Citrix Secure Private Access - 本地

Machine translated content

Disclaimer

本内容的正式版本为英文版。部分 Cloud Software Group 文档内容采用了机器翻译，仅供您参考。Cloud Software Group 无法控制机器翻译的内容，这些内容可能包含错误、不准确或不合适的语言。对于从英文原文翻译成任何其他语言的内容的准确性、可靠性、适用性或正确性，或者您的 Cloud Software Group 产品或服务沿用了任何机器翻译的内容，我们均不作任何明示或暗示的保证，并且适用的最终用户许可协议或服务条款或者与 Cloud Software Group 签订的任何其他协议（产品或服务与已进行机器翻译的任何文档保持一致）下的任何保证均不适用。对于因使用机器翻译的内容而引起的任何损害或问题，Cloud Software Group 不承担任何责任。

Contents

技术概述

June 19, 2024

Citrix Secure Private Access 本地是客户管理的零信任网络访问 (ZTNA) 解决方案，可减少对内部 Web 和 SaaS 应用程序的 VPN 访问，并提供以下功能以及无缝的最终用户体验：

- 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

该解决方案利用 StoreFront 本地和 Citrix Workspace 应用程序，为在 Citrix Enterprise Browser 中访问 Web 和 SaaS 应用程序提供无缝和安全的访问体验。该解决方案还利用 NetScaler Gateway 来强制执行身份验证和授权控制。

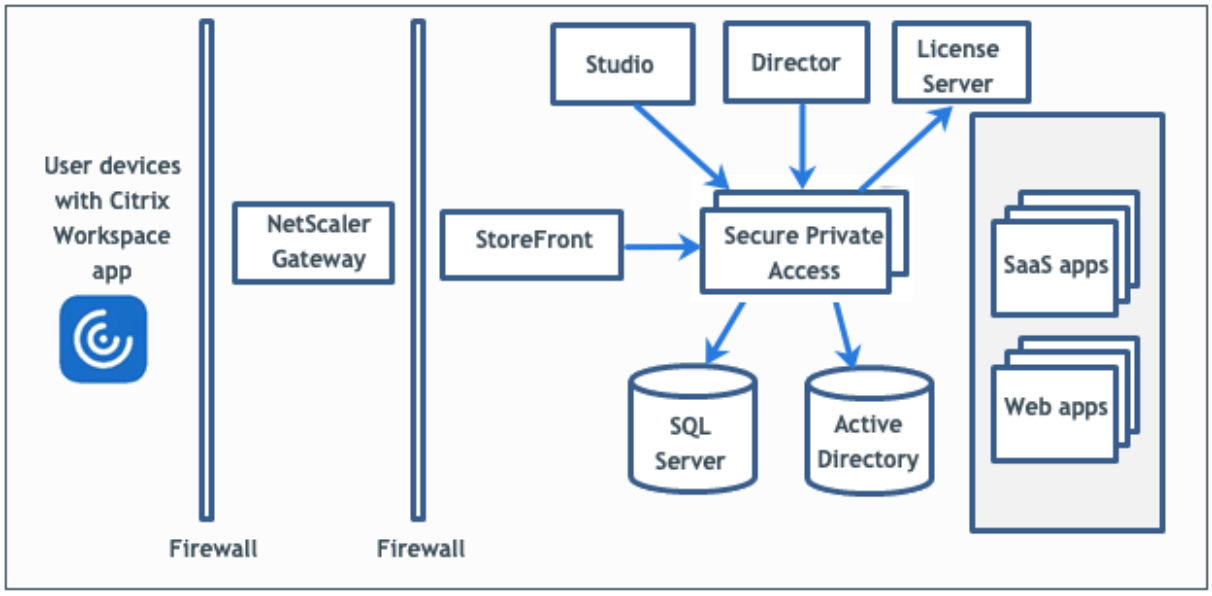
Citrix Secure Private Access 本地解决方案能够使用 StoreFront 本地门户作为 Web 和 SaaS 应用程序的统一访问门户，使用虚拟应用程序和桌面作为 Citrix Workspace 的集成部分，轻松为基于浏览器的应用程序（内部 Web 应用程序和 SaaS 应用程序）提供零信任访问权限，从而增强组织的整体安全性与合规性状况。

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

June 19, 2024

2024 年 **2** 月

Citrix Secure Private Access 与 **Director** 的集成

Citrix Secure Private Access 现已与 Director 集成，用于性能管理和增强故障排除。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

现在，您可以查看“在 Director 中查看 Secure Private Access 用户会话”。您可以查看有关活动会话和失败会话的详细信息。您还可以提供与应用程序、策略以及失败和成功会话的会话详细信息相关的信息。有关详细信息，请参阅按用户查看 Secure Private Access 会话。

Citrix Secure Private Access 与许可服务器集成

Citrix Secure Private Access 现已与许可服务器集成，用于收集和处理许可数据。有关详细信息，请参阅具有 Secure Private Access 权限的许可证服务器。

故障排除日志级别从“信息”更改为“错误”

故障排除日志级别从“信息”更改为“错误”，以减少数据库负载。有关如何更改日志级别的详细信息，请参阅更改故障排除日志的日志级别。

已修复的问题

June 19, 2024

2402 版中解决了以下问题。

管理员管理

管理员的 RBAC 角色更改仅在当前会话失效（注销或令牌到期）后才会反映出来。

管理员控制台

修改相关域条目后，已发布应用程序的编辑应用程序页面（**Secure Private Access >** 应用程序 **>** 编辑应用程序）未关闭后，编辑应用程序页面不会自动关闭。

例如，如果您在创建应用程序时输入的相关域是 `www.example.com`。应用程序发布后，将相关域 `www.example.com` 替换为 `abc.com`，然后单击保存。尽管应用程序已成功更新，但编辑应用程序页面并未关闭。

已知问题

June 19, 2024

2402 版本中存在以下问题。

域控制器配置

- 不支持不同 AD 林中的域之间信任类型为“林”的单向或双向信任。

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

- 如果安装本地 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 IIS 应用程序池中为 Secure Private Access 管理员和运行时服务添加不同的域服务帐户作为身份。

- 内联网 Secure Private Access (StoreFront) 登录和 Internet/Extranet（网关）应用程序枚举不支持备用 UPN 后缀。
- Secure Private Access 不支持通讯组。因此，策略无法搜索通讯组来添加用户和组条件。
- Secure Private Access 无法捕获管理员控制台或服务中的域详细信息。因此，它完全依赖于用户提供的域。因此，如果无法访问相应的域名或域名不是有效名称，则不支持该域。

NetScaler Gateway

以下场景不支持带有 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。
- `ns_vpn_enable_spa_onprem` 开关已启用。

解决方法：

将在 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` 开关。

有关开关的详细信息，请参阅 对智能访问标签的支持。

RfWeb/Workspace for Web

不支持 RfWeb/Workspace for Web，因此不枚举应用程序。有关详情，请参阅使用 StoreFront 版本 2311 或更高版本时。

应用程序图标

仅支持 ICO 图标格式。不支持 PNG、JPEG 和其他格式。

应用程序启动

如果满足以下所有条件，则应用程序启动失败：

- 使用的是 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 配置的后缀与实际域不同。
- LDAP UPN 和 sAMAccountName 是不同的。

升级

- 不支持将 2308 升级到 2402 及更高版本。
- 如果将自定义 SSL 证书用于 Secure Private Access 管理服务，则必须将该证书重新绑定到因特网信息服务 (IIS) 上的“Citrix Access Security Admin”站点。

StoreFront

- 在 应用商店 **>** 配置统一体验中，网站的默认接收器必须配置为 /Citrix/<StoreName>Web。在 StoreFront 的早期版本中，默认的 Receiver for Web 站点设置为空值，这不适用于 Secure Private Access。此外，早期版本的 Receiver 用户界面会显示在客户端上。有关 StoreFront 配置的信息，请参阅 StoreFront。
- 如果您使用的是 StoreFront 2308 或更早版本，则应用商店商店 **>** 管理 **Delivery Controller** 页面会将 Secure Private Access 插件类型显示为 **XenMobile**。这不会影响功能。

日志记录

- 不支持为群集生成支持包。
- 不得删除管理员和运行时服务的日志文件夹。如果删除了这些文件夹，则无法重新创建 Secure Private Access 权限。

管理员控制台

- 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，该应用程序已创建。

安装程序显示在“卸载”或“更改程序”页面中

当您使用 ISO 文件将 Secure Private Access 从 2311 升级到 2402 时，“卸载或更改程序”页面（控制面板 **>** 程序 **>** 程序和功能）会显示 Secure Private Access 安装程序的两个条目，而不是替换初始条目。

- **Citrix Virtual Apps and Desktops 7 2402 LTSR**
- **Citrix Virtual Apps and Desktops 7 2311-**安全的私人访问

您可以通过选择 **Citrix Virtual Apps and Desktops 7 2311 - Secure Private Access** 来卸载 2311 版本安装程序。

> 注意：
>
> 使用 2402 独立安装程序升级 Secure Private Access 2311 独立安装程序时，不会出现此问题。

系统要求

June 19, 2024

确保您的产品符合最低版本要求。

- Citrix Workspace 应用程序
  - Windows —2309 及更高版本
  - macOS —2309 及更高版本
- Secure Private Access 插件服务器的操作系统 - Windows Server 2019 及更高版本
- StoreFront —LTSR 2203 或 CR 2212 及更高版本
- NetScaler —13.0、13.1、14.1 及更高版本。建议使用 NetScaler Gateway 版本 13.1 或 14.1 的最新版本以优化性能。
- Director 2402 或更高版本
- 通信端口：确保已打开 Secure Private Access 插件所需的端口。有关详细信息，请参阅通信端口。

> 注意：
>
> 适用于 iOS 和 Android 的 Citrix Workspace 应用程序不支持本地 Secure Private Access。

必备条件

要创建或更新现有的 NetScaler Gateway，请确保您了解以下详细信息：

- 一台运行 IIS 且配置有 SSL/TLS 证书的 Windows 服务器计算机，将在该计算机上安装 Secure Private Access 插件。
- 要在设置期间输入的 StoreFront 应用商店 URL。
- 必须已配置 StoreFront 上的存储并且应用商店服务 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 插件主机的 IP 地址和 FQDN（如果将 Secure Private Access 插件部署为群集，则为负载平衡器）。
- 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。
- 证书配置已完成。管理员必须确保证书配置完整。如果计算机中找不到证书，Secure Private Access 安装程序会配置自签名证书。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。

管理员账号要求

设置 Secure Private Access 时需要以下管理员帐户。

- 安装 Secure Private Access：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。
- 管理 Secure Private Access：您必须使用 Secure Private Access 管理员帐户登录 Secure Private Access 管理员控制台。

通信端口

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 - 管理员控制台
Secure Private Access 插件	NTP 服务	TCP、UDP	123	时间同步
	DNS 服务	TCP、UDP	53	DNS 查询
	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)

源	目标	类型	端口	详细信息
	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 Gateway 回调
StoreFront	NTP 服务	TCP、UDP	123	时间同步
	DNS 服务	TCP、UDP	53	DNS 查询
	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 Gateway 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 与已配置的 Secure Private Access 应用程序的通信 （端口可能因应用要求而异）
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)。

尺码指南

June 19, 2024

数据库存储要求

大部分数据库存储空间都由日志消耗。与日志相比，应用程序和策略配置消耗的存储空间可以忽略不计。

下图显示了服务器存储要求：

Number of users	Number of Secure Private Access server nodes	Secure Private Access node configuration			SQL Server (Secure Private Access Database only)			Active Directory		StoreFront	
		CPU	Memory (GB)	Storage (GB)	CPU	Memory (GB)	Storage (GB)	CPU	Memory (GB)	CPU	Memory (GB)
1000	3	8	16	80	4	16	250	4	16	4	16
5000	8	8	16	80	16	16	750	16	16	4	16

> 注意：
>
> - 这些指标是基于以下假设得出的：日志事件清理已禁用，日志保留期设置为 7 天。
> - 默认情况下，日志保留 90 天或最多保留 100 K 个日志事件，具体取决于配置的设置。这些设置可在 Secure Private Access 运行时服务 appsettings.json 文件中找到，可以根据需要进行修改。有关详细信息，请参阅保留事件日志的设置。

服务器配置

下表显示了服务器配置的详细信息：

配置	详细信息
应用程序总数	250
策略总数	50

配置	详细信息
每位用户的应用程序数量	15
AD 配置	用户属于 20 个组，最多 20 个嵌套级别
故障排除日志保留期	7 天（默认）
故障排除日志级别	错误（默认）
Secure Private Access 服务器日志保留	90 天或 600 个文件

流量概况

下表显示了每位用户每天的流量配置文件详细信息。

配置文件	详细信息
枚举数	10
Enterprise Browser 策略同步	20
从 Citrix Workspace 应用程序启动应用程序	4
从 Citrix Enterprise Browser 访问应用程序	500
服务台通过 Citrix Director 对请求进行故障排除（每天）	1000

