



Citrix Secure Private Access™ 混合部署

Contents

解决方案概述	13
为何使用 Secure Private Access	13
关键组件	13
网络图	14
最终用户访问方法	15
Citrix 端点分析 (EPA) 客户端	16
限制	16
新增功能	17
31 July 2026	17
27 April 2026	17
07 April 2026	18
2025 年 11 月	18
2025 年 9 月	19
2025 年 8 月	20
2025 年 5 月	20
2025 年 4 月	21
2024 年 12 月	22
2024 年 10 月	22
初始版本	22
已知问题	28
系统要求和先决条件	30
软件版本要求	30
防火墙要求	30
先决条件	32
NetScaler 先决条件	32
Chrome 企业高级版 + Citrix 安全访问部署	33

仅限 Citrix Secure Access 部署	33
Cloud Connector 先决条件	34
StoreFront 先决条件	34
安全私有访问先决条件	34
Google 先决条件	35
Chrome 企业高级版许可证	35
Google Workspace 管理控制台	35
谷歌浏览器	36
托管的 Chrome 配置文件	36
将 Citrix Workspace 中配置的用户目录与 Google Cloud 用户目录同步	36
绕过 TLS 检查	37
Secure Private Access 混合部署入门	38
开始之前	38
验证您的 Secure Private Access 授权	38
验证必备条件	38
选择部署模式	39
后续步骤	39
步骤 1：设置 Google Chrome 企业高级版	39
Google Chrome 企业高级版配置	40
步骤 2：设置第一个数据中心	41
步骤 3：配置和分析	43
下载并运行 NetScaler 和 StoreFront 脚本	43
NetScaler 脚本	43
StoreFront 脚本	45
上传报告并分析配置	46
完成载入并发布应用程序	48
入职后任务	48
配置应用程序	48

配置访问策略	48
更新 Chrome 企业高级版 配置	49
同步配置	50
访问您的应用程序（最终用户）	50
访问 Web 和 SaaS 应用程序	50
访问 TCP/UDP（客户端/服务器）应用程序	51
数据区域化	53
支持的部署	53
配置	53
限制	54
设置组件	55
云连接器配置	55
安全私有访问服务	55
Citrix Secure Private Access 服务的端口配置	55
Secure Private Access 负载均衡器	56
在 Cloud Connector 上为 Secure Private Access 服务配置 TLS/SSL 证书	56
NetScaler	59
配置身份验证	59
身份验证配置示例	60
多重身份验证与条件身份验证	60
第三方集成与多重身份验证	60
设备状态扫描 (EPA)	60
其他场景	60
StoreFront	61
配置新 Store	61
组件分析器	62
安全私有访问分析器	63
NetScaler Gateway 分析器	64

StoreFront 分析器	64
与 Google Chrome 企业高级版 集成	65
Chrome Enterprise Premium 高级安全功能	65
成功集成的先决条件	66
Citrix Secure Private Access - 支持的部署模式	66
法律声明	67
管理员角色和权限	67
Google 自定义管理员角色权限	67
创建和分配角色和权限	69
Open ID Connect 配置文件，用于将 NetScaler Gateway 用作 IdP	69
创建 Google OIDC SSO 配置文件	70
绑定 OIDC 配置文件（到 OU 或组）	72
将 NetScaler 配置为 OAuth IdP	73
目录同步	73
使用 G Suite 连接器的 Microsoft Entra ID	73
谷歌云目录同步 (GCDS) 工具	74
活动目录	74
谷歌云目录同步配置	75
最终用户体验	84
适用于 Chrome Enterprise Premium 的 Citrix Secure Access 扩展程序	86
Secure Access 扩展程序日志	86
适用于 Chrome Enterprise 的 Citrix Secure Access 控件	87
支持的控件	90
策略中的用户和组	90
搜索用户或组	90
使用同步的用户和组	91
反键盘记录控制	91
先决条件	92

配置反键盘记录策略	92
剪贴板容器控制	92
先决条件	92
启用剪贴板容器控制	93
启用剪贴板共享范围	94
Web 应用程序的域后缀	96
先决条件	97
配置 DNS 后缀	97
会话录制控制	98
体系结构	98
必备条件	98
系统要求	99
设置环境	99
浏览器会话重新身份验证控制	100
先决条件	100
启用浏览器会话重新身份验证控制	100
SSH 控制	101
此集成的优势	102
用例	102
系统要求	102
先决条件	102
配置 Secure Private Access 以进行 SSH 访问	103
配置 SSH 策略	103
远程桌面控制	104
此集成的优势	104
用例	104
系统要求	105
先决条件	105

配置 Secure Private Access 以进行 RDP 访问	105
配置远程桌面策略	105
排查 CEP 集成问题	106
用于 CEP 故障排除的诊断日志	107
确认用户已登录到正确的 Chrome 配置文件	108
检查 Secure Enterprise Browser 扩展是否已安装	108
检查 ExtensionInstallForcelist 策略	108
排查冲突的扩展安装列表策略	109
检查 Secure Enterprise Browser 扩展策略	109
检查 Google 管理控制台中的用户扩展配置	111
检查路由是否正在获取	111
在 Secure Private Access 管理控制台中验证 CEP 集成	112
排查 Google Secure Gateway 可达性问题	112
确认应用程序包含在路由中	113
排查路由应用程序访问问题	113
确保 IdP 和 Google Directory 对齐	114
检查 Google 管理控制台中组的访问设置	114
CEP 集成中的已知问题	115
Secure Private Access 用户界面	115
自适应访问策略配置	115
Google Chrome 浏览器	115
应用程序配置和管理	117
配置企业 Web 或 SaaS 应用程序	117
删除应用程序时自动清理路由条目	119
后续步骤	120
使用 HAR 文件发现相关域	120
示例	120
先决条件	121

导入 HAR 文件	121
管理相关域	123
验证和文件要求	123
配置 TCP/UDP 应用程序	124
后续步骤	127
配置 TCP/UDP - 服务器到客户端应用程序	127
编辑应用程序	128
后续步骤	128
访问策略配置和管理	129
配置应用程序的访问策略	129
配置访问策略	129
编辑访问策略	131
更改访问策略优先级	131
后续步骤	131
策略条件	132
用户和用户组	132
验证用户和组同步	133
网络位置	134
配置会话策略	135
设备证书注册	136
设备姿态服务	138
在 NetScaler Gateway 上配置设备姿态检查	138
本地 NetScaler® Gateway 上的设备状态检查	138
授权	139
为 Secure Private Access 混合解决方案启用设备状态	139
管理设置	140
管理设置	140
应用程序域	140

配置报告	140
生成配置报告	141
安装后管理设置配置	145
重置 Secure Private Access 配置	146
升级	146
高级安全专用访问功能	147
高级数据中心配置	148
先决条件	148
GSLB 配置 CLI 命令	148
参考	149
数据中心设置和配置	150
全局服务器负载均衡连接代理	151
先决条件	151
配置 GSLB 连接代理	151
配置全局服务器负载均衡器域 URL	152
配置	152
编辑数据中心（可选）	153
配置和分析	154
基于上下文的应用程序路由	154
用例：基于上下文的路由	155
更改路由类型的步骤	156
用例：将内部企业用户直接路由到后端应用程序	156
路由优先级	156
支持的 Citrix Secure Access™ 客户端	156
示例用例	157
使用会话策略配置医院网络内的直接路由	157
发现最终用户访问的域或 IP 地址	158
新环境中的内部域应用程序发现	159

从应用程序发现页面创建应用程序	162
更新现有应用程序	162
策略建模工具	163
配置数据丢失防护 (DLP) 策略	164
高可用性部署	165
数据中心内的高可用性	165
NetScaler	165
云连接器 (Secure Private Access 服务器)	165
StoreFront 服务器	167
重置 Secure Private Access 配置	167
可见性和监控	168
服务授权	168
支持的客户端	168
如何访问 Monitor	168
会话定义	168
Web/SaaS 应用程序会话	169
TCP/UDP 应用程序会话	169
查看用户会话	170
应用程序拓扑	171
分类和故障排除	173
Citrix Secure Access 模式下的用户/客户端问题	173
用户无法登录	173
用户无法启动应用程序	174
收集具有调试级别日志记录的 NetScaler 支持包的步骤	174
恢复详细日志记录	175
有助于故障排除的工具	175
收集客户端日志	175
Chrome 企业高级版日志	175

捕获 Secure Enterprise Browser 扩展日志的步骤	175
捕获 Citrix Secure Access 扩展日志的步骤	178
使用 Monitor 进行实时会话故障排除	178
会话代码	179
应用程序枚举消息代码	179
应用程序启动消息代码	180
应用程序启动错误代码	181
最终用户体验	183
使用 Chrome Enterprise Premium 访问 Web 和 SaaS 应用程序	183
选项 1：创建托管的 Chrome 配置文件并直接访问应用程序（推荐）	183
选项 2：在现有托管 Chrome 配置文件中访问商店 URL	185
选项 3：从非受管 Chrome 配置文件或非 Chrome 浏览器（Edge、Firefox）访问应用商店 URL	186
选项 4：通过 Citrix Workspace 应用程序访问应用程序	187
访问客户端/服务器 (TCP/UDP) 应用程序	188
index	190
与 DaaS 监视器集成	190
服务授权	190
支持的客户端	190
如何访问 Monitor	190
会话定义	190
Web/SaaS 应用程序会话	191
TCP/UDP 应用程序会话	191
查看用户会话	192
应用程序拓扑	193
上下文标签	195
使用 GUI 配置自定义标签	195
配置经典网关预身份验证策略	195

将自定义标记绑定到 NetScaler Gateway	197
使用 CLI 配置自定义标记	198
添加新的上下文标签	199
关于发送到 Secure Private Access 提供程序的 EPA 标签的注意事项	199

解决方案概述

Citrix Secure Private Access™ 适用于混合部署，提供零信任网络访问 (ZTNA) 解决方案，可在您的本地环境和 Citrix Cloud 之间划分功能。这种架构使您能够利用现有投资，同时获得基于云的管理。职责分配如下：

- **本地组件（数据平面）**：您现有的 NetScaler Gateway、StoreFront 和 Windows Cloud Connector 安装仍保留在本地。这些组件负责控制和路由所有用户访问流量。
- **Citrix Cloud 组件（控制平面）**：
 - 集中管理：使用 Citrix Cloud UI 进行所有配置、管理和策略管理。
 - 监控和故障排除：利用托管的 Citrix Monitor 服务进行所有监控、分析和故障排除功能。

为何使用 Secure Private Access

Citrix Secure Private Access 解决方案通过将单点登录 (SSO)、远程访问和带外内容检查集成到统一平台中，提供端到端访问控制。

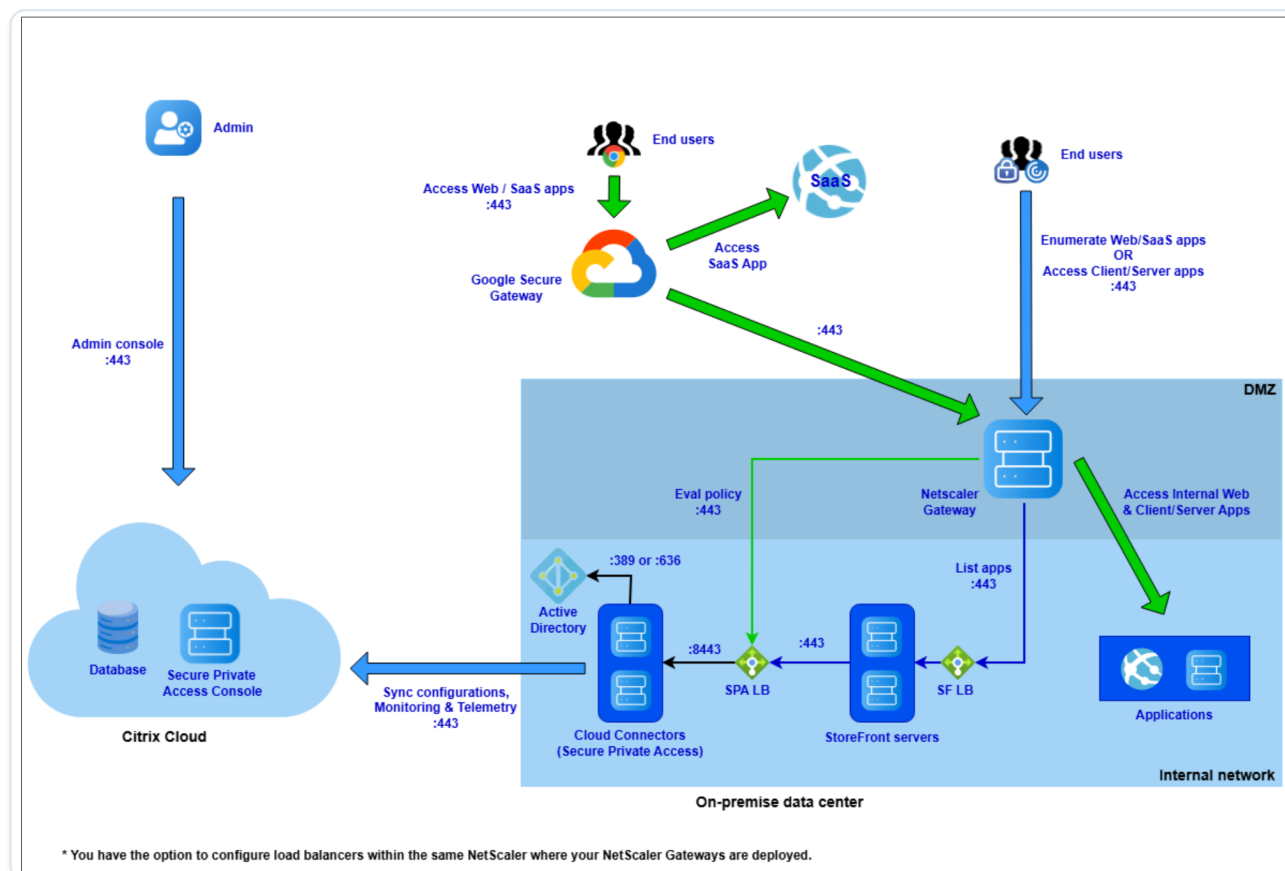
- **管理应用程序访问**：为所有批准的 SaaS 和内部应用程序强制执行安全策略并提供简化的 SSO 体验。
- **增强安全性**：通过过滤对特定网站和网站类别的访问，保护网络和设备免受恶意软件和数据泄露的影响。
- **Google Chrome Enterprise Premium 集成**：利用 Google Chrome Enterprise Premium，允许用户以熟悉且安全的方式原生访问授权的企业 Web 应用程序。有关详细信息，请参阅 [与 Google Chrome Enterprise Premium 集成](#)。
- **数据丢失防护 (DLP)**：强制执行精细控制以限制打印、下载和剪贴板复制粘贴操作。
- **分析用户活动并保护企业网络**：深入了解用户活动，例如恶意网站访问或有风险的文件传输。使用这些分析采取纠正措施并保护企业网络。
- **无缝用户体验**：从任何设备、位置或网络提供对关键业务应用程序的安全、无缝访问。

关键组件

以下部分提供了有关 Secure Private Access 混合解决方案关键组件的更多信息。

网络图

下图说明了 Secure Private Access 混合解决方案的网络图。



Secure Private Access 混合解决方案的关键组件包括：

- **Secure Private Access 管理控制台：** 单击 Citrix Cloud 中的 Secure Private Access 磁贴以访问管理控制台。使用管理控制台进行入职、配置应用程序和设置策略。站点管理集中且简化。无需本地基础设施。
- **Google Chrome 和 Chrome Enterprise Premium 安全网关：** 最终用户使用 Google Chrome 浏览器访问企业内部和 SaaS 应用程序。

Chrome Enterprise Premium 安全网关充当正向代理，以强制执行零信任访问框架。它提供对应用程序访问的精细、上下文感知控制。来自用户 Chrome 浏览器的所有流量都通过 Chrome Enterprise Premium 安全网关连接到 NetScaler Gateway，确保在授予访问权限之前应用策略。

注意：

仅当使用 Secure Private Access 提供对 SaaS 和内部 Web 应用程序的安全访问时，才需要 Google 组件。如果您计划仅将 Secure Private Access 用于 TCP/UDP（客户端/服务器）应用程序，则不需要它们。

- **NetScaler Gateway**：NetScaler Gateway 组件提供对应用程序和桌面的安全远程访问。它充当外部用户的安全入口点，允许他们从网络外部连接到企业资源。有关详细信息，请参阅 [NetScaler](#)。
- **Cloud Connector**：Cloud Connector 是一个安装在 Windows 服务器上的本地组件，充当您的网络与 Citrix Cloud 之间的安全通信桥梁。

Cloud Connector 负责同步云中 Secure Private Access 服务的所有配置和策略。然后，这些策略用于强制执行应用程序的访问规则。连接器还会持久缓存此数据，这允许用户即使在 Citrix Cloud 不可用时也能继续访问应用程序。有关详细信息，请参阅 [Cloud Connector](#)。

- **StoreFront**：本地 StoreFront 是面向用户的组件，它聚合、枚举并将所有授权的应用程序和桌面交付给最终用户。它充当企业应用商店。这种混合架构允许您利用现有的 StoreFront 设置，而无需迁移到云端。有关详细信息，请参阅 [StoreFront](#)。

注意：

如果您计划仅将 Secure Private Access 用于 TCP/UDP（客户端/服务器）应用程序，则 StoreFront 是可选的。如果您确实配置了 StoreFront，它将仅枚举配置为 Web 应用程序类型的应用程序。标准 TCP/UDP 应用程序不会显示在商店中。

最终用户访问方法

最终用户可以使用以下任一方法访问 Secure Private Access 应用程序：

- **Citrix Workspace 应用程序 (CWA) 和 Workspace UI**：这是最终用户可以用来连接和查看 Citrix Store 的两个客户端。
 - **Citrix Workspace 应用程序（本机客户端）**：这是一个安装在用户端点（例如 Windows 和 macOS）上的完整本机应用程序。它提供最丰富的用户体验，并且是某些高级功能所必需的。
 - **Citrix Workspace UI（Web 客户端）**：这是商店的基于浏览器的版本。用户通过在 Web 浏览器中导航到 StoreFront URL 来访问它。它允许用户无需安装任何客户端软件即可访问其应用程序。
- **Google Chrome**：所有 Web 和 SaaS 应用程序都通过使用托管企业配置文件的 Google Chrome 浏览器独占启动。当用户从其 Citrix Store 启动应用程序时，它会自动在此托管的 Chrome Enterprise 配置文件中打开，以强制执行所有安全控制。

注意：

如果您计划仅将 Secure Private Access 用于 TCP/UDP（客户端/服务器）应用程序，则 Google Chrome 并非强制要求。用户可以使用任何浏览器（例如非托管的 Chrome、Edge 或 Firefox）来访问 TCP/UDP 应用程序。

- **Citrix Secure Access (CSA) 客户端：**这是安装在用户端点上的客户端代理，是 ZTNA 访问所有 TCP/UDP（客户端/服务器）应用程序所必需的。

CSA 提供安全的、按应用程序的内部企业资源连接，而无需传统的全隧道 VPN。

Citrix 端点分析 (EPA) 客户端

Citrix EPA 客户端是一个轻量级插件，在用户端点上运行以执行设备姿态扫描（也称为 EPA 扫描）。仅当您配置了访问策略，在授予访问权限之前检查端点的安全姿态（例如，最新的操作系统、特定的防病毒软件或注册表项）时，才需要此客户端。

限制

- 不支持将 EPA 作为因素。相反，您可以使用设备姿态服务。有关设备姿态服务的更多信息，请参阅 [设备姿态](#)。
- 在虚拟服务器级别启用设备姿态检查不支持与 Always On 结合使用。
- 策略建模仅支持用户条件。不支持设备姿态和网络位置条件。
- StoreFront 分析器仅支持 StoreFront 中的一个 Secure Private Access 类型存储。
- 当前版本中，用于混合部署的简化 Secure Private Access 用户界面仅支持一个数据中心（一个网关和一个 StoreFront）。
- Citrix Secure Access 客户端中的网络位置不支持 IPv6。

新增功能

以下部分介绍了新功能和增强功能的详细信息。

31 July 2026

- 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。

Secure Private Access 支持以下策略。

- 防键盘记录
- 剪贴板容器
- Web 应用程序的域后缀
- 会话录制
- 浏览器会话重新身份验证

27 April 2026

- 高级数据中心配置

Secure Private Access 混合部署现在支持在多个数据中心和多站点配置中使用 NetScaler GSLB 进行主动-主动站点部署，并采用 GSLB 连接代理的站点持久性方法。有关详细信息，请参阅[高级数据中心配置](#)。

- 支持配置全局服务器负载均衡器域 URL

为了为 Secure Private Access 设置多站点冗余，您必须配置一个全局服务器负载均衡器 (GSLB) 地址。此地址充当单个入口点，根据您的流量策略（例如静态邻近性）将用户路由到特定数据中心的 Secure Private Access 网关。有关详细信息，请参阅[配置全局服务器负载均衡器域 URL](#)。

- 全局服务器负载均衡连接代理支持

全局服务器负载均衡 (GSLB) 连接使 NetScaler Gateway 能够透明地检测错误路由的请求，并将其代理到正确的站点，而无需任何用户干预。有关详细信息，请参阅 [全局服务器负载均衡连接代理](#)。

07 April 2026

- **基于上下文的应用程序路由**

配置应用程序时，会在应用程序配置下为应用程序 URL 及其相关域或应用程序目标定义路由类型。此处定义的路由类型适用于所有有权访问该应用程序的用户。但是，在某些情况下，管理员可能希望根据用户上下文以不同方式路由同一应用程序。例如，当用户在公司网络内部时，内部应用程序 URL 或目标必须直接路由，而不是通过 Secure Private Access 路由。访问策略中的“路由例外”配置允许管理员为符合策略中定义的条件或计算机编辑路由类型。有关详细信息，请参阅 [基于上下文的应用程序路由](#)。

- **在浏览器中安全访问 SSH 和 RDP 应用程序**

Citrix Secure Private Access 与 Chrome Enterprise Premium 集成，可在浏览器中直接启用安全的 SSH 和 RDP 会话。有关详细信息，请参阅以下主题：

- [在浏览器中安全访问 SSH 应用程序](#)
- [在浏览器中安全访问 RDP 应用程序](#)

2025 年 11 月

- **简化的入门流程**

用于混合部署的 Secure Private Access 入门界面现已显著简化，以精简所有组件的配置过程。增强的用户界面现在具有直观的拓扑视图，可显示每个组件的逐步配置状态。这种可视化方法使管理员能够快速了解部署状态，识别已完成的配置步骤，并确定仍待处理的操作，从而减少设置时间并最大程度地减少配置错误。

此外，NetScaler 支持 SecurePrivateAccessProfile，以简化混合部署的 NetScaler Gateway 配置。

有关详细信息，请参阅 [Secure Private Access 混合部署入门](#)。

- **谷歌浏览器企业高级版支持**

通过将 Citrix Secure Private Access 服务与 Google Chrome Enterprise Premium 集成，最终用户现在可以使用 Google Chrome 浏览器作为其企业浏览器安全地访问私有 Web/SaaS 应用程

序，并实现具有数据丢失防护 (DLP) 控制、Web 过滤和 ZTNA 策略强制执行的按应用程序访问。

有关详细信息，请参阅 [与 Google Chrome Enterprise Premium 集成](#)

- **分析器用于验证和识别组件中的配置问题**

组件分析器是一个基于 Web 的工具，用于执行 Secure Private Access 混合设置所需的配置检查。上传必要的报告后，分析器会识别问题，并提供详细的错误消息和解释，包括检测到的 StoreFront 配置错误示例。该工具还会列出解决已识别问题的潜在补救措施。

有关详细信息，请参阅 [组件分析器](#)。

- **支持使用 NetScaler Gateway URL 从 StoreFront UI 启动应用程序**

最终用户现在可以通过访问 NetScaler Gateway URL，直接从 StoreFront 用户界面无缝启动应用程序。

有关详细信息，请参阅 [访问 Web 和 SaaS 应用程序](#)。

- **访问策略中支持网络位置服务条件**

网络位置服务 (NLS) 是一种策略条件，允许您根据用户的网络位置限制访问。管理员可以根据用户访问应用程序的位置配置访问策略。该位置可以是用户访问应用程序的国家/地区，也可以是用户的网络位置。网络位置是使用 IP 地址范围或子网地址定义的。

有关详细信息，请参阅 [网络位置](#)。

- **配置报告**

客户管理员现在可以生成配置报告，以深入了解 Secure Private Access 设置。

有关详细信息，请参阅 [配置报告](#)。

2025 年 9 月

- **Secure Private Access 混合部署支持 iOS 设备**

从适用于 iOS 的 Secure Access Client 25.08.1 版开始，Secure Private Access 混合部署现在支持移动设备。移动用户可以从其 iOS 设备访问企业应用程序。

重要提示：

为了支持 iOS 平台上的 Citrix Secure Access 的 Secure Private Access，您还必须在 HTTP “User-Agent” 标头中添加字符串 “NSGiOSplugin”。

示例：`add vpn sessionPolicy PL_0Spahybrid "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\") && (HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"NSGiOSplugin\") || HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixSecureAccess\"))" AC_0Spahybrid`

有关详细信息，请参阅以下主题：

- [NetScaler 配置](#)
- [适用于移动设备的 Citrix Secure Private Access。](#)

2025 年 8 月

• 生成 Secure Private Access 站点配置报告

客户管理员现在可以生成配置报告，以深入了解 Secure Private Access 站点的设置。配置报告可用于以下场景：

- 识别并解决配置问题。
- 与 Citrix 支持团队共享，用于调查和故障排除。
- 将报告用作设置新站点或修改现有站点详细信息的参考。
- **新增仪表板小组件**

用于混合部署的 Secure Private Access 仪表板现已增强，包含以下小组件，以提供更深入的洞察和改进的监控：

- 设备状态日志
- 连接器状态
- 按启动次数排名的热门应用程序
- 按总访问量排名的热门发现应用程序
- 按强制执行情况排名的热门访问策略

有关详细信息，请参阅[可见性和监控](#)。

2025 年 5 月

• Citrix Secure Private Access™ 与 Google Chrome 企业高级版 的集成

Citrix Secure Private Access 与 Google Chrome Enterprise Premium 的集成使客户能够使用 Google Chrome Enterprise Premium 作为企业浏览器解决方案，以安全访问私有 Web 应用程序

和 SaaS 应用程序，并获得 Citrix Secure Private Access 提供的安全连接。有关详细信息，请参阅[Citrix Secure Private Access 与 Google Chrome Enterprise Premium 的集成](#)。

2025 年 4 月

- **本地 NetScaler® Gateway 上的设备状态检查**

Citrix 设备状态检查现在可以配置为与本地 NetScaler Gateway 配合使用。此集成允许管理员评估尝试访问网络资源的设备的安全性状态，并确保只有受信任的设备才能访问公司资源。

有关详细信息，请参阅以下主题：

- [设备姿态](#)
- [本地 NetScaler Gateway 上的设备姿态检查](#)
- [用于 NetScaler Gateway 身份验证的 Citrix 设备姿态服务](#)

- **StoreFront™ 到 Secure Private Access 通信的基于密钥的身份验证**

为 StoreFront 到 Secure Private Access 通信引入了一种基于安全密钥的身份验证方法。对于新客户，基于密钥的身份验证默认启用，而对于现有客户则禁用。现有客户必须启用安全密钥并再次运行 StoreFront 配置脚本。有关详细信息，请参阅[配置 StoreFront](#)。

- **ICA 代理模式下对 Web/SaaS 应用程序的支持**

ICA 代理模式现在支持 Web/SaaS 应用程序的枚举和启动。这也使得可以使用新的 StoreFront UI 来枚举应用程序。

ICA 代理模式支持仅在 NetScaler Gateway 14.1 版本 build 43.x 及更高版本中可用。有关配置详细信息，请参阅[NetScaler 配置](#)。

- **根据计算机上下文强制执行应用程序规则**

除了用户上下文之外，您现在还可以根据计算机上下文强制执行应用程序访问规则。在创建访问策略时，您可以选择计算机或用户上下文。有关详细信息，请参阅[配置应用程序的访问策略](#)。

- **将域排除在通过 NetScaler Gateway 隧道传输之外**

您现在可以配置要排除在通过 NetScaler Gateway 拦截和隧道传输之外的域。您可以将应用程序连接类型设置为“内部”或“外部”，以分别允许或排除域被拦截和隧道传输。有关详细信息，请参阅[配置 TCP/UDP 应用程序](#)。

- **Secure Private Access 混合部署的 TCP DNS 支持**

Secure Private Access 混合部署现在支持 TCP DNS。应用程序 FQDN 现在可以使用 TCP 解析。

2024 年 12 月

- **支持 FIPS 平台上的 Secure Private Access 混合解决方案**

Secure Private Access 混合解决方案现已在符合联邦信息处理标准 (FIPS) 并运行 13.1–37.219 及更高版本 FIPS 版本的 NetScaler 平台上受支持。有关详细信息，请参阅 [联邦信息处理标准](#)。

2024 年 10 月

以下各节提供了有关 2024 年 10 月的更多信息。

初始版本

适用于混合部署的 Citrix Secure Private Access 允许客户使用本地 StoreFront 和 NetScaler Gateway 组件实施零信任网络访问 (ZTNA) 解决方案，并使用 Citrix Cloud™ 来管理配置、管理和监控功能。

以下是适用于混合部署的 Citrix Secure Private Access 的一些主要功能。

- **Web/SaaS 和 TCP/UDP 支持：**

适用于混合部署的 Citrix Secure Private Access 支持 Web/SaaS 和 TCP/UDP 应用程序。有关详细信息，请参阅以下主题：

- [系统要求和先决条件](#)。
- [配置 Web/SaaS 应用程序](#)
- [配置 TCP/UDP 应用程序](#)

Add an app

To add an app, complete the steps below.

App Details

Where is the application located? *

☐ Outside my corporate network

☒ Inside my corporate network

App type *

HTTP/HTTPS

HTTP/HTTPS

TCP/UDP

App icon

 [Change icon](#)
(128 KB max, PNG)

[Use default icon](#)

☐ Do not display application icon in Workspace app

☐ Add application to favorites in Workspace app

☐ Allow user to remove from favorites

☐ Do not allow user to remove from favorites

App description

App category ⓘ

Ex.: Category\SubCategory\SubCategory

URL *

Application URL (https://...)

App Connectivity * ⓘ

Internal

Related Domains *

App Connectivity * ⓘ

Internal

[+ Add another related domain](#)

Save

Cancel

- 增强的访问限制选项：

在为应用程序创建访问策略时，您可以选择必须对应用程序强制执行的访问限制。这些安全限制在系统中是预定义的。管理员无法修改或添加其他组合。有关详细信息，请参阅 [配置访问策略](#)

。

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

23

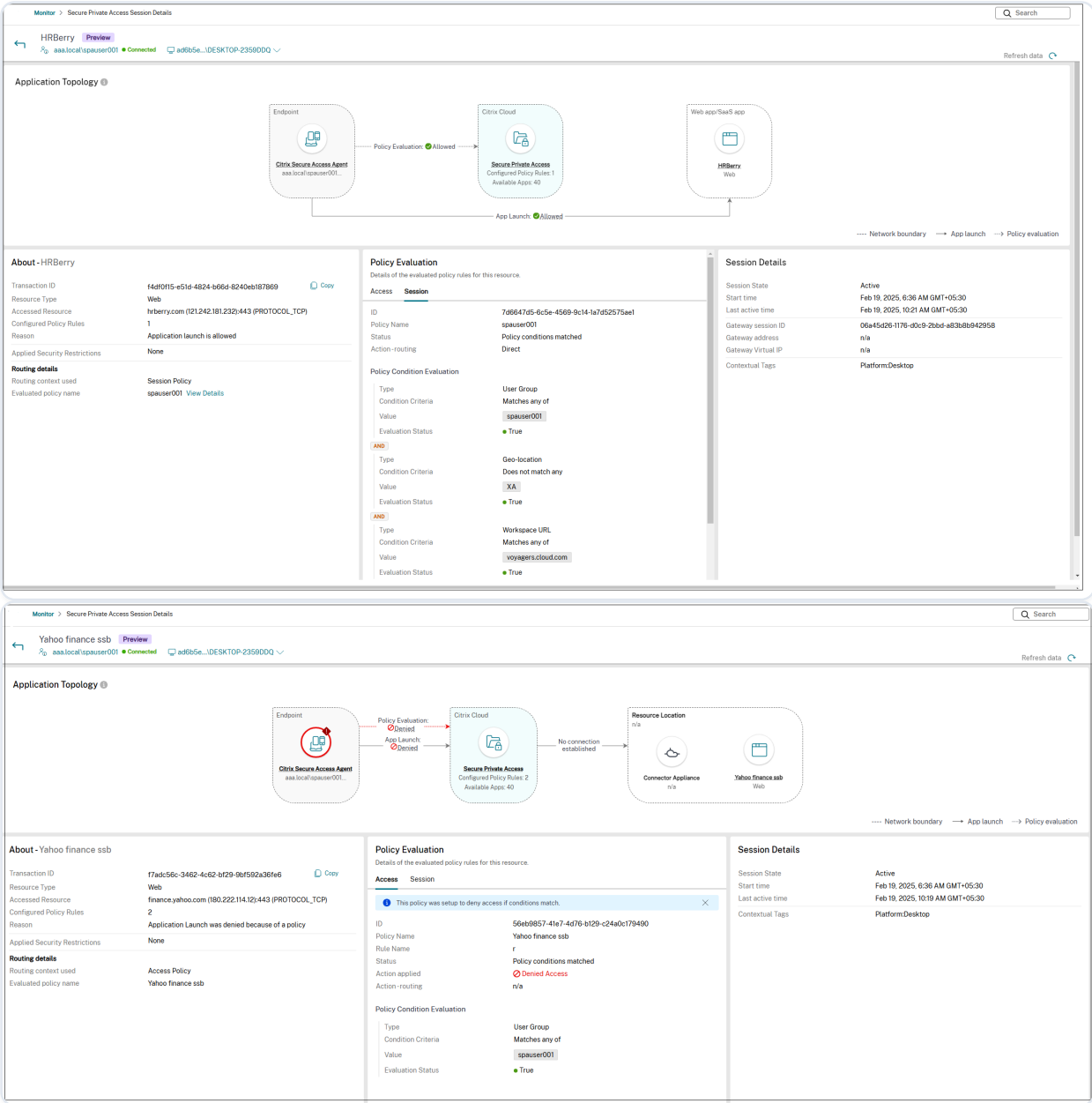
Add/edit restrictions

0 selected
☐ View selected only

	Access Settings	Current Value
> ☐	Clipboard	Enabled
> ☐	Copy	Enabled
> ☐	Download restriction by file type	Multiple options
> ☐	Downloads	Enabled
> ☐	Insecure content	Disabled
> ☐	Keylogging protection	Enabled
> ☐	Microphone	Prompt every time
> ☐	Notifications	Prompt every time
> ☐	Paste	Enabled
> ☐	Personal data masking	Multiple options
> ☐	Popups	Always block pop-ups
> ☐	Printer management	Multiple options
> ☐	Printing	Enabled
> ☐	Screen capture	Enabled
> ☐	Upload restriction by file type	Multiple options
> ☐	Uploads	Enabled
> ☒	Watermark	Disabled
> ☐	Webcam	Prompt every time

• 安全专用访问与 DaaS Monitor 集成：

安全专用访问与 Monitor（Citrix DaaS 的监视和故障排除控制台）集成。管理员和技术支持人员可以从 DaaS Monitor 监视和故障排除 Web/SaaS 和 TCP/UDP 应用程序会话和事件。有关详细信息，请参阅[安全专用访问与 DaaS Monitor 集成](#)。



• 应用程序发现：

应用程序发现功能可帮助管理员了解组织中正在访问的外部和内部应用程序（HTTP/HTTPS 和 TCP/UDP 应用程序）。此功能可发现并列列出所有已发布或未发布的域/IP 地址。因此，管理员可以查看哪些域/IP 地址正在被谁访问，并决定是否要将其发布为应用程序，从而为这些用户提供访问权限。有关详细信息，请参阅[发现最终用户访问的域或 IP 地址](#)。

App configurationApp discoverySecurity groups

All protocol

Last 1 Week

+ Add filter

App discovery shows list of domains visited by end-users. Select one or more domains to add them to a new or existing application.

2 Selected

☐ View selected only

Create application

Add to an existing application

	Domain/IP	Port	Protocol	Total Visits	Unique Users	Most Recent Visit	Assigned To App(S)
☐	meesho.com	443	HTTPS	3	1	2024-08-14 12:22:32	1
☐	www.google.com	443	HTTPS	2	1	2024-08-14 12:16:21	0
☐	www.googleadservices.com	443	HTTPS	2	1	2024-08-14 12:16:21	0
☐	www.bbc.com	443	HTTPS	1	1	2024-08-14 11:59:01	0
☐	myntna.in	443	HTTPS	1	1	2024-08-14 12:00:54	1
☐	www.apple.com	443	HTTPS	1	1	2024-08-14 12:00:54	0
☒	wikipedia.org	443	HTTPS	1	1	2024-08-14 12:16:21	0
☒	www.amazon.in	443	HTTPS	1	1	2024-08-14 12:16:21	0
☐	www.ajio.com	443	HTTPS	1	1	2024-08-14 12:22:32	0
☐	javatpoint.com	443	HTTPS	1	1	2024-08-14 12:22:32	0
☐	udemy.com	443	HTTPS	1	1	2024-08-14 12:22:32	0
☐	www.reddit.com	443	HTTPS	1	1	2024-08-14 12:22:32	0

策略建模工具：

策略建模工具**（访问策略 > 策略建模）**为管理员提供了对预期应用程序访问结果（允许/受限 允许/拒绝）的全面可见性。管理员可以检查特定用户的访问结果，并为上下文标签添加用户条件。有关详细信息，请参阅[策略建模工具](#)。

Policy configurationPolicy modeling

Model user access outcomes, given various contexts and conditions.

Device type

Desktop

Domain

spablr1.com

User name

spa user01

+ Simulate conditions

Contextual tags = term

Contextual tags

= (equals)

term

Apply

Cancel

Clear filters

Display name: spa user01
Domain name: spablr1.com

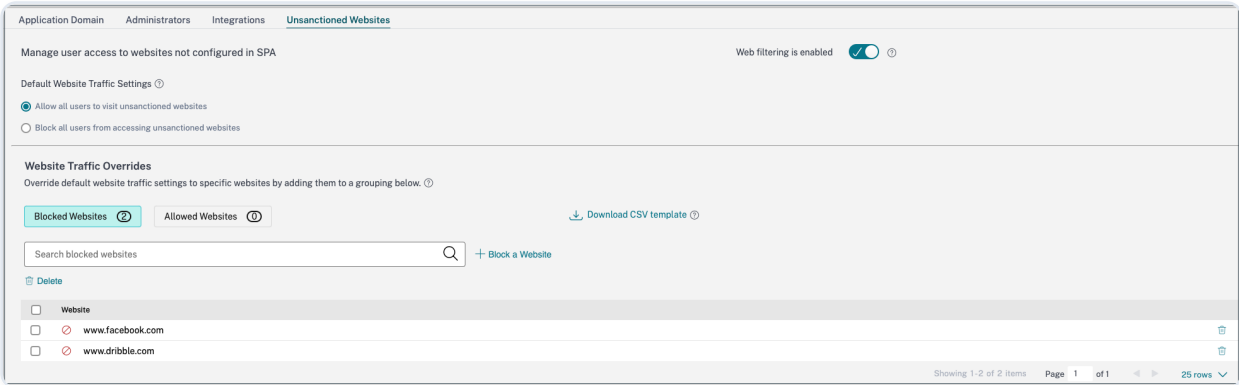
Application access

Application Name	Result	Policy Name
avanthika	✔ Access will be allowed	avanthika_pol
buddi_nani	❗ No access policy found	N/A

Showing 1-2 of 2 itemsPage 1 of 125 rows

支持未经批准的网站：

未在安全专用访问中配置的应用程序（内网或互联网）被视为“未经批准的网站”。默认情况下，如果没有为这些应用程序配置应用程序和访问策略，安全专用访问会拒绝访问所有内网 Web 应用程序。对于所有其他未配置应用程序的互联网 URL 或 SaaS 应用程序，管理员可以使用管理控制台中的[设置 > 未经批准的网站](#)选项卡，通过 Citrix Enterprise Browser 允许或拒绝访问。有关详细信息，请参阅[未经批准的网站](#)。



已知问题

2511 版本中，Secure Private Access 混合部署存在以下已知问题。

- 从 Citrix Workspace 应用程序或基于 Web 的用户界面启动应用程序时，会提示代理登录。

解决方法：取消提示以继续启动应用程序。

- 在没有 Chrome 配置文件的情况下，首次从 Citrix Workspace 应用程序或基于 Web 的用户界面启动应用程序时，在添加配置文件后，应用程序不会在 Chrome 浏览器中打开。
- 如果 NetScaler 在 Google Cloud Identity 的第三方 SSO 下作为 OIDC 的 IdP 添加，则用户在显式注销或因会话超时而注销后，无法登录 Chrome 配置文件。

解决方法：必须删除并重新添加托管配置文件。

- 在 Secure Private Access 混合 CEP 部署中，当启用 SSL 默认配置文件或密码组时，CEP 代理和 Secure Private Access 代理之间的 mTLS 握手失败。
- 网络位置服务条件（添加或删除位置标签）上的策略更改在更新时失败。
- 配置 Citrix Enterprise Premium 时，如果 Google 客户发生更改，则会显示不正确的验证和不明确的错误消息。
- 策略建模工具不显示来自已禁用策略的应用程序。
- Secure Private Access 仪表板中的应用程序启动计数图表不显示 SaaS 应用程序的启动计数。
- Secure Private Access 仪表板中的应用程序启动计数图表不显示给定时间段内所有已启动的应用程序。
- 从适用于 Linux 的 Citrix Receiver 启动 Web 应用程序时，会显示 AM_ERROR_UNEXPECTED 提示。
- 您无法从访问策略用户界面（**Secure Private Access > 访问策略**）添加基于计算机的策略条件。

- nFactor 身份验证流程不支持带有 SAML 的设备状态。
- 在 NetScaler 上配置 OAuth IdP 配置文件时，客户端密钥字段中不允许使用特殊字符（#、@、!、\、&、%）。
- 如果 NetScaler Gateway 中配置了客户端证书身份验证，适用于 Linux 的 Citrix Secure Access 客户端将无法工作。
- 如果应用程序的 FQDN 以“.local”结尾，适用于 Linux 的 Citrix Secure Access 客户端无法隧道化应用程序。
- 首次启动应用程序时，在托管配置文件中会间歇性地显示错误消息“服务不可用...”。
- 如果配置了数据丢失防护 (DLP)，Citrix Secure Access 客户端将允许应用程序访问。

系统要求和先决条件

以下部分提供了有关系统要求和先决条件的更多信息。

软件版本要求

Secure Private Access 混合配置需要以下软件版本：

- **NetScaler**：14.1–66.54 及更高版本
- **StoreFront**：2507 LTSR CU1 或 2511 CR 及更高版本
- **Cloud Connector**：6.141.0 / 4.420.200 及更高版本

最终用户设备上需要以下最低软件版本：

- **对于 Web/SaaS 应用程序：**
 - 谷歌浏览器：142
 - 适用于 Windows 的 Citrix Workspace 应用程序：2507.1 LTSR 或 2508
 - 适用于 Mac 的 Citrix Workspace 应用程序：2508.10
- **对于 TCP/UDP 应用程序：**
 - 适用于 Windows 的 思杰安全访问：25.5.1.15
 - 适用于 Mac 的 Citrix Secure Access：25.11.1.1
- **对于端点分析 (EPA)：**
 - 适用于 Windows 的 EPA 客户端: 25.10.1.7
 - 适用于 Mac 的 EPA 客户端: 25.10.3

防火墙要求

以下防火墙要求假定标准 HTTPS 端口 443 用于 StoreFront 服务器和 StoreFront 负载均衡器。如果使用非标准端口，请相应地调整端口设置。

源	源 IP	目标	协议	端口	描述
互联网	任意	NetScaler 网关	TCP	443	-
StoreFront 服务器	StoreFront 服务器计算 机 IP 地址	Secure Private Access 负载 均衡器	TCP	443	-
云连接器	云连接器计 算机 IP 地址	活动目录	TCP	389 或 636	-

如果同一 NetScaler 包含 StoreFront 和 Secure Private Access 配置的网关和负载均衡器：

源	源 IP	目标	协议	端口	描述
NetScaler	NetScaler 子网 IP (SNIP) 地址	StoreFront 服务器	TCP	443	-
NetScaler	NetScaler 子网 IP (SNIP) 地址	云连接器	TCP	8443	假设 Secure Private Access 使用 默认端口
NetScaler	NetScaler 子网 IP (SNIP) 地址	NetScaler 出站代理	TCP	取决于出站 代理端口	-
NetScaler	NetScaler 子网 IP (SNIP) 地址	后端应用程 序 (Web 应 用程序或客 户端/服务器 应用程序)	取决于后端 应用程序协 议	取决于后端 应用程序端 口	-

如果网关和 StoreFront 及 Secure Private Access 配置的负载均衡器使用不同的 NetScaler：

源	源 IP	目标	协议	端口	描述
NetScaler 网关	NetScaler 子网 IP (SNIP) 地址	StoreFront 负载均衡器	TCP	443	-
StoreFront 负载均衡器	StoreFront 负载均衡器 IP 地址	StoreFront 服务器	TCP	443	-
NetScaler 网关	NetScaler 子网 IP (SNIP) 地址	Secure Private Access 负载 均衡器	TCP	443	-
Secure Private Access 负载 均衡器	Secure Private Access 负载 均衡器 IP	云连接器	TCP	8443	假设 Secure Private Access 使用 默认端口
NetScaler 网关	NetScaler 子网 IP (SNIP) 地址	NetScaler 出站代理	TCP	取决于出站 代理端口	-
NetScaler 网关	NetScaler 子网 IP (SNIP) 地址	后端应用程 序 (Web 应 用程序或客 户端/服务器 应用程序)	取决于后端 应用程序协 议	取决于后端 应用程序端 口	-

先决条件

为确保 Citrix Workspace™ 应用程序与 Chrome Enterprise Premium 之间的最佳集成，必须满足以下先决条件。成功完成这些先决条件将使您在从 Citrix Workspace 应用程序或基于 Web 的用户界面启动应用程序时获得更高效、更无缝的体验。

NetScaler 先决条件

以下各节提供了有关 NetScaler 先决条件的更多信息。

Chrome 企业高级版 + Citrix 安全访问部署

- 确保存在具有 Citrix 桌面即服务 (DaaS) 所需设置的 NetScaler Gateway。此 NetScaler Gateway 用于在 Citrix Workspace 应用程序/Citrix Receiver for Web 中枚举 Secure Private Access 应用程序和 DaaS 应用程序。
 - 要使用向导创建网关，请参阅 [为 Citrix Virtual Apps and Desktops 设置 NetScaler](#)。
 - 要设置 NetScaler Gateway，请参阅 [如何配置 NetScaler](#)。
- 确保为新的完全限定域名 (FQDN) 存在一个新的公共 IP 地址和相应的私有 IP 地址。公共 IP 必须 NAT 到私有 IP。此信息用于为 Secure Private Access 应用程序配置新的 NetScaler Gateway。此网关 FQDN 用于使用托管 Chrome 配置文件访问私有 Web 应用程序。最终用户还可以使用 Citrix Secure Access 客户端的此 FQDN 连接到网关以访问内部应用程序。此私有 IP 地址必须用于 UI 中的“**内部 IP 地址**”字段。有关详细信息，请参阅 [Secure Private Access 混合部署入门](#)。
- 确保您拥有 NetScaler Gateway 的 SSL 服务器证书。证书必须包含必要的完全限定域名 (FQDN)，包括新的 Secure Private Access NetScaler Gateway 的 FQDN。有关相关配置详细信息，请参阅 [NetScaler 配置](#)。
- 确保 NetScaler 上配置了身份验证配置文件。您也可以使用现有的身份验证配置文件和相应的身份验证虚拟服务器。有关详细信息，请参阅 [配置身份验证](#)。

注意：

有关将 NetScaler Gateway 用作 Google OIDC 的 IdP，请参阅 [使用 NetScaler Gateway 作为 IdP 的 Open ID Connect 配置文件](#)。

仅限 Citrix Secure Access 部署

- 必须为新的完全限定域名 (FQDN) 存在一个新的公共 IP 地址和相应的私有 IP 地址。公共 IP 必须 NAT 到私有 IP 地址。此信息用于为 Secure Private Access 应用程序配置新的 NetScaler Gateway。此网关 FQDN 用于使用托管 Chrome 配置文件访问私有 Web 应用程序。最终用户还可以使用 Citrix Secure Access 客户端的此 FQDN 连接到网关以访问内部应用程序。此私有 IP 地址必须用于 UI 中的“**内部 IP 地址**”字段。有关详细信息，请参阅 [Secure Private Access 混合部署入门](#)。
- 您必须拥有适用于 NetScaler Gateway 的 SSL 服务器证书。该证书必须包含必要的完全限定域名 (FQDN)，包括用于新的 Secure Private Access NetScaler Gateway 的 FQDN。有关相关配置详细信息，请参阅 [NetScaler 配置](#)。
- 确保在 NetScaler 上配置了身份验证配置文件。

也可以使用现有的身份验证配置文件和相应的身份验证虚拟服务器。

要创建新的身份验证配置文件，请参阅 [配置身份验证](#)。

Cloud Connector 先决条件

- 确保在 Cloud Connector 上启用了 Secure Private Access 服务。如果您需要帮助，请联系 Citrix 支持。
- 确保允许 Cloud Connector 通过端口 443 对 [Connector Common](#) 和 [Secure Private Access FQDN](#) 进行出站调用。有关更多详细信息，请参阅 [Cloud Connector 的系统 and 连接要求](#)。

有关详细信息，请参阅 [Cloud Connector 配置](#)。

StoreFront 先决条件

- 确保在 StoreFront 上创建了一个启用了远程访问（已配置 NetScaler Gateway）的 Store。请参阅 [StoreFront 文档](#)。
- 将 Secure Private Access 添加为 StoreFront 应用商店中的站点：
 - 打开您的应用商店并选择 **管理站点**。
 - 单击 **添加站点**，选择 **Secure Private Access** 作为类型，然后输入显示名称和 Secure Private Access 负载均衡器 FQDN。

注意：

如果您仅将 Secure Private Access 用于 TCP/UDP（客户端/服务器）应用程序，则 StoreFront 是可选的。

有关详细信息，请参阅 [StoreFront 配置](#)。

安全私有访问先决条件

- 确保 Windows Cloud Connector 入站规则允许来自数据中心网络的端口 8443。Citrix 安全私有访问在端口 8443 公开一个纯 HTTP 服务。
- 确保用于 Citrix 安全私有访问的内部负载均衡器将 Cloud Connector 后端作为目标，端口为 8443。
- 确保在用于 Citrix 安全私有访问的内部负载均衡器上配置了 SSL 桥接或 SSL 卸载。

