Citrix Secure Private Access - 本地

Machine translated content

Disclaimer

Contents

技术概述

August 26, 2024

Citrix Secure Private Access 本地版是客户管理的零信任网络接入 (ZTNA) 解决方案，提供对内部 Web/SaaS 和 TCP/UDP 应用程序的安全访问以及无缝的最终用户体验：

- VPN 减少 SaaS 和内部 Web 应用程序的访问权限
- 最小特权原则
- 单点登录 (SSO)
- 多重身份验证
- 设备状态评估
- 应用程序级安全控制
- App Protection 功能

该解决方案使用 StoreFront 本地部署和 Citrix Workspace 应用程序来提供无缝安全的访问体验，以便在 Citrix Enterprise Browser 中访问内部 Web/SaaS 和 TCP/UDP 应用程序。该解决方案还使用 NetScaler Gateway 来强制执行身份验证和授权控制。

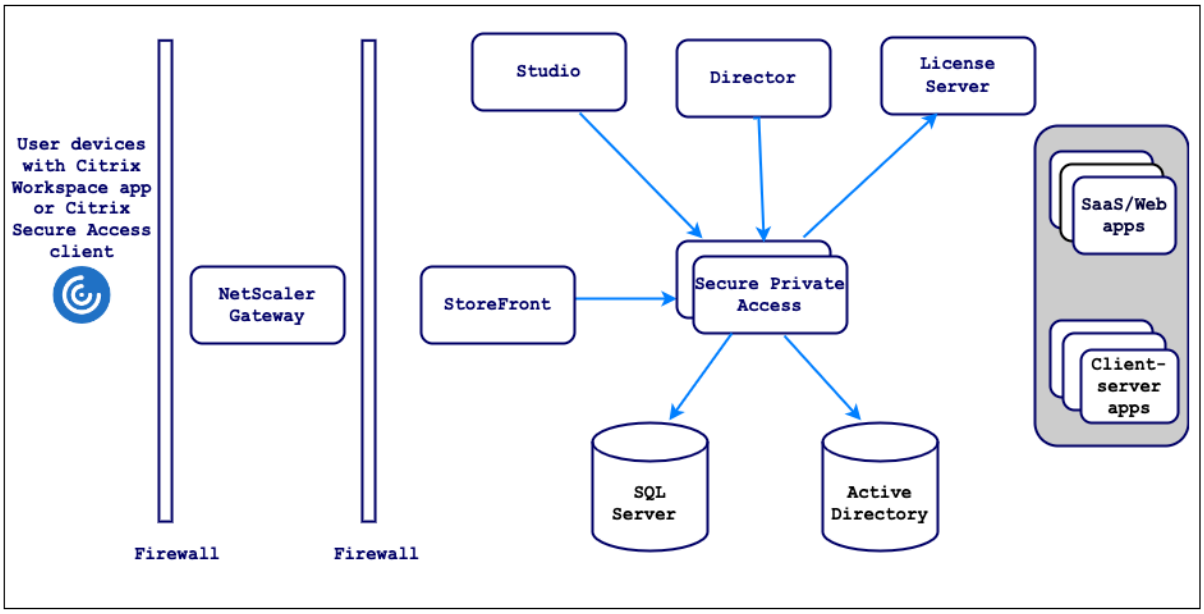
Citrix Secure Private Access 本地解决方案能够使用 StoreFront 本地门户作为内部 Web/SaaS、TCP/UDP 应用程序以及作为 Citrix Workspace 集成部分的虚拟应用程序和桌面的统一访问门户，轻松提供对基于浏览器的应用程序（内部 Web/SaaS 应用程序）和客户端服务器应用程序（TCP/UDP 应用程序）的零信任访问，从而增强了组织的整体安全与合规状况。

Citrix Secure Private Access 结合了 NetScaler Gateway 和 StoreFront 的元素，为最终用户和管理员提供集成体验。

功能	提供功能的服务/组件
一致的用户界面访问应用程序	StoreFront 本地/Citrix Workspace 应用程序
SSO 到 SaaS 和 Web 应用程序	NetScaler Gateway
多重身份验证 (MFA) 和设备状况（又名端点分析）	NetScaler Gateway
Web 和 SaaS 应用程序的安全控制和应用程序保护控制	Citrix Enterprise Browser
授权策略	Secure Private Access
强制访问	NetScaler Gateway 和 Citrix Secure Access 客户端
配置和管理	Secure Private Access
可见性、监视和故障排除	Secure Private Access、NetScaler 控制台（前身为 ADM）和 Citrix Director

组件

此插图显示了典型的 Secure Private Access 部署的组件。



有关每个组件的信息，请参阅关键组件。

新增功能

October 21, 2024

2024 年 **8** 月

应用程序发现

应用程序发现功能可帮助管理员了解其组织中的内部私有应用程序，例如 Web 应用程序和客户端服务器应用程序（基于 TCP 和 UDP 的应用程序）以及访问这些应用程序的用户。管理员可以通过指定域（通配符域）或 IP 子网的范围来发现应用程序。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

策略建模工具（访问策略 **>** 策略建模）可帮助管理员从 Admin Console 中分析和解决配置问题。有关详细信息，请参阅 策略建模工具.

为 **TCP/UDP** 服务器到客户端的连接添加了新的应用程序类型

Secure Private Access 现在支持新的应用程序类型 **TCP/UDP -** 服务器到客户端 这可用于以下使用案例。

- 内网 **IP** 地址支持： - 内网 IP 地址可用于将用户映射到 IP 地址，以进行安全审计、网络分段和合规性。有关 Intranet IP 地址的更多信息，请参阅 配置地址池.
- 服务器到客户端的连接： - 服务器到客户端的连接可用于管理和维护网络环境，例如：
  - 使用组策略进行基于域的策略推送。
  - 使用 Microsoft Endpoint Configuration Manager 或类似解决方案进行软件分发。
  - 远程协助，用于对用户工作站进行故障排除和调试。
- 客户端到客户端连接： - 客户端到客户端连接，使两台远程计算机能够直接相互通信，以在私有或共享或公共网络上共享和接收数据，而不会影响安全性和灵活性。

有关配置 TCP/UDP - 服务器到客户端应用程序的详细信息，请参阅 配置 TCP/UDP 服务器-客户端应用程序.

已修复的问题

October 21, 2024

版本 2408 中解决了以下问题。

域控制器配置

Secure Private Access 不支持用于 Intranet （StoreFront）登录和 Internet/Extranet（网关）应用程序枚举的备用 UPN 后缀。

管理员管理

管理员的 RBAC 角色更改仅在当前会话失效（通过注销或令牌过期）后反映出来。

应用程序启动

如果满足以下所有条件，则应用程序启动将失败：

- 使用 Netscaler 版本 13.0.x、13.1-48.47 之前的 13.1、14.1-4.42 之前的 14.1。
- LDAP UPN 配置了与实际域不同的后缀。

管理控制台

- 这 编辑应用程序 页面在 编辑应用程序 页面（**Secure Private Access>** 应用 **>** 编辑应用程序）在修改相关域条目后不会关闭。

  例如，如果您在创建应用程序时输入的相关域为 `www.example.com`. 应用程序发布后，您可以替换相关域 `www.example.com` 跟 `abc.com`，然后单击 救. 这 编辑应用程序 页面不会关闭，但应用程序已成功更新。

- 添加应用程序时，如果应用程序名称包含逗号，则会显示警告。但是，应用程序已创建。
- 如果应用程序 URL 包含 万维网，则 URL 将保存在路由域表（设置 **>** 应用领域）不带前缀 万维网.

升级

如果自定义 SSL 证书用于 Secure Private Access 管理服务，则必须再次将证书绑定到 Internet Information Service （IIS）上的“Citrix Access Security Admin”站点。

已知问题

October 21, 2024

版本 2408 中存在以下问题。

> 注意：
>
> 某些问题会分配一个追踪编码，仅供内部参考，不会对买家产生任何影响。

域控制器配置

- 不支持跨不同 AD 林的域之间信任类型为“林”的单向或双向信任。

  例如，如果 a.com 和 b.com 域位于两个不同的 AD 林中，并且 SPA 安装在该域加入 a.com/b.com 的计算机上，则其他域用户无法访问 SPA 发布的应用程序。

  [SPAOP-2031]

- 如果安装了适用于本地的 Secure Private Access 的计算机域与登录到 Secure Private Access 的管理员的域不同，则必须执行以下操作：

  在 Secure Private Access 管理和运行时服务的 IIS 应用程序池中添加不同的域服务帐户作为身份。

  [SPAOP-1558]

- Secure Private Access 不支持通讯组。因此，策略无法搜索通讯组以添加用户和组条件。

- Secure Private Access 不会在 Admin Console 或服务中捕获域详细信息。因此，它完全依赖于用户提供的域。因此，如果相应的域无法访问，或者域名不是有效名称，则不支持该域。

NetScaler Gateway

- 在以下情况下，不支持具有 SSL 配置文件配置的 SSL 虚拟服务器：
  - 客户使用的是 NetScaler Gateway 13.1–48.47 及更高版本或 14.1–4.42 及更高版本。
  - 这 `ns_vpn_enable_spa_onprem` toggle 已启用。

  解决方法：

  将 SSL 配置文件中配置的 SSL 参数直接绑定到 SSL 虚拟服务器，或禁用 `ns_vpn_enable_spa_onprem` 切换。

  有关切换的详细信息，请参阅 支持智能访问标签.

RfWeb / Web 工作区

- 不支持 RfWeb/Workspace for Web，因此不会枚举应用程序。有关详细信息，请参阅 使用 StoreFront 版本 2311 或更高版本时.

  [SPAOP-2487]

应用程序启动

- 如果 `ns_vpn_enable_spa_onprem` 和 `toggle_vpn_enable_securebrowse_client_mode` 旋钮未启用，或者如果您的 NetScaler Gateway 不支持这些旋钮，则应用程序启动将在 `CustomHeaderCryptoKey` 旋转。这 `CustomHeaderCryptoKey` 轮换会在 30 天后自动进行。

  [SPAOP-4528]

- 如果 LDAP UPN 和 sAMAccountName 不同，则应用程序启动将失败。

  [SPAOP-1412]

StoreFront

- 在 商店 **>** 配置统一体验，Web 站点的默认接收器必须配置为 /Citrix/<`StoreName`>蹼。在早期版本的 StoreFront 中，网站的默认接收器设置为空白值，这不适用于 Secure Private Access。此外，客户端上还会显示早期版本的 Receiver UI。有关 StoreFront 配置的信息，请参阅 店面.
- 如果您使用的是 StoreFront 版本 2308 或更早版本，则 商店 **>** 管理 **Delivery Controller** 页面显示 Secure Private Access 插件类型为 **XenMobile**. 这不会影响功能。

日志记录

- 不支持为集群生成支持捆绑包。
- 不得删除 admin 和 runtime 服务的 logs 文件夹。如果删除了这些文件夹，Secure Private Access 将无法重新创建。

TCP/UDP 监控

- 这 **SPAOP-3315-EnableZTNAA** 应用程序 功能标志在 2408 中默认处于禁用状态。因此，不会存储 TCP/UDP 监控数据，因此 Director 集成失败。

  解决办法：如果您使用的是 TCP/UDP 应用程序并希望启用 Director 集成，请手动更新数据库以启用此功能标志。

  [SPAOP-5587]

升级

- 数据库升级后，UI 中的 module/section 选项卡在一段时间内（大约一小时）未显示。

  解决办法：如果您希望在数据库升级后立即显示 UI 中的选项卡，请手动重新启动 IIS 服务。

  [SPAOP-5331]

- 尝试通过替换 MSI 将版本 2402 或 2407 升级到 2408 时，Citrix Virtual Apps and Desktops 安装程序中的 Secure Private Access 磁贴显示 可升级. 但是，单击 Secure Private Access 磁贴继续升级会导致 Secure Private Access 被卸载，而不是升级。这 核心组件 页面显示消息”**Secure Private Access** 将被删除.

  [SPAOP-5495]

- 从版本 2405 或 2407 升级到 2408 时，如果未在版本 2405 或 2407 中配置 Secure Private Access，则无法设置 Secure Private Access。数据库创建过程无法继续，因为 下一个 按钮 数据库配置 页面灰显。

  [SPAOP-5595]

- 升级到 2408 并编辑 URL 以 万维网，则 应用程序连接 字段不会填充以前的状态。您必须再次选择应用程序连接类型。这是升级后的一次性操作，之后将保存配置并继续保留。

  [SPAOP-4216]

- 升级到 2408 后，虽然您可以登录到 Admin Console，但无法管理应用程序和策略。但此时会显示错误消息。

  解决办法：您必须使用脚本升级数据库。有关详细信息，请参阅 使用脚本升级数据库.

  [SPAOP-5255]

- 升级到 2408 后，应用程序枚举和应用程序启动失败。

  解决办法：您必须使用脚本升级数据库。有关详细信息，请参阅 使用脚本升级数据库.

[SPAOP-5255]

- 如果 Secure Private Access 插件是使用 Delivery Controller 安装的，则无法将该插件从早期版本升级到 2408。

  [SPAOP-4505]

用户界面

- 这 应用程序启动计数 counter 在 **Secure Private Access >** 概述 页面不会递增 TCP/UDP 应用程序。

  [SPAOP-4201]

系统要求

October 21, 2024

确保您的产品满足最低版本要求。

产品	最低版本
Citrix Workspace 应用程序	Windows –2403 及更高版本 macOS –2402 及更高版本
StoreFront	LTSR 2203 或 CR 2212 及更高版本
NetScaler	13.1、14.1 及更高版本。建议使用最新版本的 NetScaler Gateway 版本 13.1 或 14.1 以优化性能。 对于 TCP/UDP 应用程序 - 14.1–25.56 及更高版本
Citrix Secure Access 客户端	Windows 客户端 - 24.6.1.17 及更高版本 macOS 客户端 - 24.06.2 及更高版本
Director	2402 或更高版本
Secure Private Access 插件服务器的操作系统	Windows Server 2019 及更高版本

通讯端口：确保您已打开 Secure Private Access 插件所需的端口。有关详细信息，请参阅 通讯端口.

数据库：以下是站点配置、配置日志记录和监控数据库支持的 Microsoft SQL Server 版本列表：

```
- SQL Server 2022 Express Edition、Standard Edition 和 Enterprise Edition。
- SQL Server 2019 Express Edition、Standard Edition 和 Enterprise Edition。
```



```
- SQL Server 2017 Express Edition、Standard Edition 和 Enterprise Edition。

对于新安装：默认情况下，如果未检测到支持的现有 SQL Server 安装，安装 Controller 时将安装带累积更新 16 的 SQL Server Express 2017。

对于升级，任何现有 SQL Server Express 版本都不会升级。

支持下列数据库高可用性解决方案（SQL Server Express 除外，此版本仅支持独立模式）：

- SQL Server Always On 故障转移群集实例
- SQL Server AlwaysOn 可用性组（包括 Basic 可用性组）
- SQL Server 数据库镜像

Controller 与 SQL Server 站点数据库之间的连接需要 Windows 身份验证。

有关数据库的更多信息，请参阅 [数据库](/zh-cn/citrix-virtual-apps-desktops/technical-overview/databases). > **注意：** > > - 适用于 iOS 和 Android 的 Citrix Workspace 应用程序不支持适用于本地的 Secure Private Access。 > - 适用于 Linux、iOS 和 Android 的 Citrix Secure Access 客户端不支持 Secure Private Access 本地 TCP/UDP 应用程序。
```

必备条件

要创建或更新现有 NetScaler Gateway，请确保您具有以下详细信息：

- 一台运行 IIS 的 Windows 服务器计算机，配置了 SSL/TLS 证书，Secure Private Access 插件将安装在该证书上。
- StoreFront 存储要在设置过程中输入的 URL。
- 必须已配置 StoreFront 上的 Store，并且 Store 服务 URL 必须可用。应用商店服务 URL 的格式为 `https://store.domain.com/Citrix/StoreSecureAccess`.
- NetScaler Gateway IP 地址、FQDN 和 NetScaler Gateway 回调 URL。
- Secure Private Access 插件主机（如果 Secure Private Access 插件部署为群集，则为负载均衡器）的 IP 地址和 FQDN。
- 在 NetScaler 上配置的身份验证配置文件名称。
- 在 NetScaler 上配置的 SSL 服务器证书。
- 域名.
- 证书配置完成。管理员必须确保证书配置完整。如果在计算机中找不到证书，Secure Private Access 安装程序将配置自签名证书。但是，这可能并不总是有效。

> 注意：
>
> 运行时服务（IIS 默认网站中的 secureAccess 应用程序）需要启用匿名身份验证，因为它不支持 Windows 身份验证。默认情况下，这些设置由 Secure Private Access 安装程序设置，不得手动更改。

管理员帐户要求

设置 Secure Private Access 时需要以下管理员帐户。

- 安装 Secure Private Access：您必须使用本地计算机管理员帐户登录。
- 设置 Secure Private Access：您必须使用域用户登录 Secure Private Access 管理控制台，该用户也是安装了 Secure Private Access 的计算机的本地计算机管理员。
- 管理 Secure Private Access：您必须使用 Secure Private Access 管理员帐户登录 Secure Private Access 管理控制台。

通讯端口

下表列出了 Secure Private Access 插件使用的通信端口。

源	目标	类型	端口	详细信息
管理员工作站	Secure Private Access 插件	HTTPS	4443	Secure Private Access 插件 - Admin Console
Secure Private Access 插件	NTP 服务	TCP、UDP	123	时间同步
	DNS 服务	TCP、UDP	53	DNS 查找
	Active Directory	TCP、UDP	88	Kerberos
	Director	HTTP、HTTPS	80、443	与 Director 沟通以进行绩效管理和增强的故障排除
	许可证服务器	TCP	8083	与许可证服务器通信以收集和处理许可数据
		TCP	389	基于纯文本的 LDAP (LDAP)
		TCP	636	基于 SSL 的 LDAP (LDAPS)
	Microsoft SQL Server	TCP	1433	Secure Private Access 插件 - 数据库通信
	StoreFront	HTTPS	443	身份验证验证
	NetScaler Gateway	HTTPS	443	NetScaler 网关回调

源	目标	类型	端口	详细信息
StoreFront	NTP 服务	TCP、UDP	123	时间同步
	DNS 服务	TCP、UDP	53	DNS 查找
	Active Directory	TCP、UDP	88	Kerberos
		TCP	389	基于纯文本的 LDAP (LDAP)
		TCP	636	基于 SSL 的 LDAP (LDAPS)
		TCP、UDP	464	本机 Windows 身份验证协议，允许用户更改过期的密码
	Secure Private Access 插件	HTTPS	443	身份验证和应用程序枚举
	NetScaler Gateway	HTTPS	443	NetScaler 网关回调
NetScaler Gateway	Secure Private Access 插件	HTTPS	443	应用程序授权验证
	StoreFront	HTTPS	443	身份验证和应用程序枚举
	Web 应用程序	HTTP、HTTPS	80、443	NetScaler Gateway 与配置的 Secure Private Access 应用程序的通信 （端口可能因应用程序要求而异）
用户设备	NetScaler Gateway	HTTPS	443	最终用户设备与 NetScaler Gateway 之间的通信

引用

- 身份验证配置文件.
- 身份验证策略的工作原理.
- 将 SSL 证书绑定到 NetScaler 上的虚拟服务器 (SSL)。

大小调整准则

October 21, 2024

Secure Private Access 本地数据库

Secure Private Access 本地数据库包含有关应用程序、策略和相关插图的信息。它还包含与故障排除和遥测相关的信息。

由于其动态性质，遥测和故障排除记录会经常更改，并且保留时间很短。因此，考虑到频繁更新的需要，必须配置 Secure Private Access 本地数据库。

在内部可扩展性测试期间，Secure Private Access 本地数据库的以下配置能够处理 5000 个用户的负载。

组件	规范
—————	—————
处理器	8 vCPU
内存	16 GB
网络	10 GBP 网络
主机存储	大小：127 GB
^^	IOPS：500
^^	最大吞吐量：100
操作系统	Windows Server 2022
SQL Server	SQL 服务器 2022 CU12
每天 5000 个用户使用的数据库空间	5 GB

> 注意：
>
> - 这些指标是根据以下假设得出的：日志事件清理已禁用，日志保留期设置为 7 天。
> - 默认情况下，日志将保留 90 天，或者最多保留 100 K 个日志事件，具体取决于配置的设置。这些设置在 Secure Private Access Runtime 服务 appsettings.json 文件中可用，并且可以根据需要进行修改。有关详细信息，请参阅 用于保留事件日志的设置.

决策服务器大小调整

Secure Private Access 本地服务器的可扩展性取决于所使用的数据库。数据库存储遥测和故障排除信息。数据库的规模取决于内存、磁盘速度和用于处理负载的 CPU 数量。

在内部可扩展性测试期间，确认以下 3 个 Secure Private Access 本地节点的配置能够处理 5000 个用户的负载。

组件	规范
处理器	4 vCPU
内存	8 GB
网络	10 英镑
主机存储	高级 SSD LRS 大小：127 GB IOPS：500 最大吞吐量：100
操作系统	Windows Server 2022

安装安全私人访问

October 21, 2024

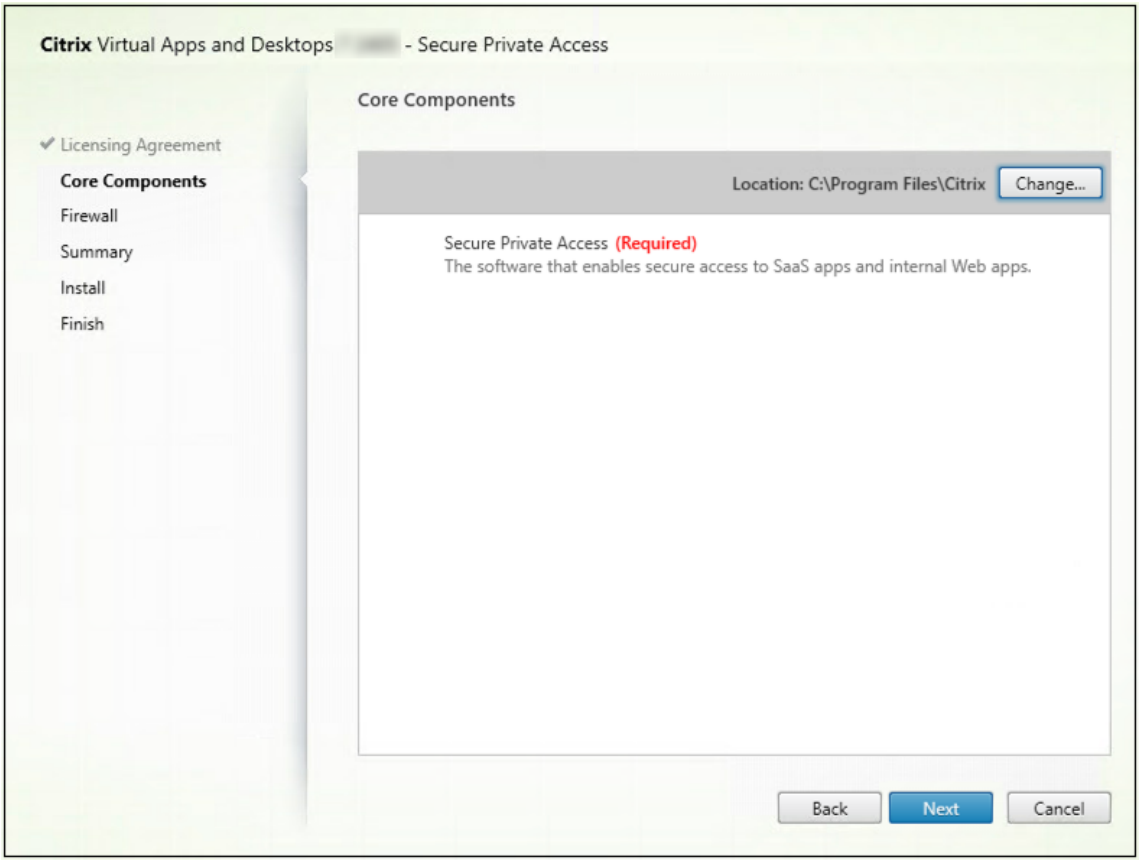
安全的 Private Access 安装程序可作为独立安装程序使用，也可作为集成 Citrix Virtual Apps 和 Desktops 安装程序的一部分使用。

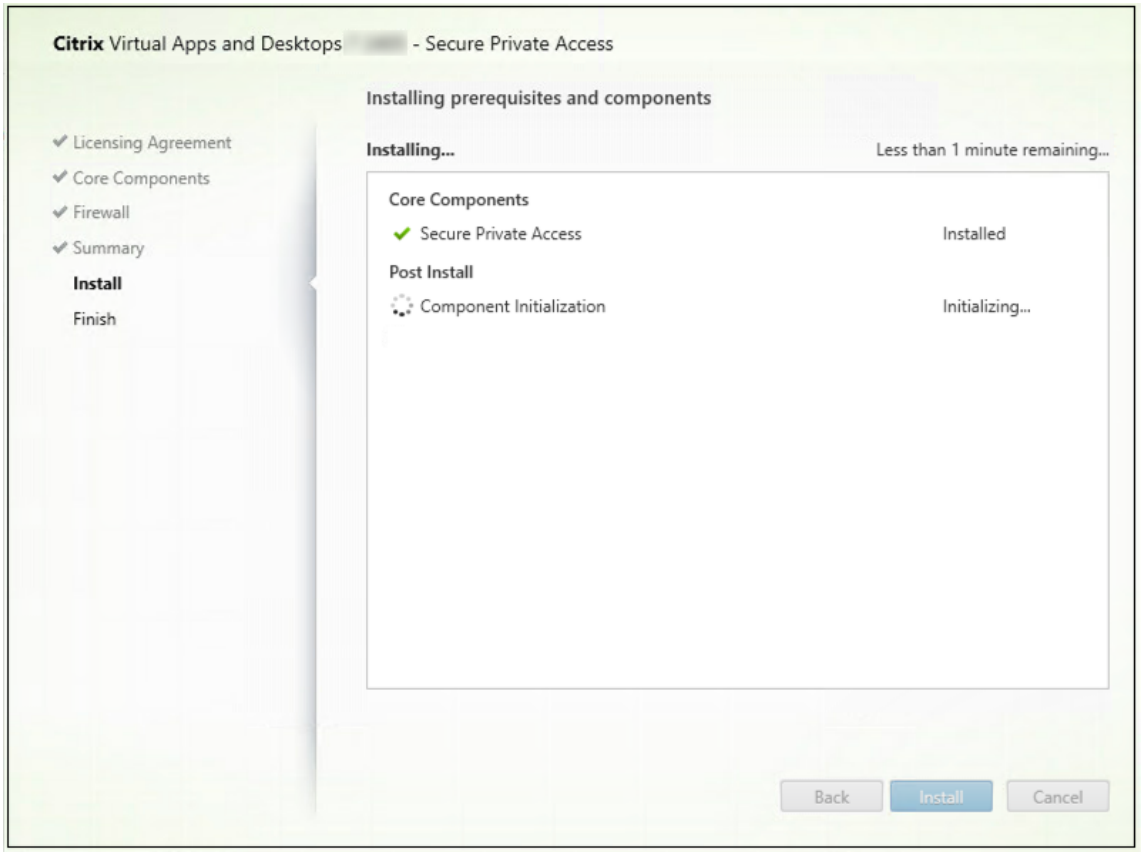
安装和管理 **Secure Private Access** 的管理员账户要求

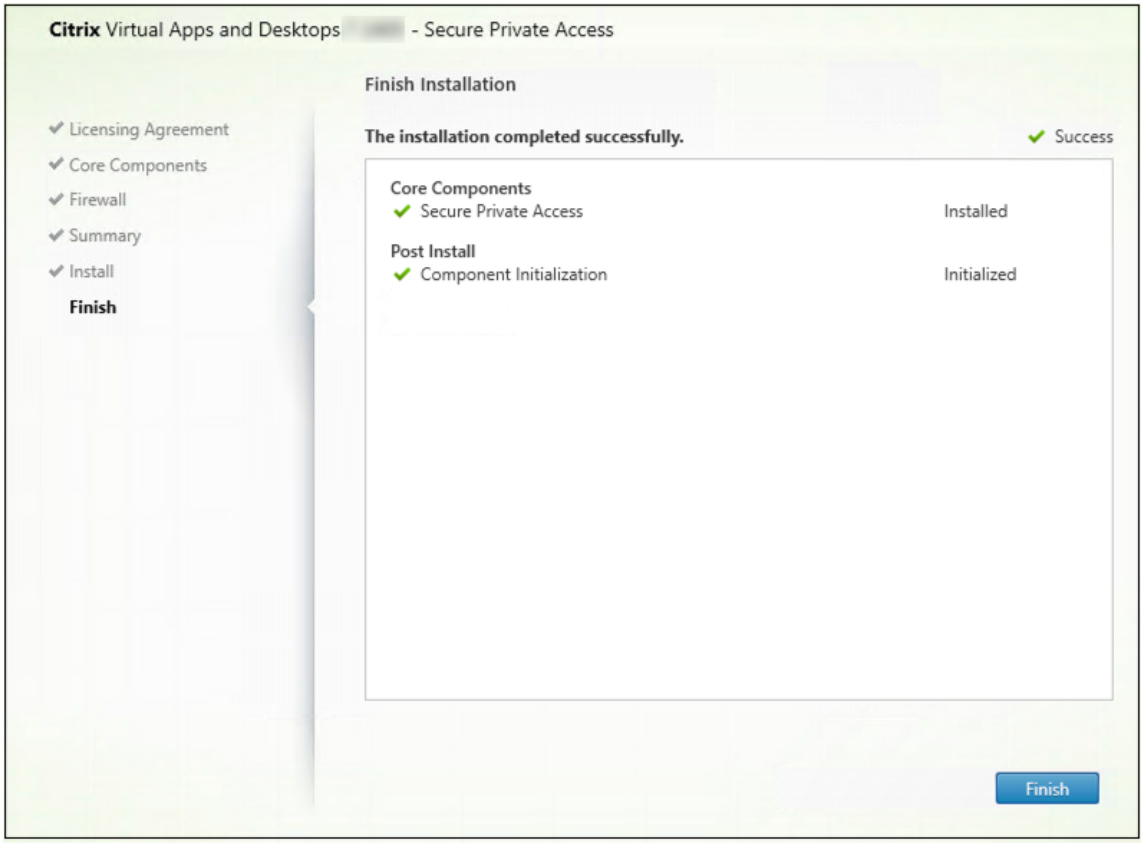
- 要安装安全私人访问，您必须使用本地机器管理员帐户登录。
- 要设置安全私人访问，您必须以域用户的身份登录安全私人访问管理控制台，该域用户也是安装安全私人访问的机器的本地机器管理员。
- 设置完成后，该用户将成为第一个安全私人访问管理员，然后可以添加其他管理员。
- 要在设置后管理 Secure Private Access，您必须使用 Secure Private Access 管理员帐户登录 Secure Private Access 管理控制台。

执行以下步骤来安装 **Secure Private Access**：

1. 从 https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/ 下载 Citrix Virtual Apps and Desktops 产品软件并启动向导。
2. 单击产品旁边的开始以安装：Virtual Apps 或 Virtual Apps and Desktops。
3. 选择 安全私人访问 并按照屏幕上的说明完成安装。

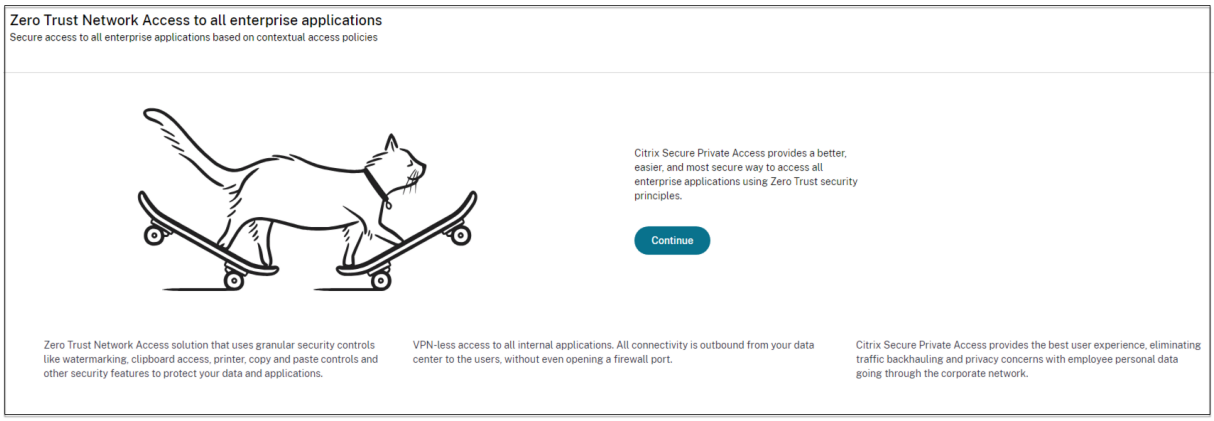




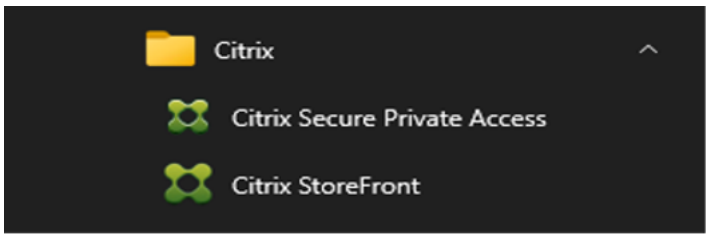


有关详细的分步说明，请参阅 安装核心组件 和 使用命令行安装。

安装完成后，首次设置管理控制台将在默认浏览器窗口中自动打开。您可以点击 继续 来设置安全私人访问。



您还可以在桌面开始菜单 (**Citrix > Citrix Secure Private Access)** 上看到 Secure Private Access 快捷方式。



SSO 到管理控制台

建议您为用于安全私人访问管理控制台的浏览器配置 Kerberos 身份验证。这是因为安全私人访问使用集成 Windows 身份验证 (IWA) 进行管理员身份验证。