部署指南

下表根据并发应用程序访问用户会话、每分钟应用程序枚举以及 Secure Private Access 使用的 CPU 等参数显示了数据库大小要求：

并行应用程序访问用户会话	每分钟应用程序枚举次数	以 GB 为单位的 Secure Private Access 内存	Secure Private Access CPU	存储空间以 GB 为单位	备注
< 20（PoC 用途）	2	4 GB	2	40 GB*	出于 PoC 的目的，可以在不更改现有虚拟机规格的情况下将 SPA 部署在与 StoreFront 相同的计算机上。

并行应用程序访问用户会话	每分钟应用程序枚举次数	以 GB 为单位的 Secure Private Access 内存	Secure Private Access CPU	存储空间以 GB 为单位	备注
20	5	8 GB	4	60 GB	-
160**	18	16 GB	4***	60 GB	可以部署 2 个或更多 SPA 节点以获得更好的性能

> 注意：
>
> - * 存储空间主要由 CDF 日志消耗。默认情况下，Secure Private Access 保留 600 个滚动日志文件，每个文件的大小为 10 MB。因此，如果 Secure Private Access 管理员和运行时服务都在同一台计算机上运行，则日志的最大存储利用率为 12 GB。此外，SQL express 可以安装在本地虚拟机上用于 PoC 目的。
> - ** 对于此负载配置文件及更高版本，建议在专用服务器上部署 Secure Private Access，而不是与 StoreFront 共同托管，除非 NetScaler Gateway 版本低于 13.0 或低于 13.1-48.47。
> - *** 建议您使用至少 2 个 Secure Private Access 节点群集来处理此类负载，因为存在一些已知的性能问题。计划在即将发布的版本中解决这些问题。

其他组件配置

组件	vCPU	内存
Secure Private Access 插件	8	16 GB
Secure Private Access SQL Server	8	16 GB
StoreFront	16	8 GB
网关	4	8 GB
Active Directory	8	14 GB
客户端	4	8 GB

安装和配置

June 19, 2024

Secure Private Access 安装程序可作为独立安装程序使用，也可以作为集成的 Citrix Virtual Apps and Desktops 安装程序的一部分使用。有关详细信息，请参阅安装核心组件或使用命令行安装。

安装完成后，首次安装的管理员控制台将在默认浏览器窗口中自动打开。您可以单击“继续”来设置 Secure Private Access。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。

安装和管理 **Secure Private Access** 的管理员帐户要求

- 要安装 Secure Private Access，必须使用本地计算机管理员帐户登录。
- 要设置 Secure Private Access，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。
- 安装完成后，该用户将成为第一个 Secure Private Access 管理员，然后可以添加其他管理员。
- 要在设置后管理 Secure Private Access，必须使用 Secure Private Access 管理员帐户登录到 Secure Private Access 管理员控制台。

设置 **Secure Private Access**

您可以通过完成以下步骤来设置 Secure Private Access：

- 通过创建新站点设置 Secure Private Access 或通过加入现有站点设置 Secure Private Access
- 配置数据库
- 集成 StoreFront、NetScaler Gateway、Director 和许可服务器

配置应用程序和访问策略

设置 Secure Private Access 环境后，必须为应用程序配置应用程序和访问策略。

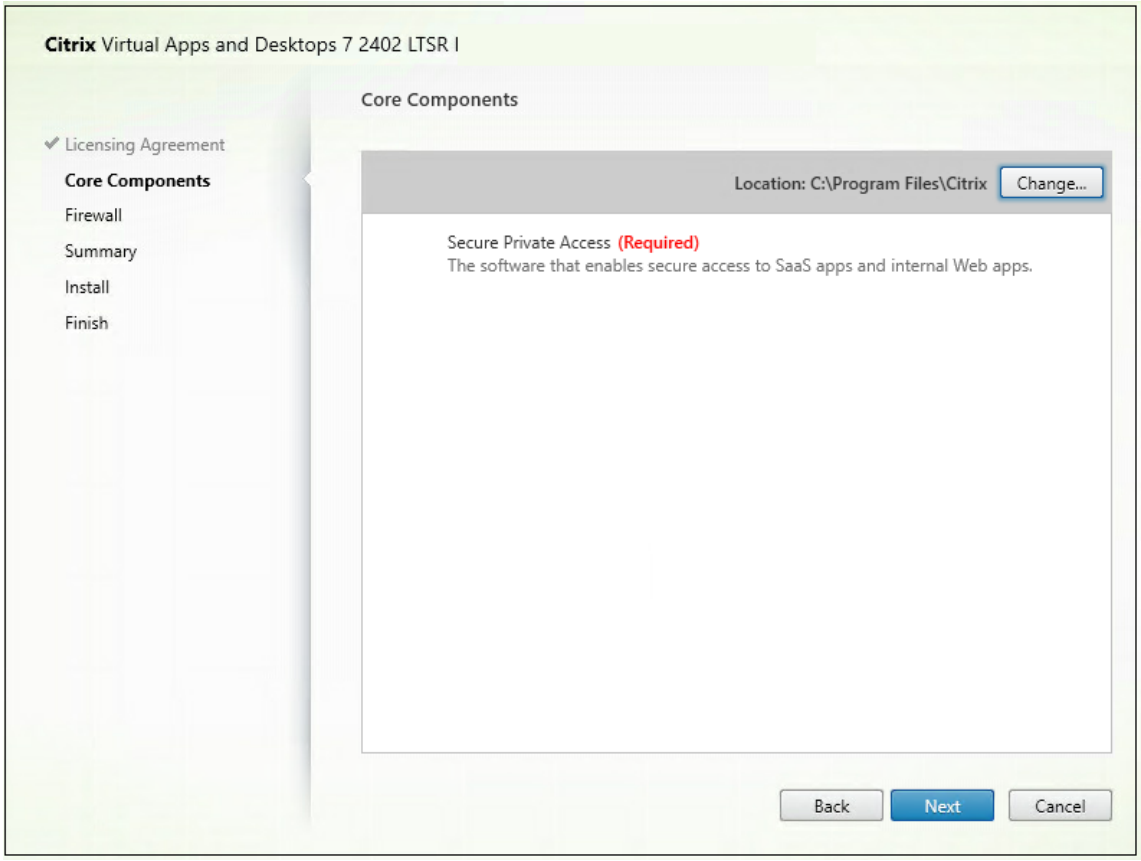
- 配置应用程序
- 为应用程序配置访问策略

Secure Private Access 安装程序

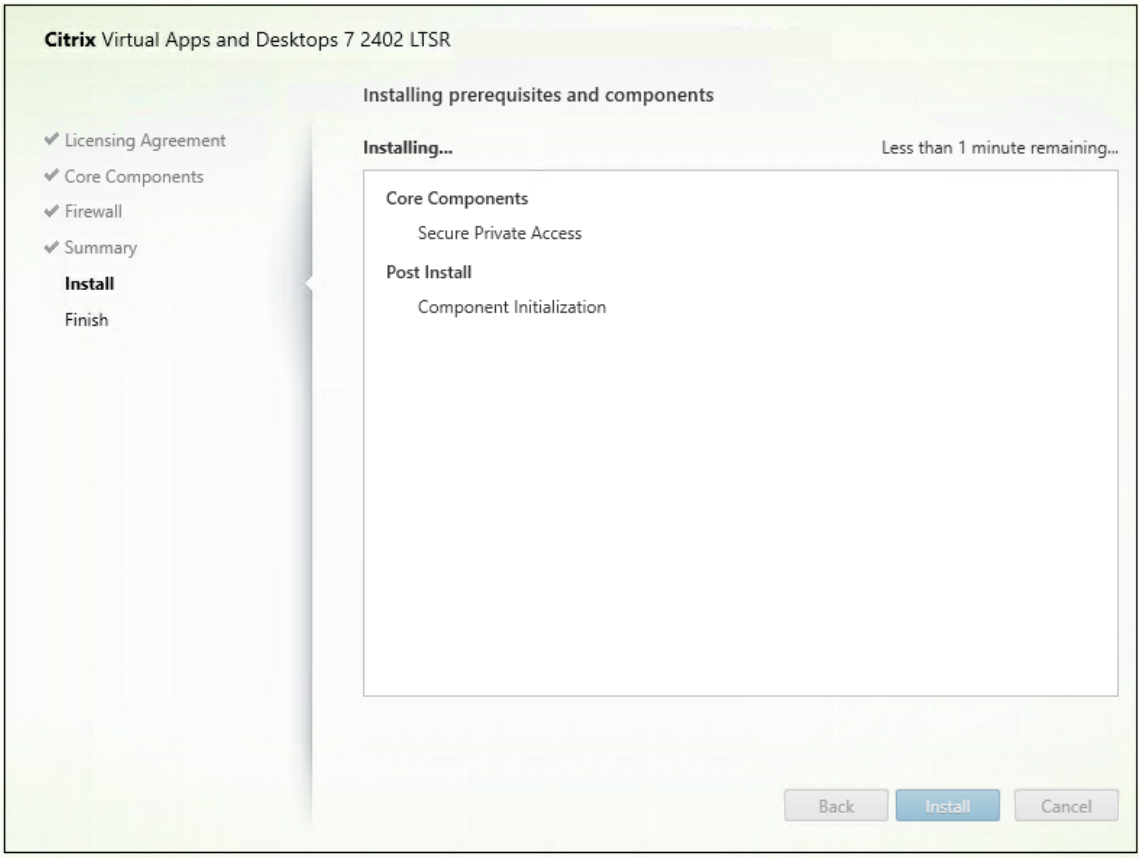
June 19, 2024

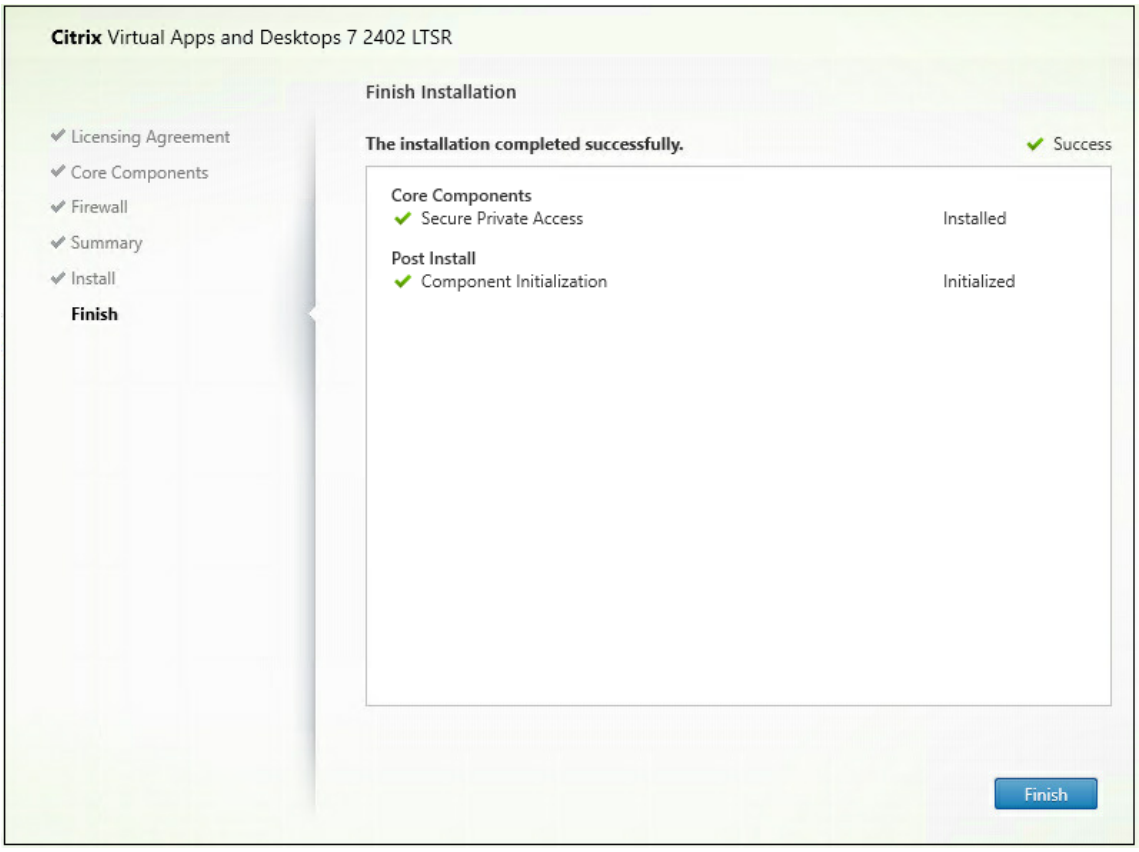
1. 从 https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/ 下载 Citrix Secure Private Access 安装程序。
2. 在加入域的计算机上以管理员身份运行.exe。

