安全访问扩展

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

Contents

适用于 Chrome Enterprise Premium 的 Citrix Secure Access 扩展程序 4

- Secure Access 扩展程序日志 4
- 适用于 Chrome Enterprise 的 Citrix Secure Access 控件 5
  - 支持的控件 8
- 策略中的用户和组 8
  - 搜索用户或组 9
  - 使用同步的用户和组 9

防键盘记录控制 10

- 先决条件 10
- 配置防键盘记录策略 10

剪贴板容器控制 12

- 先决条件 12
- 启用剪贴板容器控制 12
- 启用剪贴板共享范围 13

Web 应用程序的域后缀 16

- 先决条件 16
- 配置 DNS 后缀 16

会话录制控制 18

- 体系结构 18
- 先决条件 19
- 系统要求 19
- 设置环境 19
  - 配置会话录制站点 19
  - 在 Secure Private Access 中配置会话录制浏览器策略 19
  - 为端点安装带会话录制代理的 Workspace 应用程序 20
  - 重放录制的会话 20

© 1997–2026 Citrix Systems, Inc. All rights reserved.

最佳实践 20
浏览器会话重新身份验证控制 21
先决条件 21
启用浏览器会话重新身份验证控制 21
SSH 控制 23
此集成的优势 23
用例 23
系统要求 24
先决条件 24
配置安全私有访问以进行 SSH 访问 24
配置 SSH 策略 25
远程桌面控制 26
此集成的优势 26
用例 27
系统要求 27
先决条件 27
配置 Secure Private Access 以进行 RDP 访问 27
配置远程桌面策略 28

© 1997–2026 Citrix Systems, Inc. All rights reserved.

适用于 Chrome Enterprise Premium 的 Citrix Secure Access 扩展程序

适用于 Chrome Enterprise Premium (CEP) 的 Citrix Secure Access 扩展程序可直接从 Chrome 浏览器实现对内部和外部应用程序的安全、无客户端访问。它结合了 Citrix Secure Private Access 和 Chrome Enterprise 功能，以提供企业级安全性、零信任访问、上下文控制和现代用户体验。

组织可以使用此扩展程序提供对 SaaS 应用程序、内部 Web 应用程序、SSH 服务器和 RDP 系统的安全访问，所有这些都无需 VPN 或本机客户端安装。

当您将 Secure Private Access 与 Chrome Enterprise Premium 集成时，Secure Access 浏览器扩展程序会自动安装。有关设置说明，请参阅 设置 Google Chrome 集成。安装后，您可以从 Chrome 浏览器右上角的图标访问该扩展程序。



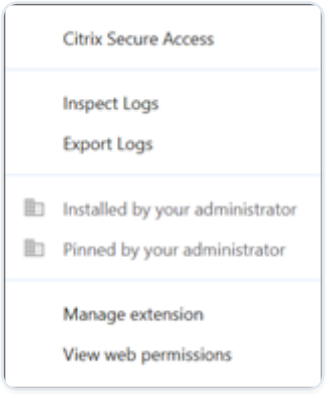
Secure Access 扩展程序日志

Secure Access 浏览器扩展程序日志对于监视和故障排除至关重要。最终用户可以查看和下载日志，以便在出现问题时与管理员或支持团队共享。

要查看或下载日志：

1. 右键单击浏览器扩展程序图标。
    - 单击 **检查日志** 以查看日志。
    - 单击 **导出日志** 以下载日志。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



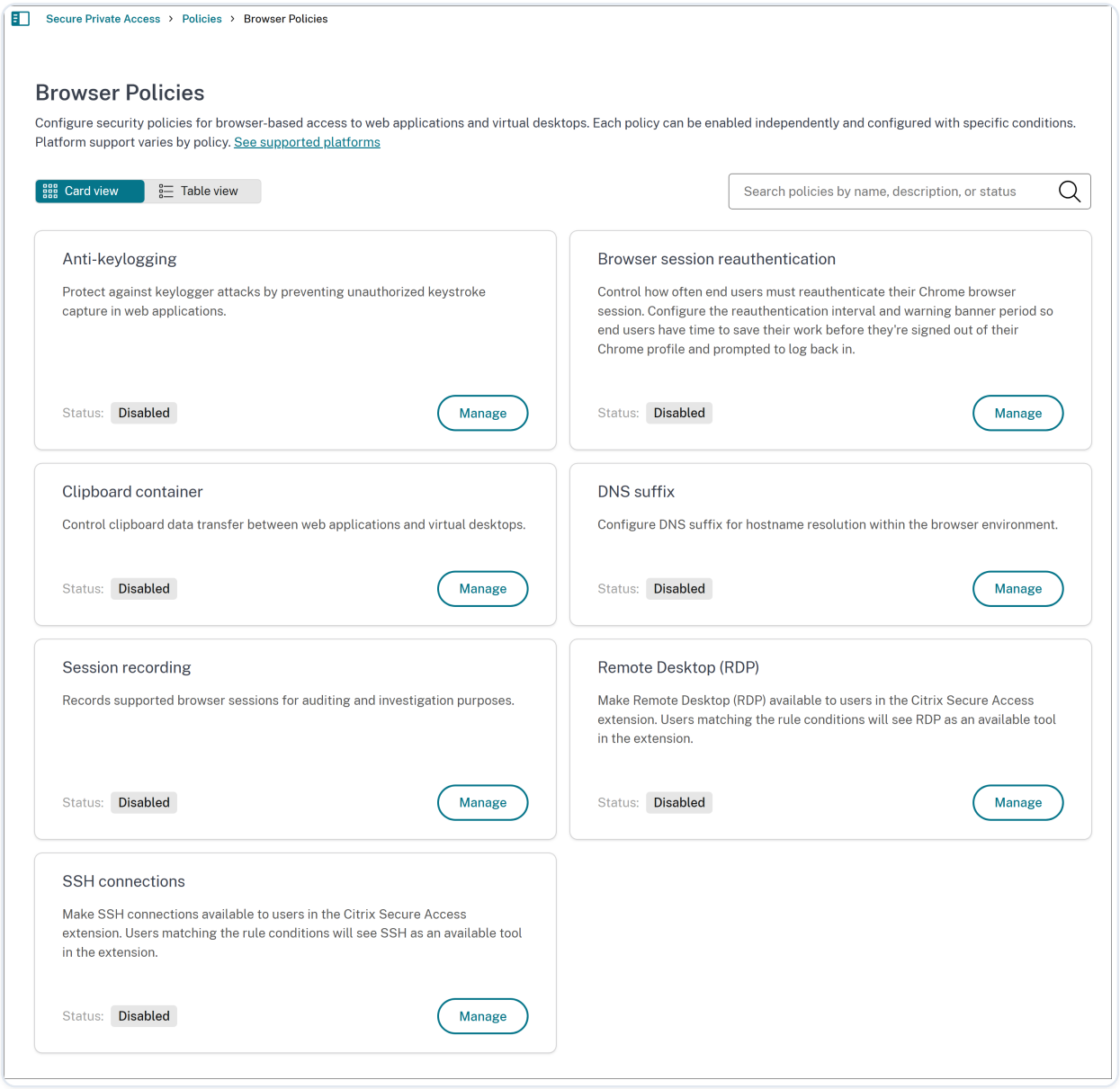
适用于 Chrome Enterprise 的 Citrix Secure Access 控件

