 访问由 Citrix Endpoint Management（以前称为 XenMobile）聚合的 Citrix 移动应用程序。 |
| 应用程序个性化服务 | 允许拥有个性化的企业体验。您可以在整个应用程序工作流中为 Citrix Workspace 应用程序设置自定义应用程序名称和联名图标。 |

## Workspace 管理

| 功能 | Windows 2403.1 和 Windows 应用商店 2403.1 | Windows 2402 LTSR | Linux 2405 | Mac 2402.10 | iOS 24.5.0 | Android 24.5.0 | HTML5 2404.1 | ChromeOS 2405 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 使用 DNS 自动配置进行电子邮件发现 | 是 | 是 | 否 | 是 | 是 | 是 | 否 | 否 |
| 集中管理设置 | 是 | 是 | 是 | 否 | 否 | 否 | 否 | 是 |

| 功能 | Windows 2403.1 和 Windows 应用商店 2403.1 | Windows 2402 LTSR | Linux 2405 | Mac 2402.10 | iOS 24.5.0 | Android 24.5.0 | HTML5 2404.1 | ChromeOS 2405 |
|---|---|---|---|---|---|---|---|---|
| Global App Config Service (Workspace) | 是 | 是 | 否 | 是 | 是 | 是 | 是 | 是 |
| Global App Config Service (StoreFront) | 是 | 是 | 否 | 是 | 是 | 是 | 是 | 是 |
| App Store 更新 | 否 | 否 | 否 | 否 | 是 | 是 | 否 | 否 |
| Citrix 自动更新 | 是 | 是 | 否 | 是 | 否 | 否 | 否 | 否 |
| 客户端应用程序管理 | 是 | 否 | 否 | 否 | 不适用 | 不适用 | 不适用 | 不适用 |

| 功能 | 定义 |
|---|---|
| 使用 DNS 自动配置进行电子邮件发现 | 允许通过自动发现的设置配置 Citrix Workspace 应用程序。 |
| 集中管理设置 | 来自集中式服务的应用程序设置，例如 Google Chrome 管理或 GPO。 |
| Global App Config Service (Workspace) | 适用于 Citrix Workspace 的 Global App Configuration Service 使 Citrix 管理员能够通过集中管理的服务提供 Workspace 服务 URL 和 Citrix Workspace 应用程序设置。 |

| 功能 | 定义 |
| --- | --- |
| Global App Config Service (StoreFront) | 适用于 Citrix StoreFront 的 Global App Configuration Service 允许 Citrix 管理员通过集中管理的服务交付 Citrix Workspace 应用程序设置。 |
| App Store 更新 | 来自供应商应用商店的更新 |
| Citrix 自动更新 | 通过 Citrix 自动升级功能提供的面向 Windows 和 Mac 的更新 |
| 客户端应用程序管理 | 使 Citrix Workspace 应用程序成为端点上安装和管理 Secure Access Agent 和 End Point Analysis (EPA) 插件等代理所需的单一客户端应用程序。借助此功能，管理员可以轻松地从单个管理控制台部署和管理所需的代理。 |

用户界面

| 功能 | Windows 2403.1 和 Windows 应用商店 2403.1 | Windows 2402 LTSR | Linux 2405 | Mac 2402.10 | iOS 24.5.0 | Android 24.5.0 | HTML5 2404.1 | ChromeOS 2405 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Desktop Viewer/工具栏 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| 多任务处理 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| “关注我”会话（工作区控制） | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| 功能 | 定义 |
| --- | --- |
| Desktop Viewer/工具栏 | 允许在会话中控制会话功能，例如通过工具栏发送 Ctrl+Alt+Del。 |
| 多任务处理 | 允许同时使用多个应用程序和桌面。 |
| “关注我”会话（工作区控制） | 允许用户在设备之间移动并自动连接到其所有会话。 |