> 注意：
>
> 出于 POC 的目的，建议您在安装 StoreFront 的同一台计算机上安装 Secure Private Access。

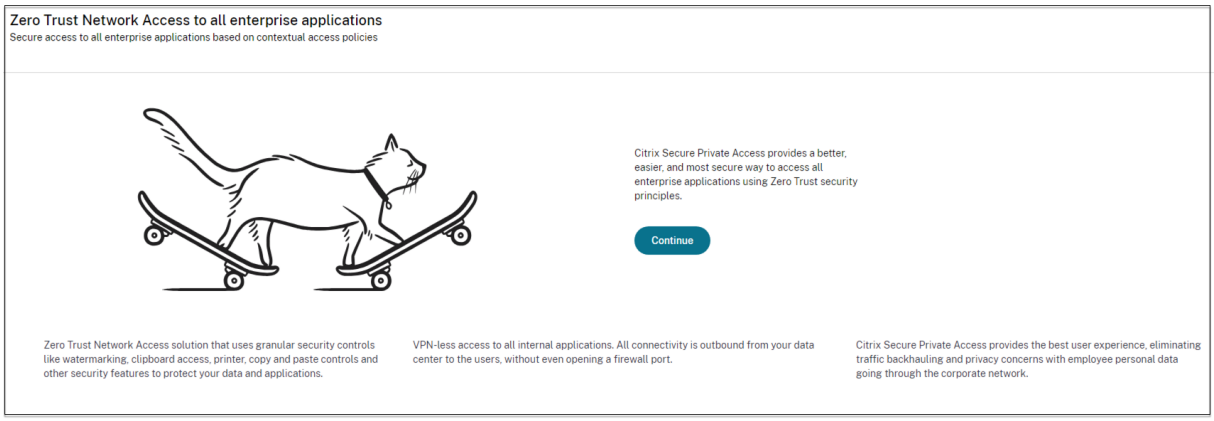


3. 按照屏幕上的说明完成安装。

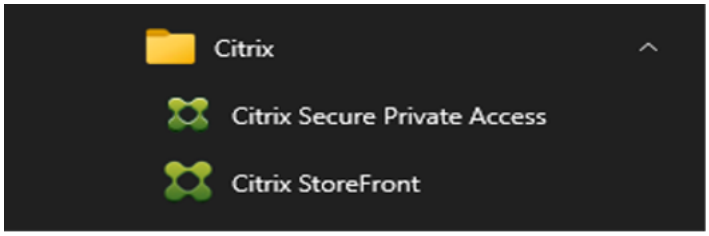




安装完成后，首次安装的管理员控制台将在默认浏览器窗口中自动打开。您可以单击“继续”来设置 Secure Private Access。



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。



有关详细信息，请参阅以下主题：

- 安装核心组件
- 使用命令行安装

SSO 到管理员控制台

建议您为用于 Secure Private Access 管理控制台的浏览器配置 Kerberos 身份验证。这是因为 Secure Private Access 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 Secure Private Access 管理控制台时，浏览器会提示您输入凭据。

- 如果您输入凭据，则会启用集成 Windows 身份验证 (IWA) 登录。
- 如果您不输入证书，则会显示 Secure Private Access 登录页面。

您必须登录管理员控制台才能继续进行 Secure Private Access 设置。如果用户在安装计算机上具有本地管理员权限，则可以为与安装计算机属于同一域的任何用户设置 Secure Private Access。

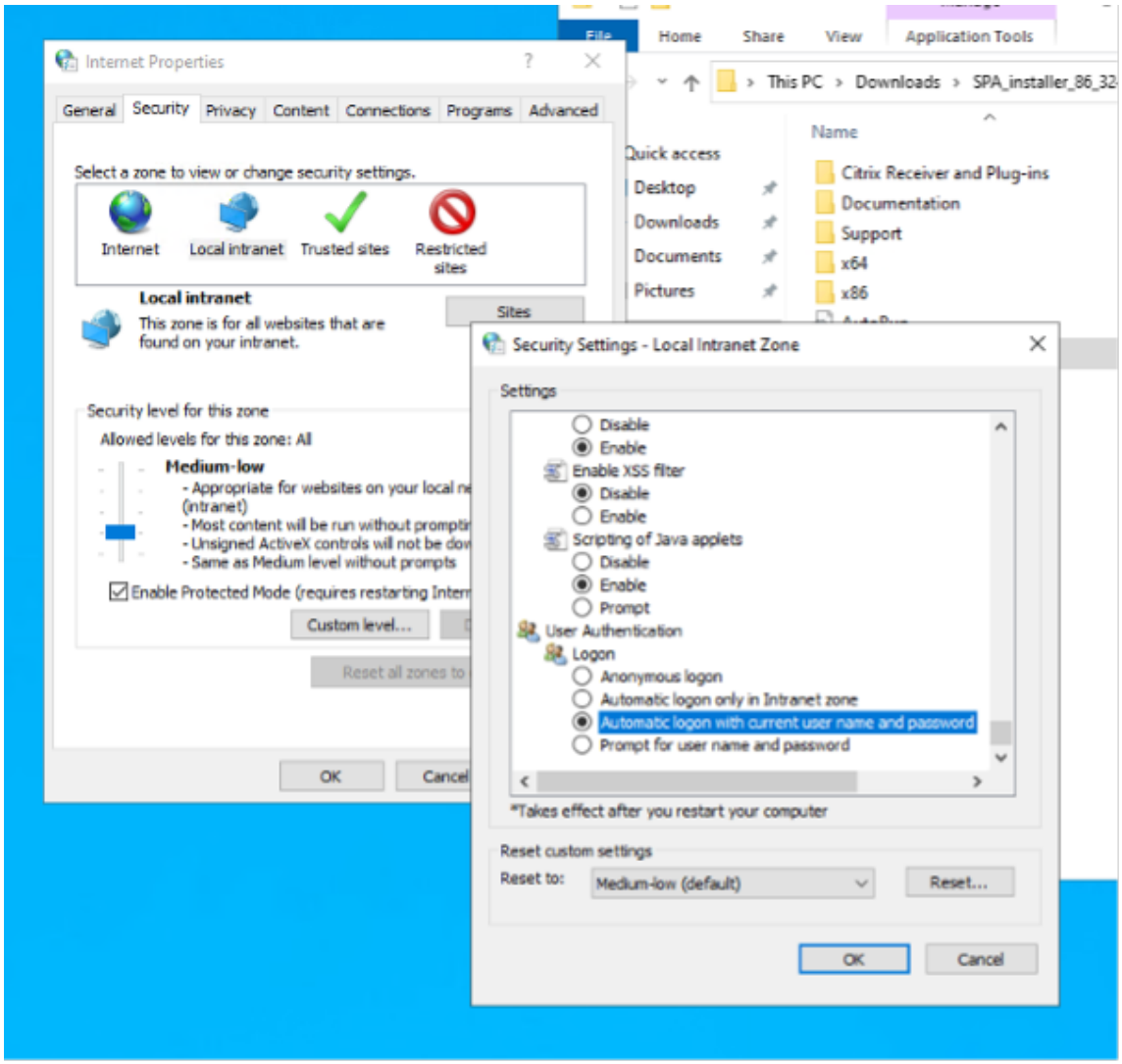
对于 Google Chrome 和 Microsoft Edge 浏览器，请执行以下步骤以启用 Kerberos。

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”，然后添加 Secure Private Access URL。

   如果计划在多台计算机上安装 Secure Private Access，也可以使用通配符。例如，`"https://*.fabrikam.local"`。

4. 单击“自定义级别”，然后在“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
>   并将值设置为 1。
> - 在 Kerberos 启用隐身模式之前，您必须重新启动所有 Chrome 窗口（包括非隐身窗口）。
> - 对于其他浏览器，请查看特定浏览器的 Kerberos 身份验证文档。

后续步骤

- 设置 Secure Private Access

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

设置 **Secure Private Access**

June 19, 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

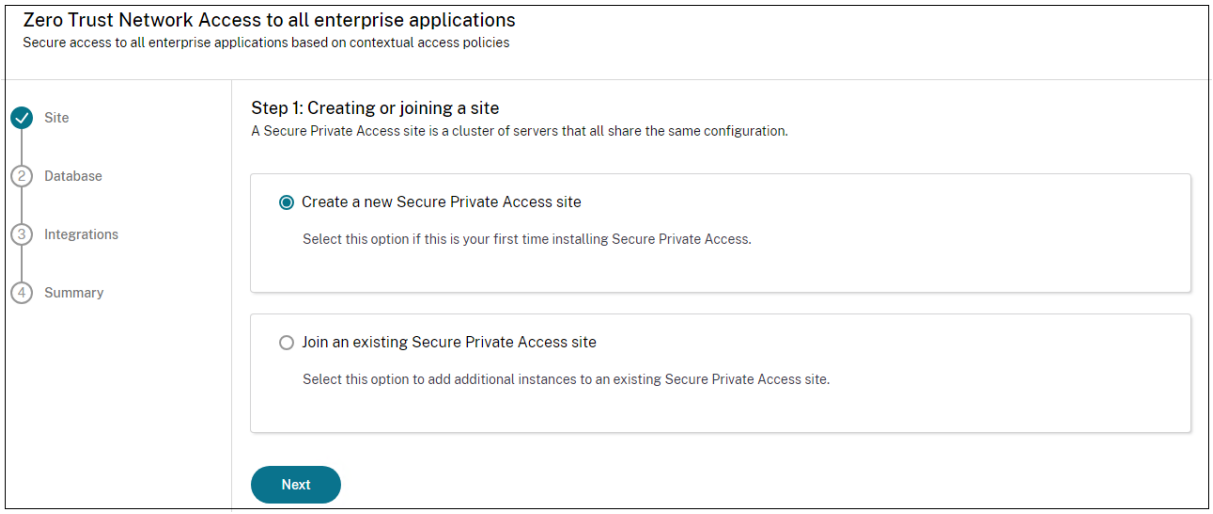
- 您必须使用域用户登录 Secure Private Access 管理员控制台，该域用户也是安装了 Secure Private Access 的计算机的本地计算机管理员。
- 在创建站点之前，必须安装 SQL 数据库服务器。

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：

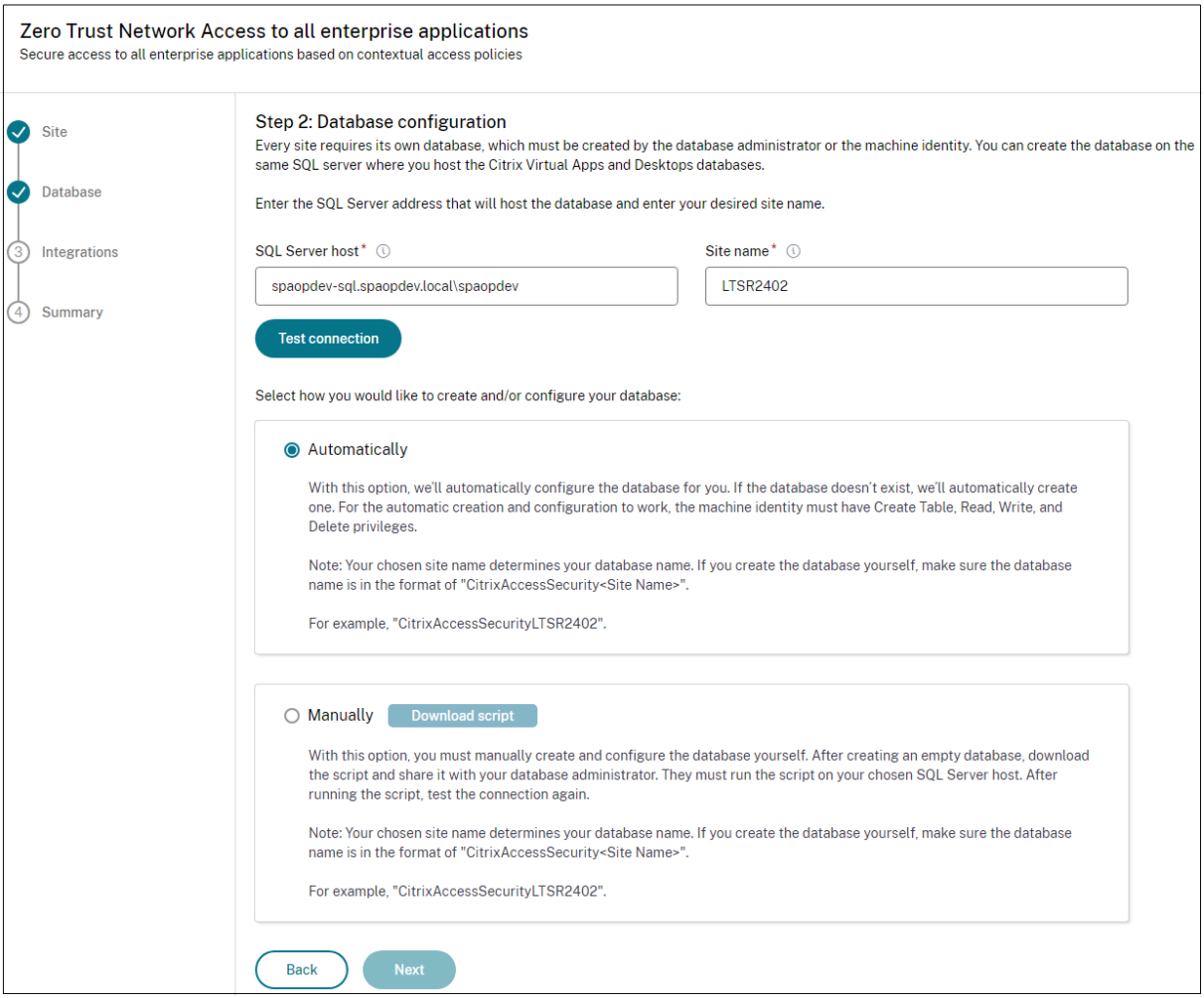
   - ServerName
   - ServerName\InstanceName
   - ServerName,PortNumber