如果未设置 Kerberos 身份验证，则在访问安全私人访问管理控制台时，浏览器会提示您输入凭据。

- 如果您输入您的凭据，则将启用集成 Windows 身份验证 (IWA) 登录。
- 如果您不输入您的凭证，您将看到安全私人访问登录页面。

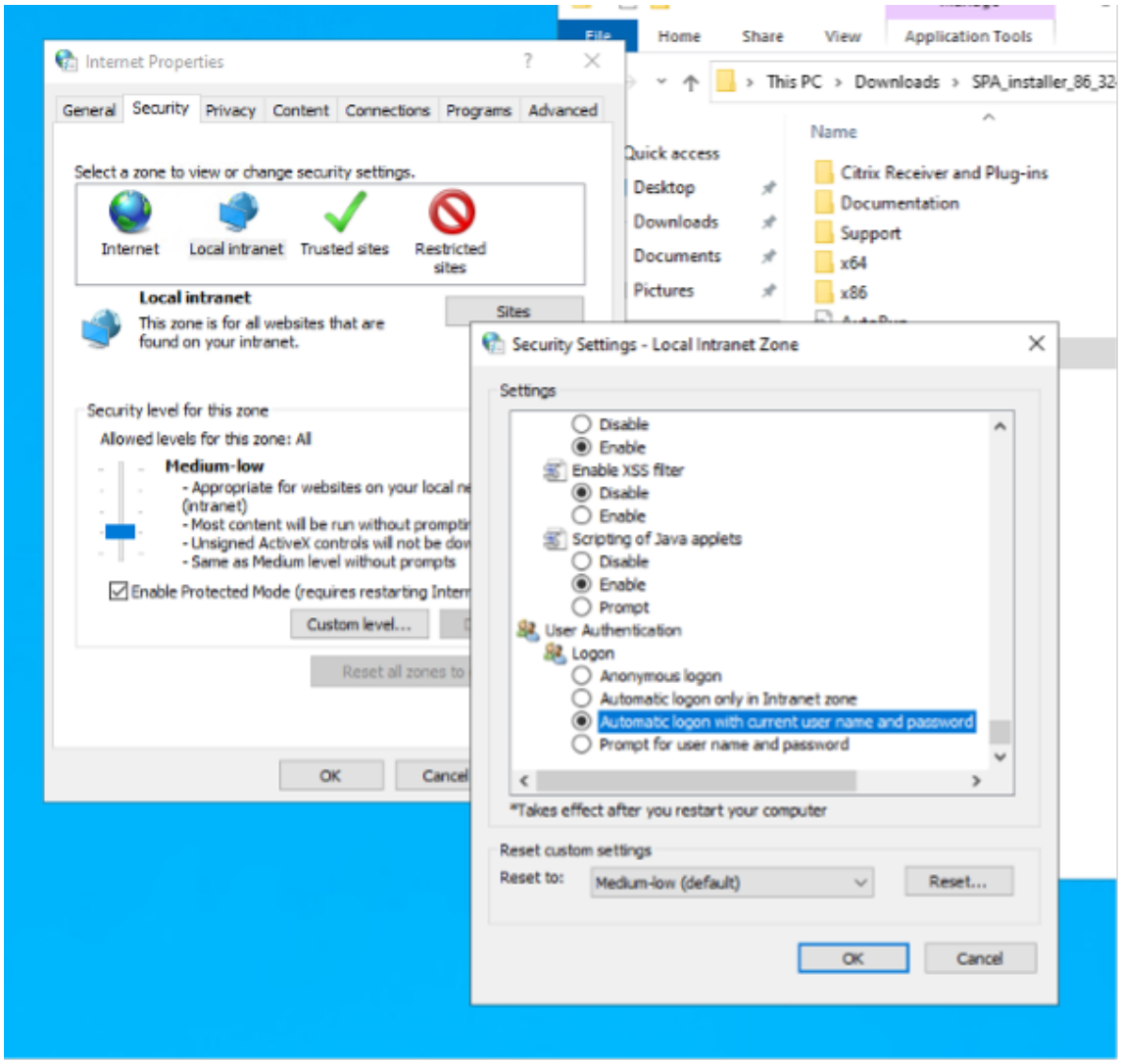
您必须登录管理控制台才能继续安全私人访问设置。如果用户在安装计算机上拥有本地管理员权限，您可以与属于与安装计算机同一域的任何用户设置安全私人访问。

对于 Google Chrome 和 Microsoft Edge 浏览器，请执行以下步骤以启用 Kerberos。

1. 打开 **Internet** 选项。
2. 选择 安全 选项卡，然后单击 本地内联网区域。
3. 单击 站点 并添加安全私人访问 URL。

   如果计划在多台机器上安装安全私人访问，您也可以使用通配符。例如，`"https://*.fabrikam.local"`。

4. 点击 自定义级别。
5. 在 用户身份验证 **>** 登录中，选择 使用当前用户名和密码自动登录。



> 注意：

- 如果使用 Chrome 隐身会话，请创建 DWORD 注册表项 Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Goo
  并将其设置为值 1。
- 您必须重新启动所有 Chrome 窗口（包括非隐身窗口），然后才能为隐身模式启用 Kerberos。
- 对于其他浏览器，请查看特定浏览器有关 Kerberos 身份验证的文档。

后续步骤

- 设置安全私人访问
- 配置 NetScaler Gateway
- 配置应用程序

- 为应用程序配置访问策略

组件

October 21, 2024

以下是用于本地部署的典型 Secure Private Access 中的关键组件。

- 店面： - StoreFront 对用户进行身份验证并管理用户访问的桌面和应用程序的存储。它可以托管企业应用商店，使用户可以自助访问您为其提供的桌面和应用程序。它还跟踪用户的应用程序订阅、快捷方式名称和其他数据。这有助于确保用户在多个设备之间具有一致的体验。有关 StoreFront 与 Secure Private Access 集成的详细信息，请参阅 店面.
- **NetScaler** 网关： - NetScaler Gateway 通过企业防火墙提供单一安全访问点。有关 NetScaler Gateway 与 Secure Private Access 集成的详细信息，请参阅 NetScaler 网关.
- 导演：（可选）Director 使您能够进行有效的性能监控和故障排除。要将 Director 与 Secure Private Access 集成，必须输入必须向 Secure Private Access 注册的 Director 服务器的 FQDN 的 IP 地址。有关 Director 与 Secure Private Access 集成的详细信息，请参阅 Secure Private Access 与 Director 的集成.
- 许可证服务器：许可证服务器收集和处理许可数据。有关许可证服务器与 Secure Private Access 集成的详细信息，请参阅 许可证服务器与 Secure Private Access 集成.
- **Web Studio**： Citrix Secure Private Access 已集成到 Web Studio 控制台中，使用户能够通过 Web Studio 无缝访问该服务。有关 Secure Private Access 与 Studio 集成的详细信息，请参阅 Secure Private Access 与 Web Studio 的集成.

有关这些产品的最低版本要求的信息，请参阅 系统要求.

> 注意：
>
> 从版本 2402 开始，Director 和许可证服务器与 Secure Private Access 集成。

StoreFront

June 19, 2024

如果 Secure Private Access 与 StoreFront 共同托管，则 StoreFront 上的 Secure Private Access 配置将由首次安装向导自动完成。

但是，如果 Secure Private Access 不是与 StoreFront 共同托管的，则某些配置更改必须手动完成。

执行以下步骤，手动配置 StoreFront。

1. 从 Secure Private Access 管理员控制台（设置 **>** 集成）下载脚本。

2. 单击与必须进行配置更改的 StoreFront 条目对应的下载脚本。

   下载的 zip 文件包含配置脚本、自述文件和配置清理脚本。如果要移除 StoreFront 和 Secure Private Access 之间的集成，则可以使用清理脚本。

3. 使用 `./ConfigureStorefront.ps1.` 命令在 PowerShell 64 位实例上以管理员身份运行脚本

   - 不需要其他参数。
   - 必须将 PowerShell 脚本执行策略设置为“不受限制”或“绕过”才能运行 StoreFront 脚本。
   - 如果将 StoreFront 配置为群集，该脚本还会将配置传播到其他 StoreFront 服务器。

使用 Secure Private Access 设置配置 StoreFront 后，即可在 StoreFront 管理界面（“管理 **Delivery Controller**”屏幕）中看到 Secure Private Access 插件配置。

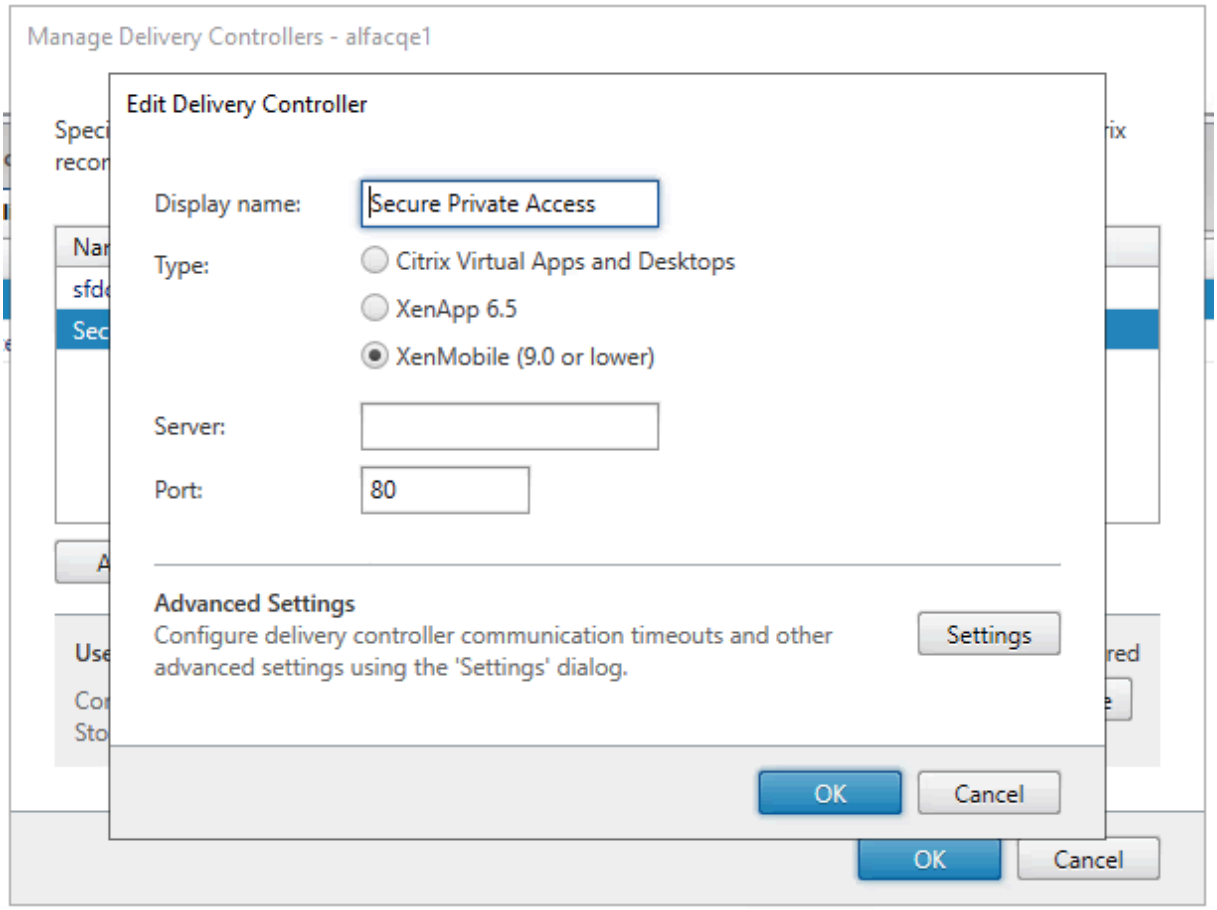
如果为 Citrix Virtual Apps and Desktops Delivery Controller 配置了 Secure Private Access 的聚合组设置，则 StoreFront 脚本会自动配置聚合组设置。默认情况下，该脚本为所有人配置 Secure Private Access（用户映射和多站点聚合配置 **>** 已配置）。

> 重要：
>
> - 建议使用从 Secure Private Access 管理界面下载的 StoreFront 脚本将 StoreFront 配置为仅限 Secure Private Access。请勿从 StoreFront 管理界面配置 Secure Private Access，因为该用户界面不包括 StoreFront 上所有必需的配置。必须运行该脚本才能完成所有必要的配置。
> - 一个 Secure Private Access 站点也可以在多个 StoreFront 部署（在同一 StoreFront 的另一个应用商店或不同的 StoreFront 部署上）上配置。
>   可以从设置 **>** 集成页面添加 StoreFront。
> - 即使 Secure Private Access 与 StoreFront 共同托管，StoreFront 自动配置也无法通过设置 **>** 集成页面运行。自动配置仅在首次设置期间完成。如果从“设置”页面添加了新的商店配置，则必须下载 StoreFront 脚本并在相应的 StoreFront 计算机上运行。

使用 **StoreFront** 版本 **2308** 或更早版本时

如果您使用的是 StoreFront 版本 2308 或更早版本，则 StoreFront 管理界面存在以下已知问题：

- Secure Private Access 插件类型显示为 XenMobile。
- 不显示 Secure Private Access 服务器 URL。
- Secure Private Access 端口始终显示为 80。



使用 **StoreFront** 版本 **2.3.11** 或更高版本时

在 StoreFront 版本 2311 及更高版本中，适用于 Web 的 Citrix Workspace 客户端不枚举 Secure Private Access 应用程序。这是因为 Secure Private Access 不支持在 Workspace for Web 平台中启动 Secure Private Access 应用程序。

NetScaler Gateway

October 21, 2024

Web/SaaS 和 TCP/UDP 应用程序都支持 NetScaler Gateway 配置。您可以为 Secure Private Access 创建 NetScaler Gateway 或更新现有 NetScaler Gateway 配置。建议您在应用这些更改之前创建 NetScaler 快照或保存 NetScaler 配置。

有关 Web/SaaS 和 TCP/UDP 应用程序的 NetScaler Gateway 配置的详细信息，请参阅以下主题：

- Web/SaaS 应用程序的 NetScaler Gateway 配置

- TCP/UDP 应用程序的 NetScaler Gateway 配置

与 **ICA** 应用程序的兼容性

为支持 Secure Private Access 插件而创建或更新的 NetScaler Gateway 也可用于枚举和启动 ICA 应用程序。在这种情况下，您必须配置 Secure Ticket Authority （STA）并将其绑定到 NetScaler Gateway。

> 注意：
>
> STA 服务器通常是 Citrix Virtual Apps and Desktops 部署的一部分。

有关详细信息，请参阅以下主题：

- 在 NetScaler Gateway 上配置 Secure Ticket Authority
- 常见问题解答：Citrix Secure Gateway/ NetScaler Gateway Secure Ticket Authority

支持智能访问标签

> 注意：
>
> - 仅当您的 NetScaler Gateway 版本低于 14.1-25.56 时，本节中提供的信息才适用。
> - 如果您的 NetScaler Gateway 版本为 14.1—25.56 及更高版本，则可以使用 CLI 或 GUI 在 NetScaler Gateway 上启用 Secure Private Access 插件。有关详细信息，请参阅 在 NetScaler Gateway 上启用 Secure Private Access 插件.

在以下版本中，NetScaler Gateway 会自动发送标记。您不必使用网关回调地址来检索智能访问标签。

- 13.1–48.47 及更高版本
- 14.1–4.42 及更高版本

智能访问标签将作为标头添加到 Secure Private Access 插件请求中。

使用切换开关 `ns_vpn_enable_spa_onprem` 或 `ns_vpn_disable_spa_onprem` 以在这些 NetScaler 版本上启用/禁用此功能。

- 您可以使用命令（FreeBSD shell）进行切换：

  ```
  nsapimgr_wr.sh -ys call=ns_vpn_enable_spa_onprem
  ```

- 通过运行以下命令（FreeBSD shell）为 HTTP callout 配置启用 SecureBrowse 客户端模式。

  ```
  nsapimgr_wr.sh -ys call=toggle_vpn_enable_securebrowse_client_mode
  ```

- 如果访问被拒绝，则启用重定向到“Access restricted”页面。

  ```
  nsapimgr -ys call=toggle_vpn_redirect_to_access_restricted_page_on_deny
  ```


- 使用 CDN 上托管的“Access restricted”页面。

  ```
  nsapimgr -ys call=toggle_vpn_use_cdn_for_access_restricted_page
  ```

- 要禁用，请再次运行相同的命令。
- 要验证切换开关是打开还是关闭，请运行 `nsconmsg` 命令。
- 要在 NetScaler Gateway 上配置智能访问标签，请参阅 配置上下文标记.

在 **NetScaler** 上保留安全私有访问插件设置

要在 NetScaler 上保留 Secure Private Access 插件设置，请执行以下操作：

1. 创建或更新文件 /nsconfig/rc.netscaler。
2. 将以下命令添加到文件中。

   ```
   nsapimgr -ys call=ns_vpn_enable_spa_onprem
   nsapimgr -ys call=toggle_vpn_enable_securebrowse_client_mode
   nsapimgr -ys call=toggle_vpn_redirect_to_access_restricted_page_on_deny

   nsapimgr -ys call=toggle_vpn_use_cdn_for_access_restricted_page
   ```

3. 保存该文件。

重新启动 NetScaler 时，将自动应用 Secure Private Access 插件设置。

在 **NetScaler Gateway** 上启用安全私有访问插件

从 NetScaler Gateway 14.1-25.56 及更高版本开始，您可以使用 NetScaler Gateway CLI 或 GUI 在 NetScaler Gateway 上启用安全私有访问插件。此配置将 `nsapimgr_wr.sh -ys 调用 = ns_vpn_enable_spa_onprem` 旋钮在 2407 之前的版本中使用。

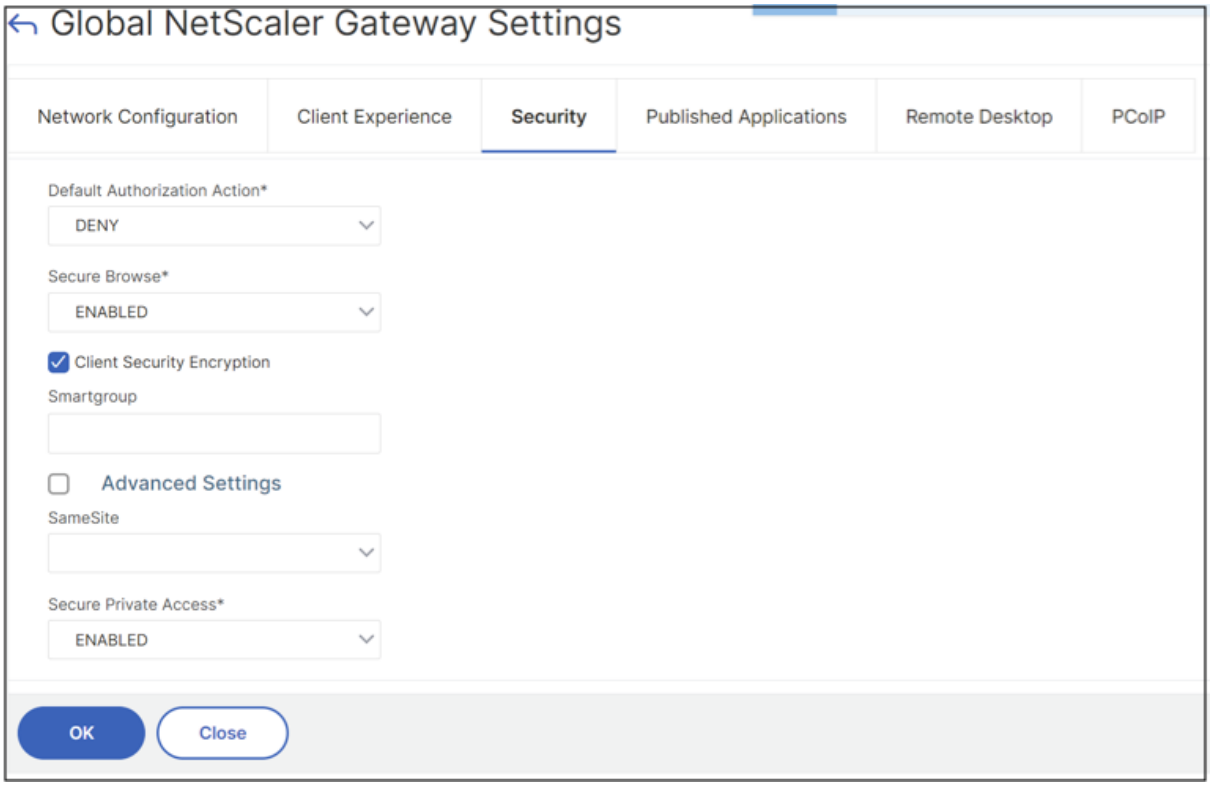
CLI:

在命令提示符下，键入以下命令：

```
set vpn parameter -securePrivateAccess ENABLED
```

GUI:

1. 导航到 **NetScaler** 网关 **>** 全局设置 **>** 更改 **Global NetScaler Gateway** 设置.
2. 单击“安全”选项卡.
3. 在 **Secure Private Access** 选择 启用。



上传公共网关证书

如果无法从 Secure Private Access 计算机访问公有网关，则必须将公有网关证书上传到 Secure Private Access 数据库。

执行以下步骤以上传公有网关证书：

1. 使用 admin 权限打开 PowerShell 或命令提示符窗口。
2. 将目录更改为 Secure Private Access 安装文件夹下的 Admin\AdminConfigTool 文件夹（例如，cd “C:\Program Files\Citrix\Citrix Access Security\Admin\AdminConfigTool”）
3. 运行以下命令：

```
\AdminConfigTool.exe /UPLOAD_PUBLIC_GATEWAY_CERTIFICATE <PublicGatewayUrl> <PublicGatewayCertificatePath>
```

已知限制

- 现有的 NetScaler Gateway 可以使用脚本进行更新，但单个脚本无法涵盖无限数量的可能 NetScaler 配置。
- 请勿在 NetScaler Gateway 上使用 ICA Proxy。配置 NetScaler Gateway 时，此功能将被禁用。
- 如果您使用部署在云中的 NetScaler，则必须在网络中进行更改。例如，允许 NetScaler 与某些端口上的其他组件之间的通信。

- 如果在 NetScaler Gateway 上启用 SSO，请确保 NetScaler 使用私有 IP 地址与 StoreFront 通信。您可能必须使用 StoreFront 私有 IP 地址将 StoreFront DNS 记录添加到 NetScaler。

Web/SaaS 应用程序的 NetScaler Gateway 配置

October 21, 2024

要为 Web/SaaS 应用程序创建 NetScaler Gateway，请执行以下步骤：

1. 下载最新脚本 *`ns_gateway_secure_access.sh`*。从 https://www.citrix.com/downloads/citrix-secure-private-access/Shell-Script/.
2. 将这些脚本上传到 NetScaler 机器。您可以使用 WinSCP 应用程序或 SCP 命令。例如，*`scp ns_gateway_secure_access.sh nsroot@nsalfa.fabrikam.local:/var/tmp`*。

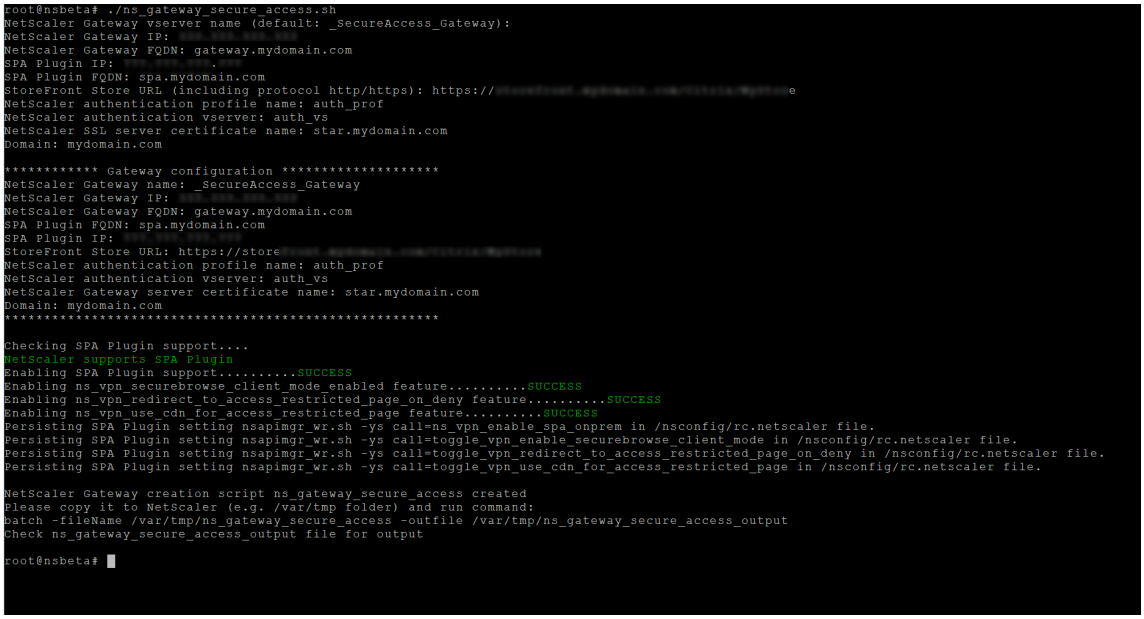
   例如，*`scp ns_gateway_secure_access.sh nsroot@nsalfa.fabrikam.local:/var/tmp`*

> 注意：
>
> - 建议使用 NetScaler /var/tmp 文件夹来存储临时数据。
> - 确保文件以 LF 行尾保存。FreeBSD 不支持 CRLF。
> - 如果您看到错误 `-bash: /var/tmp/ns_gateway_secure_access.sh: /bin/sh ^M: bad interpretationr: No such file or directory`，则表示行尾不正确。您可以使用任何富文本编辑器（例如 Notepad++）转换脚本。

1. SSH 到 NetScaler 并切换到 shell（在 NetScaler CLI 上输入“shell”）。
2. 使上传的脚本可执行。使用 chmod 命令来执行此操作。

   ```
   chmod +x /var/tmp/ns_gateway_secure_access.sh
   ```

3. 在 NetScaler shell 上运行上传的脚本。



4. 如果您打算仅为 Web 和 SaaS 应用程序配置网关，则在 启用 **TCP/UDP** 应用程序类型支持 参数中输入 **N** 。
5. 输入所需参数。有关参数列表，请参阅 先决条件.

   对于身份验证配置文件和 SSL 证书，您必须提供 NetScaler 上现有资源的名称。

   生成一个包含多个 NetScaler 命令的新文件（默认为 var/tmp/ns_gateway_secure_access）。

> 注意：
>
> 在脚本执行期间，会检查 NetScaler 和安全私有访问插件的兼容性。如果 NetScaler 支持安全私有访问插件，则该脚本将启用 NetScaler 功能来支持智能访问标签，在资源访问受到限制时发送改进并重定向到新的拒绝页面。有关智能标签的详细信息，请参阅 支持智能访问标签.
>
> /nsconfig/rc.netscaler 文件中保留的安全私人访问插件功能允许在 NetScaler 重新启动后保持它们启用状态。

```
1 ![NetScaler 配置 2](/en-us/citrix-secure-private-access/media/spaop-
    configure-netscaler2-old.png)
```

1. 切换到 NetScaler CLI 并使用批处理命令从新文件运行生成的 NetScaler 命令。举个例子;

   ```
   batch -fileName /var/tmp/ns_gateway_secure_access -outfile
   /var/tmp/ns_gateway_secure_access_output
   ```

   NetScaler 逐个运行文件中的命令。如果一个命令失败，它会继续执行下一个命令。

   如果资源存在或步骤 6 中输入的某个参数不正确，则命令可能会失败。

2. 确保所有命令均成功完成。

> 注意：
>
> 如果出现错误，NetScaler 仍会运行剩余的命令并部分创建/更新/绑定资源。因此，如果由于某个参数不正确而出现意外错误，建议从开始重新进行配置。

更新 **Web** 和 **SaaS** 应用程序的现有 **NetScaler Gateway** 配置

您可以使用现有 NetScaler Gateway 上的 `ns_gateway_secure_access_update.sh`脚本来更新 Web 和 SaaS 应用程序的配置。但是，如果要手动更新现有配置（NetScaler Gateway 版本 14.1—4.42 及更高版本），请使用 用于更新现有 NetScaler Gateway 配置的示例命令. 此外，您还必须更新 NetScaler Gateway 虚拟服务器和会话操作设置。

> 注意：
>
> 从 NetScaler Gateway 14.1–25.56 及更高版本开始，您可以使用 NetScaler Gateway CLI 或 GUI 在 NetScaler Gateway 上启用安全私有访问插件。有关详细信息，请参阅 在 NetScaler Gateway 上启用 Secure Private Access 插件.

您还可以使用现有 NetScaler Gateway 上的脚本来支持安全私有访问。但是，该脚本不会更新以下内容：

- 现有的 NetScaler Gateway 虚拟服务器
- 绑定到 NetScaler Gateway 的现有会话操作和会话策略

确保在执行之前检查每个命令并创建网关配置的备份。

NetScaler Gateway 虚拟服务器设置

添加或更新现有的 NetScaler Gateway 虚拟服务器时，请确保将以下参数设置为定义的值。有关示例命令，请参阅 用于更新现有 NetScaler Gateway 配置的示例命令.

添加虚拟服务器**:**

- tcp 配置文件名称：nstcp_default_XA_XD_profile
- 部署类型：ICA_STOREFRONT（仅适用于 `add vpn vserver` 命令）
- icaOnly：关闭

更新虚拟服务器：

- tcp 配置文件名称：nstcp_default_XA_XD_profile
- icaOnly：关闭

NetScaler Gateway 会话操作设置

会话操作通过会话策略绑定到网关虚拟服务器。创建或更新会话操作时，请确保将以下参数设置为定义的值。有关示例命令，请参阅 用于更新现有 NetScaler Gateway 配置的示例命令.