Citrix Secure Private Access 支持由适用于 Google Chrome Enterprise Premium (CEP) 的 Citrix Secure Access 扩展程序交付和强制执行的安全策略。有关详细信息，请参阅 支持的控件。

您可以从 Secure Private Access 管理控制台配置这些策略。

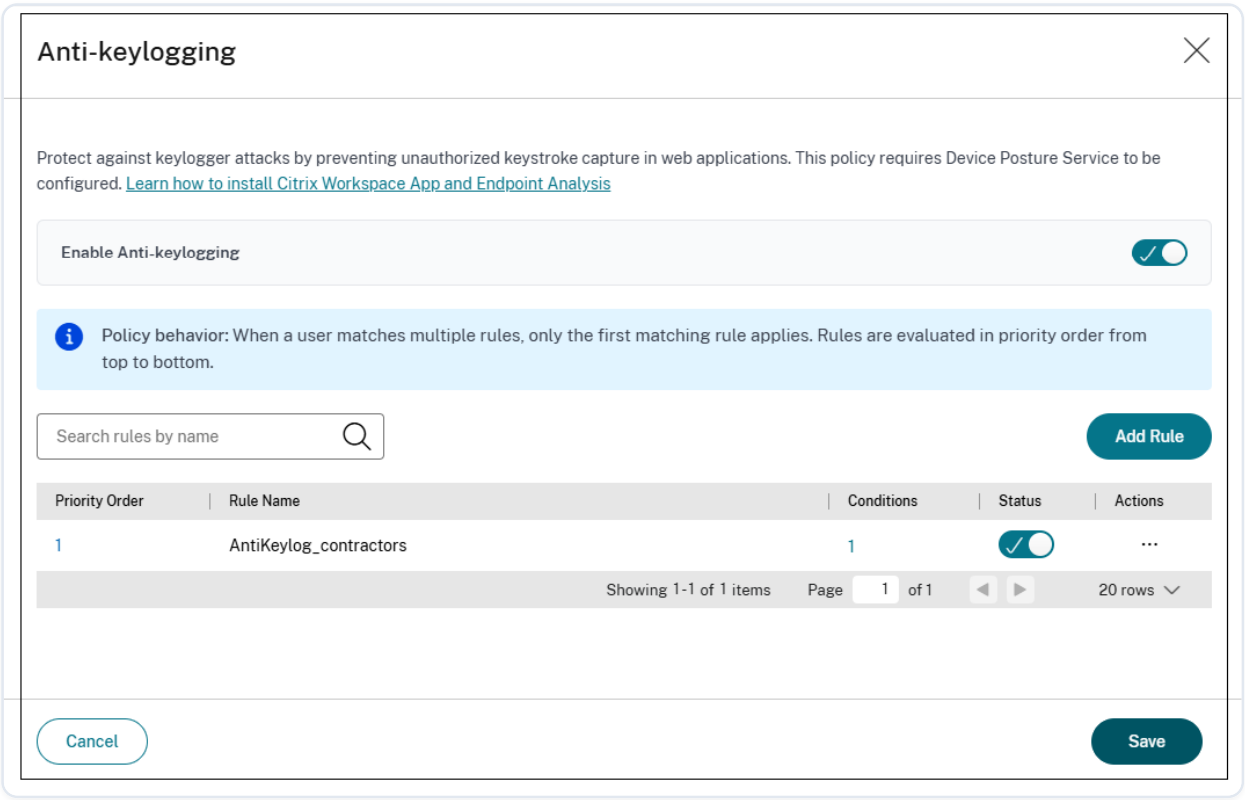
1. 转到 **策略 > 浏览器策略**，然后单击 **创建浏览器策略**。
2. 选择策略，然后单击 **管理**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