### HDX 主机核心

| 功能 | Windows 2403.1 和 Windows 应用商店 2403.1 | Windows 2402 LTSR | Linux 2405 | Mac 2402.10 | iOS 24.5.0 | Android 24.5.0 | HTML5 2404.1 | ChromeOS 2405 |
|---|---|---|---|---|---|---|---|---|
| 自适应传输 | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| HDX 自适应吞吐量 | 是 | 是 | 否 | 否 | 否 | 否 | 否 | 否 |
| SDWAN 支持 | 是 | 是 | 是 | 是 | 否 | 否 | 是 | 是 |
| 会话可靠性 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| 客户端自动重新连接 | 是 | 是 | 是 | 是 | 否 | 是 | 否 | 否 |
| 会话共享 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| 多端口 ICA | 是 | 是 | 是 | 否 | 否 | 否 | 否 | 否 |

| 功能 | 定义 |
|---|---|
| 自适应传输 | 启用 HDX 的 EDT 传输以提高吞吐量，不受网络条件影响。 |
| SDWAN 支持 | 支持对 QoS、TCP、压缩和重复数据消除执行 SDWAN 加速。 |
| 会话可靠性 | 使会话在网络连接中断时保持活动状态并显示在用户的屏幕上。 |
| 客户端自动重新连接 | 连接中断时提示并重新连接会话。 |
| 会话共享 | 已在同一服务器上运行时，使已发布的应用程序能够通过与其他已发布的应用程序相同的连接运行。 |
| 多端口 ICA | 允许支持为 HDX 流量使用多个 TCP 端口，以提高服务质量。 |

### HDX IO/设备/打印

| 功能 | Windows 2403.1 和 Windows 应用商店 2403.1 | Windows 2402 LTSR | Linux 2405 | Mac 2402.10 | iOS 24.5.0 | Android 24.5.0 | HTML5 2404.1 | ChromeOS 2405 |
|---|---|---|---|---|---|---|---|---|
| 本地打印 | 是 | 是 | 是 | 是 | 是 | 否 | 是 | 是 |
| 通用 USB 重定向 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| 客户端驱动器映射/文件传输 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| TWAIN 2.0 | 是 | 否 | 否 | 否 | 否 | 否 | 否 | 否 |

| 功能 | 定义 |
|---|---|
| 本地打印 | 使用户能够通过共享打印机或本地打印机打印文档。 |
| 通用 USB 重定向 | 允许在会话中使用 USB 设备。例如，键盘、鼠标、外部网络摄像机等。 |
| 客户端驱动器映射/文件传输 | 允许使用内置或连接的客户端驱动器进行数据存储。 |
| TWAIN | 允许映射客户端 TWAIN 设备，例如数码相机或扫描仪。 |

### HDX 集成

| 功能 | Windows 2403.1 和 Windows 应用商店 2403.1 | Windows 2402 LTSR | Linux 2405 | Mac 2402.10 | iOS 24.5.0 | Android 24.5.0 | HTML5 2404.1 | ChromeOS 2405 |
|---|---|---|---|---|---|---|---|---|
| 本地应用程序访问 | 是 | 是 | 否 | 否 | 否 | 否 | 否 | 否 |
| 多点触控 | 是 | 是 | 否 | 否 | 是 | 是 | 是 | 是 |

| 功能 | Windows 2403.1 和 Windows 应用商店 2403.1 | Windows 2402 LTSR | Linux 2405 | Mac 2402.10 | iOS 24.5.0 | Android 24.5.0 | HTML5 2404.1 | ChromeOS 2405 |
|---|---|---|---|---|---|---|---|---|
| Mobility Pack | 是 | 是 | 否 | 否 | 是 | 是 | 是 | 是 |
| HDX Insight | 是 | 是 | 是 | 是 | 否 | 否 | 是 | 是 |
| 通过 NSAP VC 获得的 HDX 见解 | 是 | 是 | 是 | 是 | 是 *(3)* | 是 *(3)* | 否 | 否 |
| EUEM 体验列表 | 是 | 是 | 是 | 是 | 否 | 是 | 是 | 是 |
| 双向内容重定向 | 是 | 是 | 否 | 否 | 否 | 否 | 否 | 否 |
| URL 重定向 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| 浏览器内容重定向 | 是 | 否 | 是 | 否 | 否 | 否 | 否 | 是 |
| 在 Citrix Workspace 应用程序中打开文件 | 是 | 是 | 是 | 否 | 是 | 是 | 否 | 是 |
| 基于位置的服务（位置可通过 API 描述获得） | 是 | 是 | 否 | 否 | 是 | 是 | 否 | 否 |