有关详细信息，请参阅 [Secure Private Access service](#)。

Google 先决条件

以下各节提供有关 Google 先决条件的更多信息。

Chrome 企业高级版许可证

确保您拥有有效的 Chrome Enterprise Premium 许可证，该许可证可通过 Citrix Cloud Platform License (CPL) 计划获得。

Google Workspace 管理控制台

- **Google 客户 ID**：从 Google 管理控制台获取您的 Google 客户 ID。此 ID 是配置 Google 服务和集成所必需的。您的客户 ID 可以通过 Google 管理控制台中的 **帐户 > 帐户设置** 进行检索。
- **在 Google 管理控制台中创建自定义角色**：要将客户加入 Chrome Enterprise Premium (CEP) 并启用 Google Chrome 集成，管理员必须在 Google 管理控制台中创建自定义角色并分配相应的权限。有关详细信息，请参阅 [Admin roles and privileges](#)。
- **代理模式配置**：将代理模式设置为“允许用户配置代理”。避免使用限制性选项，例如“无代理”、“操作系统代理”或“仅使用此代理”。

注意：

如果 Google 管理控制台设置为使用系统代理设置，则托管配置文件无法应用 Citrix 安全私有访问所需的代理配置，并且与 Chrome Enterprise Premium 的集成将失败。

- **限制 DevTools 扩展**：必须禁用强制安装扩展的 Chrome DevTools，以防止敏感数据泄露。这是 Google 管理控制台中的默认选项。
- **现在在 Google Admin console for Chrome Enterprise Premium 中配置访问限制**：以前在 Secure Private Access 控制台中配置的访问限制仅适用于 Citrix Enterprise Browser。当 Google Chrome 是企业浏览器时，必须在 Google Admin console 中将访问限制配置为策略和规则。
 - 策略在 **Google Admin console > Devices > Chrome > Settings** 中配置。这些设置允许您管理浏览器设置，例如阻止 JavaScript 和允许打印机列表。
 - 规则在 **Google Admin console > Rules** 中配置。这些规则是与 DLP 相关的高级设置，例如添加水印、阻止下载包含社会安全号码的文件以及 URL 过滤。

有关在 Google Workspace Admin console 中创建策略和规则的详细信息，请参阅以下主题：

- [为 Chrome Enterprise 设置 Chrome Enterprise 连接器策略](#)
- [数据保护规则](#)

- **许可证：** 确保您拥有有效的 Chrome Enterprise Premium 许可证，该许可证可通过 Citrix Cloud Platform License (CPL) 计划获得。

谷歌浏览器

以下部分提供了有关 Google Chrome 先决条件的更多信息。

托管的 Chrome 配置文件

所有最终用户都必须使用托管配置文件访问 Chrome。托管配置文件可确保在用户设备上强制执行 Chrome 策略、扩展和安全设置。

将 Citrix Workspace 中配置的用户目录与 Google Cloud 用户目录同步

您必须将 Citrix Workspace 或 StoreFront 中配置的用户目录与 Google Cloud 用户目录同步。具体来说，支持以下用户目录：

- 活动目录
- Microsoft Entra 标识（以前称为 Azure 活动目录）

注意：

定期同步用户目录，以确保正确强制执行应用程序访问。

填充电子邮件地址字段（强制）

Google Cloud 用户目录要求填充电子邮件地址字段。要与 Google Cloud 用户目录同步，Secure Private Access 中的用户或组对象必须具有电子邮件地址。否则，同步将失败。

确保所有需要访问集成的 Chrome Enterprise Premium 和 Secure Private Access 产品的用户，以及所有涉及访问安全策略的组，都已填充电子邮件地址字段。电子邮件地址的域部分必须是已在您的 Google 管理控制台中配置和验证的域。

活动目录同步

您必须使用 Google Cloud Directory Sync 将您的 AD 与 Google Cloud 用户目录同步，以确保在整个企业中实现无缝集成和一致的用户管理。

有关如何将 AD 与 Google Cloud 同步以在自定义架构“Citrix-schema”下包含自定义 AD 字段的详细信息，请参阅 [将 Google Cloud Identity 作为身份提供程序连接到 Citrix Cloud](#)。

微软 Entra ID

您必须将 Microsoft Entra ID 与 Google Cloud 用户目录同步，以实现 Google 和 Microsoft 云平台之间的用户和组管理。有关详细信息，请参阅 [目录同步入门](#)。

有关更多信息，请参阅 [Google 目录同步](#)。

绕过 TLS 检查

为确保 Chrome Enterprise Premium 端点在采用 TLS 检查（或 SSL 检查）的网络上正常运行，您必须将以下主机名从检查中排除。

- `ingress.cloudproxy.app`
- `securegateway.goog`
- `*.securegateway.goog`

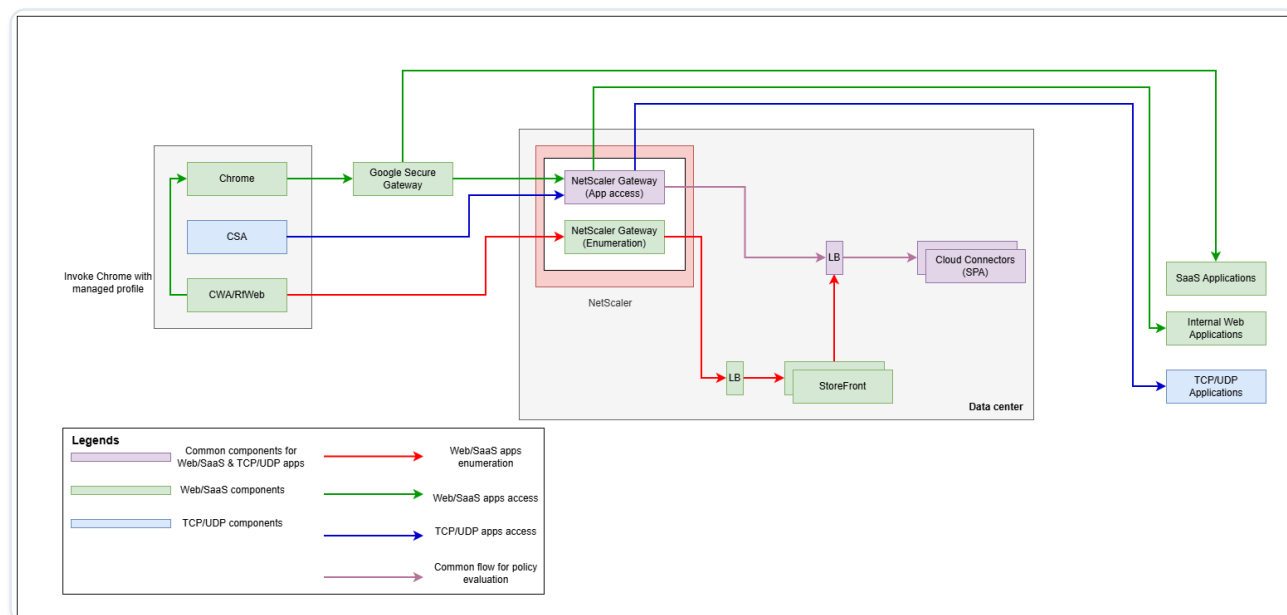
这种排除至关重要，因为许多 TLS 检查解决方案（例如 SSE 供应商或代理服务器）不完全支持 Chrome Enterprise Premium 使用的 HTTP CONNECT 方法，这可能导致流量突然中断。

此外，建议将以下主机名从 TLS 检查中排除，以避免潜在的最终用户性能问题和连接延迟。

- `safebrowsingrealtime.googleapis.com`
- `secureconnect-pa.clients6.google.com`
- `secureconnect-pa.mtls.clients6.google.com`
- `secureconnect-pa.googleapis.com`
- `chromereporting-pa.googleapis.com`

Secure Private Access 混合部署入门

本主题提供了设置 Secure Private Access 混合环境的分步说明。



开始之前

以下部分提供了有关在开始 Secure Private Access 混合部署之前必须执行的检查的详细信息。

验证您的 Secure Private Access 授权

您的 Citrix Cloud 帐户必须拥有 Secure Private Access 服务的授权。

- 登录到 Citrix Cloud 控制台。
- 在控制板上，验证 **Secure Private Access** 服务磁贴是否可见且可用。
- 如果服务不可见，则无法继续。请联系您的 Citrix 代表以解决授权问题。

验证必备条件

确保满足所有必备条件。有关详细信息，请参阅[必备条件](#)。

验证是否满足所有网络必备条件。有关所有必需端口和通信路径的完整详细信息，请参阅[网络图](#)。

选择部署模式

在欢迎屏幕上，选择 **设置为混合** 以开始配置。

后续步骤

- 步骤 1: 设置谷歌浏览器企业高级版
- 步骤 2: 设置第一个数据中心
- 步骤 3: 配置和分析

步骤 1：设置 Google Chrome 企业高级版

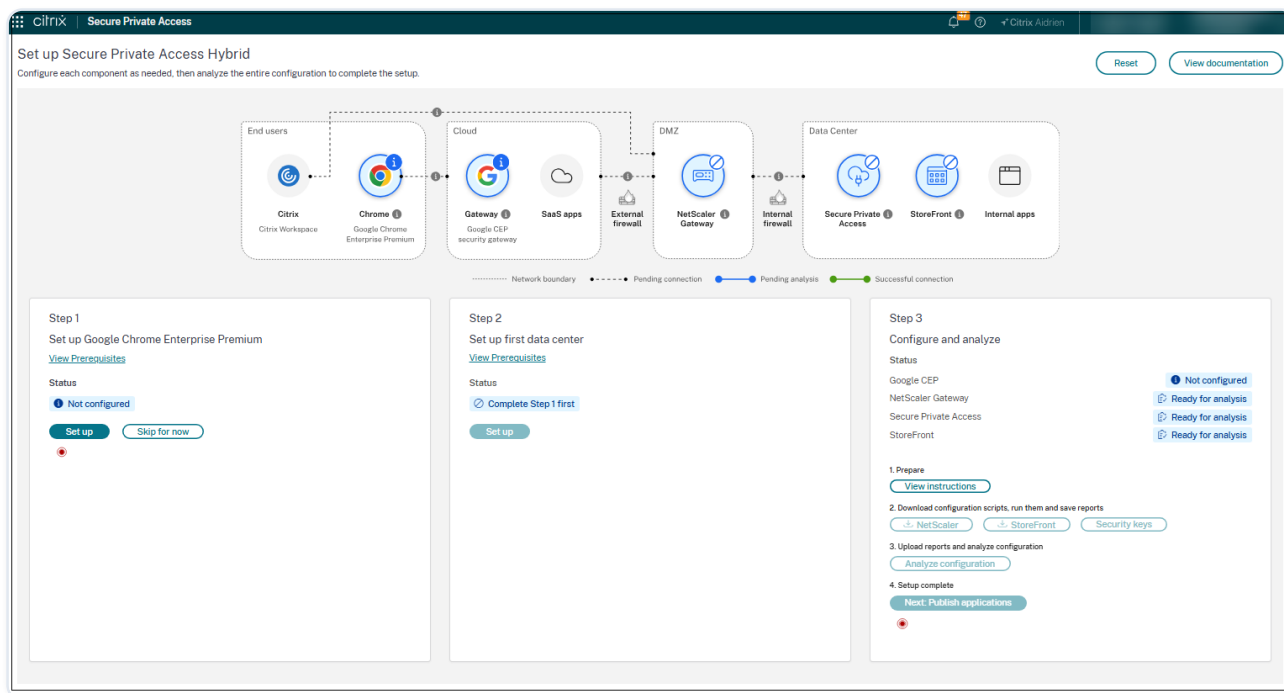
在此步骤中，系统会提示您配置 Google Chrome Enterprise Premium。

注意：

在设置 Google Chrome Enterprise Premium 之前，请考虑以下几点：

- 如果您仅将 Secure Private Access 用于 TCP/UDP（客户端/服务器）应用程序，请单击 **暂时跳过**。否则，请单击 **设置** 以开始配置 Web 或 SaaS 应用程序。
- 如果您单击 **暂时跳过**，则以后无法在不完全重置的情况下启用 Chrome Enterprise Premium。
- 如果您选择 **设置** Chrome Enterprise Premium，则表示您正在启用对 Web/SaaS 应用程序的支持。此路径还允许您配置 TCP/UDP（客户端/服务器）应用程序。如果您计划将来将 Secure Private Access 用于 Web 或 SaaS 应用程序，则现在必须单击 **设置**。

跳过此步骤后，启用 Web 或 SaaS 功能的唯一方法是重置整个 Secure Private Access 配置。为此，请联系 Citrix 支持。



Google Chrome 企业高级版配置

- 按照屏幕上的说明创建 **Google 管理员角色**。
- 按照说明将为 Secure Private Access 角色创建的新角色分配给 **Citrix 服务帐户**。Citrix 使用此帐户在您的 Google Workspace 管理控制台中执行必要的集成配置。

Google Chrome Enterprise Premium

> View Prerequisites

Step 1
Assign Service Account

Service account is used to configure Google Workspace and Secure Private Access integration

1. Copy the service account address:

tenant-sa-k1cfyqmn0rvv@verdant-bruin-438923-p6.iam.gserviceaccount.com Copy

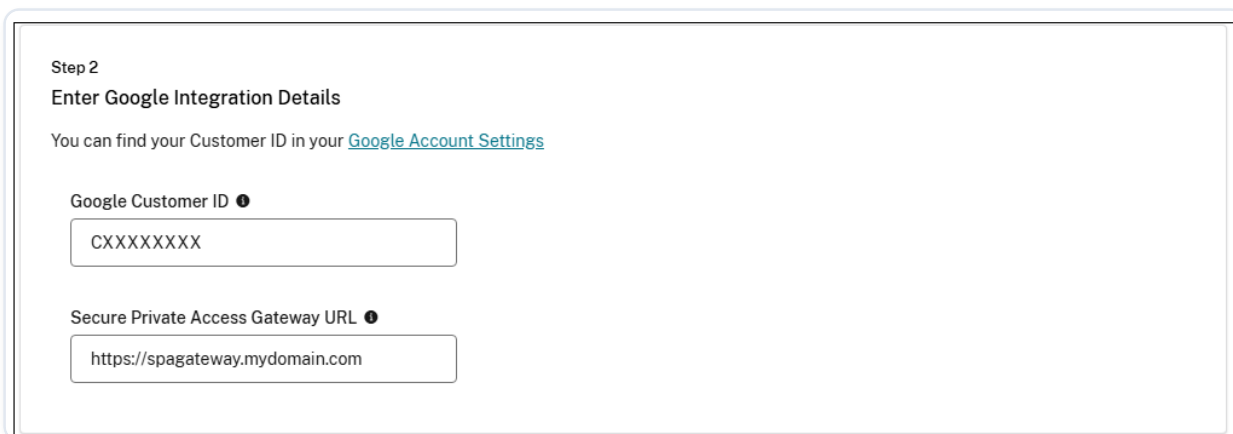
2. In the Google Workspace console, open [Account > Admin Roles](#).

3. Create new role and select the [recommended privileges](#).

4. In the new role, select **Assign service accounts** under Admins.

5. Paste the service account (tenant-sa-k1cfyqmn0rvv@verdant-bruin-438923-p6.iam.gserviceaccount.com) and click **Add**. Then click **Assign Role**.

- 按照屏幕上的说明在 Google Workspace 管理控制台中查找您的 **Google 客户 ID**。



Step 2
Enter Google Integration Details

You can find your Customer ID in your [Google Account Settings](#)

Google Customer ID ⓘ
CXXXXXXXX

Secure Private Access Gateway URL ⓘ
https://spagateway.mydomain.com

4. 复制 Google 客户 ID 并将其粘贴到 **Google 客户 ID** 输入字段中。
5. 确保您已为 NetScaler Gateway 预留了公共 IP 地址和 DNS 记录。

在 **Secure Private Access Gateway URL** 字段中输入此公共 URL。此 URL 将是您在 (/zh-cn/citrix-secure-private-access/hybrid/spa-hybrid-setup-netscaler-gateway.html) 中配置的 NetScaler Gateway 的公共地址。如果您正在配置多数据中心、多站点设置，这将是全局服务器负载平衡 (GSLB) 域 URL 的公共地址。

保存此设置会自动将 **Google Secure Gateway** 配置为使用此地址，从而使其能够连接到您的 NetScaler Gateway 以进行内部应用程序访问。

6. 选择必须授予访问权限的用户组。只有这些组的成员才能访问在 Secure Private Access 中配置的应用程序。

注意：

- 您选择的用户组必须已存在于 Google Workspace 中。
- 可选地，除了用户组之外或代替用户组，将配置应用于选定的 Google Directory 组织单位。有关更多信息，请参阅 (/zh-cn/citrix-secure-private-access/hybrid/spa-hybrid-postonboarding-tasks.html#update-the-chrome-enterprise-premium-configuration)。

7. 单击 **验证** 以确保所有配置都正确，并且 Secure Private Access 已准备好进行 Chrome Enterprise Premium 集成。
8. 单击 **保存**。

步骤 2：设置第一个数据中心

在此步骤中，系统会提示您输入在 NetScaler 上配置 Secure Private Access 所需的详细信息。

注意：

确保 NetScaler 满足所有先决条件。

NetScaler Gateway ✕

> View Prerequisites

NetScaler Gateway Virtual Server Name ⓘ

Secure Private Access site URL ⓘ

Secure Private Access Gateway URL ⓘ

Internal IP address ⓘ

Certificate-key pair name ⓘ

- **NetScaler Gateway 虚拟服务器名称：** 输入已与您的 StoreFront 部署配置的 NetScaler Gateway 虚拟服务器的名称。此虚拟服务器用于枚举 Citrix Store 中配置的 Secure Private Access 应用程序。

注意：

如果您跳过了 [Chrome Enterprise Premium 配置](#)，则不需要此输入。

- **Secure Private Access 站点 URL：** 输入将流量定向到在您的 Cloud Connectors 上运行的 Secure Private Access 服务的负载均衡器 URL。

此负载均衡器必须配置为使用 **HTTPS on port 443**。如果您尚未创建此负载均衡器，请参阅 [Secure Private Access 负载均衡器](#) 以获取说明，然后再继续。

- **Secure Private Access Gateway URL：** 此 URL 是与用户共享的 NetScaler Gateway 的公共地址。它用于连接内部应用程序。

如果您正在配置多数据中心、多站点部署，这将是全局服务器负载均衡 (GSLB) 域 URL 的公共地址。如果 URL 之前在 [步骤 1：设置 Google Chrome Enterprise Premium](#) 期间输入过，它将预填充。

- **内部 IP 地址：** 输入用于您的 Secure Private Access 网关的 **私有 IPv4 地址**。此 IP 地址在 [步骤 3 - 配置和分析](#) 中的配置期间分配给 NetScaler Gateway 虚拟服务器。
- **证书-密钥对名称：** 输入已在您的 NetScaler 上配置的 **SSL 证书-密钥对** 的名称。
- 单击 **保存**。保存后，将显示一个 **共享密钥**。您需要此共享密钥值才能在 [步骤 3 - 配置和分析](#) 中进行配置。

步骤 3：配置和分析

现在可以将配置应用于本地 StoreFront 和 NetScaler 组件。

在继续之前，请确保满足 StoreFront 和 NetScaler 的所有先决条件。

下载并运行 NetScaler 和 StoreFront 脚本

以下部分提供了有关 NetScaler 和 StoreFront 脚本的更多信息。

NetScaler 脚本

注意：

NetScaler 上的所有 Secure Private Access 配置都必须使用 **命令行界面 (CLI)** 执行。

1. 单击 **NetScaler** 下载安装脚本。此脚本是一个诊断工具，旨在为 Secure Private Access 部署配置和分析您的 NetScaler Gateway，并收集所需信息。有关更多信息，请参阅 [NetScaler Gateway Analyzer](#)。

脚本文件名具有以下格式：

```
gateway_analyzer_<customer-id>_<datacenter-name>_<timestamp>.tar.gz
```

Download NetScaler script for data centers



Caution: Running this script on any other datacenter may cause errors. Back up the configuration before running.

Select Datacenter

Blue



Download NetScaler script

Close

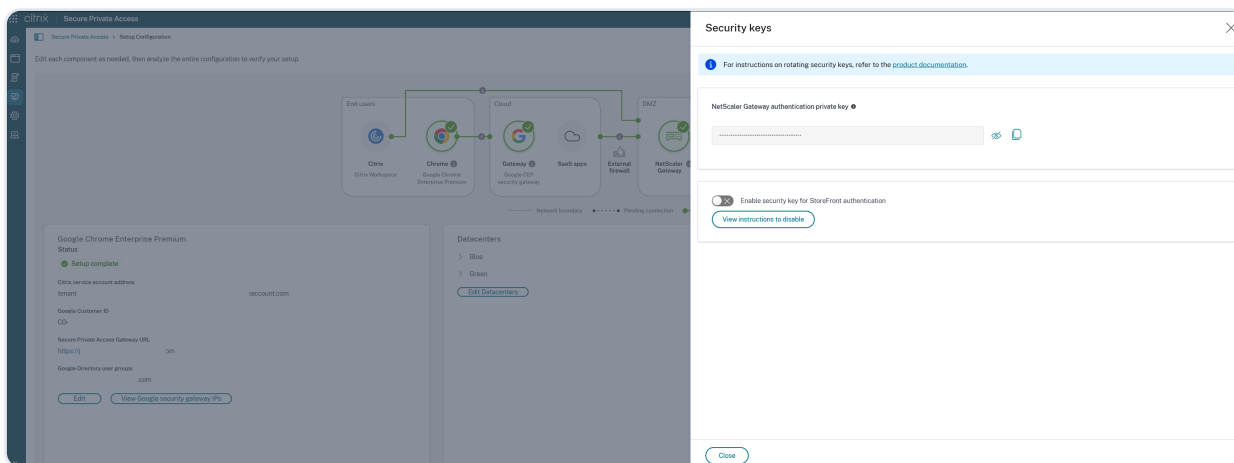
2. 使用 **SCP 客户端**（例如 `scp` 或 WinSCP）将下载的 `*.tar.gz` 文件复制到您的 **NetScaler**。
 - o.
3. 将文件放置在 `/var/tmp/` 目录中。
4. 使用 **SSH**（例如使用 PuTTY）登录到 NetScaler 的命令行界面 (CLI)，并使用管理 (`nsroot`) 权限。
5. 在 CLI 提示符下键入“shell”以访问 NetScaler shell。导航到临时目录：`cd /var/tmp/`
6. 解压存档。

注意：

您的文件名是您下载的特定文件。

```
tar -xzf gateway_analyzer_<customer-id>_<datacenter-name>_<timestamp>.tar.gz
```

7. `tar` 命令会创建一个目录。使用 `ls` 查看新文件夹的名称，然后导航到该文件夹。
8. 使用 python3 运行分析器脚本：`python3 analyzer.py`
9. 当脚本提示输入 NetScaler Gateway 身份验证私钥时：
 - a. 返回浏览器中的 Secure Private Access 设置页面，然后单击“配置和分析”卡上的“安全密钥”。



- a. 复制 NetScaler Gateway 身份验证私钥。
- b. 将密钥粘贴到 NetScaler CLI 中，然后按 **Enter**。

注意：

NetScaler Gateway 上需要此密钥才能完成 Secure Private Access 配置。

10. 脚本成功运行后，会在当前文件夹中生成一份分析报告。
11. 下载并使用 scp/winscp 保存此报告。稍后分析器需要它。

StoreFront 脚本

注意：

此步骤对于仅限 CSA 模式是可选的，即如果在[步骤 1 - 设置 Google Chrome Enterprise Premium](#)中跳过 CEP 配置。

1. 单击 **StoreFront** 下载 PowerShell 脚本。
2. 此脚本是一个诊断工具，旨在：
 - a. 分析您的本地 StoreFront 配置。
 - b. 收集部署所需的信息。

警告：

需要管理员和执行策略： 您必须以管理员权限运行此 PowerShell 脚本（例如，右键单击并选择“以管理员身份运行”）。

此外，您可能需要调整 PowerShell 执行策略以允许脚本运行。如有必要，您可以从提升的 PowerShell 提示符下运行 `Set-ExecutionPolicy Bypass`（或适用于您组织的相应策略）来执行此操作。

脚本文件名的格式如下：

```
storefront_analyzer_<tenant-id>_<timestamp>.zip.
```

3. 将下载的 .zip 文件复制到您的 **StoreFront 服务器**。
4. 在 StoreFront 服务器上，**提取** .zip 文件的内容（例如，到 C:\temp\spa-sf-script\）等文件夹）。
5. 以**管理员权限**打开 **PowerShell** 窗口（右键单击，“以管理员身份运行”）。
6. 在 PowerShell 窗口中，导航（使用 cd）到您解压脚本的目录。
7. 通过运行以下命令执行脚本：

```
.\CollectAnalyzerStorefrontInfo.ps1
```

脚本成功运行后，会生成一份分析报告。下载并保存它以备下一步使用。

上传报告并分析配置

您现在可以上传本地脚本生成的报告来验证您的配置。

1. 单击**分析**。
2. 系统会提示您上传分析报告。上传您生成的两个文件：
 - **NetScaler** 分析报告。
 - **StoreFront** 分析报告。
3. 两个文件都成功上传后，单击**分析**。
4. 等待分析完成。系统会显示所有检查的**成功/失败**结果。
5. **查看分析结果**：
 - a. **如果所有分析器步骤都已通过**：您已成功验证您的配置，可以继续下一步。

Analyze configuration

> Prepare for analysis

Secure Private Access

Setup complete

Test	Status
spa.check.cloud.access	Success
spa.check.db.access	Success
spa.check.tag.service.access	Success
spa.check.cas.access	Success

Showing 1-4 of 4 items Page 1 of 1 5 rows

NetScaler Gateway

Setup complete

Upload report to analyzer

Drag and drop report here or [Browse](#)

Test	Status
SPA vServer Configuration Check	Success
SPA Profile High Cipher Check	Success
SPA vServer SSL Profile Set Check	Success
SPA Profile Configuration Check	Success
SPA Profile Binding Check	Success

Showing 1-5 of 25 items Page 1 of 5 5 rows

Analyze

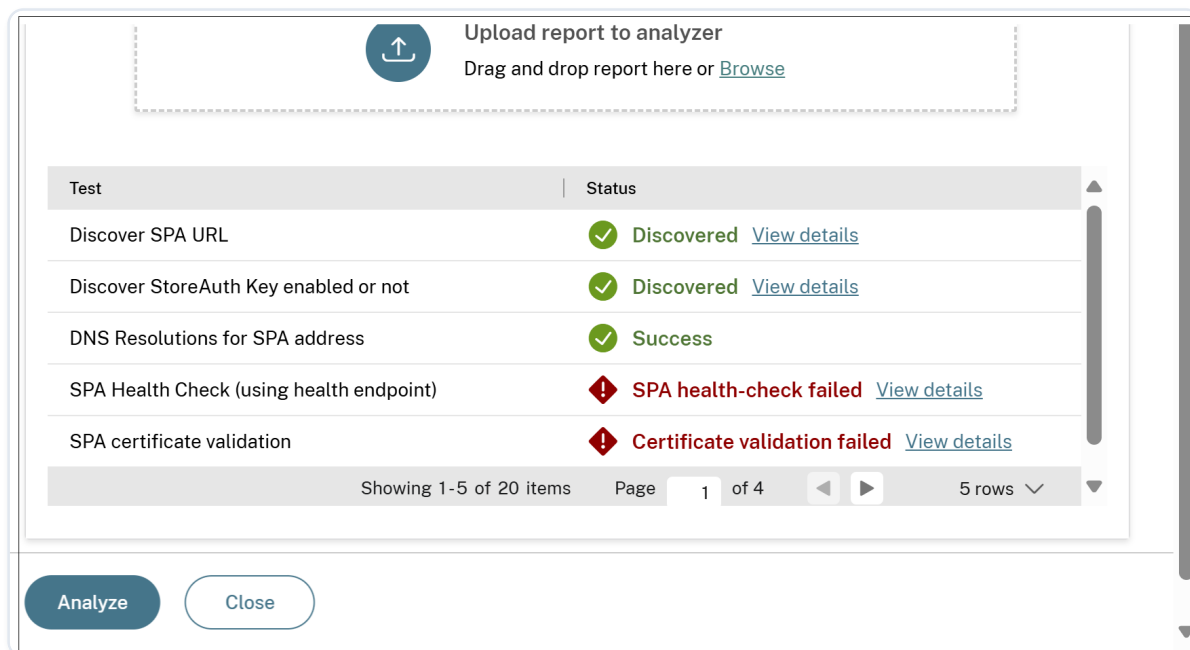
Close

b. 如果任何步骤失败：

- 报告会建议补救步骤。
- 按照建议的说明修复失败组件（NetScaler 或 StoreFront）上的错误。
- 修复问题后，在该组件上重新运行诊断脚本以生成新报告。
- 返回此步骤并重新上传新的分析报告。

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

47



完成载入并发布应用程序

单击下一步：**发布应用程序**以完成并退出设置向导。

这完成了您的初始混合载入。如果您正在配置多数据中心、多站点部署，请继续参阅[高级数据中心配置](#)。

入职后任务

以下部分提供了有关入职后任务的更多信息。

配置应用程序

您的下一个紧迫任务是发布您的第一个应用程序。建议您通过发布至少一个内部 Web 应用程序或一个 TCP/UDP 应用程序来测试您的设置。请遵循 ([/zh-cn/citrix-secure-private-access/hybrid/spa-hybrid-configure-apps.html](#)) 中的详细说明。

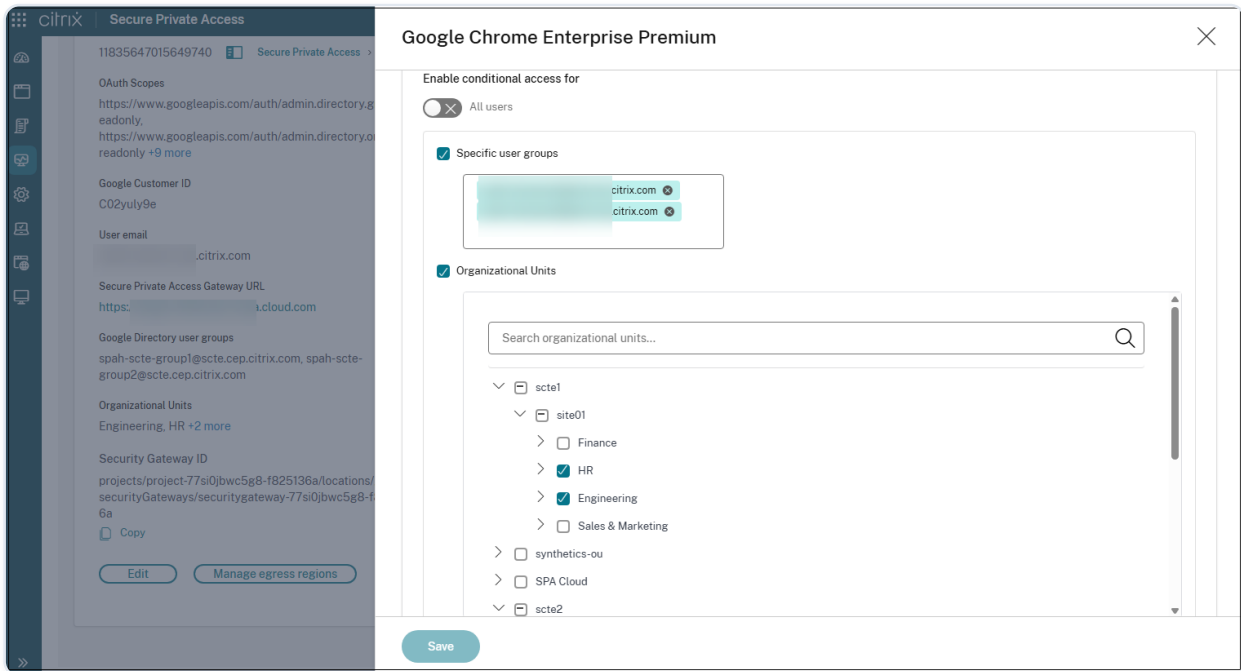
配置访问策略

- 在 Secure Private Access 管理控制台中，导航到 **策略 > 访问策略**。
- 为您的应用程序创建访问策略，确保定义 **用户条件**。
- 有关完整详细信息，请参阅 ([/zh-cn/citrix-secure-private-access/hybrid/spa-hybrid-configure-access-policies.html](#))。

更新 Chrome 企业高级版 配置

您可以在入职后更新 Chrome Enterprise Premium (CEP) 配置，以更改接收它的用户。除了所有用户和 Google Directory 用户组之外，您还可以将配置应用于选定的 Google Directory 组织单位。用户组和组织单位并非相互排斥，因此单个配置可以同时针对两者。

1. 在 Secure Private Access 控制台入职页面中，单击 Chrome Enterprise Premium 设置卡中的 **编辑**。



2. 单击 **组织单位** 以树状复选框的形式显示您的 Google Directory 层次结构，然后选择要包含的组织单位。

注意：

- 选定的组织单位是继承的。此配置适用于该组织单位及其所有子组织单位中的用户，包括以后创建的任何子组织单位。选择父级也会选择其子组织单位，这些子组织单位将显示为已选中并呈灰色。若要仅包含子集，请清除父级并选择特定的子组织单位。
- 根组织单位未在树中显示。要为所有人启用 CEP 集成，请选择“所有用户”。
- 层次结构是使用 Citrix 服务帐户从您的 Google 目录中读取的，这需要“组织单位 > 读取权限”。有关详细信息，请参阅[管理员角色和权限](#)。

3. 单击“**验证**”以验证选择，然后单击“**保存**”。

如果在成功验证后更改了选择，请在保存之前再次运行验证。

同步配置

保存更改（新应用程序或策略）后，本地 Cloud Connector 中的 Secure Private Access 组件必须从 Citrix Cloud 同步此新配置。

此过程通常需要长达 **10 分钟** 才能完成。

如何验证： 建议使用“策略建模工具”（在“策略 > 策略建模”下）检查新配置是否已应用，以查看您的新策略是否处于活动状态。

访问您的应用程序（最终用户）

本节介绍最终用户如何在其设备上访问已发布的应用程序。

支持的设备：

- **Web/SaaS 应用程序**（通过 Google Chrome 托管配置文件）可从任何桌面操作系统访问。

在 Linux、iOS 和 Android 设备上，Web/SaaS 应用程序可通过 Citrix Secure Access 客户端访问。

- **TCP/UDP 应用程序**（通过 Citrix Secure Access 客户端）支持 **Windows、macOS、Linux、iOS 和 Android**。

访问 Web 和 SaaS 应用程序

用户可以通过三种主要方式在桌面设备上访问其 Web 应用程序。所有这些方法都将自动在 Google Chrome 受管配置文件中启动应用程序。

方法 A：使用带受管配置文件的 Chrome 浏览器（推荐）

这是为用户提供的最无缝的体验。

1. 启动 **Google Chrome** 浏览器。
2. 如果这是您第一次使用，请使用在访问策略上配置的公司电子邮件地址添加新的浏览器配置文件。这将创建一个受管配置文件。
3. 在受管配置文件中，导航到您的 **NetScaler Gateway URL**（在 [步骤 2：设置第一个数据中心](#) 中配置的 URL）。
4. 登录到您的应用商店。
5. 单击 Web 或 SaaS 应用程序图标以启动它。

应用程序将在受管配置文件中的新选项卡中启动。

方法 B：使用非受管 Web 浏览器

注意：

此方法要求在桌面设备上安装受支持版本的 Citrix Workspace 应用程序。

1. 启动您偏好的任何浏览器（例如，非受管 Chrome、Edge、Firefox）。
2. 导航到您的 **NetScaler Gateway URL**（在 [步骤 2：设置第一个数据中心](#) 中为 StoreFront 配置的 URL）。
3. 登录到您的应用商店。
4. 单击 Web 或 SaaS 应用程序图标以启动它。
5. 浏览器会显示一个对话框，提示您打开 **Citrix Workspace App**。
6. 单击“继续”或“打开”。
7. Citrix Workspace 应用程序接管并在 **Google Chrome 托管配置文件中**启动应用程序。如果尚未创建配置文件，则会出现一个预填充了您电子邮件地址的设置屏幕，供您完成配置文件。

方法 C：使用 Citrix Workspace 应用程序

1. 在您的设备上启动 **Citrix Workspace App**。
2. 如果尚未配置，请使用 **NetScaler Gateway URL**（在 (/zh-cn/citrix-secure-private-access/hybrid/spa-hybrid-setup-netscaler-gateway.html) 中为 StoreFront 配置的 URL）添加您的应用商店。
3. 登录到您的应用商店。
4. 您可以看到枚举的应用程序列表。
5. 单击 Web 或 SaaS 应用程序图标以启动它。该应用程序会自动在托管的 Google Chrome 配置文件中打开。

访问 TCP/UDP（客户端/服务器）应用程序

访问 TCP/UDP 应用程序需要 Citrix Secure Access 客户端。

您必须在端点设备上安装受支持版本的 Citrix Secure Access。

连接 Secure Access 客户端

1. 启动 **Citrix Secure Access 客户端**。
2. 当系统提示输入 URL 时，请输入 **Secure Private Access 网关 URL**（在 (/zh-cn/citrix-secure-private-access/hybrid/spa-hybrid-setup-netscaler-gateway.html) 中配置的 FQDN）。

3. 完成登录和身份验证提示。
4. 客户端连接后，将在后台安全运行。

启动已发布的应用程序

如果 Secure Private Access 策略允许，您现在可以直接使用本机客户端软件。例如：

- 打开 **Microsoft 远程桌面**并连接到 RDP 服务器的内部主机名。
- 打开 **SSH 客户端**并连接到 Linux 服务器的内部 IP。

数据区域化

Citrix Secure Private Access 中的数据区域化使客户能够通过选择首选地理区域来控制其数据存储位置。客户可以选择其数据存储区域，选项包括全球、欧洲 (EU)、亚太地区 (APAC) 和北美 (NA)。所有静态配置数据都保留在所选区域内，确保其不会离开指定地理区域。

数据区域化功能提供以下优势：

- 通过将所有配置数据保留在所选区域内，确保强大的数据驻留控制。
- 帮助组织满足监管和数据主权要求。
- 通过防止数据离开指定地理区域来降低风险。
- 支持具有区域特定需求的灵活全球部署，使客户能够自信地采用与其驻留策略一致的云交付安全访问。

注意：

如果没有数据区域化，跨区域运营的组织可能面临严格的数据驻留和合规性要求，同时缺乏对其服务数据存储位置的控制。如果没有区域数据边界，配置数据可能会存储在所需地理区域之外，从而增加监管风险并限制云交付安全访问解决方案的采用。

支持的部署

此功能适用于所有 Citrix Secure Private Access 部署，包括服务模型和混合模型，对于具有区域数据驻留、合规性和监管要求的组织尤其重要。

配置

选择区域是 Secure Private Access 服务或混合部署在入职期间的一次性设置。设置后，所有数据都保留在所选区域中，对正在进行的操作或用户工作流程没有影响。

1. 登录 Citrix Cloud，然后单击 **Secure Private Access**。
2. 选择 **Setup for cloud** 或 **Hybrid**，然后单击 **Continue**。
3. 在“**选择部署区域**”中，选择必须存储数据的区域，然后单击“**继续**”。

限制

数据区域化的一些限制包括：

- 数据区域化仅适用于静态配置数据。其他数据类型（例如遥测数据或传输中数据）可能不受限于所选区域。
- 存在对其他在全球范围内运行的 Citrix Cloud 服务的依赖，这些服务可能不遵循相同的区域边界。
- 这是在入职期间的一次性配置，以后无法更改。
- 此功能目前仅适用于新客户。

设置组件

云连接器配置

Secure Private Access 服务作为 Windows 服务在 Cloud Connector 中运行。请确保 Cloud Connector 已安装在您的资源位置。如有必要，请进行设置。

有关详细信息，请参阅 [Cloud Connector 安装](#)。

确保您的 Cloud Connector（或其配置的代理）可以通过端口 443 将出站流量发送到 `allowlist.json` 文件中 [Connector Common and SPA FQDNs](#) 列出的所有 FQDN。

安全私有访问服务

用于混合部署的 Secure Private Access™ 服务提供程序作为 Citrix Cloud Connector 的一部分安装。安装 Citrix Cloud Connector 后，可以在 Windows 服务中找到 Citrix Secure Private Access 服务。Secure Private Access 服务在网络服务帐户下运行。

重要提示：

- Cloud Connector 更新后，Secure Private Access 服务将被禁用。要启用此功能，客户必须联系 Citrix 支持。
- 启用后，服务状态将变为**正在运行**，Secure Private Access 服务将在连接器计算机上自动启动。

Citrix Secure Private Access 服务的端口配置

- Citrix Secure Private Access 使用端口 8443 作为纯 HTTP 服务。
- 确保添加端口 8443 的入站规则，以允许从数据中心网络进行访问。可以通过手动配置防火墙规则或运行 Citrix Secure Private Access 配置工具来打开端口 8443。
 - 导航到 Citrix Secure Private Access 安装文件夹（默认路径 - C:\Program Files\Citrix\AccessSecurityService）。
 - 运行命令 `.\Citrix.AccessSecurityService.exe /ENABLE_SPA_PORTS 8443`。

命令成功运行后，防火墙将自动配置。

- Citrix Secure Private Access 的内部负载均衡器使用端口 8443 添加 Cloud Connector 后端服务。

Secure Private Access 负载均衡器

Secure Private Access 服务的负载均衡器必须配置为启用 TLS，使用以下两种方法之一：

- **负载均衡器上的 SSL 卸载：** Secure Private Access 负载均衡器通过端口 8443 上的 HTTP 与 Cloud Connector 上的 Secure Private Access 服务通信，TLS/SSL 证书安装在负载均衡器上。负载均衡器与 Secure Private Access 服务之间的流量是纯 HTTP 且未加密。有关详细信息，请参阅[配置 SSL 卸载](#)。
- **SSL 桥接：** 负载均衡器将加密流量转发到 Cloud Connector 上的 Secure Private Access 服务。必须在每个 Cloud Connector 主机上为 Secure Private Access 服务安装 TLS/SSL 证书。有关详细信息，请参阅[配置 SSL 桥接](#)。

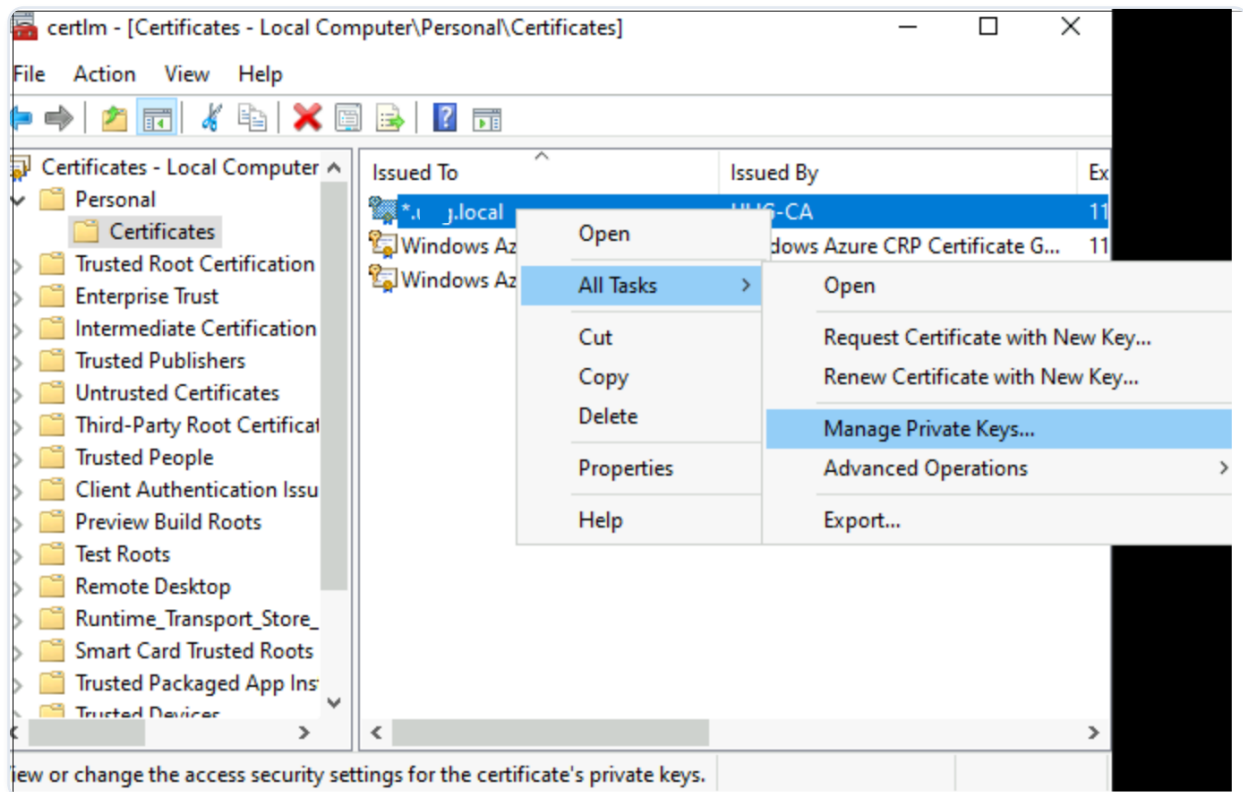
在 Cloud Connector 上为 Secure Private Access 服务配置 TLS/SSL 证书

1. 在 Cloud Connector 的本地计算机个人证书存储中安装有效的 TLS/SSL 证书。确保证书受信任。如有必要，添加颁发 CA 证书。

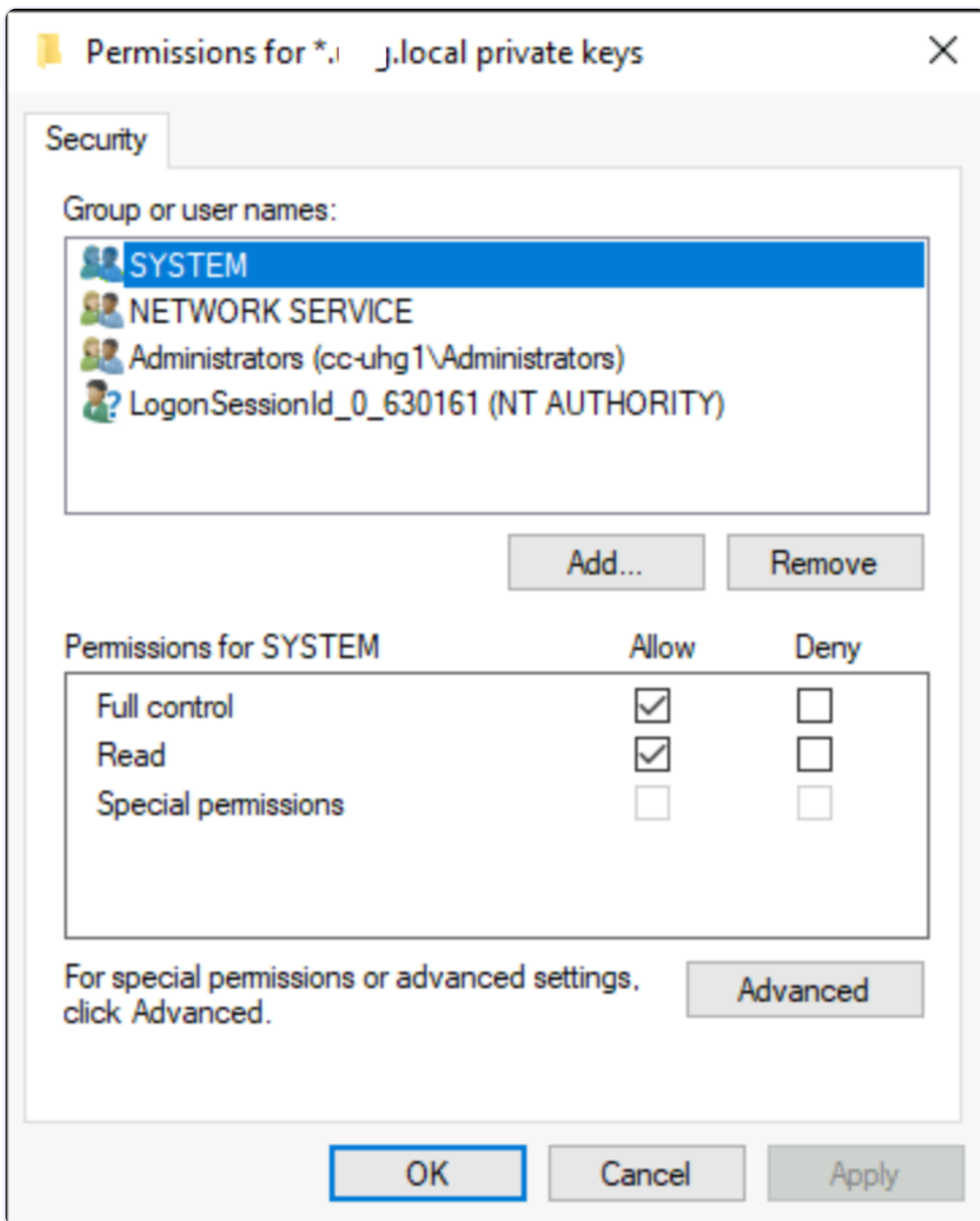
注意：

确保 TLS/SSL 证书包含 Cloud Connector FQDN 作为主题备用名称 (SAN) 的一部分。

2. 授予网络服务帐户访问已安装证书的权限。
 - a. 打开 Microsoft 管理控制台并将证书管理单元添加到本地计算机帐户，按照向导操作，然后单击“确定”。
 - b. 在 Microsoft 管理控制台中，转到“控制台根目录 > 证书 > 个人 > 证书”。
 - c. 右键单击配置 Secure Private Access 所需的证书，然后选择“所有任务 > 管理私钥”。



- a. 在“权限”窗口中，单击“添加”，然后搜索“网络服务”帐户，并选择“只读权限”。



3. 使用 TLS/SSL 证书指纹配置 Secure Private Access 服务。
 - a. 从“TLS/SSL 证书详细信息”复制指纹。
 - b. 导航到 Citrix Secure Private Access 安装文件夹（默认路径 - C:\Program Files\Citrix\AccessSecurityService）并运行 .\Citrix.AccessSecurityService.exe / CERTIFICATE_THUMBPRINT `<ThumbprintValue>`。
 - c. 重新启动 Citrix Secure Private Access 服务。