   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。

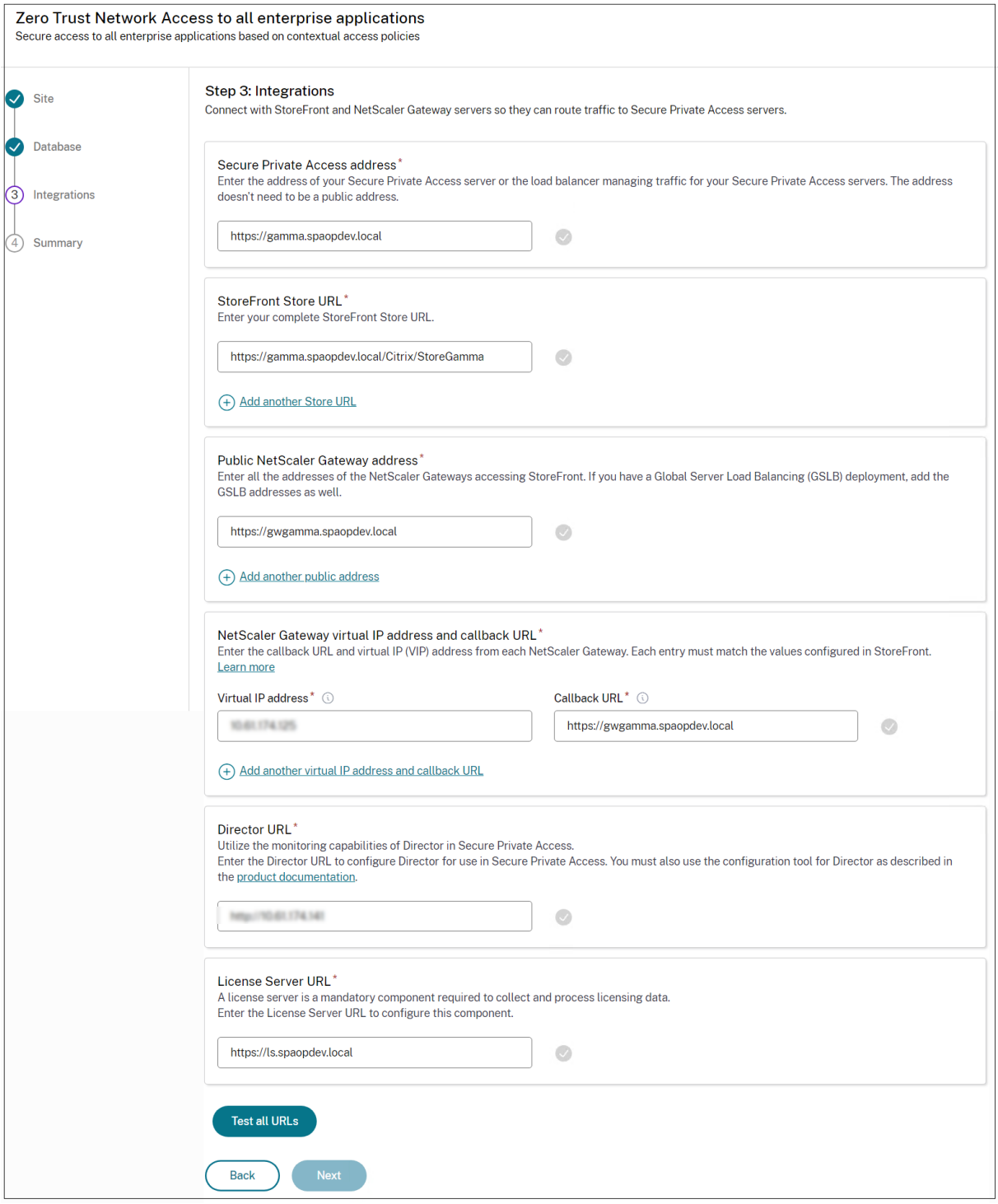
在手动配置中，必须先下载脚本，然后在在 **SQL Server** 主机字段中指定的数据库服务器上运行脚本。

> 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。

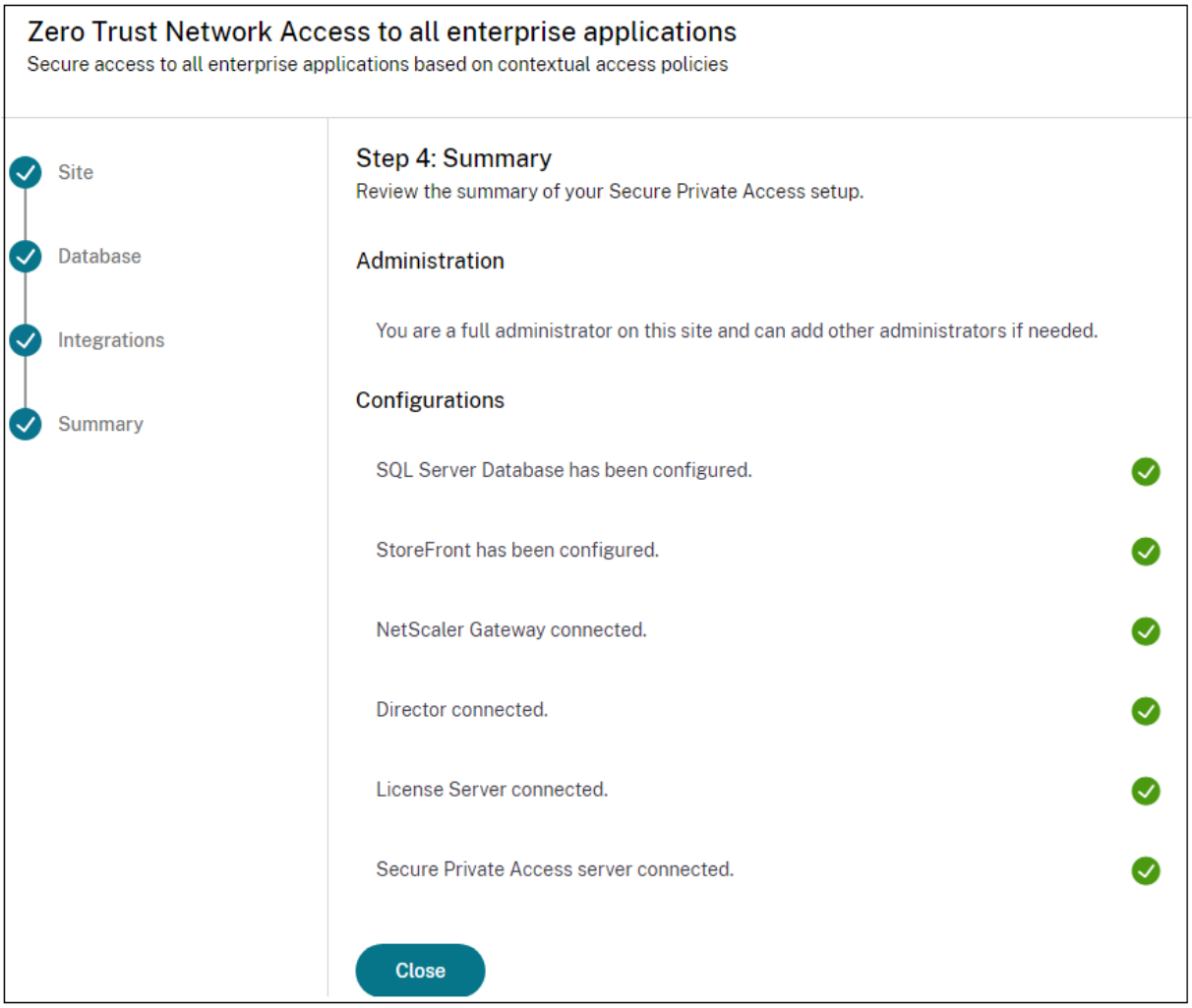
1. 输入以下详细信息。
    - **Secure Private Access** 服务器地址。例如，`https://secureaccess.domain.com`。
    - **StoreFront** 应用商店 **URL**。例如，`https://storefront.domain.com/Citrix/StoreMain`。
    - 公共 **NetScaler** 网关地址—NetScaler Gateway 的 URL。例如，`https://gateway.domain.com`。
    - 虚拟 **IP** 地址—此虚拟 IP 地址必须与 StoreFront 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**： -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。