| 功能 | 定义 |
|---|---|
| 本地应用程序访问 | 在会话中访问客户端设备上的本地应用程序。 |
| 多点触控 | 启用 Windows/Linux 桌面和应用程序的十指多点触控控制。 |

| 功能 | 定义 |
| --- | --- |
| Mobility Pack | 启用本机设备体验功能（例如，自动弹出键盘和本地设备用户界面控件）和平板电脑优化的桌面。 |
| HDX Insight | 使用 ICA 网络性能指标提供会话启动/结束时间的可见性。 |
| 通过 NSAP VC 获得的 HDX 见解 | 使用 NetScaler App Experience 或 NSAP 虚拟通道提供会话启动/结束时间的可见性，以获得 HDX 见解。 |
| EUEM 体验列表 | 通过以前称为 XenDesktop 7 Director 的 Citrix Virtual Desktops，让 Citrix 管理员能够查看登录持续时间指标。 |
| 双向内容重定向 | 启用客户端到主机和主机到客户端 URL 重定向。 |
| URL 重定向 | 允许在客户端上本地运行应用程序。 |
| 浏览器内容重定向 | 允许将整个 Web 页面（浏览器的视区）重定向到端点进行本地呈现，从而卸载服务器的负载。 |
| 在 Citrix Workspace 应用程序中打开文件 | 允许使用托管应用程序（客户端到服务器内容重定向）在 Citrix Workspace 应用程序中打开本地文件。 |
| 基于位置的服务（位置可通过 API 描述获得） | 允许由 Citrix Virtual Desktops（以前称为 XenDesktop）交付的应用程序使用位置信息。 |

### HDX 多媒体

| 功能 | Windows 2403.1 和 Windows 应用商店 2403.1 | Windows 2402 LTSR | Linux 2405 | Mac 2402.10 | iOS 24.5.0 | Android 24.5.0 | HTML5 2404.1 | ChromeOS 2405 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 音频播放 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| 双向音频 (VoIP) | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| 网络摄像机重定向 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| 视频播放 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| Microsoft Teams 优化 | 是 | 是 | 是（仅限 x64） | 是 | 否 | 否 | 是 | 是 |

| 功能 | Windows 2403.1 和 Windows 应用商店 2403.1 | Windows 2402 LTSR | Linux 2405 | Mac 2402.10 | iOS 24.5.0 | Android 24.5.0 | HTML5 2404.1 | ChromeOS 2405 |
|---|---|---|---|---|---|---|---|---|
| Skype for Business Optimization Pack | 是 | 是 | 是 | 是 | 否 | 否 | 否 | 否 |
| Cisco Jabber 统一通信优化 | 是 | 是 | 是 | 否 | 否 | 否 | 否 | 否 |
| Windows 多媒体重定向 | 是 | 是 | 是 | 否 | 否 | 否 | 否 | 否 |
| UDP 音频 | 是 | 是 | 是 | 否 | 否 | 否 | 否 | 否 |