4. 确保 Secure Private Access 服务作为 TLS 服务运行（使用浏览器或 cURL）：`https://<Cloud connector address>:<port>/secureAccess/health`。

预期结果：`response 200 OK with status "Ok"`。

NetScaler

本主题可帮助您确保满足 NetScaler 配置的所有先决条件。

- 使用以下方法之一为 Citrix Virtual Apps and Desktops 设置 NetScaler Gateway：
 - 为使用 Citrix Workspace 应用程序或 Web 浏览器的用户创建 NetScaler Gateway 虚拟服务器，以便远程访问 StoreFront。有关详细信息，请参阅 [将 NetScaler Gateway 与 StoreFront 集成](#)。
 - 配置 NetScaler Gateway 上的设置。有关详细信息，请参阅 [使用向导配置 NetScaler Gateway 设备](#)。

注意：

XenApp and XenDesktop 向导配置基本身份验证。Secure Private Access 需要高级身份验证。因此，您可以跳过 XenApp and XenDesktop 向导中的[身份验证步骤](#)。您可以在使用向导创建 NetScaler Gateway 后再配置身份验证配置文件。

- 将 SSL 证书添加到 NetScaler。有关详细信息，请参阅 [在 NetScaler 实例上安装 SSL 证书](#)。

为 StoreFront 配置负载均衡器。有关详细信息，请参阅 [使用 NetScaler 进行负载平衡](#)。

配置身份验证

执行以下步骤配置身份验证：

- 配置身份验证虚拟服务器。有关详细信息，请参阅 [身份验证虚拟服务器](#)。
- 配置身份验证配置文件。有关详细信息，请参阅 [配置身份验证配置文件](#)。
- 配置 nFactor 身份验证。有关详细信息，请参阅 [nFactor 身份验证](#)。

常用的 nFactor 身份验证方法：

- [LDAP 身份验证](#)
- [RADIUS 身份验证](#)
- [微软 Entra ID](#)

身份验证配置示例

以下各节提供了有关示例身份验证配置的更多信息。

多重身份验证与条件身份验证

- 使用双因素方案（仅一次用户输入）通过 LDAP 和 RADIUS 进行双因素身份验证
- 根据组织中用户的部门（员工、合作伙伴、供应商）的身份验证登录方法，并提供下拉菜单以选择部门
- 根据用户域的身份验证登录方法，带有下拉菜单
- 将电子邮件 ID（或用户名）输入配置为第一因素，并基于第一因素中的电子邮件 ID 进行组提取以实现条件访问，同时为每个组提供不同的登录类型
- 为具有用户证书的用户使用证书身份验证，并为非证书用户使用原生 OTP 注册的多重身份验证
- 根据用户主机名输入的不同身份验证类型与条件身份验证
- 使用原生 OTP 身份验证的双因素身份验证

第三方集成与多重身份验证

- 将 Azure AD 配置为 SAML IdP（将下一因素配置为 LDAP 策略 - NO_AUTH 以完成 OAuth 信任）
- 条件身份验证，其中第一因素是 SAML，然后根据 SAML 属性自定义登录到证书或 LDAP
- 以 webauth 登录作为第一因素，接着是 LDAP

设备状态扫描 (EPA)

- 设备状态检查用于版本检查，接着是针对合规用户 (RADIUS) 和不合规用户 (LDAP) 的自定义登录
- LDAP 身份验证，接着是强制设备状态扫描
- 在 AD 身份验证之前和之后进行设备状态检查 - 将预 EPA 和后 EPA 作为因素
- 设备证书作为 EPA 因素

其他场景

- 添加带身份验证的 EULA
- 自定义 nFactor 策略标签、登录架构

StoreFront

要在本地 Citrix Store 中显示 Secure Private Access Web 应用程序，您必须在 StoreFront 上将 Secure Private Access 服务配置为新的交付控制器。

请遵循此过程，特别是当您要与现有 Citrix DaaS 环境集成时（因为它允许您使用现有 StoreFront）。

1. 在 StoreFront 服务器上，打开 StoreFront 管理控制台。
2. 导航到用于管理交付控制器的部分（例如，选择 **Store** 并单击 **Manage sites**）。
3. 单击 **Add** 以创建新控制器。
4. 当系统提示您选择控制器类型时，选择 **Secure Private Access** 选项。
5. 在 **Server** 字段中，输入 Secure Private Access 负载均衡器的 FQDN。
6. 选择传输类型 **HTTPS** 和端口 **443**。
7. 保存您的更改。

配置新 Store

如果 Store 尚不存在，请安装受支持的 StoreFront 版本，然后按照 **Create Store** 向导进行操作。确保 Store 配置为：

- **远程访问**：远程访问配置需要 NetScaler Gateway 虚拟服务器地址，该地址用于枚举在 Secure Private Access 中发布的 Web/SaaS 应用程序。
- **身份验证方法**：确保已启用从 Citrix Gateway 直通。

有关详细信息，请参阅 [创建 Store](#)。

组件分析器

组件分析器是一个基于 Web 的工具，用于执行 Secure Private Access 混合设置所需的配置检查。上传必要的报告后，分析器会识别问题，并提供详细的错误消息和解释，包括检测到的 StoreFront 配置错误示例。该工具还会列出解决已识别问题的潜在补救措施。

应用补救措施后，您必须重新运行分析器，以确认所有配置检查均已通过。

检测到的 StoreFront 配置错误示例。



Upload report to analyzer
Drag and drop report here or [Browse](#)

Test	Status
Discover SPA URL	✓ Discovered View details
Discover StoreAuth Key enabled or not	✓ Discovered View details
DNS Resolutions for SPA address	✓ Success
SPA Health Check (using health endpoint)	✗ SPA health-check failed View details
SPA certificate validation	✗ Certificate validation failed View details

Showing 1-5 of 20 items Page 1 of 4 5 rows ▾

Analyze

Close

如果没有错误，分析器将显示所有检查的成功结果。

Analyze configuration

> Prepare for analysis

Secure Private Access

Setup complete

Test	Status
spa.check.cloud.access	Success
spa.check.db.access	Success
spa.check.tag.service.access	Success
spa.check.cas.access	Success

Showing 1-4 of 4 items Page 1 of 1 5 rows

NetScaler Gateway

Setup complete

Upload report to analyzer

Drag and drop report here or [Browse](#)

Test	Status
SPA vServer Configuration Check	Success
SPA Profile High Cipher Check	Success
SPA vServer SSL Profile Set Check	Success
SPA Profile Configuration Check	Success
SPA Profile Binding Check	Success

Showing 1-5 of 25 items Page 1 of 5 5 rows

Analyze Close

安全私有访问分析器

Secure Private Access 分析器评估 Secure Private Access 部署所需的关键 Citrix Cloud 组件的就绪情况和可达性。无需上传报告，它会自动检查与 Cloud Access、数据库服务和其他所需内部服务等基本服务的连接。

通过验证每个组件的可访问性和运行状态，该工具可帮助管理员快速识别网络或配置问题，确保所有 Citrix Cloud 依赖项都可用并正常运行，以实现 Secure Private Access 集成。

NetScaler Gateway 分析器

NetScaler Gateway 分析器通过自动化关键任务和突出显示配置问题来简化 Secure Private Access 部署。它执行有针对性的检查和验证，生成可操作的诊断结果，从而提高可靠性和性能，同时减少手动工作量和配置风险。

NetScaler Gateway 分析器功能包括：

- **配置：** NetScaler Gateway 组件的自动或交互式设置。
- **分析：** 评估 Secure Private Access 组件的连接性、合规性和运行状况。
- **清理：** 在需要时删除 Secure Private Access 配置。

每个功能都通过专用的命令行选项（请参阅 README.txt）调用，支持从初始部署到维护再到受控拆除的灵活生命周期管理。

执行会生成包含结构化日志和分析摘要的时间戳工件。输出涵盖配置状态、连接测试结果、发现的组件元数据以及已识别的问题。清理操作提供实体删除确认，以确保状态干净。所有结果均以结构化 JSON 格式交付，适用于自动化、集成和审计。

请参阅 [步骤 3：配置和分析](#)，以下载并在 NetScaler 上运行脚本。

StoreFront 分析器

StoreFront 分析器通过自动化发现和验证任务，简化了 Citrix StoreFront 的 Secure Private Access 准备情况检查。它对配置、连接、身份验证和证书进行有针对性的评估，生成可操作的诊断结果，从而提高可靠性，同时减少手动工作量和配置风险。

StoreFront 分析器功能包括：

- **分析：** 对 StoreFront 配置、网络可达性、身份验证设置、远程访问参数以及与 Secure Private Access 兼容性相关的证书有效性进行只读评估。

执行会生成包含结构化日志和分析摘要的时间戳工件。输出包括 Secure Private Access URL 发现、StoreAuth 密钥状态、DNS 解析结果、健康端点可访问性、SSL 证书验证以及发现的组件元数据。所有结果均以结构化 JSON 格式交付，适用于自动化、集成和审计。

不进行任何配置更改。分析器以只读模式运行。

请参阅 [步骤 3：配置和分析](#)，以下载并在 NetScaler 上运行脚本。

与 Google Chrome 企业高级版 集成

Citrix 客户可以利用世界上最流行、最安全的网络浏览器 Chrome，通过熟悉的用户体验本地访问授权的企业网络应用程序。Citrix Secure Private Access 根据管理员定义的策略强制执行基于应用程序的最小权限访问，这些策略通过 Secure Private Access 控制台进行集中管理。管理员可以在 Secure Private Access 控制台上轻松配置企业应用程序域和零信任访问策略。他们可以模拟策略以验证和测试安全结果，并提供适当级别的用户访问和最终用户体验。

集成解决方案包括以下组件：

- Google Chrome Enterprise Premium (CEP)，其中包括数据丢失防护 (DLP)、恶意软件和网络钓鱼防护、URL 过滤以及 Google 管理控制台等功能。
 - 在客户端计算机上本地运行的 Google Chrome 浏览器通过 Chrome 托管配置文件，作为安全浏览器，强制执行用户级别的策略。
 - 通过 Google Cloud 门户访问的 Google Chrome Enterprise Premium 控制台为 Chrome Enterprise Premium 安全策略提供管理、管控和监控控制台。
- Citrix Secure Private Access，其中包括对云基础设施、ZTNA 策略引擎以及部署在客户环境中的连接器设备的访问。
- Citrix 控制台，包括用于对私有应用程序实施零信任访问策略的 Secure Private Access 控制台，以及用于监控和故障排除的 Citrix Monitor。

Citrix Secure Private Access 服务强制执行管理员配置的所有访问策略，确保用户仅被授予对特定网络应用程序的访问权限。

Chrome Enterprise Premium 高级安全功能

以下是 Chrome Enterprise Premium 提供一些高级安全功能：

- **数据丢失防护 (DLP)**：实施精细控制和策略，防止敏感数据泄露或意外共享。
- **恶意软件深度扫描**：使用高级扫描技术检测并隔离未知或高风险文件，阻止恶意代码执行并防范零日攻击。
- **网络钓鱼防护**：通过识别和阻止网络钓鱼尝试，保护用户免受有害网站的侵害，防止登录凭据和个人信息被盗。

- **URL 分类和过滤**：根据内容类别限制对网站的访问，防止用户访问不当或恶意内容。
- **Web 使用情况洞察和分析**：提供关于网络流量的详细报告和分析，使管理员能够监控用户活动，识别潜在的安全威胁，并优化网络带宽。

有关更多信息，请参阅 [Chrome Enterprise Premium 概述](#)。

成功集成的先决条件

为确保 Citrix Workspace™ 应用程序与 Chrome Enterprise Premium 之间的最佳集成，必须满足以下先决条件。成功完成这些先决条件将使您在从 Citrix Workspace 应用程序或基于 Web 的用户界面启动应用程序时获得更高效、更无缝的体验。

先决条件大致分为以下几类。

- [NetScaler 先决条件](#)
- [Cloud Connector 先决条件](#)
- [StoreFront 先决条件](#)
- [Secure Private Access 先决条件](#)
- [Google 先决条件](#)
- [将 Citrix Workspace 中配置的用户目录与 Google Cloud 用户目录同步](#)
- [绕过 TLS 检查](#)

Citrix Secure Private Access - 支持的部署模式

集成解决方案支持 Citrix Secure Private Access 的以下部署模式：

- **Citrix Secure Private Access 服务**：在此部署模式下，所有组件（包括控制平面和网关基础架构）都托管在 Citrix Cloud 中。有关更多信息，请参阅 [Citrix Secure Private Access](#)。
- **Citrix Secure Private Access 混合部署**：此部署允许客户使用本地 StoreFront 和 NetScaler Gateway 组件实施零信任网络访问 (ZTNA) 解决方案，并使用 Citrix Cloud 管理配置、管理和监控功能。这意味着客户可以利用现有的本地 NetScaler Gateway 来控制用户流量路由，同时使用 Citrix Cloud 托管的 UI 来管理配置和策略，还可以使用 Citrix Cloud 中托管的 Citrix Monitor 来进行监控和故障排除功能。有关更多信息，请参阅 [Citrix Secure Private Access 混合部署](#)。

重要提示：

对于 Chrome Enterprise Premium (CEP)，仅支持 HTTPS 企业 Web 和 SaaS 应用程序。不支持 HTTP 企业 Web 和 SaaS 应用程序。

法律声明

Chrome Enterprise Premium 由 Google LLC 提供，您的使用受 [Google 的可接受使用政策](#) 和 [服务特定条款](#) 的约束。

管理员角色和权限

Citrix 服务帐户由 Secure Private Access 用于将用户载入 Chrome Enterprise Premium (CEP) 并启用 CEP 集成。因此，您必须在 Google 管理控制台中为该服务帐户分配具有所需权限的角色。

Google 管理控制台中提供两种类型的角色：

系统角色： 这些是 Google 提供的默认角色。除了超级管理员角色外，其余系统角色不包含 CEP 与 Secure Private Access 集成所需的所有必要权限。

自定义角色： 这些角色可以包含管理员 API 权限的任何子集。您必须创建一个自定义角色，其中包含 CEP 与 Secure Private Access 集成所需的所有权限。

您必须以超级管理员身份登录 Google 管理控制台才能执行此任务。

注意：

超级管理员角色不能分配给服务帐户。

Google 自定义管理员角色权限

对于 CEP 和 Secure Private Access 集成，Citrix 服务帐户必须在 Google 管理控制台中具有包含以下特定权限的自定义角色：

所需的管理员权限	为何需要此权限
管理客户 > 读取客户	用于读取 Google 客户组织的友好名称。

所需的管理员权限	为何需要此权限	
组织单位 > 读取	验证配置的组织单位在 Google Directory 中可用。	
服务 > Chrome 管理 > 设置 > 管理用户设置 注意：确保您选择顶级权限管理用户设置 和子权限（管理应用程序设置 和 管理 Web 设置）。	添加用户配置文件中 CEP 和 SPA 集成所需的强制扩展及其配置。	
服务 > Chrome 管理 > 设置 托管浏览器 > 读取	读取托管的 Chrome 配置文件和托管的浏览器。	
许可证管理 > 读取	查询为组织预配的 Chrome Enterprise Premium 分配的许可证总数。	
报告	读取正在积极使用其分配的许可证的用户。 读取触发数据丢失防护 (DLP) 规则时的活动事件。 读取故障事件。	
群组 > 读取	验证配置的集成组在 Google Directory 中可用。	
服务 > 警报中心 > 完全访问 > 查看访问	读取数据丢失防护的安全警报和登录失败事件。	
管理设备和设置	读取设备元数据，以便在“监视网络拓扑”视图中显示它们。	
用户 > 读取	验证配置的集成用户在 Google Directory 中可用。	

注意：

- 还需要为这些管理员权限授予等效的 OAuth 范围。
- 所有管理权限现在都可以在“**管理员权限**”部分中找到。这包括以前在“**管理控制台权限**”和“**管理 API 权限**”部分中列出的权限。此更改不影响权限的分配方式，现有权限将继续像以前一样工作。
- 确保选择顶级权限“**管理用户设置**”和子权限（“**管理应用程序设置**”和“**管理 Web 设置**”）。仅选择子权限是不够的。
- Citrix Secure Private Access 使用配置的 Citrix 服务帐户将配置部署到您的 Google 帐户。完成 Citrix Secure Private Access 和 Google CEP 集成后，打开 Google 管理控制台并导航到“**Chrome 浏览器 > 应用和扩展程序**”。请注意，已在根组织级别配置了多个浏览器扩展。这些扩展由子 OU 继承。当用户使用此租户加入 Google Chrome 配置文件时，这些扩展会自动预配。

创建和分配角色和权限

执行以下步骤以创建自定义管理员角色并分配权限：

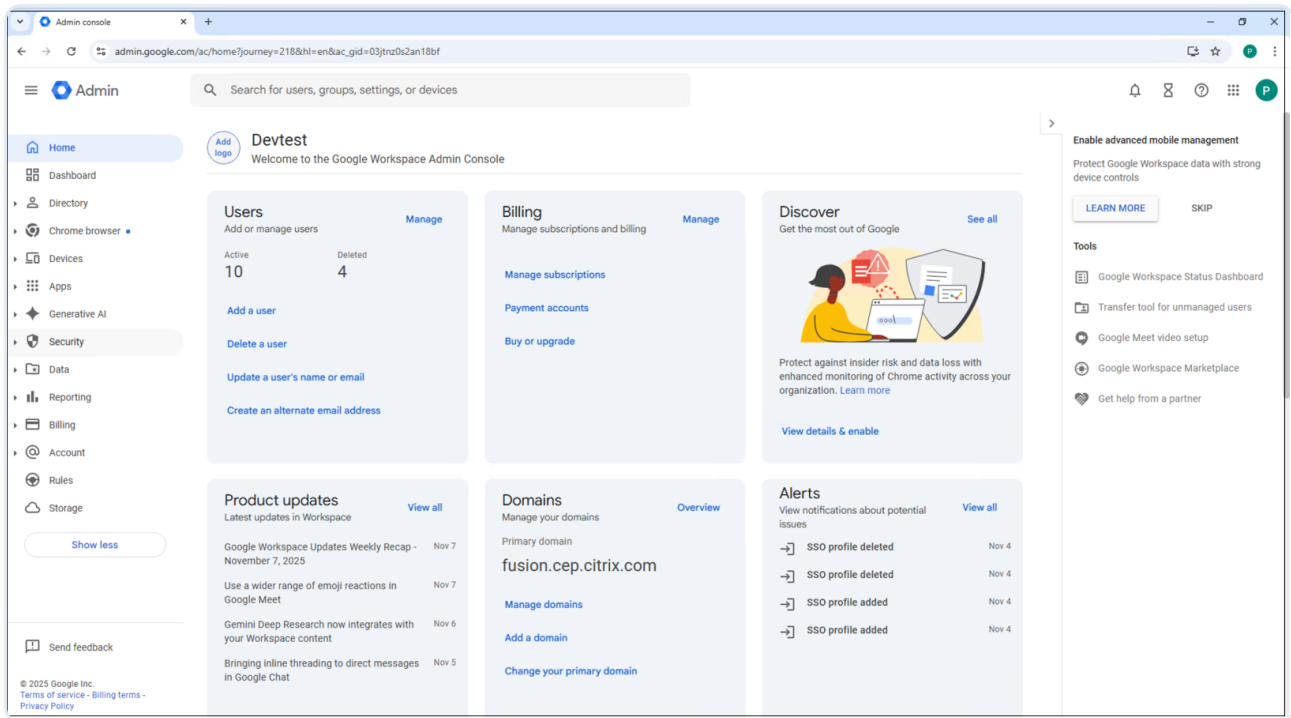
1. 在 Google 管理控制台中，导航到 **帐号 > 管理员角色**。
2. 单击 **创建新角色**，然后输入角色的名称和描述。
3. 将 Google Chrome 集成所需的所有权限添加到此自定义角色。有关所需权限的列表，请参阅 [Google 自定义管理员角色权限](#)。

有关角色和权限的更多信息，请参阅 [Google 文档](#)。

4. 保存自定义角色。

Open ID Connect 配置文件，用于将 NetScaler Gateway 用作 IdP

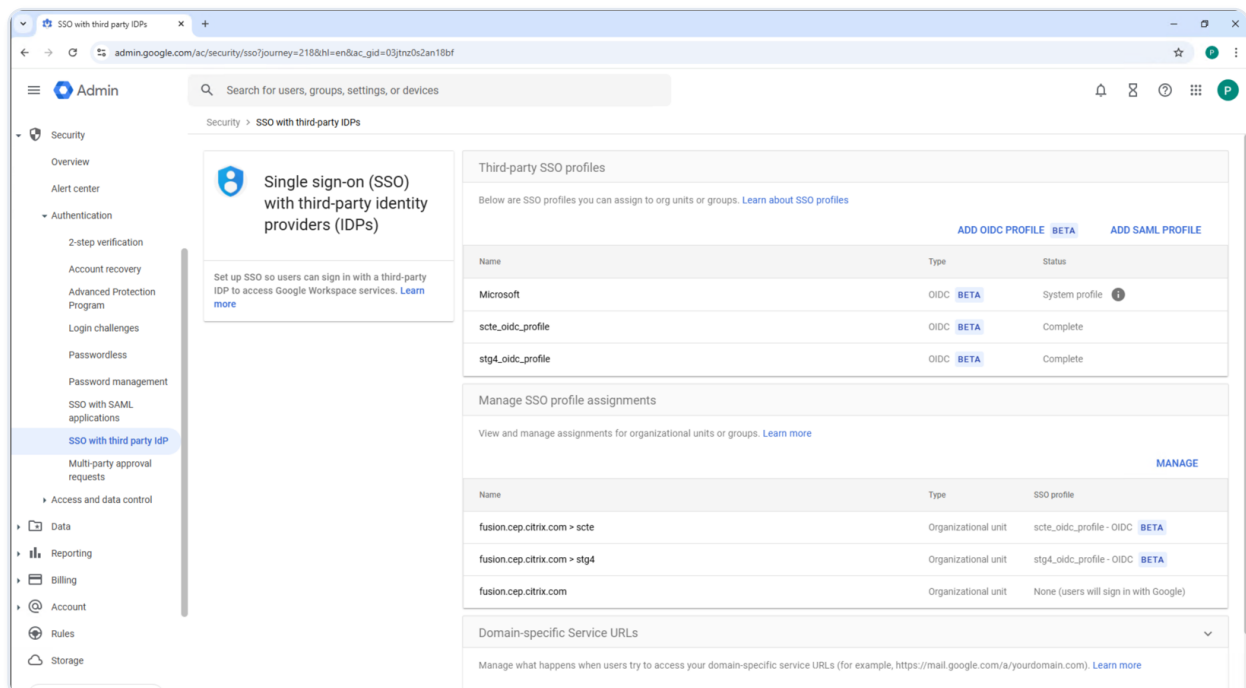
您必须在 Google 管理控制台中创建 OIDC 配置文件，才能将 NetScaler Gateway 用作 IdP。



创建 Google OIDC SSO 配置文件

在 Google 管理控制台中执行以下步骤。

1. 转到 **安全 > 身份验证 > 使用第三方 IdP 进行 SSO**，然后选择 **添加 OIDC 配置文件**。



2. 输入配置文件的名称。
3. 输入 OIDC 详细信息。

- **客户端 ID**：使用随机客户端 ID（通常是 22 个字符的数字字符串）

- **客户端密钥**：生成一个至少包含 32 个字符的随机字符串。该字符串必须包含字母数字和特殊字符。

在 NetScaler 上配置 OAuth IdP 配置文件时，**客户端密钥**字段中不允许使用某些特殊字符，例如 - #、@、!、\、&、%。因此，您不得在此处的**客户端密钥**字段中使用这些特殊字符。

注意：

您必须在 NetScaler Gateway 中手动生成客户端 ID 和客户端密钥。

- **颁发者 URL**：将此字段设置为 `https://<SPAGatewayFQDN>/oauth/idp/<OAuthIdpProfileName>`，其中 `SPAGatewayFQDN` 是与 Secure Private Access Gateway URL 对应的 FQDN，`OAuthIdpProfileName` 是在 NetScaler Gateway 上创建的 OAuth IdP 配置文件的名称。

注意：

IdP 配置文件名称中不要使用空格。

- **更改密码 URL**：留空（此时不需要）

4. 单击**保存**。

The screenshot shows the 'Add OIDC profile' form in the Google Admin console. The form is titled 'Add OIDC profile' and contains two main sections: 'OIDC SSO profile' and 'OIDC details'. The 'OIDC SSO profile' section has a text input field for 'SSO profile name' with a character count of 0/140. The 'OIDC details' section contains four text input fields: 'Client ID' (with a description: 'OAuth Client ID used to identify the client with the authorization server.'), 'Client secret' (with a description: 'OAuth Client Secret used to authenticate the client to the authorization server.'), 'Issuer URL' (with a description: 'Base URL of the OAuth authorization server.'), and 'Change password URL' (with a description: 'Must be a valid URL (for example, https://domain.com). This is the URL users are redirected to when they attempt to change their Google account password.'). At the bottom right of the form are 'CANCEL' and 'SAVE' buttons.

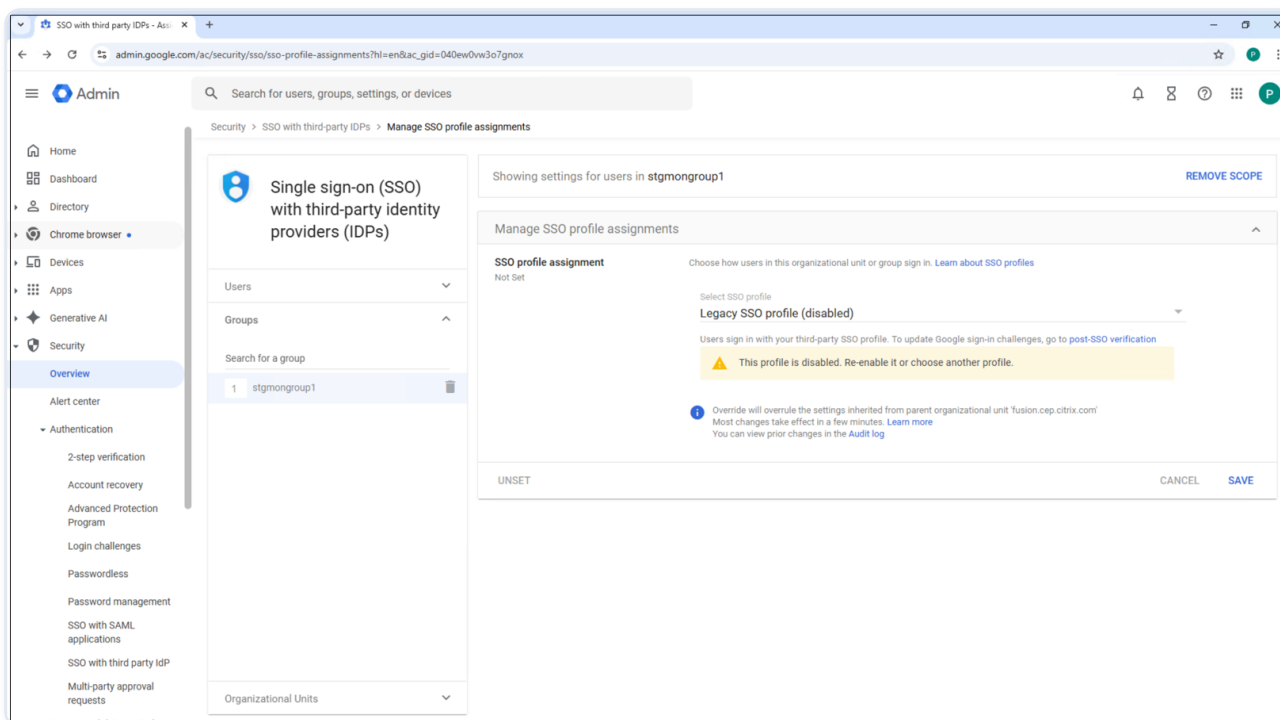
重要提示：

记下客户端 ID、客户端密钥和重定向 URL。在 NetScaler Gateway 上配置 OAuth IdP 配置文件时需要这些值。

绑定 OIDC 配置文件（到 OU 或组）

要完成 OIDC 配置文件配置，您必须将其绑定到 Google Workspace 中的特定组织单位 (OU) 或组。此绑定决定了哪些用户可以使用此 OIDC 配置文件通过 NetScaler Gateway 作为 IdP 进行身份验证。

1. 导航到**安全 > 身份验证 > 使用第三方 IdP 的 SSO**。
2. 在**管理 SSO 配置文件分配**中，单击**管理**
3. 在左侧导航窗格中，选择根组织单位 (OU) 和您的 SSO 配置文件，为组织的所有用户启用 SSO。或者，您可以将 SSO 配置文件分配给特定的组或 OU。
4. 选择您创建的 SSO 配置文件，然后单击**保存**。



将 NetScaler 配置为 OAuth IdP

有关将 NetScaler 配置为 OAuth IdP 的信息，请参阅 [NetScaler 作为 OAuth IdP](#)。

注意：

- OAuth IdP 配置文件中的 **Audience** 字段值必须与客户端 ID 值相同。
- **Issuer URL** 必须与 Google 管理控制台中配置的 URL 匹配。
- 客户端 ID、客户端密钥 和 重定向 URL 值必须从 Google 管理控制台获取。

目录同步

以下部分提供了有关目录同步的更多信息。

使用 G Suite 连接器的 Microsoft Entra ID

您必须将 Microsoft Entra ID 与 Google Cloud 用户目录同步，以便在 Google 和 Microsoft 云平台之间进行用户和组管理。有关详细信息，请参阅以下主题：

- [Microsoft Entra ID（以前称为 Azure AD）用户预配和单点登录](#)
- [由 Microsoft 配置 Google Cloud / G Suite 连接器以实现与 Microsoft Entra ID 的单点登录](#)

所有用户和组都必须填写电子邮件地址字段。电子邮件域必须与 Google Directory 中配置的域匹配。这意味着，目前不支持没有电子邮件地址的安全组或电子邮件域为 @onmicrosoft.com 的组。

单点登录：单点登录 (SSO) 配置是可选的。您可以在 Google 目录中配置单独的密码。请参阅 [使用 Open ID Connect 配置文件配置 SSO 以将 NetScaler Gateway 用作 IdP](#)。

谷歌云目录同步 (GCDS) 工具

借助 Google Cloud Directory Sync (GCDS)，您可以将 Google 帐户中的数据与 Microsoft Active Directory 或 LDAP 服务器同步。GCDS 不会将任何内容（例如电子邮件、日历事件或文件）迁移到您的 Google 帐户。您可以使用 GCDS 同步您的 Google 用户、群组 and 共享联系人，使其与 LDAP 服务器中的信息匹配。

有关详细信息，请参阅 [关于 Google Cloud Directory Sync](#)。

安装和准备 GCDS：

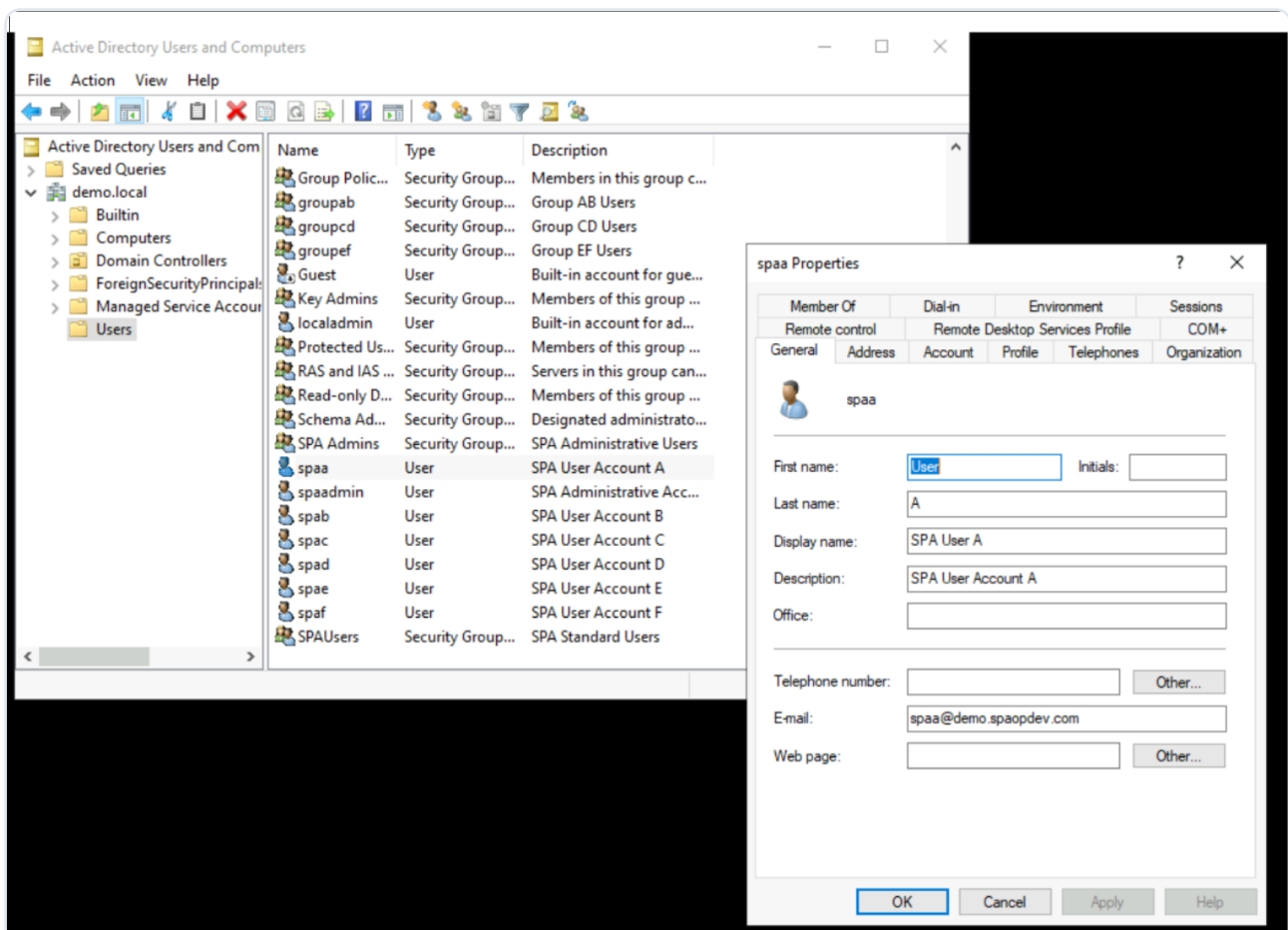
- [下载](#)
- [安装](#)

注意：

- 出于 POC 目的，GCDS 工具可以安装在 AD 计算机上。
- 以管理员权限运行安装程序。
- 配置可以保存到文件（文件\另存为）中，并在下次需要同步时打开。

活动目录

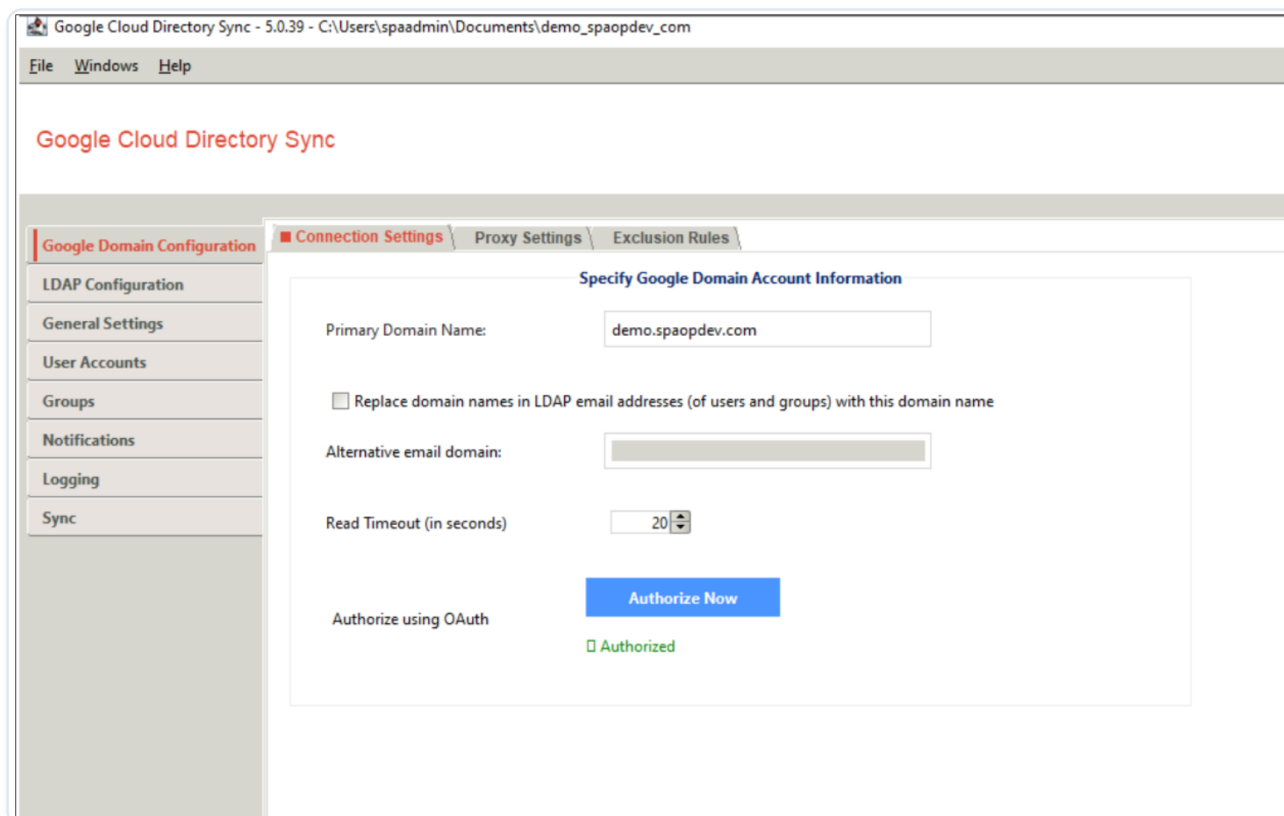
作为先决条件，请确保您已在活动目录上创建了用户和组。用户和组必须具有电子邮件属性。



谷歌云目录同步配置

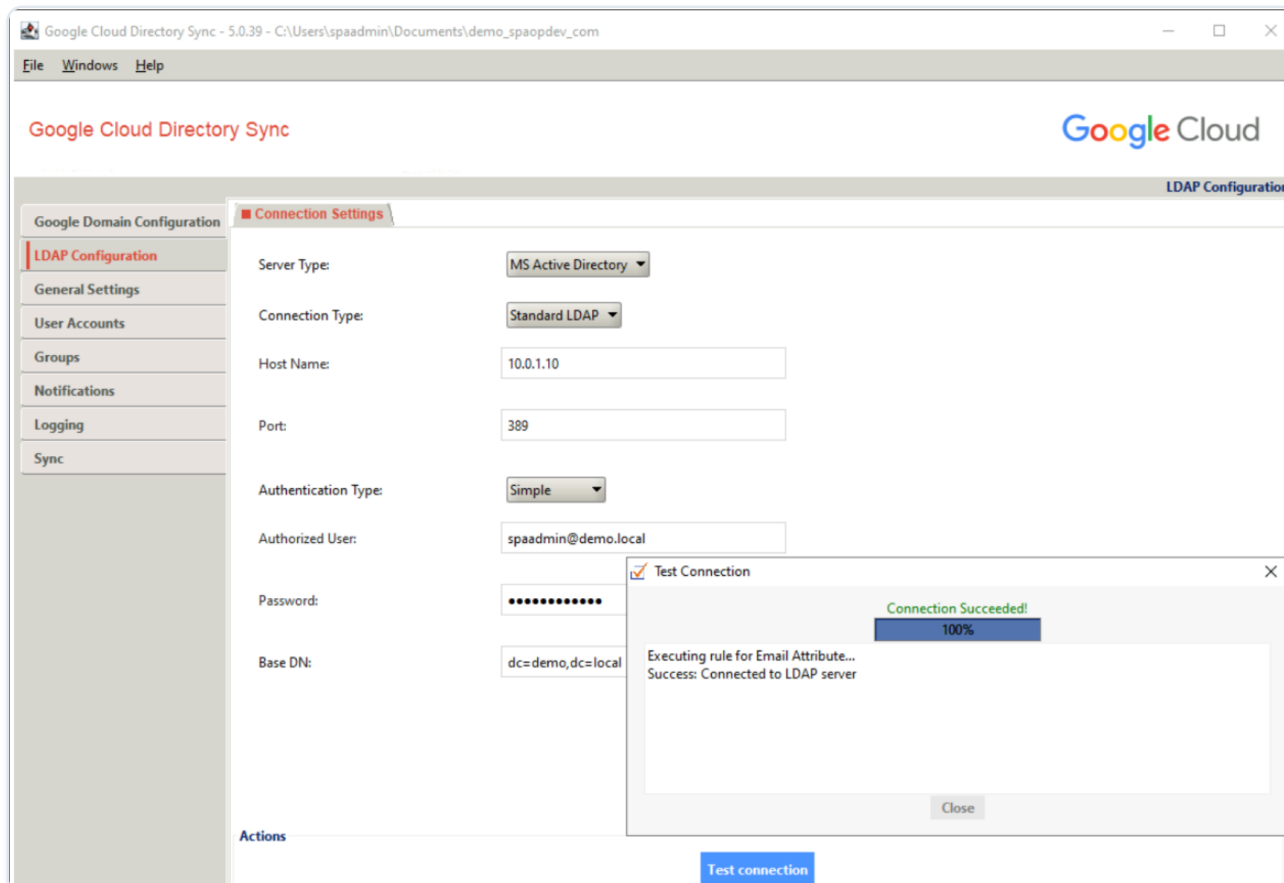
Google 域配置：

1. 输入主域名。
2. 使用 OAuth 授权。单击**立即授权**。系统会提示您输入 Google Workspace 管理员凭据，并要求您允许访问 Google Workspace 目录。



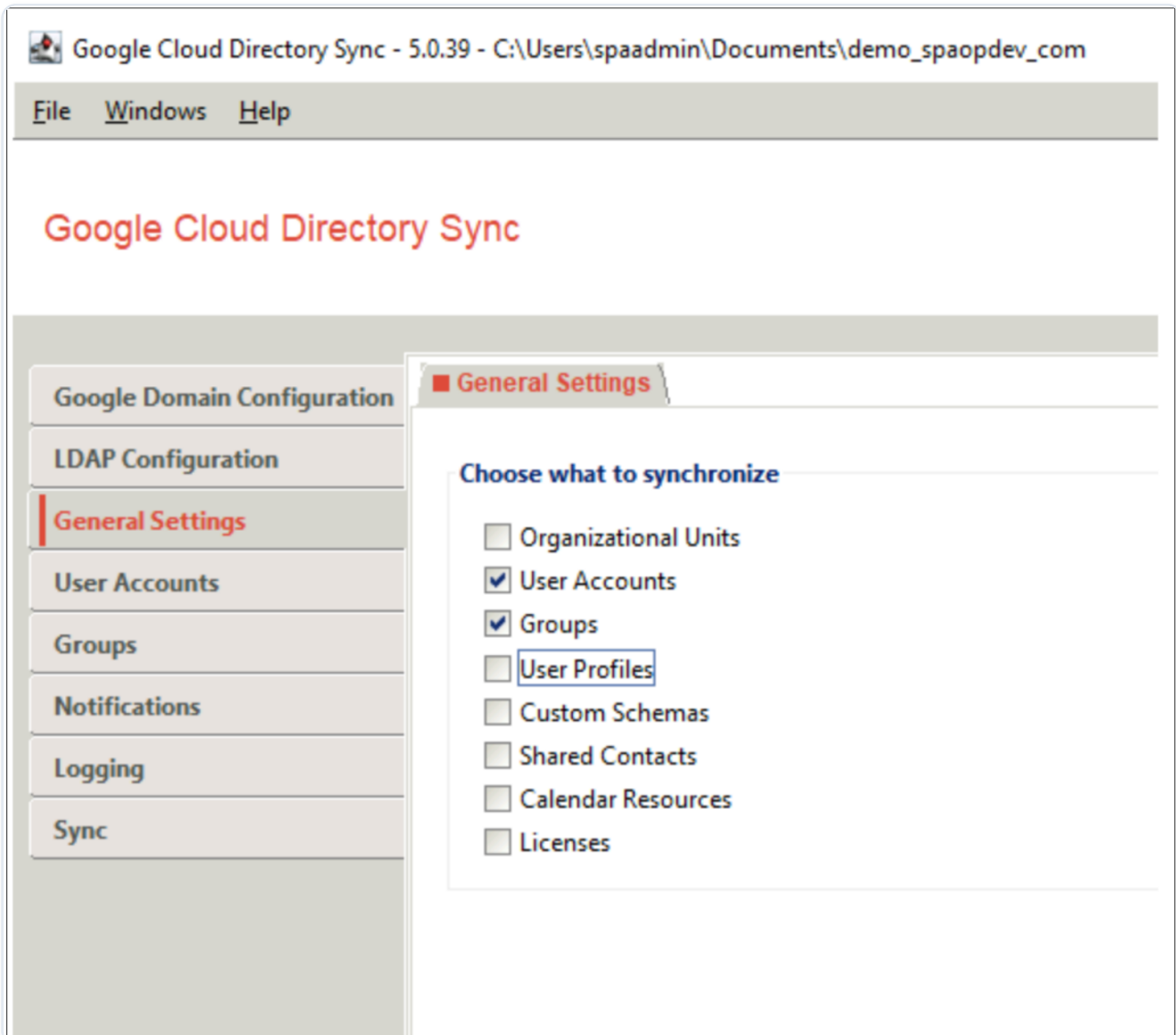
LDAP 配置：

1. 输入主机名、端口、授权用户和密码。



常规设置：

选择要同步的项目。



用户帐户：

1. 指定要导入和同步的用户。
2. 单击**使用默认值**以设置用户属性、其他用户属性和搜索规则。

Google Cloud Directory Sync - 5.0.39 - C:\Users\spadmin\Documents\demo_spaopdev_com

File Windows Help

Google Cloud Directory Sync

Google Domain Configuration

LDAP Configuration

General Settings

User Accounts

Groups

Notifications

Logging

Sync

User Attributes Additional User Attributes Search Rules Exclusion Rules

User Email

Email Address Attribute: mail

☐ Enable invalid characters replacement

Invalid characters replacement:

User Attributes

Unique Identifier Attribute: objectGUID

Alias Address Attributes: proxyAddresses

Add Remove

Google Domain Users Deletion/Suspension Policy

Actions

Use defaults

Google Cloud Directory Sync - 5.0.39 - C:\Users\spadmin\Documents\demo_spaopdev_com

File Windows Help

Google Cloud Directory Sync

User Accounts

Google Domain Configuration

LDAP Configuration

General Settings

User Accounts

Groups

Notifications

Logging

Sync

User Attributes **Additional User Attributes** Search Rules Exclusion Rules

Given Name Attribute(s): givenName

Family Name Attribute(s): sn

Display Name Attribute(s): displayName

User Password Sync

Synchronize Passwords

☒ Only for new users ☐ For new and existing users ☐ Only changed passwords

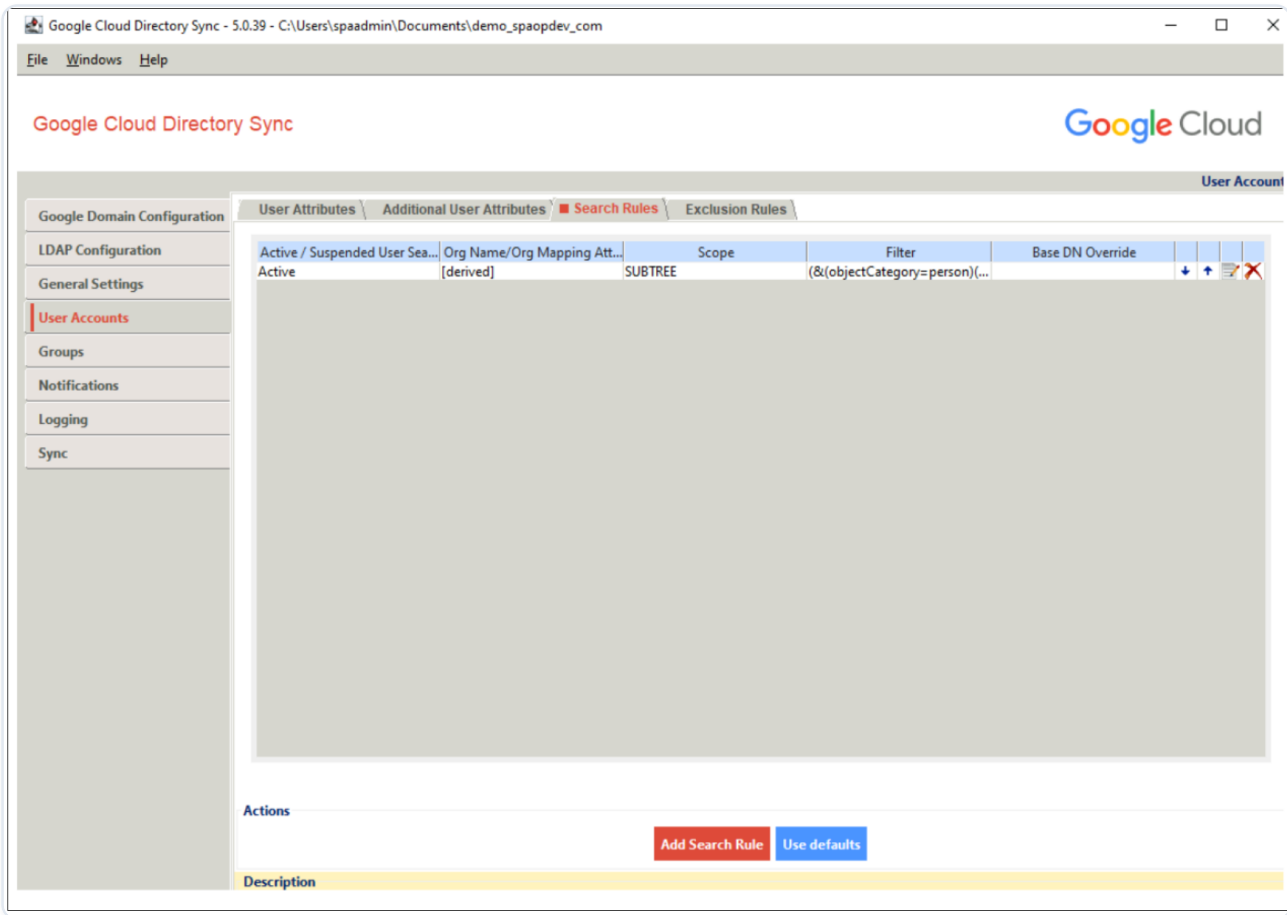
Password Attribute:

Password Timestamp Attribute:

Actions

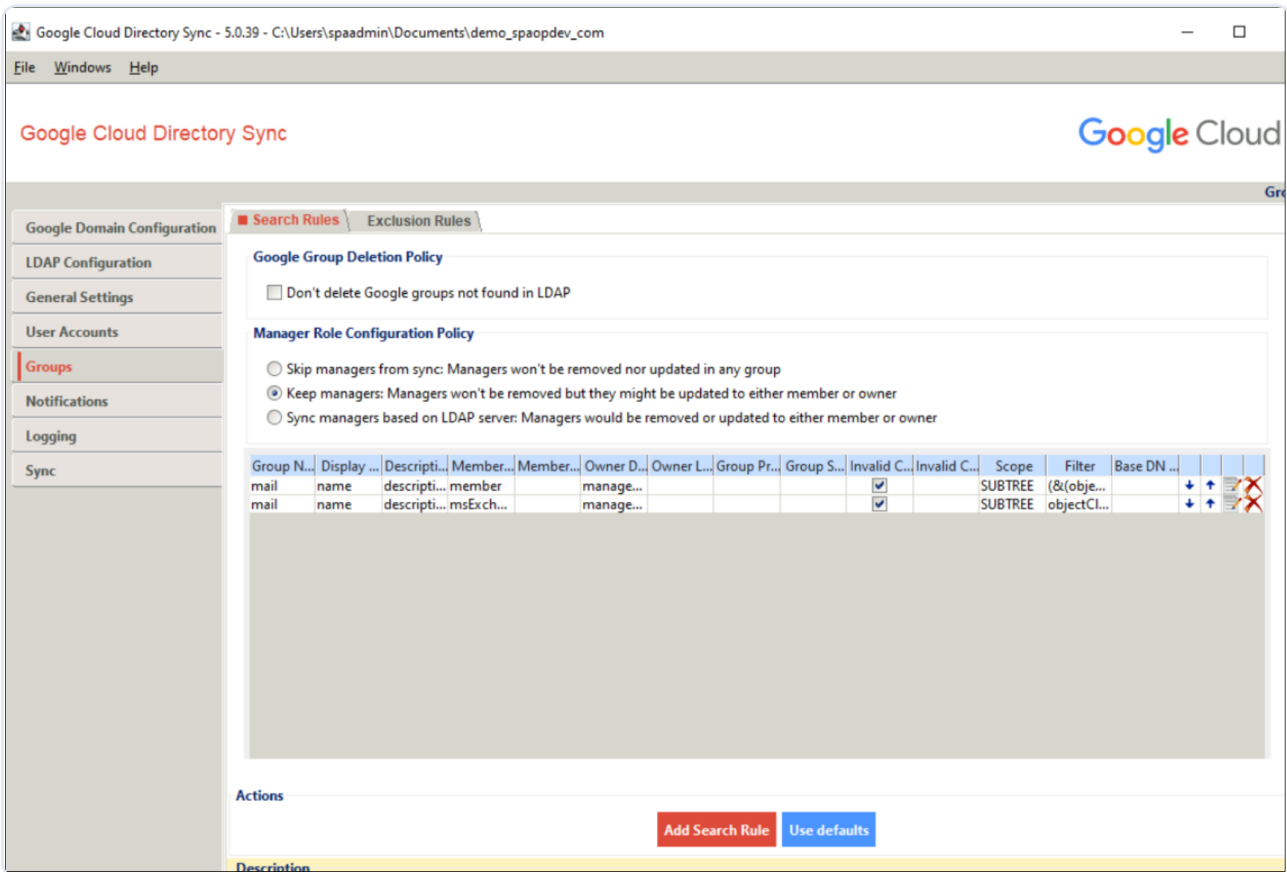
Use defaults

Description



组：

1. 指定要导入和同步的组。
2. 单击**使用默认值**以设置组的**搜索规则**。



通知：

此步骤是可选的。

同步后，Google Cloud Directory Sync 连接到您的 SMTP 中继主机并发送包含同步详细信息的通知。

- 指定您希望显示在通知标题中的发件人地址。
- 逐一输入收件人电子邮件地址，然后为每个地址单击“添加”按钮。

如果同步报告超过 24 MB，它将被压缩并作为 ZIP 附件发送。

Google Cloud Directory Sync - 5.0.39 - C:\Users\spadmin\Documents\demo_spaopdev_com

File Windows Help

Google Cloud Directory Sync

Google Domain Configuration

LDAP Configuration

General Settings

User Accounts

Groups

Notifications

Logging

Sync

■ Notification Settings

SMTP Relay Host: smtp.demo.spaopdev.com

☒ Use SMTP with TLS

User Name: spaadmin@demo.spaopdev.com

Password: ●●●●●●●●

Subject Prefix:

From address: spaadmin@demo.spaopdev.com

To addresses (recipients):
spaadmin@demo.spaopdev.com

☒ Use attachment

☒ Compress attachment

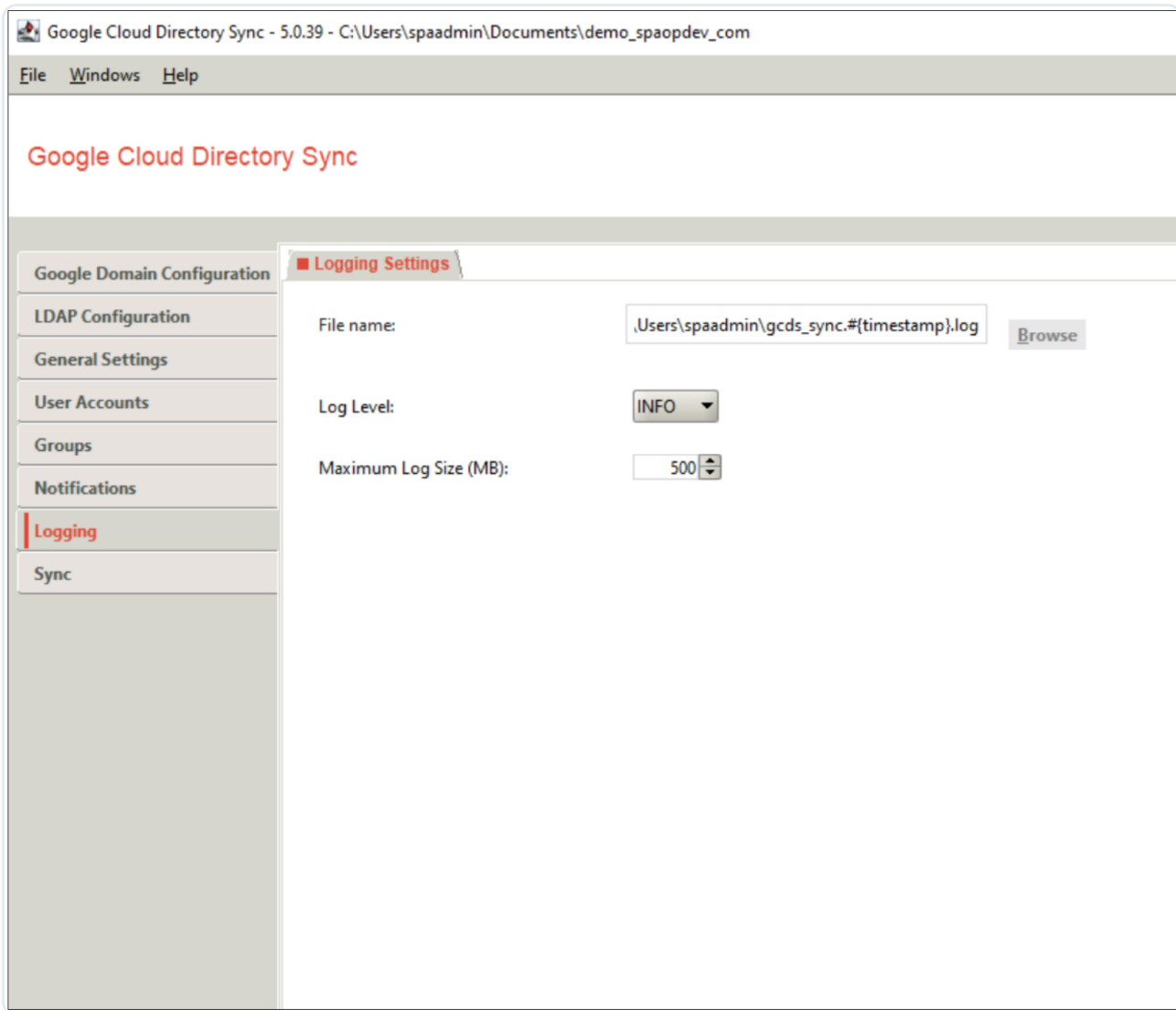
Do not include in notifications:

Actions

Test Notification

日志记录：

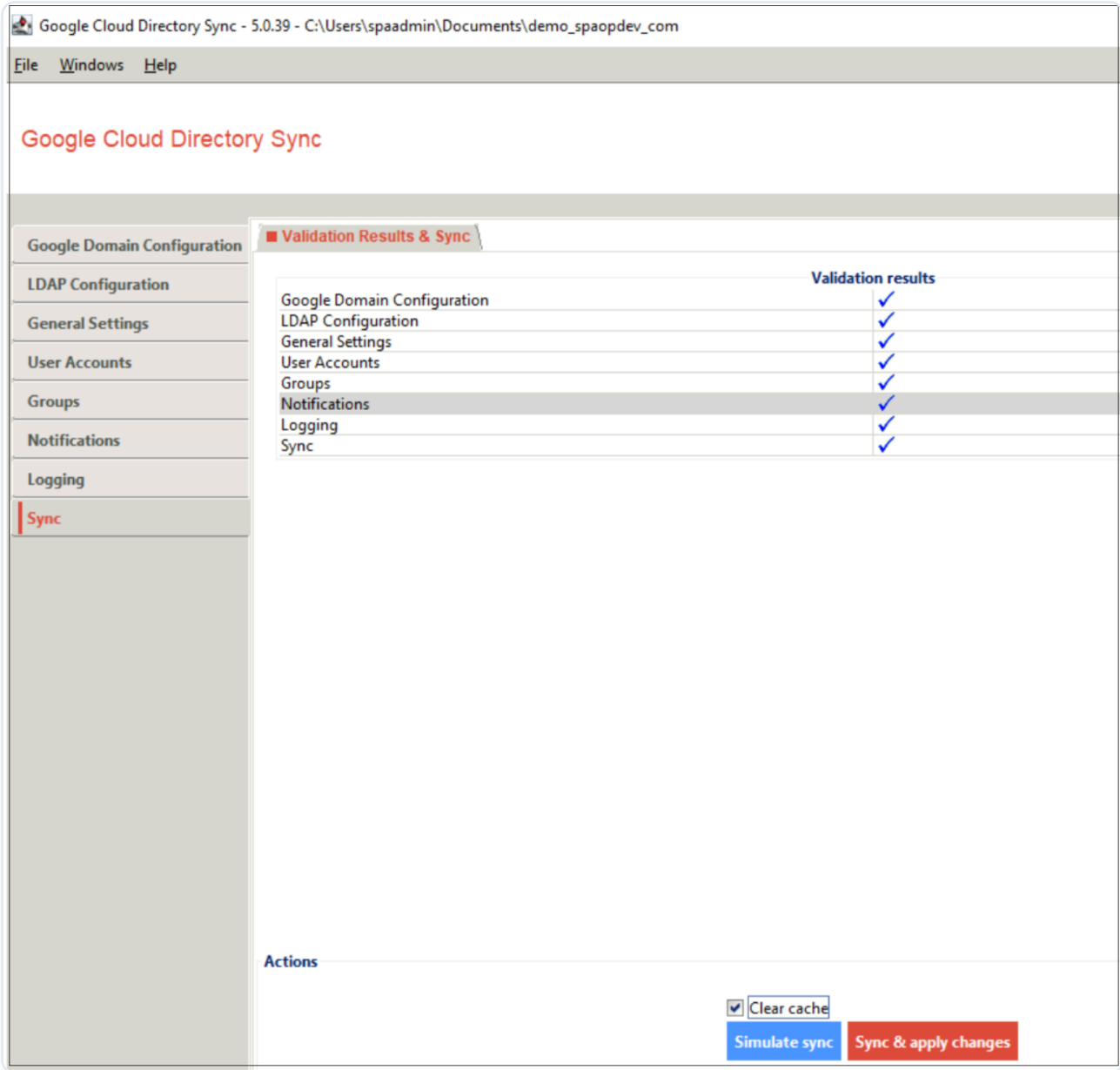
指定日志文件信息的写入位置、详细程度以及最大日志文件大小。



同步：

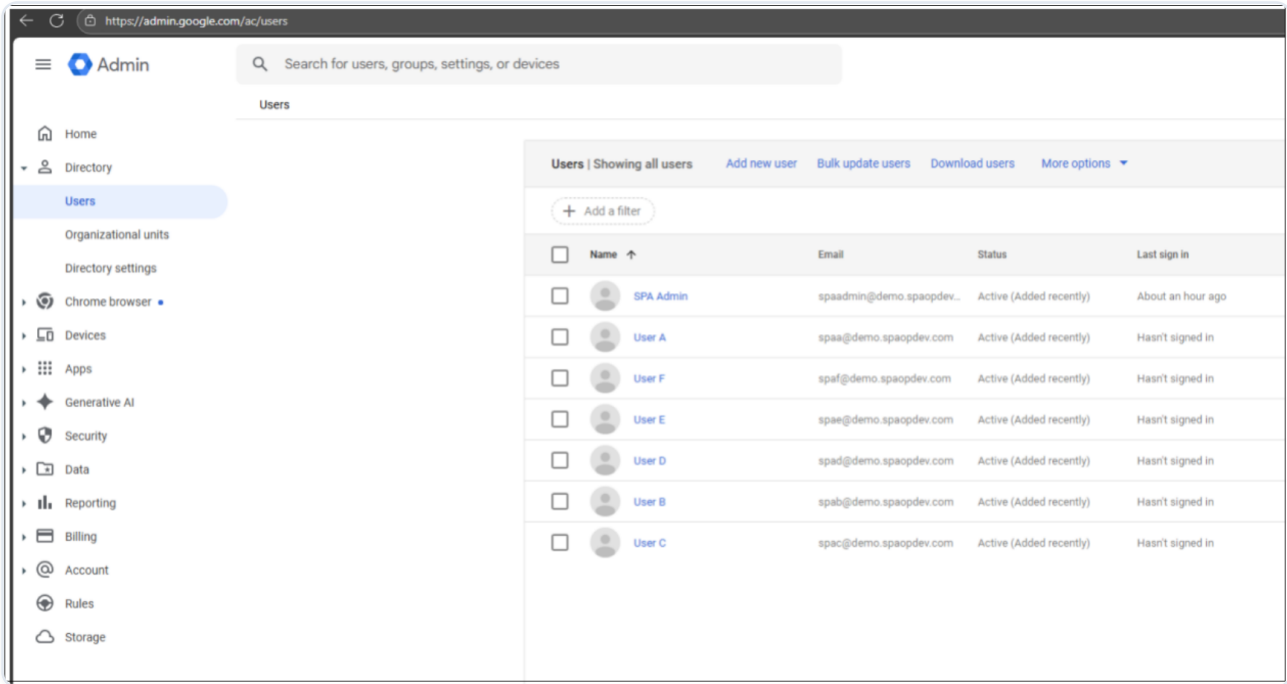
在同步之前，请检查您的设置并更正所有问题。

- 设置正确后，单击“**模拟同步**”以连接到两台服务器并生成模拟同步的更改列表。
- 要提交更改，请保存配置文件并单击“**同步**”并应用更改，或者从命令行运行 `sync -cmd`。



谷歌工作区目录：

在同步期间会创建新用户。



使用 CLI 同步：

请参阅[使用命令行同步](#)。

最终用户体验

用户可以使用以下方法通过 Secure Private Access 访问应用程序。每种访问方法都提供不同的用户体验，组织可以根据其所需的用户体验和部署策略选择最合适的方法。

- **Citrix Workspace 应用程序** - 本机桌面应用程序，提供最安全、功能最丰富的访问体验，具有完整的策略实施和单点登录功能。
- **从 Web 浏览器访问应用商店 URL** - 可通过不同浏览器环境访问的基于 Web 的界面：
 - 非 Chrome 浏览器（例如 Firefox、Safari 或 Edge）
 - 具有非托管配置文件的 Chrome（没有企业策略的个人 Chrome 浏览器）
 - 具有托管配置文件的 Chrome（具有 Chrome Enterprise Premium 策略的企业托管 Chrome 浏览器）
- **Chrome 托管配置文件** - 用户通过使用书签或在 Chrome 托管配置文件的地址栏中手动键入应用程序 URL 来直接访问应用程序。

下表总结了使用各种方法访问应用程序时的最终用户体验：

	直接	从 WEB 浏览器访问应用商店 URL	CITRIX WORKSPACE 应用程序
非 Chrome 浏览器	SaaS 应用程序访问被拒绝（假设 SaaS 应用程序已配置适当的 IP 地址允许列表）。	应用程序在应用商店中枚举。	不适用
	私有应用程序无法访问。	应用程序在相应的 Chrome 托管配置文件中启动。	
		如果尚未创建相应的托管配置文件，则会启动配置文件创建向导。	
Chrome（非托管配置文件）	SaaS 应用程序访问被拒绝（假设 SaaS 应用程序已配置适当的 IP 地址允许列表）。	应用程序在相应的 Chrome 托管配置文件中启动。	不适用
	私有应用程序无法访问。	如果尚未创建相应的托管配置文件，则会启动配置文件创建向导。	
Chrome（托管配置文件）	根据 Secure Private Access 配置，允许或拒绝应用程序。	枚举的应用程序在新选项卡中启动。	不适用
Citrix Workspace 应用程序	不适用	不适用	应用程序在商店中枚举。
			应用程序在相应的 Chrome 托管配置文件中启动。
			如果尚未创建相应的托管配置文件，则会

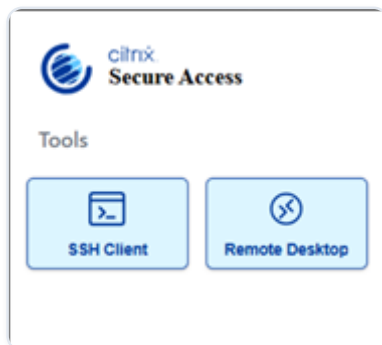
	直接	从 WEB 浏览器访问应用商店 URL	CITRIX WORKSPACE 应用程序
			启动配置文件创建向导。

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 浏览器安全地无客户端访问内部和外部应用程序。它结合了 Citrix Secure Private Access 和 Chrome Enterprise 的功能，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。



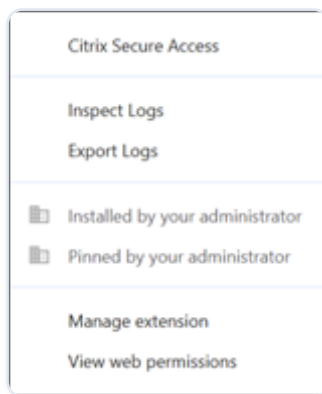
Secure Access 扩展程序日志

Secure Access 浏览器扩展程序日志对于监视和故障排除至关重要。出现问题时，最终用户可以查看和下载日志，以便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。



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**。

Secure Private Access > Policies > Browser Policies

Browser Policies

Configure security policies for browser-based access to web applications and virtual desktops. Each policy can be enabled independently and configured with specific conditions. Platform support varies by policy. [See supported platforms](#)

Card viewTable view

Search policies by name, description, or status

Anti-keylogging

Protect against keylogger attacks by preventing unauthorized keystroke capture in web applications.

Status: DisabledManage

Browser session reauthentication

Control how often end users must reauthenticate their Chrome browser session. Configure the reauthentication interval and warning banner period so end users have time to save their work before they're signed out of their Chrome profile and prompted to log back in.

Status: DisabledManage

Clipboard container

Control clipboard data transfer between web applications and virtual desktops.

Status: DisabledManage

DNS suffix

Configure DNS suffix for hostname resolution within the browser environment.

Status: DisabledManage

Session recording

Records supported browser sessions for auditing and investigation purposes.

Status: DisabledManage

Remote Desktop (RDP)

Make Remote Desktop (RDP) available to users in the Citrix Secure Access extension. Users matching the rule conditions will see RDP as an available tool in the extension.

Status: DisabledManage

SSH connections

Make SSH connections available to users in the Citrix Secure Access extension. Users matching the rule conditions will see SSH as an available tool in the extension.

Status: DisabledManage

3. 为策略添加规则。

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

88

Anti-keylogging

Protect against keylogger attacks by preventing unauthorized keystroke capture in web applications. This policy requires Device Posture Service to be configured. [Learn how to install Citrix Workspace App and Endpoint Analysis](#)

Enable Anti-keylogging ☒

i Policy behavior: When a user matches multiple rules, only the first matching rule applies. Rules are evaluated in priority order from top to bottom.

Search rules by name

Add Rule

Priority Order	Rule Name	Conditions	Status	Actions
1	AntiKeylog_contractors	1	☒	...

Showing 1-1 of 1 items Page 1 of 1 20 rows

Cancel **Save**

4. 选择必须评估策略的条件。

Edit Rule

1 Rule details

2 Conditions

3 Actions

4 Summary

Step 2: Conditions

Conditions ②

User:

Matches any of

* Ad

aaa.local

Enter name, user ID, or email address

Selected users/groups (1)

Filter by name

Remove selected (1)

Users / Groups	Action
☒ gwaasdevuser1 Email: gwaasdevuser1@.com IdP type: Ad OID: 4e337f9a-57ed164e Domain: .com ☒	☒ ☐

+ Add condition

Activate Windows
Go to Settings to activate Windows.

Cancel **Back** **Next**

Citrix Secure Access 浏览器策略支持混合部署和基于服务的 Secure Private Access 部署，并与 Chrome Enterprise Premium (CEP) 配合使用。

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，这些控件通过 Secure Private Access 和 Chrome Enterprise Premium 集成提供：

控件	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(/zh-cn/citrix-secure-private-access/secure-access-extension/spa-cep-clipboard-container.html)	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(/zh-cn/citrix-secure-private-access/secure-access-extension/spa-cep-dns-suffix.html)	自动将短内部 URL（例如“wiki/”）补全为完整地址。
会话录制(/zh-cn/citrix-secure-private-access/secure-access-extension/spa-cep-session-recording.html)	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(/zh-cn/citrix-secure-private-access/secure-access-extension/spa-cep-session-reauthentication.html)	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(/zh-cn/citrix-secure-private-access/secure-access-extension/spa-cep-ssh-access.html)	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)(/zh-cn/citrix-secure-private-access/secure-access-extension/spa-cep-rdp-access.html)	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

以下部分提供了有关用户和组的更多信息：

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**将其一并删除。

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**用户 > 读取和组 > 读取权限**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。

反键盘记录控制

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 浏览器扩展支持反键盘记录功能，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，它将只记录不可读的字符，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 会话不支持反键盘记录功能。

先决条件

在启用反键盘记录功能之前，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。

配置反键盘记录策略

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 **反键盘记录**，然后单击 **管理**。
4. 单击 **添加规则** 为用户添加规则以后用防键盘记录功能。
 - 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 **设备状态检查** 等条件。
 - c. 单击 **下一步**。
5. 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 > 防键盘记录** 选项卡中。

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。这提高了安全性，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 和 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），请启用以下功能：
 - **DaaS 跨剪贴板容器**功能。有关详细信息，请参阅 [DaaS 跨剪贴板容器](#)。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 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**，然后单击 **管理**。
4. 单击 **添加规则** 以添加 VDA 和浏览器之间剪贴板共享的规则。
 - 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. 单击 **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。

Edit Rule

Step 3: Actions

STORE

cepspastagingdemo.cloudburrito.com

cepspastagingdemo2.cloudburrito.com

Policy scope

☐ Apply to entire browser

☒ Apply to specific applications and URLs

Applications

Select application

URL or Domain

.cnn.com/

Copy from Virtual Apps & Desktops to Web Apps

Enable users to copy content from virtual apps and paste into web browsers or SaaS applications.

Policy scope

☐ Apply to entire browser

☒ Apply to specific applications and URLs

Applications

Select application

URL or Domain

https://www.w3schools.com/*

Cancel Back Next

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

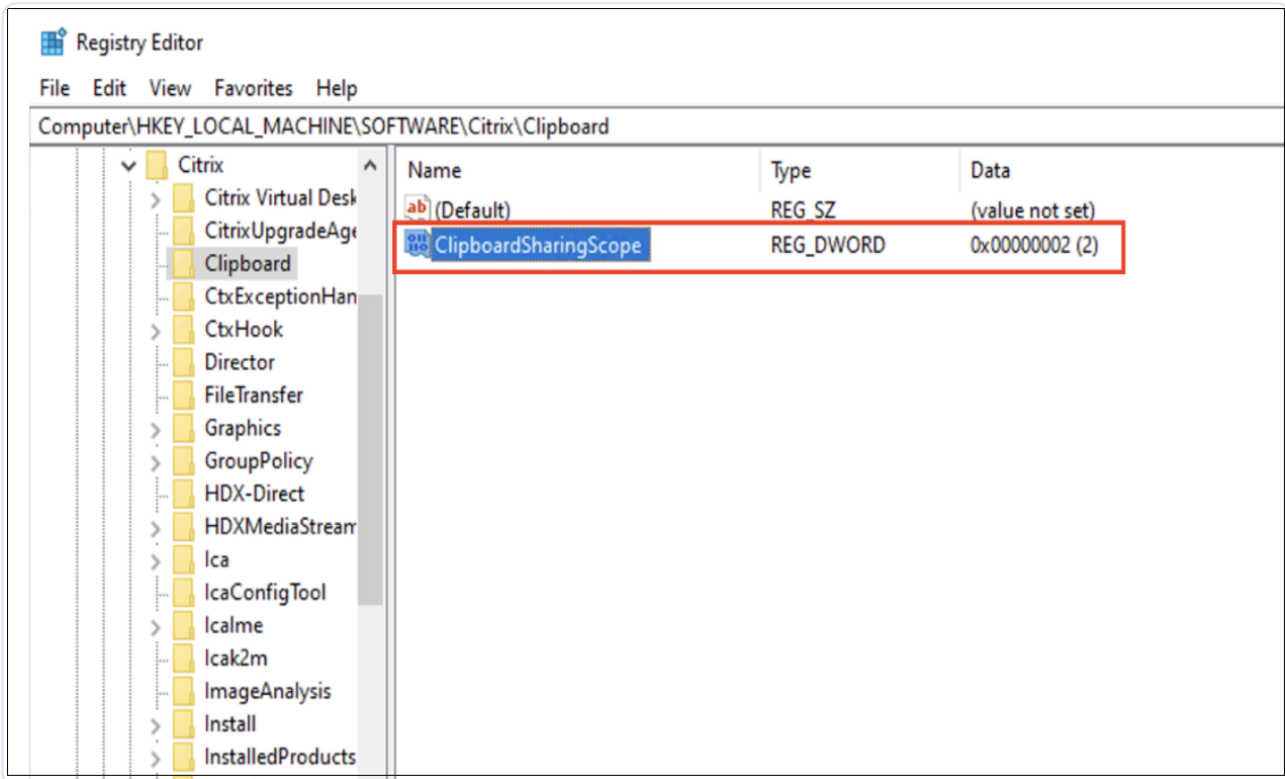
适用于 VDA 版本 2607：

请参阅[工作原理](#)。

适用于 VDA 版本 2507：

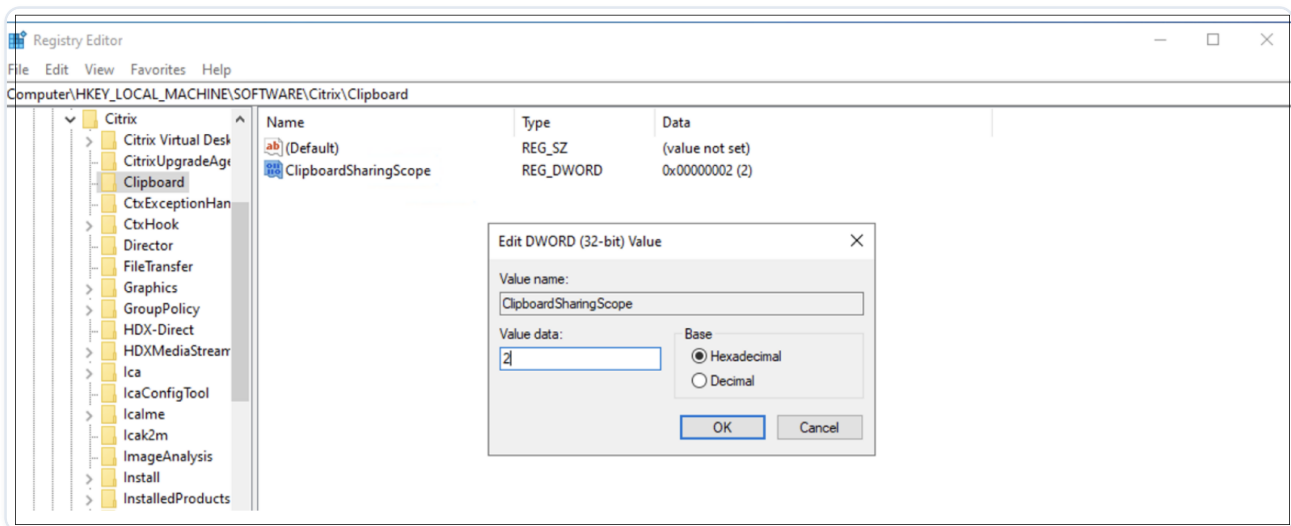
启用此 **剪贴板共享范围** 注册表项。

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。



`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 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 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	剪贴板数据 VDA 和 CEP 均可访问。客户端系统剪贴板无法访问剪贴板内容。

**注意：**

- 仅 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.

Web 应用程序的域后缀

在用户于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。

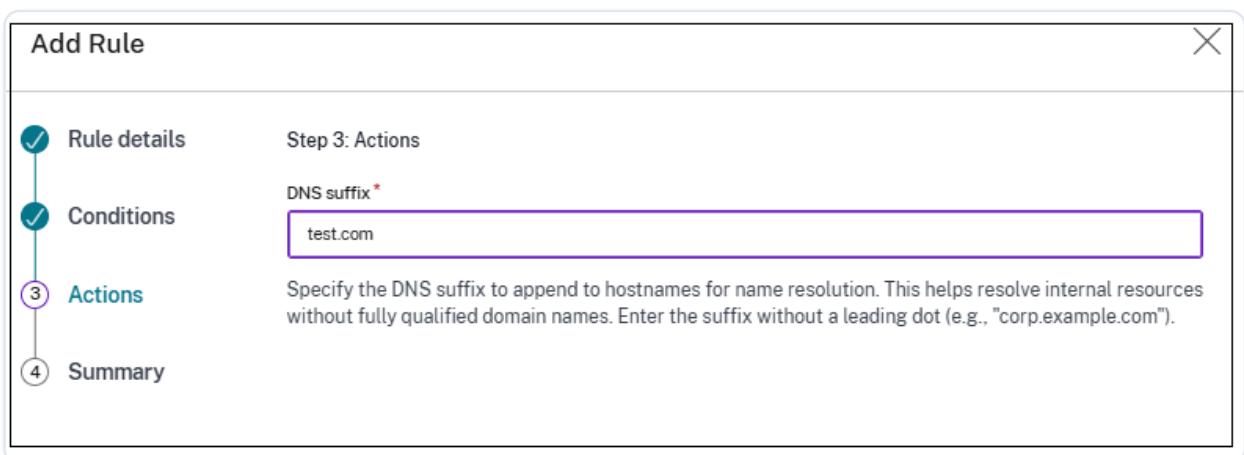
支持的平台： Windows 和 macOS。

先决条件

确保 Citrix Secure Access 与 Chrome Enterprise 的集成已配置。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**。
 - b. 根据您的要求（例如用户或组）选择条件。您还可以添加以下条件，例如 **地理位置**、**网络位置** 和 **设备状态检查**。
 - c. 单击 **下一步**。
 - d. 定义要用于访问的附加域。



Add Rule

Step 3: Actions

DNS suffix *

test.com

Specify the DNS suffix to append to hostnames for name resolution. This helps resolve internal resources without fully qualified domain names. Enter the suffix without a leading dot (e.g., "corp.example.com").

5. 单击 **保存**。

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

会话录制控制

会话录制可录制、编目和存档会话，以便进行检索和回放。

会话录制提供以下主要优势：

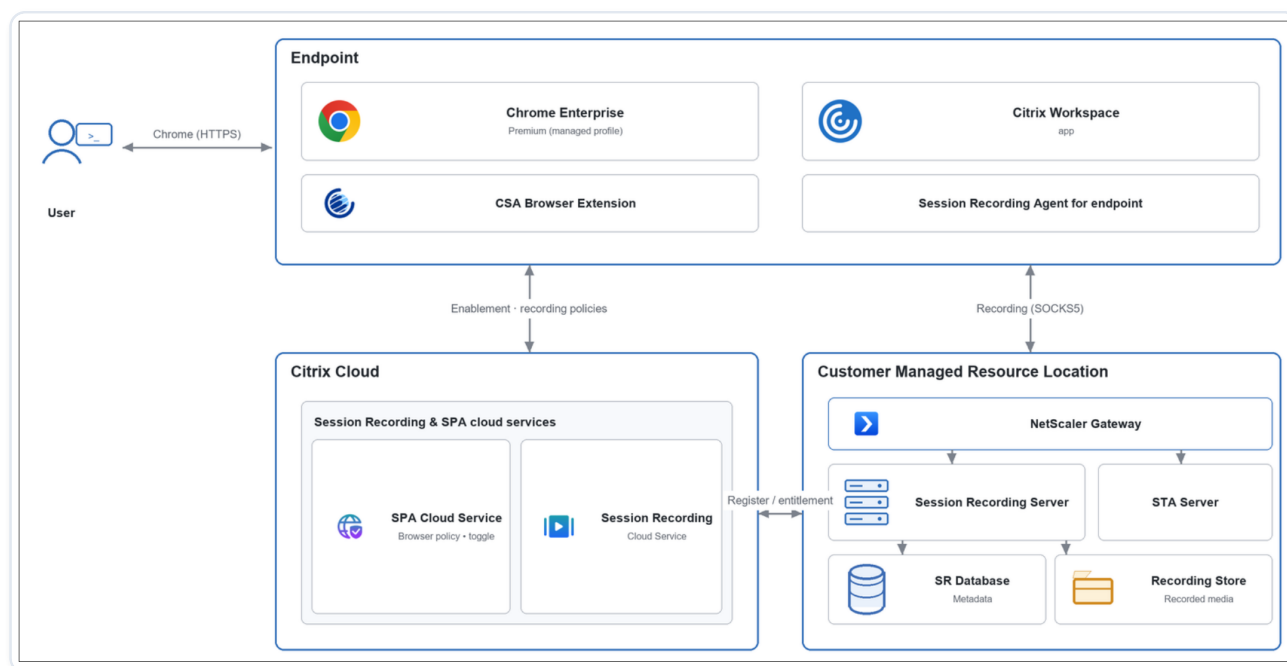
- 提供灵活的策略，可自动触发应用程序和桌面会话的录制。
- 使 IT 人员能够监控和检查用户活动，并支持内部控制以实现法规遵从性和安全监控。
- 通过加快问题识别和缩短解决时间来协助技术支持。

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层面：

- 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。



必备条件

- 适用于 Windows 2603.10 或更高版本的 Citrix Workspace 应用程序
- 端点分析 (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，带会话录制服务器 2511 或更高版本。有关详细信息，请参阅 [入门](#)。
- Windows 64 位或 32 位端点，具有以下组件：
 - Citrix 端点分析 (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](#) 中所述的步骤进行操作。

注意：

端点录制需要 NetScaler Gateway。它通过 STA 将录制流量路由到会话录制服务器，适用于两种 Secure Private Access 部署类型。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**。
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。

回放录制的会话

录制内容可在会话录制控制台中查看。

- 与用户的 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。
- 失焦的窗口或被其他应用程序遮挡的窗口仍将完整录制。
- 最小化的窗口和启用了防屏幕捕获的窗口在回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。
- **对齐区域。**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。

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。用户需要在配置的会话持续时间后重新进行身份验证，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 **设备状态检查** 等条件。
- c. 单击 **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，并以分钟、小时或天为单位进行配置。
 - **首次警告横幅时间**：在用户浏览器会话过期前向用户显示的、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，随后在会话结束时出现会话过期叠加层。
 - **身份提供程序域**：您的身份提供程序的完全限定域名 (FQDN)，以逗号分隔值表示。您可以指定 1 到 25 个域。会话横幅和阻止叠加层在 IdP 页面上被抑制，以确保身份验证流程不中断。这些域的 Cookie 在会话过期时会被清除，以确保旧会话被完全移除。支持通配符（例如，*.auth0.com）。

会话重新身份验证(/en-us/citrix-secure-private-access/media/spa-browser-reauthentication-settings.png)

5. 单击 **下一步**，然后单击 **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。

SSH 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 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 客户端的传统方法会使端点暴露于非托管环境，并且缺乏强大的数据丢失防护 (DLP) 强制执行，从而带来风险，使合规性变得具有挑战性。

SSH 会话现在在 Chrome 浏览器中启动，而不是在独立的 SSH 客户端中启动，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：

- **增强安全性：** 消除对非托管 SSH 客户端的依赖，降低安全风险。
- **简化访问：** 提供浏览器原生访问，无需额外安装软件。
- **合规性：** 直接在浏览器中强制执行企业 DLP 策略，有助于满足法规要求。
- **运营效率：** 降低与端点管理和客户端部署相关的 IT 开销。

用例

此功能支持多种用例，例如：

- **医疗自助服务终端：** 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。
- **IT 管理：** 允许管理员通过受管 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，同时不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，以后用对 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 SSH 访问

1. 登录到 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 SSH 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。
 - SSH 支持默认端口和非默认端口。
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 - [支持 TCP/UDP 应用程序](#)
- 混合部署 – [支持 TCP/UDP 应用程序](#)

配置 SSH 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 **SSH**，然后单击 **Manage**。
4. 单击 **添加规则**，为用户添加规则以启用 SSH。
5. 输入规则名称，然后单击 **下一步**。
6. 根据您的要求（例如用户或组）选择条件。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 > SSH** 选项卡中。

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。这种不足会增加安全风险，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 Chrome Enterprise Premium 集成的 Secure Private Access 设置，用于混合和云部署。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，帮助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 浏览器安全访问 RDP，提供一致且安全的体验。

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：** 允许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，而无需安装额外的软件。

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

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](#)。
- 最终用户已安装最新版 Google Chrome 浏览器并带有 Citrix Secure Access 浏览器扩展程序。
- 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 **应用程序 > 应用程序配置**，然后单击 **添加应用程序**。
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。

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（例如用户或组）选择条件。1. 您还可以添加诸如地理位置、网络位置和设备状态检查之类的条件。
7. 单击“下一步”。
8. 单击“保存”。

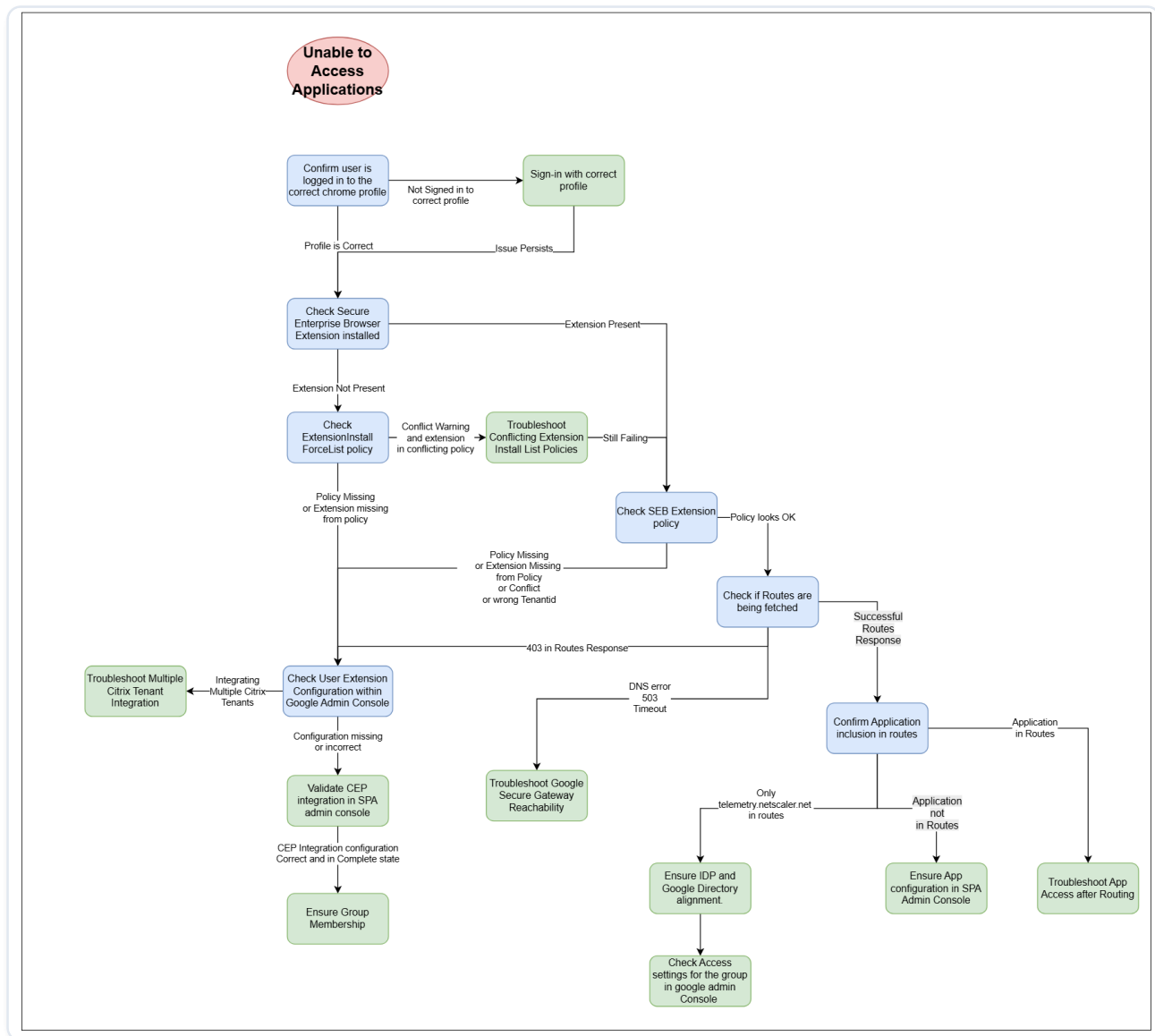
为防键盘记录策略配置的规则数量显示在“浏览器策略 > 远程桌面”选项卡中。

排查 CEP 集成问题

本文提供了一个故障排除工作流，适用于已完成 Chrome Enterprise Premium (CEP) 与 Citrix Secure Private Access 集成但无法访问应用程序的客户管理员。

基本假设：

- 客户管理员已完成与 Google Directory 的目录同步。
- 客户已成功完成 Secure Private Access 中的 Chrome Enterprise 入门。
- 应用程序和访问策略已在 Secure Private Access 管理控制台中配置，以允许用户或用户所属的组访问相关应用程序。
- 用户正在登录到已加入的域。
- 浏览器具有 Internet 连接。



用于 CEP 故障排除的诊断日志

为了简化调查，请在开立支持案例之前收集以下诊断信息，并在每次提交时附上。

1. 导出 Chrome 策略。
 - a. 打开 Chrome 并导航到 `chrome://policy/`。
 - b. 单击**更多操作**，然后选择**导出为 JSON**。
 - c. 将导出的文件附加到您的支持案例。
2. 为 Secure Enterprise Browser 扩展启用详细日志记录。
 - a. 单击 Secure Enterprise Browser 扩展旁边的省略号图标。
 - b. 单击选项，然后将 **日志级别** 设置为 **所有**。
 - c. 关闭并重新打开 Chrome。

- d. 返回扩展选项（省略号图标），然后单击 **下载日志**。
3. 收集扩展日志。
 - a. 关闭并重新打开 Chrome。
 - b. 重复步骤 2 以访问 **扩展** 选项，然后单击 **下载日志**。
 - c. 将下载的文件附加到您的支持案例。
 4. 捕获网络日志。
 - a. 在 Chrome 中，导航到 `chrome://net-export/` 并单击 **开始记录到磁盘**（默认文件名为 `chrome-net-export-log.json`）。
 - b. 访问一些 SaaS 和 Web 应用程序，然后返回 `chrome://net-export/` 并单击 **停止记录**。
 - c. 将生成的文件附加到您的支持案例。

确认用户已登录到正确的 Chrome 配置文件

如何检查： 在 Chrome 浏览器的右上角，单击个人资料图标。它必须显示您打算通过其访问应用程序的个人资料的正确用户和正确域。

此外，请确保配置文件未显示**已暂停**或**单击以登录**。如果显示，则必须重新进行身份验证。

- **配置文件正确且已通过身份验证：** 继续执行[检查 Secure Enterprise Browser 扩展是否已安装](#)。
- **配置文件不正确或未通过身份验证：** 使用正确的配置文件登录或重新进行身份验证。确保用户电子邮件的域后缀与安装了 Secure Private Access 的 Google 管理员帐户的域一致。

检查 Secure Enterprise Browser 扩展是否已安装

如何检查： 在 Chrome 浏览器的右上角，应该有一个绿色的盾牌图标，对应于 Secure Enterprise Browser 扩展。您可能需要单击拼图块才能看到所有扩展。

- **扩展存在：** 继续执行[检查 Secure Enterprise Browser 扩展策略](#)。
- **扩展不存在：** 继续执行[检查 ExtensionInstallForcelist 策略](#)。

检查 ExtensionInstallForcelist 策略

如何检查： 导航到 `chrome://policy`，然后在**Chrome 策略**下查找名为 **ExtensionInstallForcelist** 的策略。单击相应行末尾的**显示更多**以查看策略详细信息。

在此强制列表中，您应该会看到 ID 为 `ekajlcmdfcigmdbphhifahdfjbkciflj` 的扩展。这对应于 Secure Enterprise Browser 扩展。

您可能会看到一条警告，提示存在两个冲突的策略。

- **冲突警告和冲突策略中的扩展：** 继续执行[排查冲突的扩展安装列表策略](#)。
- **策略缺失：** 完全没有此策略表明用户未配置为使用 Secure Enterprise Browser，您必须[检查 Google 管理控制台中的用户扩展配置](#)。
- **策略中缺少扩展：** 继续执行[检查 Google 管理控制台中的用户扩展配置](#)。

排查冲突的扩展安装列表策略

冲突的策略不一定是支持 CEP 与 Secure Private Access 的障碍。但是，有效策略必须强制安装以下三个扩展：

- 安全企业浏览器 (`ekajlcmdfcigmdbphhifahdfjbkciflj`)
- Citrix 安全访问 (`loifegnemklkgbmonigcdkmniboieigl`)
- 端点验证 (`callobklhcbilhphinckomhgkigmfocg`)

要解决 Secure Private Access 的扩展策略冲突，请根据 [Chrome 策略层次结构指南](#) 执行以下步骤。

1. **识别冲突：** 导航到 `chrome://policy`。找到 **ExtensionInstallForcelist** 并检查**状态和来源**。
2. **分析优先级：** 请注意，机器级策略 (GPO) 通常会取代云/用户级策略。
3. **协调：** 确保最高优先级的策略包含所有三个必需的扩展 ID（如果包含其他扩展，则没关系）。或者，如果浏览器和配置文件由同一个 Google Workspace 组织管理，您可以使用策略合并功能。
4. **验证：** 单击**重新加载策略**。“适用于”和“级别”列必须确认所需的扩展是**强制性的**，并且在有效级别处于活动状态。

如果在更正扩展安装列表策略后问题仍然存在，请继续执行 [检查 Secure Enterprise Browser 扩展策略](#)。

检查 Secure Enterprise Browser 扩展策略

如何检查： 导航到 `chrome://policy` 并在 **Secure Enterprise Browser** 下查找名为 **securityGateway** 的策略。单击**显示更多**以显示完整的策略配置。其值应具有以下格式：

```
{  
  
  "authentication": {},  
  
  "context": {
```

```
    "resource": "projects/project-<tenant_id>-<random-hex-characters>/
locations/global/securityGateways/securitygateway-<tenant_id>-<random-hex-
characters>"

  },

  "externalHelper": {

    "id": "com.citrix.device_posture_context_provider",

    "metadata": {

      "action": "device/metadata",

      "input": [

        {

          "key": "tenantId",

          "stringValue": "<tenant_id>"

        }

      ]

    }

  },

  ...

}
```

确保 `tenant_id` 字段的值与您的 Citrix Cloud 租户 ID 对应。如果此值不同，则可能是第二个租户已配置为与此 Google 帐户集成。

- **策略缺失或为空：**策略完全缺失表明 Secure Enterprise Browser 扩展不仅由 Secure Private Access 配置，而且也由客户配置，并且用户正在从以前或手动配置中获取扩展的空配置。您必须 [检查 Google Admin Console 中的用户扩展配置](#)。

- **策略填充了错误的 Citrix 租户 ID：**如果策略存在但值与示例不符，则租户 ID 不同或存在两个冲突的策略。继续执行 [检查 Google Admin Console 中的用户扩展配置](#)。
- **策略看起来正确：**继续 [检查路由是否正在获取](#)。

检查 Google 管理控制台中的用户扩展配置

如何检查：导航到 <https://admin.google.com>。在此处，转到“**Chrome 浏览器 > 应用和扩展程序**”。在此视图中，您必须找到所有正在应用的策略配置。

单击“概览”选项卡（假设它存在），然后选择“**Secure Enterprise Browser**”应用。在左侧，“**安装策略**”下必须显示“**强制安装并固定在 \<primary domain\> 中**”，其中 \<primary domain\> 对应于您的 Google 管理控制台的顶级组织单位。

当点击查看扩展程序的“**部署设置**”时，查找“**扩展程序策略**”配置。这必须与 [检查 Secure Enterprise Browser 扩展策略](#) 部分中描述的内容一致。

- **单个策略看起来正确：**如果父 OU 的策略看起来正确，您必须确保您正在测试的用户属于相关帐户，并且在子 OU 或组级别没有其他配置可能覆盖父 OU 的策略。如果成员资格已确认但问题仍然存在，请联系 Citrix 支持。
- **策略缺失：**策略完全缺失表明此 Google 帐户未配置为使用 Secure Enterprise Browser，并且您必须 [在 Secure Private Access 管理控制台中验证 CEP 集成](#)。
- **多个策略 - 多个 Citrix 帐户：**如果您看到 Secure Enterprise Browser 扩展程序的多个配置，那么这可能是关联策略配置不正确的原因。将多个 Citrix 帐户关联到同一个 Google 帐户并非禁止，但可能会导致集成无法正常工作。
- **多个策略 - 单个 Citrix 帐户：**如果您只集成了一个 Citrix 租户，您必须确保组织中没有其他管理功能可能正在配置此扩展程序。如果您确信没有其他人为此扩展程序提供策略配置，您可以继续删除那些与您通过 Secure Private Access 管理控制台集成的 Citrix 租户不对应的策略配置。