- transparentInterception: 关闭
- SSO: 开启
- ssoCredential: 主要
- 使用MIP: NS
- useIIP: 关闭
- icaProxy: 关闭
- wihome: "https://storefront.mydomain.com/Citrix/MyStoreWeb" - 用真实商店 URL 替换。存储路径 /Citrix/MyStoreWeb 是可选的。
- 客户端选择: 关闭
- ntDomain: mydomain.com - 用于 SSO（可选）
- defaultAuthorizationAction: 允许
- authorizationGroup: SecureAccessGroup（确保创建此组，用于绑定安全私人访问特定的授权策略）
- clientlessVpnMode: 开启
- clientlessModeUrlEncoding: 透明
- 安全浏览: 已启用
- Storefronturl: "https://storefront.mydomain.com"
- sfGatewayAuthType: 域

更新现有 **NetScaler Gateway** 配置的示例命令

添加/更新虚拟服务器。

- add vpn vserver SecureAccess_Gateway SSL 999.999.999.999 443 -Listenpolicy NONE -tcpProfileName nstcp_default_XA_XD_profile -deploymentType ICA_STOREFRONT -vserverFqdn gateway.mydomain.com -authnProfile auth_prof_name -icaOnly OFF
- set vpn vserver SecureAccess_Gateway -icaOnly OFF

添加会话操作。

- add vpn sessionAction AC_OSspaonprem -transparentInterception OFF -defaultAuthorizationAction ALLOW -authorizationGroup SecureAccessGroup -SSO ON -ssoCredential PRIMARY -useMIP NS -useIIP OFF -icaProxy OFF -wihome "https://storefront.example.corp/Citrix/SPAWeb"-ClientChoices OFF -ntDomain example.corp -clientlessVpnMode ON -clientlessModeUrlEncoding TRANSPARENT -SecureBrowse ENABLED -storefronturl "https://storefront.example.corp"-sfGatewayAuthType domain
- add vpn sessionAction AC_WBspaonprem -transparentInterception OFF -defaultAuthorizationAction ALLOW -authorizationGroup


```
SecureAccessGroup -SSO ON -ssoCredential PRIMARY -useMIP NS -
useIIP OFF -icaProxy OFF -wihome "https://storefront.example.
corp/Citrix/SPAWeb"-ClientChoices OFF -ntDomain example.corp -
clientlessVpnMode ON -clientlessModeUrlEncoding TRANSPARENT -
SecureBrowse ENABLED -storefronturl "https://storefront.example.
corp"-sfGatewayAuthType domain
```

添加会话策略。

- `add vpn sessionPolicy PL_OSspaonprem "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\")"AC_OSspaonprem`
- `add vpn sessionPolicy PL_WBspaonprem "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\").NOT && HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"plugin\").NOT"AC_WBspaonprem`

将会话策略绑定到 VPN 虚拟服务器。

- `bind vpn vserver SecureAccess_Gateway -policy PL_OSspaonprem -priority 111 -gotoPriorityExpression NEXT -type REQUEST`
- `bind vpn vserver SecureAccess_Gateway -policy PL_WBspaonprem -priority 110 -gotoPriorityExpression NEXT -type REQUEST`

将 Secure Private Access 插件绑定到 VPN 虚拟服务器。

- `bind vpn vserver spaonprem -appController "https://spa.example.corp"`

有关会话操作参数的详细信息，请参阅 vpn-sessionAction。

其他信息

有关 NetScaler Gateway 用于安全私有访问的其他信息，请参阅以下主题：

- 与 ICA 应用程序的兼容性
- 支持智能访问标签
- 在 NetScaler 上保留安全私有访问插件设置
- 在 NetScaler Gateway 上启用安全私有访问插件
- 上传公共网关证书
- 已知限制

TCP/UDP 应用程序的 NetScaler Gateway 配置

October 21, 2024

您可以使用 适用于 Web/SaaS 应用程序的 NetScaler Gateway 配置 配置 TCP/UDP 应用程序。要为 TCP/UDP 应用程序配置网关，必须通过输入 **Y** 对于 启用 **TCP/UDP** 应用程序类型支持 参数。

下图显示了 启用 **TCP/UDP** 应用程序类型支持 参数启用 TCP/UDP 支持。

```
root@ns32201# ./ns_gateway_secure_access_2405.sh
NetScaler Gateway vserver name (default: _SecureAccess_Gateway): spaonprem
NetScaler Gateway IP:
NetScaler Gateway FQDN: ns32205.cgwsanity.net
SPA Plugin IP:
SPA Plugin FQDN:
StoreFront Store URL (including protocol http/https):
NetScaler authentication profile name: authnprof
NetScaler SSL server certificate name: ns32205
Domain: cgwsanity.net
Enable TCP/UDP Apptype support (Y/N): Y

************ Gateway configuration ********************
NetScaler Gateway name: spaonprem
NetScaler Gateway IP:
NetScaler Gateway FQDN: ns32205.cgwsanity.net
SPA Plugin FQDN: spa.cgwsanity.net
SPA Plugin IP:
StoreFront Store URL:
NetScaler authentication profile name: authnprof
NetScaler Gateway server certificate name: ns32205
Domain: cgwsanity.net
Enable App type TCP/UDP:
*****************************************************

Checking SPA Plugin support....
NetScaler supports SPA CLI, skipping nsapimgr commands
Number of PEs running: 3
Changing ns_vpn_enable_spa_tcp_udp_apps from 0 to 3 Done.
Changing ns_vpn_enable_spa_tcp_udp_apps from 0 to 3 Done.
Changing ns_vpn_enable_spa_tcp_udp_apps from 0 to 3 Done.
TCP/UDP Apptype support is enabled
Persisting TCP/UDP Apptype support setting: nsapimgr_wr.sh -ys ns_vpn_enable_spa_tcp_udp_apps=3 in /nsconfig/rc.netscaler file.

NetScaler Gateway creation script ns_gateway_secure_access created
Please copy it to NetScaler (e.g. /var/tmp folder) and run command:
batch -fileName /var/tmp/ns_gateway_secure_access -outfile /var/tmp/ns_gateway_secure_access_output
Check ns_gateway_secure_access_output file for output
```

```
root@ns# cat ns_gateway_secure_access
############################################################################################################################
#1. Upload file to NetScaler (e.g. to /var/tmp)                                                                            #
#2. Run batch command (e.g. batch -fileName /var/tmp/ns_gateway_secure_access -outfile /var/tmp/ns_gateway_secure_access_output) #
#3. Analyze output (e.g. cat /var/tmp/ns_gateway_secure_access_output)                                                     #
############################################################################################################################

# Enable NetScaler features
enable ns feature SSL SSLVPN AAA REWRITE IC

# Add NetScaler Gateway vserver
add vpn vserver _SecureAccess_Gateway SSL 333.333.333.333 443 -Listenpolicy NONE -tcpProfileName nstcp_default_XA_XD_profile -deploymentType ICA_STOREFRONT -vserverFqdn gateway.domain.com -authnProfile
auth_prof -icaOnly OFF

# Add default AAA group for authenticated users
add aaa group SecureAccessGroup

# Add excluded domains
bind policy patset ns_cvpn_default_bypass_domains storefront.domain.com
bind policy patset ns_cvpn_default_bypass_domains spa.domain.com
bind policy patset ns_cvpn_default_bypass_domains citrix.com

# Add session actions
add vpn sessionAction AC_OS_SecureAccess_Gateway -transparentInterception OFF -SSO ON -ssoCredential PRIMARY -useMIP NS -useIIP OFF -icaProxy OFF -wihome "https://storefront.domain.com/Citrix/SPAStoreWe
b" -ClientChoices OFF -ntDomain domain.com -defaultAuthorizationAction ALLOW -authorizationGroup SecureAccessGroup -clientlessVpnMode ON -clientlessModeUrlEncoding TRANSPARENT -SecureBrowse ENABLED -sto
refronturl "https://storefront.domain.com" -sfGatewayAuthType domain
add vpn sessionAction AC_WB_SecureAccess_Gateway -transparentInterception OFF -SSO ON -ssoCredential PRIMARY -useMIP NS -useIIP OFF -icaProxy OFF -wihome "https://storefront.domain.com/Citrix/SPAStoreWe
b" -ClientChoices OFF -ntDomain domain.com -defaultAuthorizationAction ALLOW -authorizationGroup SecureAccessGroup -clientlessVpnMode ON -clientlessModeUrlEncoding TRANSPARENT -SecureBrowse ENABLED -sto
refronturl "https://storefront.domain.com" -sfGatewayAuthType domain

# Add session policies
add vpn sessionPolicy PL_OS_SecureAccess_Gateway "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\")" AC_OS_SecureAccess_Gateway
add vpn sessionPolicy PL_WB_SecureAccess_Gateway "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\").NOT" AC_WB_SecureAccess_Gateway

# Add rewrite policies for Citrix headers
add rewrite action Add_X-Citrix-Via insert_http_header X-Citrix-Via "\"gateway.domain.com\""
add rewrite action Add_X-Citrix-Via-VIP insert_http_header X-Citrix-Via-VIP "\"333.333.333.333\""
add rewrite action Add_X-GW-SessionId insert_http_header X-GW-SessionId AAA.USER.SESSIONID
add rewrite policy Add_X-Citrix-ViaPol "HTTP.REQ.HOSTNAME.CONTAINS(\"spa.domain.com\") && HTTP.REQ.HEADER(\"X-Citrix-Via\").EXISTS.NOT" Add_X-Citrix-Via
add rewrite policy Add_X-Citrix-Via-VIPPol "HTTP.REQ.HOSTNAME.CONTAINS(\"spa.domain.com\") && HTTP.REQ.HEADER(\"X-Citrix-Via-VIP\").EXISTS.NOT" Add_X-Citrix-Via-VIP
add rewrite policy Add_X-GW-SessionIdPol "HTTP.REQ.HOSTNAME.CONTAINS(\"spa.domain.com\")" Add_X-GW-SessionId

# Add SSO traffic policy for SPA Plugin
add vpn trafficAction _SecureAccess_Gateway_Traffic_Action http -SSO ON
```


更新 **TCP/UDP** 应用程序的现有 **NetScaler Gateway** 配置

如果要将配置从早期版本更新到 2407，建议您手动更新配置。有关详细信息，请参阅 用于更新现有 NetScaler Gateway 配置的示例命令. 此外，您还必须更新 NetScaler Gateway 虚拟服务器和会话操作设置。

NetScaler Gateway 虚拟服务器设置

添加或更新现有的 NetScaler Gateway 虚拟服务器时，请确保将以下参数设置为定义的值。有关示例命令，请参阅 用于更新现有 NetScaler Gateway 配置的示例命令. 此外，您还必须更新 NetScaler Gateway 虚拟服务器和会话操作设置。

添加虚拟服务器**:**

- tcp 配置文件名称：nstcp_default_XA_XD_profile
- 部署类型：ICA_STOREFRONT（仅适用于 `add vpn vserver` 命令）
- icaOnly：关闭

更新虚拟服务器：

- tcp 配置文件名称：nstcp_default_XA_XD_profile
- icaOnly：关闭

有关虚拟服务器参数的详细信息，请参阅 vpn-session 操作.

NetScaler Gateway 会话策略设置

会话操作通过会话策略绑定到网关虚拟服务器。创建或更新会话操作时，请确保将以下参数设置为定义的值。有关示例命令，请参阅 用于更新现有 NetScaler Gateway 配置的示例命令. 此外，您还必须更新 NetScaler Gateway 虚拟服务器和会话操作设置。

- `transparentInterception` （透明拦截）：上
- `SSO`: 开启
- `ssoCredential`: 主要
- `使用MIP`: NS
- `useIIP`: 关闭
- `icaProxy`: 关闭
- `客户选择`：上
- `ntDomain`: mydomain.com - 用于 SSO（可选）
- `defaultAuthorizationAction`: 允许
- `authorizationGroup`：安全访问组
- `无客户端VpnMode`：关闭
- `clientlessModeUrlEncoding`: 透明
- `安全浏览`: 已启用

更新现有 **NetScaler Gateway** 配置的示例命令

> 注意：
>
> 如果要手动更新现有配置，则除了以下命令之外，还必须使用命令 `nsapimgr_wr.sh -ys ns_vpn_enable_spa_tcp_udp_apps=3`.

- 添加 VPN 会话操作以支持基于 Citrix Secure Access 的连接。

```
add vpn sessionAction AC_AG_PLGspaonprem -splitDns BOTH -splitTunnel
 ON -transparentInterception ON -defaultAuthorizationAction ALLOW
 -authorizationGroup SecureAccessGroup -SSO ON -ssoCredential
PRIMARY -useMIP NS -useIIP OFF -icaProxy OFF -ClientChoices ON -
ntDomain example.corp -clientlessVpnMode OFF -clientlessModeUrlEncoding
 TRANSPARENT -SecureBrowse ENABLED
```

- 添加 VPN 会话策略以支持基于 Citrix Secure Access 的连接。

```
add vpn sessionPolicy PL_AG_PLUGINspaonprem "HTTP.REQ.HEADER
(\"User-Agent\").CONTAINS(\"CitrixReceiver\").NOT && (HTTP.REQ
.HEADER(\"User-Agent\").CONTAINS(\"plugin\")|| HTTP.REQ.HEADER(\"
User-Agent\").CONTAINS(\"CitrixSecureAccess\"))"AC_AG_PLGspaonprem
```

- 将会话策略绑定到 VPN 虚拟服务器以支持基于 Citrix Secure Access 的连接。

```
bind vpn vserver spaonprem -policy PL_AG_PLUGINspaonprem -priority
 105 -gotoPriorityExpression NEXT -type REQUEST
```

- 添加 HTTP callout 策略以支持对基于 TCP/UDP 的连接的授权验证。

> 注意：
>
> 仅当您的 NetScaler Gateway 版本低于 14.1-29.x 时，才需要执行此步骤。

```
1 `add policy httpCallout SecureAccess_httpCallout_TCP -IPAddress
     192.0.2.24 -port 443  -returnType BOOL -httpMethod POST -hostExpr "
     \"spa.example.corp\"" -urlStemExpr "\"/secureAccess/authorize\"" -
     headers Content-Type("application/json") X-Citrix-SecureAccess-Cache
     ("dstip="+HTTP.REQ.HEADER("CSIP").VALUE(0)+"&sessid="+aaa.user.
     sessionid) -bodyExpr q/"{
2  "+"\"userName\":\""+aaa.USER.NAME.REGEX_REPLACE(re#\\#,"\\\\",ALL)+"
     \","+"\"domain\":\""+aaa.USER.DOMAIN+"\","+"\"customTags\":\""+http
     .REQ.HEADER("X-Citrix-AccessSecurity").VALUE(0)+"\","+"\"
     gatewayAddress\":\"ns224158.example.corp\","+"\"userAgent\":\"
     CitrixSecureAccess\","+"\"applicationDomain\":\""+http.REQ.HEADER("
     CSHOST").VALUE(0)+"\","+"\"smartAccessTags\":\""+aaa.user.attribute
     ("smartaccess_tags")+"\",\"applicationType\":\"ztna\",\"
     applicationDetails\":{
```



```
 \"destinationIp\":\""+HTTP.REQ.HEADER("CSIP").VALUE(0)+"\",\"
    destinationPort\":\""+HTTP.REQ.HEADER("PORT").VALUE(0)+"\",\"
    protocol\":\"TCP\" }
  }
 "/ -scheme https -resultExpr "http.RES.HEADER(\"X-Citrix-SecureAccess-
    Decision\").contains(\"ALLOW\")"`

其中
-  **192.0.2.24** 是 Secure Private Access 插件 IP 地址
-  **spa.example.corp** 是 Secure Private Access 插件的 FQDN
-  **ns224158.example.corp 公司** 是网关 VPN 虚拟服务器的 FQDN
```

- 添加授权策略以支持基于 TCP/UDP 的连接。

  ```
  add authorization policy SECUREACCESS_AUTHORIZATION_TCP "HTTP.REQ
  .URL.EQ(\"/cs\")&& HTTP.REQ.HEADER(\"PRTCL\").EQ(\"TCP\")&& sys.
  HTTP_CALLOUT(SecureAccess_httpCallout_TCP)"ALLOW
  ```

- 将授权策略绑定到身份验证和授权组，以支持基于 TCP/UDP 的应用程序。

  ```
  bind aaa group SecureAccessGroup -policy SECUREACCESS_AUTHORIZATION_TCP
   -priority 1010 -gotoPriorityExpression END
  ```

- 将 Secure Private Access 插件绑定到 VPN 虚拟服务器。

  ```
  bind vpn vserver spaonprem -appController "https://spa.example.
  corp"
  ```

其他信息

有关适用于 Secure Private Access 的 NetScaler Gateway 的其他信息，请参阅以下主题：

- 与 ICA 应用程序的兼容性
- 支持智能访问标签
- 在 NetScaler 上保留安全私有访问插件设置
- 在 NetScaler Gateway 上启用安全私有访问插件
- 上传公共网关证书
- 已知限制

上下文标记

October 21, 2024

Secure Private Access 插件根据用户会话上下文（如设备平台和操作系统、已安装的软件、地理位置）提供对 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中。Secure Private Access 插件上的上下文标记是指应用到经过身份验证的用户的会话的 NetScaler Gateway 策略（会话、预身份验证、EPA）的名称。

Secure Private Access 插件可以作为标头（新逻辑）或通过对网关进行回调来接收智能访问标签。有关详细信息，请参阅 智能访问标签.

> 注意：
>
> - 从 NetScaler Gateway 14.1-25.x 及更高版本开始，支持 nFactor EPA 策略。
> - 如果您的 NetScaler Gateway 版本低于 14.1-25.x，则只能在 NetScaler Gateway 上配置经典网关预身份验证策略。

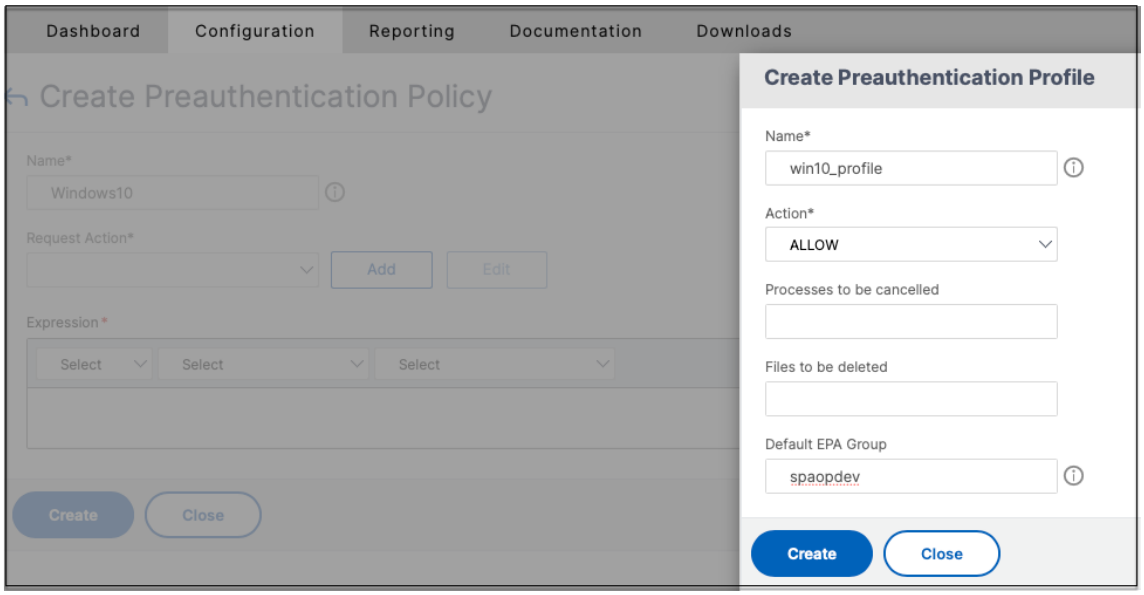
使用 **GUI** 配置自定义标记

配置上下文标记涉及以下高级步骤。

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

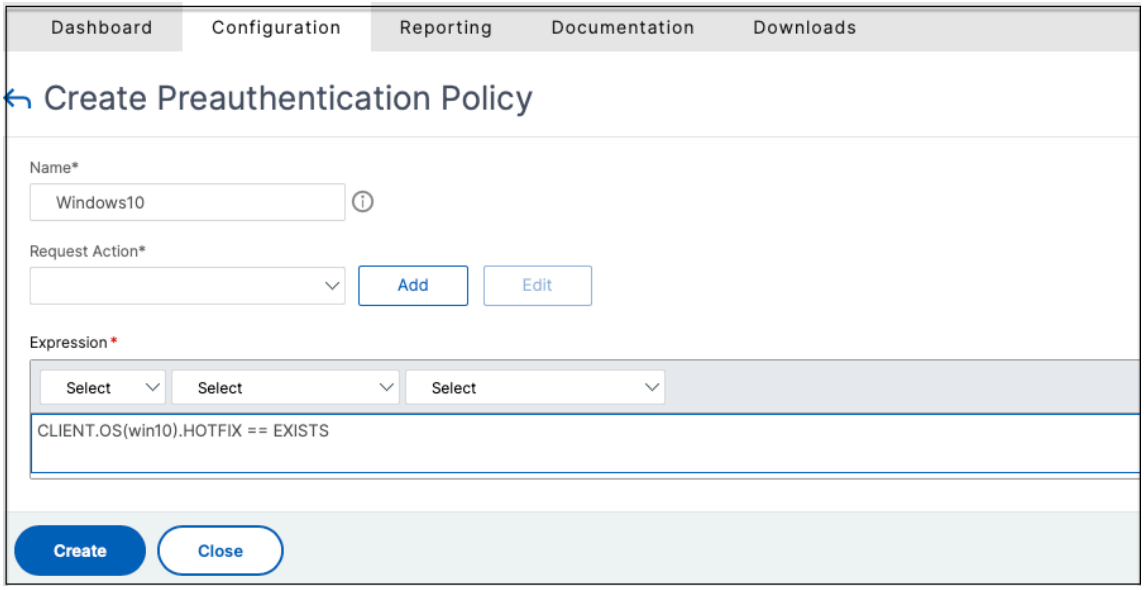
配置经典网关预身份验证策略

1. 导航到 **NetScaler** 网关 **>** 政策 **>** 预身份验证，然后单击 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 请求操作点击 加 以创建操作。您可以对多个策略重复使用此操作，例如，使用一个操作允许访问，使用另一个操作拒绝访问。

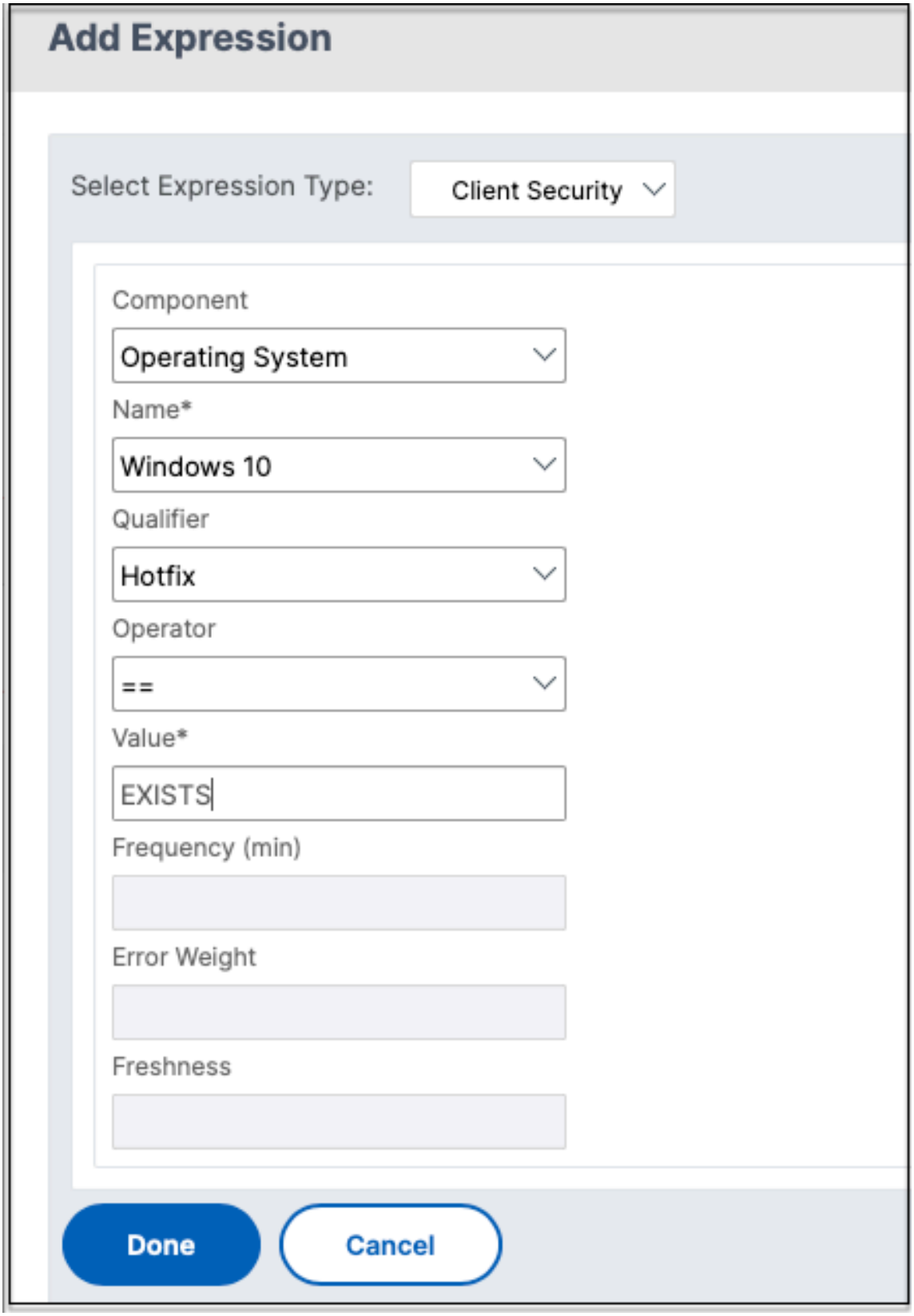


4. 在必填字段中填写详细信息，然后单击 创造.

5. 在 表达，请手动输入表达式或使用表达式编辑器为策略构建表达式。



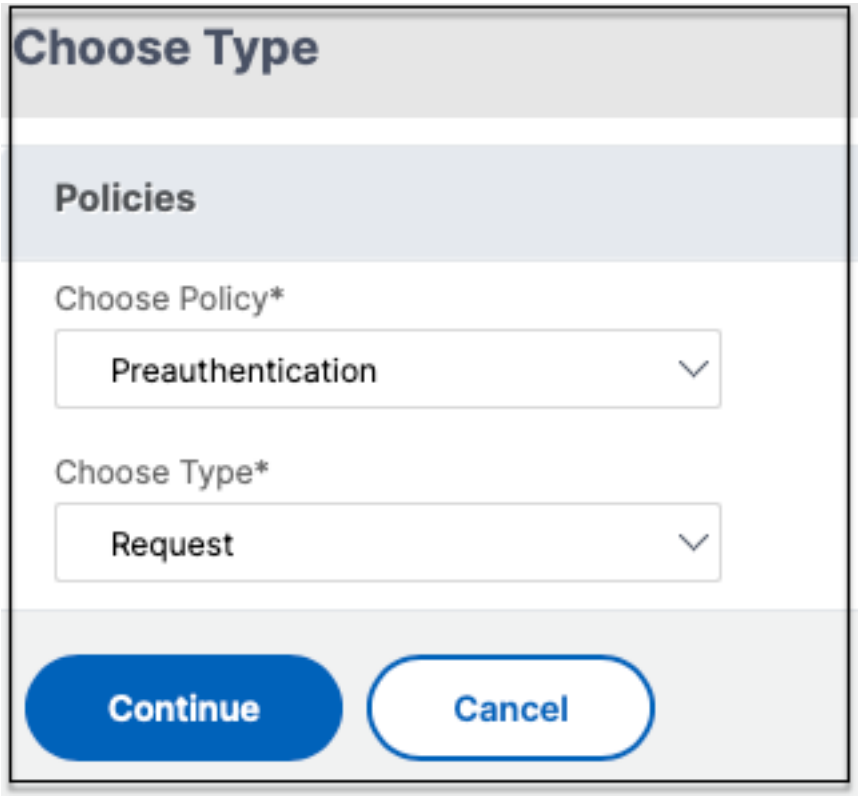
下图显示了为检查 Windows 10 操作系统而构建的示例表达式。



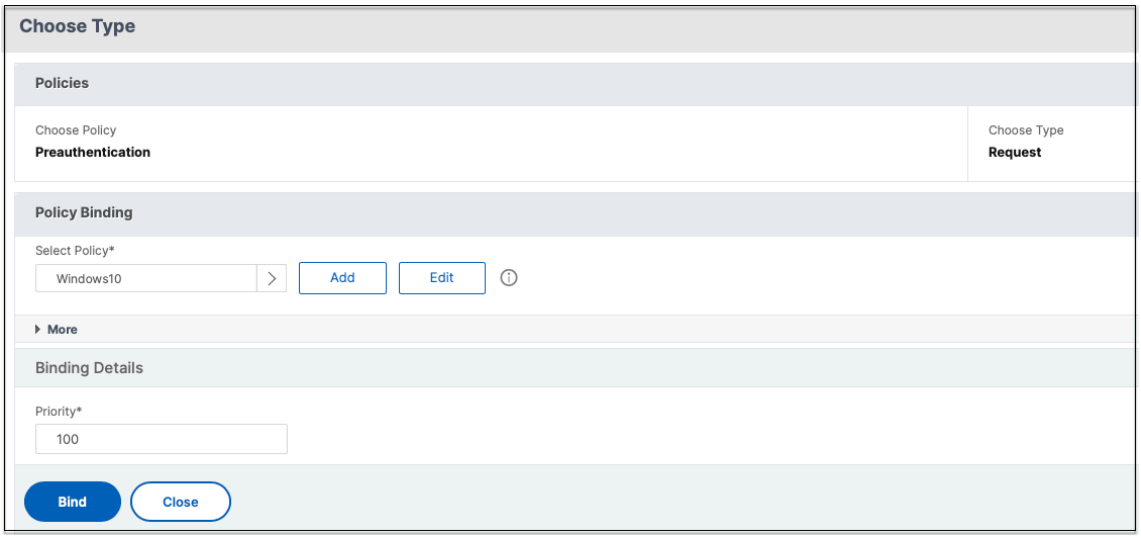
6. 单击“创建”。

将自定义标记绑定到 **NetScaler Gateway**

1. 导航到 **NetScaler Gateway >** 虚拟服务器。
2. 选择要为其绑定预身份验证策略的虚拟服务器，然后单击 编辑.
3. 在 政策 部分中，单击 **+** 以绑定策略。
4. 在 选择 **Policy** （策略），选择预身份验证策略，然后选择 请求 在 选择 **Type** （类型）.



5. 选择策略名称和策略评估的优先级。
6. 单击绑定。



使用 **CLI** 配置自定义标签

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`

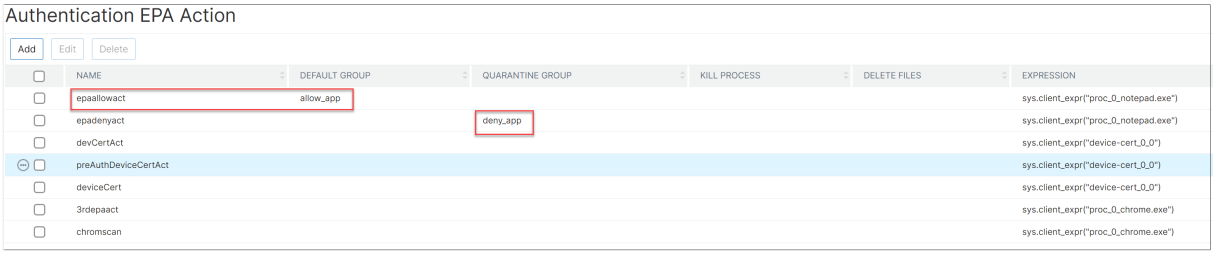
添加新的上下文标记

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 并选择 上下文标签, 匹配所有，然后输入上下文标签名称（例如 `Windows10操作系统`).

有关发送到 **Secure Private Access** 插件的 **EPA** 标记的说明

在 nFactor EPA 策略中配置的 EPA 操作名称以及作为 Secure Private Access 插件的智能访问标签的关联组名称。但是，发送的标签取决于 EPA 行动评估的结果。

- 如果 nFactor EPA 策略中的所有 EPA 操作都导致操作 否认 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 允许，则与操作关联的 EPA 策略名称和默认组名称（如果已配置）将作为智能访问标记发送。



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 插件。允许操作时，*EPAALLOWACT* 和 *allow_app* 将作为智能访问标签发送到 Secure Private Access 插件。

引用

- 为应用程序配置访问策略.
- 支持智能访问标签.

许可证服务器

October 21, 2024

Secure Private Access 插件的许可证服务器是收集和处理授权数据所需的必需组件。许可证服务器可以在初始设置期间注册到 Secure Private Access，也可以在设置完成后对其进行配置或更新。有关向 Secure Private Access 注册许可证服务器的详细信息，请参阅 集成 StoreFront 和 NetScaler Gateway 服务器.

您必须指定许可证服务器 URL 才能将 Secure Private Access 与许可证服务器连接。Secure Private Access 插件会自动在许可证服务器上注册自身。

> 注意：
>
> - 您必须在许可证服务器上至少安装一个 Citrix Virtual Apps and Desktops 代理许可证，才能在许可证服务器上注册 Secure Private Access 插件。
> - 版本 11.17.2 版本 45000 及更高版本支持 Secure Private Access 插件的许可证服务器。如果您已经拥

> 有许可证服务器，则必须将许可证服务器升级到版本 11.17.2 build 45000 版本或更高版本。

配置工具参数

以下配置工具参数可用于许可证服务器：

- 散列法- `.\AdminConfigTool.exe LICENSE_SERVER_ENABLE_HASHING <true|false>`
- 下载 PII 数据 - `.\AdminConfigTool.exe DOWNLOAD_PII_DATA <filename>`

有关许可服务器的更多信息，请参阅 许可服务器.

Citrix Secure Access 客户端

October 21, 2024

借助 Citrix Secure Private Access 客户端，您现在可以使用本机浏览器或通过计算机上运行的 Citrix Secure Access 客户端访问所有私有应用程序，包括 TCP/UDP 和 HTTPS/HTTP 应用程序。

借助 Citrix Secure Private Access 中对 TCP/UDP 应用程序的额外支持，您现在可以消除对传统 VPN 解决方案的依赖，为远程用户提供对所有私有应用程序的访问。

工作原理

最终用户只需在其客户端设备上安装 Citrix Secure Access 客户端，即可轻松访问其所有经批准的私有应用程序。

- 对于 Windows，客户端版本（24.6.1.17 及更高版本）可以从 https://www.citrix.com/downloads/citrix-gateway/plug-ins/citrix-secure-access-client-for-windows.html.
- 对于 macOS，可以从 App 下载客户端版本（24.06.2 及更高版本）

在 Windows 计算机上安装 Citrix Secure Access 客户端

支持的操作系统版本：

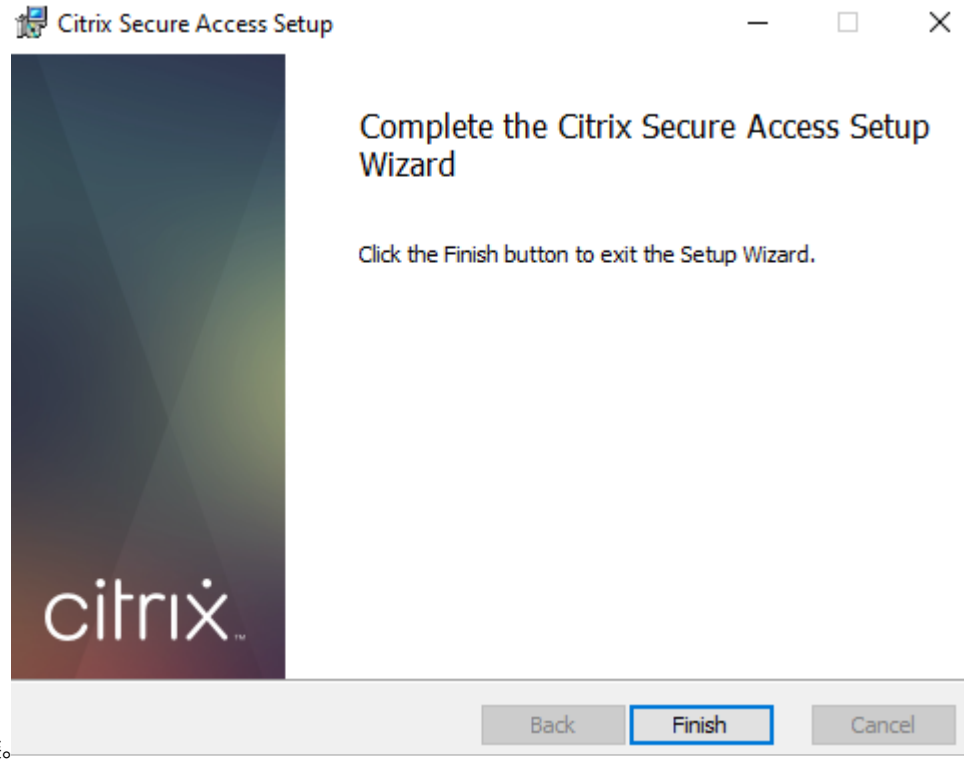
Windows –Windows 11、Windows 10、Windows Server 2016 和 Windows Server 2019。

以下是在 Windows 计算机上安装 Citrix Secure Access 客户端的步骤。

1. 从以下位置下载 Citrix Secure Access 客户端 https://www.citrix.com/downloads/citrix-gateway/plug-ins/citrix-secure-access-client-for-windows.html.

2. 点击 安装 以在 Windows 计算机上安装客户端。如果您有现有的 Citrix Gateway 客户端，则会升级相同的客户端。

3. 点击 完成 以完成安装。



> 注意：
>
> 不支持 Windows 中的多用户会话。

在 **macOS** 计算机上安装 **Citrix Secure Access** 客户端

1. 从 App Store 下载适用于 macOS 的 Citrix Secure Access 客户端。
2. 点击 打开 下载完成后。

> 注意：
>
> - 适用于 macOS 的 Citrix Secure Access 客户端可从 macOS 10.15 （Catalina）及更高版本获得。
> - 预览版本在 TestFlight 应用程序中仅可用于 macOS Monterey （12.x）。
> - 如果要在 App Store 应用程序和 TestFlight 预览应用程序之间切换，则必须重新创建要用于 Citrix Secure Access 应用程序的配置文件。例如，如果您一直在使用 `blr.abc.company.com`，删除 VPN 配置文件，然后再次创建相同的配置文件。

支持的操作系统版本：

macOS - 14.x （索诺玛）、13.x （文图拉）、12.x （蒙特雷）

不受支持的功能

适用于本地的 Secure Private Access 解决方案不支持以下功能。

- 在 Windows 登录之前始终打开（计算机隧道）
- DNS-TCP

不支持的客户端平台

适用于本地的 Secure Private Access 解决方案不支持以下平台。

- Linux
- iOS
- Android

Director

October 21, 2024

Director 与 Secure Private Access 的集成可实现有效的性能监控和故障排除。要将 Director 与 Secure Private Access 集成，必须输入必须向 Secure Private Access 注册的 Director 服务器的 FQDN 的 IP 地址。有关详细信息，请参阅 集成服务器.