| 功能 | 定义 |
|---|---|
| 音频播放 | 启用服务器呈现的音频播放。 |
| 双向音频 (VoIP) | 允许使用托管软件电话/语音聊天协作应用程序。 |
| 网络摄像机重定向 | 允许使用使用本地网络摄像机的视频聊天协作应用程序。 |
| 视频播放 | 允许观看录制的视频。 |
| Microsoft Teams 优化 | 将 Microsoft Teams 媒体处理从 Citrix 服务器卸载到用户设备。 |
| Skype for Business 优化 | 将 Skype for Business 媒体处理从 Citrix 服务器卸载到用户设备。对于适用于 Android 的 Citrix Workspace 应用程序，我们仅支持在 Chrome 设备上使用。 |
| Cisco Jabber 统一通信优化 | 将 Jabber 媒体处理从 Citrix 服务器卸载到用户设备。 |
| Windows 多媒体重定向 | 允许在用户设备上呈现 Windows 多媒体，从而卸载服务器的负载。 |
| UDP 音频 | 支持通过 UDP 进行音频输入和输出。 |

| 功能 | 定义 |
| --- | --- |

安全性

| 功能 | Windows 2403.1 和 Windows 应用商店 2403.1 | Windows 2402 LTSR | Linux 2405 | Mac 2402.10 | iOS 24.5.0 | Android 24.5.0 | HTML5 2404.1 | ChromeOS 2405 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| TLS 1.2 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| TLS 1.0/1.1 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| DTLS 1.0 | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| DTLS 1.2 | 是 | 是 | 是 | 是 | 否 | 否 | 否 | 否 |
| SHA2 证书 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| 智能访问 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| 通过 Citrix Gateway 进行远程访问 | 是 *(1)* | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| Workspace for Web 访问 | 是 | 是 | 是 | 是 | 通过 ICA 文件 | 是 | 是 | 是 |
| IPV6 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| App Protection | 是 | 是 | 是 | 是 | 否 | 否 | 否 | 否 |

| 功能 | 定义 |
| --- | --- |
| TLS 1.2 | SSL 的后继产品，强大的通信通道安全性。 |
| TLS 1.0/1.1 | SSL 的后继产品，强大的通信通道安全性。 |

| 功能 | 定义 |
| --- | --- |
| DTLS 1.0 | DTLS 是 SSL 协议的衍生协议。它提供相同的安全服务（完整性、身份验证和机密性），但采用 UDP 协议。 |
| DTLS 1.2 | DTLS 是 SSL 协议的衍生协议。它提供相同的安全服务（完整性、身份验证和机密性），但采用 UDP 协议。 |
| SHA2 证书 | 能够使用 SHA2 证书。 |
| 智能访问 | 使用网关策略和过滤器控制对可用应用程序的访问。 |
| 通过网关进行远程访问 | 为用户提供在没有 VPN 客户端的情况下随时随地安全访问企业应用程序、虚拟桌面和数据的权限。 |
| Workspace for Web 访问 | 使用浏览器访问托管应用程序或虚拟桌面。 |
| IPV6 | 允许在 IPV6 网络中使用。 |

### HDX 显卡

| 功能 | Windows 2403.1 和 Windows 应用商店 2403.1 | Windows 2402 LTSR | Linux 2405 | Mac 2402.10 | iOS 24.5.0 | Android 24.5.0 | HTML5 2404.1 | ChromeOS 2405 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| H.264 增强型超级编解码器 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| 客户端硬件加速 | 是 | 是 | 是 | 是 | 否 | 是 | 否 | 否 |
| 3DPro 显卡 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| 支持外部显示器 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| 桌面组合重定向 | 是 | 是 | 否 | 否 | 否 | 否 | 否 | 否 |
| 真正的多显示器 | 是 | 是 | 是 | 是 | 否 | 否 | 是 | 是 |

| 功能 | 定义 |
| --- | --- |
| H.264 增强型超级编解码器 | 使用 XenApp/Desktop 7.X H264 增强型超级编解码器简化应用程序的交付。 |
| 客户端硬件加速 | 为显卡、网络摄像机等 HDX 功能启用硬件加速。硬件功能的使用因不同的 Citrix Workspace 应用程序而异。 |
| 3DPro 显卡 | 支持使用数据中心中托管的 3D 专业图形应用程序。 |
| 支持外部显示器 | 允许使用外部显示器。 |
| 桌面组合重定向 | 启用远程连接到客户端的图形命令进行呈现，以确保服务器可扩展性。在适用于 Mac 的 Receiver 12.9 版本中已弃用。 |
| 真正的多显示器 | XenApp 或 XenDesktop 创建的显示器数量与客户端支持的显示器数量相同。 |