如果您删除了多余的扩展程序配置，并且在重启浏览器后仍然无法访问您的应用程序，请联系 Citrix 支持。

检查路由是否正在获取

如何检查：导航到 <chrome://extensions/?options=ekajlcmdfcigmdbphhifahdfjbkciflj> 或右键单击 Secure Enterprise Browser 扩展程序并选择“**选项**”。

将日志级别设置为“**ALL**”并单击“**显示日志**”。日志显示后，关闭浏览器并重复此过程以转到日志页面。这可确保您已检索到故障排除所需的完整日志集。

在日志中，搜索包含以下内容的日志行：

```
Calling 'https://api.prod.securegateway.goog/api/v1/routes'
```

之后必须有如下响应：

```
[260220 17:07:51.64] [SG.ApiClient] [DEBUG] Response: {expirationTime:  
'2026-02-20T15:37:51Z', proxyUrl: 'https://api.prod.securegateway.goog', ...}
```

- **上下文路由在日志中显示 403 状态代码：**此 403 错误可能由 Zscaler、Umbrella 等拦截防火墙返回。
 - 在这种情况下，请确保根据[集成解决方案的先决条件](#)允许流向 Google Security Gateway 的流量。
 - 如果不是，则可能是用户配置文件存在身份验证问题，并且可能意味着 Secure Private Access 与 CEP 的集成不完整。请继续执行在 [Secure Private Access 管理控制台中验证 CEP 集成](#)。
- **上下文路由显示超时、DNS 错误或 503 错误：**请继续执行[排查 Google Secure Gateway 可达性问题](#)。
- **上下文路由显示成功 (200 OK)：**请继续执行[确认路由中包含应用程序](#)。

在 Secure Private Access 管理控制台中验证 CEP 集成

访问 Citrix Cloud 控制台的 Secure Private Access 中的[浏览器设置](#)部分。

在此部分中，验证以下内容：

- **Google Chrome 集成状态**必须显示为**完成**。如果发现失败，请确保已按照[文档](#)完成 CEP 集成的先决条件步骤，然后重试。如果问题仍然存在，请联系 Citrix 支持。
- **客户 ID**必须具有与您正在集成的 Google 帐户对应的值。您可以在 Google 管理控制台的[帐户 > 帐户设置](#)下找到该值。

如果上述所有值都正确，但您仍然无法在 Chrome 浏览器中获取正确的扩展程序配置，请联系 Citrix 支持。

排查 Google Secure Gateway 可达性问题

如何检查：复制 URL `https://api.prod.securegateway.goog/api/v1/routes` 并在浏览器地址栏中导航到此 URL。您必须收到 HTTP 401 错误响应。这是预期行为，表示可以成功建立与 Google Secure Gateway 的网络连接。

- **DNS 解析错误：**这表明您的公司可能设置了一些限制性 DNS 解析配置，阻止查找 Google 安全网关 FQDN。但是，这是使用此功能的先决条件，并且必须能够解析相应的 FQDN。

- **请求挂起或显示超时错误页面：** 这强烈表明浏览器和互联网之间的防火墙正在丢弃发往 Google 安全网关的流量。请遵循 (</zh-cn/citrix-secure-private-access/service/prerequisites-for-cep-spa-integration.html>) 以确保您的网络可以访问先决条件互联网位置。

如果您仍然没有收到正确的路由，请联系 Citrix 支持。

确认应用程序包含在路由中

成功的路由响应包括与您的 Secure Private Access 管理员配置的应用程序对应的 FQDN。例如：

```
[260318 06:42:38.99] [SG.ApiClient] [DEBUG] Response: {expirationTime: '2026-03-18T14:15:05Z', proxyUrl: 'https://via.prod.securegateway.goog', endpointMatchers: [{hostname: 'telemetry.netscalergateway.net'}, {hostname: 'www.workday.com'}, {hostname: '*.workday.com'}, {hostname: 'jira.internal.corp'}, {hostname: '*.jira.internal.corp'}]}
```

此行是否包含您尝试访问的应用程序？

- **路由响应中包含无法访问的应用程序：** 请继续执行 (#troubleshoot-routed-application-access)。
- **路由响应中仅包含 `telemetry.netscalergateway.net`：** 尝试配置其他应用程序和包含性应用程序策略。如果您仍然在路由中看不到它，这强烈表明组员资格存在问题，或者 Citrix 中配置的 IdP 与 Google Directory 之间的组不一致。请继续执行 (#ensure-idp-and-google-directory-alignment)。
- **路由响应中不包含无法访问的应用程序：** 这表明应用程序未在 Secure Private Access 管理控制台中正确配置。请验证应用程序是否存在并具有关联的策略（允许或拒绝访问）。如果您确定应用程序已配置但仍缺少上述路由，请联系 Citrix 支持。

排查路由应用程序访问问题

当尝试访问您的应用程序（显示在路由列表中）时，观察到的行为是什么？

- **您收到域名解析错误 (ERR_NAME_NOT_FOUND)**

这很可能表明应用程序未正确配置或未正确接收上下文路由。

- **显示“访问被拒绝”的米黄色页面**

这表明 Secure Private Access 控制台中的策略配置未设置为包含当前用户。

- **一个奶油黄色页面显示“哎呀！出错了。”**

此错误页面的最常见原因是连接器无法访问目标应用程序。在这种情况下，请根据 Citrix 文档排查连接器对内部应用程序的访问问题。常见问题包括：

- 内部 DNS 可达性
 - 后端服务已关闭
 - 防火墙规则
- 一个白色页面，以大红色字体显示“服务不可用”

这可能是一个暂时性错误，几分钟后可能会自行解决。

如果问题仍然存在，请联系 Citrix 支持。

- 超时

- 首先，通过在 Chrome 地址栏中输入 `via.prod.securegateway.goog` 来验证其是否可达。您必须收到 401 响应。如果超时，则表示中间防火墙或代理正在阻止访问，必须先解决此问题才能访问应用程序。
- 应用程序超时的另一个潜在原因是防火墙阻止了流向互联网以及特别是 Google 安全网关的流量。这在客户需要显式代理才能访问互联网的场景中很常见。Secure Private Access 与 Chrome Enterprise Premium 的集成不支持此代理配置。

- 证书错误

应用程序可能正在使用私有 CA 证书，因此浏览器可能会抛出“不受信任的证书错误”。通过 Chrome Enterprise Premium 配置，客户可以将其受信任的根 CA 推送到浏览器。有关详细信息，请参阅 [使用 Chrome Enterprise Premium 管理根证书配置](#)。

确保 IdP 和 Google Directory 对齐

对于 Secure Private Access 与 Chrome Enterprise Premium 的集成，您的目录与 Google Directory 的同步必须遵循 [集成解决方案的先决条件](#) 中涵盖的一些规范。

如果用户和用户组电子邮件正确，并且与源目录中的配置一致，请继续检查 Google 管理控制台中组的访问设置(#check-access-settings-for-the-group-in-google-admin-console)。

检查 Google 管理控制台中组的访问设置

在 Google 管理控制台中，导航到 **目录 > 群组** 并选择您已配置访问策略但应用程序未加载的群组。

在那里，选择 **访问设置** 并确保 **谁可以查看成员** 行中的 **群组成员** 选项已启用。此配置必须应用于您希望在 Secure Private Access 中创建策略的所有群组。

如果此选项已启用，请联系 Citrix 支持。

CEP 集成中的已知问题

以下是 Secure Private Access 与 Chrome Enterprise Premium 集成中存在的已知问题。

Secure Private Access 用户界面

- **问题：** 会话策略配置目前只允许用户添加两个模拟条件，尽管有三个条件可用。这限制了策略创建的灵活性。

解决方法： 创建两个独立的会话策略；一个包含两个模拟条件，另一个包含剩余的条件。

- **问题：** TCP/UDP 服务器到客户端配置选项目前并非在所有客户环境的应用配置 UI 中都可用。这限制了定义服务器到客户端流量行为的能力。

自适应访问策略配置

- **问题：** 当规则中指定 Okta 组时，访问策略创建失败。此问题仅影响 Okta 目录中存在的组。

解决方法： 您可以将 Okta 用作身份提供程序，但不能用作目录。要将 Okta 用作 IdP，您必须首先将本地 AD 与 Okta 集成。有关详细信息，请参阅 [将 Okta 作为身份提供程序连接到 Citrix Cloud](#)。

Google Chrome 浏览器

- **问题：** 如果 Google 配置文件选择器处于打开状态，并且用户尝试从 CWA 或非 Chrome 浏览器启动应用程序，而此时没有现有配置文件，则不会触发配置文件创建工作流。

解决方法： 关闭配置文件选择器并重新启动应用程序。

- **问题：** 使用托管 Chrome 配置文件登录 CWA 并启动应用程序后，用户不会在配置文件创建后跳转到原始内部应用程序 URL。

解决方法： 配置文件创建后，重新启动应用程序。

- **问题：** 从 Google 管理控制台同步群组时，群组中的用户不会自动同步。在同步期间，`whoCanViewGroupMembership` 设置被显式覆盖为 `ALL_MANAGERS_CAN_VIEW`。因此，受限可见性是预期行为。

解决方法： 在 Google 管理控制台上手动更新 Google 群组权限或通过 API 进行更新。有关详细信息，请参阅 [网址](https://developers.google.com/workspace/admin/groups-settings/manage)。

- **问题：** 用户通过托管 Chrome 配置文件访问已发布的 SaaS/Web 应用程序时，系统会通过代理弹出窗口提示用户使用用户名和密码进行身份验证。这通常发生在一段时间不活动之后：

原因：

- 代理令牌不可用，或者代理令牌可用但随后已过期。
- 由于延迟初始化，SEB 扩展需要重新初始化。

解决方法： 在新窗口中重新启动 Chrome 会话。

- **问题：** 用户通过托管 Chrome 配置文件或 Citrix Workspace 应用程序访问外部 SaaS 应用程序时，可能会遇到间歇性“服务不可用”错误。此问题是由于 Google 基础设施上未解决的后端问题造成的。

解决方法： 联系 Google 团队寻求支持。

应用程序配置和管理

Citrix Secure Private Access 提供了一个用户友好、集中式的平台，用于配置和管理对各种应用程序（SaaS/Web 和 TCP/UDP）的访问。Secure Private Access 控制台通过为各种配置任务提供单一控制点来简化管理。管理员可以使用配置向导，在同一控制台中轻松设置自适应身份验证、配置应用程序、定义访问策略以控制用户权限，并实施安全限制以保护敏感数据。此外，Secure Private Access 支持对企业 Web 应用程序进行无代理访问，无需安装 VPN 客户端。

有关详细信息，请参阅以下主题：

- [配置企业 Web 或 SaaS 应用程序](#)
- [配置 TCP/UDP 应用程序](#)
- [配置 TCP/UDP - 服务器到客户端应用程序](#)

配置企业 Web 或 SaaS 应用程序

设置 Secure Private Access 后，您可以从管理控制台配置应用程序和访问策略。

1. 在管理控制台中，单击“**应用程序**”。
2. 单击“**添加应用程序**”。
3. 选择应用程序所在的位置。
 - 对于外部应用程序，选择“**在我的公司网络外部**”。
 - 对于内部应用程序，选择“**在我的公司网络内部**”。
4. 在“应用程序详细信息”部分输入以下详细信息，然后单击“**下一步**”。
 - “**应用程序类型**” - 选择应用程序类型。

“

注意：

对于 Chrome Enterprise Premium (CEP)，仅支持 HTTPS 企业 Web 和 SaaS 应用程序。不支持 HTTP 企业 Web 和 SaaS 应用程序。

- **“应用程序名称”** – 应用程序的名称。
- **“应用程序描述”** - 应用程序的简要说明。此说明将显示给用户在其商店中。您还可以按 `KEYWORDS: <keyword_name>` 格式输入应用程序的关键字。您可以使用关键字来筛选应用程序。
- **“应用程序类别”** - 添加您发布的应用程序必须在商店 UI 中显示的类别和子类别名称（如果适用）。您可以为每个应用程序添加新类别，或使用商店 UI 中的现有类别。为 Web 或 SaaS 应用程序指定类别后，该应用程序将显示在商店 UI 中的特定类别下。
 - 类别/子类别可由管理员配置，管理员可以为每个应用程序添加新类别。
 - 类别/子类别名称必须用反斜杠分隔。例如，Business And Productivity\Engineering。此外，此字段区分大小写。管理员必须确保他们定义了正确的类别。如果商店 UI 中的名称与在“应用程序类别”字段中输入的类别名称不匹配，则该类别将作为新类别列出。

例如，如果您在“应用程序类别”字段中错误地将 Business and Productivity 类别输入为 Business And productivity，则除了 Business And Productivity 类别之外，商店 UI 中还会列出一个名为 Business and productivity 的新类别。
- **应用程序图标** – 单击**更改图标**以更改应用程序图标。图标文件大小必须为 128x128 像素，并且仅支持 ICO 和 PNG 格式。如果您不更改图标，则会显示默认图标。
- **不向用户显示应用程序** - 如果您不想向用户显示应用程序，请选择此选项。
- **URL** – 应用程序的 URL。
- **相关域** – 相关域根据应用程序 URL 自动填充。管理员可以添加更多相关的内部或外部域。

注意：

- 确保一个应用程序的相关域不与另一个应用程序的相关域重叠。如果发生这种情况，请从所有应用程序中删除相关域，并使用此域创建一个新应用程序，然后在访问策略中相应地设置访问权限。您还可以考虑是否要在 StoreFront™ 中显示此应用程序或将其隐藏。您可以在发布应用程序时使用**不向用户显示应用程序**选项在 StoreFront 中隐藏应用程序。
- 同样，已发布的应用程序的 URL 不得添加为另一个应用程序的相关域。
- 有关更多详细信息，请参阅[Web 和 SaaS 应用程序配置的最佳实践](#)。

- **自动将应用程序添加到收藏夹** – 单击此选项可将应用程序作为收藏夹应用程序添加到 Citrix Workspace 应用程序中。选择此选项后，Citrix Workspace 应用程序中应用程序的左上角会显示一个带挂锁的星形图标。
 - **允许用户从收藏夹中删除** – 单击此选项可允许应用程序订阅者从 Citrix Workspace 应用程序中的收藏夹应用程序列表中删除应用程序。选择此选项后，Citrix Workspace 应用程序中应用程序的左上角会显示一个黄色星形图标。
 - **不允许用户从收藏夹中删除** – 单击此选项可阻止订阅者从 Citrix Workspace 应用程序中的收藏夹应用程序列表中删除应用程序。

如果您从 Secure Private Access 控制台中删除了标记为收藏夹的应用程序，则必须从其商店的收藏夹列表中手动删除这些应用程序。如果从 Secure Private Access 控制台中删除了应用程序，则这些应用程序不会自动从商店中删除。

- **应用程序连接** - Web 应用程序选择**内部**，SaaS 应用程序选择**外部**。

5. 点击“**保存**”，然后点击“**完成**”。

您可以在“**设置 > 应用程序域**”中查看所有已配置的应用程序域。有关更多详细信息，请参阅[安装后管理设置](#)。

删除应用程序时自动清理路由条目

配置应用程序时，其目标（FQDN 或应用程序域）会添加到路由表中，Secure Private Access 使用该表进行路由决策。删除应用程序时，Secure Private Access 会根据以下规则清理路由条目：

- **未引用的条目将被删除** - 如果与已删除应用程序关联的路由条目（FQDN 或应用程序域）未被任何其他应用程序引用，Secure Private Access 将自动将其从路由表中删除。

- **共享条目将保留** - 如果路由条目被多个应用程序使用，删除其中一个应用程序不会删除共享条目。只要至少有一个活动应用程序引用该条目，该条目就会保留在路由表中。
- **不追溯删除** - 路由条目仅作为应用程序删除的一部分进行评估和删除。除非确认现有条目未被任何应用程序使用，否则不会追溯删除。

注意：

- 当从“应用程序”页面（使用省略号 (...) 菜单）删除应用程序时，清理会自动运行。无需管理员操作。
- 由于共享路由条目已保留，删除应用程序不会中断对共享相同目标的其他应用程序的访问。

后续步骤

为应用程序配置访问策略。

使用 HAR 文件发现相关域

Secure Private Access 允许您上传 HTTP Archive (HAR) 文件，以自动发现应用程序访问的域。您可以查看发现的域，并选择要添加到应用程序相关域配置中的域。这通过减少手动识别和配置相关域的需要，简化了应用程序的入职过程。

以前，管理员必须提前了解应用程序的所有相关域，或者在用户遇到被阻止的 URL 时被动地发现它们。由于默认情况下会阻止除已配置 URL 之外的所有 URL，因此这种被动方法会导致糟糕的用户体验。Secure Private Access 无法识别应用程序内部或嵌入的 URL。

示例

假设您正在配置一个主域为 `example.com` 的应用程序。在使用该应用程序时，浏览器还会访问其他几个域。例如：

- `api.example.com` – 处理应用程序的后端 API 调用。
- `auth.example.com` – 管理登录和身份验证。
- `cdn.example.com` – 提供静态内容，例如图像、脚本和样式表。
- `login.microsoftonline.com` – 提供第三方身份验证。
- `player.vimeo.com` – 加载嵌入式视频内容。

无需手动识别每个域：

1. 在使用应用程序时捕获 HAR 文件。
2. 将 HAR 文件导入 Secure Private Access。
3. 查看 Secure Private Access 发现的域。例如，导入可能会显示 `api.example.com`、`auth.example.com` 和 `cdn.example.com` 作为必需域，以及您可以选择排除的 `player.vimeo.com` 等域。
4. 选择应用程序所需的域。
5. 根据需要配置路由和资源位置。

这提供了一种更快的方法来识别和配置应用程序连接所需的域。

先决条件

确保在访问 Web 或 SaaS 应用程序时已捕获 HAR 文件。HAR 文件必须包含网络请求信息，并且大小必须为 50 MB 或更小。

导入 HAR 文件

1. 在 Secure Private Access 管理门户中，打开要配置的 Web 或 SaaS 应用程序。
2. 转到 **应用程序连接**，然后单击 **导入 HAR**。

Add an app

App Connectivity

URL *

Routing Type *

Primary Resource Location * ?

Secondary Resource Location (optional) ?

● 2 connectors are available [Refresh](#)

Related Domains
 [Add](#)

[Import HAR](#)

Search related domains

☐	Related Domains	Routing Type	Primary Resource Location	Available Connectors/Gatew...	Actions
☐	*.wikipedia.org ⚠	External via Google Secure C			Edit Delete

Showing 1-1 of 1 items Page 1 of 1 5 rows

3. 将 HAR 文件拖放到导入窗口中，或从设备中选择文件。
4. Secure Private Access 分析 HAR 文件并显示从网络请求中识别的域。

Import HAR

cnn_domains_sample.har

File size: 8.30 KB
Importing 5 total rows

Extracted Websites (Domains):

☐	Domain Name
☐	www.cnn.com
☐	cdn.cnn.com
☐	api.cnn.com
☐	metrics.cnn.com
☐	edition.cnn.com

Showing 1-5 of 5 items Page of 1 10 rows

[Delete HAR file](#)

- 查看发现的域。
- 选择要添加到应用程序的域。
- 选择 **导入**。

所选域将添加到应用程序的 **相关域** 配置中。

Add an app

Routing Type
Primary Resource Location
Secondary Resource Location (optional)

Internal via Connector
spablr1
None

	Related Domains	Routing Type	Primary Resource Location	Available Connectors/Gatew...	Actions
☒	www.cnn.com	Internal via Connector	Spablr1	2	
☒	cdn.cnn.com	Internal via Connector	Spablr1	2	
☒	api.cnn.com	Internal via Connector	Spablr1	2	
☒	metrics.cnn.com	Internal via Connector	Spablr1	2	

Showing 1-4 of 4 items
Page 1 of 1
5 rows

☐ Maintain consistent connection
Use the same connector appliance for the entire length of the session while accessing the application.

注意：

在导入之前，请查看发现的域。HAR 文件可能包含应用程序连接不需要的域。

管理相关域

导入域后，您可以从“相关域”表中对其进行管理：

- **搜索域** – 使用搜索字段筛选表并快速查找特定域。
- **选择域** – 选择单个域，或使用表标题复选框选择多个域。此选择可用于同时对多个域执行操作。
- **编辑域配置** – 更新相关域的配置，包括路由类型、主资源位置和辅助资源位置。
- **批量编辑域** – 选择多个符合条件的域，并同时更新其路由和资源位置设置。批量编辑适用于适用的内部域。外部域可能不支持所有配置选项。
- **资源位置** – 配置相关域时，分配主资源位置以及（如适用）辅助资源位置。使用这些设置来定义 Secure Private Access 如何路由相关域流量以及使用哪些资源位置来提供连接。

验证和文件要求

HAR 导入功能在处理上传的文件之前会对其进行验证。

- 只能导入包含网络请求条目的有效 HAR 文件。
- 支持的最大文件大小为 **50 MB**。
- 域会自动从 HAR 文件中的 URL 中提取。

- 重复的域会自动移除。
- 域在添加到相关域配置之前会进行规范化。

配置 TCP/UDP 应用程序

在配置 TCP/UDP 应用程序之前，请参阅[系统要求](#)。

要从管理控制台配置 TCP/UDP 应用程序，请执行以下步骤：

1. 在管理控制台中，单击**应用程序**，然后单击**添加应用程序**。
2. 选择位置在**我的公司网络中**。
3. 输入以下详细信息：
 - **应用程序类型** – 选择 **TCP/UDP** 以启动与数据中心后端服务器的连接。
 - **应用程序名称** – 应用程序的名称。
 - **应用程序描述** – 您正在添加的应用程序的描述。此字段是可选的。
 - **目标** – 位于数据中心的后端计算机的 IP 地址或 FQDN。可以按如下方式指定一个或多个目标。
 - **IP 地址 v4**
 - **IP 地址范围** – 示例：10.68.90.10-10.68.90.99
 - **CIDR** – 示例：10.106.90.0/24
 - **计算机的 FQDN 或域名** – 单个或通配符域。示例：ex.destination.domain.com, *.domain.com

注意：

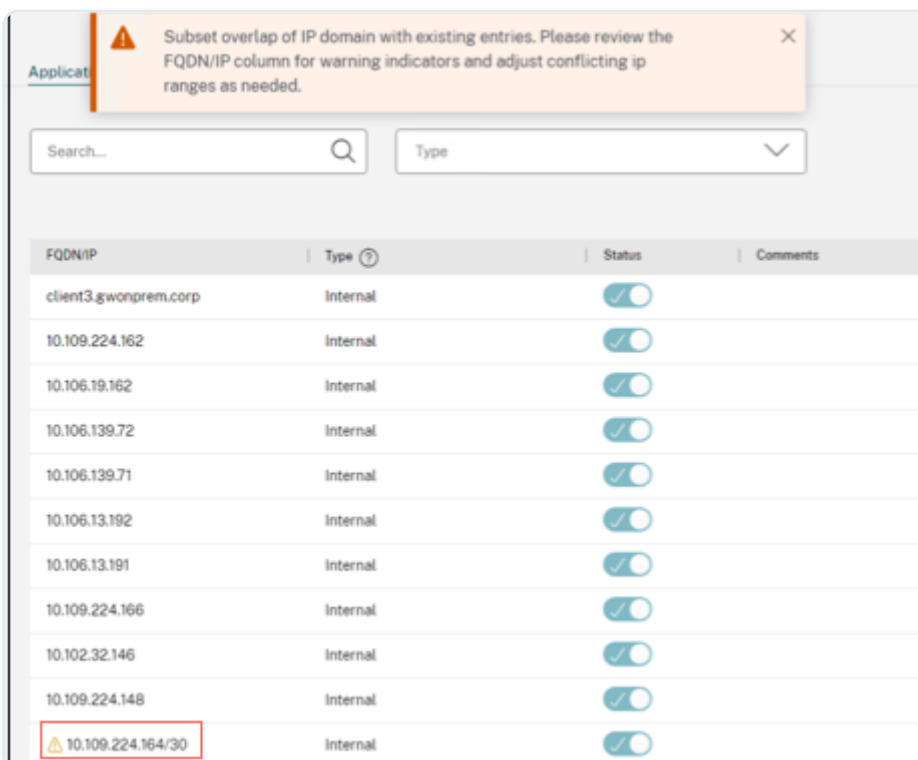
- 最终用户可以使用 FQDN 访问应用程序，即使管理员使用 IP 地址配置了应用程序。这是可能的，因为 Citrix Secure Access™ 客户端可以将 FQDN 解析为真实的 IP 地址。

下表提供了各种目标以及如何使用这些目标访问应用程序的示例：

目标输入	如何访问应用程序
10.10.10.1-10.10.10.100	最终用户应仅通过此范围内的 IP 地址访问应用程序。

目标输入	如何访问应用程序
10.10.10.0/24	最终用户应仅通过在 IP CIDR 中配置的 IP 地址访问应用程序。
10.10.10.101	最终用户应仅通过 10.10.10.101 访问应用程序
.info.citrix.com	最终用户应访问 info.citrix.com 的子域以及 info.citrix.com（父域）。例如，info.citrix.com, sub1.info.citrix.com, level1.sub1.info.citrix.com 注意： 通配符必须始终是域的起始字符，并且只允许一个。
info.citrix.com	最终用户应仅访问 info.citrix.com，而不访问任何子域。例如，sub1.info.citrix.com 不可访问。

目标 IP 地址在所有资源位置中必须是唯一的。如果存在冲突配置，在“应用程序域”表中，特定 IP 地址旁边会显示一个警告符号 (设置 > 应用程序域)。



- **端口** – 应用程序运行的目标端口。管理员可以为每个目标配置多个端口或端口范围。

下表提供了可为目标配置的端口示例。

端口输入	描述
*	默认情况下，端口字段设置为 <code>"*"</code> （任意端口）。目标支持 1 到 65535 的端口号。
1300–2400	目标支持 1300 到 2400 的端口号。
38389	目标仅支持端口号 38389。
22,345,5678	目标支持端口 22、345、5678。
1300–2400, 42000-43000,22,443	目标支持 1300 到 2400、42000 到 43000 的端口号范围以及端口 22 和 443。

注意：

通配符端口 (*) 不能与端口号或范围共存。

- 协议 – TCP/UDP

4. 应用程序连接：定义应用程序流量的路由方式。

- **内部：** DNS 解析通过远程 DNS 服务器完成。

默认情况下，所有标记为**内部**的域流量都会被拦截并通过 NetScaler Gateway 隧道传输。例如，如果 `.example.net` 的连接设置为**内部**，则其所有相关域/子域（例如 `code.example.net`、`test.example.net`、`123.example.net`）都将被拦截并通过 NetScaler Gateway 隧道传输。

- **外部：** DNS 解析通过本地 DNS 服务器完成。

当相关域/子域被标记为**外部**时，流向该域的流量不会被拦截并通过 NetScaler Gateway 隧道传输。例如，如果 `code.example.net` 的连接设置为**外部**，则流向此域的流量将直接通过互联网路由，而流向子域（例如 `text.example.net` 和 `123.example.net`）的流量将通过 NetScaler Gateway 隧道传输。

5. 单击**添加**以相应地添加其他目标或服务器。

6. 单击**保存**。应用程序将添加到**应用程序配置**页面。配置应用程序后，您可以从**应用程序**页面编辑或删除应用程序。为此，请单击应用程序旁边的省略号按钮并相应地选择操作。

- 编辑应用程序
- 删除

后续步骤

配置应用程序的访问策略。

配置 TCP/UDP - 服务器到客户端应用程序

TCP/UDP - 服务器到客户端应用程序类型可用于支持以下功能：

- 使用 Microsoft Endpoint Configuration Manager 或类似解决方案进行软件分发
- 使用 GPO Push 在托管设备上执行远程策略更新
- 远程协助以排查和调试用户工作站。

先决条件：

- Secure Private Access 设置已完成。
- 客户端版本满足以下要求：
 - Windows - 24.6.1.18 及更高版本
 - macOS - 24.06.2 及更高版本
- 内网 IP 地址已在 NetScaler® Gateway 上配置，并绑定到相应的 VPN 虚拟服务器。请参考以下示例命令：

```
set vpn sessionAction ns_default_vpn_session_profile_spa_tcp_udp_apps -useMIP  
NS -useIIP NOSPILLOVER
```

(用户可以选择使用 `-useMIP NS -useIIP NOSPILLOVER` 创建 VPN 会话配置文件和会话操作)

绑定 vpn vserver `<spa vserver name>` -intranetIP `<IP address>`

执行以下步骤以从管理控制台配置 TCP/UDP 应用程序：

1. 在管理控制台中，单击**应用程序**，然后单击**添加应用程序**。
2. 选择位置**我的公司网络内部**。
3. 输入以下详细信息：
 - **应用程序类型** – 选择**TCP/UDP - 服务器到客户端**。

- **应用程序名称** – 应用程序的名称。
- **应用程序描述** – 您正在添加的应用程序的描述。此字段是可选的。
- **服务器** - 获授权与客户端建立连接的应用程序服务器的详细信息。您可以输入 IP 地址、IP 地址范围或 CIDR。
- **端口** – 客户端端口号。
- **协议** – TCP/UDP。

4. 单击**添加**以添加其他服务器。

5. 单击**保存**。应用程序将添加到**应用程序配置**页面。配置应用程序后，您可以从**应用程序**页面编辑或删除应用程序。为此，请单击应用程序行中的省略号按钮并相应地选择操作。

- **编辑应用程序**
- **删除**

重要提示：

添加用于服务器-客户端通信的应用程序后，在 NetScaler Gateway 上配置的内部网 IP 地址范围必须添加为 TCP/UDP 应用程序，以后用服务器-客户端和客户端-客户端通信。

内网 IP 地址(/en-us/citrix-secure-private-access/media/spaop-tcp-upd-intranet-ip-app.png)

编辑应用程序

1. 在安全私有访问管理控制台中，单击**应用程序**。
2. 单击要修改的应用程序所在行中的省略号按钮，然后单击**编辑应用程序**。
3. 编辑应用程序详细信息。
4. 单击**保存**。

后续步骤

[配置应用程序的访问策略。](#)

访问策略配置和管理

在当今瞬息万变的形势下，应用程序安全对任何企业都至关重要。制定上下文感知的安全决策，然后启用对应用程序的访问，可以降低相关风险，同时允许用户访问。

Citrix Secure Private Access™ 自适应访问功能提供了一种全面的零信任访问方法，可为应用程序提供安全访问。自适应访问使管理员能够根据上下文为用户提供对应用程序的精细访问。

Secure Private Access 中的访问策略允许您根据用户或用户设备的上下文启用或禁用对应用程序的访问。

有关详细信息，请参阅以下主题：

- [配置应用程序的访问策略](#)
- [策略条件](#)
- [配置会话策略](#)
- [设备证书注册](#)

配置应用程序的访问策略

Secure Private Access 中的访问策略允许您根据用户或用户设备的上下文启用或禁用对应用程序的访问。

访问限制必须通过 Google 管理控制台配置，而不是在 Secure Private Access 界面中配置。

规则在 **Google 管理控制台 > 规则** 中配置。这些规则是与 DLP 相关的高级设置，例如添加水印、阻止下载包含社会安全号码的文件以及 URL 过滤。

有关在 Google 管理控制台中为 Google Chrome 创建策略和规则的详细信息，请参阅以下主题：

- [为 Chrome Enterprise 设置 Chrome Enterprise 连接器策略](#)
- [数据保护规则](#)

配置访问策略

1. 在管理控制台中，单击 **访问策略**。
2. 单击 **创建策略**。

3. 在 **创建访问策略** 页面中，选择以下选项之一：

- **用户/用户组**
- **计算机/计算机组**

应用程序访问规则根据访问策略中的选择，基于用户或计算机的上下文强制执行。

您可以选择 **计算机/计算机组** 以后用 Always On 连接。对于 Always On 连接，您必须已注册设备证书。有关详细信息，请参阅 [设备证书注册配置](#)。

有关计算机隧道的更多信息，请参阅 [Always On VPN before Windows Logon](#)。

4. a. 在 **策略名称** 中，输入策略的名称。

5. 在 **应用程序** 中，选择要强制执行访问策略的应用程序。

6. 在 **用户条件** 中 – 根据必须允许或拒绝应用程序访问的条件以及用户或用户组进行选择。

- **匹配以下任意项**：仅允许与字段中列出的任何名称匹配的用户或组访问。
- **不匹配任何项**：除字段中列出的用户或组外，所有用户或组都允许访问。

您可以按显示名称、电子邮件 ID 或用户主体名称搜索用户。此搜索选项允许管理员准确识别并授予正确用户访问权限，即使他们有多个帐户。有关详细信息，请参阅 [Policy conditions](#)。

7. （可选）单击 + 以根据上下文添加多个条件。

当您根据上下文添加条件时，将对这些条件应用 AND 运算，并且仅当满足用户和可选的基于上下文的条件时，才会评估策略。您可以根据上下文应用以下条件。

- **网络位置** - 选择用户访问应用程序所使用的条件和网络。
 - **匹配以下任意项**：仅允许从列出的任何网络位置访问应用程序的用户或用户组访问应用程序。
 - **不匹配任何项**：除来自列出的网络位置的用户或用户组外，所有用户或用户组都允许访问。
- **设备状态** - 选择用户设备必须满足才能访问应用程序的条件。

有关详细信息，请参阅 [Policy conditions](#)。

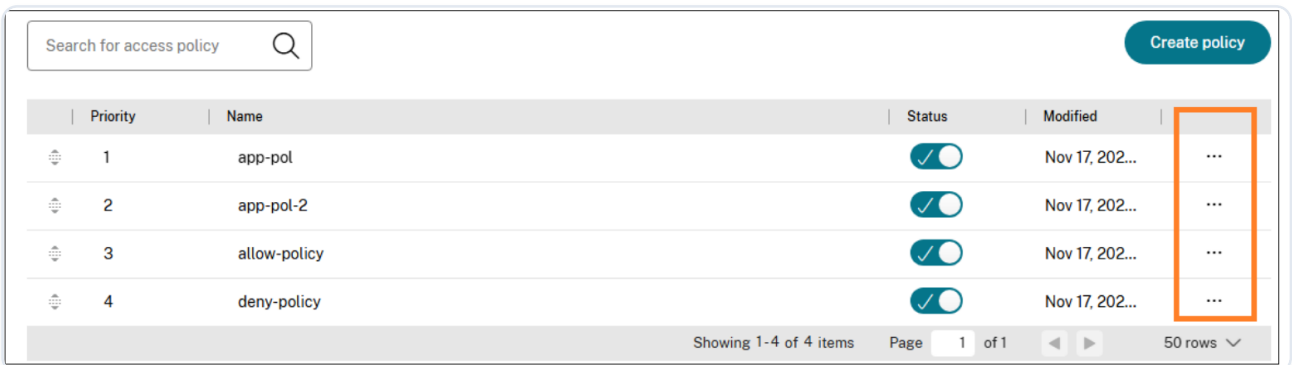
8. 在 **操作** 中，选择基于条件评估必须在应用程序上强制执行的以下操作之一。

- **允许访问**
- **拒绝访问**

9. 选择 **保存时启用策略**。如果您不选择此选项，则策略仅创建而不会在应用程序上强制执行。或者，您也可以通过使用切换开关从“访问策略”页面启用策略。

编辑访问策略

1. 在 Secure Private Access 管理控制台中，单击 **访问策略**。
2. 单击要修改的策略所在行中的省略号按钮，然后单击 **编辑访问策略**。
3. 编辑策略详细信息。
4. 单击 **更新**。



	Priority	Name	Status	Modified	
	1	app-pol		Nov 17, 202...	...
	2	app-pol-2		Nov 17, 202...	...
	3	allow-policy		Nov 17, 202...	...
	4	deny-policy		Nov 17, 202...	...

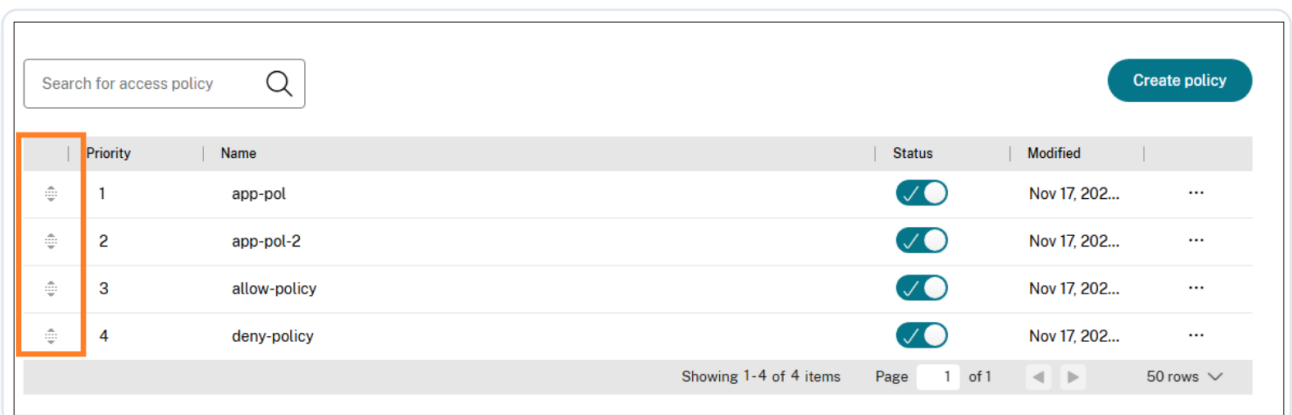
Showing 1-4 of 4 items Page 1 of 1 50 rows

更改访问策略优先级

创建访问策略后，默认情况下会为该访问策略分配一个优先级编号。您可以在“访问策略”主页上查看优先级。

优先级值越低，偏好越高，并首先进行评估。如果此策略不符合定义的条件，则会评估下一个优先级编号较低的策略，依此类推。

您可以通过使用 **优先级** 列中的上下箭头图标向上或向下移动策略来更改优先级顺序。



	Priority	Name	Status	Modified	
	1	app-pol		Nov 17, 202...	...
	2	app-pol-2		Nov 17, 202...	...
	3	allow-policy		Nov 17, 202...	...
	4	deny-policy		Nov 17, 202...	...

Showing 1-4 of 4 items Page 1 of 1 50 rows

后续步骤

- 从客户端计算机（Windows 和 macOS）验证您的配置。

- 对于 TCP/UDP 应用程序，通过登录 Citrix Secure Access 客户端，从客户端计算机（Windows 和 macOS）验证您的配置。

示例配置验证

策略条件

以下部分提供了有关策略条件的更多信息。

用户和用户组

用户条件定义了访问策略适用于哪些用户、组或身份属性。这些规则允许管理员在确定对应用程序的访问权限时包含或排除特定的身份。

用户条件包含三个主要组成部分：

匹配类型： 此下拉列表控制如何评估所选身份列表。

- **匹配以下任意项：**
 - 当策略必须仅适用于选定的用户或组时，请使用此项。
 - 如果列表中的至少一个身份匹配，则满足条件。
 - 作用类似于 IN 过滤器。
- **不匹配任何项**
 - 使用此项可将策略应用于除选定用户或组之外的所有人。
 - 仅当您选择的身份均不匹配时，才满足条件。
 - 作用类似于 NOT IN 过滤器。

Secure Private Access > Policies > Create/Edit Policy

Select User/User Groups or Machine/Machine Groups below to proceed

User/user groups

Policy name and applications

Policy name

Test

Applications

HelpCenter

Conditions

User conditions

Matches any of

gwonprem.corp

gwonprem.corp\Administrator - Administrator@gwonprem.corp

AND

Network location

Matches any of

fil_test

+ Create network location

域选择器：

域下拉列表按目录或身份源筛选身份。

- **身份选择器（用户电子邮件、组电子邮件）** - 此字段允许选择一个或多个身份，包括用户电子邮件和组电子邮件。

验证用户和组同步

在用户查找期间，管理员可以验证所选目录中的用户是否与 Google Directory 同步。仅当用户与 Google Directory 同步时，Secure Private Access 策略才能正确评估。否则，可能会出现以下警告：

- **租户帐户权限缺失：**

解决方法：

在 Google 管理控制台中，将**用户 > 读取**权限分配给租户服务帐户。Secure Private Access 需要这些权限来验证用户是否存在。

- **用户未同步：**

解决方法：

搜索或选定的用户未与 Google Directory 同步。在使用目录实体之前，请将其与 Google Directory 同步，然后再在 Secure Private Access 策略中使用。

注意：

此功能仅在 Google Chrome 集成成功完成后可用。

网络位置

网络位置服务 (NLS) 是一种策略条件，允许您根据用户的网络位置限制访问。管理员可以根据用户访问应用程序的位置配置访问策略。该位置可以是用户访问应用程序的国家/地区，也可以是用户的网络位置。网络位置使用 IP 地址范围或子网地址定义。

要根据位置配置访问策略，请执行以下操作：

1. 在“条件”部分下，单击“添加条件”。
2. 选择“网络位置”。

创建网络位置(/en-us/citrix-secure-private-access/media/spa-hybrid-create-network-location2.png)

如果您已配置多个网络位置，请根据您的要求选择以下其中一个。

- **匹配任意一个** – 网络位置与数据库中配置的任意一个网络位置匹配。
- **不匹配任何一个** – 网络位置与数据库中配置的任何网络位置都不匹配。

注意：

对于“网络位置”，您可以选择现有网络位置或创建网络位置。要创建新的网络位置，请单击“创建网络位置”。

- 确保您已从 **Citrix Cloud > StoreFront Cloud > Access > Adaptive Access** 启用自适应访问。否则，您将无法添加位置标签。有关详细信息，请参阅[启用自适应访问](#)。

您还可以从 Citrix Cloud 控制台创建网络位置。有关详细信息，请参阅[连接到 DaaS 资源](#)。

3. 完成策略配置。

配置会话策略

您可以使用会话策略，通过绕过 NetScaler Gateway 隧道来允许用户直接访问后端应用程序。

1. 导航到 **策略 > 会话策略**，然后单击 **创建会话策略**。

Secure Private Access > Policies > Create/Edit Session Policy

Policy name
hospital_policy

Description (optional)
Enter a description

Conditions ⓘ

User:
All users

AND

Network location Matches any of hospital_network1 ⓘ
⊕ Create network location

⊕ Add condition

Settings
Choose at least one setting to add to this policy.

✓ Direct routing
Route all users externally for all applications.

Policy enablement
✓ Enable policy after creation

Cancel Save

2. 输入策略的名称和描述。
3. 选择您要对其应用这些设置的用户和条件。

您可以将条件应用于所有用户或部分用户。

例如，您可以定义 **网络位置** 条件以后用整个会话的动态路由。这可确保仅当用户位于公司企业网络内部时才启用直接路由。

当您根据上下文添加其他条件时，将对条件应用 AND 运算，并且仅当用户和可选的基于上下文的条件都满足时，才会评估策略。

4. 选择 **直接路由** 以将用户流量直接发送到后端应用程序，而无需 NetScaler Gateway 隧道。
5. 选择 **创建后启用策略**。如果您不选择此选项，则策略仅创建，而不会在应用程序上强制执行。

或者，您也可以通过使用 **状态** 列中的切换开关，从“会话策略”页面启用策略。

6. 单击 **保存**。

注意：

网络位置更改会触发会话策略刷新，这可能会按如下方式影响最终客户端：

- ****Citrix Secure Access 客户端：**策略刷新可能会更改路由配置，从而影响应用程序访问。
- ****Chrome 安全浏览扩展程序：**策略刷新每 30 分钟发生一次。用户必须重新启动浏览器或等待刷新才能访问应用程序。

设备证书注册

必须注册设备证书以用于“始终开启”配置，从而确保设备能够持续安全地连接到网络。

设备证书注册涉及以下步骤：

1. Active Directory 企业证书颁发机构颁发用于机器身份验证的设备证书。
2. 证书颁发机构必须发布 CRL 分发点 (CDP) 扩展的 LDAP URL。

始终开启 CRL CDP(/en-us/citrix-secure-private-access/media/spa-ztna-always-on-crl-cdp.png)

3. 必须在此证书颁发机构中创建证书模板，以注册具有以下详细信息的设备证书。
 - a. 打开证书模板管理单元，并复制“**计算机**”或“**工作站身份验证**”（首选）模板。
 - b. 为证书提供一个新名称。
 - c. 切换到“**使用者名称**”选项卡，将“**使用者名称格式**”设置更改为“**通用名称**”，并选中“**用户主体名称 (UPN)**”以包含在备用使用者名称中。

始终开启使用者名称(/en-us/citrix-secure-private-access/media/spa-ztna-always-on-common-name-upn.png)

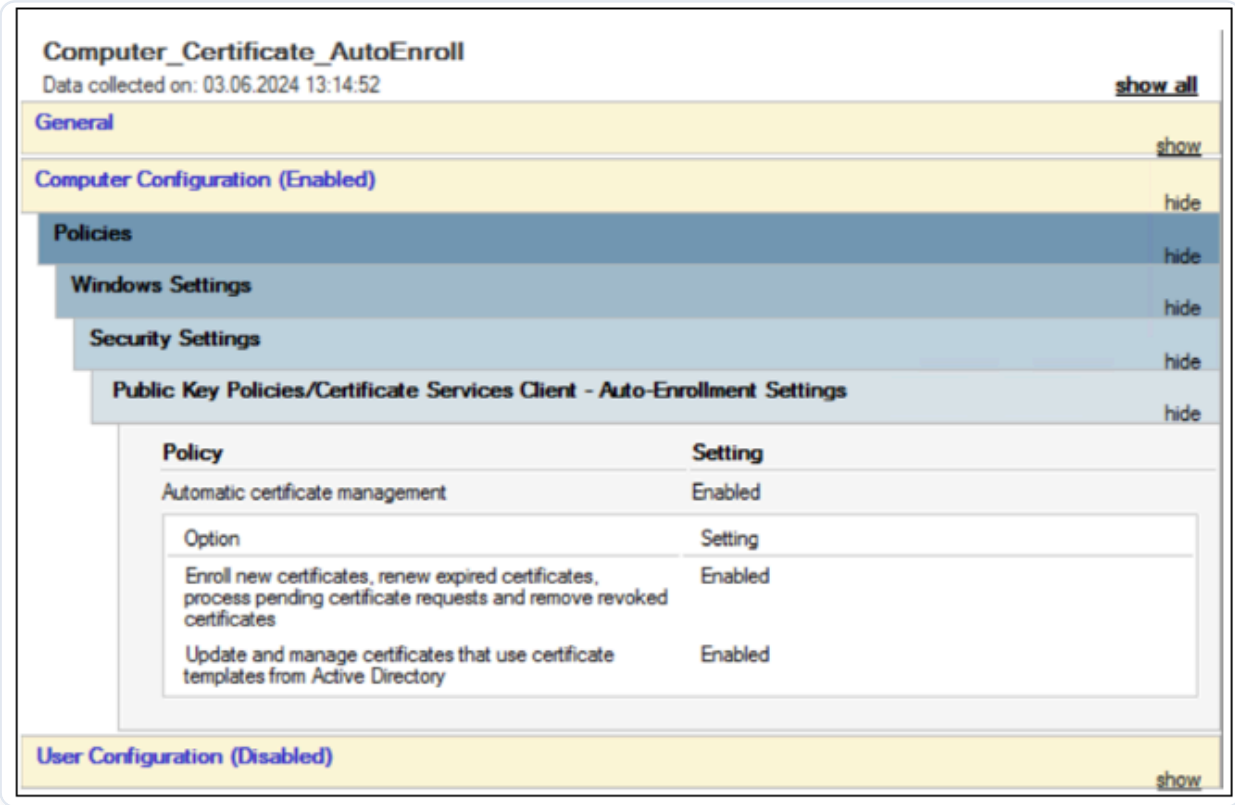
- d. 切换到“**安全**”选项卡，并添加一个安全组（仅包含计算机帐户），您希望将新的证书模板自动注册到该组。选择添加的组，然后为“**自动注册**”选择“**允许**”。

始终开启已验证用户(/en-us/citrix-secure-private-access/media/spa-ztna-always-on-auto-enroll.png)

注意：

在上图中，已验证用户（所有计算机对象）被允许注册或自动注册新的证书模板。

- e. (可选) 创建一个组策略对象 (GPO)，以允许自动证书注册，并将其绑定到组织单位 (OU) 或在域级别。



设备姿态服务

Citrix 设备姿态服务是一种基于云的解决方案，可帮助管理员强制执行终端设备必须满足的某些要求，以便访问 Citrix DaaS（虚拟应用和桌面）或 Citrix Secure Private Access 资源（SaaS、Web 应用、TCP 和 UDP 应用）。通过检查设备姿态来建立设备信任对于实施基于零信任的访问至关重要。设备姿态服务通过在允许最终用户登录之前检查终端设备是否合规（托管/BYOD 和安全姿态），从而在您的网络中强制执行零信任原则。

有关设备姿态的更多信息，请参阅 [设备姿态](#)。

在 NetScaler Gateway 上配置设备姿态检查

Citrix 设备姿态服务已与 NetScaler Gateway 集成。您可以在 NetScaler Gateway 上配置设备姿态检查。

有关更多信息，请参阅 [NetScaler® Gateway 上的设备姿态检查](#)。

注意：

- 建议在虚拟服务器级别启用设备姿态检查。
- 确保使用 `set dps parameter`（即 `set dps parameter -CustomerID <CCID>`）设置客户 ID。其余参数将自动填充。

本地 NetScaler® Gateway 上的设备状态检查

Citrix 设备状态服务是一种基于云的解决方案，可帮助管理员强制执行终端设备必须满足的某些要求，才能访问 Citrix Secure Private Access 资源，例如 SaaS/Web 和 TCP/UDP 应用程序。通过检查设备的姿态来建立设备信任对于实施基于零信任的访问至关重要。设备状态服务通过在允许最终用户登录之前检查终端设备的合规性（托管/BYOD 和安全姿态）来在您的网络中强制执行零信任原则。有关设备状态服务的详细信息，请参阅 [设备状态](#)。

授权

设备状态服务作为 Universal Hybrid Multi Cloud (UHMC) 许可证和 Citrix Platform License (CPL) 的一部分提供。有关更多信息，请参阅 <https://www.citrix.com/buy/licensing/product.html>。

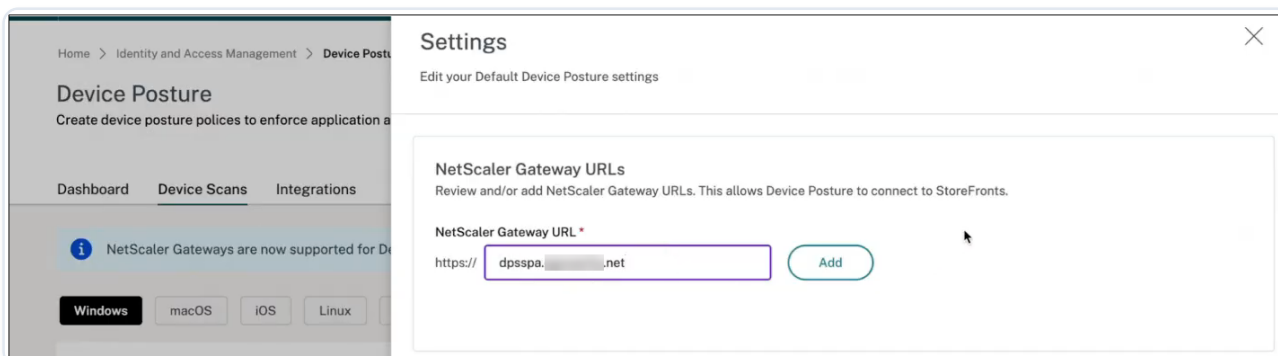
为 Secure Private Access 混合解决方案启用设备状态

设备状态服务与 Secure Private Access 混合解决方案的集成仅从 NetScaler Gateway 14.1 版本 build 43.x 开始支持。必须在 NetScaler Gateway 上启用设备状态功能，设备状态扫描才能在 Secure Private Access 混合部署中运行。

有关在 NetScaler Gateway 上启用设备状态检查的详细信息，请参阅 [NetScaler Gateway 上的设备状态检查](#)。

除了在 NetScaler Gateway 上启用设备状态功能外，您还必须在设备状态设置页面中添加访问 StoreFront™ 的 NetScaler Gateway 的 URL。

1. 在 Secure Private Access 管理控制台导航窗格中，单击**设备状态**。
2. 在**设备扫描**页面中，单击**设置**。
3. 在**NetScaler Gateway URL**中，输入必须启用设备状态检查的虚拟服务器的 FQDN。例如，<https://gw.example.net>。



管理设置

在加入后，您可以更新和维护 Secure Private Access 混合部署设置。

- 管理应用程序域路由并生成配置报告。报告可以包括有关访问策略、应用程序、路由域、资源位置、安全组、云连接器、站点配置和浏览器设置的详细信息。有关详细信息，请参阅[加入后管理设置](#)。
- 管理加入配置输入。更改可能会造成破坏，因为多个组件依赖于这些值。根据更改的内容，所需的后续操作可能包括重新配置和重新分析 NetScaler、重新配置 StoreFront 以及重新分析 StoreFront。有关详细信息，请参阅[安装后管理设置配置](#)。
- 从 Citrix Enterprise Browser 集成切换到 Chrome Enterprise Premium 时重置配置。有关详细信息，请参阅[重置 Secure Private Access 配置](#)。
- 默认情况下，当可用时，Cloud Connector 更新会一次安装一个连接器，并且 Secure Private Access 会作为 Cloud Connector 升级的一部分进行升级。有关详细信息，请参阅[组件升级](#)。

管理设置

以下部分提供了有关设置的更多信息。

应用程序域

Secure Private Access 管理员可以查看添加到 Secure Private Access 设置中的应用程序域列表。应用程序域表列出了所有相关域以及应用程序流量的路由方式（外部或内部）。

1. 单击 **设置 > 应用程序域**。
2. 单击编辑图标，并在必要时更改路由类型。

配置报告

客户管理员可以生成配置报告，以深入了解 Secure Private Access 设置。配置报告包含以下类别的信息：

- 管理应用程序和资源访问的访问策略。
- 在 Secure Private Access 中配置的应用程序。
- 为应用程序设置的路由域。

- 与客户关联的资源位置。
- 安全组。
- 云连接器。
- 站点配置。
- 浏览器设置。

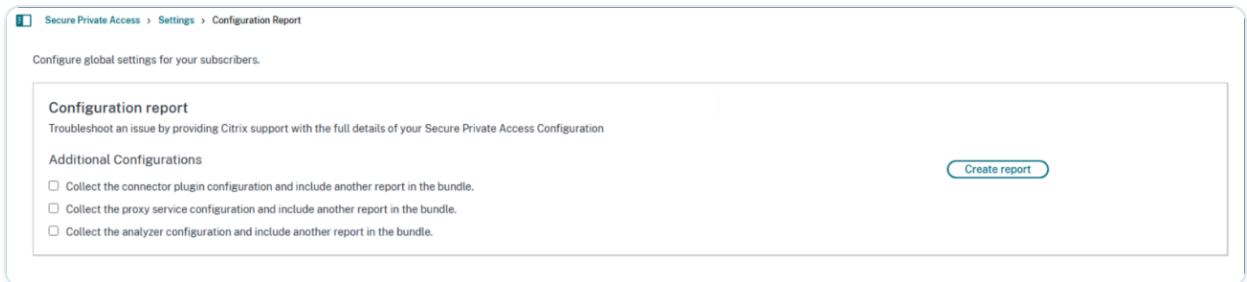
您还可以在捆绑包中包含其他配置报告：

- 连接器插件数据库中的详细信息。
- 代理服务中的详细信息。
- 分析器配置中的详细信息。

生成配置报告

执行以下步骤生成配置报告：

1. 在 Secure Private Access 管理控制台中，转到 **设置 > 配置报告**。



2. 要在捆绑包中包含其他报告，方法是收集存储在连接器插件数据库、代理服务或分析器配置中的配置详细信息，请选中“**其他配置**”部分下的相应复选框。
3. 单击“**创建报告**”以启动报告生成过程。

报告生成后，“**配置报告**”对话框将显示以下状态：

- **报告已完成**：表示所有必需的详细信息都已成功包含在报告中。
- **报告部分完成**：表示某些详细信息缺失或未生成。
- 该对话框还会列出报告生成不完整的类别。

下图显示了一个包含完整和部分完成状态的**配置报告**对话框示例。

Configuration report

Report Completed

The report includes configuration information for your:

- Access Policies
- Applications
- Security Groups
- Site Configurations
- Browser Settings
- Routing Domains
- Resource Locations
- Connectors

Additional Configurations

- ✔ Successfully collected the connector plugin configuration.
- ✔ Successfully collected the proxy service configuration.
- ✔ Successfully collected the analyzer configuration.