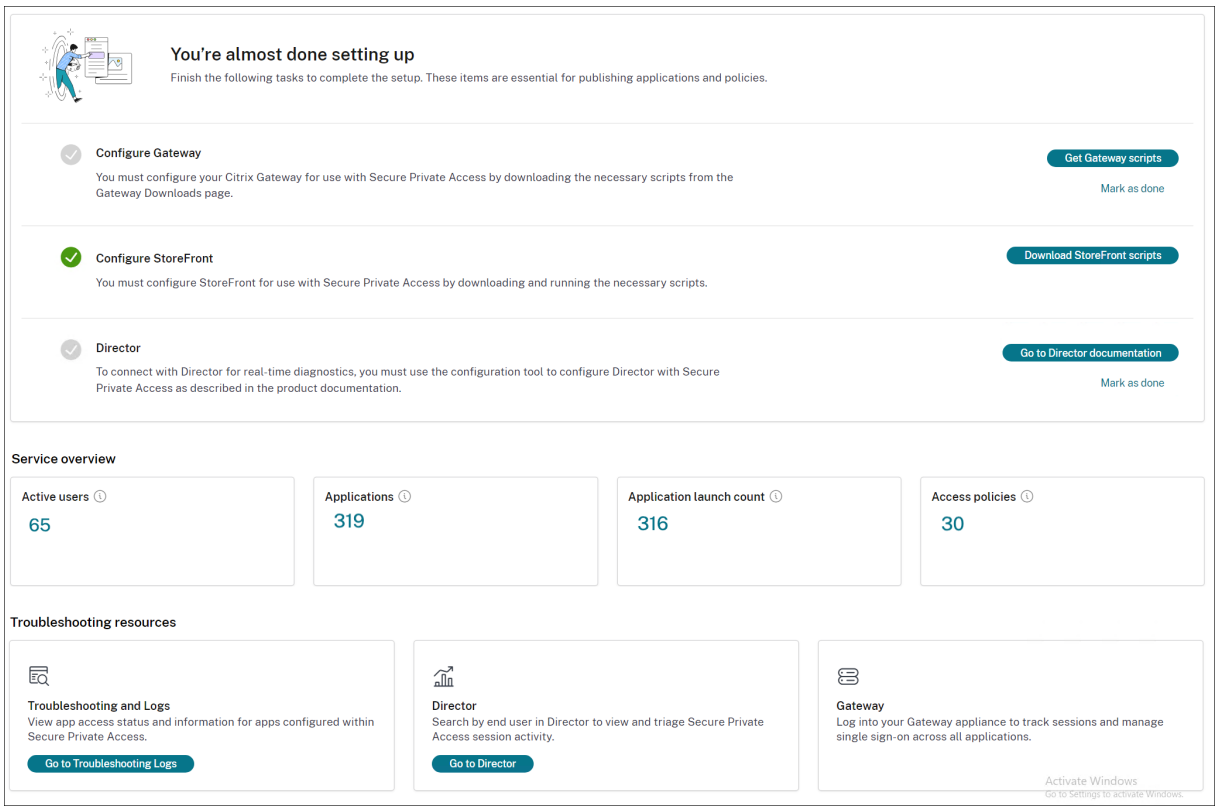
步骤 **4**：配置摘要

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。

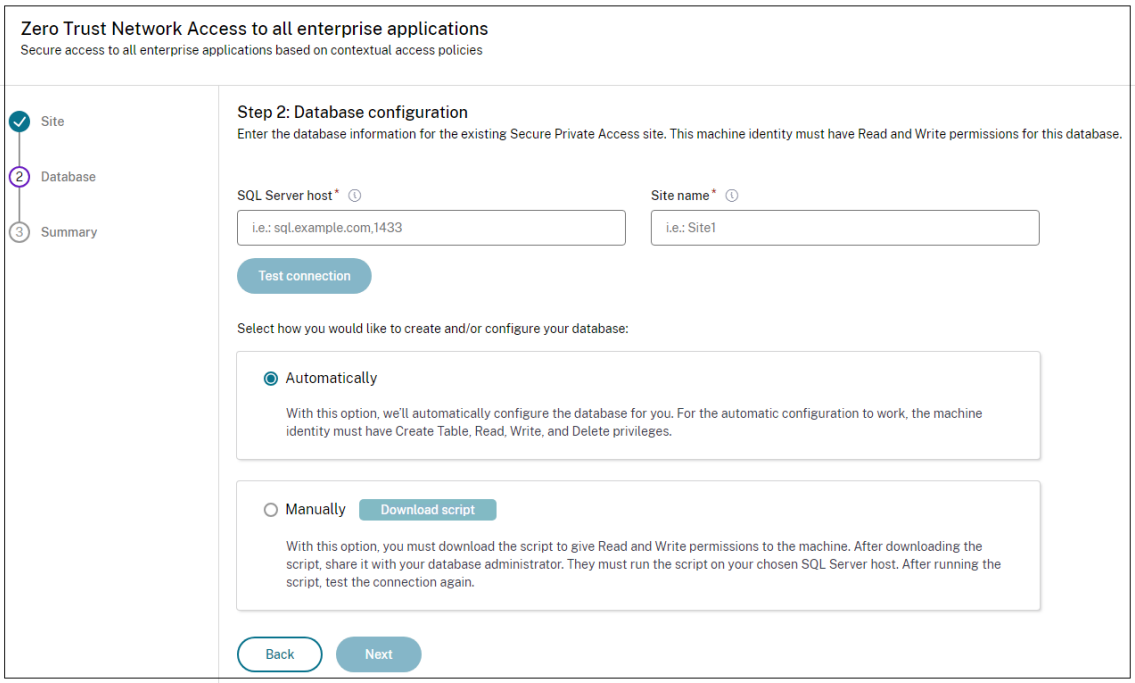


> 注意：
>
> - 设置环境后，您可以从 Web 管理员控制台中的“设置” > “集成”修改设置。
> - 首次安装 Secure Private Access 权限的管理员被授予完全权限。然后，该管理员可以将其他管理员添加到设置中。您可以从“设置” > “管理员”中查看管理员列表。
> - 您还可以添加管理员组，以便为该组中的所有管理员启用访问权限。

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”。

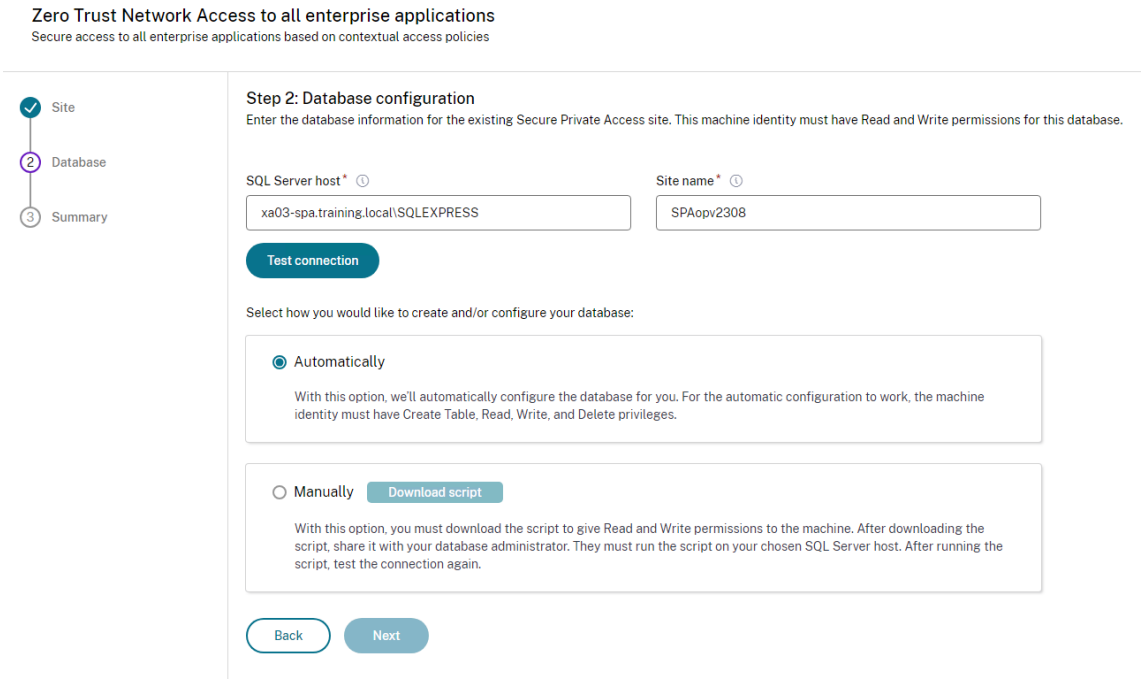


2. 在 **SQL Server** 主机中，输入服务器主机名。确保所选的 SQL Server 中已经存在与您输入的站点名称对应的数据库。可以使用以下格式之一指定数据库地址：

   - 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

组件

June 19, 2024

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

- **StoreFront**： - StoreFront 对用户进行身份验证并管理用户访问的桌面和应用商店。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。StoreFront 还跟踪用户的应用程序订阅、快捷方式名称以及其他数据。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 StoreFront。

- **NetScaler Gateway**： - 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 Gateway。
- **Director**：Director 使您能够进行有效的性能监视和故障排除。要将 Director 与 Secure Private Access 集成，必须输入必须在 Secure Private Access 中注册的 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。有关与 Web Studio 集成的 Secure Private Access 的详细信息，请参阅 Secure Private Access 与 Web Studio 的集成。

> 注意：
>
> 从 2402 版开始，Director 和 License Server 已集成到 Secure Private Access 中。

NetScaler Gateway

June 19, 2024

> 重要：
>
> 我们建议您在应用这些更改之前创建 NetScaler 快照或保存 NetScaler 配置。

1. 从 https://www.citrix.com/downloads/citrix-secure-private-access/Shell-Script/Shell-Script-for-Gateway-Configuration.html 中下载脚本。

   要创建新的 NetScaler Gateway，请使用 *ns_gateway_secure_access.sh*。

   要更新现有 NetScaler Gateway，请使用 *ns_gateway_secure_access_update.sh*。

2. 将这些脚本上载到 NetScaler 计算机。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`*

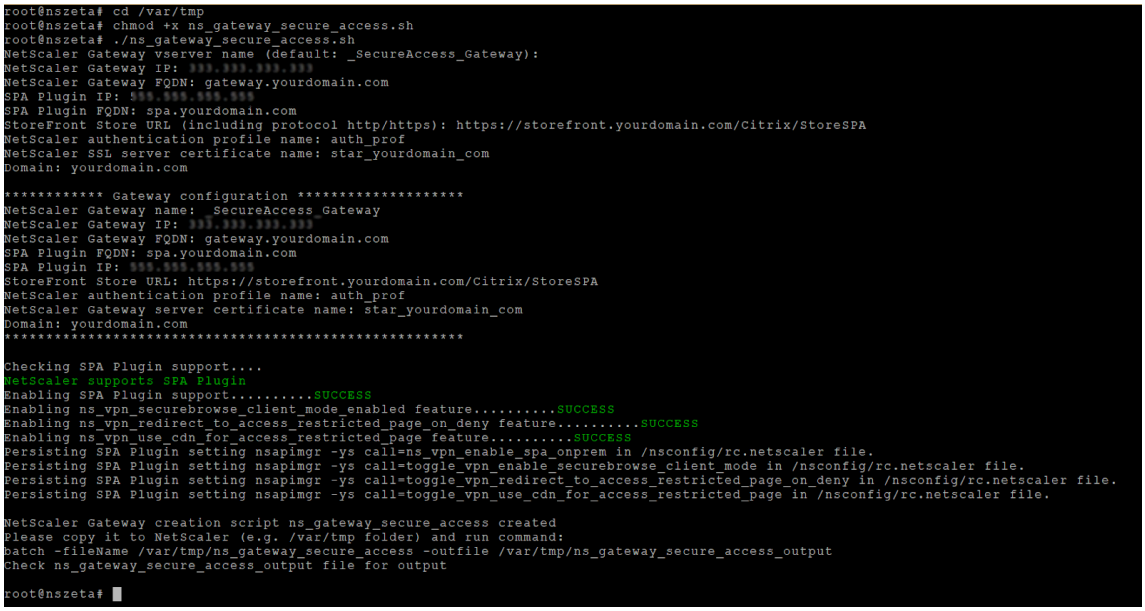
   > 注意：
   >
   > - 建议使用 NetScaler /var/tmp 文件夹来存储临时数据。
   > - 确保文件以 LF 行结尾保存。FreeBSD 不支持 CRLF。
   > - 如果您看到错误 `-bash: /var/tmp/ns_gateway_secure_access.sh: /bin`

> `/sh^M: bad interpreter: 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++）来转换脚本。

3. 通过 SSH 连接到 NetScaler 并切换到 shell（在 NetScaler CLI 上键入“shell”）。
4. 使上载的脚本可执行。使用 chmod 命令来执行此操作。

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

5. 在 NetScaler shell 上运行上载的脚本。

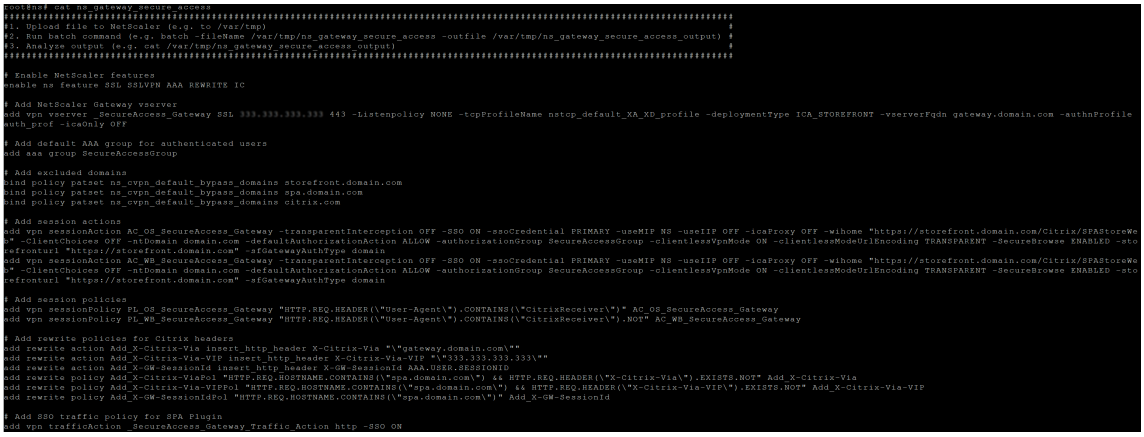


6. 输入所需的参数。有关参数列表，请参阅 必备条件。

   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。

   生成了一个包含多个 NetScaler 命令（默认为 var/tmp/ns_gateway_secure_access）的新文件。

   > 注意：
   >
   > 在脚本执行期间，将检查 NetScaler 和 Secure Private Access 插件的兼容性。如果 NetScaler 支持 Secure Private Access 插件，则该脚本使 NetScaler 功能能够支持智能访问标签，在资源访问受限时发送改进和重定向到新的“拒绝页面”。有关智能标签的详细信息，请参阅对智能访问标签的支持。
   >
   > /nsconfig/rc.netscaler 文件中保留的 Secure Private Access 插件功能允许在 NetScaler 重新启动后保持启用状态。



7. 切换到 NetScaler CLI，然后使用批处理命令从新文件中运行生成的 NetScaler 命令。例如;

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

   NetScaler 逐一运行文件中的命令。如果命令失败，则继续执行下一个命令。

   如果资源存在或步骤 6 中输入的参数之一不正确，则命令可能会失败。

8. 确保所有命令都成功完成。

> 注意：
>
> 如果出现错误，NetScaler 仍会运行其余命令并部分创建/更新/绑定资源。因此，如果您看到由于其中一个参数不正确而出现意外错误，建议从头开始重新进行配置。