身份验证

| 功能 | Windows 2403.1 和 Windows 应用商店 2403.1 | Windows 2402 LTSR | Linux 2405 | Mac 2402.10 | iOS 24.5.0 | Android 24.5.0 | HTML5 2404.1 | ChromeOS 2405 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 联合身份验证 (SAML/Azure AD) | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| ADC 完整 VPN | 是 | 是 | 是 | 是 | 否 | 否 | 否 | 否 |
| RSA 软令牌 | 否 | 否 | 否 | 否 | 是 | 是 | 否 | 否 |
| 质询响应 SMS (Radius) | 是 | 是 | 否 | 是 | 否 | 否 | 否 | 否 |

| 功能 | Windows 2403.1 和 Windows 应用商店 2403.1 | Windows 2402 LTSR | Linux 2405 | Mac 2402.10 | iOS 24.5.0 | Android 24.5.0 | HTML5 2404.1 | ChromeOS 2405 |
|---|---|---|---|---|---|---|---|---|
| 通过网关进行用户证书身份验证（通过本机 Workspace 应用程序） | 否 | 否 | 否 | 否 | 是 | 是 | 是 | 是 |
| 通过网关进行用户证书身份验证（通过浏览器） | 是 *(4)* | 是 *(4)* | 否 | 是 | 否 | 否 | 是 | 是 |
| 智能卡（CAC、PIV 等） | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 是 |
| 临近感应式/非接触式卡 | 是 | 是 | 是 | 否 | 否 | 否 | 否 | 是 |
| 凭据插入（例如，Fast Connect、Storebrowse） | 是 | 是 | 是 | 否 | 否 | 否 | 否 | 是 |
| 直通身份验证 | 是 | 是 | 否 | 否 | 否 | 否 | 否 | 否 |
| 保存凭证 * 本地且仅限 StoreFront | 是 | 是 | 否 | 是 | 否 | 否 | 否 | 否 |

| 功能 | Windows 2403.1 和 Windows 应用商店 2403.1 | Windows 2402 LTSR | Linux 2405 | Mac 2402.10 | iOS 24.5.0 | Android 24.5.0 | HTML5 2404.1 | ChromeOS 2405 |
|---|---|---|---|---|---|---|---|---|
| ADC nFactor 身份验证 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| ADC 本机 OTP | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |
| 生物特征身份验证 (Touch ID、面容 ID) | 否 | 否 | 否 | 否 | 是 | 否 | 否 | 否 |
| 单点登录到 Citrix 移动应用程序 | 否 | 否 | 否 | 否 | 是 | 是 | 否 | 否 |
| 匿名应用商店访问 | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| 功能 | 定义 |
|---|---|
| 联合身份验证 (SAML/Azure AD) | 使 FAS 服务器能够进行通过 Azure AD 或 SAML 委派微软 ADFS 服务器（或其他 SAML 感知 IdP）的用户身份验证。 |
| ADC (NetScaler) 完整 VPN | 为网关构建完整 VPN 通道。 |
| RSA 软令牌 | 在使用 RSA 软令牌时启用简化的身份验证。 |
| 质询响应 SMS (Radius) | 允许使用质询响应身份验证，例如使用 SMS 通行码。 |
| 通过网关进行用户证书身份验证（仅通过浏览器） | 允许使用用户证书作为使用网关进行身份验证的一个因素，即在 Windows 上进行基于浏览器的身份验证。 |
| 智能卡（CAC、PIV 等） | 允许使用标准 PC/SC 兼容的加密智能卡进行身份验证和签名。 |
| 临近感应式/非接触式卡 | 使用临近感应式智能卡或非接触式智能卡进行身份验证，用户将能够使用 Citrix 应用程序或桌面。 |