使用 Secure Private Access 注册 Director 是本地版本 2402 客户的 Secure Private Access 的强制性配置。如果未配置 Director，则必须安装最新版本的 Director，即 LTSR 2402 或更高版本。如果您已经配置了 Director，则必须将其升级到最新版本 LTSR 2402 或更高版本。如果不注册 Director，则无法完成 Secure Private Access 设置。在以下情况下，验证也会失败。

- Director 未在 Secure Private Access 中注册。
- 您输入的 Director IP 地址或 FQDN 不存在。

有关使用 Secure Private Access 注册 Director 的详细信息，请参阅 集成 StoreFront 和 NetScaler Gateway 服务器 和 安装后管理设置.

> 注意：
>
> - 从 Secure Private Access 2407 或更高版本开始，除了 Web/SaaS 应用程序之外，还会在 Director 控制板中显示 TCP/UDP 会话。
> - Director 注册或登录不支持集成 Windows 身份验证（IWA）。如果管理员已使用 IWA 登录到 Secure Private Access 控制台，则系统会提示管理员输入 Director 注册的凭据。
> - 如果管理员已手动登录到 Secure Private Access 控制台，则这些详细信息将用于向 Director 服务器进行身份验证。如果不成功，系统会提示管理员输入凭证。
> - 如果管理员必须在设置完成后添加其他 Director，请从 管理设置 页。在设置后更新 Director 详细信息时，管理员必须输入凭据才能进行更改。编辑 Director URL IPv6 和 SSLv3 时不支持单点登录。

使用 **Director** 配置工具通过 **Secure Private Access** 配置 **Director**

使用 Config 工具使用 Secure Private Access 配置 Director 是完成集成的必要步骤。有关详细信息，请参阅 Secure Private Access 与 Director 的集成.

在 **Director** 中查看 **Secure Private Access** 用户会话

您可以在 Director 中查看 View Secure Private Access 用户会话。有关详细信息，请参阅 按用户查看 Secure Private Access 会话.

Web Studio

August 26, 2024

Citrix Secure Private Access 还集成到 Web Studio 控制台中，使用户能够通过 Web Studio 无缝访问该服务。

要启用此集成，必须安装 Web Studio 版本 2308 或更高版本。

有关详细信息，请参阅 Secure Private Access 与 Web Studio 的集成。

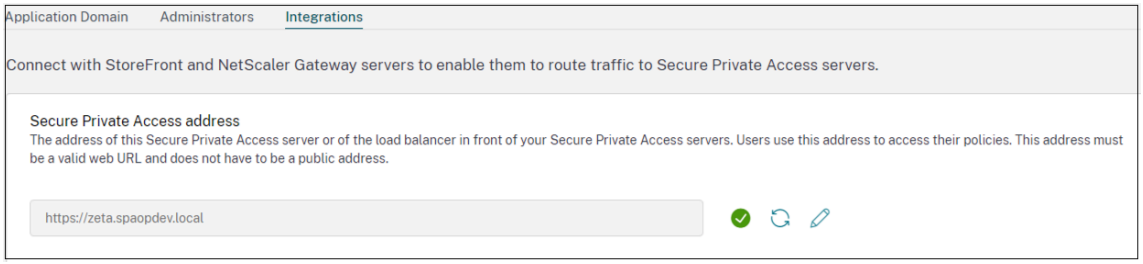
将 **Secure Private Access** 部署为群集

October 21, 2024

Secure Private Access 本地解决方案可以部署为集群，以实现高可用性、高吞吐量和可扩展性。对于大型部署（例如，超过 5000 个用户），可以部署多个单独的 Secure Private Access 节点来分配工作负载并增强可扩展性。

创建 **Secure Private Access** 节点

- 创建新的 Secure Private Access 站点。有关详细信息，请参阅 设置 Secure Private Access 站点.
- 将所需数量的群集节点添加到 Secure Private Access 站点。有关详细信息，请参阅 通过加入现有站点设置 Secure Private Access.
- 在每个 Secure Private Access 节点中，配置相同的服务器证书。证书使用者公用名或使用者备用名称必须与负载均衡器 FQDN 匹配。
- 在 Secure Private Access 中配置第一个节点时，请使用负载均衡器名称。要添加后续节点，请在 Integrations 选项卡中指定数据库地址，然后手动运行数据库脚本。有关使用脚本升级数据库的详细信息，请参阅 使用脚本升级数据库.



负载均衡器配置

Secure Private Access 群集设置没有特定的负载平衡配置要求。如果您使用 NetScaler 作为负载均衡器，请注意以下事项：

- 用于访问 StoreFront 的 FQDN 作为主题备用名称（SAN）包含在 DNS 字段中。如果您使用的是负载均衡器，请同时包含单个服务器的 FQDN 和负载均衡器 FQDN。这适用于 SSL 证书。对于 Secure Private Access，配置负载均衡器就足够了。有关详细信息，请参阅 使用 NetScaler 进行负载平衡. 在配置 Secure Private Access 之前，必须配置 StoreFront Store。如果使用负载均衡器，请使用负载均衡器名称配置基 URL，并使用 HTTPS 进行安全通信。有关详细信息，请参阅 使用 HTTPS 保护 StoreFront.
- 建议 Secure Private Access 服务以 HTTPS 格式运行，但这不是强制性要求。Secure Private Access 服务也可以部署为 HTTP。

- 支持 SSL 卸载或 SSL 网桥，因此可以使用任何负载均衡器配置。使用 SSL 网桥时，请确保在每个 Secure Private Access 节点中配置相同的服务器证书。此外，证书使用者公用名或使用者备用名称（SAN）必须与负载均衡器 FQDN 匹配。此外，必须在负载均衡器服务中配置 SAN。
- 正确的 SSL 证书绑定到 IIS 服务器和 NetScaler。
- 使用安全密码。
- Secure Private Access 服务（管理员和运行时）是无状态的，因此不需要持久性。
- 负载均衡器（例如 NetScaler）具有用于后端服务器的默认内置监视器（探测器）。如果必须为 Secure Private Access 本地服务器配置基于 HTTP 的自定义监控器（探测），则可以使用以下终端节点：

  `/secureAccess/health`

  预期响应：

  ```
  1    Http status code: 200 OK
  2
  3    Payload:
  4
  5    {
  6  "status":"OK","details":{
  7  "duration":"00:00:00.0084206","status":"OK" }
  8   }
  ```

  有关配置 NetScaler 负载均衡器的详细信息，请参阅 设置基本负载均衡.

为 **Secure Private Access** 创建监控器

使用以下 CLI 命令为 Secure Private Access 创建监控器。

```
add lb monitor SPAHealth HTTP -respCode 200 -httpRequest "GET /
secureAccess/health"-secure YES
```

创建监控器后，将证书绑定到监控器。

有关使用 NetScaler UI 创建监视器的详细信息，请参阅 创建监视器.

配置 **Secure Private Access** 插件

October 21, 2024

安装 Citrix Secure Access 插件后，您可以设置 Secure Private Access 环境，然后为应用程序配置应用程序和访问策略。Secure Private Access 支持 Web/SaaS 和 TCP/UDP 应用程序。访问策略允许您根据用户或用户组启用或禁用对应用程序的访问。此外，您还可以通过启用适当的安全限制来启用对应用程序（HTTP/HTTPS 和 TCP/UDP）的受限访问。

- 配置 HTTP/HTTPS 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
- 为应用程序配置访问策略
- 访问限制选项

设置 **Secure Private Access**

August 26, 2024

您可以通过创建新站点或加入现有站点来设置 Secure Private Access。在这两种情况下，您都可以使用 Web 管理员控制台来设置 Secure Private Access 环境。

- 通过创建新站点来设置 Secure Private Access
- 通过加入现有站点来设置 Secure Private Access

必备条件

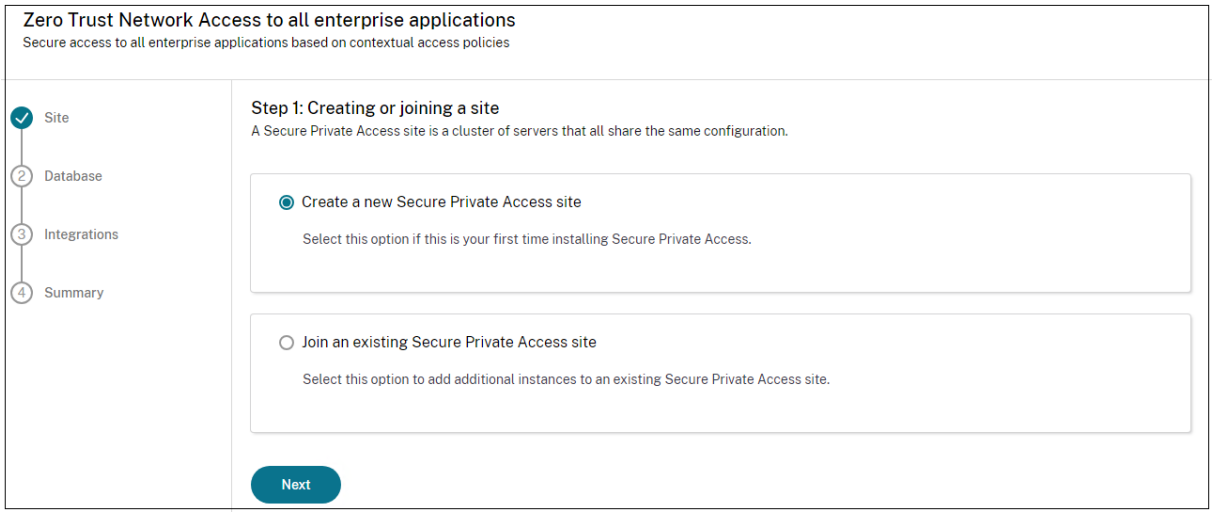
- 您必须使用域用户登录 Secure Private Access 管理员控制台，该域用户也是安装了 Secure Private Access 的计算机的本地计算机管理员。
- 在创建站点之前，必须安装 SQL 数据库服务器。

通过创建新站点来设置 **Secure Private Access**

步骤 **1**：设置 **Secure Private Access**

站点是您的 Secure Private Access 部署的名称。您可以创建网站或加入现有站点。

1. 启动 Secure Private Access Web 管理员控制台。
2. 默认情况下，在“创建或加入站点”页面上，“创建新的 **Secure Private Access** 站点”处于选中状态。
3. 单击下一步。



选择创建站点时，必须自动或手动为新站点配置数据库，因为与该站点名称对应的数据库可能在设置中不可用。

步骤 **2**：配置数据库

您必须为新的 Secure Private Access 站点创建数据库。这可以手动或自动完成。

1. 在 **SQL Server** 主机中，输入服务器主机名。例如，`sql1.fabrikam.local\citrix`。

   可以使用以下格式之一指定数据库地址：

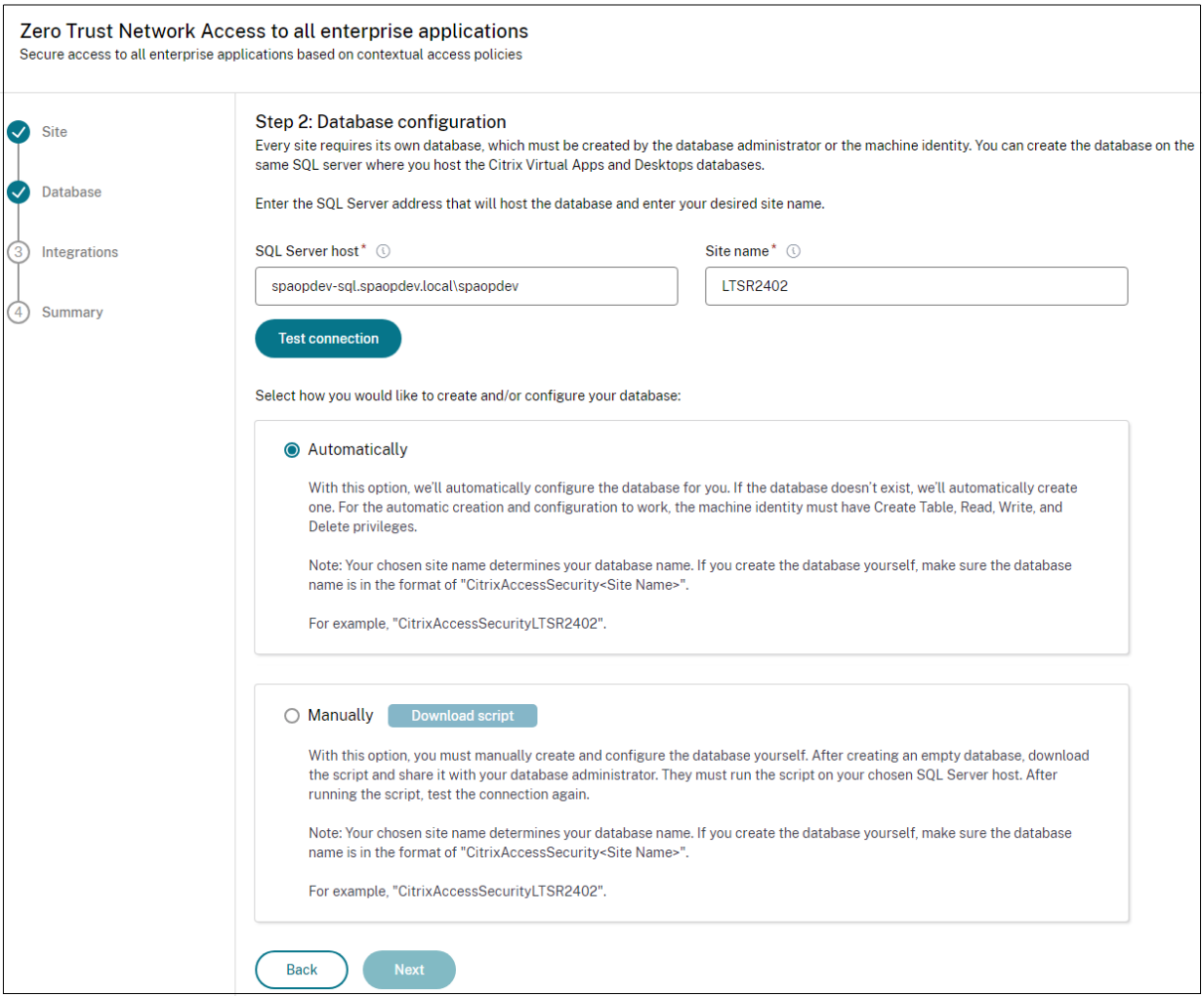
   - ServerName
   - ServerName\InstanceName
   - ServerName,PortNumber

   有关详细信息，请参阅数据库。

2. 在站点中，键入 Secure Private Access 站点的名称。

   > 注意：
   >
   > 您输入的站点名称是数据库名称的后缀。数据库名称格式是 `CitrixAccessSecurity<sitename>` 且无法修改。如果需要自定义数据库名称，请联系 Citrix 支持部门。

3. 单击“测试连接”以检查 SQL Server 实例是否有效，并确认该站点的指定数据库是否存在。



> 注意：

- 如果 SQL Server 不适用于该站点，则连接检查将失败。
- 如果 SQL Server 可用但数据库不存在，则连接检查通过。但是，会显示一条警告消息。
- Secure Private Access 使用计算机身份的 Windows 身份验证对 SQL Server 进行身份验证。

自动配置：

- 只有当计算机身份具有所需的数据库权限时，才能使用 自动配置 选项。
- 如果指定地址不存在数据库，则会自动创建数据库。
- 创建数据库时，请确保该数据库为空但具有所需的数据库权限。有关权限的详细信息，请参阅 设置数据库所需的权限。

手动配置：

您可以使用“手动配置”选项来设置数据库。

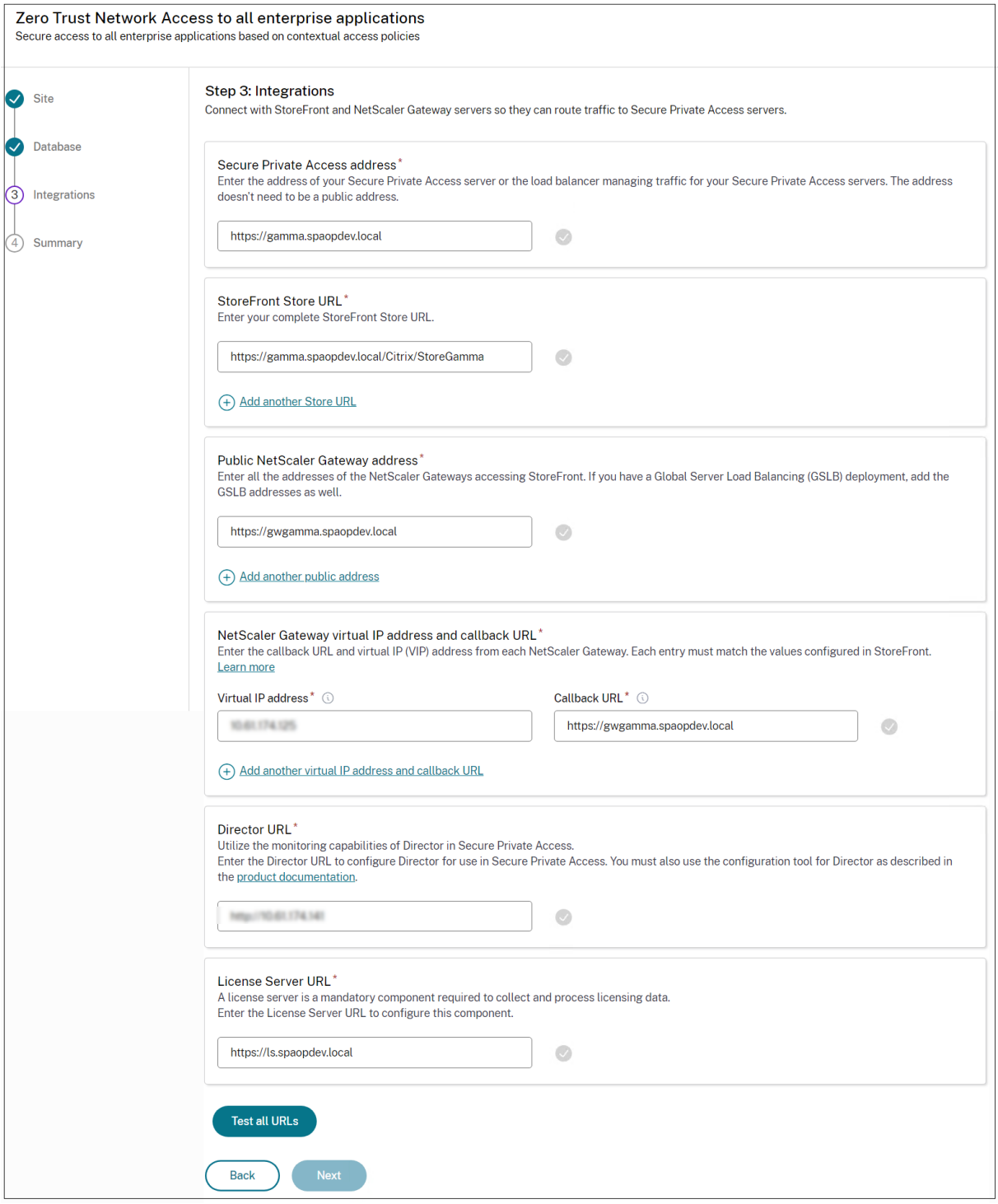
在手动配置中，必须先下载脚本，然后在在 **SQL Server** 主机字段中指定的数据库服务器上运行脚本。

> 注意：
>
> 如果计算机不具有“读取”、“写入”和”更新”权限来在 SQL Server 上的数据库中创建表，则数据库创建可能会失败。必须在计算机上启用相应的权限。有关详细信息，请参阅 设置数据库所需的权限。

步骤 **3**：集成服务器

要将 Secure Private Access 与 StoreFront 和 NetScaler Gateway 服务器连接起来，必须指定 StoreFront 和 NetScaler Gateway 服务器的详细信息。必须建立此连接才能让 StoreFront 和 NetScaler Gateway 将流量路由到 Secure Private Access。您还必须指定 Director 服务器和许可服务器的详细信息。

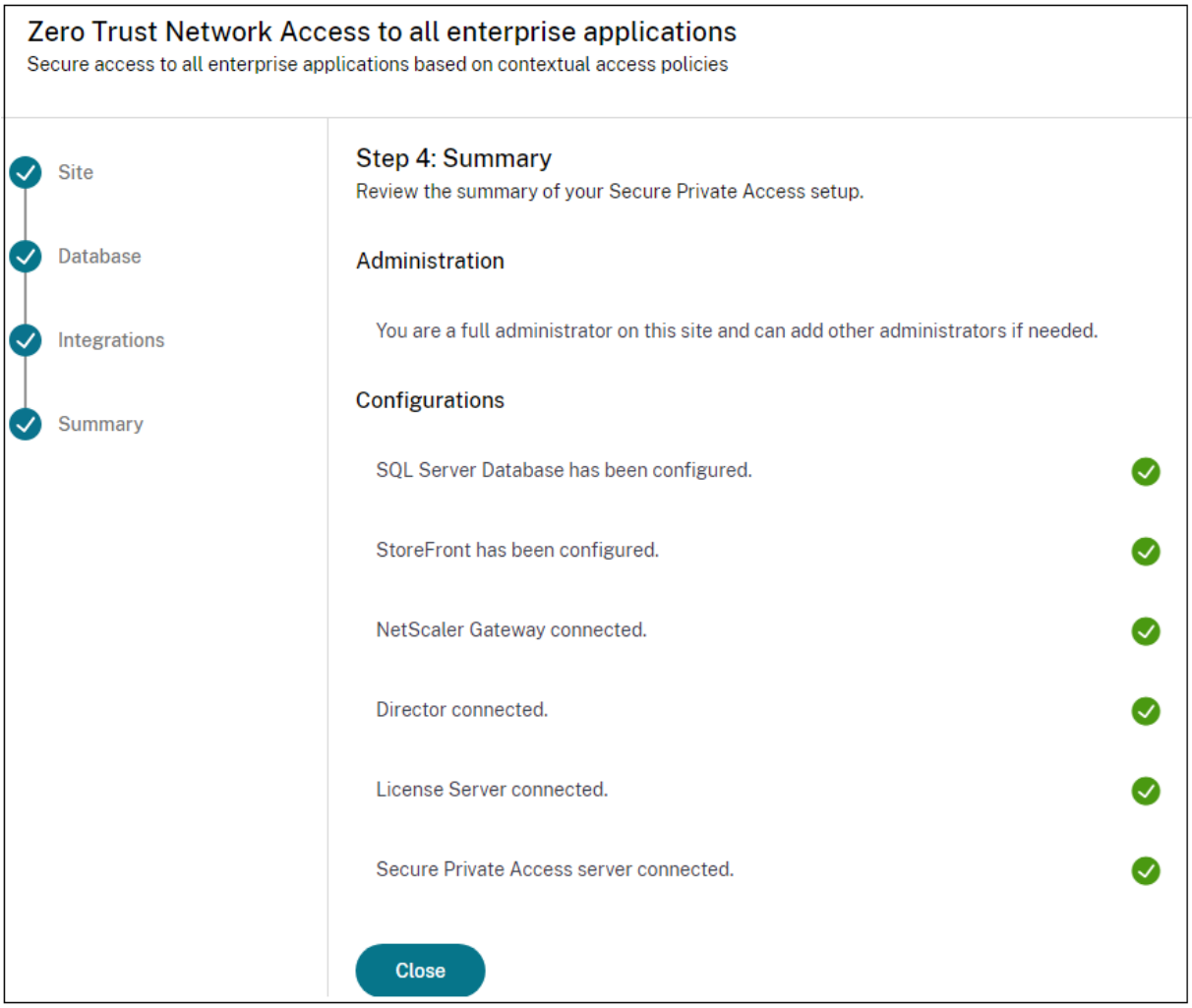
1. 输入以下详细信息。
    - **Secure Private Access** 服务器地址。例如，`https://secureaccess.domain.com`。
    - **StoreFront** 应用商店 **URL**。例如，`https://storefront.domain.com/Citrix/StoreMain`。
    - 公共 **NetScaler** 网关地址—NetScaler Gateway 的 URL。例如，`https://gateway.domain.com`。
    - 虚拟 **IP** 地址—此虚拟 IP 地址必须与 StoreFront 中为回调配置的虚拟 IP 地址相同。
    - 回调 **URL** —此 URL 必须与 StoreFront 中配置的相同。例如，`https://gateway.domain.com`。
    - **Director URL**：-（可选）用于将 Secure Private Access 与 Citrix Director 连接的 Director 服务器 IP 地址或 FQDN。
    - 许可证服务器 **URL**： - 用于收集和处理许可数据的许可证服务器 IP 地址。
2. 单击验证所有 **URL**
3. 单击下一步，然后单击保存。



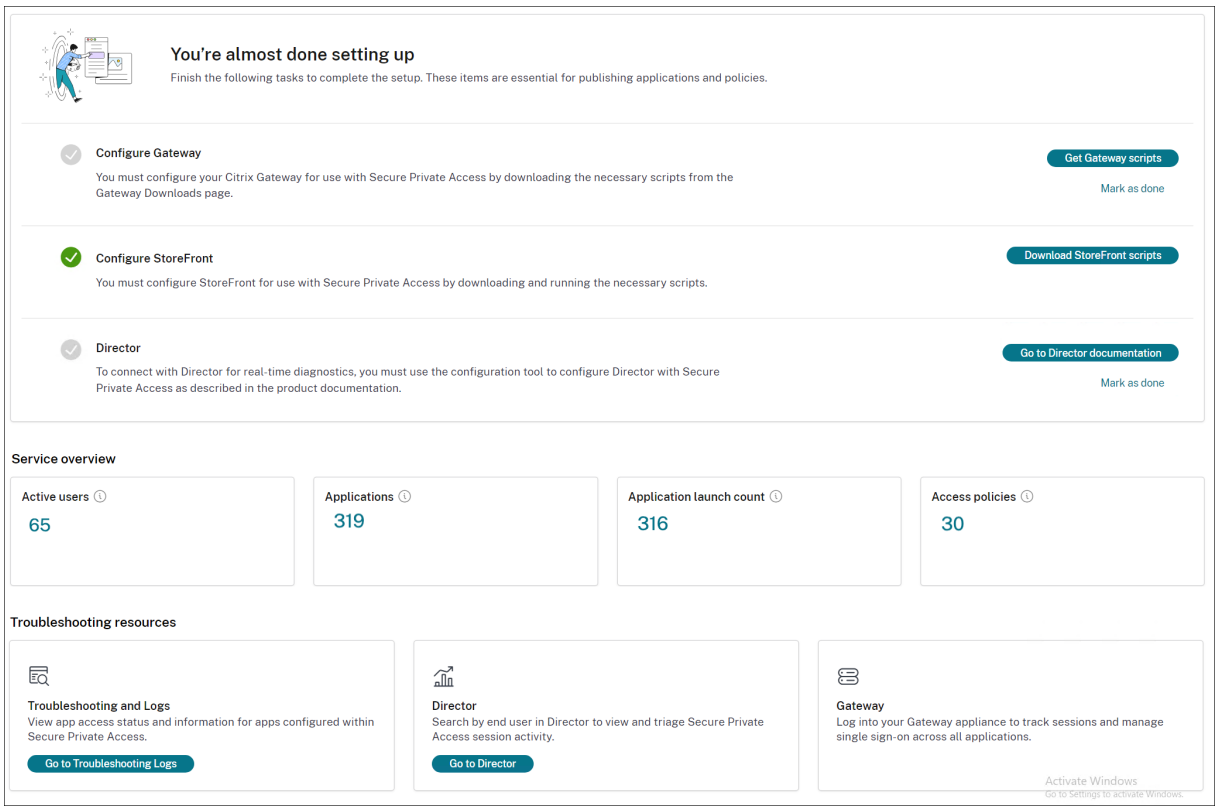
步骤 **4**：配置摘要

配置完成后，将进行验证以确保配置的服务器可以访问。此外，还会进行检查以确保可以访问 Secure Private Access 服务器。

如果配置摘要页面显示任何错误，请参阅错误故障排除以了解详细信息。如果这不能解决问题，请联系 Citrix 支持部门。



安装完成后，单击“摘要”页面上的“关闭”后，将显示以下页面。

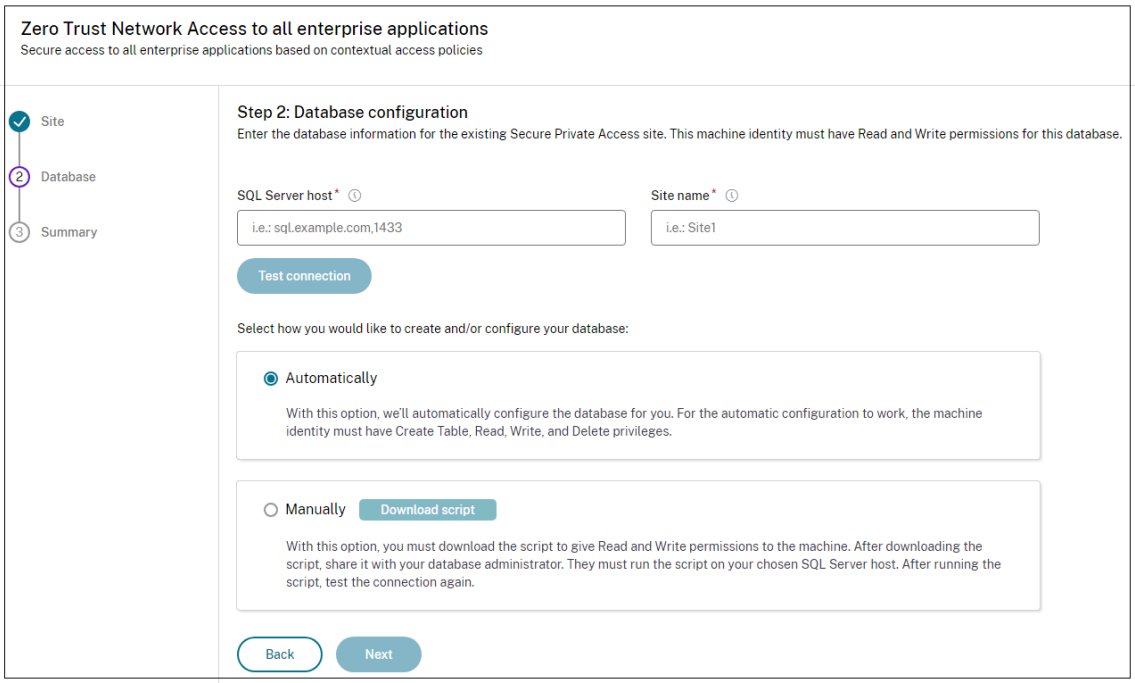


> 注意：
>
> - 设置环境后，您可以从 Web 管理员控制台中的“设置” > “集成”修改设置。
> - 首次安装 Secure Private Access 权限的管理员被授予完全权限。然后，该管理员可以将其他管理员添加到设置中。您可以从“设置” > “管理员”中查看管理员列表。
> - 您还可以添加管理员组，以便为该组中的所有管理员启用访问权限。

有关详细信息，请参阅 安装后管理设置。

通过加入现有站点来设置 **Secure Private Access**

1. 在“创建或加入站点”页面上，选择“加入现有站点”，然后单击“下一步”。

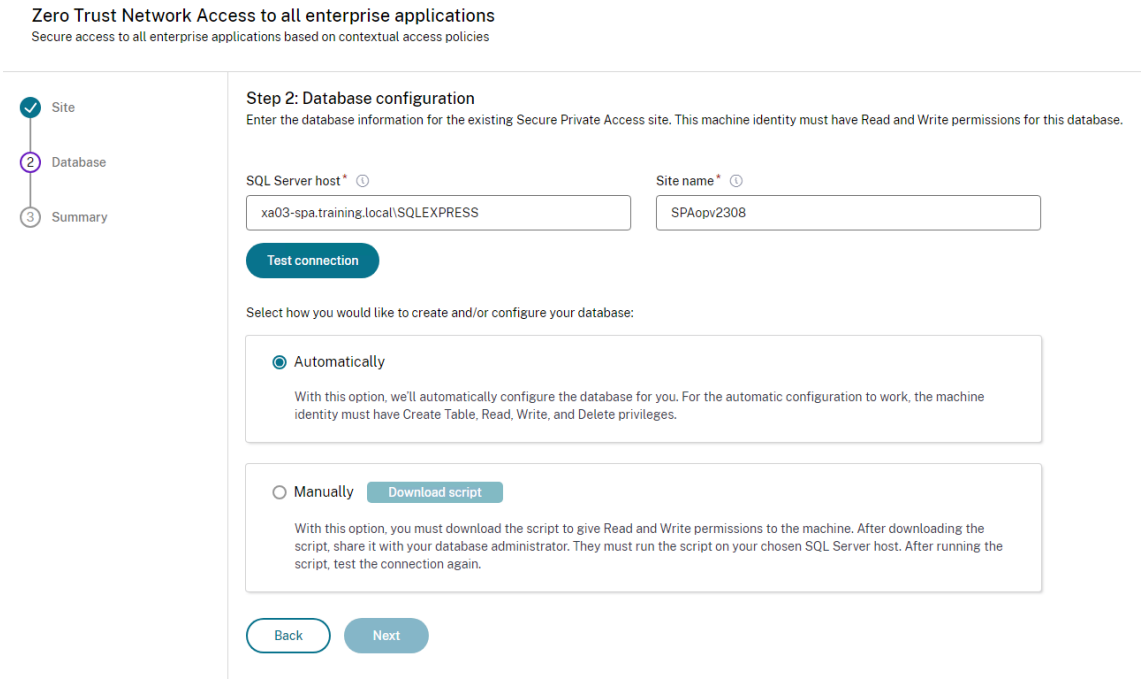


2. 在 **SQL Server** 主机中，输入服务器主机名。确保所选的 SQL Server 中已经存在与您输入的站点名称对应的数据库。可以使用以下格式之一指定数据库地址：

   - ServerName
   - ServerName\InstanceName
   - ServerName,PortNumber

   有关详细信息，请参阅数据库。

3. 在站点中，键入 Secure Private Access 站点的名称。
4. 单击“测试连接”以检查 SQL Server 实例是否有效，并确认数据库中是否存在指定的站点。



如果该站点没有相应的数据库，则连接检查失败。

5. 单击“保存”。

进行配置验证检查是为了确保 SQL 数据库服务器已配置好并检查是否可以访问 Secure Private Access 服务器。

后续步骤

- 配置 NetScaler Gateway
- 配置应用程序
- 为应用程序配置访问策略

配置 **Web/SaaS** 应用程序

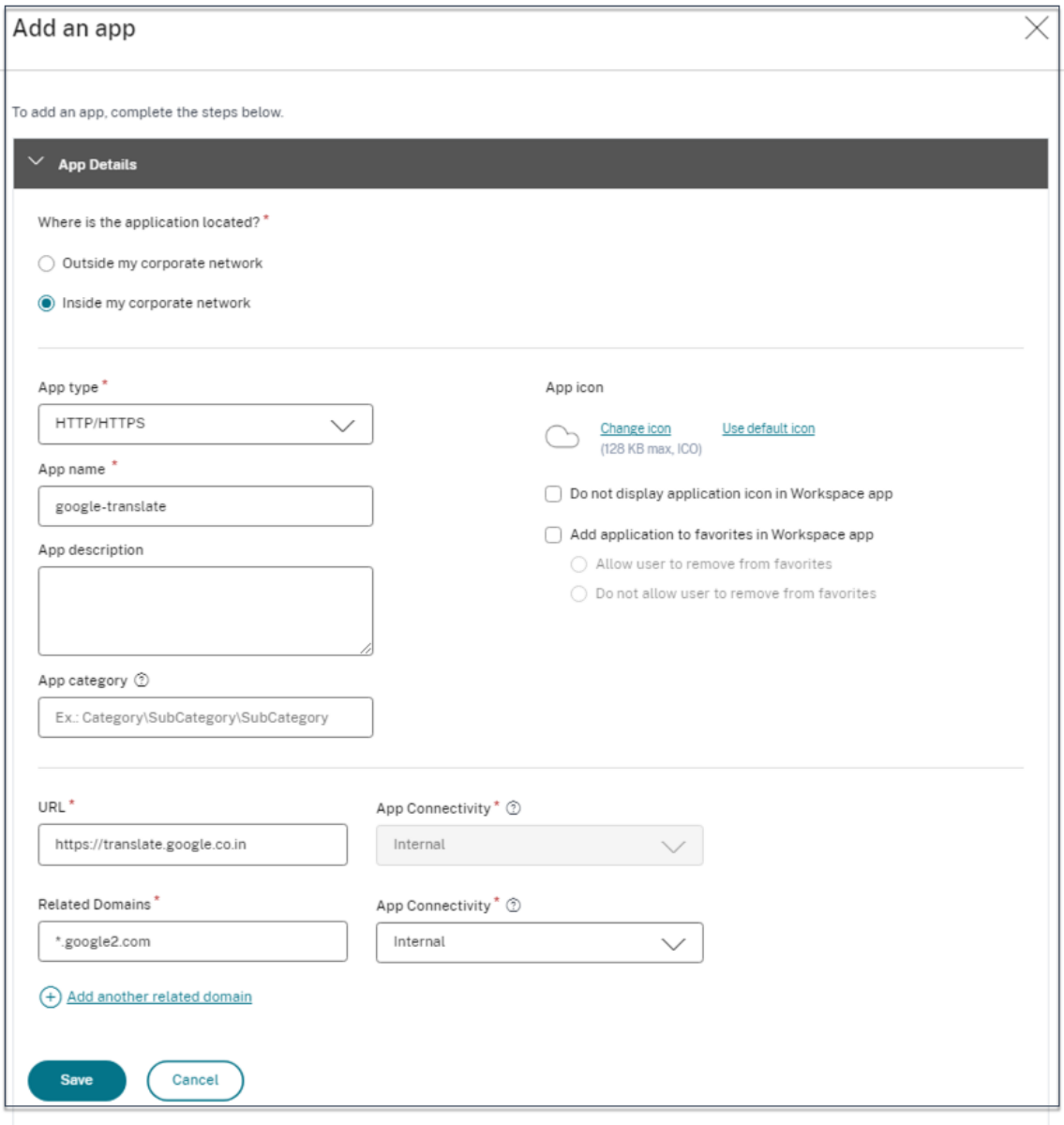
October 21, 2024

设置 Secure Private Access 后，您可以从 Admin Console 配置应用程序和访问策略。

1. 在 Admin Console 中，单击 应用.
2. 点击 添加应用程序.
3. 选择应用程序所在的位置。
    - 在我的公司网络之外 用于外部应用。

- 在我的公司网络内部 用于内部应用。

4. 在 App Details 部分输入以下详细信息，然后单击 下一个.