使用现有配置在 **NetScaler Gateway** 上配置 **Secure Private Access**

您还可以在现有 NetScaler Gateway 上使用脚本来支持 Secure Private Access。但是，该脚本不会更新以下内容：

- 现有 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条命令并创建网关配置的备份。

NetScaler Gateway 虚拟服务器上的设置

添加或更新现有 NetScaler Gateway 虚拟服务器时，请确保将以下参数设置为定义值。

添加虚拟服务器：

- tcpProfileName：nstcp_default_XA_XD_profile
- deploymentType：ICA_STOREFRONT（仅在 `add vpn vserver` 命令中可用）

- icaOnly：OFF

更新虚拟服务器：

- tcpProfileName：nstcp_default_XA_XD_profile
- icaOnly：OFF

示例：

要添加虚拟服务器，请执行以下操作：

```
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
```

要更新虚拟服务器，请执行以下操作：

```
set vpn vserver _SecureAccess_Gateway -icaOnly OFF
```

有关虚拟服务器参数的详细信息，请参阅 vpn-sessionAction。

NetScaler Gateway 会话操作

会话操作绑定到具有会话策略的网关虚拟服务器。创建会话操作时，请确保将以下参数设置为已定义的值。

- `transparentInterception`：关
- `SSO`：开
- `ssoCredential`：PRIMARY
- `useMIP`：NS
- `useIIP`：关
- `icaProxy`：关
- `wihome`：`"https://storefront.mydomain.com/Citrix/MyStoreWeb"` - 替换为真实的应用商店 URL。存储路径 `/Citrix/MyStoreWeb` 是可选的。
- `ClientChoices`：关
- `ntDomain`：mydomain.com - 用于 SSO（可选）
- `defaultAuthorizationAction`：ALLOW
- `authorizationGroup`：SecureAccessGroup（确保创建了该组，它用于绑定 Secure Private Access 特定的授权策略）
- `clientlessVpnMode`：开
- `clientlessModeUrlEncoding`：TRANSPARENT
- `SecureBrowse`：ENABLED
- `Storefronturl`：`"https://storefront.mydomain.com"`
- `sfGatewayAuthType`：domain

示例：

要添加会话操作，请执行以下操作：

```
add vpn sessionAction AC_OS_SecureAccess_Gateway -transparentInterception
 OFF -SSO ON -ssoCredential PRIMARY -useMIP NS -useIIP OFF -icaProxy
 OFF -wihome "https://storefront.mydomain.com/Citrix/MyStoreWeb"-
ClientChoices OFF -ntDomain mydomain.com -defaultAuthorizationAction
 ALLOW -authorizationGroup SecureAccessGroup -clientlessVpnMode
ON -clientlessModeUrlEncoding TRANSPARENT -SecureBrowse ENABLED -
storefronturl "https://storefront.mydomain.com"-sfGatewayAuthType
domain
```

要更新会话操作，请执行以下操作：

```
set vpn sessionAction AC_OS_SecureAccess_Gateway -transparentInterception
 OFF -SSO ON
```

有关会话操作参数的详细信息，请参阅 https://developer-docs.netscaler.com/en-us/adc-command-reference-int/13-1/vpn/vpn-sessionaction。

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 DDC 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

在以下版本中，NetScaler Gateway 会自动发送标签。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

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

在这些 NetScaler 版本上，使用开关 `ns_vpn_enable_spa_onprem` 或 `ns_vpn_disable_spa_onprem` 启用/禁用此功能。

- 您可以使用命令进行切换（FreeBSD shell）：

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


- 运行以下命令（FreeBSD shell），为 HTTP 标注配置启用 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“访问受限”页面。

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

- 使用 CDN 上托管的“访问受限”页面。

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

- 要禁用，请再次运行相同的命令。
- 要验证开关处于开启还是关闭状态，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签。

在 **NetScaler** 上保留 **Secure Private Access** 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. 将以下命令添加到该文件中。