| 功能 | 定义 |
| --- | --- |
| 凭据插入（例如，Fast Connect、Storebrowse） | 使用临近感应式智能卡或非接触式智能卡进行身份验证，用户将能够使用 Citrix 应用程序或桌面。Storebrowse 是一款命令行实用程序工具，可与适用于 Windows 的 Citrix Workspace 应用程序结合使用。可以使用 Storebrowse 实用程序编写脚本来自定义 Citrix Workspace 应用程序。 |
| 直通身份验证 | 将用户凭据传递到 Web Interface 站点，然后传递给 Citrix Virtual Apps and Desktops 服务器。此过程可防止用户在 Citrix 应用程序启动过程中随时进行显式身份验证。 |
| 保存凭证 * 本地且仅限 StoreFront | 启用本地保存凭据，且仅使用 Citrix StoreFront。 |
| 网关本机 OTP | 通过将整个配置保留在 NetScaler 设备上，网关无需使用第三方服务器即可支持一次性密码 (OTP)。 |
| NetScaler nFactor 身份验证 | nFactor 身份验证可根据用户配置文件启用动态身份验证流程。有时，这些流程可以是简单的流程，以对用户直观显示。所需的 NetScaler 的最低版本为 12.1.49.x。 |
| 生物特征身份验证（Touch ID、面容 ID） | 启用生物识别身份验证，例如 Touch ID 和面容 ID。 |
| 单点登录到 Citrix 移动应用程序 | 启用对 Citrix Mobile 应用程序的单点登录。 |
| 匿名应用商店访问 | 支持未经身份验证的（匿名）用户进行访问。 |

输入体验

| 功能 | Windows 2403.1 和 Windows 应用商店 2403.1 | Windows 2402 LTSR | Linux 2405 | Mac 2402.10 | iOS 24.5.0 | Android 24.5.0 | HTML5 2404.1 | ChromeOS 2405 |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 键盘布局同步 - 客户端到 VDA (Windows VDA) | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |

| 功能 | Windows 2403.1 和 Windows 应用商店 2403.1 | Windows 2402 LTSR | Linux 2405 | Mac 2402.10 | iOS 24.5.0 | Android 24.5.0 | HTML5 2404.1 | ChromeOS 2405 |
|---|---|---|---|---|---|---|---|---|
| 键盘布局同步 - 客户端到 VDA (Linux VDA) | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| 键盘布局同步 - VDA 到客户端 (Windows VDA) | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 否 |
| 键盘布局同步 - VDA 到客户端 (Linux VDA) | 否 | 否 | 否 | 否 | 否 | 否 | 否 | 否 |
| Unicode 键盘布局映射 | 否 | 否 | 是 | 是 | 是 | 是 | 是 | 是 |
| 键盘输入模式 - unicode | 否 | 否 | 是 | 是 | 是 | 是 | 是 | 是 |
| 键盘输入模式 - scancode | 是 | 是 | 是 | 是 | 否 | 否 | 是 | 是 |
| 服务器 IME | 是 | 是 | 是 | 是 | 是 | 是 | 是 | 是 |

| 功能 | Windows 2403.1 和 Windows 应用商店 2403.1 | Windows 2402 LTSR | Linux 2405 | Mac 2402.10 | iOS 24.5.0 | Android 24.5.0 | HTML5 2404.1 | ChromeOS 2405 |
|---|---|---|---|---|---|---|---|---|
| CJK IME 的通用客户端 IME (CTXIME) | 是 | 是 | 否 | 是 | 是 | 是 | 是 | 是 |
| 命令行接口 | 是 | 是 | 否 | 否 | 否 | 否 | 否 | 否 |
| 键盘同步设置 UI 和配置 | 是 | 是 | 是 | 是 | 是 | 是 | 否 | 否 |
| 输入模式设置 UI 和配置 | 否 | 否 | 是 | 是 | 是 | 否 | 否 | 否 |
| 语言栏设置 UI 和配置 | 是 | 是 | 否 | 是 | 否 | 否 | 否 | 否 |