- 应用程序名称–应用程序的名称。
- 应用程序描述 - 应用程序的简要描述。此描述将在工作区中向您的用户显示。您还可以以 关键字：<keyword_name>. 您可以使用关键字来筛选应用程序。有关详细信息，请参阅 按包含的关键字筛选资源.
- 应用类别 - 添加类别和子类别名称（如果适用），您正在发布的应用程序必须显示在 Citrix Workspace UI 中。您可以为每个应用程序添加新类别，也可以使用 Citrix Workspace 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 Workspace UI 中的特定类别下。
  - 类别/子类别是管理员可配置的，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 Citrix Workspace 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，则该类别将列为新类别。

    例如，如果您在应用程序类别字段中输入了 Business and Productivity 类别，则除了 Business And Productivity 类别之外，Citrix Workspace 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 格式。如果不更改图标，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。
- 网址–应用程序的 URL。
- 相关领域–相关域将根据应用程序 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 App 的 Related Domain 不与其他 App 的 Related Domain 重叠。If this occurs, remove the related domain from all apps and create a new app with this domain and then set access accordingly in the access policy. You can also consider if you want to display this app in StoreFront or hide it. You can hide the app in StoreFront using the option **Do not display application to users** while publishing the app.
  > - 同样，不得将已发布应用程序的 URL 添加为其他应用程序的相关域。
  > - 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]（/zh-cn/citrix-secure-private-access/service/best-practices-app-configurations#same-related-domains-must-not-be-a-part-of-multiple-applications）。

- 自动将应用程序添加到收藏夹–单击此选项可将应用程序添加为 Citrix Workspace 应用程序中的收藏应用程序。选择此选项时，在 Citrix Workspace 应用程序中，应用程序的左上角会显示一个带有挂锁的星形图标。

  - 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 应用程序的收藏夹应用程序列表中删除该应用程序。选择此选项时，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 应用程序的收藏夹应用程序列表中删除该应用程序。

  如果从 Secure Private Access 控制台中删除标记为收藏夹的应用程序，则必须从 Citrix Workspace 的收藏夹列表中手动删除这些应用程序。如果从 Secure Private Access 控制台中删除应用程序，则不会自动从 StoreFront 中删除这些应用程序。

- 应用程序连接 -选择 内部 用于 Web 应用程序和 外部 适用于 SaaS 应用程序。

5. 点击 救，然后单击 完成.

您可以查看在 设置 **>** 应用领域. 有关更多详细信息，请参阅 安装后管理设置.

后续步骤

为应用程序配置访问策略

配置 **TCP/UDP** 应用程序

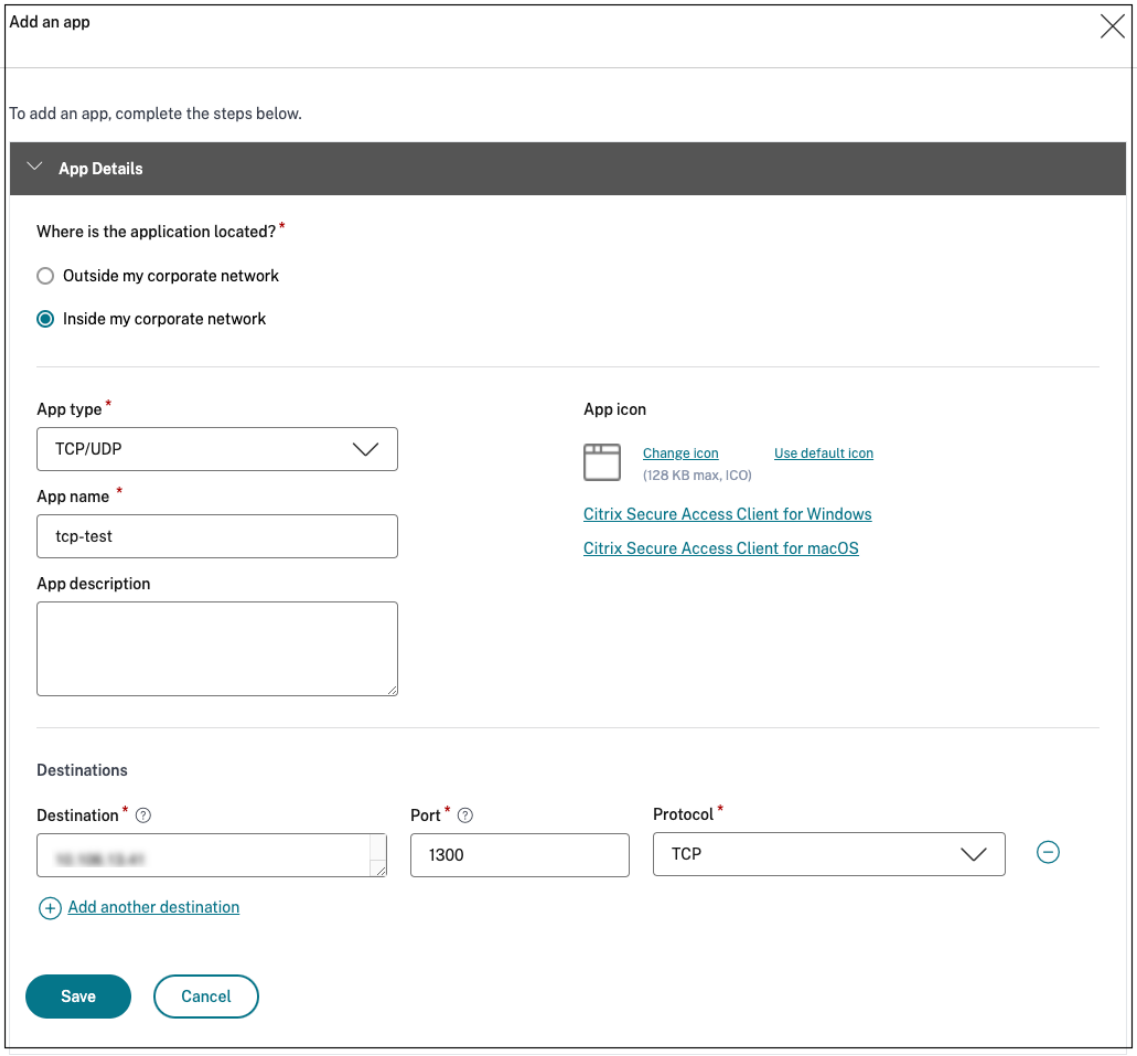
October 21, 2024

必备条件：

- Secure Private Access 设置已完成。
- 客户端版本满足以下要求：
  - Windows - 24.6.1.17 及更高版本
  - macOS - 24.06.2 及更高版本

执行以下步骤以从 **Admin Console** 配置 **TCP/UDP** 应用程序：

1. 在 Admin Console 中，单击 应用，然后单击 添加应用程序.
2. 选择位置 在我的公司网络内部.



3. 输入以下详细信息：

   - 应用类型–选择 **TCP/UDP** 协议 用于启动与驻留在数据中心的后端服务器的连接。

> 注意：
>
> 如果禁用了 SPAOP-3315-EnableZTNAApplications 功能标志，则 TCP/UDP 选项将显示为灰色。您必须手动更新数据库才能启用此功能标志。

```
- **应用名称** – 应用程序的名称。
- **应用描述** – 您要添加的应用程序的描述。 此字段为可选字段。
- **目的地** – 驻留在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 （云安全段）** – 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：** > > – 即使管理员使用 IP 地址配置了应用程序，最终用户也可以使用 FQDN 访问应用
```



```
程序。 这是可能的，因为 Citrix Secure Access 客户端可以将 FQDN 解析为实际 IP 地址。

下表提供了各种目标的示例，以及如何通过这些目标访问应用程序：

| 目标输入                | 如何访问应用程序
                                                                                                    |
| ----------------------- | -----------------------------------------------------------------------------------------------------
                                                                                                    |
| 10.10.10.1-10.10.10.100 | 最终用户只能通过此范围内的 IP 地址访问应用程序。
                                                                                                    |
| 10.10.10.0/24           | 最终用户只能通过在 IP CIDR 中配置的 IP 地址访问应用程序。
                                                                                                    |
| 10.10.10.101            | 最终用户只能通过 10.10.10.101 访问应用程序
                                                                                                    |
| `*.info.citrix.com`     | 最终用户应访问 `info.citrix.com` 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，并且只能是一个 \*。 是允许的。 |
| info.citrix.com         | 最终用户应访问 `info.citrix.com` only 和 no subdomains。 例如 `sub1.info.citrix.com` 无法访问。
                                                                                                    |

目标 IP 地址在资源位置之间必须是唯一的。 如果存在冲突的配置，则会针对应用程序域表中的特定 IP 地址显示一个警告符号 （**设置 > 应用领域**)。

![冲突](/en-us/citrix-secure-private-access/media/spaop-warning-conflict-config.png)

-       **Port** - The destination port on which the app is running. Admins can configure multiple ports or port ranges per destination.

        The following table provides examples of ports that can be configured for a destination.

        |Port input|Description|
        |---|---|
        |\*|By default, the port field is set to ` “*” ` \(any port). The port numbers from 1 to 65535 are supported for the destination.|
        |1300 - 2400|The port numbers from 1300 to 2400 are supported for the destination.|
```



```
31            |38389|Only the port number 38389 is supported for the
                 destination.|
32            |22,345,5678|The ports 22, 345, 5678 are supported for the
                 destination.|
33            |1300 - 2400, 42000-43000,22,443|The port number range from
                 1300 to 2400, 42000 - 43000, and ports 22 and 443 are
                 supported for the destination.|
34
35          >**注 意： **
36          >
37          >通 配 符 端 口 （*） 不 能 与 端 口 号 或 范 围 共 存 。
38
39  -         **Protocol** - TCP/UDP
```

1. 点击 加 以相应地添加其他目标或服务器。
2. 单击保存。该应用程序将添加到 应用程序配置 页。您可以从 应用 页面。为此，请单击与应用程序一致的省略号按钮，然后相应地选择操作。
   - 編輯應用
   - 删除

为 **TCP/UDP** 应用程序配置访问策略

要为用户启用对应用程序的访问权限，管理员需要创建访问策略。有关详细信息，请参阅 配置访问策略.

引用

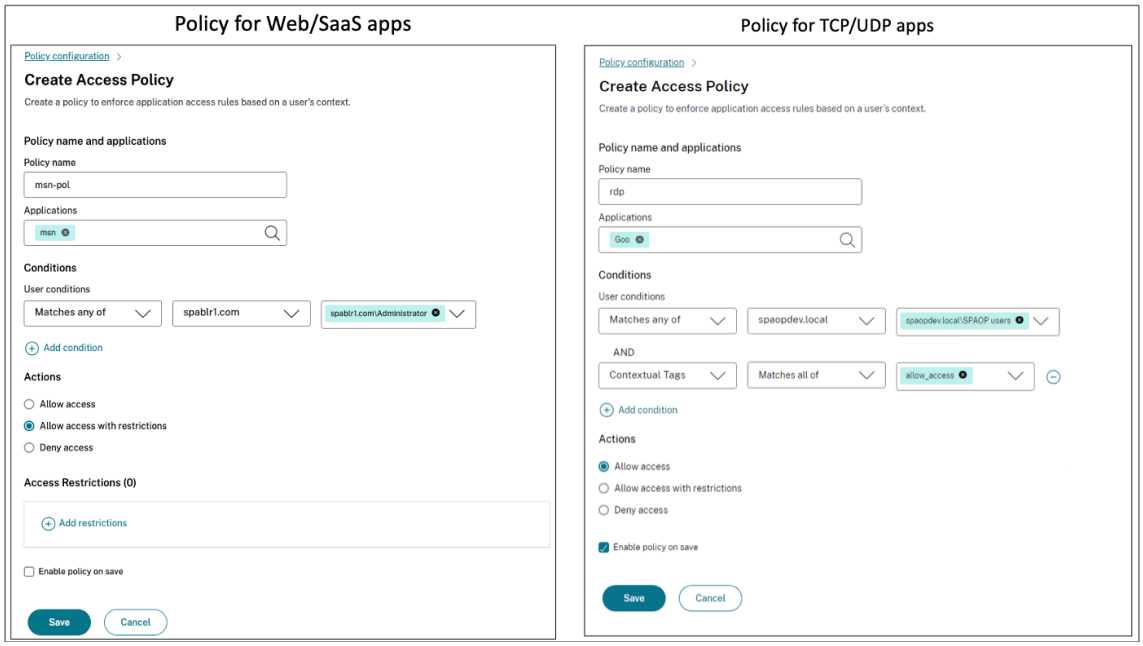
Citrix Secure Access 客户端.

为应用程序配置访问策略

August 26, 2024

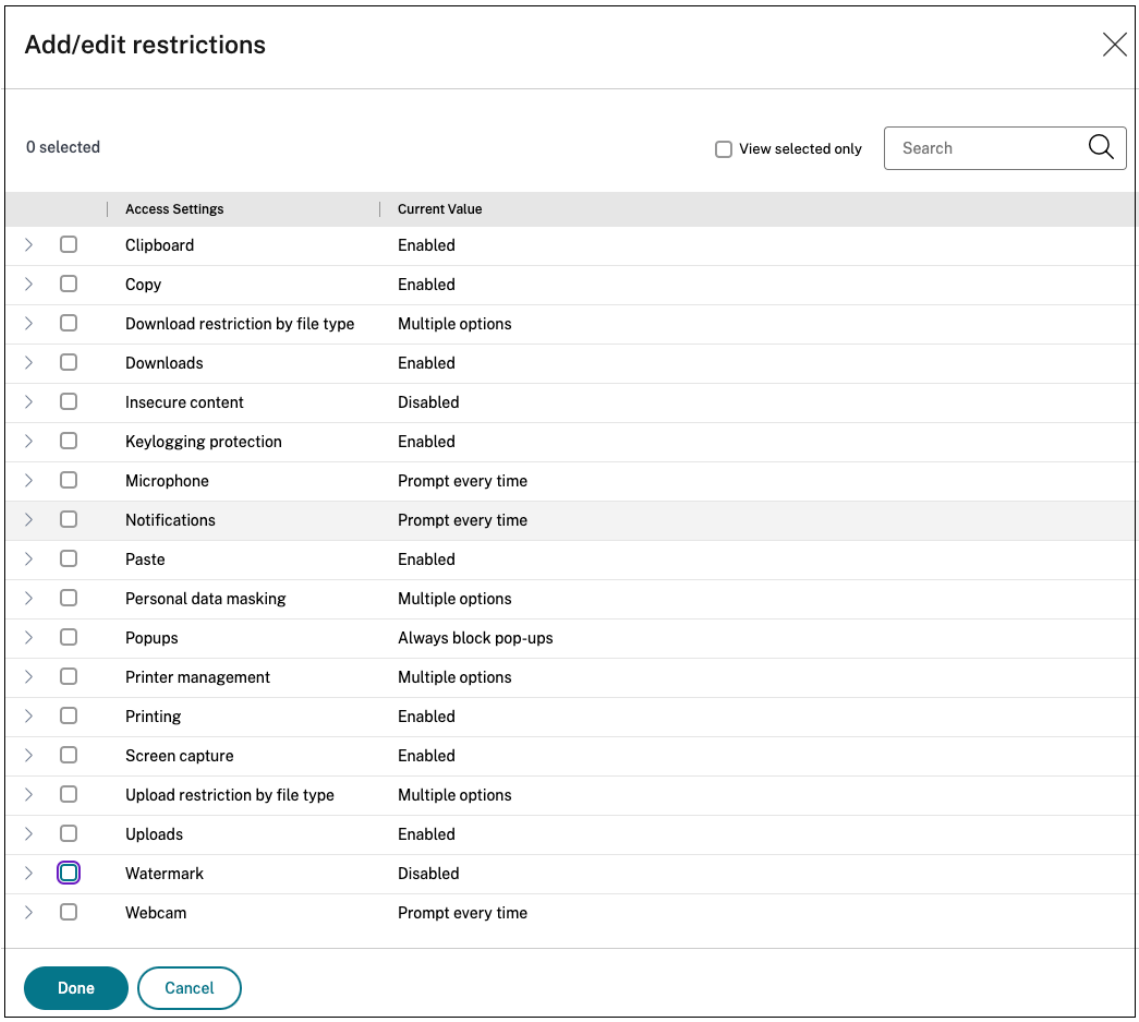
访问策略允许您根据用户或用户组启用或禁用对应用程序的访问权限。此外，您可以通过添加安全限制来启用对应用程序（HTTP/HTTPS 和 TCP/UDP）的受限访问。

1. 在管理员控制台中，单击“访问策略”。
2. 单击创建策略。



3. a) 在 策略名称中，输入策略的名称。
4. 在 应用程序中，选择要强制执行访问策略的应用程序。
5. 在用户条件中 - 选择必须允许或拒绝应用程序访问的条件和用户或用户组。
   - 匹配以下任一项：仅允许与字段中列出的任何名称相匹配的用户或组进行访问。
   - 与任何用户或组都不匹配：允许除字段中列出的用户或组之外的所有用户或组进行访问。
6. 单击“添加条件”，根据上下文标签添加另一个条件。这些标签源自 NetScaler Gateway。
7. 在操作中，选择必须根据条件评估在应用程序上强制执行的以下操作之一。
   - 允许访问
   - 允许有限制的访问
   - 拒绝访问

> 注意：
>
> - “允许有限访问”操作不适用于 TCP/UDP 应用程序。
> - 选择“允许有限制的访问”时，必须单击“添加限制”以选择限制。有关每项限制的更多信息，请参阅可用访问限制。



8. 选择限制，然后单击“完成”。
9. 选择“保存时启用策略”。如果不选择此选项，则仅在应用程序上创建策略，而不强制执行该策略。或者，您也可以使用切换开关从“访问策略”页面启用该策略。

访问策略优先级

创建访问策略后，默认情况下会为访问策略分配优先级。您可以在“访问策略”主页上查看优先级。

值较低的优先级具有最高优先级，并首先进行评估。如果此策略与定义的条件不匹配，则评估下一个优先级数较低的策略，依此类推。

您可以通过使用“优先级”列中的向上或向下移动策略来更改 优先级 顺序。

后续步骤

- 在客户端（Windows 和 macOS）上验证您的配置。

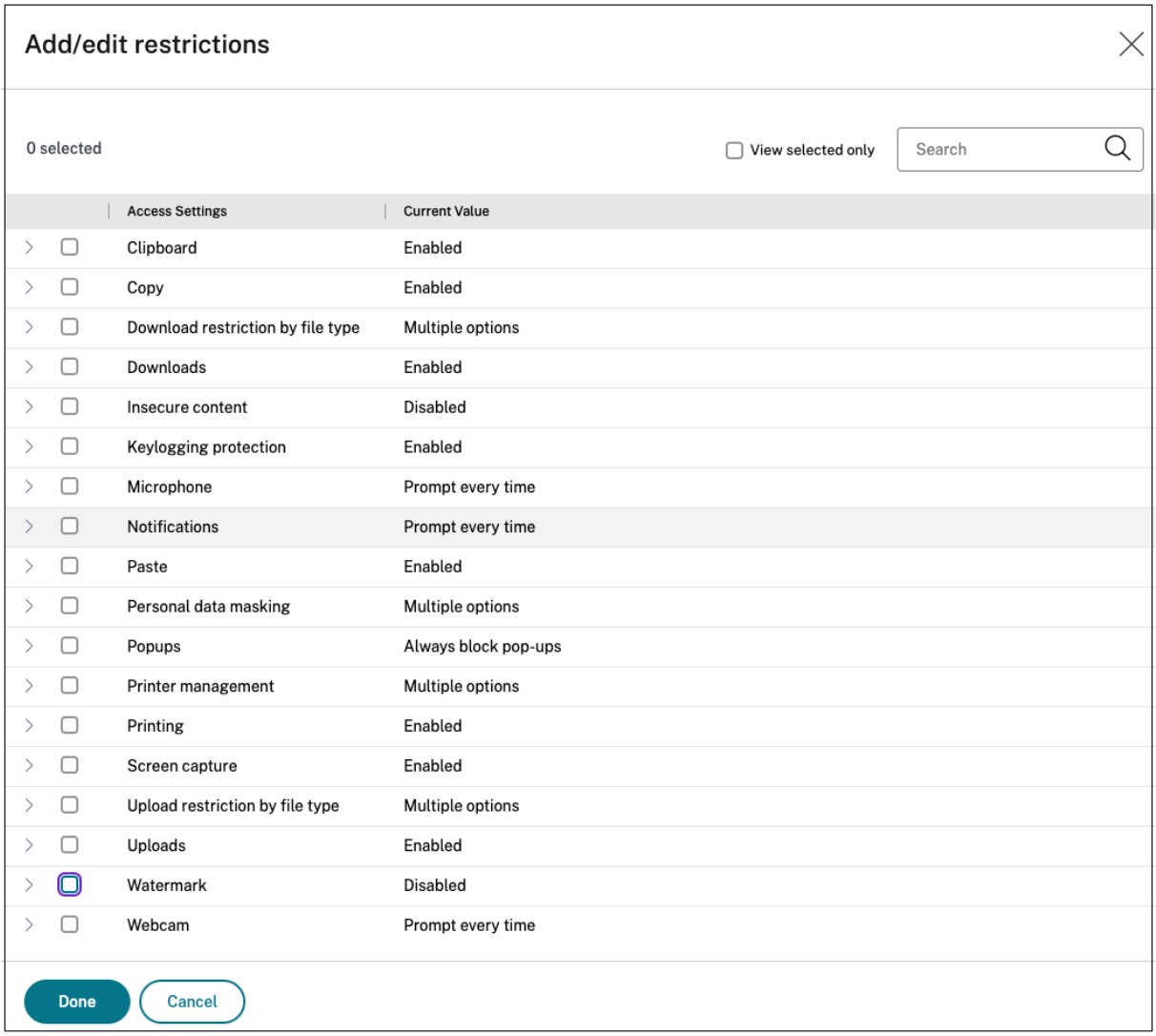
- 对于 TCP/UDP 应用程序，登录到 Citrix Secure Access 客户端，在客户端计算机（Windows 和 macOS）上验证您的配置。

配置验证示例

访问限制选项

October 21, 2024

当您选择操作时 允许访问（有限制），您可以根据需要选择安全限制。这些安全限制在系统中预定义。管理员无法修改或添加其他组合。



剪贴板

通过 Citrix Enterprise Browser 访问时，使用此访问策略在 SaaS 或内部 Web 应用程序上启用/禁用剪切/复制/粘贴操作。默认值：Enabled。

复制

通过 Citrix Enterprise 浏览器访问时，使用此访问策略启用/禁用从 SaaS 或内部 Web 应用程序复制数据。默认值：Enabled。

> 注意：
>
> - 如果两者都 剪贴板 和 复制 限制，则 剪贴板 restriction 优先于 复制 限制。
> - 最终用户必须使用 Citrix Enterprise Browser 版本 126 或更高版本来访问启用了此限制的应用程序。否则，应用程序访问将受到限制。
> - 为了对应用程序内的复制操作进行精细控制，管理员可以使用 安全组 限制。有关详细信息，请参阅 安全组的剪贴板限制.

下载

启用/禁用用户在通过 Citrix Enterprise Browser 访问时，使用此策略从 SaaS 或内部 Web 应用程序下载的能力。默认值：Enabled。

> 注意：
>
> - 如果您已禁用 下载 限制，则最终用户可以在通过 Citrix Enterprise Browser 访问时从应用程序内请求下载访问权限。有关详细信息，请参阅 通过请求下载访问权限.
> - 如果两者都 下载 和 按文件类型划分的下载限制 限制，则 下载 restriction 优先于 按文件类型划分的下载限制.

按文件类型划分的下载限制

启用/禁用用户在通过 Citrix Enterprise Browser 访问时，使用此策略从 SaaS 或内部 Web 应用程序中下载特定 MIME（文件）类型的能力。

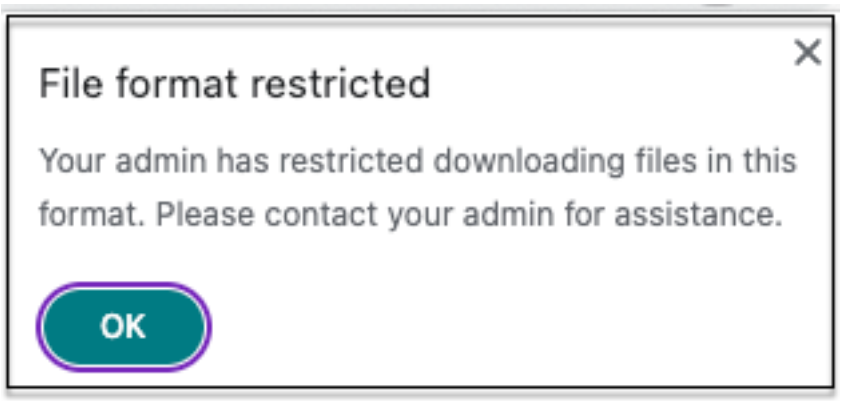
> 注意：
>
> - 这 按文件类型划分的下载限制 除了 下载 限制。
> - 如果两者都 下载 和 按文件类型划分的下载限制 限制，则 下载 restriction 优先于 按文件类型划分的下载限制 限制。
> - 最终用户必须使用 Citrix Enterprise Browser 版本 126 或更高版本来访问启用了此限制的应用程序。否则，应用程序访问将受到限制。

要启用 MIME 类型的下载，请执行以下步骤：

1. 创建或编辑访问策略。有关创建访问策略的详细信息，请参阅 配置访问策略.
2. 在 行动选择 允许但有限制.
3. 点击 按文件类型划分的下载限制，然后单击 编辑.
4. 在 按文件类型设置设置的下载限制 页面上，选择以下选项之一：
   - 允许所有下载，但有例外–选择必须阻止的类型并允许所有其他类型。
   - 阻止所有下载，但有例外–仅选择可以上传的类型并阻止所有其他类型的类型。
5. 如果列表中不存在该文件类型，请执行以下操作：
   a) 点击 添加自定义 **MIME** 类型.
   b) 在 添加 **MIME** 类型中，在格式 类别/子类别<extension>. 例如 图片/png.
   c) 单击完成。

   MIME 类型现在显示在例外列表中。

当最终用户尝试下载受限制的文件类型时，Citrix Enterprise Browser 会显示以下警告消息：



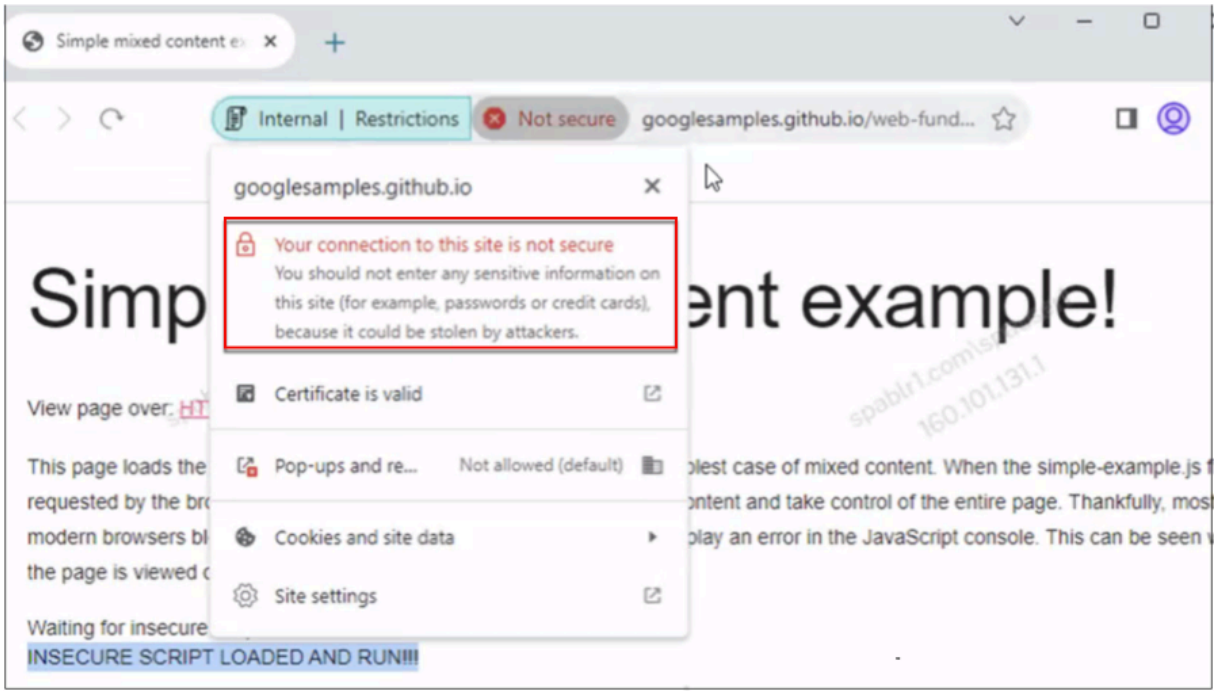
不安全的内容

启用/禁止最终用户在通过 Citrix Enterprise Browser 访问时访问配置了此策略的 SaaS 或内部 Web 应用程序中的不安全内容。不安全内容是指使用 HTTP 链接（而不是 HTTPS 链接）从网页链接到的任何文件。默认值：已禁用.

要启用查看不安全内容，请执行以下步骤：

1. 创建或编辑访问策略。有关创建访问策略的详细信息，请参阅 配置访问策略.
2. 在 行动选择 允许但有限制.
3. 点击 不安全的内容.
4. 点击 救，然后单击 做.

下图显示了访问不安全内容时的示例通知。



键盘记录保护

启用/禁用键盘记录器在通过 Citrix Enterprise Browser 访问时，使用此访问策略从 SaaS 或内部 Web 应用程序捕获击键。默认值：Enabled。

麦克风

通过 Citrix Enterprise Browser 访问麦克风时，提示/不每次都提示用户访问配置了此策略的 SaaS 或内部 Web 应用程序中的麦克风。默认值：每次提示。

最终用户必须使用 Citrix Enterprise Browser 版本 126 或更高版本来访问其中 麦克风 限制已启用。

要每次都允许麦克风而不出现提示，请执行以下步骤：

1. 创建或编辑访问策略。有关详细信息，请参阅 配置访问策略.
2. 在 行动选择 允许但有限制.
3. 点击 麦克风，然后单击 编辑.
4. 在 麦克风设置 页面上，单击 始终允许访问.
5. 点击 救，然后单击 做.