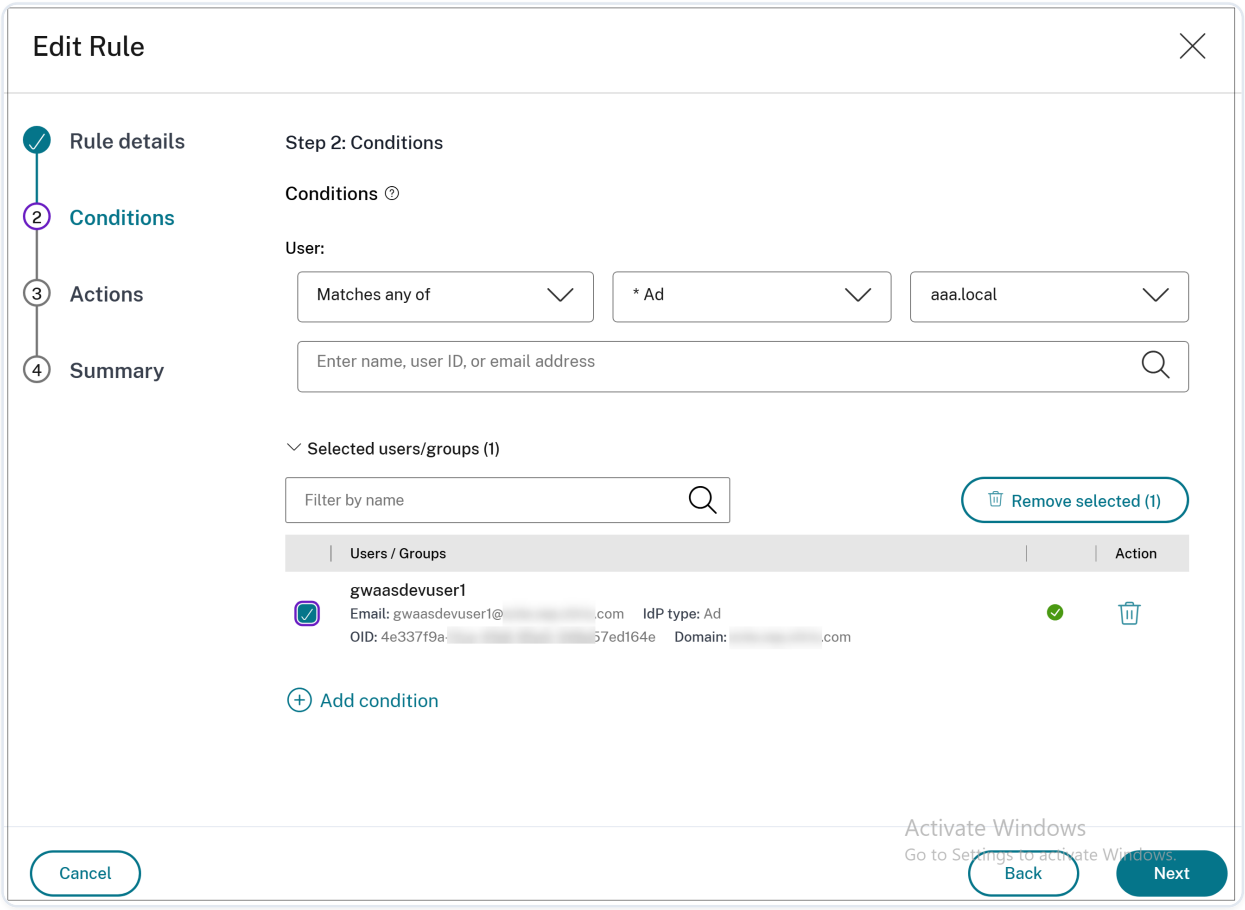


3. 为策略添加规则。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. 添加 **访问模式** 条件，以将浏览器控件限定到浏览器会话。对于浏览器策略，值为 **浏览器**。有关访问模式的更多信息，请参阅基于访问模式的策略实施。
5. 选择必须评估策略的条件。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

注意：

- 选择用户或组时，管理员可以验证所选用户目录中的条目是否已与 Google Directory 同步并正确配置。Secure Private Access 策略仅在使用同步的用户和组时才能正确评估。否则，可能会出现警告。有关详细信息，请参阅 使用同步的用户和组。
- 另请参阅 和 ，了解有关用户和组的更多信息。

有关详细配置步骤，请参阅每个控件的文档。

支持的控件

Citrix 支持以下 Secure Access 控件，并与 Secure Private Access 和 Chrome Enterprise Premium 集成：

控件	其功能
防键盘记录	混淆击键，以防止端点上的键盘记录恶意软件捕获用户输入。
剪贴板容器	控制用户在浏览器和其他应用程序之间复制和粘贴的内容。
DNS 后缀	自动将简短的内部 URL（如“wiki/”）补全为完整地址。
会话录制	记录浏览器会话活动，用于审计和合规性。
浏览器会话重新身份验证	在配置的时间间隔后，强制对浏览器会话进行定期重新身份验证。
SSH 连接	使用户能够直接在浏览器选项卡中建立 SSH 连接，而无需终端客户端。
远程桌面 (RDP)	使用户能够直接在浏览器选项卡中启动远程桌面会话，而无需 RDP 客户端。

策略中的用户和组

以下各节提供了有关用户和组的更多信息：

© 1997–2026 Citrix Systems, Inc. All rights reserved.

搜索用户或组

您选择的用户和组将显示在网格中。网格中的每一行都显示以下身份详细信息，以便您可以清楚地区分不同域、林或身份提供商 (IdP) 中同名用户或组：

- **名称** – 用户或组的显示名称。
- **电子邮件** – 与身份关联的电子邮件地址。
- **IDP 类型** – 身份提供商，例如 Azure AD、Active Directory、Okta 或 Google。
- **OID** – 身份的对象 ID 或安全标识符。
- **域** – 用户或组所属的域。

您可以按名称筛选网格、删除单个行，或者选择多个条目并使用**删除所选内容**将其一起删除。

使用同步的用户和组

选择用户或组时，管理员可以验证所选用户目录中的条目是否已与 Google Directory 同步并正确配置。Secure Private Access 策略仅在使用同步的用户和组时才能正确评估。否则，可能会出现以下警告：

- **缺少租户帐户权限。**

  补救措施： 在 Google 管理控制台中，将 **Users > Read** 和 **Groups > Read** 权限分配给租户服务帐户。SPA 需要这些权限来验证用户或组是否存在。

- **用户或组未同步。**

  补救措施： 搜索或选定的用户或组未与 Google Directory 同步。在使用目录实体作为 SPA 策略之前，请将其与 Google Directory 同步。

- **组访问设置不足。**

  补救措施： 在 Google 管理控制台中，打开所选组的访问设置，并确保“**谁可以查看成员**”至少选择了“**组成员**”选项。

注意：

此功能仅在 Google Chrome 集成成功完成后可用。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

防键盘记录控制

网络犯罪分子使用键盘记录器等恶意软件窃取敏感信息，例如密码、信用卡号和机密公司数据。

适用于 Chrome Enterprise Premium (CEP) 的 Citrix Secure Access 浏览器扩展支持防键盘记录功能，以帮助保护您的数据。此功能会扰乱击键，因此如果恶意程序尝试捕获键入的输入，它只会记录不可读的字符，而实际文本会安全地传送到您的工作应用程序。

支持的部署： Citrix Secure Private Access 服务和混合部署。

支持的平台： Windows 11 及更高版本。

注意：

本机 RDP 会话不支持防键盘记录。

先决条件

在启用防键盘记录之前，请确保满足以下先决条件：

- 已安装 CWA 2603 及更高版本。
- Citrix Secure Access 与 Chrome Enterprise Premium (CEP) 之间的集成已完成。

配置防键盘记录策略

1. 登录到 Secure Private Access 管理控制台。
2. 转到“**策略 > 浏览器策略**”，然后单击“**创建浏览器策略**”。
3. 选择“**防键盘记录**”，然后单击“**管理**”。
4. 点击 **添加规则** 为用户添加规则以启用防键盘记录。
    a. 输入规则名称，然后点击 **下一步**。
    b. 根据您的要求选择条件，例如用户或组。您还可以添加诸如 **地理位置**、**网络位置** 和 **设备状态检查** 等条件。
    c. 点击 **下一步**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. 点击 **保存**。

   为防键盘记录策略配置的规则数量显示在 **浏览器策略 > 防键盘记录** 选项卡中。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

剪贴板容器控制

使用 Chrome 进行 Web 访问和使用 VDI 进行本机应用程序的部署可以使用剪贴板容器功能来控制浏览器和 VDI 会话之间的数据共享。剪贴板数据在 Citrix 会话之间直接传输，而不会写入本地端点剪贴板。 这在提高安全性的同时，仍为用户提供了在两种环境中工作的灵活性。

支持的部署： Secure Private Access 服务和混合部署。

支持的平台： Windows。

先决条件

确保满足以下先决条件：

- Citrix Secure Access 与 Chrome Enterprise Premium (CEP) 之间的集成已完成。
- Citrix Workspace 应用程序 2603.10 或更高版本。
- 运行 2607 LTSR 或更高版本的 Windows VDA（剪贴板共享范围的 GA 版本）。有关详细信息，请参阅 剪贴板共享范围。
- 运行 2507 LTSR 的 Windows VDA（剪贴板共享范围的预览版本），启用以下功能：
  - **与 DaaS 交叉剪贴板容器**功能。有关详细信息，请参阅 与 DaaS 交叉剪贴板容器。此功能目前在 DaaS 中作为预览版提供。
  - **剪贴板共享范围**注册表。有关详细信息，请参阅 启用剪贴板共享范围注册表。