| 功能 | 定义 |
|---|---|
| 键盘布局同步 - 客户端到 VDA (Windows VDA) | 允许用户在客户端设备上同步活动键盘布局或者在首选键盘布局之间切换。客户端设备上的键盘布局会在 Windows VDA 上自动设置。 |
| 键盘布局同步 - 客户端到 VDA (Linux VDA) | 允许用户在客户端设备上同步活动键盘布局或者在首选键盘布局之间切换。客户端设备上的键盘布局会在 Linux VDA 上自动设置。 |
| 键盘布局同步 - VDA 到客户端 (Windows VDA) | 使用户能够同步活动键盘布局或者在 Windows VDA 上的首选键盘布局之间切换。Windows VDA 上的键盘布局会在客户端设备上自动设置。 |
| 键盘布局同步 - VDA 到客户端 (Linux VDA) | 使用户能够同步活动键盘布局或者在 Linux VDA 上的首选键盘布局之间切换。Linux VDA 上的键盘布局会在客户端设备上自动设置。 |
| Unicode 键盘布局映射 | 支持 Windows VDA 与非 Windows Citrix Workspace 应用程序之间的 Unicode 键盘布局映射。 |

| 功能 | 定义 |
| --- | --- |
| 键盘输入模式 - unicode | Unicode 输入模式将密钥从客户端键盘发送到 VDA，VDA 在 VDA 中生成相同的字符。应用客户端键盘布局。 |
| 键盘输入模式 - scancode | Scancode 输入模式将按键位置从客户端键盘发送到 VDA，VDA 将生成相应的字符。应用服务器端键盘布局。 |
| 服务器 IME | 提供服务（或 VDA）端输入法编辑器 (IME) 的可用性和体验。 |
| CJK IME 的通用客户端 IME (CTXIME) | 为东亚语言（中文、日语、韩语）提供增强的客户端 IME 可用性并改善无缝体验。 |
| 命令行接口 | 用户可以使用命令行界面启用或禁用客户端 IME。 |
| 键盘同步设置 UI 和配置 | 用户可以使用 GUI 选择不同的键盘布局同步选项。 |
| 输入模式设置 UI 和配置 | 用户可以使用 GUI 选择不同的键盘输入模式选项。 |
| 语言栏设置 UI 和配置 | 用户可以选择使用 GUI 在 VDA 应用程序会话中显示或隐藏远程语言栏。语言栏显示会话中的首选输入语言。 |
| 键盘布局同步 GPO 管理模板 | 管理员可以通过从 Citrix Workspace 应用程序组策略对象管理模板部署相应的策略来覆盖键盘布局同步配置。 |

表格指标

| 指标 | 说明 |
| --- | --- |
| 1 | 仅限 StoreFront |
| 2 | 对于这些 Citrix Workspace 应用程序，HDX 3D Pro 将还原为 JPEG。建议使用 3 Mbps，而使用 H.264 深度压缩时建议使用 1.5 Mbps。 |
| 3 | 对于 NSAP VC，适用于 iOS/Android 的 Workspace 应用程序支持此功能，但对于 ADC/ADM，是否支持仍然待定。 |
| 4 | “通过网关进行用户证书身份验证（仅通过浏览器）”身份验证方法不支持 Citrix Workspace 应用程序客户端检测。只有在下载 ICA 文件才能使用 Citrix Workspace 应用程序打开虚拟应用程序或桌面。 |

> 注意：
>
> 针对我们的产品描述的任何特性或功能的开发、发布和执行时间由我们自行决定。本文中提供的信息仅供参考，并不是提供任何资料、代码或功能的保证、承诺或法律义务，并且不应依赖于制定购买决策或纳入任何合同。针对我

> 们的产品描述的任何特性或功能的开发、发布和执行时间仍由我们自行决定，如有变更，恕不另行通知或协商。