Attach the saved report to your support ticket.

<https://support.citrix.com/case/manage>

Download

Cancel

Configuration report

Report Partially Complete

Some of the configuration information could not be retrieved:

- Browser Settings

Additional Configurations

 Failed to collect the connector plugin configuration.

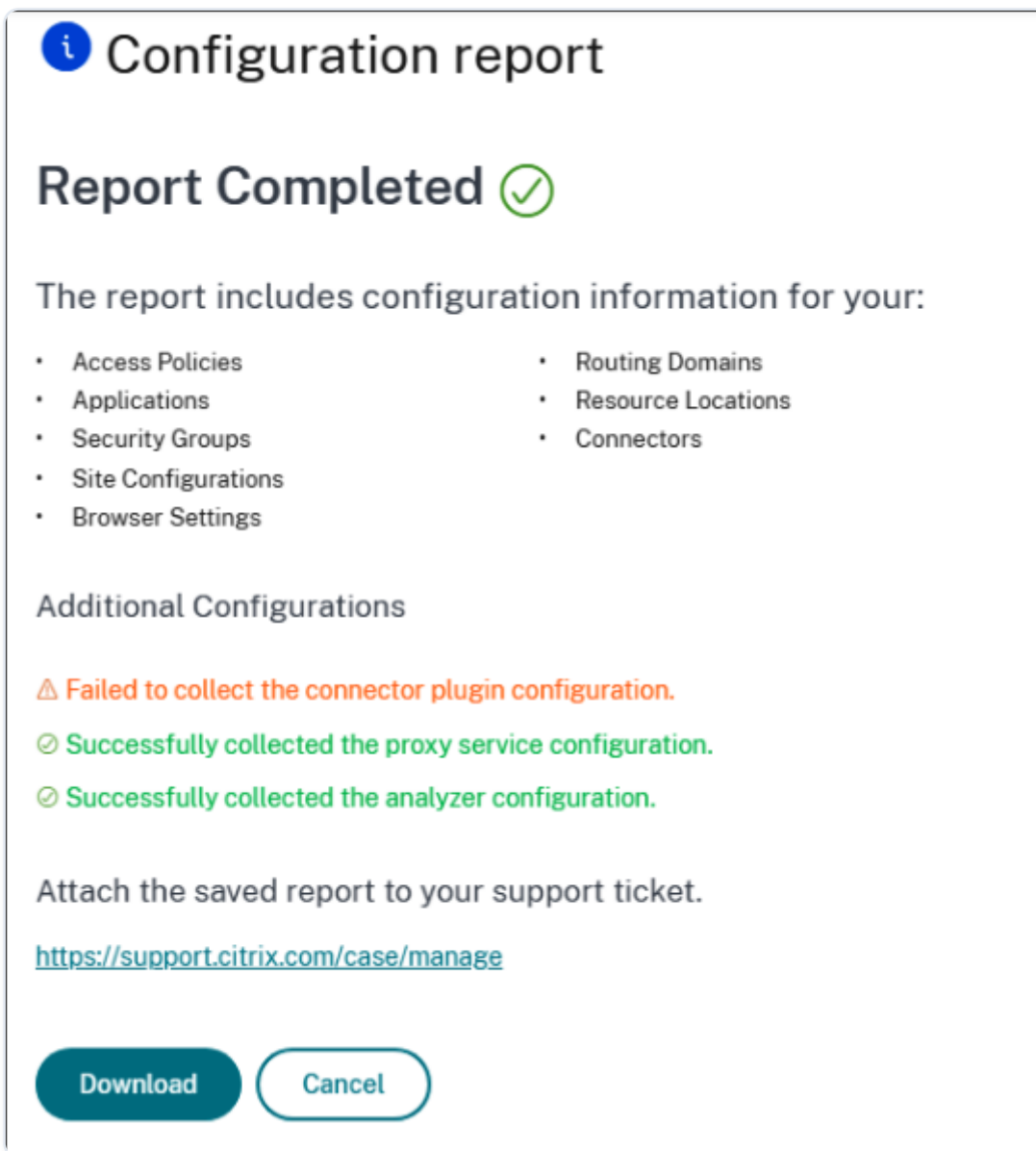
 Successfully collected the proxy service configuration.

Attach the saved report to your support ticket.

<https://support.citrix.com/case/manage>

Download

Cancel



4. 单击**下载**可手动将报告导出到本地驱动器。

重要提示：

生成配置报告仅限于具有以下 Secure Private Access 角色的管理员：

- 完全访问权限管理员
- 只读管理员
- 完全监视管理员

具有 Help Desk Administrator 角色的管理员无法生成配置报告。

注意：

报告可能包含敏感数据。

安装后管理设置配置

设置配置菜单选项可用于管理在入门期间提供的各种配置输入。

警告：

更改配置值可能会造成中断。由于此配置被多个组件引用，因此更改可能需要在依赖组件中重新配置，以避免服务中断。

下表总结了更改任何配置后所需的额外操作。

配置名称	所需操作	描述
步骤 1		
Google 客户 ID	通过再次下载脚本来重新配置和重新分析 NetScaler。	Google 服务会自动重新配置。
安全私有访问网关 URL	通过再次下载脚本来重新配置和重新分析 NetScaler。	Google 服务会自动重新配置。
		注意 如果跳过 CEP 配置，此设置是步骤 2 的一部分。
Google Workspace 用户组	无需手动操作	保存设置后，新用户组会在所需的 Google 服务上自动配置。
步骤 2		
NetScaler Gateway 虚拟服务 器名称	仅重新运行 NetScaler Analyzer	运行 NetScaler 脚本时，使用 分析选项。
安全私有访问站点 URL	使用新的 Secure Private Access 地址重新配置 StoreFront。	
	通过再次下载脚本重新分析 StoreFront	
	重新下载脚本以重新配置和重 新分析 NetScaler。	

配置名称	所需操作	描述
内部 IP 地址（用于安全专用访问网关 URL）	重新下载脚本以重新配置和分析 NetScaler。	
证书-密钥对名称	重新下载脚本以重新配置和重新分析 NetScaler。	

重置 Secure Private Access 配置

如果您有集成了 Citrix Enterprise Browser 的 Citrix Secure Private Access 混合部署，并且您想切换到 Chrome Enterprise Premium，您可以重置 Secure Private Access 配置。此操作将删除整个配置，包括应用程序和访问策略。StoreFront 和 NetScaler 配置需要手动清理。配置重置后，您可以再次加入 Secure Private Access 混合部署并选择 Chrome Enterprise Premium。

如果您需要重置配置，请联系 Citrix 支持。

升级

Citrix 会定期发布更新，以增强 Cloud Connector 的性能、安全性和可靠性。默认情况下，Citrix Cloud 会在更新可用时，逐个在每个连接器上安装这些更新。默认情况下，Secure Private Access 会作为 Cloud Connector 升级的一部分进行升级。

有关 Cloud Connector 升级的详细信息，请参阅[连接器更新](#)。

注意：

通过 GUI 升级 NetScaler 有时不会安装 Python。建议您通过 CLI 升级 NetScaler。

有关其他组件升级的详细信息，请参阅以下主题：

- [StoreFront](#)
- [NetScaler 网关](#)

高级安全专用访问功能

以下是安全专用访问支持的一些高级功能：

- **高级数据中心配置**：安全专用访问混合部署支持在多数数据中心和多站点配置中使用 NetScaler GSLB，采用主动-主动站点部署模式，并结合站点持久性方法用于 GSLB 连接代理。有关详细信息，请参阅[高级数据中心配置](#)。
- **全局服务器负载均衡连接代理**：全局服务器负载均衡 (GSLB) 连接代理使 NetScaler Gateway 能够透明地检测错误路由的请求，并将其代理到正确的站点，无需任何用户干预。有关详细信息，请参阅[全局服务器负载均衡连接代理](#)。
- **配置全局服务器负载均衡器域 URL**：要为安全专用访问设置多站点冗余，您必须配置一个全局服务器负载均衡器 (GSLB) 地址。此地址充当单一入口点，根据您的流量策略（例如静态邻近性）将用户路由到特定数据中心的安全专用访问网关。有关详细信息，请参阅[配置全局服务器负载均衡器域 URL](#)。
- ****基于上下文的应用程序路由****：配置应用程序时，会在应用程序配置下为其应用程序 URL 及其相关域或应用程序目标定义路由类型。此处定义的路由类型适用于所有有权访问该应用程序的用户。但是，在某些情况下，管理员可能希望根据用户上下文以不同方式路由同一应用程序。例如，当用户在公司网络内部时，内部应用程序 URL 或目标必须直接路由，而不是通过安全专用访问路由。有关详细信息，请参阅[基于上下文的应用程序路由](#)。
- ****发现最终用户访问的域或 IP 地址****：应用程序发现功能可帮助管理员了解组织中正在访问的外部 and 内部应用程序（HTTP/HTTPS 和 TCP/UDP 应用程序）。此功能可发现并列出所有已发布或未发布的域/IP 地址。因此，管理员可以查看哪些域/IP 地址正在被谁访问，并决定是否将其发布为应用程序，从而为这些用户提供访问权限。有关详细信息，请参阅[发现最终用户访问的域或 IP 地址](#)。
- **策略建模工具**：管理员可以创建多个策略并将这些策略分配给多个应用程序。因此，管理员可能难以了解其最终用户的应用程序访问结果。也就是说，最终用户是否被允许或拒绝访问取决于应用程序和访问策略配置。策略建模工具（访问策略 > 策略建模）通过让管理员全面了解预期的应用程序访问结果（允许/受限允许/拒绝）来帮助解决这些问题。有关详细信息，请参阅[策略建模工具](#)。
- **配置数据丢失防护 (DLP) 策略**：访问限制在 Google 管理控制台中为 CEP 配置。以前在安全专用访问控制台中配置的访问限制仅适用于 Citrix Enterprise Browser。当 Google Chrome 是企业浏览器时，访问限制必须在 Google 管理控制台中配置为策略和规则。有关详细信息，请参阅[配置数据丢失防护 \(DLP\) 策略](#)。

- **高可用性部署**：您只需几个简单的步骤即可为安全专用访问配置高可用性。有关详细信息，请参阅[高可用性部署](#)。
- **重置安全专用访问配置**：如果您有集成了 Citrix Enterprise Browser 的 Citrix 安全专用访问混合部署，并且想要切换到 Chrome Enterprise Premium，则可以重置安全专用访问配置。有关详细信息，请参阅[重置安全专用访问配置](#)。

高级数据中心配置

Secure Private Access 混合部署支持在多数数据中心多站点配置中使用 NetScaler GSLB，采用主动-主动站点部署和 GSLB 连接代理的站点持久性方法。

多数数据中心部署(/en-us/citrix-secure-private-access/media/spa-hybrid-multi-datacenter.png)

本主题提供了在多数数据中心多站点配置中设置 Secure Private Access 混合部署的分步说明。

先决条件

确保满足以下先决条件，以便在多数数据中心部署 Secure Private Access 混合。

- NetScaler Gateway 14.1–66.59 版及更高版本。
- NetScaler GSLB 采用主动-主动站点部署。GSLB 域必须在所有站点上配置。如果尚未配置 GSLB，请参阅 [主动-主动站点部署](#) 获取说明。
- GSLB 上已启用源 IP 持久性。
- 已为 CEP 会话启用连接代理持久性。有关详细信息，请参阅 [全局服务器负载平衡连接代理](#)。

GSLB 配置 CLI 命令

建议使用 NetScaler CLI 配置 GSLB。以下是 CLI 命令模板和示例配置。

- `add service <ADNS_SERVICE_NAME> <ADNS_IP> ADNS 53`
- `add gslb site <SITE_NAME> <SITE_IP> -sitePassword "<SITE_PASSWORD>"`
- `add gslb service <GSLB_SERVICE_NAME> <SERVICE_IP> SSL 443 -publicIP <PUBLIC_IP> -publicPort 443 -siteName <SITE_NAME>`
- `add gslb vserver <VSERVER_NAME> SSL`
- `bind gslb vserver <VSERVER_NAME> -serviceName <GSLB_SERVICE_NAME>`
- `bind gslb vserver <VSERVER_NAME> -domainName <GSLB_DOMAIN_FQDN>`
- `set lb vserver <VSERVER_NAME> -PersistenceType SOURCEIP`
- `set gslb service <GSLB_SERVICE_NAME> -sitePersistence ConnectionProxy`

- `bind ssl service <GSLB_SERVICE_NAME> -certKeyName <SERVICE_CERT_KEY>`
- `bind ssl vservice <VSERVER_NAME> -certKeyName <CA_CERT_KEY> -CA`
- `bind ssl vservice <VSERVER_NAME> -certKeyName <EXTERNAL_CA_CERT_KEY> -CA`
- `bind ssl vservice <VSERVER_NAME> -certKeyName <SERVER_CERT_KEY>`

参考

下表总结了 CLI 命令中使用的占位符及其简要说明。

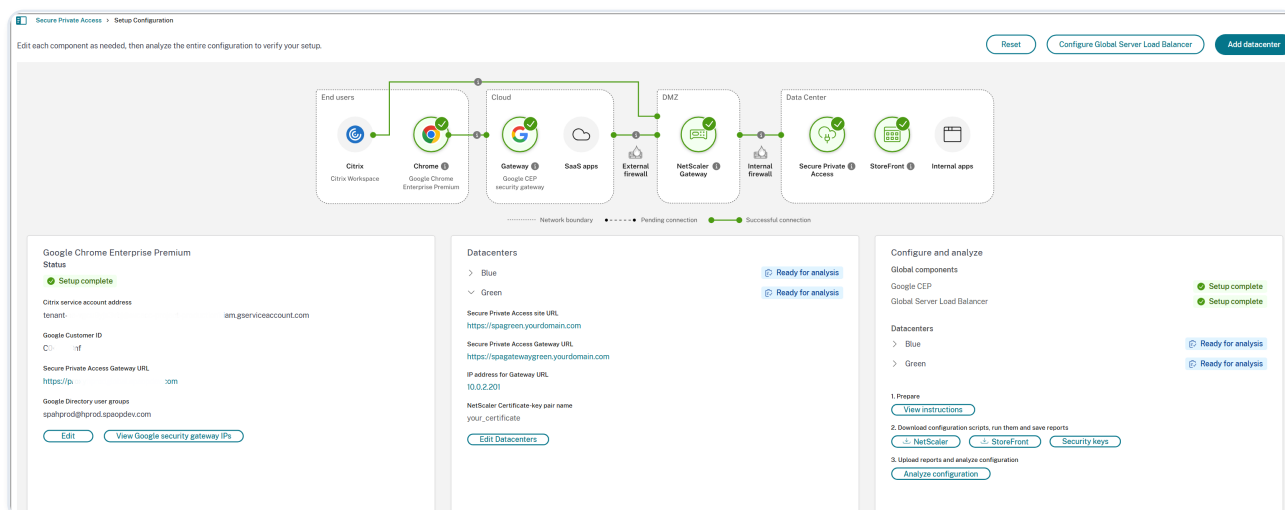
占位符	描述
<code><ADNS_SERVICE_NAME></code>	ADNS 服务的名称 (例如, adns_<env>)
<code><ADNS_IP></code>	此 NetScaler 上 ADNS 侦听器的 IP 地址
<code><SITE_NAME></code>	GSLB 站点标识符 (例如, 蓝色、绿色)
<code><SITE_IP></code>	GSLB 站点 IP (用于 MEP 通信的 SNIP 或管理 IP)
<code><SITE_PASSWORD></code>	用于 GSLB 站点到站点 MEP 身份验证的共享密钥
<code><GSLB_SERVICE_NAME></code>	绑定到本地/远程负载均衡虚拟服务器的 GSLB 服务名称
<code><SERVICE_IP></code>	后端负载均衡虚拟服务器或服务的 IP 地址
<code><PUBLIC_IP></code>	可从互联网访问的公共 (NAT) IP 地址
<code><VSERVER_NAME></code>	GSLB 虚拟服务器的名称
<code><GSLB_DOMAIN_FQDN></code>	GSLB 为客户端解析的 FQDN
<code><SERVICE_CERT_KEY></code>	绑定到 GSLB 服务的 SSL 证书密钥名称
<code><CA_CERT_KEY></code>	内部 CA 证书密钥名称 (绑定为 -CA)
<code><EXTERNAL_CA_CERT_KEY></code>	外部/公共 CA 证书密钥名称 (绑定为 -CA)
<code><SERVER_CERT_KEY></code>	绑定到虚拟服务器的服务器证书密钥名称

配置示例：

- `add service adns_staging 10.100.5.50 ADNS 53`
- `add gslb site us-east-dc1 10.100.5.60 -sitePassword "password"`
- `add gslb service us-east-dc1-svc1 10.100.5.80 SSL 443 -publicIP 203.0.113.42 -publicPort 443 -siteName us-east-dc1`
- `add gslb vserver staging_us-east_vs SSL`
- `bind gslb vserver staging_us-east_vs -serviceName us-east-dc1-svc1`
- `bind gslb vserver staging_us-east_vs -domainName proxy-staging.example.com`
- `set lb vserver staging_us-east_vs -PersistenceType SOURCEIP`
- `set gslb service us-east-dc1-svc1 -sitePersistence ConnectionProxy`
- `bind ssl service us-east-dc1-svc1 -certKeyName star_staging_local`
- `bind ssl vserver staging_us-east_vs -certKeyName ca_staging.local -CA`
- `bind ssl vserver staging_us-east_vs -certKeyName CA.csg.proxy.ext.example -CA`
- `bind ssl vserver staging_us-east_vs -certKeyName csg.proxy.ext.example`

数据中心设置和配置

下图显示了多数据中心中安全私有访问混合部署的拓扑图。



1. 添加数据中心。有关详细信息，请参阅[步骤 2：设置第一个数据中心](#)。
2. 对于每个数据中心，下载并运行 NetScaler 和 StoreFront 脚本。有关详细信息，请参阅[下载并运行 NetScaler 和 StoreFront 脚本](#)。
3. 对于每个数据中心，上传报告并分析配置。有关详细信息，请参阅[上传报告并分析配置](#)。

4. 查看分析结果。

如果每个数据中心的所有分析器步骤都已通过，则您已成功验证您的配置，并且可以继续执行入职后任务。有关详细信息，请参阅[入职后任务](#)。

全局服务器负载均衡连接代理

全局服务器负载均衡 (GSLB) 连接代理使 NetScaler Gateway 能够透明地检测错误路由的请求，并将其代理到正确的站点，无需任何用户干预。

在使用 GSLB 的多站点 Citrix Secure Private Access 混合部署中，DNS 解析有时可能会将用户请求路由到非预期站点。发生这种情况时，用户会进入一个未建立其会话的站点，这可能会阻止访问内部 Web 应用程序。

GSLB 连接代理通过使 NetScaler Gateway 能够透明地检测错误路由的请求，并将其代理到正确的站点，无需任何用户干预，从而解决了此问题。此过程对最终用户是透明的，并提高了会话持久性，消除了由非最佳 DNS 路由导致的会话中断和应用程序访问失败。

先决条件

确保满足以下先决条件以支持 GSLB 连接代理：

- 跨站点 Secure Private Access 混合部署，并在所有站点上配置了 GSLB。
- GSLB 上启用了源 IP 持久性。有关详细信息，请参阅[根据源 IP 地址配置持久性](#)。
- 配置了静态邻近性（由管理员管理的 IP 数据库）。有关详细信息，请参阅[静态邻近性](#)。
- NetScaler Gateway 版本为 14.1 或更高版本。

配置 GSLB 连接代理

要启用 GSLB 连接代理，请将证书绑定到所有 GSLB 服务和 VPN 虚拟服务器：

1. 生成具有通用名称的自签名客户端证书，例如 `csg.proxy.ext.goog`。
2. 将证书绑定到所有站点的所有 GSLB 服务。
3. 将颁发者证书作为 CA 证书绑定到 VPN 虚拟服务器。
4. 在部署中的每个站点上的每个 GSLB 服务重复服务绑定。

CLI 命令：

- 将证书绑定到 GSLB 服务。

```
bind ssl service <gslb-service-name> -certKeyName <certificate-name>
```

- 将颁发者证书绑定到 VPN 虚拟服务器。

```
bind ssl vsrver <vpn-vserver-name> -certKeyName <certificate-name> -CA
```

配置全局服务器负载均衡器域 URL

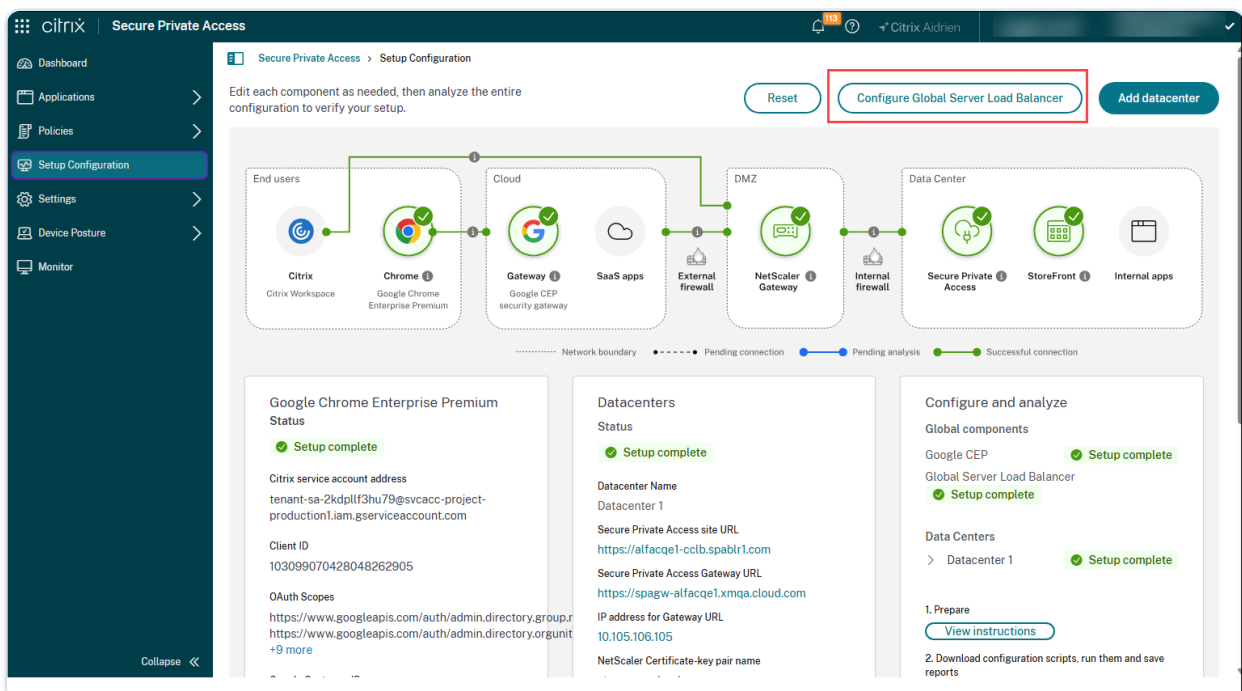
要为 Secure Private Access 设置多站点冗余，您必须配置全局服务器负载均衡器 (GSLB) 地址。此地址充当单一入口点，根据您的流量策略（例如静态邻近性）将用户路由到特定数据中心的 Secure Private Access 网关。

为 Secure Private Access 部署配置 GSLB 时，必须在 Google Secure Gateway（在 Google Cloud 服务中）内更新 GSLB 地址。如果之前使用了特定于数据中心的 Secure Private Access 网关，提供 GSLB 地址会自动覆盖现有配置，以指向新的全局地址。

配置

出现提示时，输入全局服务器负载均衡器 (GSLB) 域 URL 详细信息，以使用 GSLB 域更新 Chrome Enterprise Premium (CEP) 配置。更新后，重新配置第一个数据中心中的 NetScaler Gateway。

1. 登录到 **Secure Private Access** 管理控制台。
2. 转到 **设置配置**。
3. 单击 **全局服务器负载均衡器 (GSLB)**。



4. 在 **Secure Private Access 网关 URL** 字段中输入 GSLB 域 URL 的公共地址。

Global Service Load Balancer (GSLB) ✕

> View Prerequisites

Enter details

Secure Private Access Gateway global URL ⓘ

Save

注意：

这将更新 CEP 集成，并将 Secure Private Access 网关 URL 替换为您输入的 GSLB 域 URL。

编辑数据中心（可选）

仅当您需要更改数据中心时才需要此步骤。

Datacenters

Select Datacenter

Blue

> View Prerequisites

Global Server Load Balancer (GSLB) required for NetScaler Gateways

Before adding another datacenter, ensure that Global Server Load Balancing (GSLB) is properly configured for your NetScaler Gateways. Verify that your existing GSLB setup is correct before proceeding.

Configure GSLB

Datacenter Name ⓘ

Blue

Secure Private Access site URL ⓘ

https://spa.yourdomain.com

Secure Private Access Gateway URL ⓘ

https://spagateway.yourdomain.com

IP address ⓘ

10.0.2.200

NetScaler Certificate-key pair name ⓘ

your_certificate

Save

配置和分析

完成上述步骤后，您可以更新第一个数据中心中本地 StoreFront 和 NetScaler 组件的配置。

请按照 [步骤 3：配置和分析](#) 完成数据中心 NetScaler 组件的重新配置，并在必要时分析 NetScaler 和 StoreFront 配置。

基于上下文的应用程序路由

配置应用程序时，会在应用程序配置下为其应用程序 URL 及其相关域或应用程序目标定义路由类型。此处定义的路由类型适用于所有有权访问该应用程序的用户。但是，在某些情况下，管理员可能希望根据用户上下文以不同方式路由同一应用程序。例如，当用户位于公司网络内部时，内部应用程序 URL 或目标必须直接路由，而不是通过 Secure Private Access 路由。

您可以使用 **访问策略（针对特定用户）** 或 **会话策略（所有用户）** 中的**路由例外**来配置此项。访问策略中的路由例外配置允许管理员为符合策略中定义的条件或计算机编辑路由类型。由于此设置是访问策略的一部分，因此它仅适用于该策略中包含的用户和计算机。

注意：

如果访问策略中存在路由配置，则它会覆盖应用程序配置。

以下示例演示了路由例外用例。

- **基于上下文的路由**
- **将内部公司用户直接路由到后端应用程序**

用例：基于上下文的路由

场景：

- A 组用户：ABC 公司的员工，通过内部路由的 NetScaler Gateway 访问 Outlook 应用程序和 Microsoft Teams 应用程序。
- B 组用户：与 ABC 合作的第三方公司的员工。他们通过 NetScaler Gateway 访问某些应用程序（不包括 Outlook）。他们还有通过互联网访问的自己的 Outlook 应用程序，不希望通过 NetScaler Gateway 路由其 Outlook 流量。

问题：

- B 组用户登录 Secure Access 客户端以访问 ABC 应用程序。
- 他们通过本机浏览器访问 Outlook 的请求通过 NetScaler Gateway 路由，导致访问被拒绝。
- Outlook 应用程序的目标域对于 A 组和 B 组用户来说是相同的。
- 访问策略仅允许 A 组用户访问，导致 B 组用户在尝试启动 Microsoft Teams 或 Outlook 时被拒绝访问。
- 由于此路由问题，B 组用户无法访问其公司 Outlook。

解决方案：

ABC 公司管理员可以进行以下配置更改来解决此问题：

1. 专门为访问 Office 365 应用程序的 B 组用户定义新的访问策略。
2. 在访问策略中，启用**路由例外**选项。

管理员可以查看与访问策略关联的所有内部应用程序的所有 URL 和相关域的列表。

3. 对于所有 Office 365 应用程序 URL，将路由配置为在外部进行。

这确保了 B 组用户访问其 Outlook 应用程序的请求通过互联网路由，绕过 NetScaler Gateway。

通过实施这些更改，B 组用户可以通过互联网访问其公司 Outlook 应用程序，而无需通过 NetScaler Gateway 路由，同时仍可根据需要访问其他 ABC 应用程序。

更改路由类型的步骤

1. 创建或编辑访问策略。有关详细说明，请参阅[配置访问策略](#)。
2. 在访问策略中，将路由例外切换为“开”。
3. 从与访问策略关联的应用程序 URL 和相关域列表中，找到要更改其路由类型的域。
4. 根据您要应用的用户上下文，更改所选域的路由类型（例如，从 **Internal** 到 **External**）。
5. 保存访问策略。

路由例外(/en-us/citrix-secure-private-access/media/spa-hybrid-routing-exceptions.png)

用例：将内部企业用户直接路由到后端应用程序

管理员可以配置会话策略，将内部企业用户直接路由到后端应用程序，而无需通过 NetScaler Gateway 隧道传输流量。会话策略根据网络位置和设备状态等因素提供动态路由。

有关配置会话策略的详细信息，请参阅 [配置会话策略](#)。

注意：

- 会话策略设置在会话级别应用于所有应用程序，而不是绑定到特定应用程序。
- 会话策略可以分配给所有用户或部分用户。

路由优先级

会话策略与访问策略协同工作，如果存在冲突，访问策略优先。在这种情况下，访问策略路由例外会覆盖会话策略。如果既未配置访问策略也未配置会话策略，则全局路由设置（**设置 > 应用程序域**）将适用。

支持的 Citrix Secure Access™ 客户端

以下版本的 Citrix Secure Access 客户端支持将用户直接路由到后端应用程序。

- macOS - 24.11.1 及更高版本。

- Windows - 24.11.1.17 及更高版本。此外，必须启用 **EnableContextualAccess** VPN 客户端注册表。有关详细信息，请参阅 [NetScaler Gateway Windows VPN 客户端注册表项](#)。

示例用例

场景：

在医院中，当用户连接到医院网络“hospital_network1”时，来自应用程序的流量必须直接流向后端应用程序，因为这些应用程序在医院网络上可以直接访问。如果用户在医院网络之外，则应用程序流量必须通过隧道传输。

解决方案：

1. 添加 app1、app2，并将路由设置为**内部**。
2. 为应用程序（app1、app2）添加访问策略以授予访问权限。
3. 添加会话策略以配置条件，指定在授予访问权限时必须考虑的用户组和网络位置。
4. 选择**用户**条件并将其设置为**所有用户**。
5. 添加**网络位置**条件。将其设置为**匹配以下任意一项**，并指定网络位置“hospital_network1”。这可确保来自“hospital_network1”的流量直接流向后端应用程序。

您还可以为此场景启用路由例外。例如，如果 app1 即使在医院网络上也必须始终通过隧道传输，则可以在访问策略中为 app1 的域配置路由例外。完成此操作后，路由例外将优先于会话策略。

使用会话策略配置医院网络内的直接路由

您可以使用会话策略允许用户通过绕过 NetScaler Gateway 隧道直接访问后端应用程序。

有关配置会话策略的详细信息，请参阅[配置会话策略](#)。

Secure Private Access > Policies > Create/Edit Session Policy

Policy name

hospital_policy

Description (optional)

Enter a description

Conditions ⓘ

User:

All users

AND

Network location

Matches any of

hospital_network1

Create network location

Add condition

Settings

Choose at least one setting to add to this policy.

✓ Direct routing

Route all users externally for all applications.

Policy enablement

✓ Enable policy after creation

Cancel

Save

发现最终用户访问的域或 IP 地址

应用程序发现功能可帮助管理员了解组织中正在访问的外部 and 内部应用程序（HTTP/HTTPS 和 TCP/UDP 应用程序）。此功能可发现并列出所有已发布或未发布的域/IP 地址。因此，管理员可以查看正在访问哪些域/IP 地址、由谁访问，并决定是否要将其发布为应用程序，从而为这些用户提供访问权限。

应用程序发现功能为管理员提供以下功能：

- 提供最终用户访问的内部或外部域/IP 地址的可视性。
- 全面了解所有类型的访问应用程序（HTTP、HTTPS、TCP 和 UDP）。支持访问 Citrix Enterprise Browser™ 和 Citrix Secure Access 代理。

- 显示最终用户访问的已发布或未发布的域/IP 地址。

下图显示了一个示例“应用程序发现”页面。“应用程序发现”页面允许根据协议（HTTP/HTTPS、TCP/UDP）以及域/IP 地址和端口号筛选域。它还显示最终用户访问的未发布（未分配给任何应用程序）域。

App configurationApp discoverySecurity groups

All protocol

Last 1 Week

+ Add filter

App discovery shows list of domains visited by end-users. Select one or more domains to add them to a new or existing application.

2 Selected

☐ View selected only

Create application

Add to an existing application

	Domain/IP	Port	Protocol	Total Visits	Unique Users	Most Recent Visit	Assigned To App(S)
☐	meesho.com	443	HTTPS	3	1	2024-08-14 12:22:32	1
☐	www.google.com	443	HTTPS	2	1	2024-08-14 12:16:21	0
☐	www.googleadservices.com	443	HTTPS	2	1	2024-08-14 12:16:21	0
☐	www.bbc.com	443	HTTPS	1	1	2024-08-14 11:59:01	0
☐	myntra.in	443	HTTPS	1	1	2024-08-14 12:00:54	1
☐	www.apple.com	443	HTTPS	1	1	2024-08-14 12:00:54	0
☒	wikipedia.org	443	HTTPS	1	1	2024-08-14 12:16:21	0
☒	www.amazon.in	443	HTTPS	1	1	2024-08-14 12:16:21	0
☐	www.ajio.com	443	HTTPS	1	1	2024-08-14 12:22:32	0
☐	javatpoint.com	443	HTTPS	1	1	2024-08-14 12:22:32	0
☐	udemy.com	443	HTTPS	1	1	2024-08-14 12:22:32	0
☐	www.reddit.com	443	HTTPS	1	1	2024-08-14 12:22:32	0

新环境中的内部域应用程序发现

如果您正在设置新的 Secure Private Access 环境并希望了解要配置的应用程序，则可以使用应用程序发现功能。此功能可发现并列出最终用户访问的所有域/IP 地址，以便您可以将其配置为应用程序。在设置 Secure Private Access 环境时，请按照以下步骤启用应用程序发现功能：

- 要发现内部 Web 应用程序，请在 Secure Private Access 中配置一个应用程序，并指定属于您要发现的应用程序的域/子域的通配符相关域。

例如，如果您想发现域为 citrix.com 的所有应用程序，请创建一个应用程序，其相关通配符域为 `*.citrix.com`。为了完成应用程序配置，请添加任何测试 URL 作为主 Web 应用程序 URL 部分。

App type * HTTP/HTTPS	App icon  Change icon Use default icon (128 KB max, PNG)
App name * Discover_app1	☐ Do not display application icon in Workspace app
App description 	☐ Add application to favorites in Workspace app ☐ Allow user to remove from favorites ☐ Do not allow user to remove from favorites
App category ? Ex.: Category\SubCategory\SubCategory	
☐ Direct Access Enable direct browser-based access to internal web applications.	
URL * https://test.citrix.com	
Related Domains * ? *.docs.citrix.com	

Web 应用程序 URL: `https://test.citrix.com/` 相关域: `*.citrix.com`

- 对于内部 TCP/UDP 应用程序，请在 Secure Private Access 中配置一个应用程序，并指定子网以及 TCP/UDP 协议和端口范围（输入 `*` 以包含整个范围）。这使得可以从 Citrix Secure Access 代理发现所有 TCP 和 UDP 应用程序。例如，如果您想发现子网 10.0.0.0/8 中的所有应用程序，请使用以下详细信息配置应用程序：示例：10.0.0.0/8:

端口: (*)

协议: TCP

App type * TCP/UDP	App icon  Change icon (128 KB max, PNG) Citrix Secure Access Client for Windows Citrix Secure Access Client for macOS
App name * Discover_app2	
App description 	
Destinations	
Destination * ? 10.0.0.0/8	Port * ? 443
Protocol * TCP	

- 创建应用程序后，您还必须定义允许访问配置了域和 IP 子网的应用程序的用户。创建访问策略，并将您希望允许访问所创建应用程序中配置的 FQDN/IP 地址的用户分配给该策略。这些可以是初始测试用户集，也可以是您最初希望授予访问权限的有限用户数。
- 创建应用程序和相应的访问策略后，用户可以继续从 Citrix Workspace 应用程序访问应用程序并访问不同的域。最终用户访问的所有 FQDN/IP 地址都将开始显示在“应用程序发现”页面中。

注意：

- 在几天/几周内发现并识别出大多数应用程序后，我们建议删除最初创建的应用程序，以便通过通配符域和 IP 子网授予的更广泛访问权限可以关闭，并且只有发现的特定应用程序 URL 和 IP 地址才必须通过新应用程序允许访问。
- 在应用程序名称中添加前缀 **Discover**，以指示这是一个特殊的应用程序配置，用于启用发现监控和报告。此命名有助于您识别以删除通配符域或 IP 子网或两者，以便您可以在几周或一个月后将整体应用程序访问区域缩小到特定的 FQDN 和 IP/端口组合。
- 要访问 TCP/UDP 应用程序，用户必须使用 Citrix Secure Access 代理。根据应用程序的域和子网配置，监控来自各种访问方法的应用程序访问，并在“**应用程序发现**”页面中报告。
- 即使在您删除了已发现的应用程序之后，此功能仍会继续发现您的用户访问的域/IP 地址。因此，您可以随时返回“**应用程序发现**”页面，查看正在访问的内容，以及是否有任何新发现的域/IP 地址需要配置为应用程序。

有关添加域、FQDN 或 IP 地址的详细信息，请参阅以下主题。

- [配置 HTTP/HTTPS 应用程序](#)

- [配置 TCP/UDP 应用程序](#)

从应用程序发现页面创建应用程序

要为主要域和未发布的域从“应用程序发现”页面创建应用程序，请执行以下步骤：

1. 导航到 **应用程序 > 应用程序发现**。
2. 从列表选择一个域。

注意：

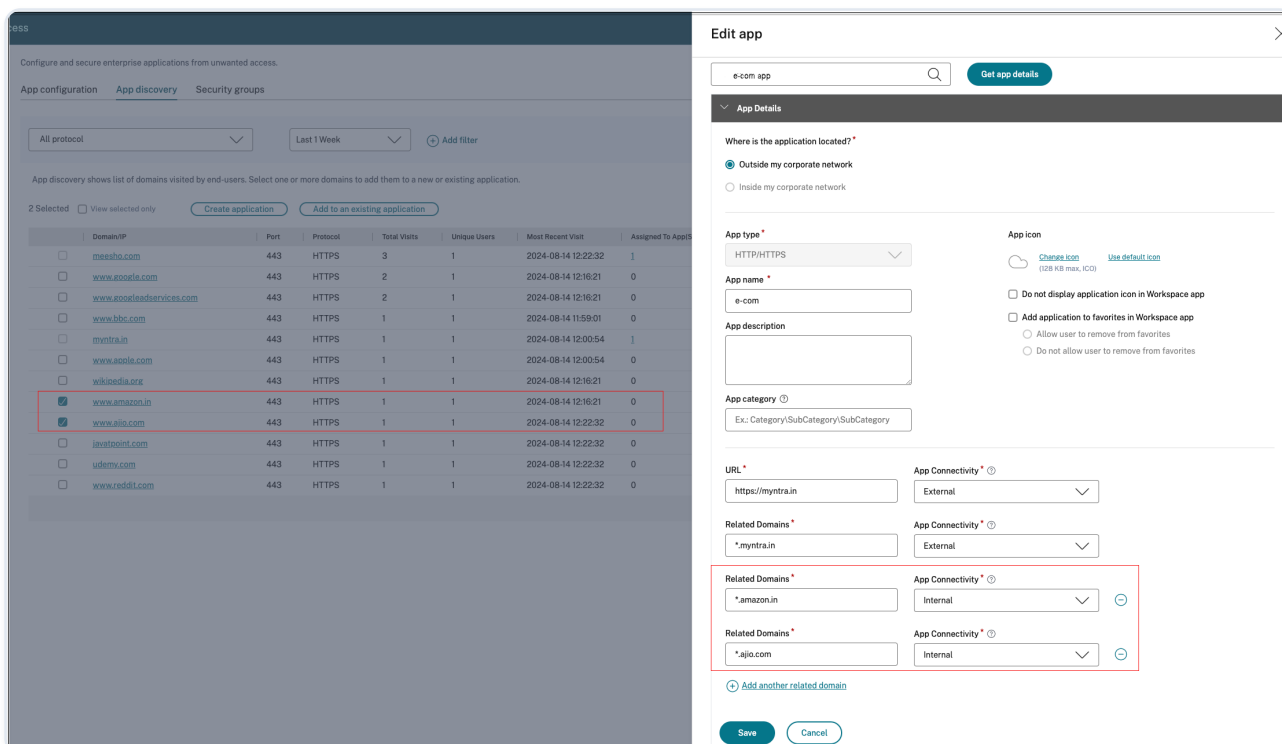
- 您不能选择属于不同协议的域来创建应用程序。当您选择属于不同协议的域时，将显示错误消息。
- 如果一个域已与某个应用程序关联，则不能再次选择该域来创建应用程序。与该域对应的复选框将显示为灰色，当您将鼠标悬停在该复选框上时，将显示一个工具提示。

3. 单击“**创建应用程序**”。有关创建应用程序的详细信息，请参阅[配置 HTTP/HTTPS 应用程序](#)和[配置 TCP/UDP 应用程序](#)。

更新现有应用程序

要将域添加到现有应用程序，请执行以下步骤：

1. 选择必须添加到应用程序的域。
2. 单击“**添加到现有应用程序**”。
3. 在“**应用程序**”中，选择要添加这些域的应用程序。
4. 单击“**获取应用程序详细信息**”。
5. **相关域**字段在单独的行中显示您之前选择的所有域。
6. 单击“**完成**”。



注意：

- 您只能将 TCP/UDP 目标 IP 地址添加到现有的 TCP/UDP 应用程序。“应用程序”字段仅列出系统中配置的 TCP/UDP 应用程序。
- 您可以选择现有的 HTTP/HTTPS 或 TCP/UDP 应用程序，以添加协议为 HTTP/HTTPS 的域（主域或单个条目）。
- 您不能选择已与某个应用程序关联的域。

策略建模工具

管理员可以创建多个策略并将这些策略分配给多个应用程序。因此，管理员可能难以了解其最终用户的应用程序访问结果。也就是说，最终用户是否被允许或拒绝访问取决于应用程序和访问策略配置。策略建模工具（**访问策略 > 策略建模**）通过让管理员全面了解预期的应用程序访问结果（允许/限制性允许/拒绝）来帮助解决这些问题。管理员可以检查特定用户的访问结果，并为上下文标记添加用户条件。该工具还会显示与应用程序关联的策略列表。

要分析访问策略配置，请执行以下步骤。

1. 在 Secure Private Access 控制台中，单击**访问策略**，然后单击**策略建模**选项卡。
2. 添加以下详细信息：

- **设备类型**：默认选择“桌面”。
- **域**：选择与用户关联的域。
- **用户**：选择要分析其应用程序和关联策略的用户名。

3. 您还可以根据最终用户及其设备上的上下文标记模拟条件。

- 单击**模拟条件**。“上下文标记”条件默认处于选中状态。
- 在**值**中输入上下文标记。
- 单击 **+** 号添加其他条件。

4. 单击**应用**。

所选用户的应用程序和关联策略以表格形式显示。

Application Name	Result	Policy Name
avanthika	Access will be allowed	avanthika_pol
buddi_nani	No access policy found	N/A

配置数据丢失防护 (DLP) 策略

访问限制在 Google 管理控制台中为 CEP 配置。以前在 Secure Private Access 控制台中配置的访问限制仅适用于 Citrix Enterprise Browser。当 Google Chrome 是企业浏览器时，访问限制必须在 Google 管理控制台中配置为策略和规则。

策略在 **Google 管理控制台 > 设备 > Chrome > 设置** 中配置。这些设置允许您管理浏览器设置，例如阻止 JavaScript 和允许打印机列表。