启用剪贴板容器控制

1. 登录到 Secure Private Access 管理控制台。
2. 转到“**策略 > 浏览器策略**”，然后单击“**创建浏览器策略**”。
3. 选择 **剪贴板容器**，然后点击 **管理**。
4. 点击 **添加规则**，为 VDA 和浏览器之间的剪贴板共享添加规则。
   a. 输入规则名称，然后点击 **下一步**。
   b. 根据您的要求（例如用户或组）选择条件。您还可以添加诸如 **地理位置**、**网络位置** 和 **设备态势检查** 等条件。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c. 点击 **下一步**。

d. 定义允许剪贴板共享的 URL 和 Secure Private Access 应用程序。

e. 选择策略范围。

- **应用于整个浏览器** — 该策略管理托管配置文件中的所有剪贴板活动。
- **应用于特定应用程序和 URL** — 该策略仅限于选定的应用程序和输入的 URL/域模式。
  - **选择应用程序** — 使用应用程序选择器选择特定的已发布应用程序。
  - **URL 或域** - 输入特定应用程序的 URL 或域。

剪贴板容器操作(/en-us/citrix-secure-private-access/media/spa-cep-clipboard-container-action.png)

5. 点击 **保存**。

为剪贴板容器策略配置的规则数量显示在 **浏览器策略 > 剪贴板容器** 选项卡中。

启用剪贴板共享范围

适用于 VDA 版本 2607：

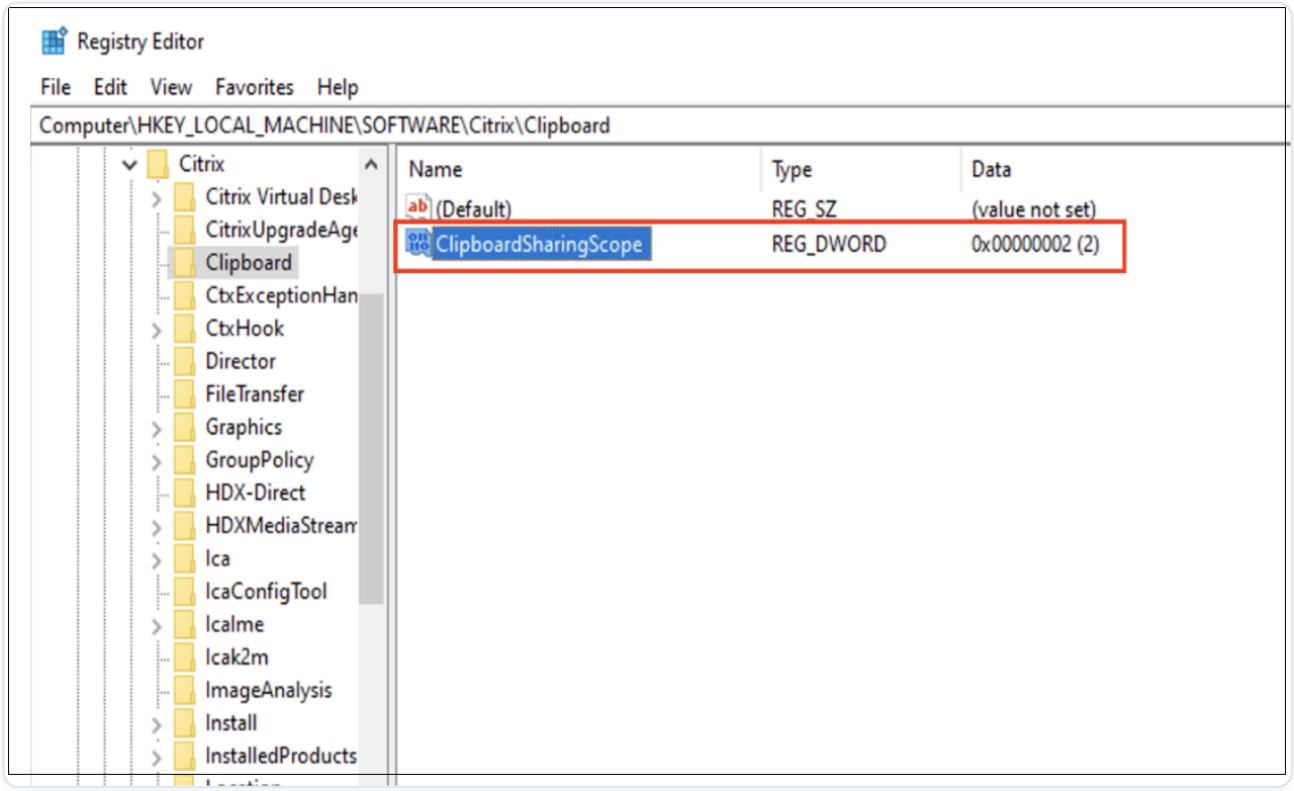
请参阅 工作原理。

适用于 VDA 版本 2507：

启用此 **剪贴板共享范围** 注册表项。

1. 使用 regedit.exe 打开 Windows 注册表编辑器。
2. 导航到 HKEY_LOCAL_MACHINE\Software\Citrix\Clipboard\。
3. 创建一个名为 `ClipboardSharingScope` 的 REG_DWORD 值。

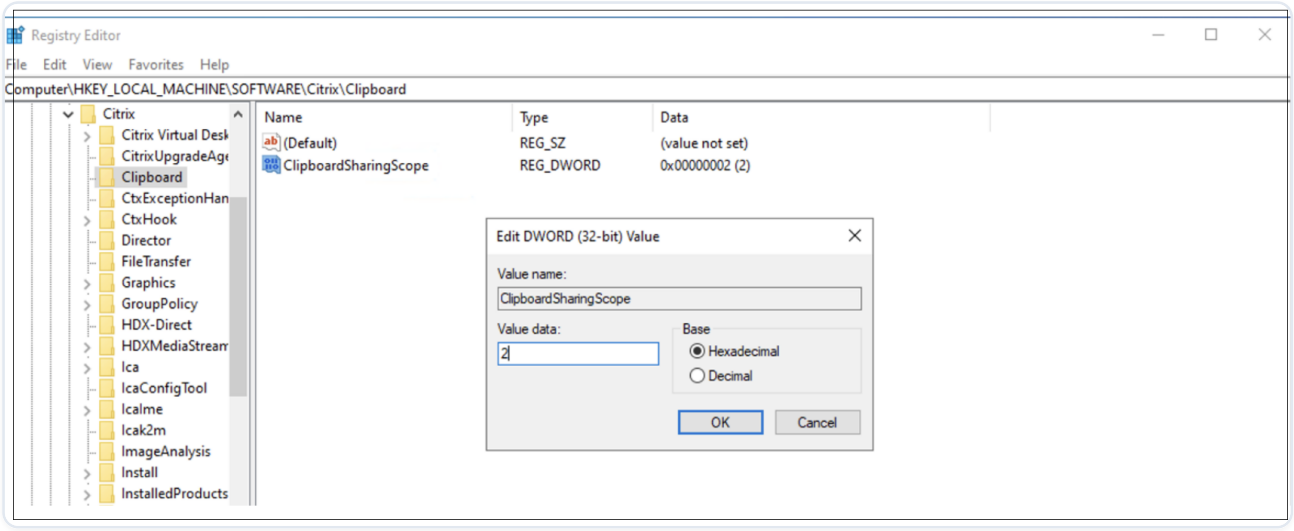
© 1997–2026 Citrix Systems, Inc. All rights reserved.