> 注意：
>
> - 如果 麦克风 在 Secure Private Access 策略中启用限制，Citrix Enterprise Browser 将显示设置 允许.

> - 如果选项 每次提示 在 Secure Private Access 策略中，Citrix Enterprise Browser 上应用的设置会有所不同，具体取决于是否使用 Global App Configuration Service（GACS）来管理 Citrix Enterprise Browser。
> - 如果使用 GACS，则 GACS 设置将应用于 Citrix Enterprise Browser。
> - 如果未使用 GACS，则 Citrix Enterprise Browser 将显示该设置 问.
> - 目前，Secure Private Access 不支持阻止麦克风。如果您必须阻止麦克风，则必须通过 GACS 进行。

有关 GACS 的更多信息，请参阅 通过 Global App Configuration Service 管理 Citrix Enterprise Browser.

通知

通过 Citrix Enterprise Browser 访问时，允许/提示用户每次查看配置了此策略的 SaaS 或内部 Web 应用程序中的通知。默认值：每次提示。

最终用户必须使用 Citrix Enterprise Browser 版本 126 或更高版本来访问启用了此限制的应用程序。

要在不提示的情况下阻止显示通知，请执行以下步骤。

1. 创建或编辑访问策略。有关详细信息，请参阅 配置访问策略.
2. 在 行动选择 允许但有限制.
3. 点击 通知，然后单击 编辑.
4. 在 通知设置 页面上，单击 始终阻止通知.
5. 点击 救，然后单击 做.

粘贴

通过 Citrix Enterprise Browser 访问时，使用此访问策略启用/禁用将复制的数据粘贴到 SaaS 或内部 Web 应用程序中。默认值：Enabled。

> 注意：
>
> - 如果两者都 剪贴板 和 糊 限制，则 剪贴板 restriction 优先于 糊 限制。
> - 最终用户必须使用 Citrix Enterprise Browser 版本 126 或更高版本来访问启用了此限制的应用程序。否则，应用程序访问将受到限制。
> - 为了对应用程序内的粘贴操作进行精细控制，管理员可以使用 安全组 限制。有关详细信息，请参阅 安全组的剪贴板限制.

个人数据屏蔽

通过 Citrix Enterprise Browser 访问时，使用此策略在 SaaS 或内部 Web 应用程序上启用/禁用编辑或屏蔽个人身份信息（PII）。

> 注意：
>
> 最终用户必须使用 Citrix Enterprise Browser 版本 126 或更高版本来访问启用了此限制的应用程序。否则，应用程序访问将受到限制。

要隐去或屏蔽个人身份信息，请执行以下步骤：

1. 创建或编辑访问策略。有关详细信息，请参阅 配置访问策略.
2. 在 行动选择 允许但有限制.
3. 点击 个人数据屏蔽，然后单击 编辑.
4. 选择要遮挡或遮罩的信息类型，然后单击 加.

   如果信息类型未显示在预定义列表中，则可以添加自定义信息类型。有关详细信息，请参阅 添加自定义信息类型.
5. 选择遮罩类型。

   - 完全遮罩–完全覆盖敏感信息以使其不可读。
   - 部分遮罩–部分覆盖敏感信息。仅涵盖相关部分，其余部分保持不变。

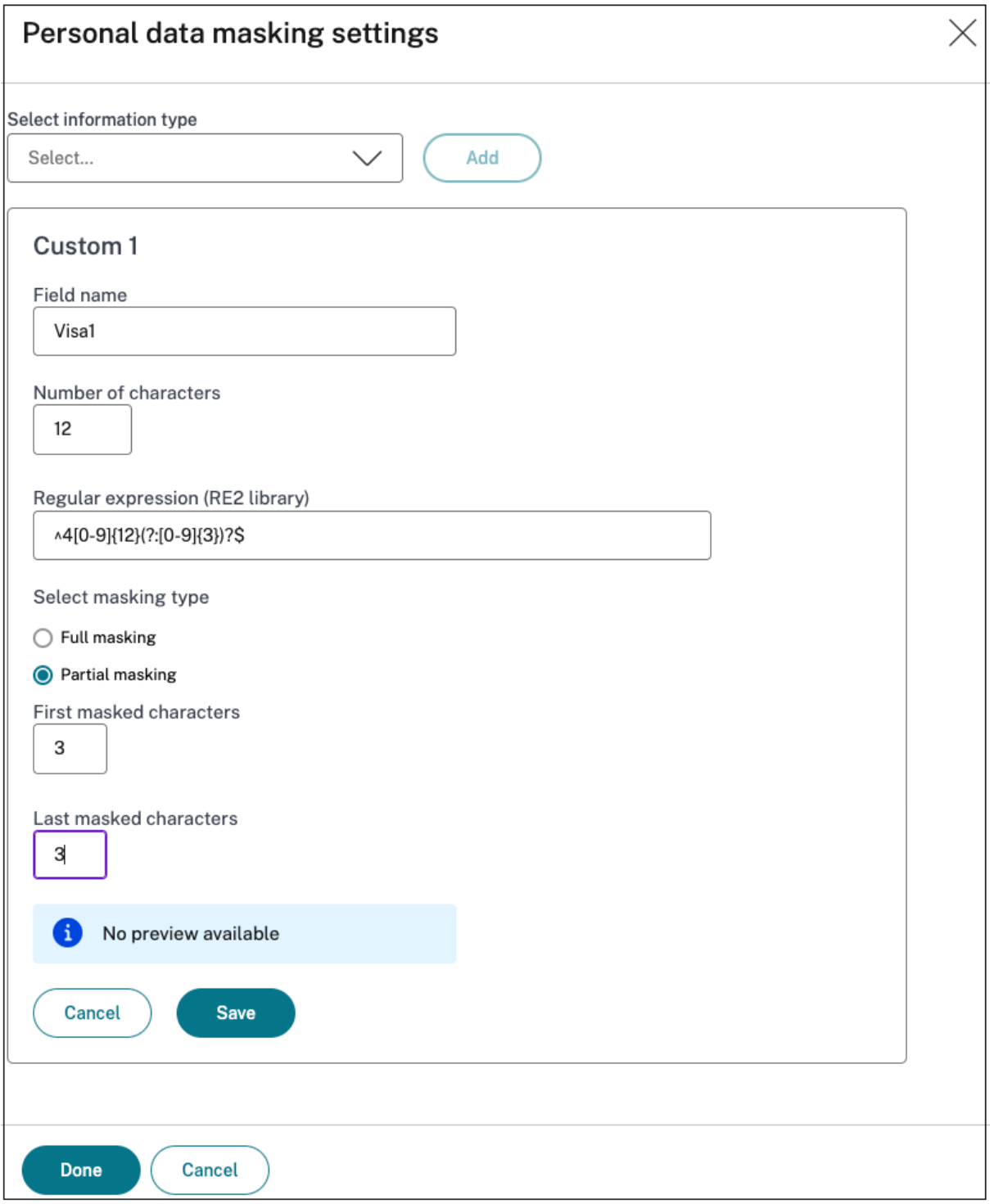
     当您选择 部分标记中，必须选择从文档开头或结尾开始的字符。您必须在 第一个蒙面角色 和 最后一个掩码字符 领域。

     这 预览 字段显示掩码格式。此预览版不适用于自定义策略。
6. 点击 救，然后单击 做.

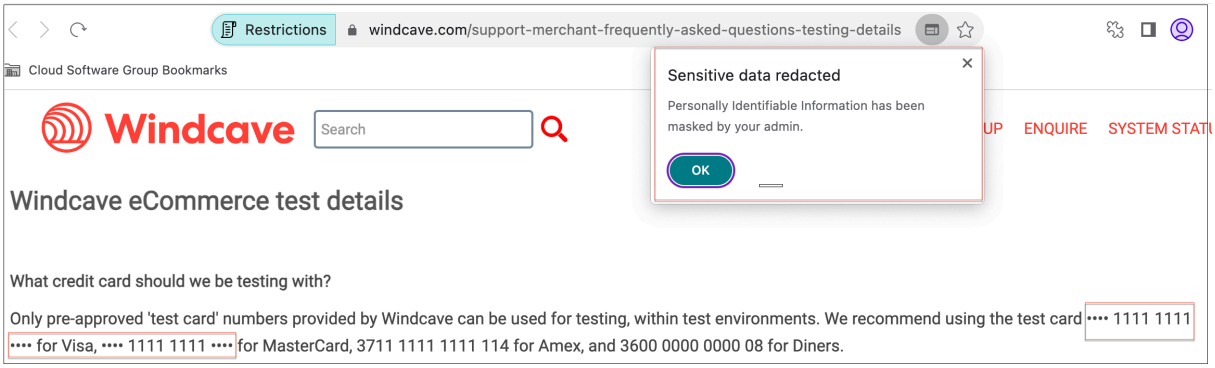
添加自定义信息类型

您可以通过添加信息类型的正则表达式来添加自定义信息类型。

1. 在 选择信息类型选择 习惯，然后单击 加.
2. 在 字段名称中，输入要屏蔽的信息类型的名称。
3. 在 字符数中，输入信息类型的字符数。
4. 在 正则表达式（**RE2** 库）中，输入自定义信息类型的表达式。例如 `^4[0-9]{ 12 } (?:[0-9]{ 3 } )?$`.
5. 如果要遮罩完整信息或前几个或后几个字符，请选择遮罩类型。
6. 点击 救，然后单击 做.



下图显示了一个屏蔽了 PII 的示例应用程序。该图还显示了与 PII 屏蔽相关的通知。



弹出窗口

启用/禁用通过 Citrix Enterprise Browser 访问时，在配置了此策略的 SaaS 或内部 Web 应用程序中显示弹出窗口。默认情况下，网页中的弹出窗口处于禁用状态。默认值：始终阻止弹出窗口。

最终用户必须使用 Citrix Enterprise Browser 版本 126 或更高版本来访问启用了此限制的应用程序。

要启用弹出窗口的显示，请执行以下步骤：

1. 创建或编辑访问策略。有关详细信息，请参阅 配置访问策略.
2. 在 行动选择 允许但有限制.
3. 点击 弹出窗口，然后单击 编辑.
4. 在 弹出窗口设置 页面上，单击 始终允许弹出窗口.
5. 点击 救，然后单击 做.

打印

通过 Citrix Enterprise Browser 访问时，使用此策略启用/禁用从配置的 SaaS 或内部 Web 应用程序打印数据。默认值：Enabled。

当最终用户尝试从启用了打印限制的应用程序打印内容时，将显示以下消息。

> 注意：
>
> - 如果为最终用户禁用了打印选项，则最终用户可以在通过 Citrix Enterprise Browser 访问时从应用程序内请求打印访问权限。有关详细信息，请参阅 根据请求进行打印访问.

> - 如果两者都 印刷 和 打印机管理 限制，则 印刷 restriction 优先于 打印机管理 限制。

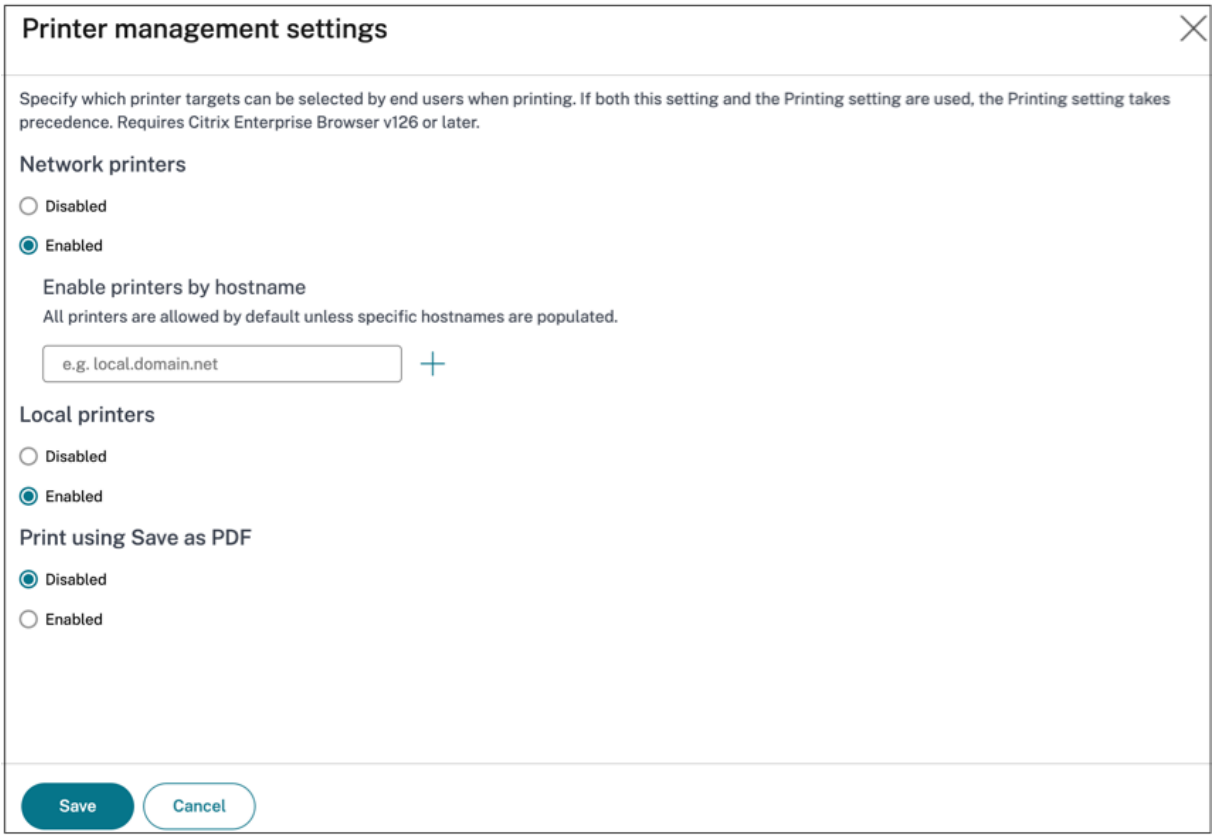
打印机管理

通过 Citrix Enterprise Browser 访问时，使用具有此策略的已配置 SaaS 或内部 Web 应用程序中的管理员配置的打印机启用/禁用打印数据。

> 注意：
>
> - 这 打印机管理 除了 印刷 启用或禁用打印的限制。如果两者都 印刷 和 打印机管理 限制在访问策略中启用时，印刷 restriction 优先于 打印机管理 限制。
> - 最终用户必须使用 Citrix Enterprise Browser 版本 126 或更高版本来访问启用了此限制的应用程序。否则，应用程序访问将受到限制。

要启用/禁用打印限制，请执行以下步骤：

1. 创建或编辑访问策略。有关创建访问策略的详细信息，请参阅 配置访问策略.
2. 在 行动选择 允许但有限制.
3. 点击 打印机管理，然后单击 编辑.



1. 根据您的要求选择例外。

   - 网络打印机 - 网络打印机是可以连接到网络并由多个用户使用的打印机。

  - 禁用：从网络中的任何打印机打印均被禁用。
  - 已启用：允许从所有网络打印机进行打印。如果指定了打印机主机名，则除指定打印机以外的所有其他网络打印机都将被阻止。

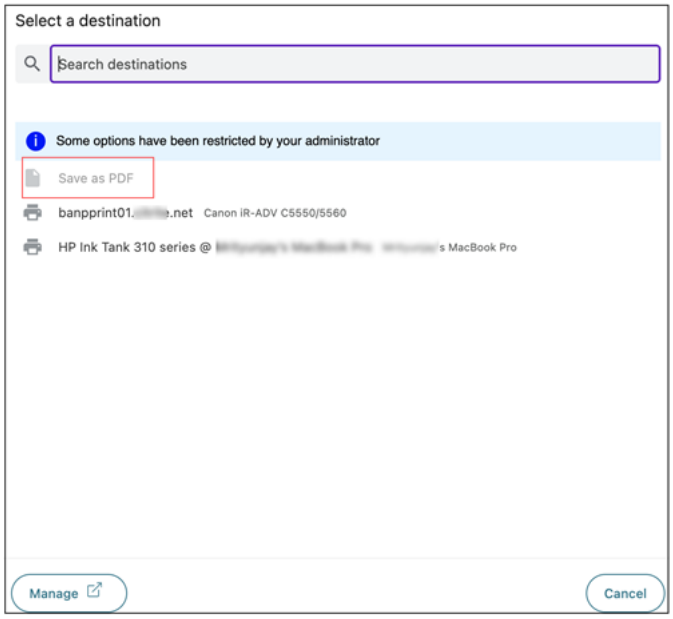
  注意：网络打印机由其主机名标识。

- 本地打印机 - 本地打印机是通过有线连接直接连接到单个计算机的设备。这种连接通常通过 USB、并行端口或其他直接接口来实现。
  - 已禁用：禁用从所有本地打印机进行打印。
  - 已启用：允许从所有本地打印机进行打印。
- 使用“另存为 **PDF**”进行打印
  - 禁用：以 PDF 格式保存应用程序中的内容被禁用。
  - 启用：启用以 PDF 格式保存应用程序中的内容。

2. 单击保存。

如果禁用了网络打印机，则当您尝试在 目的地 田。

此外，如果 使用另存为 **PDF** 进行打印 处于禁用状态，则当您单击 查看更多 链接 目的地 字段、另存为 **PDF** 选项显示为灰色。



屏幕截图

使用任何屏幕捕获程序或应用程序通过 Citrix Enterprise Browser 访问屏幕时，使用此策略启用/禁用从 SaaS 或内部 Web 应用程序捕获屏幕的功能。如果用户尝试捕获屏幕，则会捕获空白屏幕。默认值：Enabled。

按文件类型划分的上载限制

启用/禁用用户在通过 Citrix Enterprise Browser 访问时，使用此策略从 SaaS 或内部 Web 应用程序下载特定 MIME（文件）类型的能力。

> 注意：
>
> - 这 按文件类型划分的上传限制 除了 上传 限制。
> - 如果两者都 上传 和 按文件类型划分的上传限制 限制，则 上传 restriction 优先于 按文件类型划分的上传限制 限制。
> - 最终用户必须使用 Citrix Enterprise Browser 版本 126 或更高版本来访问启用了此限制的应用程序。否则，应用程序访问将受到限制。

要启用/禁用 MIME 类型的上传，请执行以下步骤：

1. 创建或编辑访问策略。有关详细信息，请参阅 创建访问策略.
2. 在 行动选择 允许但有限制.
3. 点击 按文件类型划分的上传限制，然后单击 编辑.
4. 在 按文件类型设置设置的上传限制 页面上，选择以下选项之一：

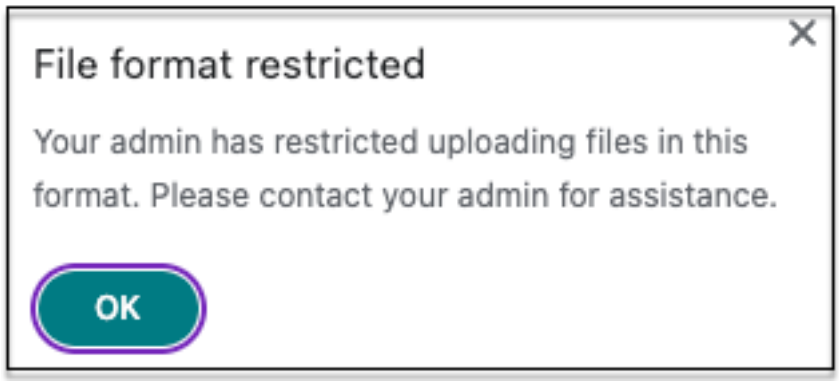
   允许所有上传，但有例外–上传除所选类型之外的所有文件。阻止所有上传，但有例外–阻止上传除所选类型之外的所有文件类型。

5. 如果列表中不存在该文件类型，请执行以下操作：

   a) 点击 添加自定义 **MIME** 类型.
   b) 在 添加 **MIME** 类型中，在格式 类别/子类别<extension>. 例如 图片/png.
   c) 单击完成。

   MIME 类型现在显示在例外列表中。

当最终用户尝试上载受限制的文件类型时，Citrix Enterprise Browser 会显示一条警告消息。



上传

启用/禁用用户在通过 Citrix Enterprise Browser 访问时，在配置了此策略的 SaaS 或内部 Web 应用程序中上传的能力。默认值：Enabled。

> 注意：
>
> 如果两者都 上传 和 按文件类型划分的上传限制 限制，则 上传 restriction 优先于 按文件类型划分的上传限制 限制。

水印

启用/禁用用户屏幕上显示用户计算机的用户名和 IP 地址的水印。默认值：已禁用.

网络摄像机

通过 Citrix Enterprise Browser 访问时，提示/不每次都提示用户访问配置了此策略的 SaaS 或内部 Web 应用程序中的网络摄像头。默认值：每次提示。

最终用户必须使用 Citrix Enterprise Browser 版本 126 或更高版本来访问其中 网络摄像头 限制已启用。

要每次都允许网络摄像头而不提示，请执行以下步骤：

1. 创建或编辑访问策略。有关详细信息，请参阅 配置访问策略.
2. 在 行动选择 允许但有限制.
3. 点击 网络摄像头，然后单击 编辑.
4. 在 网络摄像头设置 页面上，单击 始终允许访问.
5. 点击 救，然后单击 做.

> 注意：
>
> - 如果在 Secure Private Access 策略中启用了网络摄像头限制，则 Citrix Enterprise Browser 将显示设置 允许.
> - 如果选项 每次提示 在 Secure Private Access 策略中，则应用于 Citrix Enterprise Browser 的设置会有所不同，具体取决于是否使用 Global App Configuration Service（GACS）来管理 Citrix Enterprise Browser。
> - 如果使用 GACS，则 GACS 设置将应用于 Citrix Enterprise Browser。
> - 如果未使用 GACS，则 Citrix Enterprise Browser 将显示该设置 问.
> - 目前，Secure Private Access 不支持阻止网络摄像头。如果您必须阻止网络摄像头，则必须通过 GACS 进行。

有关 GACS 的更多信息，请参阅 通过 Global App Configuration Service 管理 Citrix Enterprise Browser.

安全组的剪贴板限制

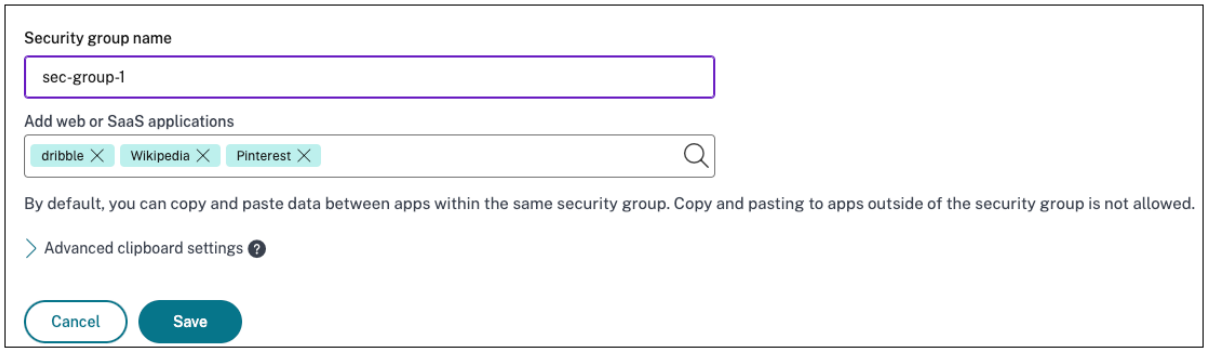
您可以使用 安全组 限制 （应用 **>** 安全组）. 为安全组分配了一组应用程序，可在其中执行复制和粘贴操作。要在安全组的应用程序内启用剪贴板访问，您必须只使用操作配置访问策略 允许 或 允许（有限制）而不选择任何访问设置。

- 当 安全组 限制，则无法在不同安全组中的应用程序之间复制/粘贴数据。例如，如果应用程序“ProdDocs”属于安全组“SG1”，应用程序“Edocs”属于安全组“SG2”，则即使 复制 / 糊 为两个组启用限制。
- 对于不属于安全组的应用程序，您可以使用 action 创建访问策略 允许（有限制）并选择限制（复制, 糊或 剪贴板). 在这种情况下，应用程序不是安全组的一部分，因此 复制 / 糊 限制可以应用于该应用程序。

> 注意：
>
> 您还可以通过 Global App Configuration Service （GACS）限制通过 Citrix Enterprise Browser 访问的应用程序的剪贴板访问。如果您使用 GACS 管理 Citrix Enterprise Browser，请使用 启用沙盒剪贴板 用于管理剪贴板访问权限的选项。当您通过 GACS 限制剪贴板访问时，它将应用于通过 Citrix Enterprise Browser 访问的所有应用程序。有关 GACS 的更多信息，请参阅 通过 Global App Configuration Service 管理 Citrix Enterprise Browser.

要创建安全组，请执行以下步骤：

1. 在 Secure Private Access 控制台中，单击 应用，然后单击 安全组.
2. 点击 添加新的安全组.

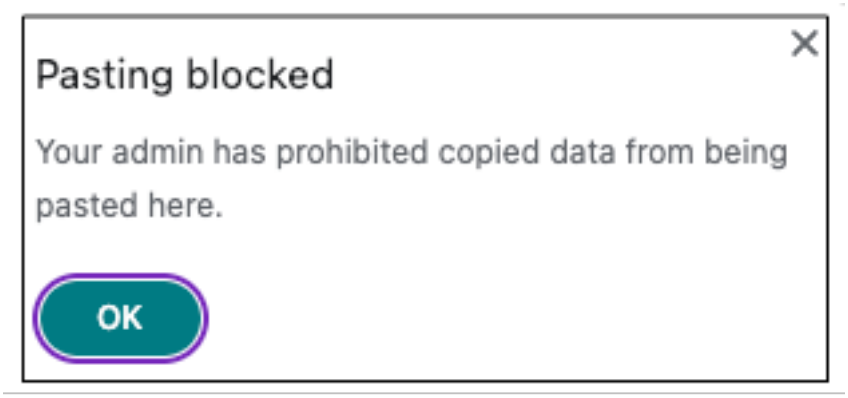


1. 输入安全组的名称。
2. 在 添加 **Web** 或 **SaaS** 应用程序，选择要分组以启用 COPY and PASTE 控件的应用程序。例如，Wikipedia、Pinterest 和 Dribble。
3. 单击保存。

有关高级剪贴板设置的详细信息，请参阅 为本机应用程序和未发布的应用程序启用复制/粘贴控件.

当最终用户从 Citrix Workspace 启动这些应用程序（Wikipedia、Pinterest 和 Dribble）时，他们必须能够将数据从一个应用程序共享（复制/粘贴）到安全组内的其他应用程序。复制/粘贴的发生与已为应用程序启用的其他安全限制无关。

但是，最终用户无法将内容从其计算机上的本地应用程序或未发布的应用程序复制并粘贴到这些指定的应用程序，反之亦然。将内容从指定的应用程序复制到另一个应用程序时，将显示以下通知：



> 注意：
>
> 您可以使用以下选项从用户计算机上的本地应用程序或未发布的应用程序控件中复制/粘贴内容 高级剪贴板设置部分。有关详细信息，请参阅 为本机应用程序和未发布的应用程序启用复制/粘贴控件.

启用粒度级别的复制/粘贴

您可以在指定组中的应用程序内启用精细级别的剪贴板访问。为此，您可以为应用程序创建访问策略并启用 复制 / 糊 根据您的要求进行限制。

> 注意：
>
> 确保您为精细级别剪贴板访问创建的特定访问策略的优先级高于您为安全组创建的策略。

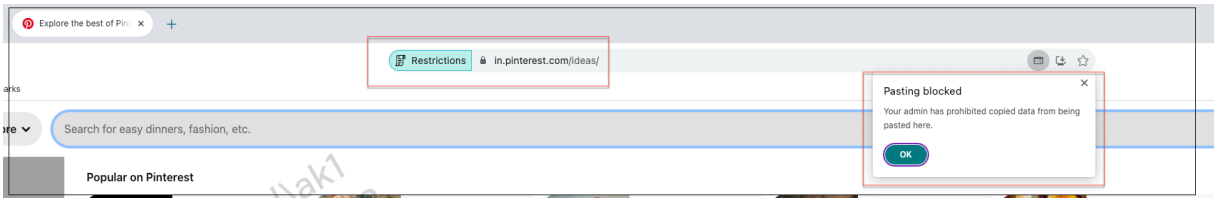
示例：

假设您创建了一个包含三个应用程序（即 Wikipedia、Pinterest 和 Dribble）的安全组。

现在，您想要限制将 Wikipedia 或 Dribble 中的内容粘贴到 Pinterest 中。为此，请执行以下步骤：

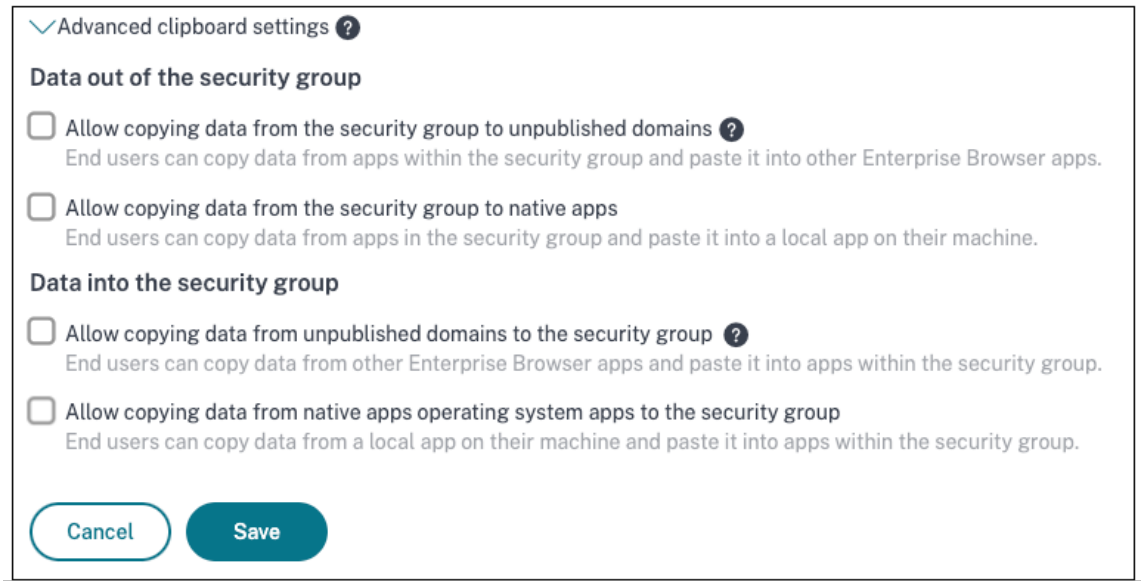
1. 创建或编辑为应用程序分配的访问策略 `Pinterest 公司`. 有关创建访问策略的详细信息，请参阅 配置访问策略.
2. 在 行动选择 允许但有限制.
3. 选择 糊.

尽管 Pinterest 是安全组的一部分，该安全组还包含 Wikipedia 和 Dribble，但用户无法将 Wikipedia 或 Dribble 中的内容复制到 Pinterest，因为与 Pinterest 相关的访问策略中，糊 限制已启用。



为本机应用程序和未发布的应用程序启用复制/粘贴控件

1. 创建安全组。有关详细信息，请参阅 复制和粘贴限制的剪贴板安全组.
2. 扩大 高级剪贴板设置.



3. 根据您的要求选择以下选项：
   - 允许将数据从安全组复制到未发布的域—允许将数据从安全组中的应用程序复制到未在 Secure Private Access 中发布的应用程序。
   - 允许将数据从安全组复制到本机应用程序 - 允许将数据从安全组中的应用程序复制到计算机上的本地应用程序。
   - 允许将数据从未发布的域复制到安全组–允许将未通过 Secure Private Access 发布的应用程序中的数据复制到安全组中的应用程序。
   - 允许从本机应用程序操作系统安全组复制数据 - 支持将数据从计算机上的本地应用程序复制到应用程序。

已知问题

- （设置 > 应用领域）保留已删除应用程序的域。因此，这些应用程序也被视为 Secure Private Access 中的已发布应用程序。如果直接从 Citrix Enterprise Browser 访问这些域，则无论您在中选择的选项如何，都将从这些应用程序中禁用复制/粘贴 高级剪贴板设置.

  例如，假设以下场景：

  – 您删除了名为 Jira2 （`https://test.citrite.net`），该安全组的一部分。
  – 您已启用该选项 允许将数据从安全组复制到未发布的域.