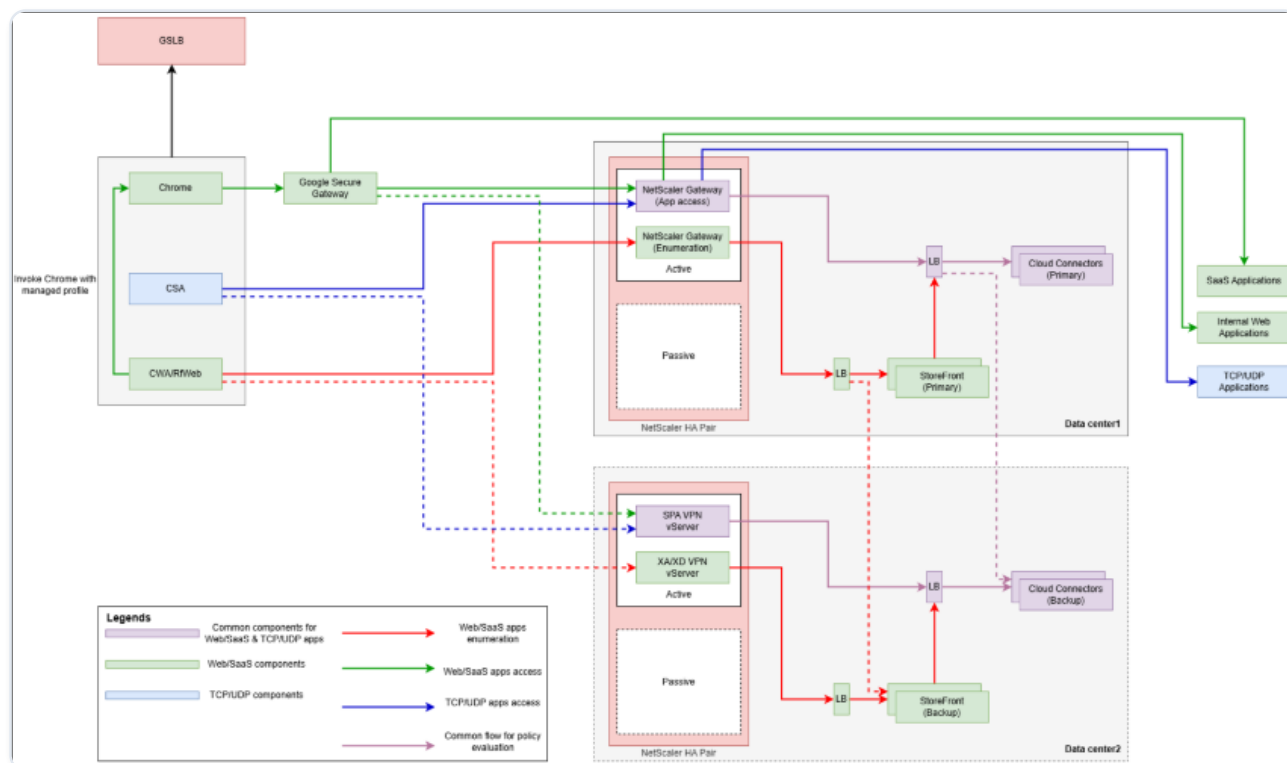
规则在 **Google 管理控制台 > 规则** 中配置。这些规则是与 DLP 相关的高级设置，例如添加水印、阻止下载包含社会安全号码的文件以及 URL 过滤。

有关在 Google Workspace 管理控制台中创建策略和规则的详细信息，请参阅以下主题：

- [为 Chrome Enterprise 设置 Chrome Enterprise 连接器策略](#)
- [数据保护规则](#)

高可用性部署

您只需几个简单的步骤即可为 Secure Private Access 配置高可用性。



数据中心内的高可用性

以下部分提供了有关数据中心内高可用性的更多信息。

NetScaler

为了实现高可用性，建议创建 [NetScaler 高可用性对](#)。这是一个主动-被动 NetScaler 对。

如果活动 NetScaler 发生故障，被动 NetScaler 会自动提升为活动状态，并且所有用户流量都会路由到新的活动 NetScaler。由于会话也会在 NetScaler 高可用性对之间同步，因此用户无需重新进行身份验证。

有关 NetScaler HA 对的更多详细信息，请参阅[高可用性](#)。

云连接器 (Secure Private Access 服务器)

为 Secure Private Access 配置具有服务组配置的 NetScaler 负载均衡器。

1. 在 NetScaler 上创建新的服务组：导航到 **Configuration > Traffic Management > Load Balancing > Service Groups**。
2. 单击添加。
3. 输入服务组的名称，例如 `primary_spa_servers`。

4. 根据负载均衡器类型（**SSL** 或 **SSL_BRIDGE**），为服务组选择相应的**协议**。
5. 其他字段保留默认值，然后点击 **OK** 保存服务组。
6. 点击 **No Service Group Member** 以添加当前数据中心的 Cloud Connector。
7. 使用 **IP Based** 选项并添加当前数据中心的 Cloud Connector 的 **IP address** 和 **Port**。默认情况下，Secure Private Access 使用端口 **8443**。其他字段可以保留默认值。
8. 如果需要添加额外的 Cloud Connector，请重复此步骤。
9. 点击 **Create** 以创建负载均衡服务。
10. 点击 **OK** 将服务添加到服务组。

注意：

您可以选择为 Secure Private Access 服务添加 HTTP 监视器。可以使用以下 URL 路径来完成此操作。

`/secureAccess/health`

如果 Secure Private Access 正常运行，它将返回 **200 OK**。

11. 点击 **Done**。
12. 现在创建一个负载均衡器。导航到 **Configuration > Traffic Management > Load Balancing > Virtual Servers**。
13. 点击 **Add**。
14. 输入负载均衡器名称。
15. 选择适当的 **Protocol**，例如 **SSL** 或 **SSL_BRIDGE**。
16. 将 **IP 地址类型** 设置为 **IP 地址**，将 **端口** 设置为 `443`。

注意：

协议必须是 **SSL** 或 **SSL_BRIDGE**。Secure Private Access 负载均衡器不支持 **HTTP** 类型。端口必须是 **443**。不支持自定义 **HTTPS** 端口。

17. 单击 **确定**。
18. 单击 **无负载均衡虚拟服务器服务组绑定**。
19. 单击以选择之前创建的服务组，然后单击 **选择**。
20. 将 **顺序** 值设置为 **10**。单击 **绑定**，然后单击 **继续**。

21. 如果使用 **SSL** 类型 协议，请单击 **无服务器证书** 以绑定相应的服务器证书。对于 SSL_BRIDGE 类型的负载均衡器，负载均衡器中不需要服务器证书，但必须在 Cloud Connector 中为 Secure Private Access 服务配置服务器证书。有关详细信息，请参阅 [在 Cloud Connector 上为 Secure Private Access 服务配置 TLS/SSL 证书](#)。

Secure Private Access 的负载均衡器与服务组配置到此结束。

负载均衡器中的所有 Secure Private Access 服务器都处于活动状态。如果一个 Secure Private Access 服务器出现故障，用户不会受到影响，因为其他 Secure Private Access 服务器会继续处理流量。Secure Private Access 服务器是无状态的，因此没有持久性要求。

StoreFront 服务器

在同一数据中心内进行故障转移时，StoreFront 服务器的行为也与 Secure Private Access 服务器相同。

重置 Secure Private Access 配置

如果您有集成了 Citrix Enterprise Browser 的 Citrix Secure Private Access 混合部署，并且您想切换到 Chrome Enterprise Premium，您可以重置 Secure Private Access 配置。此操作将删除整个配置，包括应用程序和访问策略。StoreFront 和 NetScaler 配置需要手动清理。配置重置后，您可以再次加入 Secure Private Access 混合部署并选择 Chrome Enterprise Premium。

如果您需要重置配置，请联系 Citrix 支持。

可见性和监控

Secure Private Access 与 Monitor（Citrix DaaS 的监控和故障排除控制台）集成。管理员和技术支持人员除了可以使用 Secure Private Access 控制板之外，还可以从 DaaS Monitor 监控和排查 Web/SaaS 和 TCP/UDP 应用程序会话和事件。

服务授权

要将 DaaS Monitor 功能与 Secure Private Access 结合使用，您必须同时拥有 Secure Private Access 和 DaaS 授权。

支持的客户端

- Citrix Workspace™ 应用程序 - 2409 及更高版本
- 适用于 Windows 的 Citrix Secure Access - 24.8.1.19 及更高版本
- 适用于 macOS 的 Citrix Secure Access - 24.10.1 及更高版本

如何访问 Monitor

您可以从 Secure Private Access 控制板（[转到 Monitor](#)）或 Citrix DaaS™ 服务磁贴访问 Monitor。

在 **Monitor** 页面中，搜索用户以查看会话。

会话定义

Secure Private Access 会话提供最终用户在特定设备上的会话生命周期、应用程序活动和用户体验的全面摘要。会话通过提供以下方面的可见性，作为故障排除和分析的统一记录：

- 详细了解应用程序的访问方式，包括启动跃点、网络拓扑、连接和路由详细信息。这些详细信息对于解决与访问策略相关的问题至关重要。
- 跟踪所有会话活动，包括：
 - 访问 Web 或 SaaS 应用程序的浏览器。
 - 用于使用 TCP/UDP 协议的私有应用程序的 Citrix Secure Access 客户端。

Secure Private Access 会话的一些主要特征包括：

- 每个会话都分配有一个唯一的 ID，用于跟踪和分析。
- 单个会话可以包含多个应用程序启动，并提供该特定会话中用户活动的全面视图。
- 对于每个应用程序，会话会跟踪：
 - 适用于该应用程序的安全控制。
 - 触发安全控制的策略显示名称和 ID。
 - 导致策略强制执行的条件。
- 会话会跟踪用户在 Citrix Enterprise Browser™ 中访问过的所有内部域，从而深入了解用户在安全环境中的导航情况。

Web/SaaS 应用程序会话

Web/SaaS 应用程序的会话开始和结束定义如下：

- 开始：在 Citrix Workspace 应用程序中打开 Citrix Enterprise Browser 并访问应用程序。
- 结束：会话在以下情况下结束。
 - 您关闭思杰企业浏览器。
 - 在 30 分钟不活动后，如果没有报告会话活动。

Citrix Enterprise Browser 客户端每 15 分钟向 Monitor 发送一次会话活动。如果 30 分钟内未收到此会话活动，这可能是由于以下原因造成的：

- 网络故障。
- 互联网连接问题。
- 在 30 分钟不活动间隔后，会话将自动关闭。

注意：

对于通过本机浏览器（无代理）启动的应用程序，会话在 120 分钟不活动后结束。

TCP/UDP 应用程序会话

TCP/UDP 应用程序的会话开始和结束定义如下：

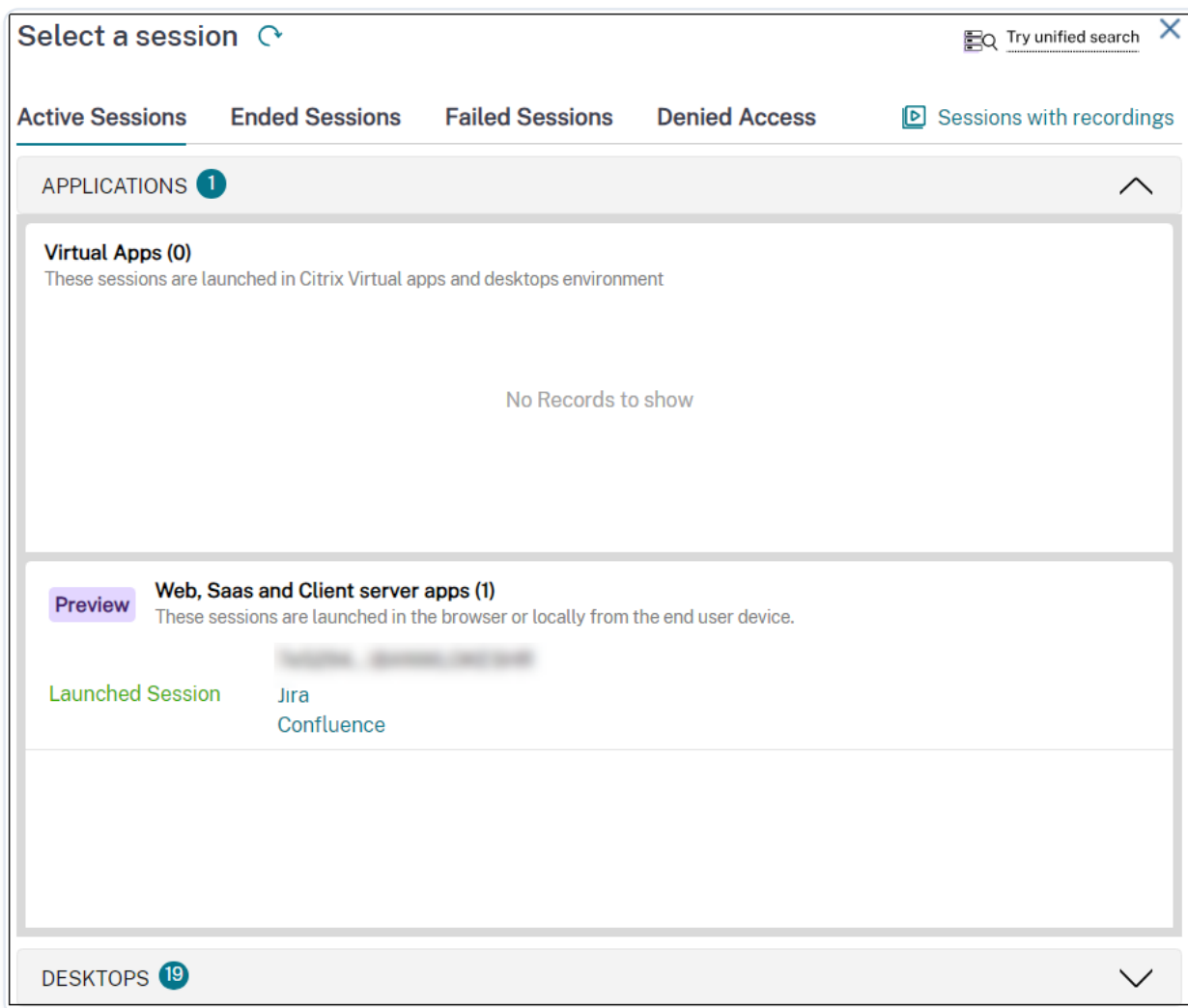
- 开始：您登录 Citrix Secure Access™ 客户端并访问应用程序。
- 结束：会话在以下情况下结束。
 - 您退出 Citrix Secure Access 客户端。

- 在 30 分钟不活动后，如果没有报告会话活动。

查看用户会话

执行以下步骤以查看用户会话：

1. 搜索用户以查看会话。
 - “**选择会话**”页面显示所有活动会话。如果您在“**活动会话**”选项卡中找不到您的会话，请在“**拒绝访问**”选项卡中查看。
 - “**已结束会话**”和“**失败会话**”选项卡不适用于 Secure Private Access。



2. 在“**活动会话**”选项卡中，单击会话 ID 以查看会话详细信息。

此时将显示“**活动管理器**”页面。

3. 单击以下选项卡之一：
 - **已启动的应用程序**：查看用户启动的所有应用程序以及访问策略评估的结果（允许或拒绝）。

如果在同一会话中多次访问某个应用程序，则仅捕获最新的启动详细信息。

- **可用应用程序：** 查看此用户启动的所有应用程序的应用程序枚举详细信息。
 - 如果 Citrix Workspace 应用程序为用户发送了多个枚举请求，则仅捕获最新的枚举详细信息。
 - 对于 TCP/UDP 应用程序（Web 和 ZTNA），尽管没有应用程序枚举的概念，但所有已配置并与用户关联的应用程序都列在“可用应用程序”列表中。
 - “可用应用程序”列表不包含通过 Citrix Secure Access 客户端枚举的外部应用程序，因为它们未通过 Secure Private Access 进行隧道传输。
 - 对于 Citrix Secure Access 代理，“可用应用程序”列表仅显示内部 Web 和 TCP/UDP 应用程序。

The screenshot shows the Citrix Activity Manager interface. The left sidebar contains navigation options: Dashboard, Trends, Filters, Alerts, Applications, Probes, Cost optimization, Infrastructure, Integrations and data exports, Analytics, Settings, and Secure Private Access. The main area is titled 'Activity Manager' and shows a list of 'Launched Apps (Sessions)'. The table below displays the details of two launched applications.

Launch Time	Resource Name	Resource Type	Accessed Resource	Status	Transaction ID
10/03/2024 2:54 PM	Jira	SaaS	Atlassian Cloud (Jira)	Allow	e7e9ab67-5f31-4858-9991-cd8cc9584
10/03/2024 2:54 PM	Confluence	Web	Atlassian Cloud (Confluence)	Allow	8ae5f593-fb23-43fc-99df-8fc9eetcc4f

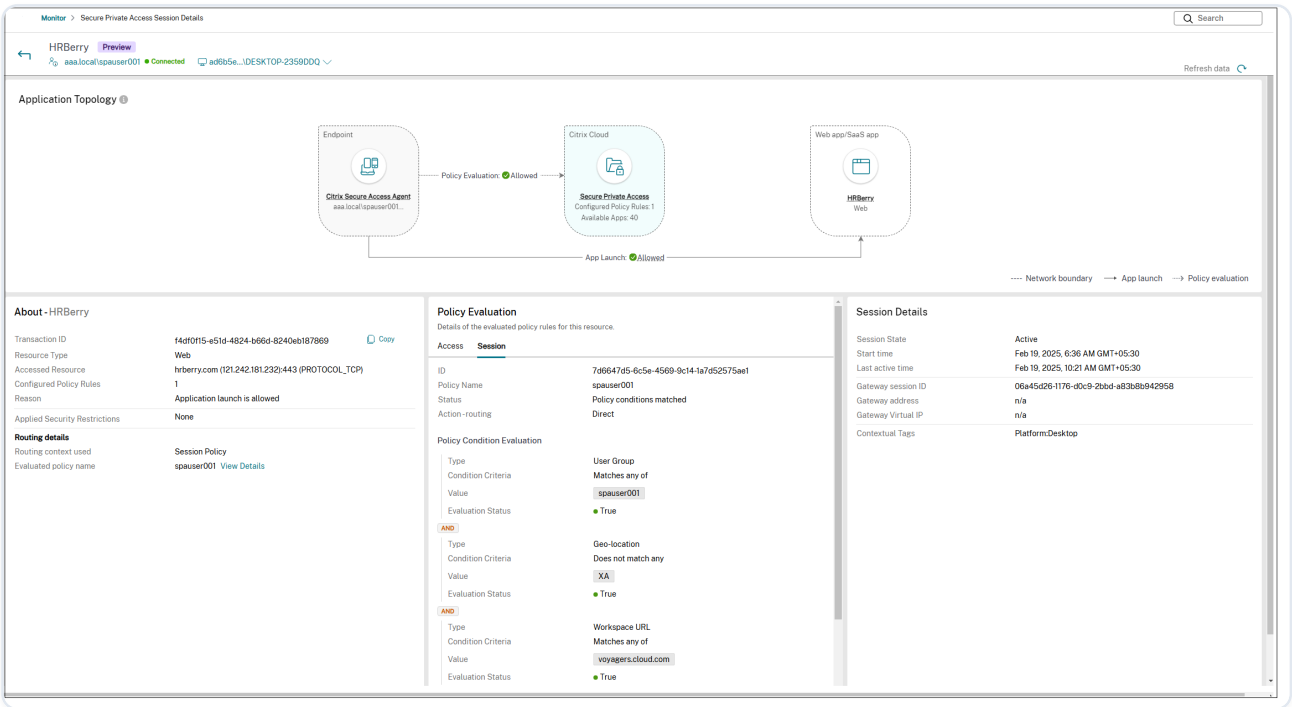
应用程序拓扑

当您从“已启动的应用程序”或“可用应用程序”选项卡中单击某个应用程序时，将显示应用程序拓扑页面，其中显示有关该应用程序的完整信息。

- **会话拓扑：** 显示应用程序启动流程。
- **关于：** 显示应用程序相关信息，例如应用程序类型、策略规则数量、安全限制和访问的资源。
访问的资源 部分中显示的数据因应用程序类型而异。
 - SaaS 应用程序 - URL 或应用程序 FQDN
 - TCP/UDP – IP 地址/FQDN、端口和协议
 - Web 应用程序（通过 Citrix Secure Access 客户端启动） - FQDN、端口和协议
 - Web 应用程序（通过 Citrix Workspace 应用程序启动） - URL

- **策略评估：** 显示与访问策略相关的信息，例如规则、操作和条件。
- **会话详细信息：** 显示与会话相关的信息，包括会话开始和结束时间、会话状态以及与策略关联的上下文标签。
 - **访问的域**字段仅适用于 Web/SaaS 应用程序，并且仅在 15 分钟后更新，因为 macOS 和 Windows 上的 Citrix Enterprise Browser 客户端每 15 分钟发送一次会话活动。
 - 对于从“**可用应用程序**”选项卡中点击的应用程序，“**会话详细信息**”列部分保持为空，因为应用程序枚举不与会话关联。

下图显示了成功启动的应用程序的示例拓扑图。



下图显示了访问被拒绝的应用程序的示例拓扑图。

访问被拒绝的应用程序的应用程序拓扑(/en-us/citrix-secure-private-access/media/spa-monitor-application-topology-denied-access.png)

分类和故障排除

本主题概述了有效排查和分类与 Citrix Secure Private Access 相关问题的重要注意事项和步骤。管理员可以使用本文档作为识别、诊断和解决问题，确保用户无缝安全访问的指南。

Citrix Secure Access 模式下的用户/客户端问题

以下部分提供了有关 Citrix Secure Access 模式下用户/客户端问题的更多信息。

用户无法登录

要检查的事项：

- 检查 VPN 虚拟服务器和身份验证虚拟服务器是否处于 UP 状态。

```
> show vpn vserver _spa_cep_csa_vpn_vs_10.8.0.35
_spa_cep_csa_vpn_vs_10.8.0.35 (10.8.0.35:443) - SSL      Type: CONTENT
State: UP

> show authentication vserver authvs
authvs (0.0.0.0:0) - SSL      IPSet: ???      Type: CONTENT
State: UP  ARP:DISABLED
```

- 检查 Secure Private Access 配置文件 URL 状态是否处于 UP 状态。

```
> show vpn securePrivateAccessProfile _spa_cep_csa_profile
1)      Name: _spa_cep_csa_profile
        URL: https://stg4spalb.spagwcep.corp [Status: UP]
```

- 确保在 Secure Private Access 管理控制台中为用户正确配置了应用程序和访问策略。请参阅 [应用程序配置和管理](#) 和 [配置应用程序的访问策略](#)。
- 检查负载均衡器虚拟服务器状态，确保所有连接器服务器都已添加并处于 UP 状态。
- 要排查任何 nFactor 身份验证问题，请参阅 [排查身份验证、授权和审计问题](#)。

确认上述内容后，请执行以下操作：

1. 启用调试级别日志记录并从 NetScaler 收集支持包。
2. 在 CSA 客户端上启用详细日志记录并收集客户端日志。

3. 联系 Citrix 支持并提供收集到的诊断信息。

用户无法启动应用程序

要检查的事项：

- 在 Citrix Monitor 中，搜索用户 UPN 并验证是否存在活动的 Secure Private Access 会话。

Monitor 中的活动会话(/en-us/citrix-secure-private-access/media/spa-hybrid-active-session.png)

- 启动的应用程序必须显示在“可用应用程序”下。
- 应用程序的“应用程序启动允许”事件必须在“已启动应用程序”下可见。

已启动应用程序(/en-us/citrix-secure-private-access/media/spa-hybrid-monitor1.png)

- 如果不存在，请检查 Secure Private Access 管理控制台中是否为用户正确配置了应用程序和访问策略。
- 在 Citrix Monitor 中，在“已启动应用程序”下查找应用程序的任何应用程序启动错误事件。

已启动应用程序错误(/en-us/citrix-secure-private-access/media/spa-hybrid-monitor-2.png)

- 常见错误：DNS 解析失败/TCP 连接失败。
- 从 NetScaler CLI，验证从相应的 SNIP 到应用程序的连接。

收集具有调试级别日志记录的 NetScaler 支持包的步骤

1. 从 CLI 设置调试级别的 syslog。

```
set syslogparams loglevel ALL DEBUG
```

2. 从 Shell 启用 Secure Private Access 特定的详细日志记录。

```
nsapimgr_wr.sh -ys ns_vpn_enable_spa_verbose_logging=1
```

3. 收集支持包（和可选跟踪）
4. 使用您的标准方法收集 NetScaler 支持包。
5. 如果支持人员要求，可选择捕获额外的跟踪。

重要提示：

收集包后，恢复详细日志记录。保持详细日志记录启用可能会生成过多的日志并影响性能。收集完成后，务必恢复详细日志记录。

恢复详细日志记录

1. 从 CLI 恢复 syslog 级别。

```
set syslogparams loglevel ALL
```

2. 从 Shell 禁用 Secure Private Access 特定的详细日志记录。

```
nsapimgr_wr.sh -ys ns_vpn_enable_spa_verbose_logging=0
```

其他参考：

- [如何为 NetScaler® 实例日志生成技术支持包](#)
- [如何在 NetScaler 上记录数据包跟踪](#)

有助于故障排除的工具

- [配置报告](#)
- [组件分析器](#)
- [策略建模](#)

收集客户端日志

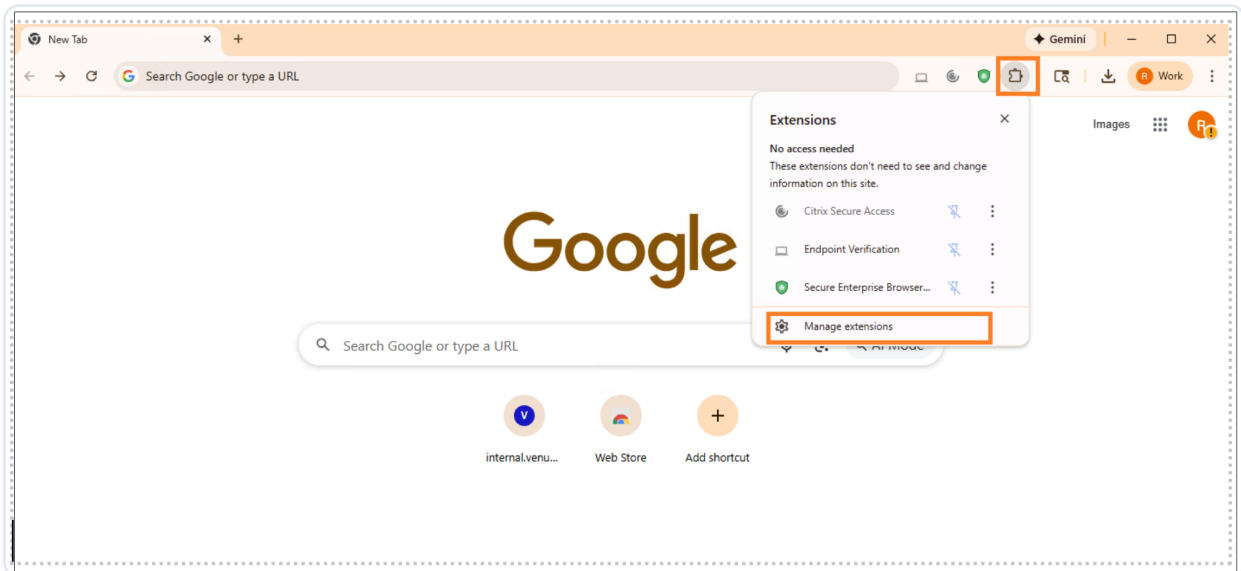
以下部分提供了有关收集客户端日志的更多信息。

Chrome 企业高级版日志

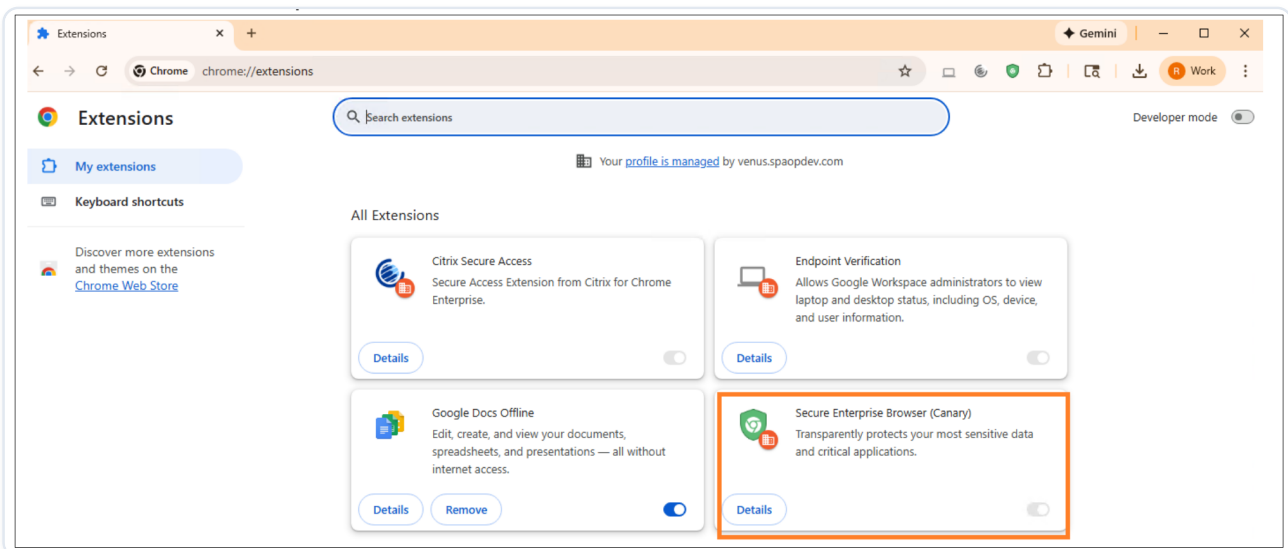
如果您在使用 Chrome Enterprise Premium 时遇到客户端问题，请收集 Secure Enterprise Browser 和 Citrix Secure Access 的扩展日志。

捕获 Secure Enterprise Browser 扩展日志的步骤

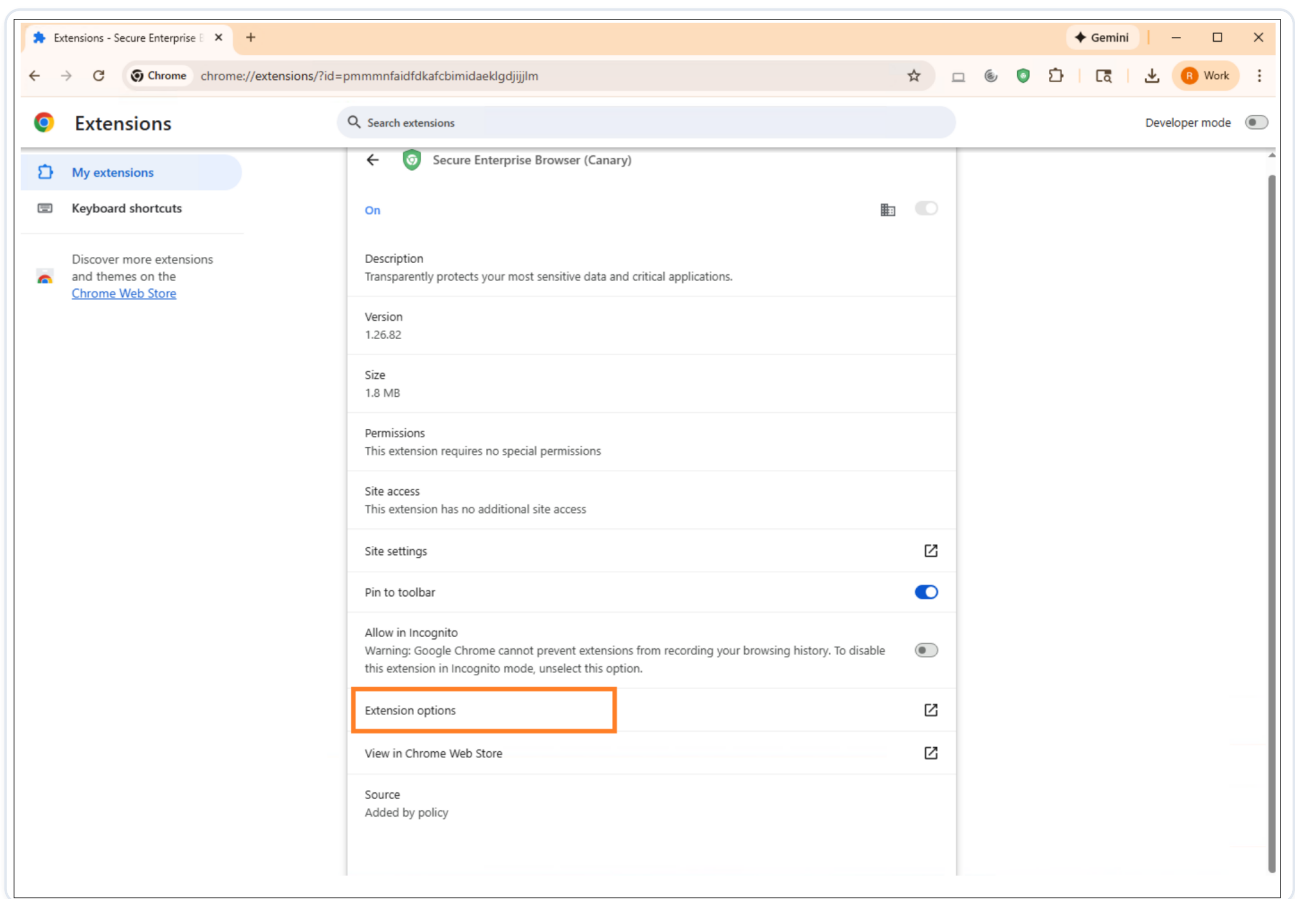
1. 打开 Chrome 浏览器。
2. 切换到您的托管 Chrome 配置文件。
3. 单击“**扩展程序**”图标并选择“**管理扩展程序**”。



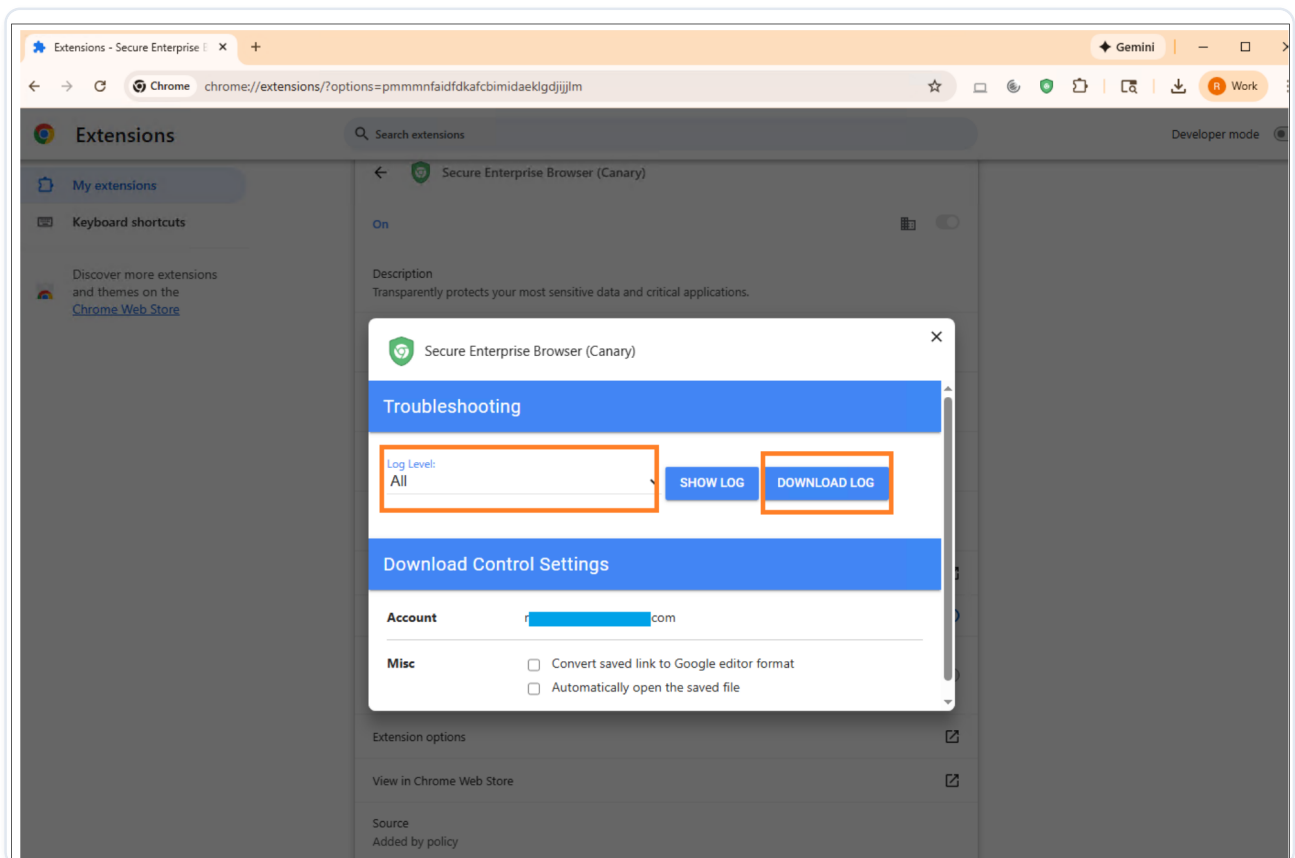
4. 在 Secure Enterprise Browser 下，单击“详细信息”。



1. 选择“扩展程序选项”。



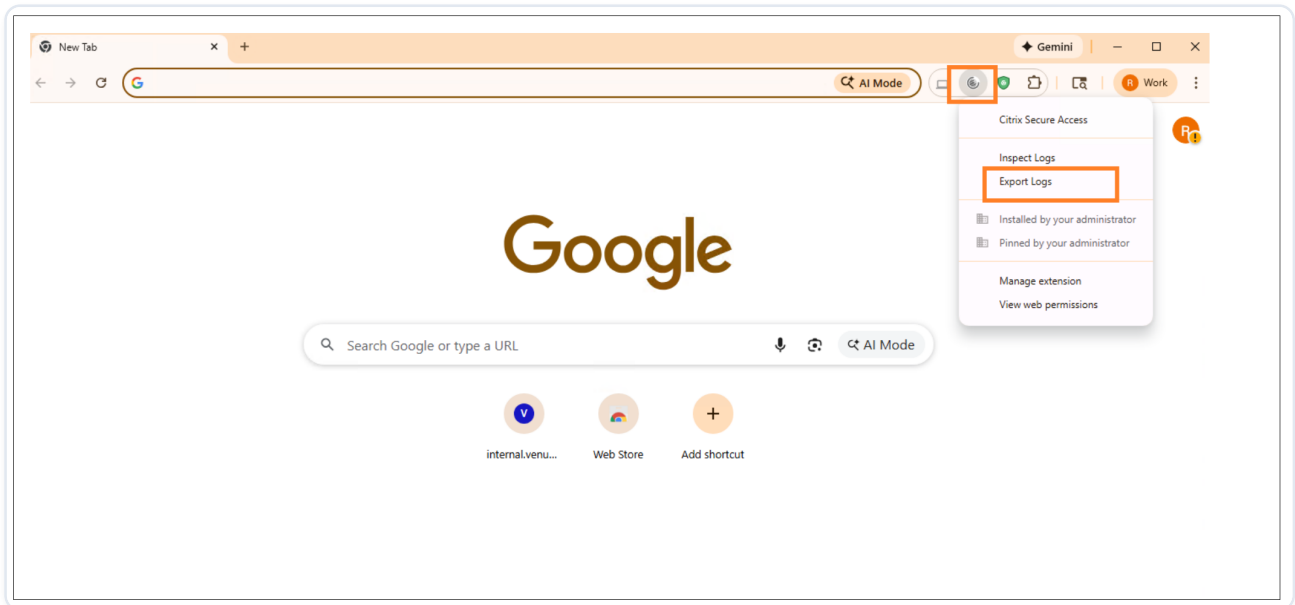
1. 单击“下载日志”。



1. 将下载的日志文件保存到您的计算机。

捕获 Citrix Secure Access 扩展日志的步骤

1. 打开 Chrome 浏览器。
2. 切换到您的托管 Chrome 配置文件。
3. 单击地址栏旁边的 **Citrix Secure Access** 扩展图标。
4. 选择 **导出日志**。



1. 将导出的日志文件保存到您的计算机。

使用 Monitor 进行实时会话故障排除

管理员可以使用 Monitor 控制台实时监控 Secure Private Access 会话并排除故障。

有关相关信息，请参阅以下主题：

- 有关将 Secure Private Access 与 Monitor 集成的信息，请参阅 [Integration with DaaS monitor](#)。
- 您可以在 Monitor 中搜索 Secure Private Access 用户会话，以快速定位用于故障排除和报告的特定会话。有关详细信息，请参阅 [View a Secure Private Access session by user](#)。
- 有关 Monitor 的更多信息，请参阅 [DaaS Monitor](#)。

捕获了 Secure Private Access 混合部署的以下错误代码：

- [会话代码](#)
- [应用程序枚举消息代码](#)
- [应用程序启动消息代码](#)
- [应用程序启动错误代码](#)

会话代码

代码	状态	描述
2101	失败	会话失败
2102	活动/非活动/失败	会话处于活动状态或已终止，或者会话中至少有一个应用程序启动失败
2000	活动	会话处于活动状态
2001	非活动	会话已终止/非活动

应用程序枚举消息代码

代码	状态	描述
1000	成功	枚举成功。至少枚举了一个应用程序
1001	成功	未枚举任何应用程序，因为它们都被策略拒绝
1002	成功	未枚举任何应用程序，因为没有策略匹配
1003	成功	未枚举任何应用程序，因为有些被拒绝，而另一些没有策略匹配
1004	成功	没有枚举任何应用程序，因为没有要评估的策略
1101	失败	枚举期间发生内部错误
1102	失败	枚举了部分应用程序，但至少有一个应用程序评估失败
1103	失败	没有枚举任何应用程序，并且至少有一个应用程序评估失败
3000	允许	允许应用程序枚举

代码	状态	描述
3001	拒绝	应用程序枚举被策略拒绝
3002	拒绝	未枚举应用程序，因为没有策略匹配
3003	未知	应用程序枚举状态未知
3004	从 CEB 启动应用程序	尝试从 Citrix Enterprise Browser™ 启动应用程序
3101	失败	应用程序枚举 - 发生内部错误（当前未使用）
3102	失败	应用程序未被枚举，因为策略评估期间发生异常
3103	失败	应用程序枚举状态为 null - 策略评估期间发生内部错误
3104	允许/拒绝/失败	检索应用程序策略详细信息时出错

应用程序启动消息代码

代码	状态	描述
4000	允许	允许应用程序启动
4001	拒绝	由于策略原因，应用程序启动被拒绝
4002	拒绝	由于没有匹配的策略，应用程序启动被拒绝
4101	失败	应用程序启动错误 - 应用程序启动期间发生内部错误
4102	失败	应用程序启动错误（内部）
4103	允许/拒绝/失败	检索应用程序策略详细信息时出错

代码	状态	描述
4104	故障	应用程序启动错误 - 未找到应用程序配置

应用程序启动错误代码

代码	描述	解决方案/变通方法
5001	TCP - 连接失败	验证到目标的网络可达性（从 NetScaler Gateway ping <code>-S <SNIP></code> ）。
5003	TCP - 探测失败	同上
5002	TCP - 代理服务器已关闭	确保代理主机已启动。
5004	TCP - 网关内存分配失败	启用调试级别日志记录并从 NetScaler 收集支持包。
5005	TCP - 服务器宕机	验证到目标的网络可达性（从 NetScaler Gateway ping <code>-S <SNIP></code> ），并检查服务器是否已关闭。
5006	TCP - 代理连接失败	确保代理主机已启动并接受连接。
5007	TCP - 代理探测失败	验证到目标的网络可达性（从 NetScaler Gateway ping <code>-S <SNIP></code> ）。启用调试级别日志记录并从 NetScaler 收集支持包。
5008	SPA - 服务器宕机	验证 Secure Private Access 站点 URL 是否已启动。（使用 NetScaler CLI 上的 <code>show vpn securePrivateAccessProfile</code> CLI 命令检查 URL 状态）。

代码	描述	解决方案/变通方法
5009	SPA - 呼出请求错误	验证 Secure Private Access 站点 URL 是否已启动。启用调试级别日志记录并从 NetScaler 收集支持包。 ^
5010	SPA - 呼出响应错误	
5011	TCP - 会话已过期	这表示在用户会话不再活动时访问了应用程序。启动新的活动用户会话。
5013	TCP - 网关内部错误	启用调试级别日志记录并从 NetScaler 收集支持包。
5014	TCP - DNS 服务器已关闭	确保 DNS 服务器已启动。
5015	TCP - 网关 DNS 内部错误	确保 DNS 服务器已启动。启用调试级别日志记录并从 NetScaler 收集支持包。
5016	目标服务器连接失败	验证到目标的网络可达性（从 NetScaler Gateway 使用 ping -S <SNIP>）。
5017	目标服务器 DNS 解析失败	确保您的应用程序使用的主机名由预期的 DNS 服务器（内部或公共）解析。
5018	网关内部错误	启用调试级别日志记录并从 NetScaler 收集支持包。
0x1300000C	应用程序域的 DNS 解析失败	确保您的应用程序使用的主机名由预期的 DNS 服务器（内部或公共）解析。

最终用户体验

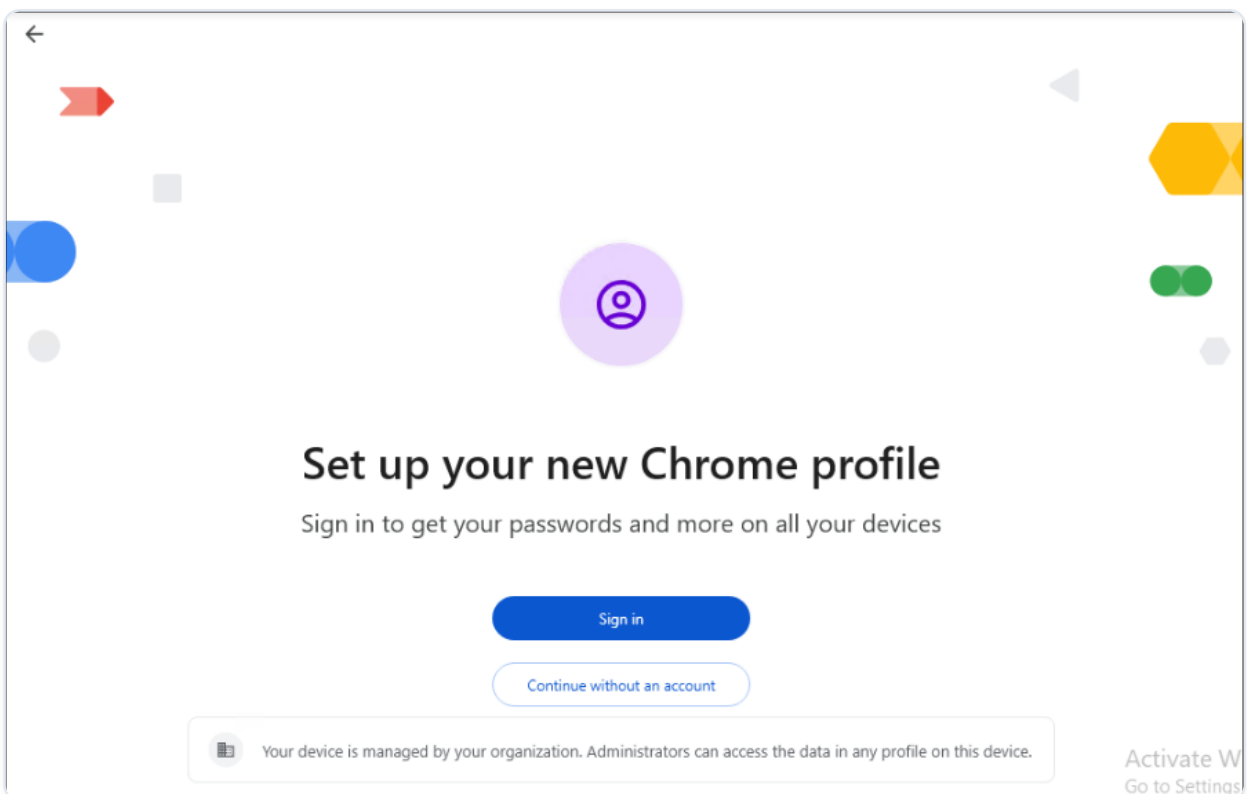
以下各节提供了有关最终用户体验的更多信息。

使用 Chrome Enterprise Premium 访问 Web 和 SaaS 应用程序

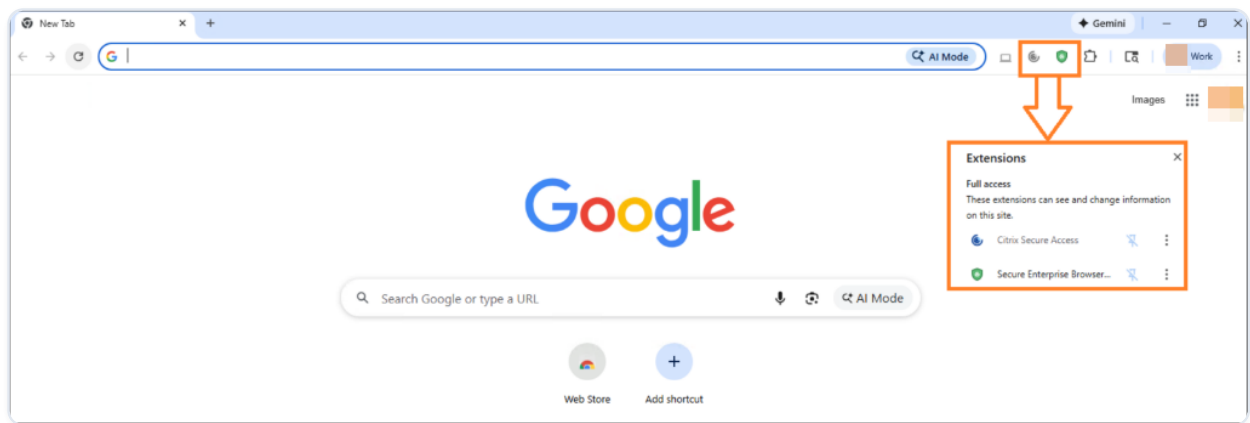
您可以通过四种不同的方式使用 Chrome Enterprise Premium 访问已发布的内部 Web 应用程序和外部 SaaS 应用程序。选择适用于您环境的选项。