`ClipboardSharingScope` 策略控制 VDA 剪贴板数据可以在何处共享。在新 DDC 策略可用之前，可以使用上述注册表项配置此设置。

支持的值	范围	描述
0	无限制	剪贴板数据将复制到客户端系统剪贴板，并且可由客户端、VDA 和 CEP 访问。
1	仅限 VDA	剪贴板数据仅 VDA 可访问。客户端系统剪贴板和 CEP 无法访问剪贴板内容。
2	仅限 CEP	剪贴板数据仅 CEP 可访问。客户端系统剪贴板和 VDA 无法访问剪贴板内容。
3	VDA 和 CEP	VDA 和 CEP 均可访问剪贴板数据。客户端系统剪贴板无法访问剪贴板内容。

© 1997–2026 Citrix Systems, Inc. All rights reserved.



注意：

- 仅限 CEP (2) 和 VDA 和 CEP (3) 模式旨在与 CEP 扩展中的剪贴板容器功能配合使用。
- 启用剪贴板容器策略后，只有管理员配置的 URL 才能与 VDI 交换剪贴板数据。

```
>-  Content copied from the approved web applications can be pasted into
the VDI.

>-  Content copied from the VDI can be pasted only into administrator-
configured, paste-allowed URLs.

>-  If a user attempts to paste VDI clipboard content into a website that
is not included in the policy, the paste operation is blocked and an error
message appears.
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Web 应用程序的域后缀

在用户在浏览器中输入简短的内部主机名（例如，`sw` 或 `server001`）的场景中，域后缀功能会自动附加 DNS 后缀，并使用浏览器管理的 DNS 后缀策略将其转换为完全限定域名 (FQDN)，而不是依赖操作系统的 DNS 后缀配置。

DNS 后缀功能在 **Windows** 和 **macOS** 平台上均受支持，并始终适用于常见的 URL 输入格式，包括：

- `sw`
- `http://sw`
- `https://sw/`
- `sw/`
- `http://sw/`
- `https://sw/`

支持的部署： Secure Private Access 服务和混合部署。

支持的平台： Windows 和 macOS。

先决条件

确保已配置 Citrix Secure Access 与 Chrome Enterprise 的集成。有关详细信息，请参阅与 Google Chrome Enterprise Premium 集成。

配置 DNS 后缀

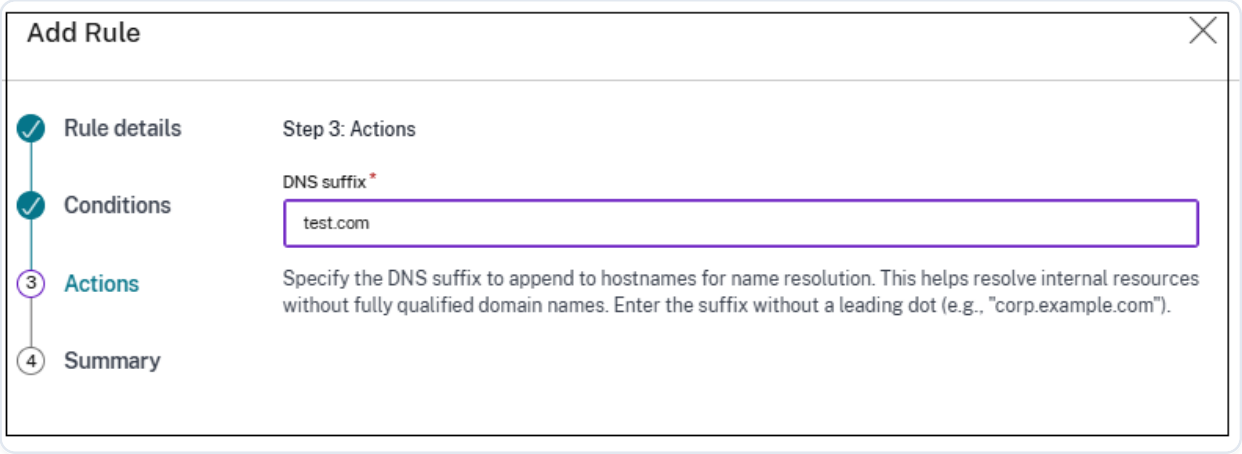
1. 登录到 Secure Private Access 管理控制台。
2. a. 转到 **策略 > 浏览器策略**，然后单击 **创建浏览器策略**。
3. 选择 **DNS 后缀**，然后单击 **管理**。
4. 单击 **添加规则**，为要添加到 URL 的域添加规则。
    a. 输入规则名称，然后单击 **下一步**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b. 根据您的要求（例如用户或组）选择条件。您还可以添加条件，例如 **地理位置**、**网络位置** 和 **设备状态检查**。

c. 单击 **下一步**。

d. 定义要附加以进行访问的域。



5. 单击 **保存**。

为 DNS 后缀策略配置的规则数显示在 **浏览器策略 > DNS 后缀** 选项卡中。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

会话录制控制

会话录制会记录、编目和存档会话，以便检索和回放。

会话录制提供以下主要优势：

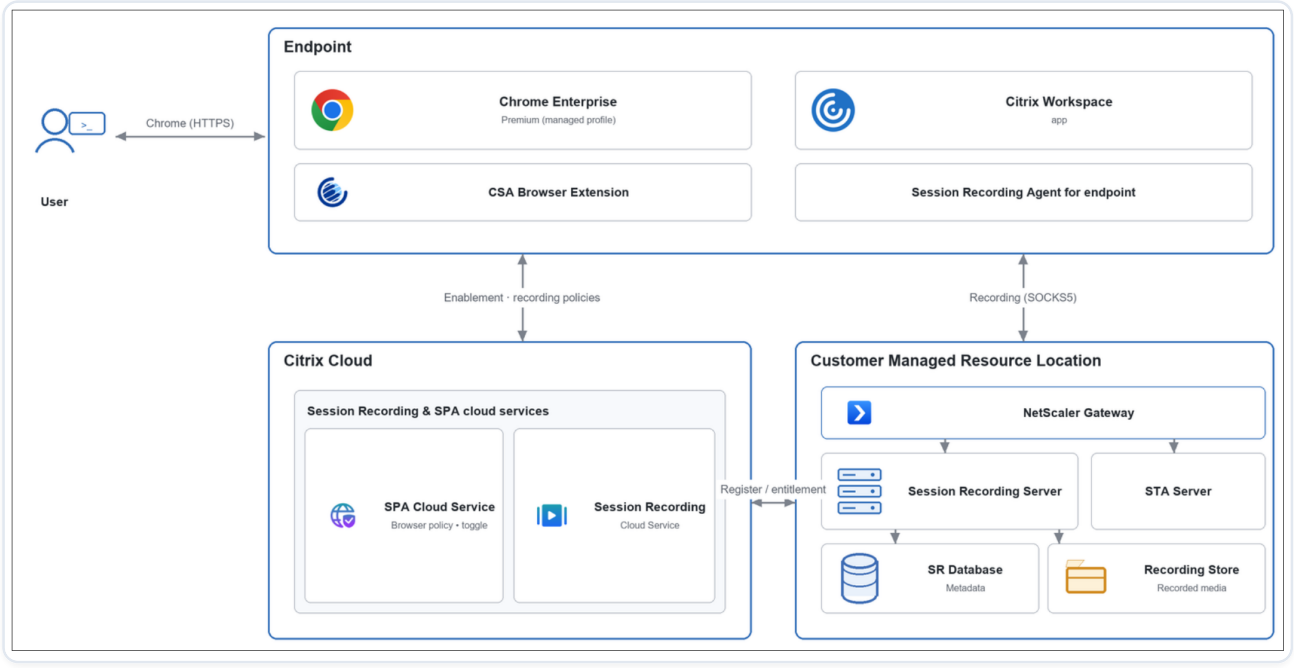
- 提供灵活的策略，自动触发应用程序和桌面会话的录制。
- 使 IT 人员能够监视和检查用户活动，并支持内部控制以实现法规遵从性和安全监视。
- 通过加快问题识别和缩短解决时间来帮助技术支持。

有关详细信息，请参阅优势。

体系结构

会话录制解决方案涵盖三个平面：

- 具有托管 Chrome 配置文件、Citrix Secure Access 扩展和适用于端点的会话录制代理的端点。
- Citrix Cloud 控制平面，其中包含 Secure Private Access 和会话录制云服务。
- 客户管理的资源位置，包括 NetScaler Gateway、STA 服务器、会话录制服务器及其数据库和录制存储。



© 1997–2026 Citrix Systems, Inc. All rights reserved.

先决条件

- 适用于 Windows 2603.10 或更高版本的 Citrix Workspace 应用程序