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

   nsapimgr_wr.sh -ys call=toggle_vpn_redirect_to_access_restricted_page_on_d

   nsapimgr_wr.sh -ys call=toggle_vpn_use_cdn_for_access_restricted_page
   ```

3. 保存该文件。

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

已知限制

- 现有的 NetScaler Gateway 可以使用脚本进行更新，但可能有无限数量的 NetScaler 配置，单个脚本无法涵盖。
- 请勿在 NetScaler Gateway 上使用 ICA 代理。配置 NetScaler Gateway 时，此功能将被禁用。

- 如果您使用部署在云端的 NetScaler，则必须在网络中进行一些更改。例如，允许 NetScaler 与其他组件在特定端口上进行通信。
- 如果您在 NetScaler Gateway 上启用 SSO，请确保 NetScaler 使用私有 IP 地址与 StoreFront 通信。您可能需要使用 StoreFront 私有 IP 地址向 NetScaler 添加一条新的 StoreFront DNS 记录。

上载公共网关证书

如果无法从 Secure Private Access 计算机访问公共网关，则必须将公共网关证书上载到 Secure Private Access 数据库。

执行以下步骤上载公共网关证书：

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. 运行以下命令：

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

配置上下文标记

February 20, 2024

Secure Private Access 插件根据用户会话上下文（例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 应用程序的情境访问（智能访问）。

管理员可以在访问策略中添加带有上下文标记的条件。Secure Private Access 插件上的上下文标记是应用于经过身份验证的用户会话的 NetScaler Gateway 策略（会话、预身份验证、EPA）的名称。

Secure Private Access 插件可以将智能访问标记作为标头（新逻辑）或通过向网关进行回调来接收。有关详细信息，请参阅智能访问标记。

> 注意：
>
> Secure Private Access 插件仅支持可在 NetScaler Gateway 上配置的经典网关预身份验证策略。

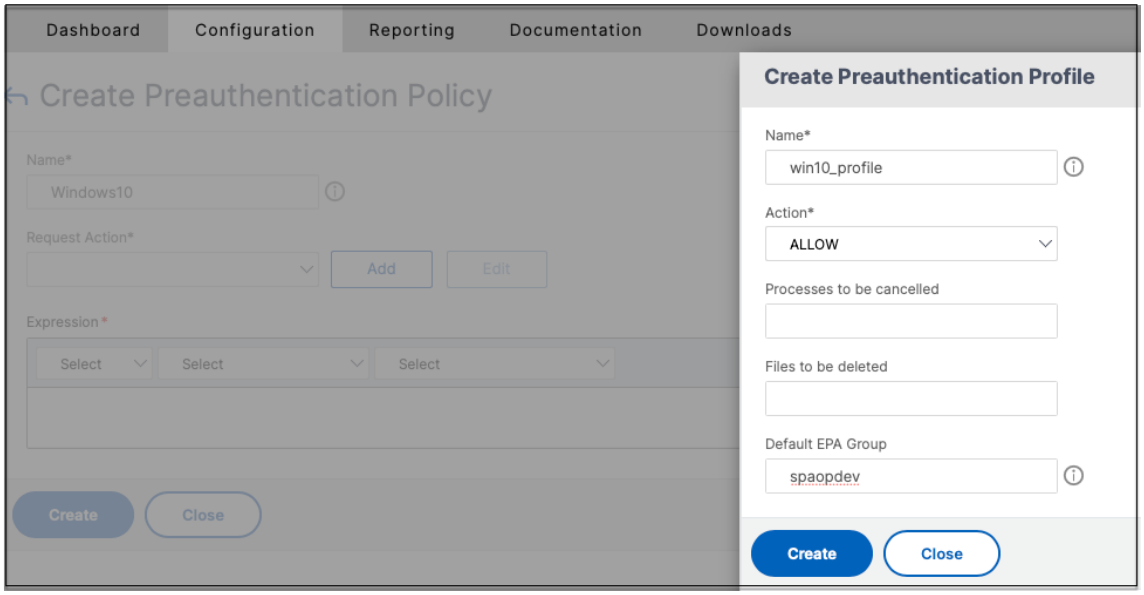
使用 **GUI** 配置自定义标记

配置上下文标记涉及以下高级步骤。

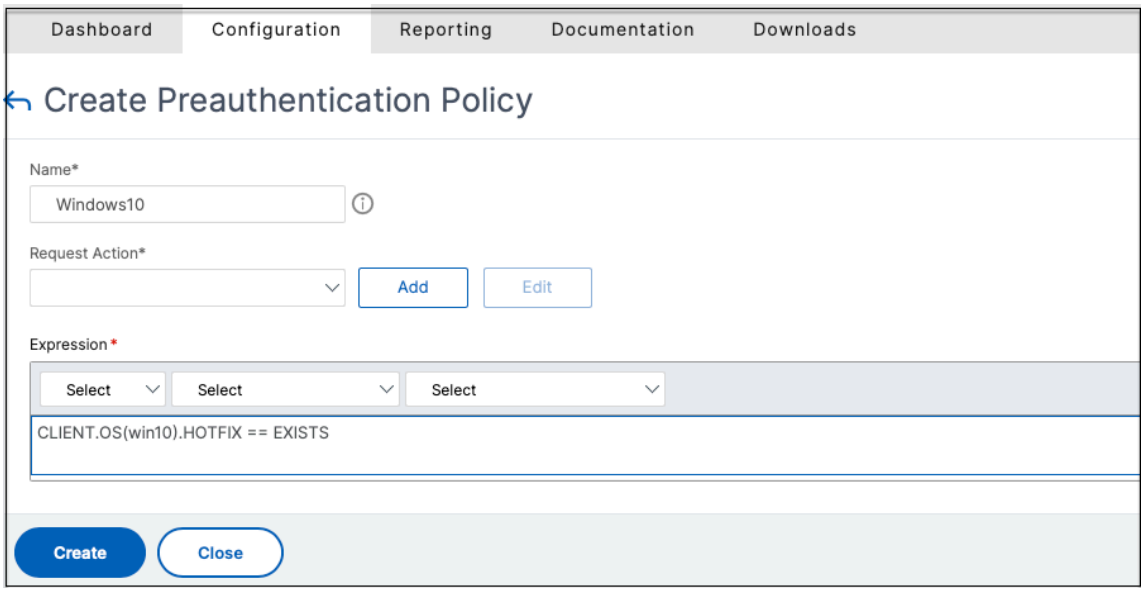
1. 配置经典网关预身份验证策略
2. 将经典预身份验证策略绑定到网关虚拟服务器

配置经典网关预身份验证策略

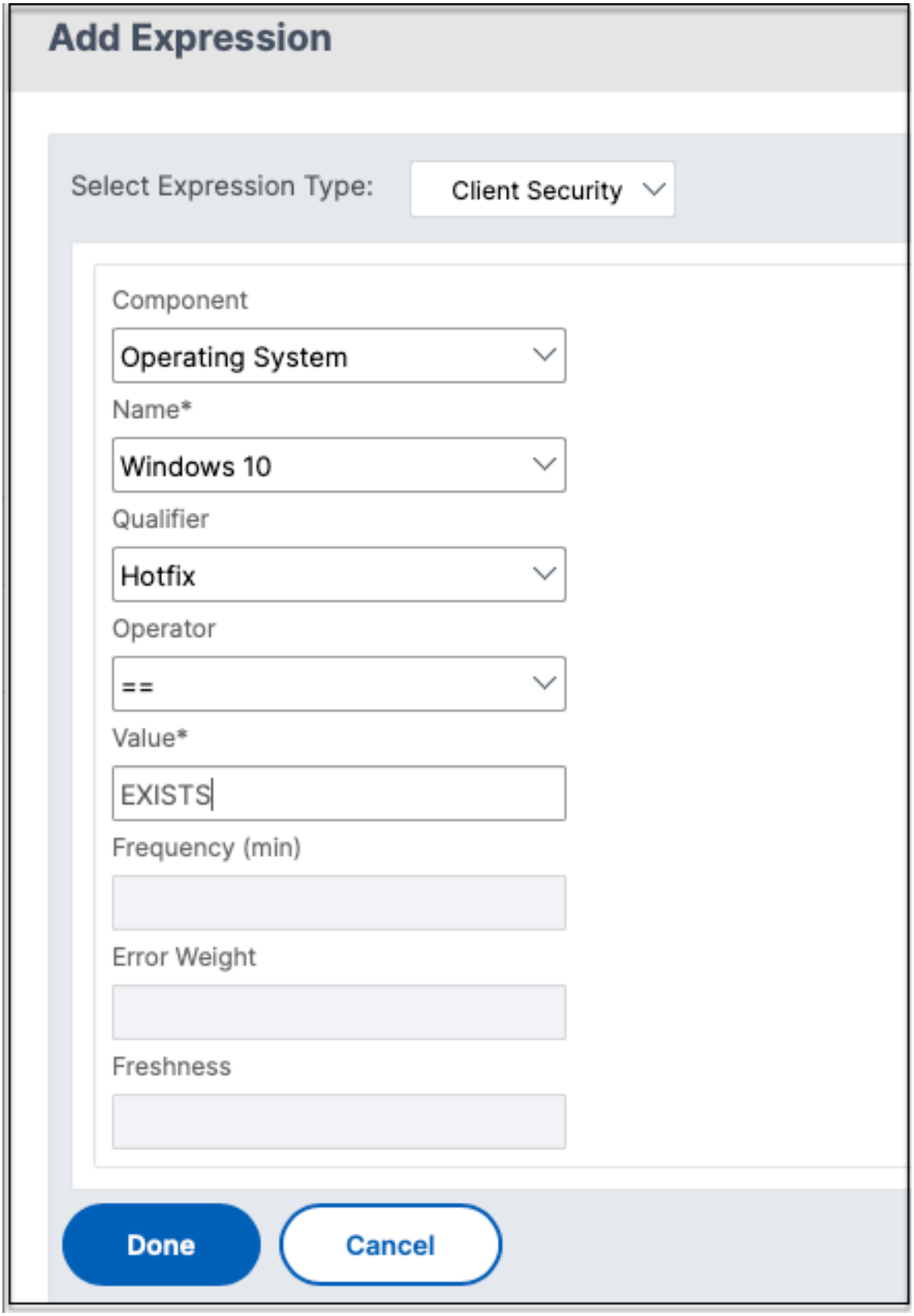
1. 导航到 **NetScaler Gateway >** 策略 **>** 预身份验证，然后单击添加。
2. 选择现有策略或为该策略添加名称。此策略名称用作自定义标记值。
3. 在请求操作中，单击添加以创建操作。您可以将此操作重复用于多个策略，例如，使用一个操作允许访问，使用另一个操作拒绝访问。



4. 在必填字段中填写详细信息，然后单击创建。
5. 在表达式中，手动输入表达式或使用表达式编辑器为策略构造表达式。



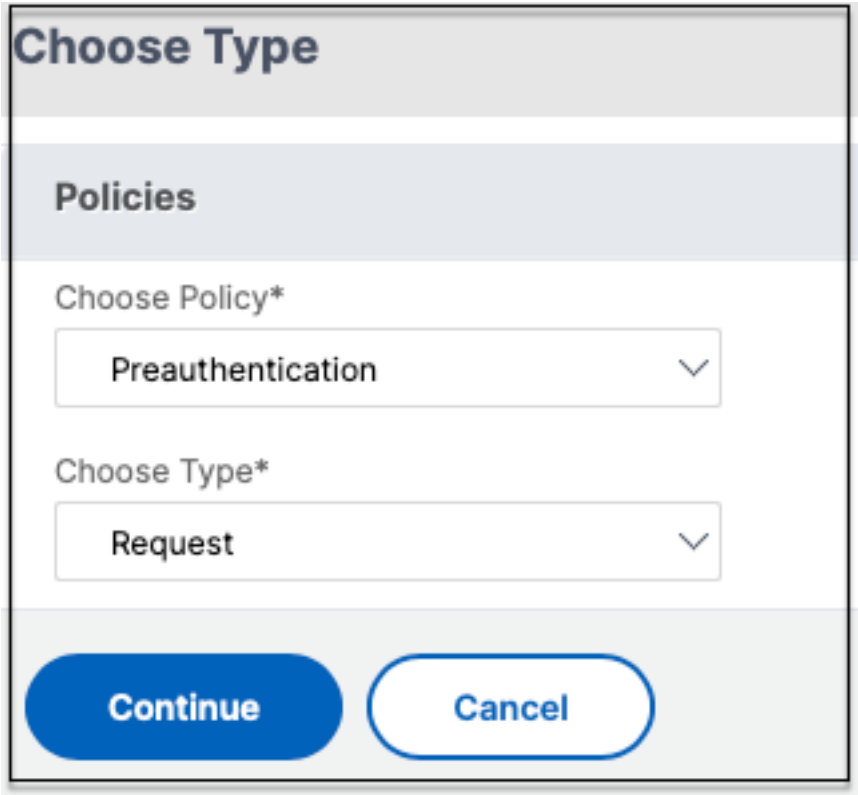
下图显示了为检查 Windows 10 操作系统而构造的示例表达式。



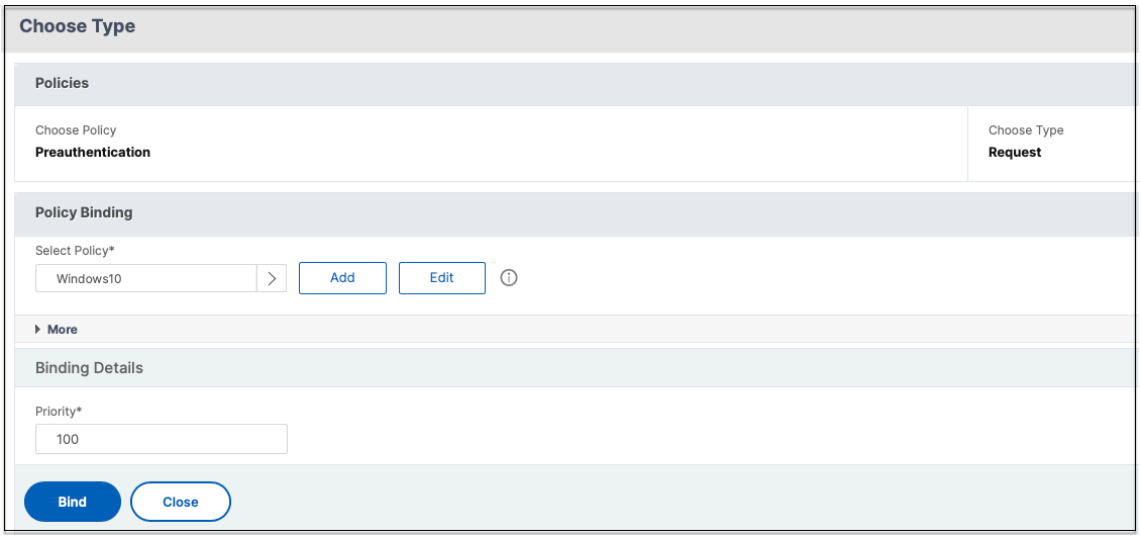
6. 单击创建。

将定制标记绑定到 **NetScaler Gateway**

1. 导航到 **NetScaler Gateway >** 虚拟服务器。
2. 选择要绑定预身份验证策略的虚拟服务器，然后单击编辑。
3. 在策略部分中，单击 **+** 绑定策略。
4. 在选择策略中，选择预身份验证策略，然后在选择类型中选择请求。



5. 选择策略名称和策略评估的优先级。
6. 单击绑定。



使用 **CLI** 配置自定义标记

在 NetScaler CLI 上运行以下命令来创建和绑定预身份验证策略：

示例：

- `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`

添加新的上下文标记

1. 打开 Secure Private Access 管理员控制台并单击访问策略。
2. 创建新策略或选择现有策略。
3. 在如果满足以下条件部分中，单击添加条件，选择上下文标记，全部匹配，然后输入上下文标记名称（例如，`Windows10`）。

引用

- 为应用程序配置访问策略。
- 支持智能访问标签。

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。

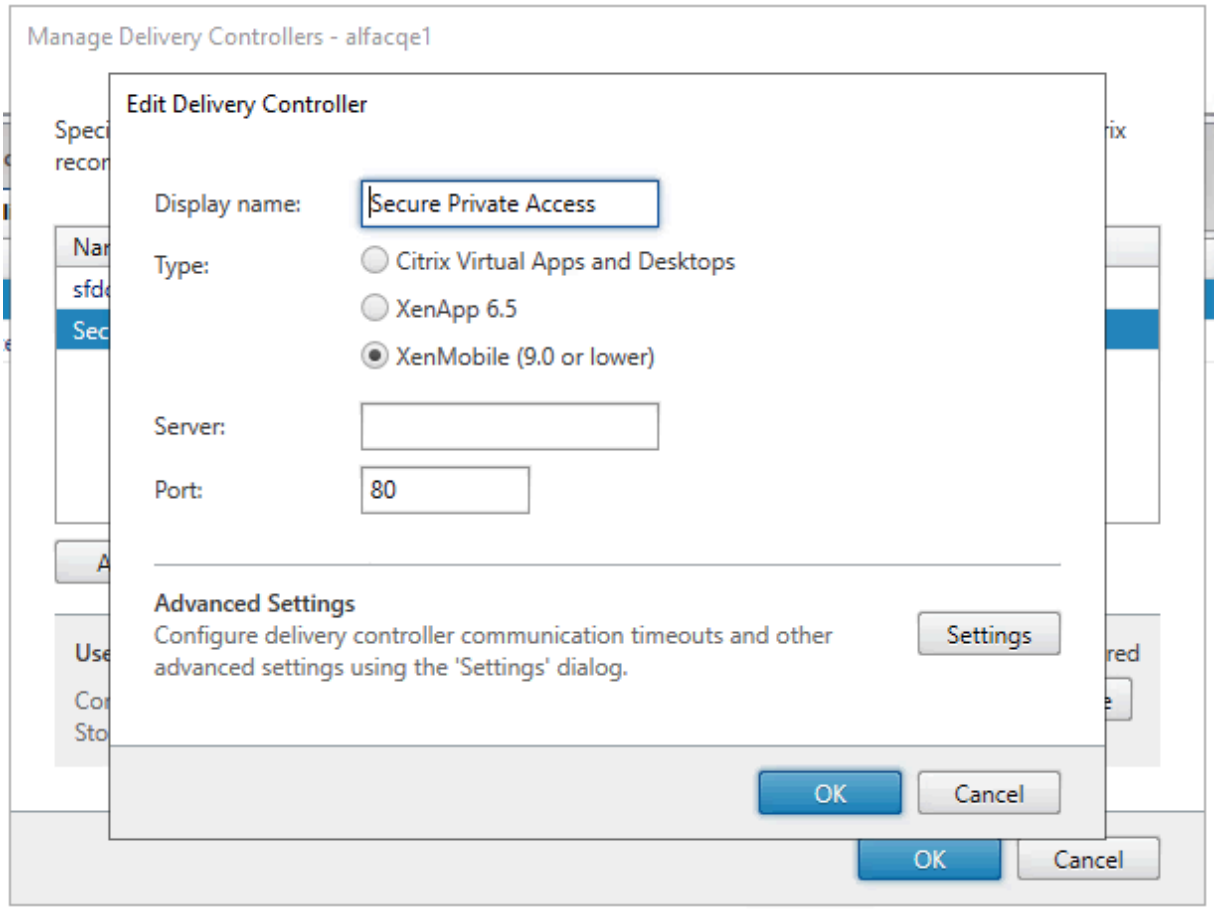
如果为 Citrix Virtual Apps and Desktops Delivery Controller 配置了 Secure Private Access 的聚合组设置，则 StoreFront 脚本会自动配置聚合组设置。默认情况下，该脚本为所有人配置 Secure Private Access（用户映射和多站点聚合配置 **>** 已配置）。

> 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。

Director

June 19, 2024

Director 与 Secure Private Access 的集成可以实现有效的性能监视和故障排除。要将 Director 与 Secure Private Access 集成，必须输入必须在 Secure Private Access 中注册的 Director 服务器的 FQDN 的 IP 地址。有关详细信息，请参阅集成服务器。

将 Director 注册到 Secure Private Access 权限是本地版本 2402 客户的 Secure Private Access 的强制性配置。如果您没有配置 Director，则必须安装最新版本的 Director，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，即 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 服务器以及在安装后管理设置。

> 注意：
>
> - Director 注册或登录不支持集成的 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。
> - 如果管理员手动登录到 Secure Private Access 控制台，则会利用这些详细信息对 Director 服务器进行身份验证。如果不成功，则系统会提示管理员输入凭据。