选项 1：创建托管的 Chrome 配置文件并直接访问应用程序（推荐）

- 打开 Chrome 浏览器。
- 使用您公司的凭据添加新的 Chrome 配置文件（即，创建托管的 Chrome 配置文件）。

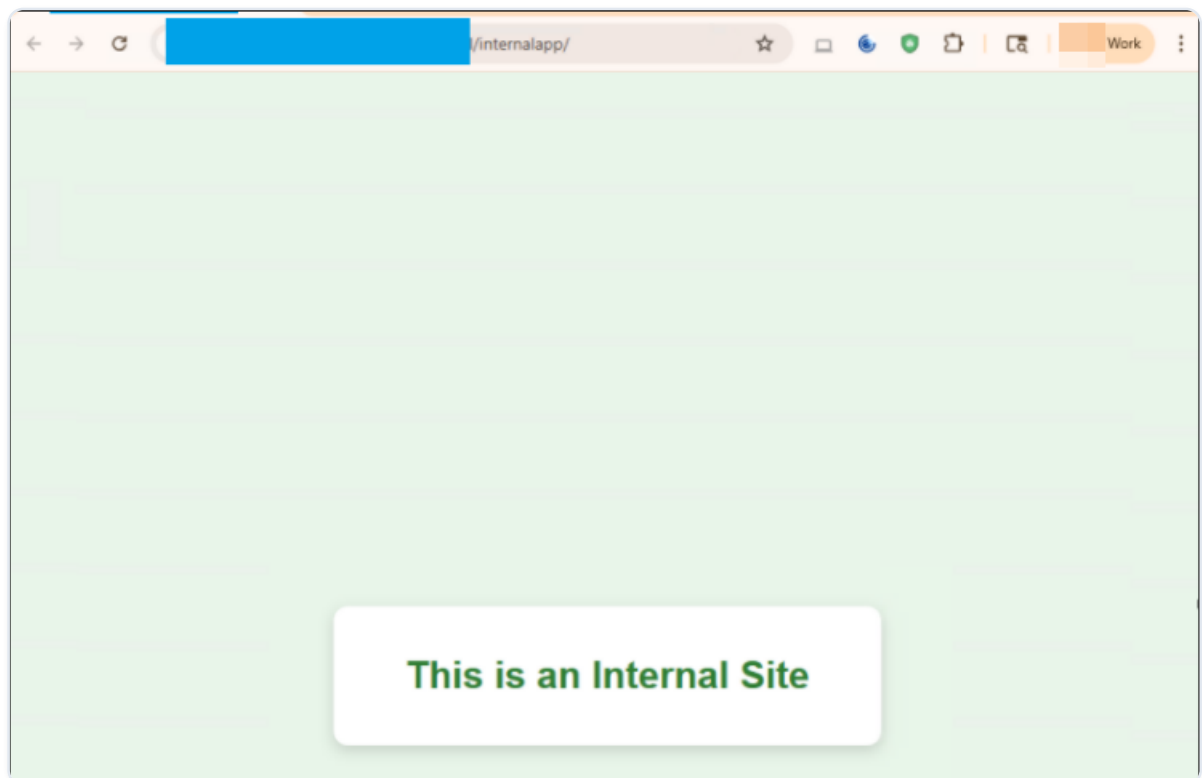


- 配置文件创建后，将自动安装两个扩展程序：
 - Citrix 安全访问
 - 安全企业浏览器



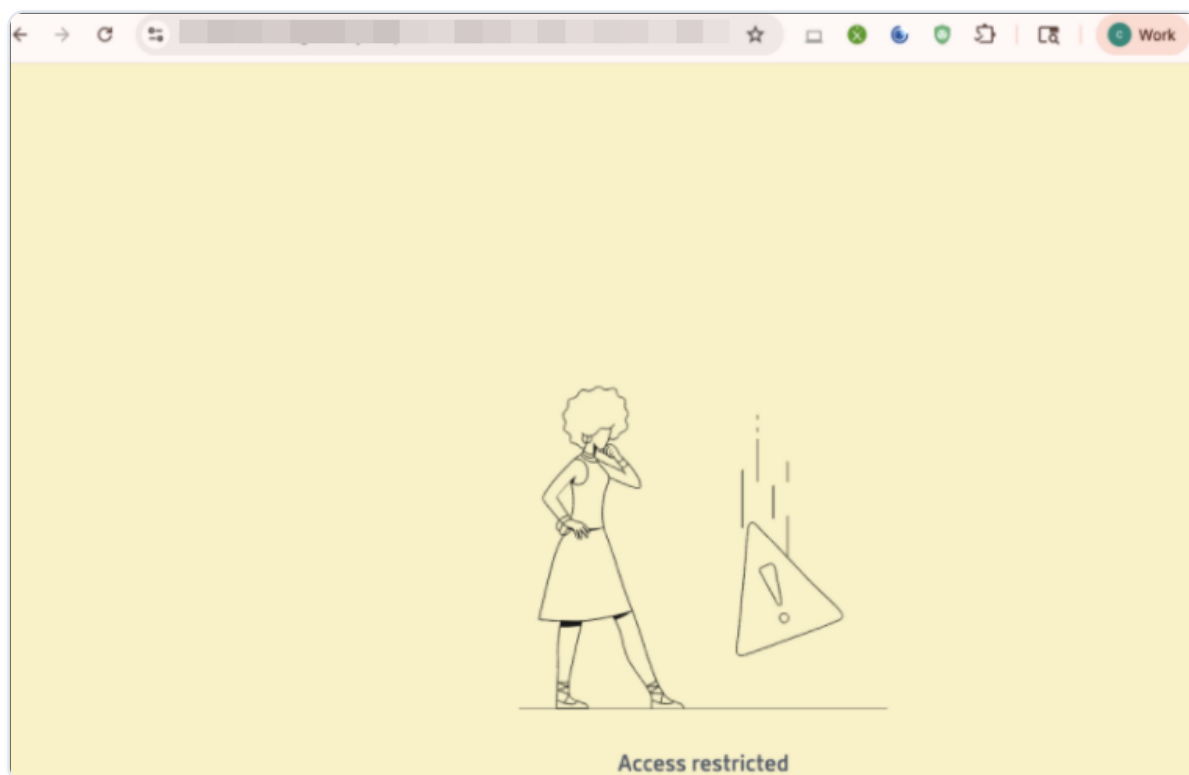
- 通过在地址栏中输入 URL 或导航到已发布的站点来访问内部和外部应用程序。
- 手动输入 URL 时的行为：
 - **内部 Web 应用程序（允许）：**

请求通过 Secure Private Access 安全地隧道传输，然后站点加载。



- **内部 Web 应用程序（已拒绝）：**

Secure Private Access 阻止请求，并显示“访问受限”页面。



- 外部 SaaS 应用程序（已允许）：

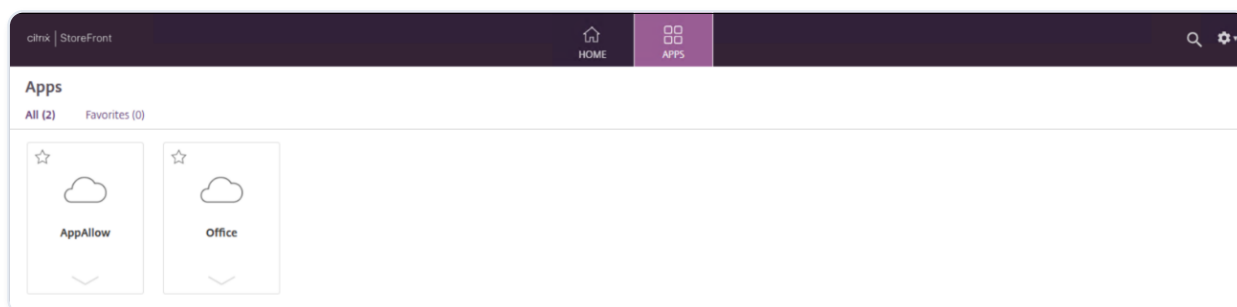
请求直接允许，无需隧道传输。

- 外部 SaaS 应用程序（已拒绝）：

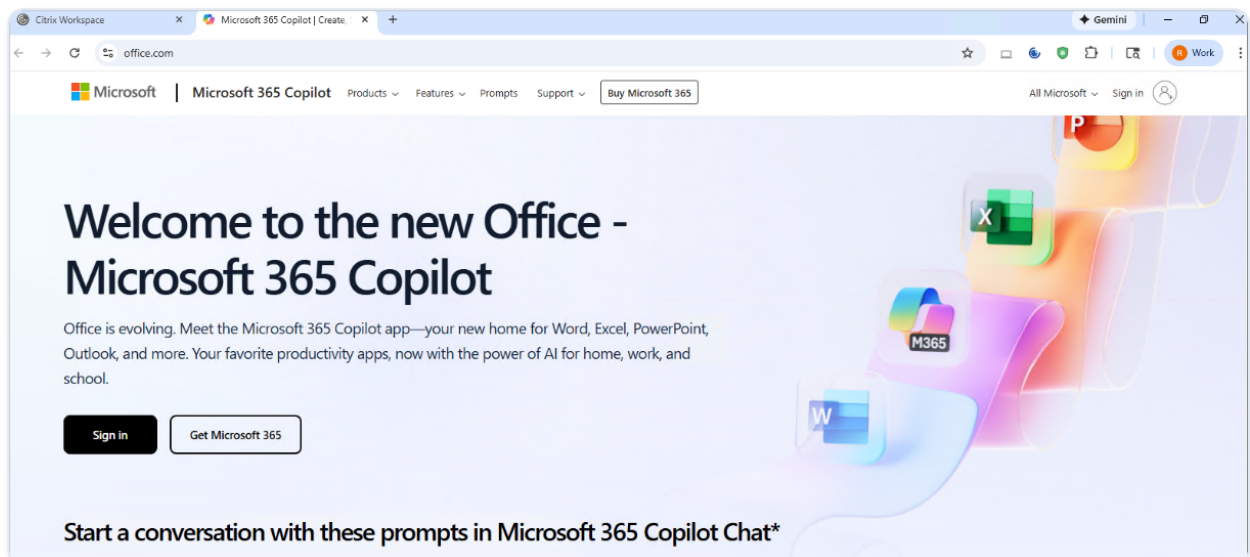
Secure Private Access 阻止请求，并显示“访问受限”页面。

选项 2：在现有托管 Chrome 配置文件中访问商店 URL

- 确保已存在包含公司凭据的托管 Chrome 配置文件。
- 使用正确的公司托管配置文件启动 Chrome。
- 在 Web 浏览器中打开商店 URL。
- 登录商店。
- 转到“应用程序”选项卡，然后选择贵公司管理员发布的 Web/SaaS 应用程序。



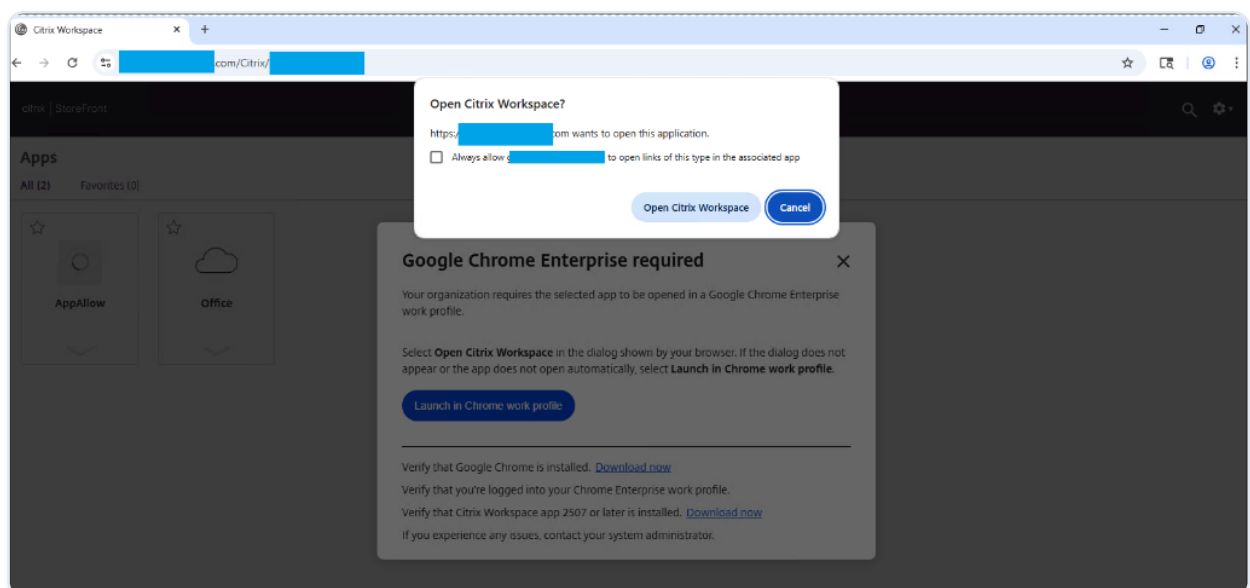
- Web/SaaS 应用程序会在同一个受管 Chrome 配置文件中的新选项卡中无缝启动。



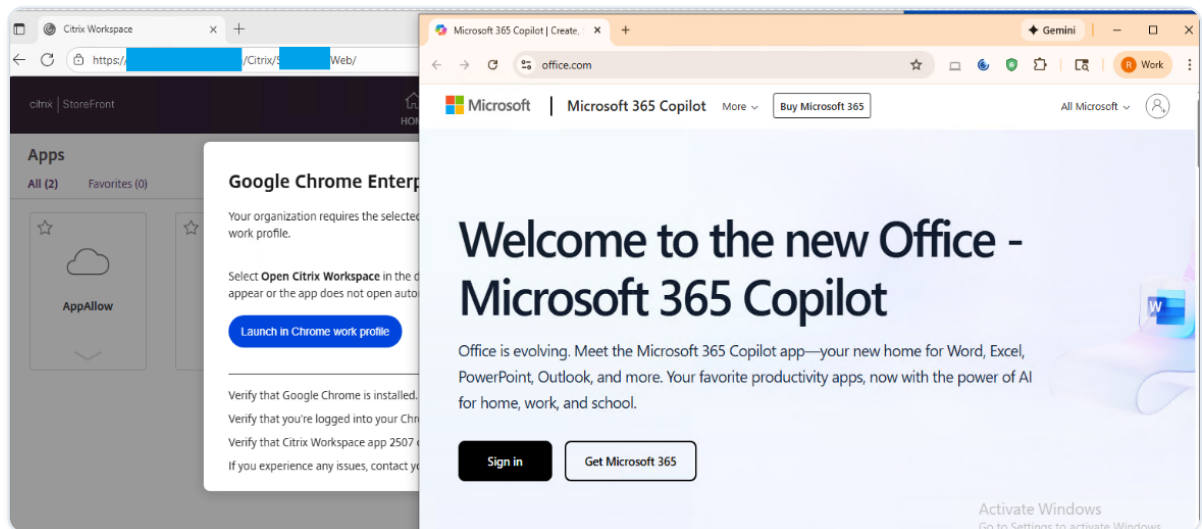
- 允许和拒绝逻辑与 选项 1 相同。

选项 3：从非受管 Chrome 配置文件或非 Chrome 浏览器（Edge、Firefox）访问应用商店 URL

- 启动 Edge、Firefox 或非受管 Chrome 配置文件。
- 在 Web 浏览器中打开应用商店 URL
- 登录到应用商店。
- 转到应用程序选项卡并选择已发布的 Web 应用程序。
- 将出现一个弹出窗口，其中包含显示“打开 Citrix Workspace”按钮的对话框。单击此按钮以继续。



- 单击按钮后，将发生以下情况之一：
 - **受管 Chrome 配置文件已存在：**应用程序直接在受管配置文件中启动。



- ****受管 Chrome 配置文件不存在：****在应用程序启动之前，系统会提示您创建受管 Chrome 配置文件。

创建 Chrome 配置文件(/en-us/citrix-secure-private-access/media/spa-hybrid-chrome-profile-create.png)

- 允许和拒绝逻辑与 (/zh-cn/citrix-secure-private-access/hybrid/spa-hybrid-end-user-flow.html#option-1-create-a-managed-chrome-profile-and-access-apps-directly-recommended) 相同。

选项 4：通过 Citrix Workspace 应用程序访问应用程序

- 使用 Citrix Workspace 应用程序打开 StoreFront 商店。
- 登录到商店。
- 转到“应用程序”选项卡并选择已发布的 Web 应用程序。
- Workspace 应用程序自动启动 Chrome。根据您的设置：
 - **托管 Chrome 配置文件存在：** 应用程序直接在托管配置文件中打开。

现有 Chrome 配置文件(/en-us/citrix-secure-private-access/media/spa-hybrid-chrome-profile-exist.png)

- **托管 Chrome 配置文件不存在：** 系统会提示您在应用程序打开之前创建一个。

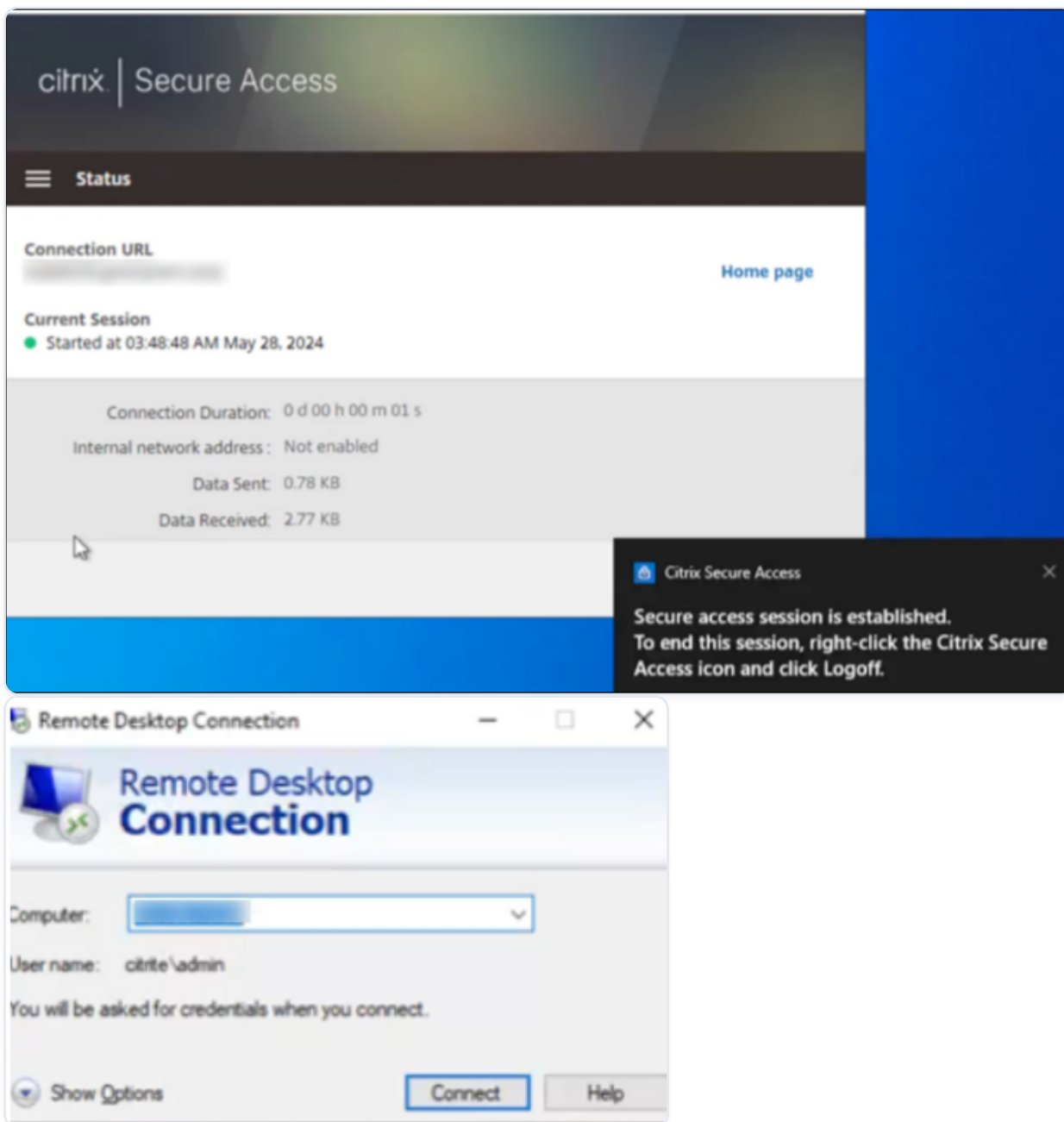
创建 Chrome 配置文件(/en-us/citrix-secure-private-access/media/spa-hybrid-chrome-profile-create.png)

- 允许和拒绝逻辑与 (/zh-cn/citrix-secure-private-access/hybrid/spa-hybrid-end-user-flow.html#option-1-create-a-managed-chrome-profile-and-access-apps-directly-recommended) 相同。

访问客户端/服务器 (TCP/UDP) 应用程序

如果配置了 RDP，最终用户必须执行以下步骤才能访问 TCP/UDP 应用程序：

1. 登录到 Citrix Secure Access 客户端。
2. 安全访问会话建立后，启动远程桌面连接。



- a. 按 Windows 键，键入 **远程桌面连接**，然后按 **Enter**。
- b. 输入您尝试连接的计算机的 IP 地址或主机名。
- c. 单击 **连接**。系统可能会提示您输入凭据。
- d. 输入远程计算机的用户名和密码，然后单击 **确定**。

现已建立远程桌面连接，最终用户可与远程计算机进行交互。

index

- [与 DaaS 监视器集成](#)
- [上下文标签](#)

与 DaaS 监视器集成

Secure Private Access 与 Monitor（Citrix DaaS 的监视和故障排除控制台）集成。管理员和帮助台人员除了可以通过 Secure Private Access 控制板之外，还可以通过 DaaS Monitor 监视和排除 Web/SaaS 和 TCP/UDP 应用程序会话和事件的故障。

服务授权

要将 DaaS Monitor 功能与 Secure Private Access 结合使用，您必须同时拥有 Secure Private Access 和 DaaS 授权。

支持的客户端

- Citrix Workspace™ 应用程序 - 2409 及更高版本
- 适用于 Windows 的 Citrix Secure Access - 24.8.1.19 及更高版本
- 适用于 macOS 的 Citrix Secure Access - 24.10.1 及更高版本

如何访问 Monitor

您可以从 Secure Private Access 控制板（[转到 Monitor](#)）或 Citrix DaaS™ 服务磁贴访问 Monitor。

在 **Monitor** 页面中，搜索用户以查看会话。

会话定义

Secure Private Access 会话提供了最终用户会话生命周期、应用程序活动以及特定设备上的用户体验的全面摘要。会话通过提供以下方面的可见性，作为故障排除和分析的统一记录：

- 详细了解应用程序的访问方式，包括启动跳转、网络拓扑、连接和路由详细信息。这些详细信息对于解决与访问策略相关的问题至关重要。
- 跟踪所有会话活动，包括：

- 访问 Web 或 SaaS 应用程序的浏览器。
- 用于使用 TCP/UDP 协议的私有应用程序的 Citrix Secure Access 客户端。

Secure Private Access 会话的一些主要特征包括：

- 每个会话都分配有一个唯一的 ID，用于跟踪和分析。
- 单个会话可以包含多个应用程序启动，并提供该特定会话中用户活动的全面视图。
- 对于每个应用程序，会话会跟踪：
 - 适用于该应用程序的安全控制。
 - 触发安全控制的策略显示名称和 ID。
 - 导致策略强制执行的条件。
- 会话会跟踪用户在 Citrix Enterprise Browser™ 中访问过的所有内部域，从而深入了解用户在安全环境中的导航情况。

Web/SaaS 应用程序会话

Web/SaaS 应用程序的会话开始和结束定义如下：

- 开始：在 Citrix Workspace 应用程序中打开 Citrix Enterprise Browser 并访问应用程序。
- 结束：会话在以下情况下结束。
 - 您关闭思杰企业浏览器。
 - 30 分钟不活动后，如果没有报告会话活动。

Citrix Enterprise Browser 客户端每 15 分钟向 Monitor 发送一次会话活动。如果 30 分钟内未收到此会话活动，这可能是由于以下原因造成的：

- 网络故障。
- 互联网连接问题。
- 在 30 分钟间隔内没有会话活动后，会话将自动关闭。

注意：

对于通过本机浏览器（无代理）启动的应用程序，会话在 120 分钟不活动后结束。

TCP/UDP 应用程序会话

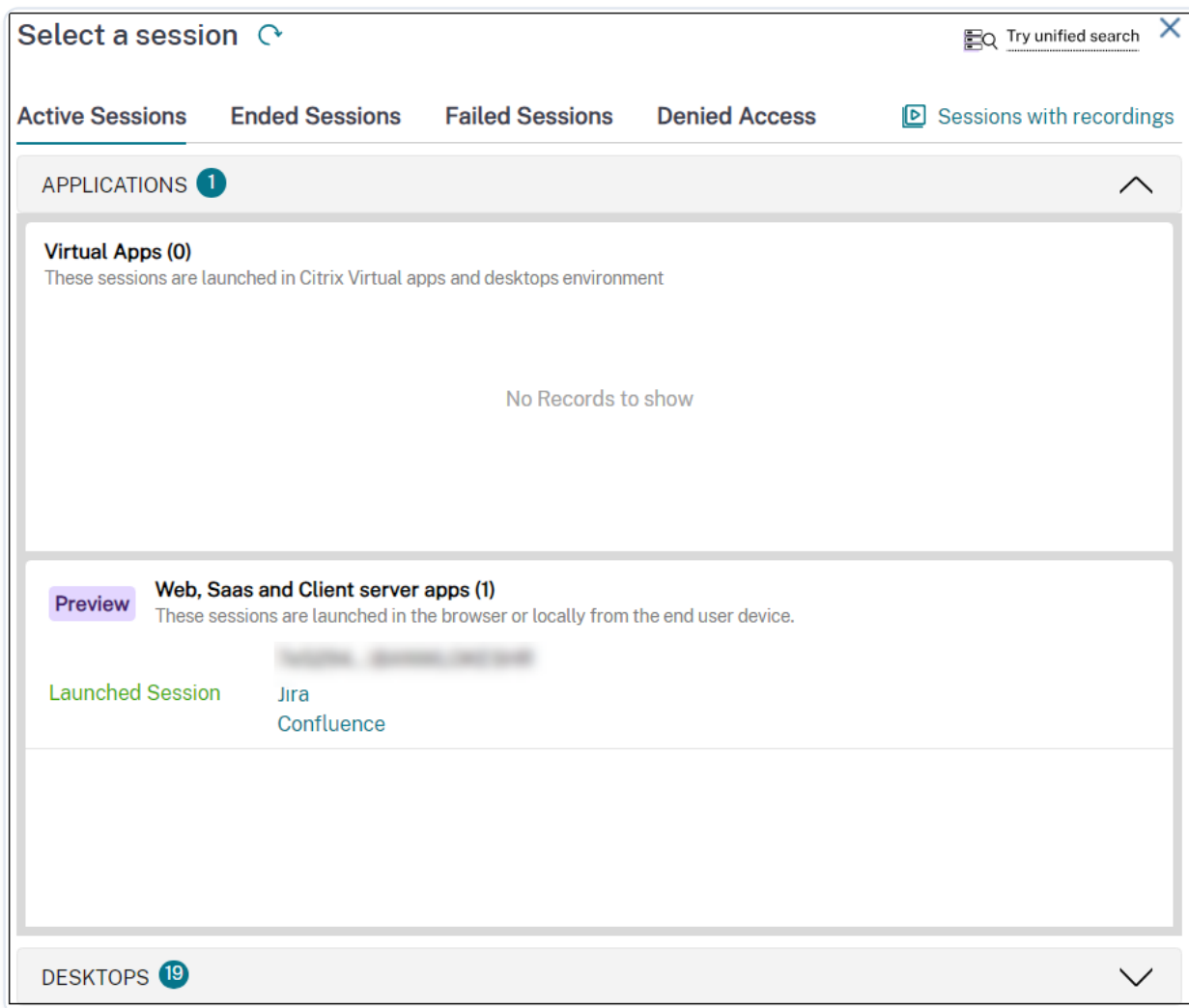
TCP/UDP 应用程序的会话开始和结束定义如下：

- 开始：您登录到 Citrix Secure Access™ 客户端并访问应用程序。
- 结束：会话在以下情况下结束。
 - 您从 Citrix Secure Access 客户端注销。
 - 30 分钟不活动后，如果没有报告会话活动。

查看用户会话

执行以下步骤以查看用户会话：

1. 搜索用户以查看会话。
 - “**选择会话**”页面显示所有活动会话。如果您在“**活动会话**”选项卡中找不到您的会话，请在“**拒绝访问**”选项卡中查看。
 - “**已结束会话**”和“**失败会话**”选项卡不适用于 Secure Private Access。



2. 在“**活动会话**”选项卡中，单击会话 ID 以查看会话详细信息。

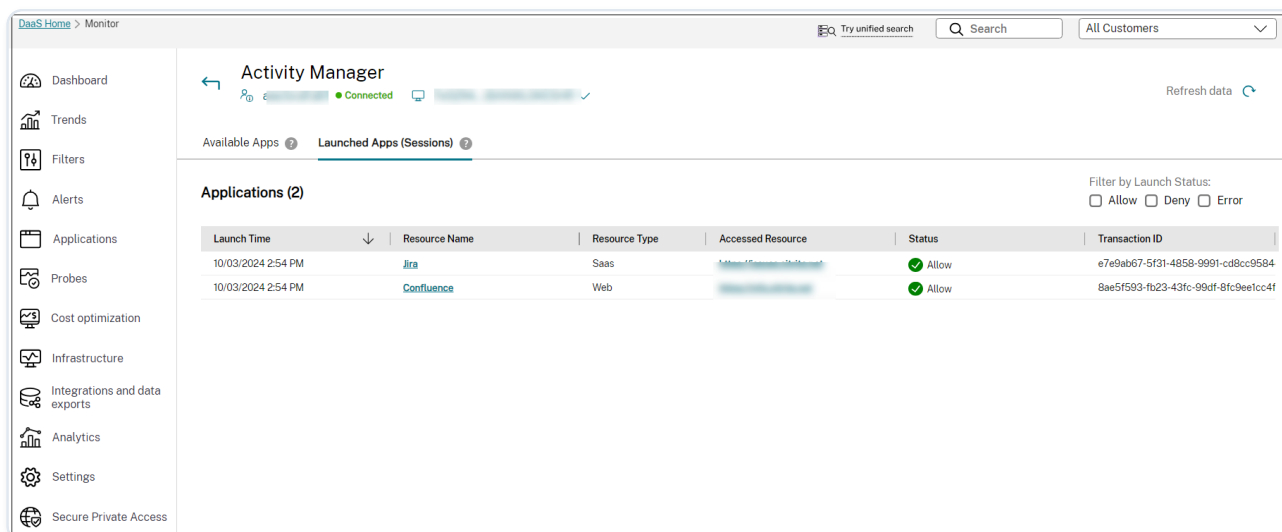
此时将显示“**活动管理器**”页面。

3. 单击以下选项卡之一：

- **已启动的应用程序**：查看用户启动的所有应用程序以及访问策略评估的结果（允许或拒绝）。

如果在同一会话中多次访问某个应用程序，则仅捕获最新的启动详细信息。

- **可用应用程序**：查看此用户启动的所有应用程序的应用程序枚举详细信息。
 - 如果 Citrix Workspace 应用程序为用户发送了多个枚举请求，则仅捕获最新的枚举详细信息。
 - 对于 TCP/UDP 应用程序（Web 和 ZTNA），尽管没有应用程序枚举的概念，但所有已配置并与用户关联的应用程序都列在“可用应用程序”列表中。
 - “可用应用程序”列表不包含通过 Citrix Secure Access 客户端枚举的外部应用程序，因为它们未通过 Secure Private Access 进行隧道传输。
 - 对于 Citrix Secure Access 代理，“可用应用程序”列表仅显示内部 Web 和 TCP/UDP 应用程序。



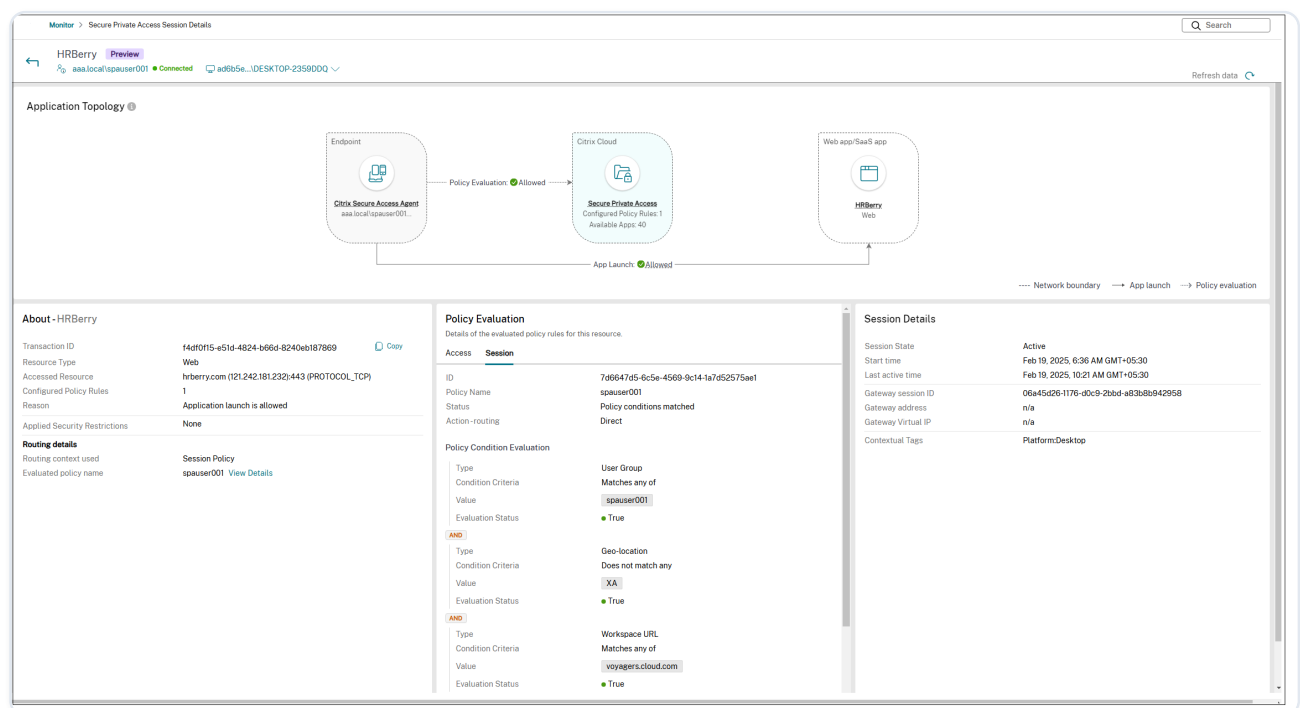
应用程序拓扑

当您从“已启动的应用程序”或“可用应用程序”选项卡中单击某个应用程序时，将显示应用程序拓扑页面，其中显示有关该应用程序的完整信息。

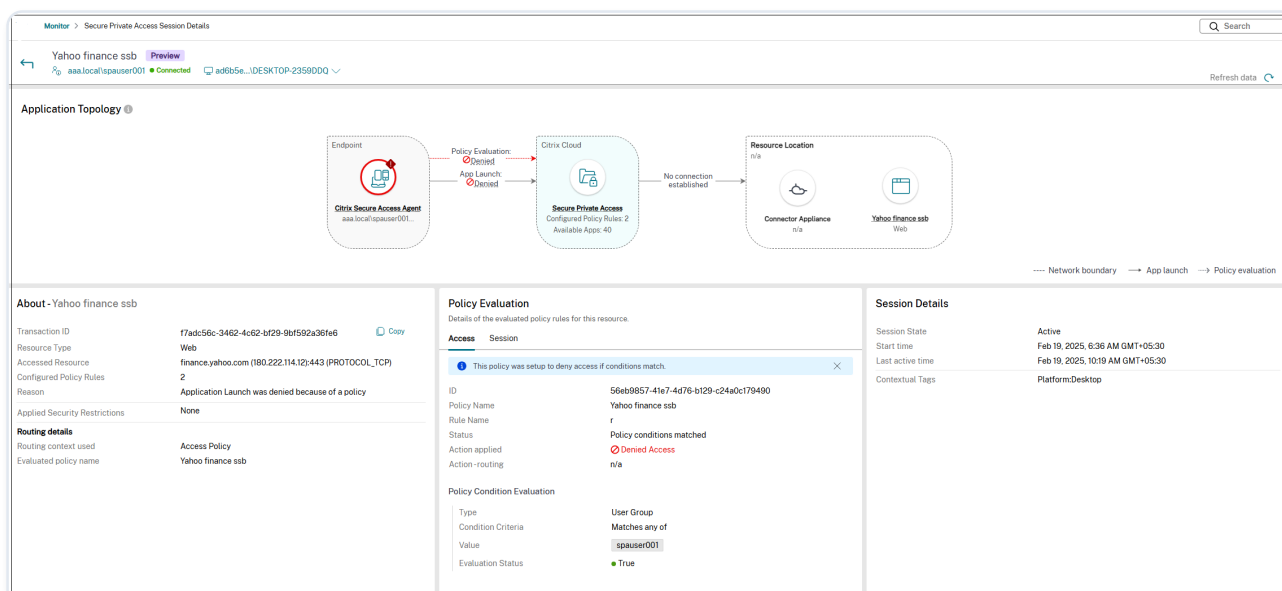
- **会话拓扑**：显示应用程序启动流程。
- **关于**：显示与应用程序相关的信息，例如应用程序类型、策略规则数、安全限制和访问的资源。**访问的资源**部分中显示的数据因应用程序类型而异。
 - SaaS 应用程序 - URL 或应用程序 FQDN
 - TCP/UDP – IP 地址/FQDN、端口和协议

- Web 应用程序（通过 Citrix Secure Access 客户端启动）- FQDN、端口和协议
- Web 应用程序（通过 Citrix Workspace 应用程序启动）- URL
- **策略评估：** 显示与访问策略相关的信息，例如规则、操作和条件。
- **会话详细信息：** 显示与会话相关的信息，包括会话开始和结束时间、会话状态以及与策略关联的上下文标记。
- “访问的域”字段仅适用于 Web/SaaS 应用程序，并且仅在 15 分钟后更新，因为 macOS 和 Windows 上的 Citrix Enterprise Browser 客户端每 15 分钟发送一次会话活动。
- 对于从“可用应用程序”选项卡中单击的应用程序，“会话详细信息”列部分仍为空，因为应用程序枚举未与会话关联。

下图显示了成功启动的应用程序的示例拓扑图。



下图显示了访问被拒绝的应用程序的示例拓扑图。



上下文标签

Secure Private Access 提供程序根据用户会话上下文（例如设备平台和操作系统、已安装软件、地理位置）启用对 Web 或 SaaS 应用程序的上下文访问（智能访问）。

管理员可以将带有上下文标签的条件添加到访问策略。Secure Private Access 提供程序上的上下文标签是应用于已验证用户会话的 NetScaler® Gateway 策略（会话、预身份验证、EPA）的名称。

Secure Private Access 提供程序可以以标头（新逻辑）形式接收智能访问标签，或通过回调到 Gateway。有关详细信息，请参阅[添加新的上下文标签](#)。

使用 GUI 配置自定义标签

配置上下文标签涉及以下高级步骤。

1. 配置经典网关预身份验证策略。
2. 将经典预身份验证策略绑定到网关虚拟服务器。

配置经典网关预身份验证策略

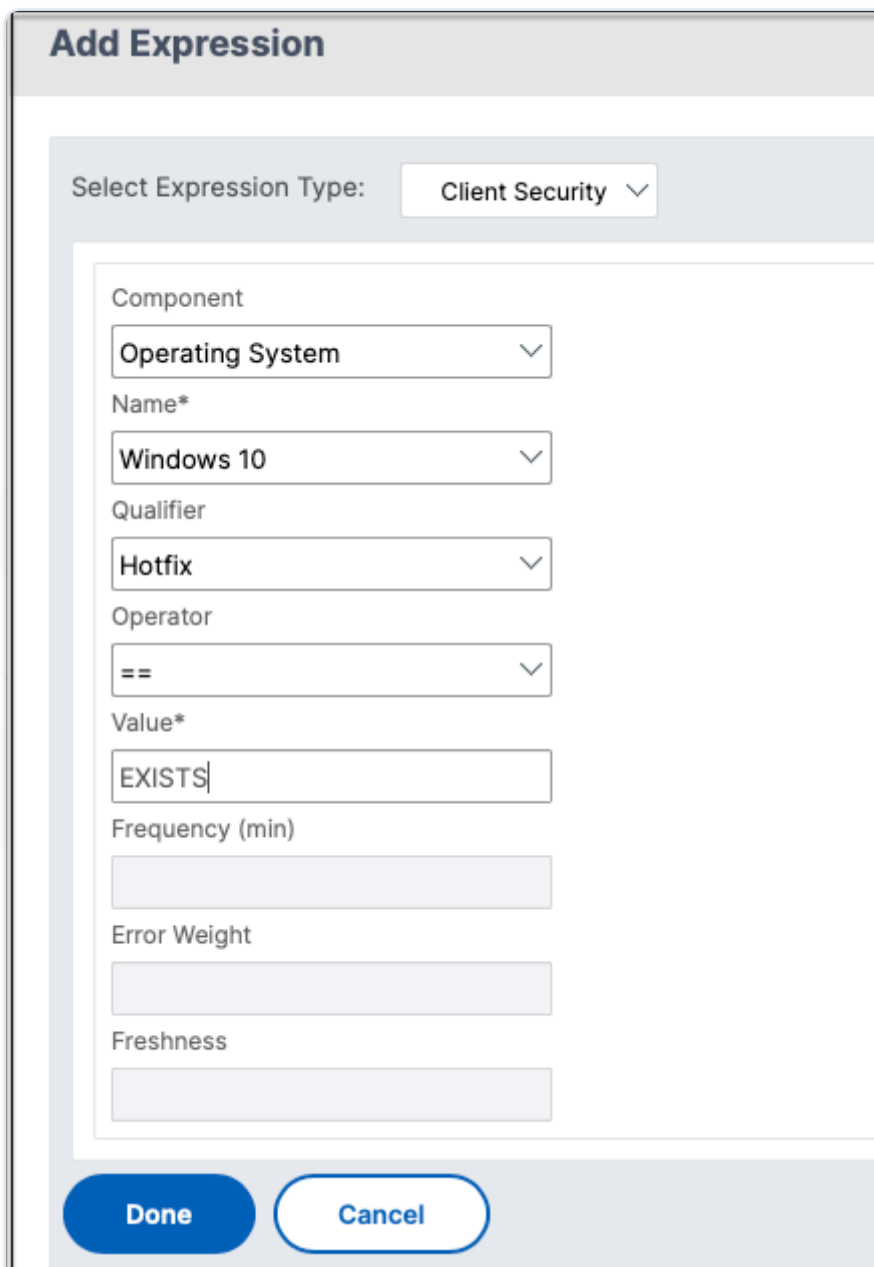
1. 导航到 **NetScaler Gateway > 策略 > 预身份验证**，然后单击**添加**。
2. 选择现有策略或为策略添加名称。此策略名称用作自定义标签值。
3. 在**请求操作**中，单击**添加**以创建操作。您可以为多个策略重用此操作，例如，使用一个操作允许访问，另一个操作拒绝访问。

The screenshot shows the Citrix Secure Private Access console with the 'Configuration' tab selected. The main area displays the 'Create Preauthentication Policy' form, which is partially obscured by a modal window titled 'Create Preauthentication Profile'. The 'Create Preauthentication Policy' form includes fields for 'Name*' (containing 'Windows10'), 'Request Action*' (a dropdown menu), and 'Expression*' (three 'Select' dropdown menus). At the bottom of this form are 'Create' and 'Close' buttons. The 'Create Preauthentication Profile' modal window includes fields for 'Name*' (containing 'win10_profile'), 'Action*' (a dropdown menu set to 'ALLOW'), 'Processes to be cancelled' (an empty text box), 'Files to be deleted' (an empty text box), and 'Default EPA Group' (containing 'spaopdev'). It also has 'Create' and 'Close' buttons at the bottom.

4. 填写必填字段中的详细信息，然后单击**创建**。
5. 在**表达式**中，手动输入表达式或使用表达式编辑器为策略构建表达式。

This screenshot shows the 'Create Preauthentication Policy' form in the Citrix Secure Private Access console. The 'Name*' field contains 'Windows10'. The 'Request Action*' field is a dropdown menu. The 'Expression*' field contains the text 'CLIENT.OS(win10).HOTFIX == EXISTS'. At the bottom of the form are 'Create' and 'Close' buttons.

下图显示了为检查 Windows 10 操作系统而构建的示例表达式。

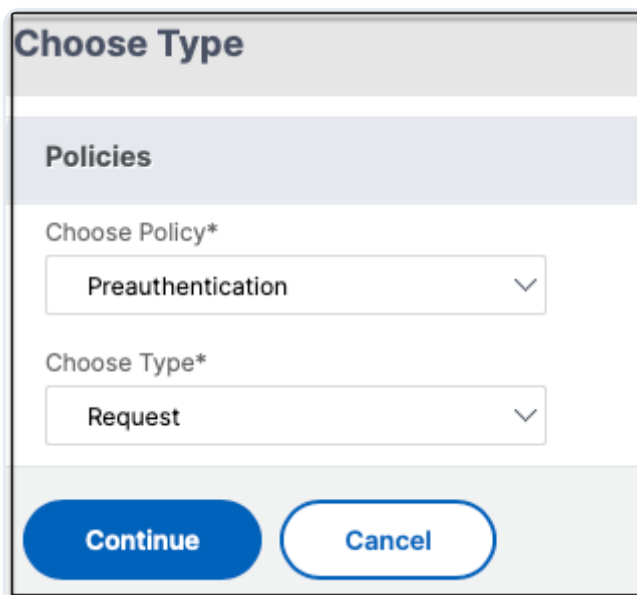


The image shows a dialog box titled "Add Expression". At the top, it says "Select Expression Type:" followed by a dropdown menu set to "Client Security". Below this, there are several fields: "Component" with a dropdown set to "Operating System", "Name*" with a dropdown set to "Windows 10", "Qualifier" with a dropdown set to "Hotfix", "Operator" with a dropdown set to "==", and "Value*" with a text input containing "EXISTS". Below these are three empty text input fields labeled "Frequency (min)", "Error Weight", and "Freshness". At the bottom of the dialog are two buttons: "Done" and "Cancel".

6. 单击“创建”。

将自定义标记绑定到 NetScaler Gateway

1. 导航到“NetScaler Gateway > 虚拟服务器”。
2. 选择要绑定预身份验证策略的虚拟服务器，然后单击“编辑”。
3. 在“策略”部分，单击“+”以绑定策略。
4. 在“选择策略”中，选择预身份验证策略，并在“选择类型”中选择“请求”。



Choose Type

Policies

Choose Policy*

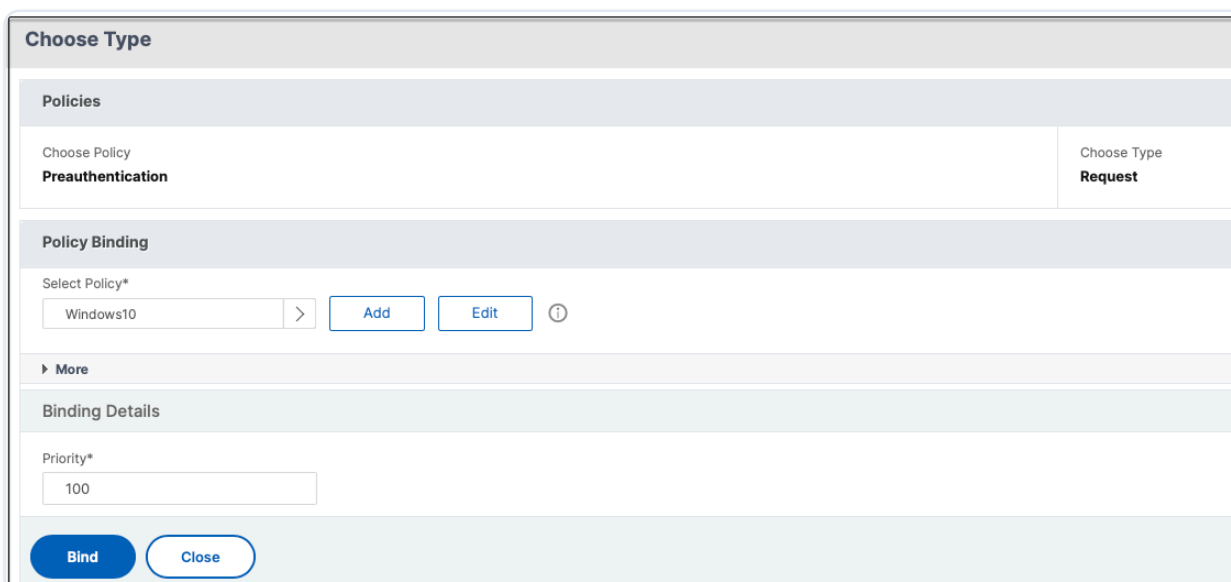
Preauthentication

Choose Type*

Request

Continue **Cancel**

5. 选择策略名称和策略评估的优先级。
6. 单击“绑定”。



Choose Type

Policies

Choose Policy
Preauthentication

Choose Type
Request

Policy Binding

Select Policy*

Windows10 > **Add** **Edit** ⓘ

► **More**

Binding Details

Priority*

100

Bind **Close**

使用 CLI 配置自定义标记

在 NetScaler CLI 上运行以下示例命令以创建和绑定预身份验证策略：

- `add aaa preauthenticationaction win10_prof ALLOW`
- `add aaa preauthenticationpolicy Windows10 "CLIENT.OS(win10) EXISTS"`
`win10_prof`
- `bind vpn vserver _SecureAccess_Gateway -policy Windows10 -priority 100`

在 NetScaler CLI 上运行以下示例命令以配置 nFactor EPA 策略：

- `add authentication epaAction epaallowact -csecexpr "sys.client_expr(\"proc_0_notepad.exe\")" -defaultEPAGroup allow_app -quarantineGroup deny_app`
- `add authentication Policy epaallow -rule true -action epaallowact`

添加新的上下文标签

1. 打开 Secure Private Access 管理控制台，然后单击“访问策略”。
2. 创建新策略或编辑现有策略。
3. 在“条件”部分中，单击“添加条件”，选择“上下文标签”、“匹配所有”，然后输入上下文标签名称（例如，`Windows10`）。

关于发送到 Secure Private Access 提供程序的 EPA 标签的注意事项

在 nFactor EPA 策略中配置的 EPA 操作名称以及关联的组名称作为智能访问标签发送到 Secure Private Access 提供程序。但是，发送的标签取决于 EPA 操作评估的结果。

- 如果 nFactor EPA 策略中的所有 EPA 操作都导致操作 **DENY** 并且在最后一个操作中配置了隔离组，则隔离组名称将作为智能访问发送。
- 如果 nFactor EPA 策略中的 EPA 操作导致操作 **ALLOW**，则与该操作关联的 EPA 策略名称和默认组名称（如果已配置）将作为智能访问标签发送。

智能访问标签(/en-us/citrix-secure-private-access/media/epa-smart-access-tags.png)

在此示例中，当操作被拒绝时，`deny_app` 作为智能访问标签发送到 Secure Private Access 提供程序。当操作被允许时，`epaallowact` 和 `allow_app` 作为智能访问标签发送到 Secure Private Access 提供程序。