- Endpoint analysis (EPA) 版本：26.5.1.7 及更高版本

系统要求

- Citrix Secure Private Access，以服务模式或混合模式部署，并结合 Chrome Enterprise Premium（带托管配置文件）。
- 会话录制云服务，使用会话录制服务器 2511 或更高版本。有关详细信息，请参阅入门。
- 具有以下组件的 Windows 64 位或 32 位端点：
  - Citrix Endpoint Analysis (EPA) 插件 26.5.1.7 或更高版本。
  - 适用于 Windows 的 Citrix Workspace 应用程序，版本 2603.10 或更高版本，并安装了会话录制端点代理

设置环境

完成以下步骤以启用和验证 Chrome Enterprise 会话的端点录制。

配置会话录制站点

按照配置端点录制策略中记录的步骤操作。

注意：

端点录制需要 NetScaler Gateway。它在两种 Secure Private Access 部署类型中都通过 STA 将录制流量路由到会话录制服务器。即使使用 Secure Private Access 服务（其中 NetScaler 不管理用户到应用程序的访问），您也必须为录制流量提供网关 URL。

在 Secure Private Access 中配置会话录制浏览器策略

1. 登录到 Secure Private Access 管理控制台。
2. 转到 **策略 > 浏览器策略**，然后单击 **创建浏览器策略**。
3. 选择 **会话录制**，然后单击 **管理**。
4. 单击 **添加规则**，输入规则名称，然后单击 **下一步**。
5. 设置条件（用户和组）。（可选）添加 **地理位置**、**网络位置** 和 **设备状态检查**，然后单击 **下一步**。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. 单击 **保存**。规则计数显示在 **浏览器策略 > 会话录制** 选项卡上。

为端点安装带会话录制代理的 Workspace 应用程序

请按照 会话录制附加组件支持 中记录的步骤操作。

重放录制的会话

录制内容可在会话录制控制台中查看。

- 与用户 Chrome 工作配置文件关联的所有窗口都将被录制。
- 跨一个或多个显示器的多个窗口都将被录制。
- 失焦或被其他应用程序遮挡的窗口仍将完整录制。
- 最小化的窗口以及启用了防屏幕捕获的窗口在播放期间显示为黑色矩形。

最佳实践

- **保留一个全局站点**。使用单个全局端点录制站点并记录配置。更改它可能会无意中禁用其他站点的已配置策略。
- **区域对齐**。将会话录制云服务 URL、云客户端和后端保留在同一 Citrix Cloud 区域中，以避免延迟和数据驻留问题。
- **规划存储**。全屏 Web/SaaS 录制可能会占用大量存储空间。相应地调整服务器、会话录制数据库和录制存储的大小，并密切监控存储消耗。
- **首先验证授权和角色**。Citrix DaaS 和 Citrix Secure Private Access 授权不匹配是部署失败最常见的原因。在启用策略之前，请确认存在单个活动的客户记录，并且已分配所需的管理角色。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

浏览器会话重新身份验证控制

Citrix Secure Private Access 允许管理员对 Chrome Enterprise Premium (CEP) 浏览器会话强制执行会话超时策略。用户在配置的会话持续时间后需要重新进行身份验证，无论浏览器活动如何。这加强了通过 Google Chrome 工作配置文件访问的应用程序的零信任访问控制。

会话过期后，用户必须使用企业凭据和多重身份验证 (MFA) 重新进行身份验证。成功重新身份验证后，将恢复其上次活动的页面并重新启动会话计时器。

支持的部署： Secure Private Access 服务和混合部署。

支持的平台： Windows、macOS、Linux、ChromeOS。

先决条件

确保满足以下先决条件：

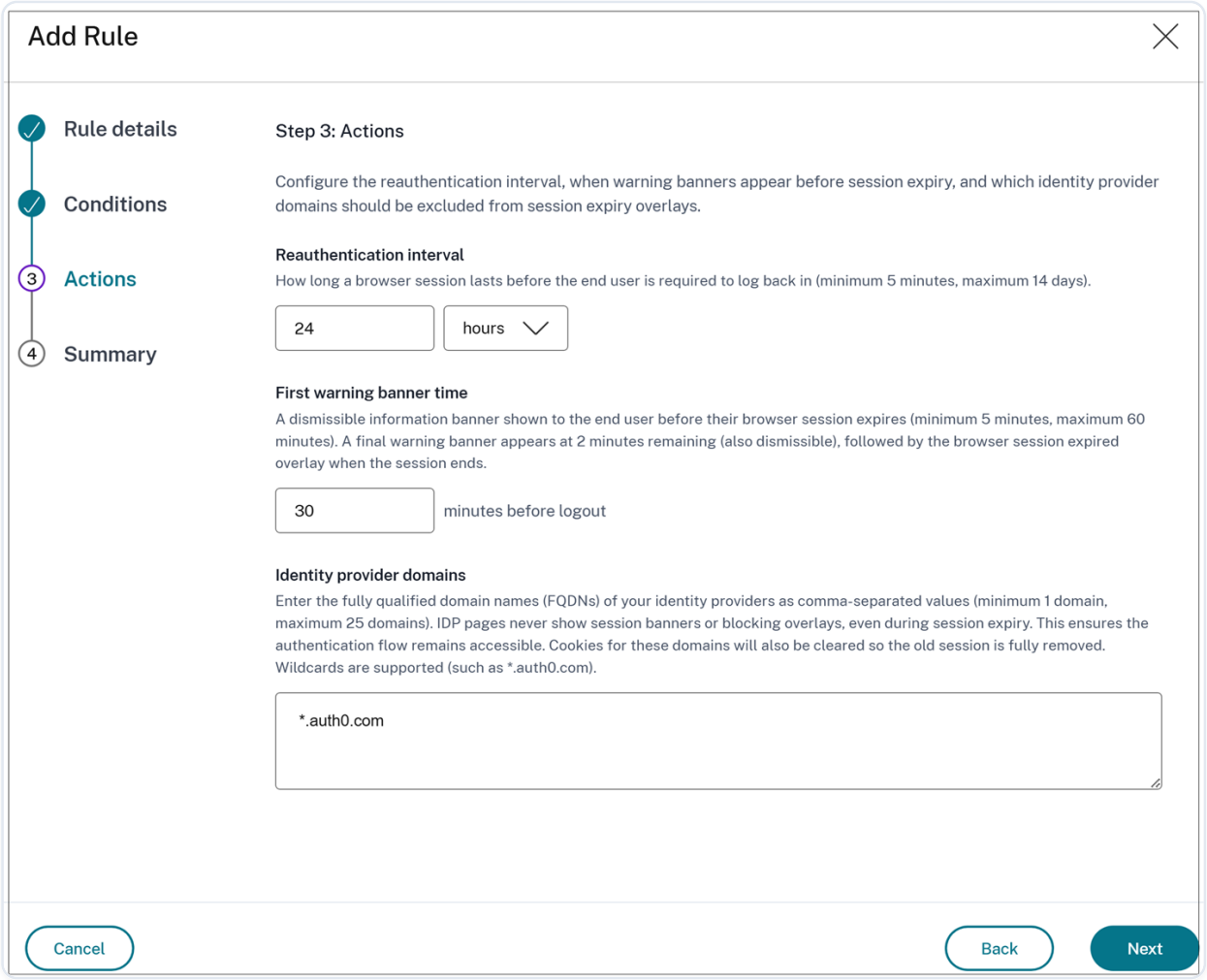
- Citrix Secure Access 与 Chrome Enterprise Premium (CEP) 之间的集成已完成。

启用浏览器会话重新身份验证控制

1. 登录 Secure Private Access 管理控制台。
2. 转到 **策略 > 浏览器策略**，然后单击 **创建浏览器策略**。
3. 选择 **浏览器会话重新身份验证**，然后单击 **管理**。
4. 单击 **添加规则** 以添加规则来启用浏览器会话重新身份验证。
    a. 输入规则名称，然后单击 **下一步**。
    b. 根据您的要求选择条件，例如用户或组。您还可以添加诸如 **地理位置**、**网络位置** 和 **设备姿态检查** 等条件。
    c. 点击 **下一步**。
    d. 配置以下内容：