  在这种情况下，如果用户尝试将数据从此应用程序复制到同一安全组中的另一个应用程序，则粘贴控制将被禁用。将向用户显示有关相同的通知。

- 对于 SaaS 应用程序，如果应用程序配置了具有操作的访问策略，则可以拒绝应用程序访问 拒绝访问。最终用户仍然可以访问该应用程序，因为应用程序流量未通过 Secure Private Access 进行隧道传输。此外，如果应用程序是安全组的一部分，则不支持安全组设置，因此您无法从应用程序中复制/粘贴内容。

最终用户流程

August 26, 2024

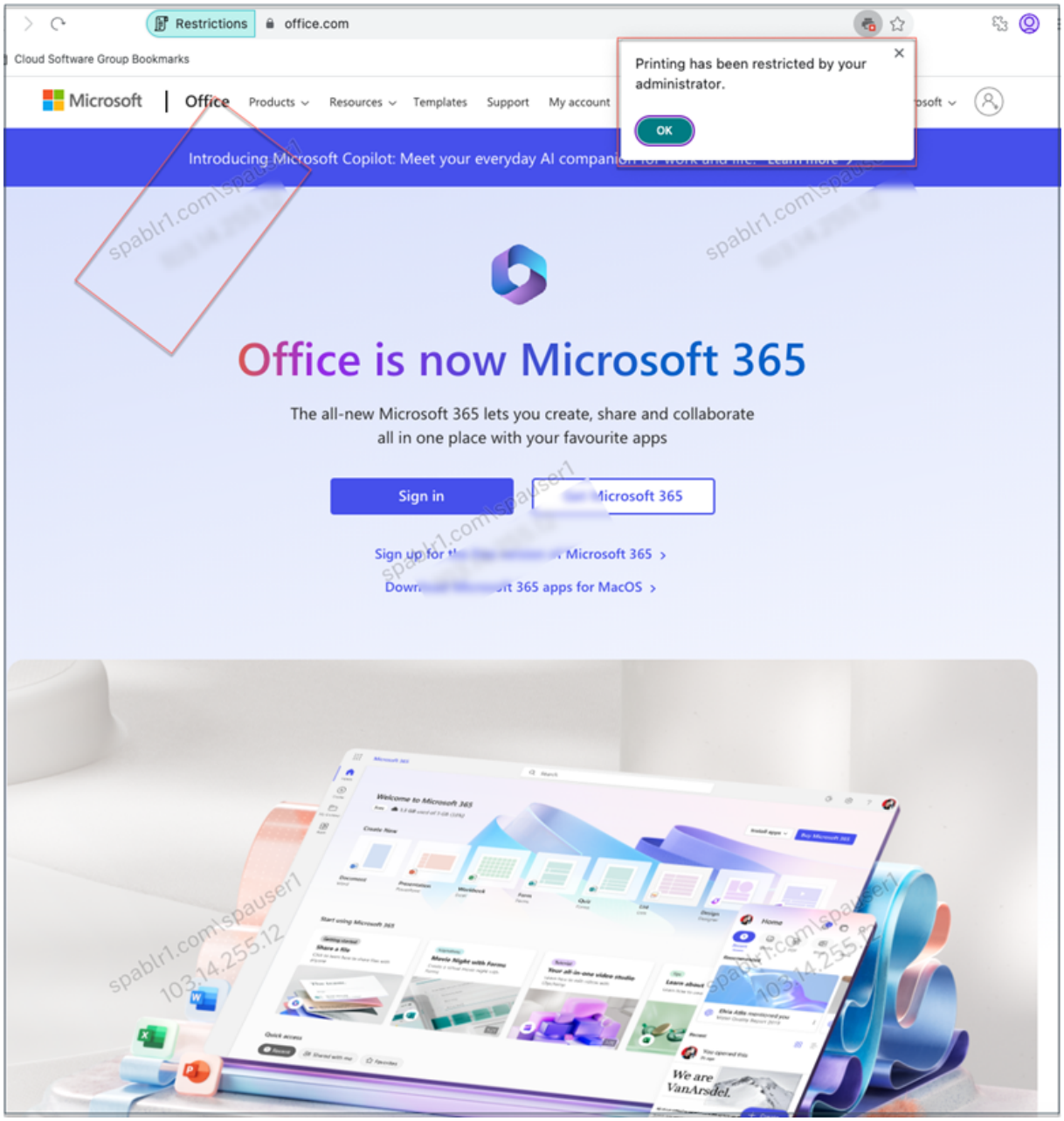
SaaS 应用程序

假设管理员已为 Office365 应用程序配置了针对最终用户的水印和打印限制。现在，当最终用户访问 Office365 应用程序时，必须对该应用程序应用水印和打印限制。

最终用户必须执行以下步骤才能访问 Office365 应用程序：

1. 通过 Citrix Workspace 应用程序访问 StoreFront 应用商店。
2. 登录应用商店。
3. 单击“应用程序”选项卡，然后单击 **Office365** 应用程序。

   最终用户现在必须注意到 Office365 应用程序已启动并包含水印。此外，如果最终用户尝试从 Office365 应用程序打印某些数据，则必须向用户显示打印限制消息。



注意：

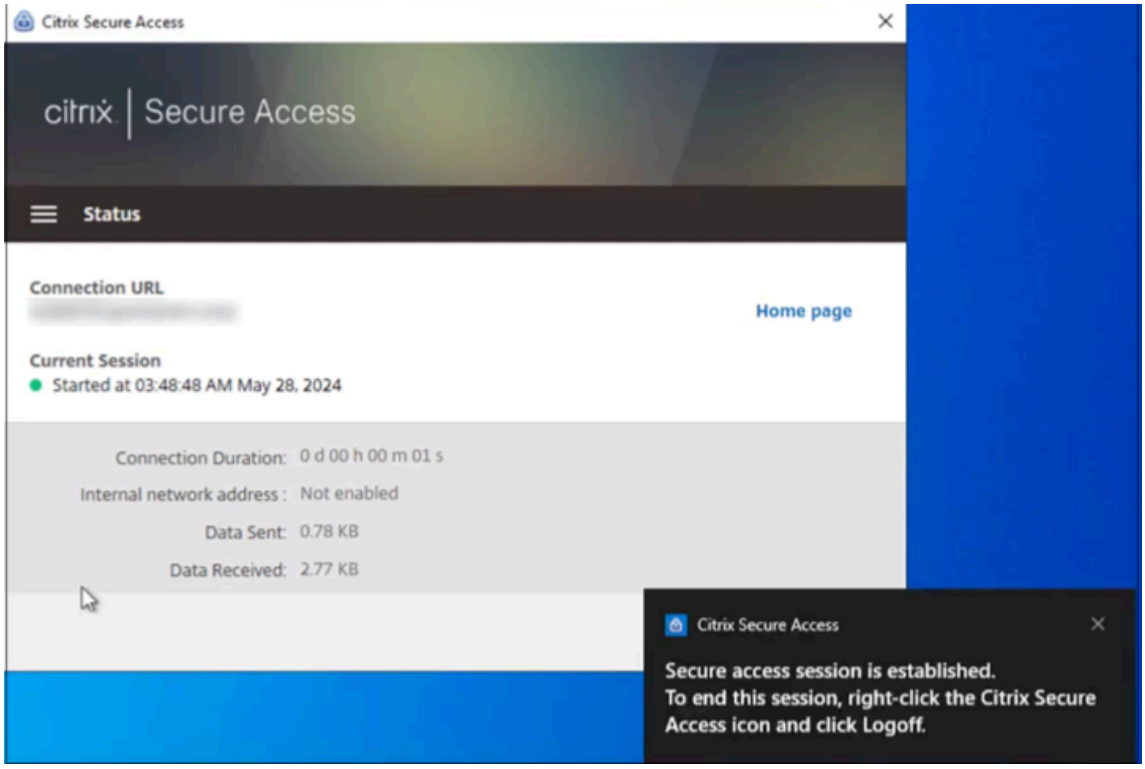
管理员必须向用户提供他们访问虚拟桌面和应用程序所需的帐户信息。有关详细信息，请参阅向 Citrix Workspace 应用程序添加应用商店 URL。

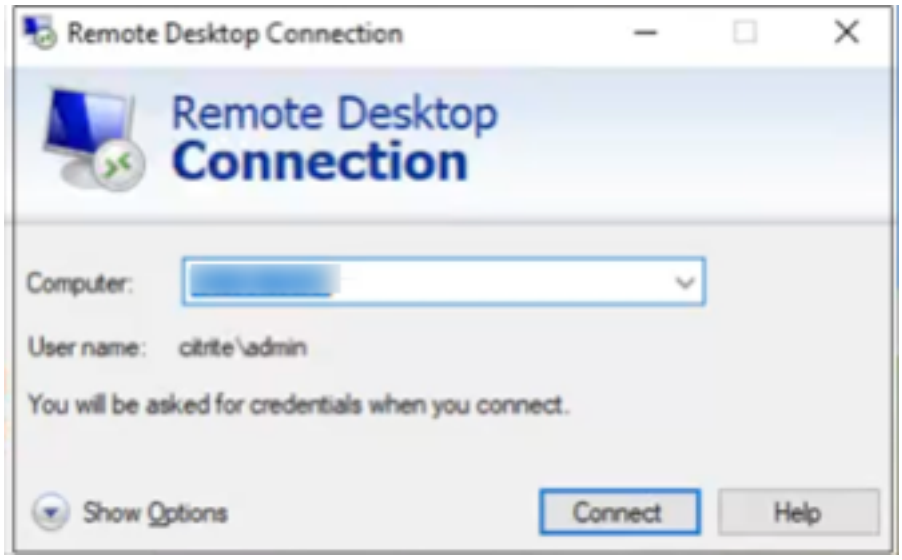
TCP/UDP 应用程序

如果配置了 RDP，则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 Citrix Secure Access 客户端。

2. 建立安全访问会话后，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”。

现在已建立远程桌面连接，最终用户可以与远程计算机进行交互。

升级

October 21, 2024

您可以将 Secure Private Access 部署升级到较新版本，而无需先设置新计算机或站点。在升级之前，我们建议您创建快照或保存配置。要开始升级，请从新版本运行安装程序，以升级以前安装的 Secure Private Access 插件。

升级顺序

升级顺序如下：

1. 您可以根据最初安装 Secure Private Access 的方式，通过 Delivery Controller 或安装程序 UI 中的专用 Secure Private Access 磁贴升级 Secure Private Access。
    - 如果您已通过 Delivery Controller 安装了 Secure Private Access，则无法单独升级 Secure Private Access 组件。相反，您必须升级所有组件。有关详细信息，请参阅 升级部署.
    - 如果您已通过专用的 Secure Private Access 磁贴安装了 Secure Private Access，则可以单独升级它。有关详细信息，请参阅 升级 Secure Private Access 安装程序.

> 注意：
>
> 我们建议您通过 Delivery Controller 为 POC 环境安装 Secure Private Access，但是，对于生产环境，我们建议您使用专用安装程序，以便调整新特性或功能。

1. 运行数据库脚本。有关详细信息，请参阅 使用脚本升级数据库.
2. 重新启动 默认网站 和 **Citrix Access Security** 管理员站点 在 **Internet** 信息服务（**IIS**）管理器 控制台以应用更改。
3. 再次运行 StoreFront 配置。从 下载 StoreFront 脚本 设置 **>** 配置，然后在相应的 StoreFront 计算机上运行脚本。有关详细信息，请参阅 修改集成设置.

> 注意：
>
> 如果不运行脚本，则不会触发终端节点。

1. （可选）运行 NetScaler Gateway 脚本。有关详细信息，请参阅 NetScaler 网关.

组件升级

有关升级 Secure Private Access 本地部署中涉及的组件的信息，请参阅以下主题。

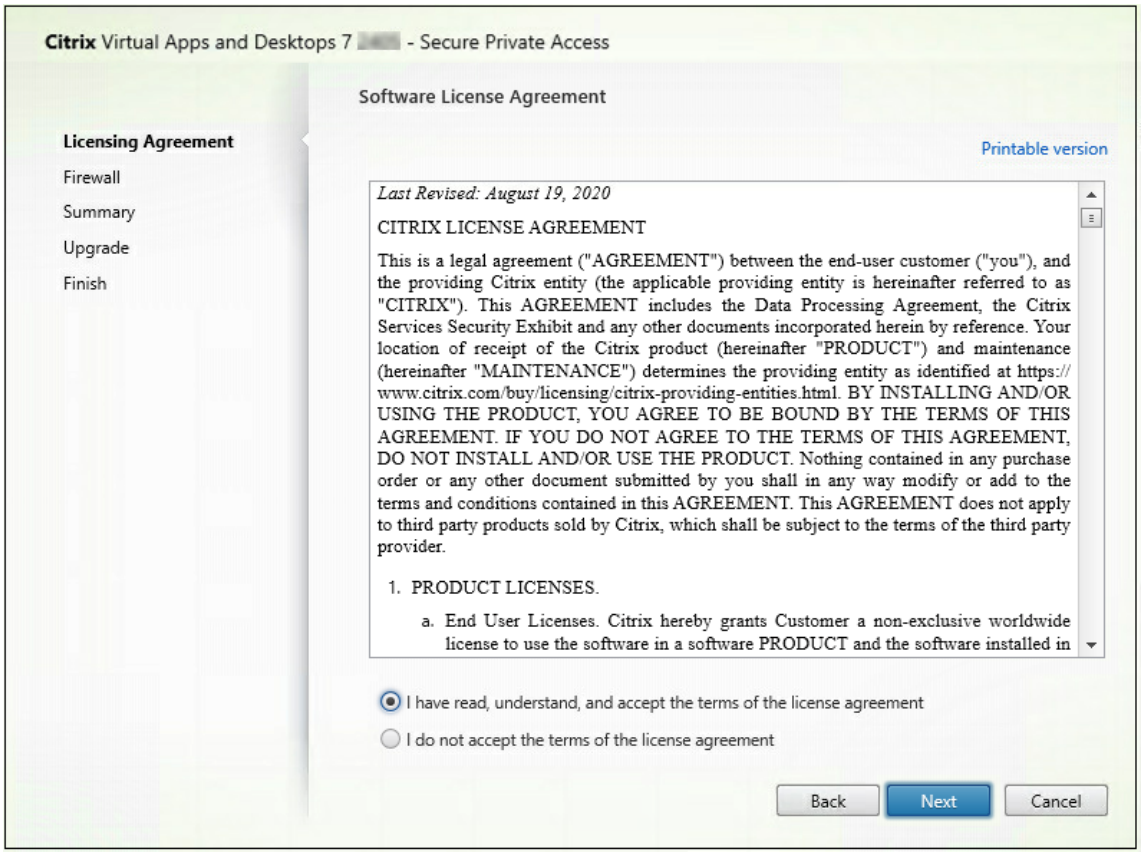
- Cloud Connector
- StoreFront
- NetScaler Gateway

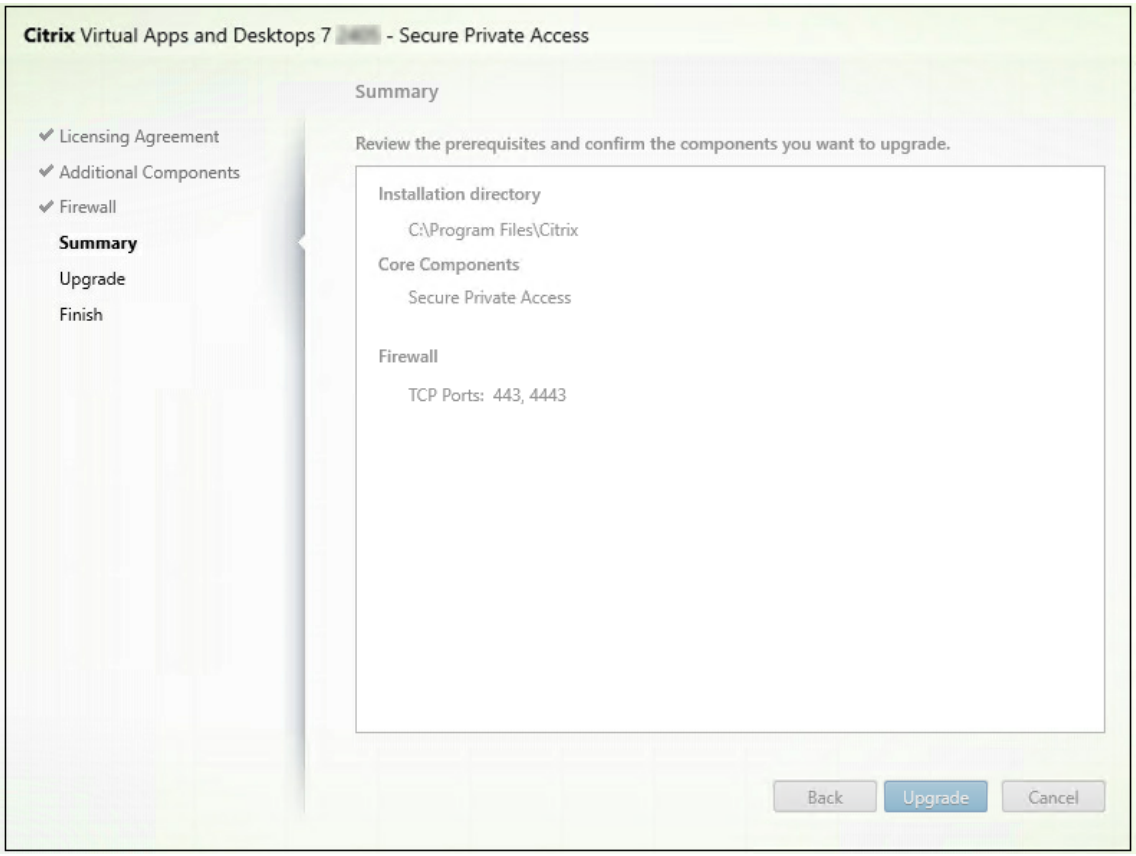
- 许可证服务器
- Web Studio
- Director

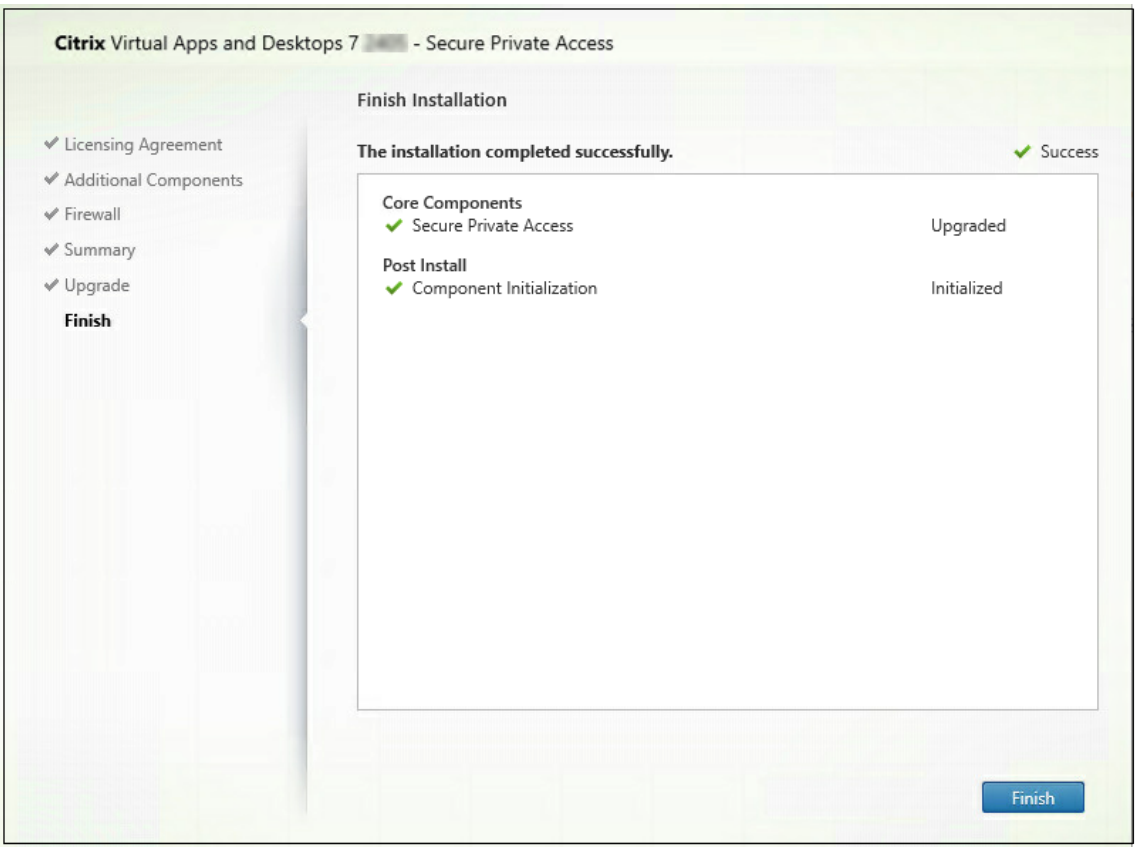
升级 **Secure Private Access** 安装程序

October 21, 2024

1. 从 https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/.
2. 在已加入域的计算机上以管理员身份运行.exe。
3. 按照屏幕上的说明完成安装。







> 重要提示：
>
> 升级安装程序以发布最新版本后，必须重新运行 StoreFront 脚本，以便新的端点详细信息可用。

后续步骤

- 设置安全私人访问
- 配置 NetScaler Gateway
- 配置应用程序
- 为应用程序配置访问策略

使用脚本升级数据库

January 9, 2024

您可以使用管理员配置工具下载 Secure Private Access 插件的数据库升级脚本。

1. 使用管理员权限打开 PowerShell 或命令提示符窗口。
2. 将目录更改为 Secure Private Access 安装文件夹下的 Admin\AdminConfigTool 文件夹（例如，cd “C:\Program Files\Citrix\Citrix Access Security\Admin\AdminConfigTool”）。
3. 请运行以下命令：

   ```
   .\AdminConfigTool.exe /DOWNLOAD_UPGRADE_DB_SCRIPTS <output folder>
   ```

管理配置

October 21, 2024

安装 Secure Private Access 后，您可以从 设置 页。您可以管理应用程序域、管理员的路由，并修改集成设置。

要修改设置，您必须使用 Secure Private Access 管理员帐户登录 Secure Private Access 管理控制台。

有关如何更新或修改设置的详细信息，请参阅以下主题：

- 管理应用程序域的路由
- 管理管理员
- 修改集成设置

管理未经批准的网站

您还可以为未批准的网站配置规则。未在 Secure Private Access 中配置的应用程序（Intranet 或 Internet）被视为“未经批准的网站”。有关详细信息，请参阅 未经批准的网站.

策略建模工具

策略建模工具提供对应用程序访问结果的可见性（允许或允许但有限制或被拒绝）。管理员可以查看特定用户的访问结果和用户条件。有关详细信息，请参阅 策略建模工具.

未经批准的 **Web** 站点

August 26, 2024

未在 Secure Private Access 中配置的应用程序（内联网或 Internet）被视为“未经批准的 Web 站点”。默认情况下，如果没有为所有内联网 Web 应用程序配置应用程序和访问策略，Secure Private Access 会拒绝访问这些应用程序。

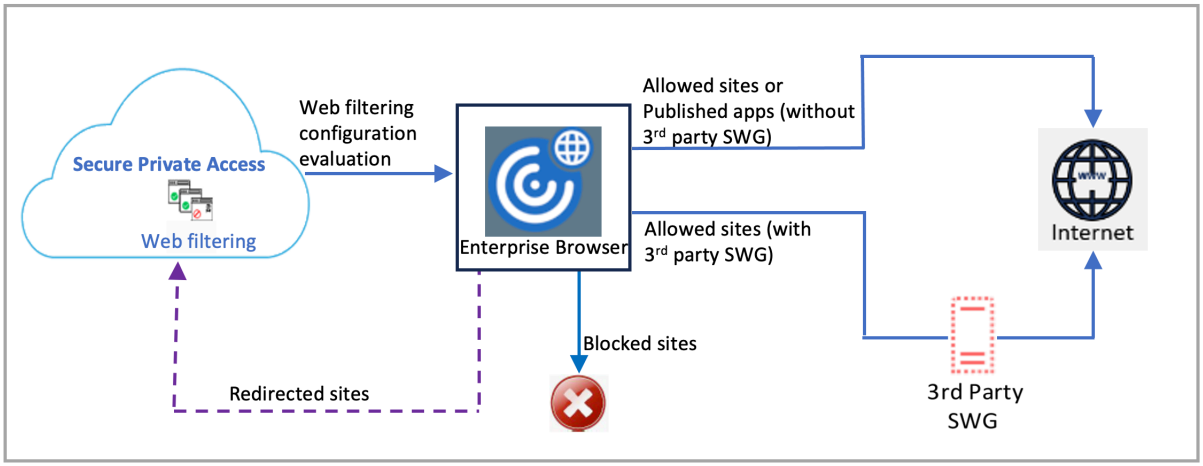
对于所有其他未配置应用程序的 Internet URL 或 SaaS 应用程序，管理员可以使用管理控制台中的设置 **>** 未经批准的 **Web** 站点选项卡，允许或拒绝通过 Citrix Enterprise Browser 进行访问。

> 注意：
>
> 默认情况下，设置配置为允许通过 Citrix Enterprise Browser 访问所有 Internet URL 或 SaaS 应用程序。

未经批准的 **Web** 站点是如何运作的

1. 完成 URL 分析检查以确定该 URL 是否为 Citrix 服务 URL。
2. 然后检查该 URL 以确定它是企业 Web 应用程序 URL 还是 SaaS 应用程序 URL。
3. 然后检查该 URL 以确定它是否被识别为被屏蔽的 URL 或者是否允许访问该 URL。

下图说明了最终用户流量。



当请求到达时，将执行以下检查并采取相应的操作：

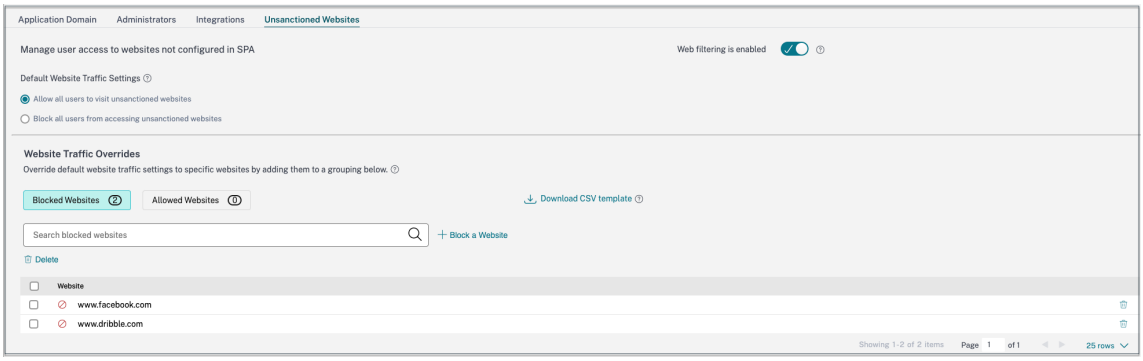
1. 请求是否与全局允许列表匹配?
   a) 如果匹配，则用户可以访问请求的网站。
   b) 如果不匹配，则检查网站列表。
2. 请求是否与配置的网站列表匹配?
   a) 如果匹配，则以下顺序确定操作。
      i. 阻止
      ii. 允许
   b) 如果不匹配，则应用默认操作 (ALLOW)。无法更改默认操作。

为未经批准的 **Web** 站点配置规则

1. 在 Secure Private Access 管理员控制台中，单击“设置” > “未经批准的 **Web** 站点”。

   注意：

   - 默认情况下，网络过滤功能处于启用状态，允许访问所有未经批准的 Internet URL。
   - 您可以将设置更改为阻止所有用户访问未经批准的 **Web** 站点，以阻止所有用户通过 Citrix Enterprise Browser 访问任何 Internet URL。



您还可以通过将特定 URL 添加到被封锁的网站或允许的网站来更改特定 URL 的设置。

例如，如果您在默认情况下封锁了对所有未经批准的 URL 的访问权限，并且只想允许访问几个特定的 Internet URL，则可以通过执行以下步骤来实现：

a) 单击“允许的网站”选项卡，然后单击“允许使用网站”。

b) 添加必须允许访问的网站地址。您可以手动添加网站地址，也可以拖放包含该网站地址的 CSV 文件。

c) 单击“添加 **URL**”，然后单击“保存”。

该 URL 将添加到允许的网站列表中。

安装后管理设置

October 21, 2024

管理应用程序域的路由

您可以查看在安全私人访问设置中添加的应用程序域列表。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. 如果需要，您可以单击编辑图标并更改路由类型。

管理管理员

您可以查看管理员列表，也可以从 设置 **>** 管理员 页面添加管理员。首次安装安全私人访问的管理员被授予完全权限。然后，该管理员可以将其他管理员添加到设置中。

您还可以添加管理员组，以便该组中的所有管理员都可以访问。

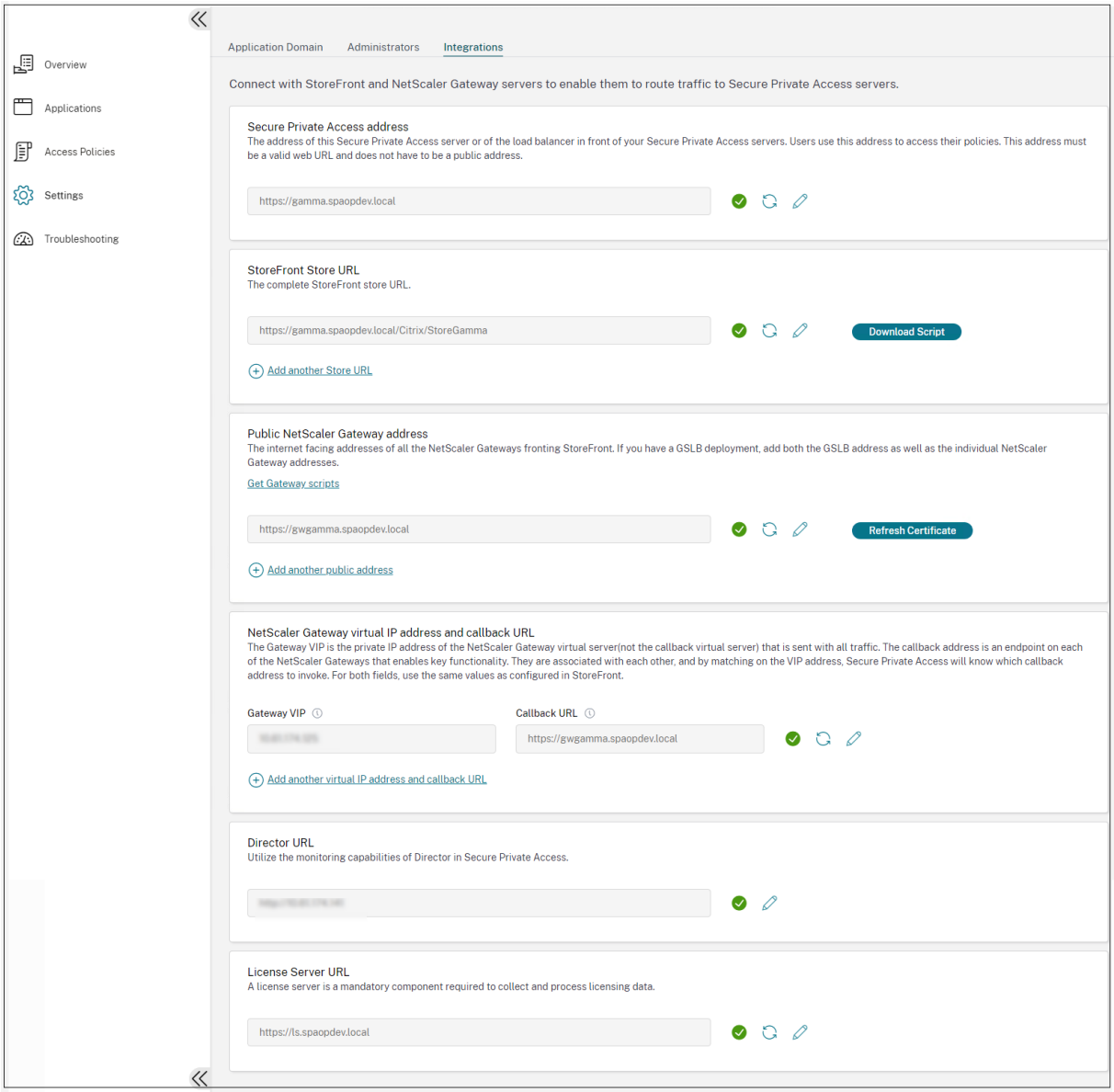
1. 在 管理员 页面中，单击 添加。
2. 在 域中，选择必须添加该管理员的域。
3. 在 用户或用户组中，选择该用户所属的用户或组。
4. 在 管理类型中，选择必须分配给该用户的权限类型。

修改集成设置

设置安全私有访问后，您可以从 集成 选项卡修改或更新 StoreFront 和 NetScaler Gateway 条目。

1. 单击 设置 **>** 集成。
2. 单击与您想要修改的设置相符的编辑图标并更新条目。
3. 单击刷新图标以确保设置有效。

> 注意：
>
> - 如果安全私有访问地址发生更改，则下载 StoreFront 脚本并在 StoreFront 主机上运行它。
> - 如果 Secure Private Access 安装在与 StoreFront 不同的机器上，则下载 StoreFront 脚本并在 StoreFront 上运行它。



管理应用程序和策略

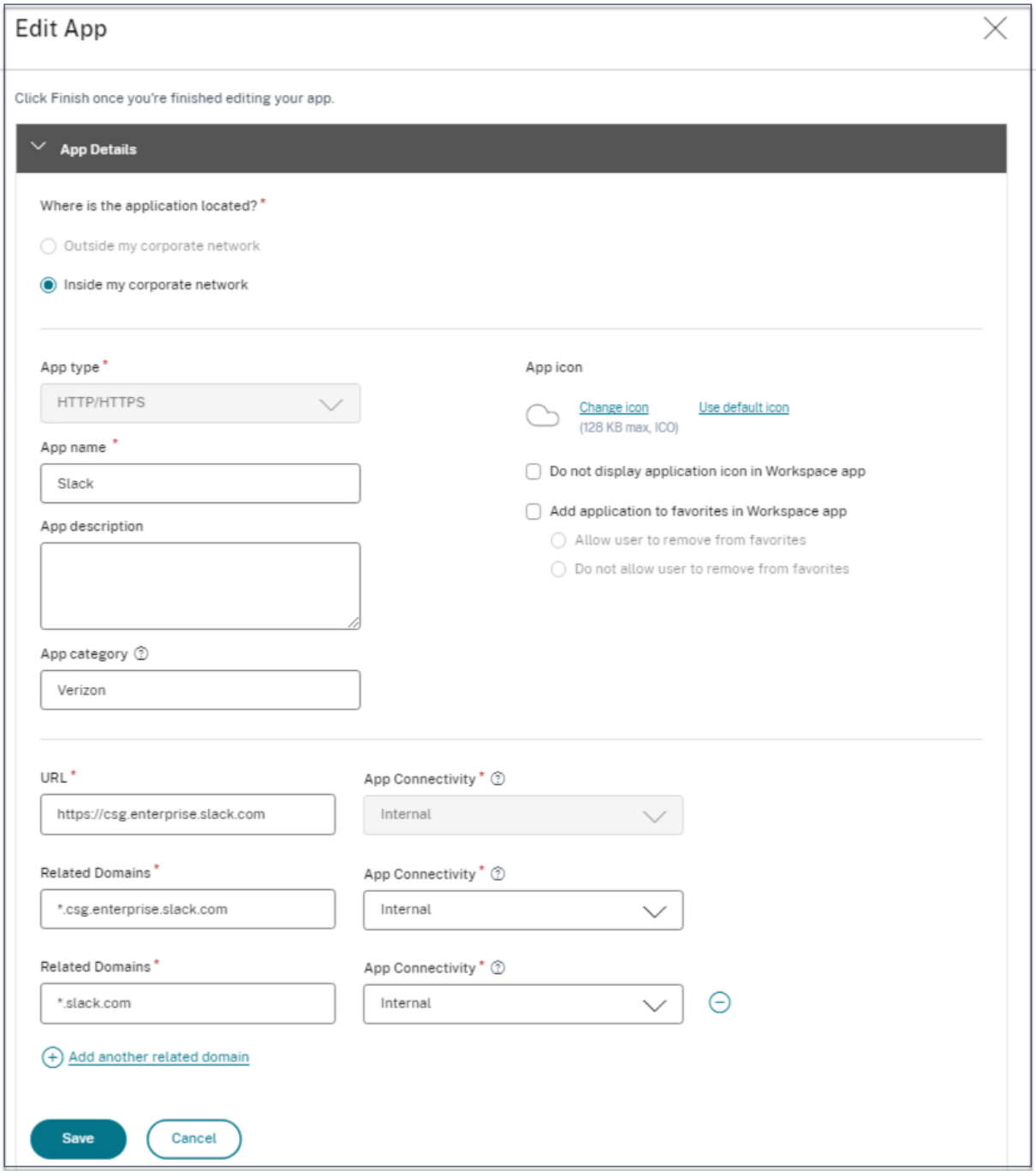
June 19, 2024

配置应用程序和访问策略后，如有必要，您可以对其进行编辑。

编辑应用程序

1. 在 Secure Private Access 管理员控制台中，单击“应用程序”。

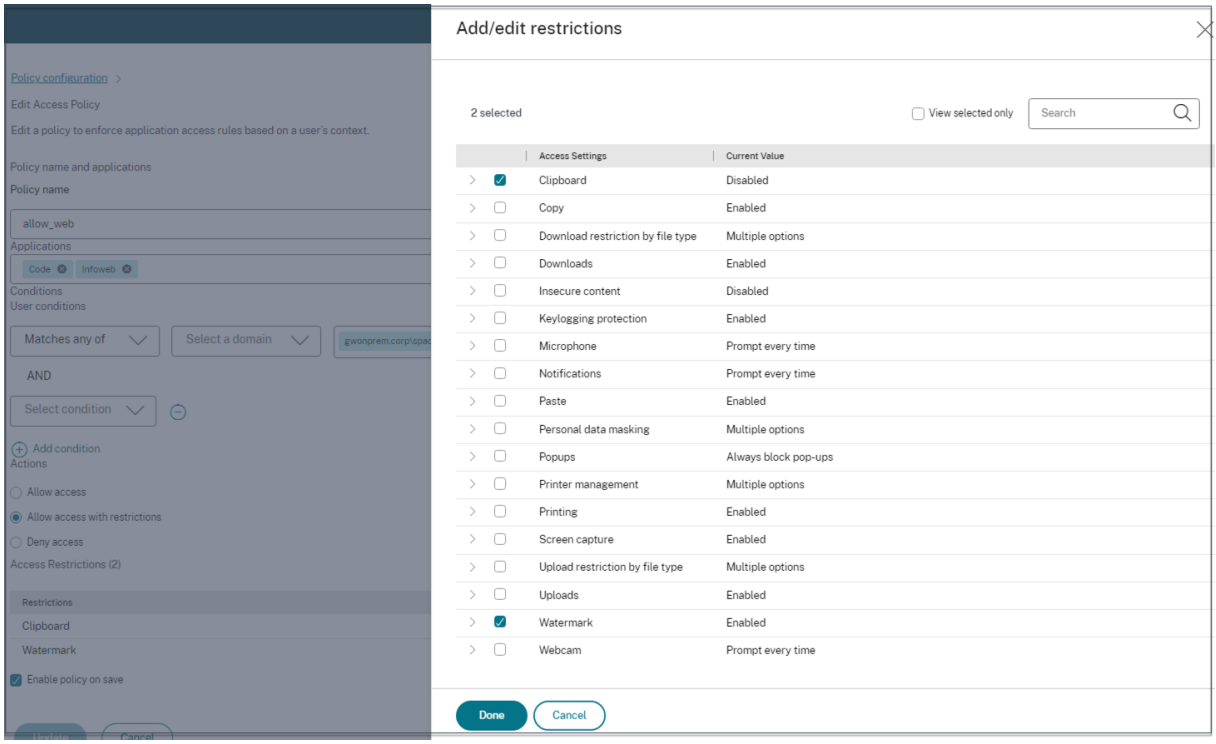
2. 单击与要修改的应用程序对应的省略号按钮，然后单击“编辑应用程序”。
3. 编辑应用程序的详细信息。
4. 单击保存。



编辑访问策略

1. 在“Secure Private Access”管理员控制台中，单击“访问策略”。

2. 单击与要修改的策略对应的省略号按钮，然后单击“编辑访问策略”。
3. 编辑策略详情。
4. 单击更新。



卸载 **Secure Private Access**

October 21, 2024

您可以从 控制面板 **>** 程序 **>** 程序和功能.