    - **重新身份验证间隔**：用户需要重新进行身份验证之前浏览器会话的持续时间。间隔可以设置为 5 分钟到 14 天之间，并以分钟、小时或天为单位进行配置。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **首次警告横幅时间**：在浏览器会话过期之前向用户显示的、可关闭的警告横幅。该值可以在过期前 5 到 60 分钟之间设置。当剩余 2 分钟时，会出现第二个警告横幅，会话结束时会显示会话过期叠加层。
- **身份提供商域**：您的身份提供商的完全限定域名 (FQDN)，以逗号分隔。您可以指定 1 到 25 个域。在 IdP 页面上会抑制会话横幅和阻止叠加层，以确保身份验证流程不中断。当会话过期时，这些域的 Cookie 将被清除，以确保旧会话被完全移除。支持通配符（例如，*.auth0.com）。



5. 点击 **下一步**，然后点击 **保存**。

为剪贴板容器策略配置的规则数量显示在 **浏览器策略 > 浏览器会话重新身份验证** 选项卡中。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SSH 控制

Citrix Secure Private Access 与 Chrome Enterprise Premium 集成，可在浏览器内直接启用安全的 SSH 会话。此集成增强了安全性并简化了管理员和用户的访问。

组织需要对基于 SSH 的系统进行安全的远程管理。使用独立 SSH 客户端的传统方法存在风险，因为它们会将端点暴露给非托管环境，并且缺乏强大的数据丢失防护 (DLP) 强制执行，从而使合规性变得具有挑战性。

SSH 会话现在在 Chrome 浏览器中启动，而不是使用独立的 SSH 客户端，这减少了对本地安装的依赖并提高了合规性。

注意：

- 此功能适用于混合和云部署中集成了 Chrome Enterprise Premium 的 Secure Private Access 设置。有关详细信息，请参阅以下主题：
- 您必须拥有管理员权限才能配置 Secure Private Access 和 Chrome Enterprise Premium 策略。
- 不支持连接到 FreeBSD 服务器。

此集成的优势

此集成提供以下主要优势：

- **增强的安全性：** 消除了对非托管 SSH 客户端的依赖，降低了安全风险暴露。
- **简化访问：** 提供浏览器原生访问，无需安装额外的软件。
- **合规性：** 直接在浏览器内强制执行企业 DLP 策略，有助于满足法规要求。
- **运营效率：** 降低了与端点管理和客户端部署相关的 IT 开销。

用例

此功能支持各种用例，例如：

- **医疗保健自助服务终端：** 无需安装本机客户端即可实现安全的 SSH 访问，用于设备故障排除。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **IT 管理：** 允许管理员从受管 Chrome 浏览器安全地访问 Linux 服务器，并强制执行 DLP 策略。
- **承包商访问：** 为第三方供应商提供临时 SSH 访问，而不会损害组织的安全状况。

系统要求

确保您的环境满足以下要求：

- 最新版本的 Chrome Enterprise Premium。
- Citrix Secure Private Access 已配置为进行集成。
- 必须在 Secure Private Access 管理控制台中创建允许 SSH 流量的访问策略。

先决条件

确保满足以下先决条件，以启用对 SSH 应用程序的安全访问：

- Citrix Secure Private Access 已配置 Google Chrome Enterprise Premium 集成。有关详细信息，请参阅与 Google Chrome Enterprise Premium 集成。
- 最终用户已安装最新版 Google Chrome 浏览器并安装了 Citrix Secure Access 浏览器扩展。
- 有关部署特定的先决条件，请参阅以下主题：
  - 云部署 - Citrix Secure Private Access 入门
  - 混合部署 – 系统要求和先决条件

配置安全私有访问以进行 SSH 访问

1. 登录到 Citrix Cloud，然后单击 **安全私有访问**。
2. 在管理控制台中，单击 **应用程序 > 应用程序配置**，然后单击 **添加应用程序**。
3. 在安全私有访问中将 SSH 应用程序配置为 TCP/UDP 应用程序。
   - 应用程序可以具有确切的 IP 地址或范围、FQDN 或服务器的主机名。
   - 支持通过默认端口和非默认端口使用 SSH。
4. 将访问权限分配给相关用户组。

有关创建 TCP/UDP 应用程序的详细信息，请参阅以下主题。

- 云部署 - 对 TCP/UDP 应用程序的支持
- 混合部署 – 对 TCP/UDP 应用程序的支持

© 1997–2026 Citrix Systems, Inc. All rights reserved.

配置 SSH 策略

1. 登录到安全私有访问管理控制台。
2. 转到 **策略 > 浏览器策略**，然后单击 **创建浏览器策略**。
3. 选择 **SSH**，然后单击 **管理**。
4. 点击 **添加规则** 为用户添加规则以启用 SSH。
5. 输入规则名称，然后点击 **下一步**。
6. 根据您的要求选择条件，例如用户或组。1. 您还可以添加条件，例如 **地理位置、网络位置** 和 **设备姿态检查**。
7. 点击 **下一步**。
8. 点击 **保存**。

为防键盘记录策略配置的规则数量显示在 **浏览器策略 > SSH** 选项卡中。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

远程桌面控制

Citrix Secure Private Access 与 Chrome Enterprise Premium 集成，可在浏览器中直接启用安全的 RDP 会话。此集成增强了安全性，并简化了管理员和用户的访问。

传统的远程桌面访问通常依赖于本机 RDP 客户端，这些客户端通常缺乏基于浏览器的 DLP 强制执行。这种缺陷会增加安全风险，尤其是在非托管环境中，并使合规性变得具有挑战性。组织需要一个安全、合规且简化的远程访问解决方案来解决这些问题。

此集成使管理员能够强制执行企业级 DLP 控制，例如剪贴板控制和屏幕截图预防。

注意：

- 此功能适用于混合和云部署的 Chrome Enterprise Premium 集成 Secure Private Access 设置。有关详细信息，请参阅以下主题：
- 您必须拥有管理员权限才能配置 Secure Private Access 和 Chrome Enterprise Premium 策略。

不支持的功能：

不支持以下功能：

- 剪贴板共享
- 音频/网络摄像头/智能卡/USB 重定向
- 双因素和生物识别身份验证

此集成的优势

此集成提供以下主要优势：

- **安全性：** 通过强制执行精细的 DLP 策略，防止远程会话期间的数据泄露。
- **合规性：** 通过强大的安全控制，有助于满足敏感环境的法规要求。
- **易用性：** 无需安装单独的 RDP 客户端，简化了用户访问和部署。
- **灵活性：** 支持从托管的 Chrome 浏览器进行安全的 RDP 访问，提供一致且安全的体验。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

用例

此功能支持多种用例，例如：

- **企业承包商：** 为第三方供应商提供安全的远程桌面访问，同时不损害内部安全性。
- **医护人员：** 支持在医疗环境中从自助服务终端或共享工作站安全访问 Windows 系统。
- **IT 支持：** 允许 IT 人员对远程桌面进行故障排除，无需安装额外的软件。

系统要求

请确保您的环境满足以下要求：

- 最新版本的 Chrome Enterprise Premium。
- Citrix Secure Private Access 已配置为集成。
- 必须在 Secure Private Access 管理控制台中创建允许 RDP 流量的访问策略。

先决条件

请确保满足以下先决条件，以启用对 RDP 应用程序的安全访问：

- Citrix Secure Private Access 已配置 Google Chrome Enterprise Premium 集成。有关详细信息，请参阅 与 Google Chrome Enterprise Premium 集成。
- 最终用户已安装带有 Citrix Secure Access 浏览器扩展的最新 Google Chrome 浏览器。
- 有关部署特定的先决条件，请参阅以下主题：
  - 云部署 - Citrix Secure Private Access 入门
  - 混合部署 – 系统要求和先决条件

配置 Secure Private Access 以进行 RDP 访问

1. 登录 Citrix Cloud，然后单击 **Secure Private Access**。
2. 在管理控制台中，单击 **Applications > App Configuration**，然后单击 **Add an app**。
3. 将 RDP 应用程序配置为 Secure Private Access 中的 TCP/UDP 应用程序。
   - 该应用程序可以具有服务器的精确 IP 地址或范围、FQDN 或主机名。
   - RDP 支持默认端口和非默认端口。
4. 将访问权限分配给相关的用户组。

© 1997–2026 Citrix Systems, Inc. All rights reserved.

有关创建 TCP/UDP 应用程序的详细信息，请参阅以下主题。

- 云部署 - 支持 TCP/UDP 应用程序
- 混合部署 – 支持 TCP/UDP 应用程序

配置远程桌面策略

1. 登录到 Secure Private Access 管理控制台。
2. 转到 **策略 > 浏览器策略**，然后单击 **创建浏览器策略**。
3. 选择 **远程桌面**，然后单击 **管理**。
4. 单击 **添加规则** 为用户添加规则以启用远程桌面。
5. 输入规则名称，然后单击 **下一步**。
6. 根据您的要求选择条件，例如用户或组。 1. 您还可以添加诸如 **地理位置、网络位置** 和 **设备姿态检查** 等条件。
7. 单击 **下一步**。
8. 单击 **保存**。

为防键盘记录策略配置的规则数量显示在 **浏览器策略 > 远程桌面** 选项卡中。

© 1997–2026 Citrix Systems, Inc. All rights reserved.