1. 选择 **Citrix Virtual Apps and Desktops 7 2408 —Secure Private Access**.
2. 点击 卸载.
3. 按照屏幕上的说明完成卸载。

> 注意：
>
> 如果 Secure Private Access 安装后设置已完成，则在卸载 Secure Private Access 之前，请从 Admin Console 下载 StoreFrontScripts.zip 文件，以从 StoreFront 应用商店配置中删除 Secure Private Access 插件。

要下载 StoreFrontScripts zip 文件，请执行以下步骤：

1. 登录到 Secure Private Access 管理控制台。

2. 点击 设置，然后单击 集成 标签。
3. 点击 下载脚本 在 StoreFront Store URL 部分中。

从 **StoreFront** 应用商店配置中删除 **Secure Private Access** 插件

卸载 Secure Private Access 后，必须从 StoreFront 应用商店配置中删除 Secure Private Access 插件。

1. 登录到 StoreFront 计算机。
2. 下载 StoreFrontScripts.zip 文件。
3. 将 StoreFrontScripts.zip 解压缩到一个文件夹中。
4. 使用 admin 权限打开 PowerShell 窗口。
5. 运行以下命令：

```
cd <unzipped folder> .\RemoveStorefrontConfiguration.ps1
```

监视和故障排除

August 26, 2024

Secure Private Access 故障排除控制板显示与应用程序启动、应用程序枚举及其状态相关的日志。有关详细信息，请参阅控制板概述。

故障排除

在设置 Secure Private Access 时或之后，您可能会遇到与以下相关的问题：

- 证书错误
- 数据库创建错误
- StoreFront 故障
- 公共网关/回调网关故障
- 无法访问 Secure Private Access 服务器

有关修复这些问题的详细信息，请参阅基本故障排除。

Director 中的会话相关代码

Director 与 Secure Private Access 的集成可实现有效的性能监视和故障排除，因为 Secure Private Access 设置中所有组件的问题都会在 Director 中捕获。建议您通过检查日志来解决故障或异常问题。如果仍无法解决问题，请联系支持人员。

引用

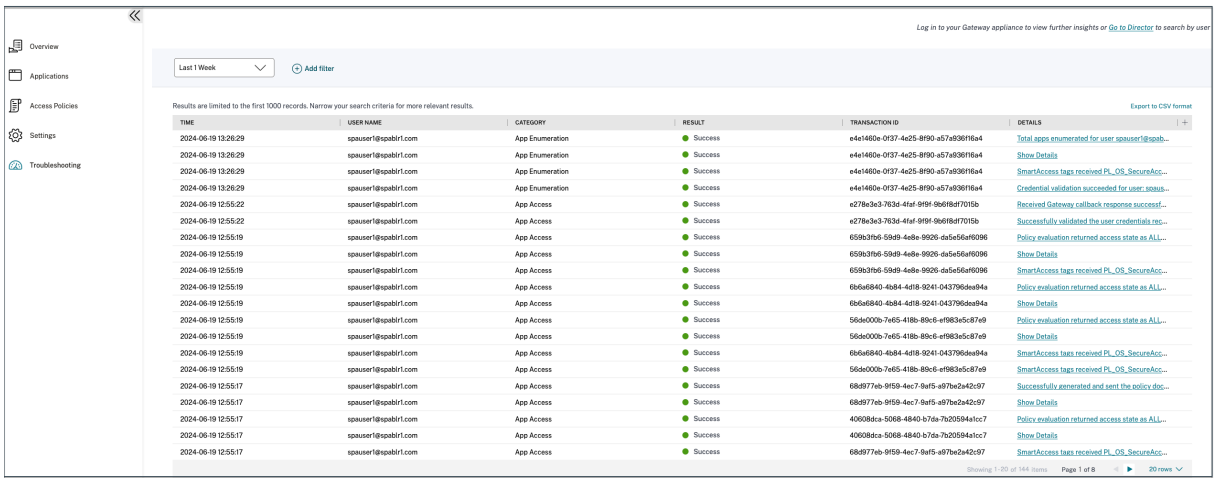
- 使用 Secure Private Access 配置 Director
- 在 Director 中查看 Secure Private Access 会话
- Director 中的 Secure Private Access 会话代码列表。
- Director。

控制板概述

August 26, 2024

故障排除控制板显示与应用程序启动、应用程序枚举和状态相关的日志。您可以查看预设时间或自定义时间轴的日志。您可以使用“添加过滤器”选项根据应用程序类别、用户名、事务 ID 等各种条件来细化搜索。例如，在搜索字段中，您可以选择事务 ID =（等于某个值），然后按此顺序输入 7456c0fb-a60d-4bb9-a2a2-edab8340bb15，搜索与该事务 ID 相关的所有日志。

您可以通过单击 + 符号向图表添加列，具体取决于您要在控制板中看到的信息。您可以将用户日志导出为 CSV 格式。



您可以使用“添加过滤器”选项使用以下搜索运算符来细化搜索：

- **=**（等于某个值）：搜索与搜索条件完全匹配的日志/策略。
- **!=**（不等于某个值）：搜索不包含指定条件的日志/策略。
- **~**（包含一些值）：搜索与搜索条件部分匹配的日志/策略。
- **!~**（不包含某些值）：搜索不包含某些指定条件的日志/策略。

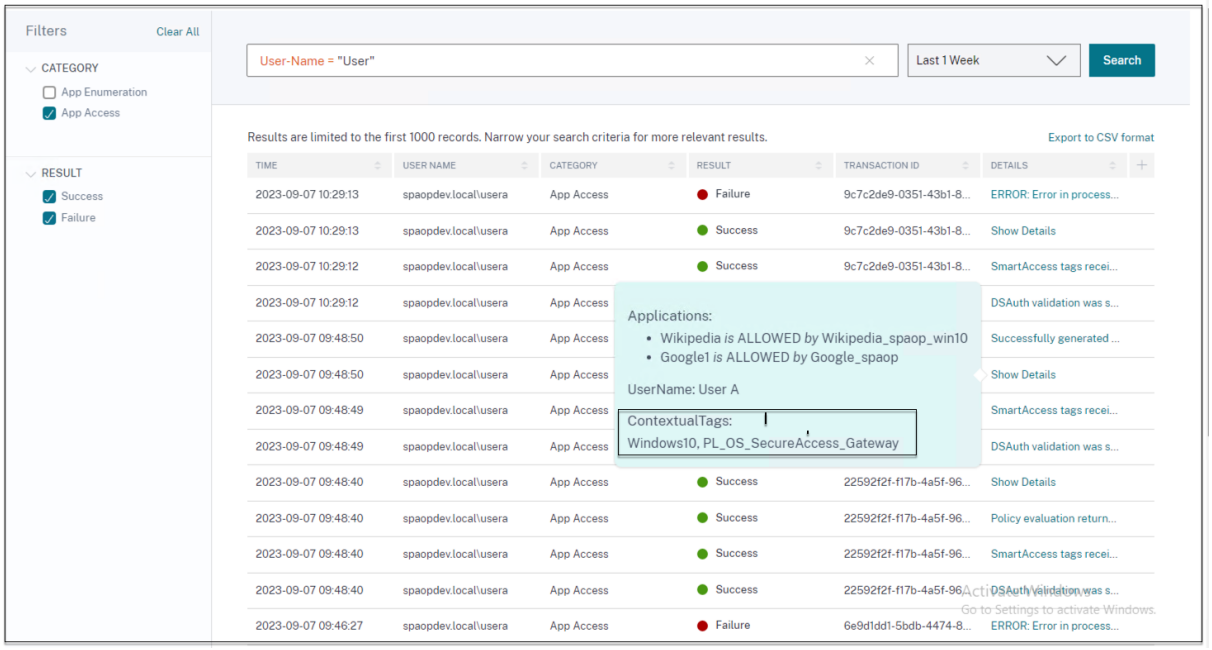
例如，您可以使用搜索字段中的字符串 **Event-Type > =**（等于某个值）**>** 枚举来搜索事件类型“枚举”。

同样，要搜索部分包含“operator”一词的用户，请使用字符串 **User-Name > ~**（包含一些值）**> operator**。此搜索列出了所有包含“操作员”一词的用户名。例如，“local operator”、“admin operator”。

您可以使用事务 ID 搜索与单个事件相关的所有日志。事务 ID 关联访问请求的所有 Secure Private Access 日志。一个应用程序访问请求可以生成多个日志，从身份验证开始，然后是应用程序枚举，然后是应用程序访问本身。所有这些事件都会生成自己的日志。事务 ID 用于关联所有这些日志。您可以使用事务 ID 筛选日志，查找与特定应用程序访问请求相关的所有日志。

查看日志中的上下文标签

详细信息列中的显示详细信息链接显示与特定访问策略相关的应用程序列表以及与该策略相关的上下文标签。如果配置了 nFactor 身份验证，则针对当前用户进行验证的 nFactor EPA 操作名称也将作为上下文标签的一部分捕获。



基本故障排除

August 26, 2024

本主题列出了您在设置 Secure Private Access 时或之后可能遇到的一些错误。

证书错误

数据库创建错误

StoreFront 故障

公共网关/回调网关故障

无法访问 Secure Private Access 服务器

证书错误

错误消息：无法自动从一个或多个网关服务器获取证书。

当您尝试添加公有 NetScaler Gateway 地址但获取证书时出现问题时，会出现此错误消息。在设置 Secure Private Access 或在安装完成后更新设置时，可能会出现此问题。

解决方法：更新网关证书的方式与 Citrix Virtual Apps and Desktops 的更新方式相同。

数据库创建错误

- 错误消息：无法创建数据库

  解决方案：对于自动用例-计算机必须具有读取、写入、更新权限才能在 SQL Server 上的数据库中创建表。

- 错误消息：无法创建数据库：数据库已经存在。

  此错误消息可能出现在以下任何场景中。

  - 如果在配置数据库时选择了自动配置选项。
  - 如果管理员正在创建数据库，则它必须是一个空数据库。如果数据库是非空数据库，则可能会出现此错误消息。

    解决方案：必须创建一个空数据库。
  - 您卸载了 Secure Private Access，然后使用相同的站点名称重试设置。在这种情况下，先前安装的数据库不会被删除。

    解决方案：必须手动删除数据库。
  - 您选择使用脚本手动设置数据库（通过在“配置数据库”页面中选择“手动配置”），然后更改为“自动配置”选项，但使用相同的站点名称。在这种情况下，运行脚本时已经创建了同名数据库。

    解决方案：您必须重命名该站点，然后再次运行脚本。
  - 计算机没有读取、写入、更新权限，无法在 SQL Server 的数据库中创建表。

    解决方案：在计算机上启用相应的权限。有关详细信息，请参阅 设置数据库所需的权限。

- 错误消息：无法创建数据库：连接失败

  解决方案：

  - 检查计算机上的数据库网络连接。确保防火墙上的 SQL Server 端口处于打开状态。
  - 如果使用远程 SQL Server，请检查 SQL Server 是否使用 Secure Private Access 计算机标识 Domain\hostname$ 创建了登录名。
  - 如果使用远程 SQL Server，请确认为计算机身份分配了正确的角色，即系统管理员角色。
  - 如果使用本地 SQL Server（不是安装程序），请检查 NT AUTHORITY\SYSTEM 用户是否必须创建登录名。

StoreFront 故障

- 错误消息：无法为以下内容创建 StoreFront 条目：<Store URL>

  如果 StoreFront 条目不可见，请从“设置”标签中更新该条目。使用向导设置 Secure Private Access 后，可以从“设置”选项卡编辑 StoreFront 条目。记下发生此错误的 StoreFront 应用商店 URL。

  解决方案：

  1. 单击“设置”，然后单击“集成”选项卡。
  2. 如果 StoreFront 条目不可见，请在 **StoreFront** 应用商店 **URL** 中添加该条目。

- 错误消息：无法为以下内容配置 StoreFront 条目：<Store URL>

  解决方案：

  1. 可能有 PowerShell 的执行策略限制。运行 PowerShell 脚本命令 `Get-ExecutionPolicy` 以了解详细信息。
  2. 如果受到限制，则必须绕过此设置并手动运行 StoreFront 配置脚本。
  3. 单击“设置”，然后单击“集成”选项卡。
  4. 在 **StoreFront** 应用商店 **URL** 中，识别出现错误的 StoreFront URL 条目。
  5. 单击此应用商店 URL 旁边的下载脚本按钮，并在安装了相应的 StoreFront 的计算机上以管理员权限运行此 PowerShell 脚本。此脚本必须在所有 StoreFront 计算机上运行。

  > 注意：
  >
  > 如果您在卸载后重试安装，请确保在 StoreFront 配置中没有名为“Secure Private Access”的条目（**StoreFront >** 应用商店 **> Delivery Controller -> Secure Private Access**）。如果存在 Secure Private Access，请删除此条目。从“设置”>“集成”页面手动下载并运行脚本。

- 错误消息：StoreFront 的配置不是本地配置：<Store URL>

  使用向导设置 Secure Private Access 后，可以从“设置”选项卡编辑网关条目。记下发生此错误的 StoreFront 应用商店 URL。

  解决方案：

  如果 StoreFront 与 Secure Private Access 未安装在同一台计算机上，则会出现此问题。您必须在安装了 StoreFront 的计算机上手动运行 StoreFront 配置。

  1. 单击“设置”，然后单击“集成”选项卡。
  2. 在 **StoreFront** 应用商店 **URL** 中，识别出现错误的 StoreFront URL 条目。
  3. 单击此应用商店 URL 旁边的下载脚本按钮，并在安装了相应的 StoreFront 的计算机上以管理员权限运行此 PowerShell 脚本。此脚本必须在所有 StoreFront 计算机上运行。

> 注意：
>
> 要运行 StoreFront PowerShell 脚本，请使用管理员权限打开兼容 Windows x64 的 PowerShell 窗口，然后运行 ConfigureStorefront.ps1。StoreFront 脚本与 Windows PowerShell (x86) 不兼容。

- 错误消息："Get-STFStoreService : Exception of type 'Citrix.DeliveryServices.Framework.Feature.Exceptions.Reg was thrown."（在使用 PowerShell 运行 StoreFront 脚本时）。

  当在兼容 x86 的 PowerShell 窗口上运行 StoreFront 脚本时，就会出现此错误。

  解决方案：

  要运行 StoreFront PowerShell 脚本，请使用管理员权限打开兼容 Windows x64 的 PowerShell 窗口，然后运行 `ConfigureStorefront.ps1`。

公共网关/回调网关故障

错误消息：无法为以下项创建网关条目：<`Gateway URL`> 或无法为以下项创建回调网关条目：<`Callback Gateway URL`>

解决方案：

记下发生故障的公共网关或回调网关 URL。使用向导设置 Secure Private Access 后，可以从"设置"选项卡编辑网关条目。

1. 单击"设置"，然后单击"集成"选项卡。
2. 更新公共网关地址或回调网关地址以及发生故障的虚拟 IP 地址。

无法访问 **Secure Private Access** 服务器

错误消息：更新 IIS 池失败。无法重新启动 IIS 池

解决方案：

转到 Internet Information Services (IIS) 中的应用程序池，检查以下应用程序池是否已启动并正在运行：

- Secure Private Access 运行时池
- Secure Private Access 管理池

还要检查默认 IIS 站点 `"Default Web Site"` 是否已启动并正在运行。

数据库连接检查失败

错误消息：连接检查失败

数据库连接检查可能由于多种原因而失败：

- 由于防火墙，无法从 Secure Private Access 插件主机访问数据库服务器。

  解决方案：检查防火墙上是否打开了数据库端口（默认端口 1433）。

- Secure Private Access 插件主机没有权限连接到数据库。

  解决方案：请参阅 Secure Private Access 的 SQL 数据库权限。

网关连接检查失败。无法获取公共证书

错误消息：安装后配置失败，并显示错误“网关连接检查失败。无法获取公共证书…”

解决方案：

- 使用配置工具手动将网关公共证书上载到 Secure Private Access 数据库。
- 使用管理员权限打开 PowerShell 或命令提示符窗口。
- 将目录更改为 Secure Private Access 安装文件夹下的 Admin\AdminConfigTool 文件夹（例如，cd “C:\Program Files\Citrix\Citrix Access Security\Admin\AdminConfigTool”）
- 运行以下命令：

```
.\AdminConfigTool.exe /UPLOAD_PUBLIC_GATEWAY_CERTIFICATE <PublicGatewayUrl
> <PublicGatewayCertificatePath>
```

应用程序枚举失败

如果 StoreFront URL 或 NetScaler Gateway URL 包含尾部斜杠 (/)，则应用程序枚举中断。

解决方案：

删除 StoreFront 应用商店 URL 或 NetScaler Gateway URL 中的尾部斜杠。有关详情，请参阅设置后更新 StoreFront 或 NetScaler Gateway 服务器详细信息。

其他

无法完成首次设置

如果 Director 配置在首次设置期间失败，则可能无法重新配置许可服务器。

解决方案：

手动清理 license_server 表。

创建 **Secure Private Access** 诊断支持包

执行以下步骤以创建 Secure Private Access 诊断支持包：

- 使用管理员权限打开 PowerShell 或命令提示符窗口。
- 将目录更改为 Secure Private Access 安装文件夹下的 Admin\AdminConfigTool 文件夹（例如，cd “C:\Program Files\Citrix\Citrix Access Security\Admin\AdminConfigTool”）。
- 运行以下命令：

```
.\AdminConfigTool.exe /SUPPORTBUNDLE <output folder>
```

Secure Private Access 的 **SQL** 数据库权限

要自动创建数据库，Secure Private Access 插件主机必须具有连接到数据库和创建数据库架构的权限。

远程数据库：

执行以下步骤来设置远程数据库的权限。

1. 使用名称语法 CitrixAccessSecurity<Site Name> 创建空数据库。其中，<Site Name> 是 Secure Private Access 的站点名称。（例如，CitrixAccessSecuritySPA）。

   ```
   CREATE DATABASE CitrixAccessSecurity<SiteName>
   ```

2. 为 Secure Private Access 虚拟机的计算机身份创建 SQL Server 登录名。例如，如果您的 Secure Private Access 代理计算机名为 HOST1，计算机域为 DOMAIN1，则计算机标识为 “DOMAIN1\HOST1$”。如果登录名已经创建，则可以忽略此步骤。

   ```
   USE CitrixAccessSecurity<SiteName>
   CREATE LOGIN [DOMAIN1\HOST1$] FROM WINDOWS
   ```

   可以使用以下查询找到域名：

   ```
   SELECT DEFAULT_DOMAIN()[DomainName]
   ```

3. 将 db_owner 角色分配给计算机身份。

   ```
   USE CitrixAccessSecurity<SiteName>
   EXEC sys.sp_addrolemember [db_owner], 'DOMAIN1\HOST1$'
   ALTER USER [DOMAIN1\HOST1$] WITH DEFAULT_SCHEMA = dbo;
   ```

本地数据库：

执行以下步骤来设置本地数据库的权限。

1. 使用名称语法 `CitrixAccessSecurity<Site Name>` 创建空数据库。其中，`<Site Name>` 为 Secure Private Access 的站点名称。（例如，CitrixAccessSecuritySPA）。

   ```
   CREATE DATABASE CitrixAccessSecurity<SiteName>
   ```

2. 为 `NT AUTHORITY\SYSTEM` 用户创建 SQL Server 登录名。如果登录名已经创建，则可以忽略此步骤。

   ```
   USE CitrixAccessSecurity<SiteName>

   CREATE LOGIN [NT AUTHORITY\SYSTEM] FROM WINDOWS
   ```

3. 将 db_owner 角色分配给“NT AUTHORITY\SYSTEM”用户。

   ```
   USE CitrixAccessSecurity<SiteName>

   EXEC sys.sp_addrolemember [db_owner], 'NT AUTHORITY\SYSTEM'

   ALTER USER [NT AUTHORITY\SYSTEM] WITH DEFAULT_SCHEMA = dbo;
   ```

当您手动创建数据库时，下载的数据库脚本会将权限添加到计算机标识中。

更改故障排除日志的日志级别

故障排除日志是默认的错误日志级别。

要更改故障排除日志的日志级别，请在 runtime service appsettings.json (C:\Program Files\Citrix\Citrix Access Security\Runtime\RuntimeService) 中，将 `TroubleshootingSql` 的 `restrictedToMinimumLevel` 更新为以下值之一：

```
-  Information
-  Debug
-  Warning
-  Error

"TroubleshootingSql": {

  "restrictedToMinimumLevel": "Error",
  "batchPostingLimit": 50,
  "batchPeriod": "00:00:05" // 5 seconds
 }
```

使用 **Director** 对会话进行故障排除

October 21, 2024

Director 与 Secure Private Access 的集成实现了有效的性能监控和故障排除，因为 Secure Private Access 设置中所有组件的问题都会被捕获到 Director 中。下表列出了 Director 中显示的各种错误代码和相关条件。

有关更多信息，请参阅以下主题。

- 使用 Secure Private Access 配置 Director
- 在 Director 中查看安全私有访问会话

> 注意：
>
> - 第二位包含“0”的代码表示正常执行流程。例如，1000 代表应用程序枚举成功。
> - 第二位数字包含“1”的代码表示失败或异常。例如 2101 代表会话失败。对于失败或异常，建议您通过检查日志来解决此类问题。如果这不能解决问题，请联系支持人员。

枚举相关代码

代码	状态	说明
1101	失败	枚举期间发生内部错误。
1102	失败	已枚举一些应用程序，但至少有一个应用程序评估失败。
1103	失败	未枚举任何应用程序，且至少有一个应用程序评估失败。
1000	成功	枚举成功。至少已枚举一个应用程序。
1001	成功	没有枚举任何应用程序，因为它们都被策略拒绝。
1002	成功	由于没有匹配的策略，因此未枚举任何应用程序。
1003	成功	没有列举任何应用程序，因为有些应用程序被拒绝，而对于其他应用程序，没有匹配的策略。
1004	成功	由于没有需要评估的策略，因此未枚举任何应用程序。

会话相关代码

代码	状态	说明
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	不活跃	会话已终止/不活动。

应用枚举消息代码

代码	状态	说明
3101	失败	应用程序枚举 - 发生内部错误（当前未使用）。
3102	失败	由于策略评估期间出现异常，因此未枚举应用程序。
3103	失败	应用程序枚举状态为空 - 策略评估期间发生内部错误。
3104	允许/拒绝/失败	检索应用程序的策略详细信息时出错。
3000	允许	允许应用程序枚举。
3001	否定	策略拒绝应用程序枚举。
3002	否定	由于没有匹配的策略，因此未枚举应用程序。
3003	未知	应用程序枚举状态未知。
3004	CEB 发布应用程序	尝试从 Citrix Enterprise 浏览器启动应用程序。

应用程序启动消息代码

代码	状态	说明
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	检索应用的政策详情时出错
4000	允许	允许应用程序启动。
4001	否定	由于政策原因，应用程序启动被拒绝。
4002	否定	由于没有匹配的策略，应用程序启动被拒绝。

SIEM 集成

August 26, 2024

Secure Private Access 插件支持与 Security Information and Event Management (SIEM) 服务集成。安全事件实时存储在 Windows 事件日志（事件查看器\应用程序和服务日志\Citrix Access Security）中，可以由第三方工具收集和分析。

下表列出了 Secure Private Access 插件的安全事件：

事件 ID	摘要	说明	源
4624	帐户已成功登录	在 Secure Private Access 管理员登录到 Secure Private Access 管理员控制台时创建的事件	Citrix Access Security Admin 服务
4625	账号登录失败	Secure Private Access 管理员无法登录到 Secure Private Access 管理员控制台	Citrix Access Security Admin 服务
4634	帐户已注销	在 Secure Private Access 管理员控制台注销时创建的事件	Citrix Access Security Admin 服务
4720	用户帐户已创建	添加新的 Secure Private Access 管理员时创建的事件	Citrix Access Security Admin 服务
4738	用户帐户已更改	更新新的 Secure Private Access 管理员时创建的事件	Citrix Access Security Admin 服务
4726	用户帐户已删除	移除新的 Secure Private Access 管理员时创建的事件	Citrix Access Security Admin 服务
8001	用户安全访问会话	用户会话在端点上启动或终止时创建的事件。包含用户、会话和设备详细信息，以及会话期间访问的内部和外部域	Citrix Access Security Admin 服务

8002	用户访问授权请求	当 Secure Private Access 插件授权访问资源时创建的事件。包含资源 FQDN 和授权决策	Citrix Access Security Admin 服务

引用

- Security Information and Event Management (SIEM) 集成
- 关于将日志共享到 SIEM 解决方案

Scout 集成

August 26, 2024

Citrix Scout 与 Secure Private Access 集成在一起，使管理员能够收集日志和指标以进行故障排除。有关收集哪些信息的信息，请参阅收集的内容。

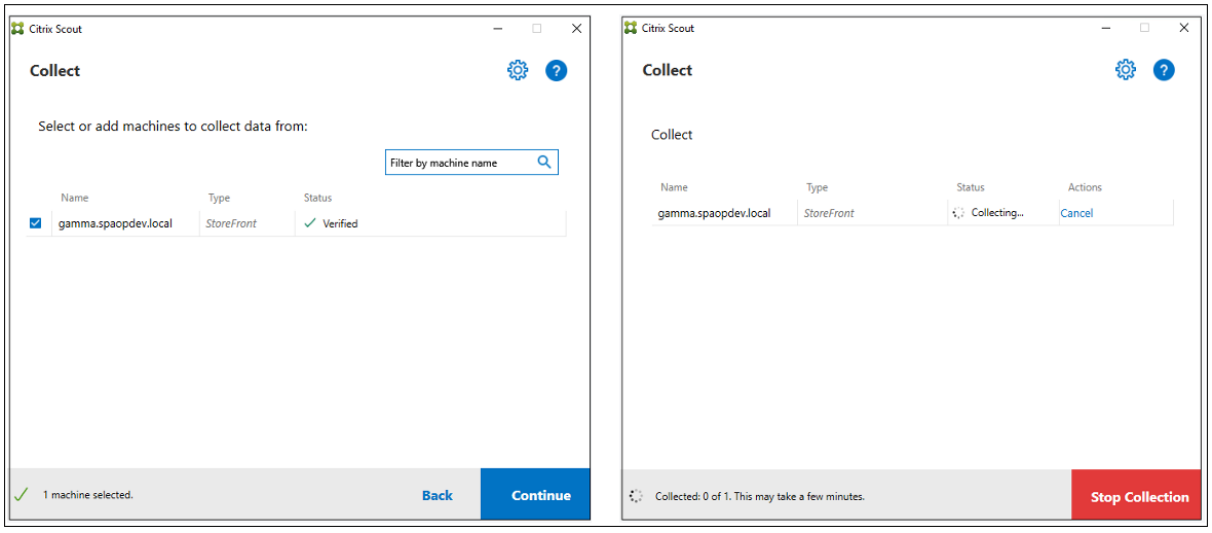
要开始收集 Secure Private Access 日志，请执行以下步骤：

1. 选择一台 Secure Private Access 计算机开始收集。
2. 单击继续。

您可以随时单击“停止收集”来停止收集。

Citrix Scout 还会检索以下日志。这些日志以包形式存储在本地计算机中，可以上载到 Citrix Cloud。

- C:\Program Files\Citrix\Citrix Access Security\Admin\AdminService\logs\spa-admin
- C:\Program Files\Citrix\Citrix Access Security\Runtime\RuntimeService\logs\spa-runtime



日志保留设置

June 19, 2024

这些日志在 Secure Private Access 数据库中存储七天。如果总日志数变得过大，例如超过 100,000，则可以删除早于 90 天的最旧日志。默认情况下，清理任务每 12 小时运行一次。每当运行时服务重新启动时，该作业也会运行。

自定义故障排除日志保留设置

日志的清理可通过运行时服务安装文件夹中的 appsettings.json 文件进行配置。您可以根据日志的期限和可以存储在数据库中的日志数量来设置清理。根据需要修改 appsettings.json 文件中的以下条目：

示例 **appsettings.json** 文件：

```
1   "TroubleshootingLogs": {
2
3     "CleanupPeriodInHours": 12,
4     "CleanupDataOlderThanDays": 7,
5     "CleanupOldestDataIfEntriesCountAbove": 0
6    }
```

要禁用清理，请根据需要配置以下设置：

- 要仅保留日志 7 天，请将 `CleanupDataOlderThanDays` 设置为 7。
- 要禁用基于天数的清理，请将 `CleanupDataOlderThanDays` 设置为 0。
- 要禁用基于计数的清理，请将 `CleanupOldestDataIfEntriesCountAbove` 设置为 0。
- 如果这两个设置都设置为 0，或者将 `CleanupPeriodInHours` 设置为 0，则日志将永久保留。
  - 不建议将 `CleanupDataOlderThanDays` 和 `CleanupOldestDataIfEntriesCountAbove` 两者都设置为 0 或者将 `CleanupPeriodInHours` 设置为 0，因为这可能会导致 100% 的磁盘使用率问题。
  - 也可以通过修改 `CleanupPeriodInHours` 条目来更改日志清理频率。

> 注意：
>
> 如果将 Secure Private Access 部署为群集，则必须在每个群集节点中修改这些设置。如果节点设置不匹配，则最常清理的实例优先。

日志和遥测清理

June 19, 2024

遥测数据清理

遥测数据在 Secure Private Access 数据库中存储 3 个月。每隔 30 秒进行一次检查，以识别应进行清理的遥测数据。

> 注意：
>
> 必须运行运行时服务才能触发遥测数据清理。

CDF 日志清理

CDF 日志存储在 Secure Private Access 安装计算机上，位于管理员和运行时服务的安装文件夹中。CDF 日志放在.csv 文件中，每个文件的大小限制为 10MB。
管理服务一次最多可以保留 90 个 CDF 日志文件，之后它会删除最旧的文件，为要创建的新 CDF 日志文件腾出空间。
运行时服务的工作方式与管理服务相同，但可以同时保留更多数量的文件，最多 600 个。

自定义清理 **CDF** 日志

CDF 日志清理可通过管理员和运行时服务的安装文件夹中的 appsettings.json 文件进行配置。要更改文件的文件大小和数量限制，请更新 appsettings.json 文件中的以下条目：

```
"CdfFile": {

      "fileSizeLimitBytes": 10485760, // 10 MB
      "retainedFileCountLimit": 600
     }
```

> 注意：
>
> 如果为站点设置了多个 Secure Private Access 实例，请在每台 Secure Private Access 安装计算机上更新 appsettings.json 文件以清理 CDF。

第三方通知

January 9, 2024

适用于本地的 Citrix Secure Private Access