> - 如果管理员在设置完成后必须添加其他 Director，请从“管理设置”页面注册新的 Director。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、SSLv3 不支持单点登录。

使用 **Director** 配置工具使用 **Secure Private Access** 权限配置 **Director**

使用配置工具为 Director 配置 Secure Private Access 权限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 中查看查看 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。

许可证服务器

June 19, 2024

Secure Private Access 插件的许可证服务器是收集和处理许可数据所需的必备组件。许可证服务器可以在初始设置期间使用 Secure Private Access 注册，也可以在设置完成后进行配置或更新。有关使用 Secure Private Access 注册许可服务器的详细信息，请参阅集成 StoreFront 和 NetScaler Gateway 服务器以及在安装后管理设置。

要将 Secure Private Access 与许可证服务器连接，必须指定许可证服务器 URL。Secure Private Access 插件会自动在许可证服务器上注册自己。

> 注意：
>
> - 您必须在许可服务器上安装至少一个 Citrix Virtual Apps and Desktops 代理许可，才能在许可服务器上注册 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 11.17.2 版本 45000 版本或更高版本。

有关许可服务器的更多信息，请参阅许可服务器。

Web Studio

June 19, 2024

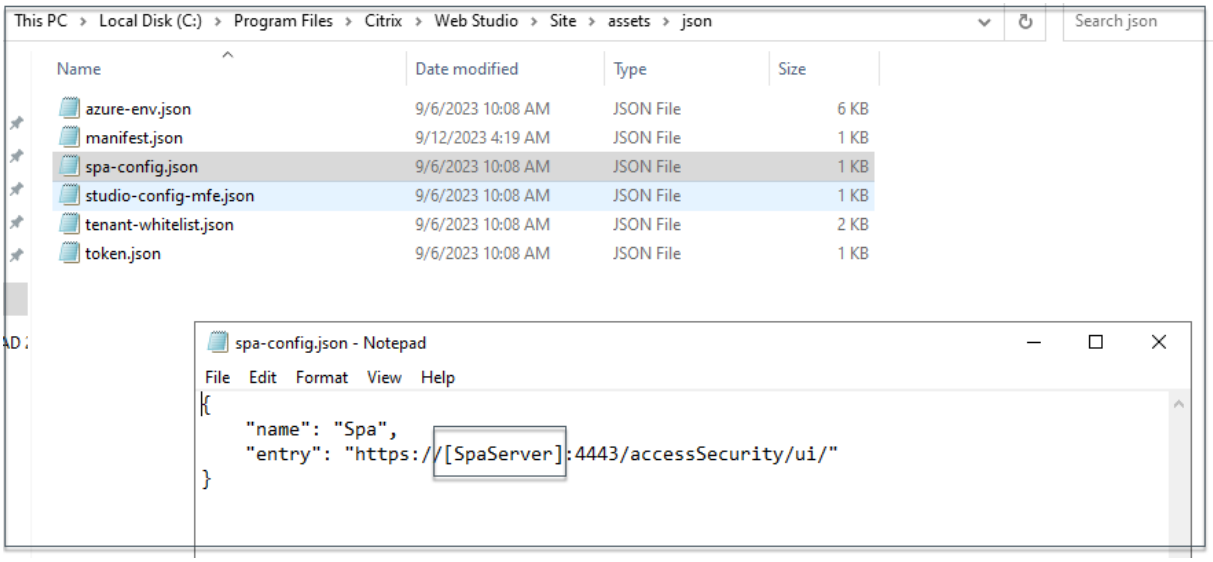
Citrix Secure Private Access 还集成到 Web Studio 控制台中，使用户能够通过 Web Studio 无缝访问该服务。

您必须安装 Web Studio 版本 2308 或更高版本。

执行以下步骤以启用 Web Studio 集成：

1. 使用 Citrix Virtual Apps and Desktops 安装程序或集成的 DDC 安装程序安装 Citrix Web Studio。
2. 按照屏幕上的说明完成安装。当提示输入控制器地址时，输入 DDC FQDN 作为控制器地址。
3. 成功安装后，导航到 C:\Program Files\Citrix\Web Studio\Site\assets\json 文件夹，然后修改 spa-config.json 文件的内容。

   如果使用非默认位置安装 Web Studio，请将 C:\Program Files\Citrix 中的默认安装位置替换为正确的位置。



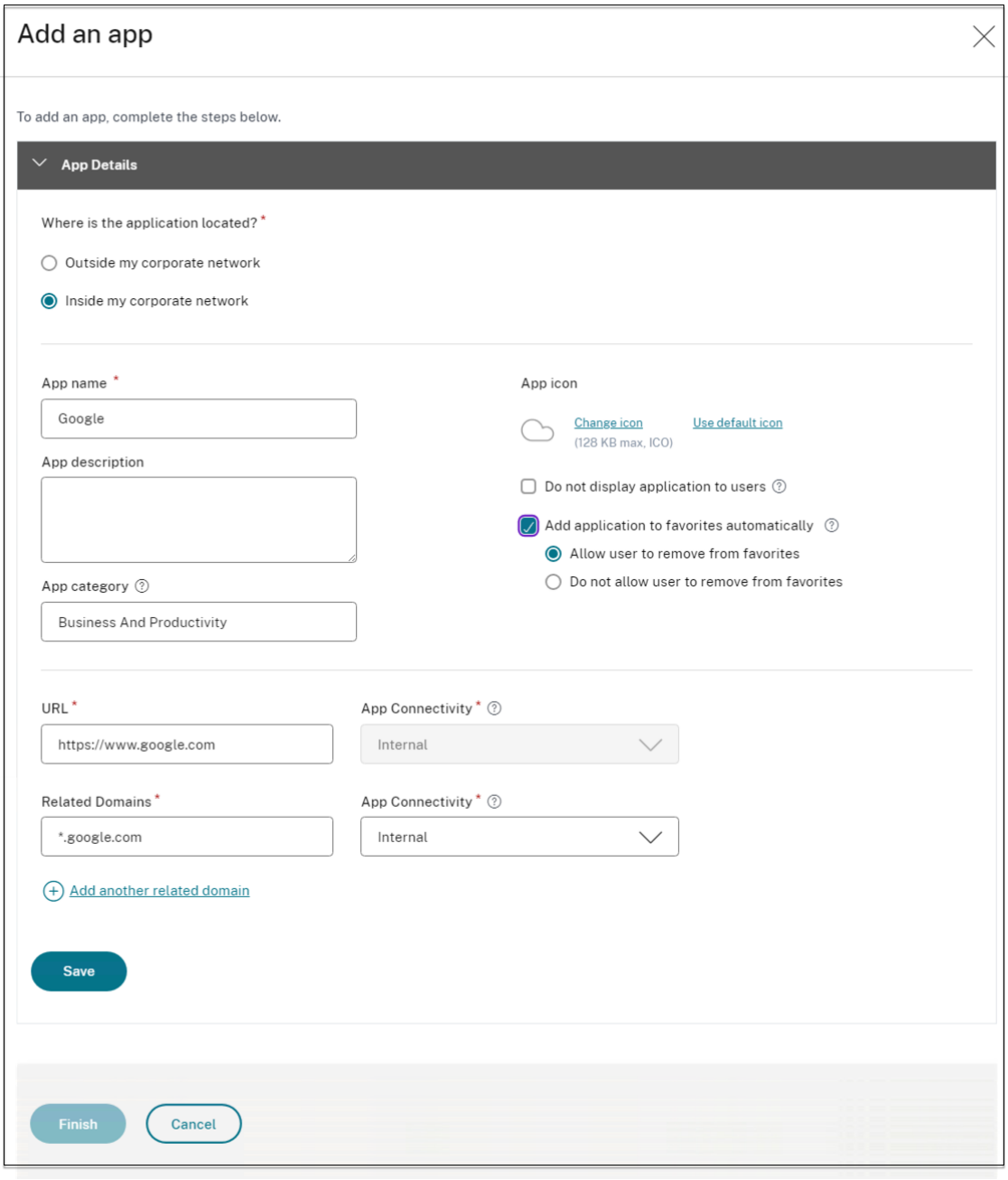
1. 将“SpaServer”替换为您的 Secure Private Access 插件的 FQDN。
2. 登录到 Web Studio。
3. 在左侧导航菜单上，单击“**Secure Private Access**”，从 Web Studio 访问 Secure Private Access 管理控制台。

配置应用程序

June 19, 2024

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

1. 在管理员控制台中，单击“应用程序”。
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 之外供外部应用程序使用。
   - 在我的公司网络 中，用于内部应用程序。
4. 在“应用程序详细信息”部分中输入以下详细信息，然后单击“下一步”。



- 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显示给您的用户。您也可以按以下格式输入应用程序的关键字：KEYWORDS： <keyword_name>。您可以使用关键字筛选应用程序。有关详细信息，请参阅按包含的关键字筛选资源。
- 应用程序类别 - 添加类别和子类别名称（如果适用），您发布的应用程序必须显示在 Citrix Workspace 用户界面中。您可以为每个应用程序添加新类别，也可以使用 Citrix Workspace 用户界面中的现有类别。为 Web 或 SaaS 应用程序指定类别后，该应用程序将显示在 Workspace 用户界面中的特定类别下。
  - 类别/子类别可由管理员配置，管理员可以为每个应用程序添加新类别。

  - 类别/子类别名称必须用反斜杠分隔。例如，业务与生产力\工程。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 用户界面中的名称与在 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错误地将业务和工作效率类别输入为业务和工作效率类别，则除业务和工作效率类别外，Citrix Workspace UI 中还会列出一个名为业务和工作效率的新类别。

- 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。
- **URL** —应用程序的 URL。
- 相关域 -根据应用程序 URL 自动填充相关域。管理员可以添加更多相关的内部或外部域。
- 自动将应用程序添加到收藏夹 -单击此选项可将此应用程序添加为 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，带有挂锁的星形图标将显示在应用程序的左上角。
  - 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，在 Citrix Workspace 应用程序中，该应用程序的左上角会出现一个黄色星形图标。
  - 不允许用户从收藏夹中删除 -单击此选项可防止订阅者从 Citrix Workspace 应用程序的收藏夹应用程序列表中删除该应用程序。

  如果您从 Secure Private Access 控制台中移除标记为收藏的应用程序，则必须手动将这些应用程序从 Citrix Workspace 的收藏列表中删除。如果将应用程序从 Secure Private Access 控制台中删除，则这些应用程序不会自动从 StoreFront 中删除。
- 应用程序连接 -为 Web 应用程序选择“内部”，为 SaaS 应用程序选择“外部”。

5. 单击“保存”，然后单击“完成”。

您可以查看在“设置” **>** “应用程序域”中配置的所有应用程序域。有关更多详细信息，请参阅 安装后管理设置。

后续步骤

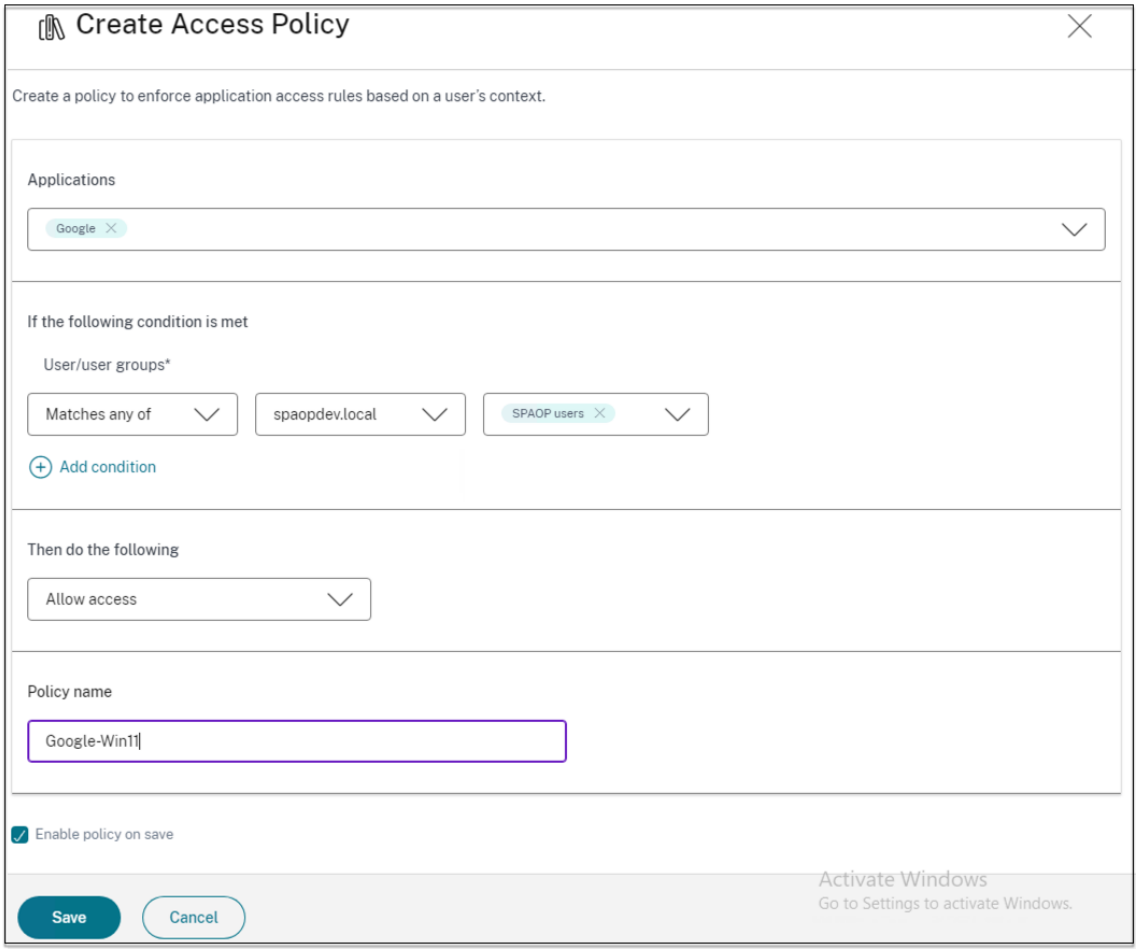
为应用程序配置访问策略

为应用程序配置访问策略

June 19, 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的限制访问。

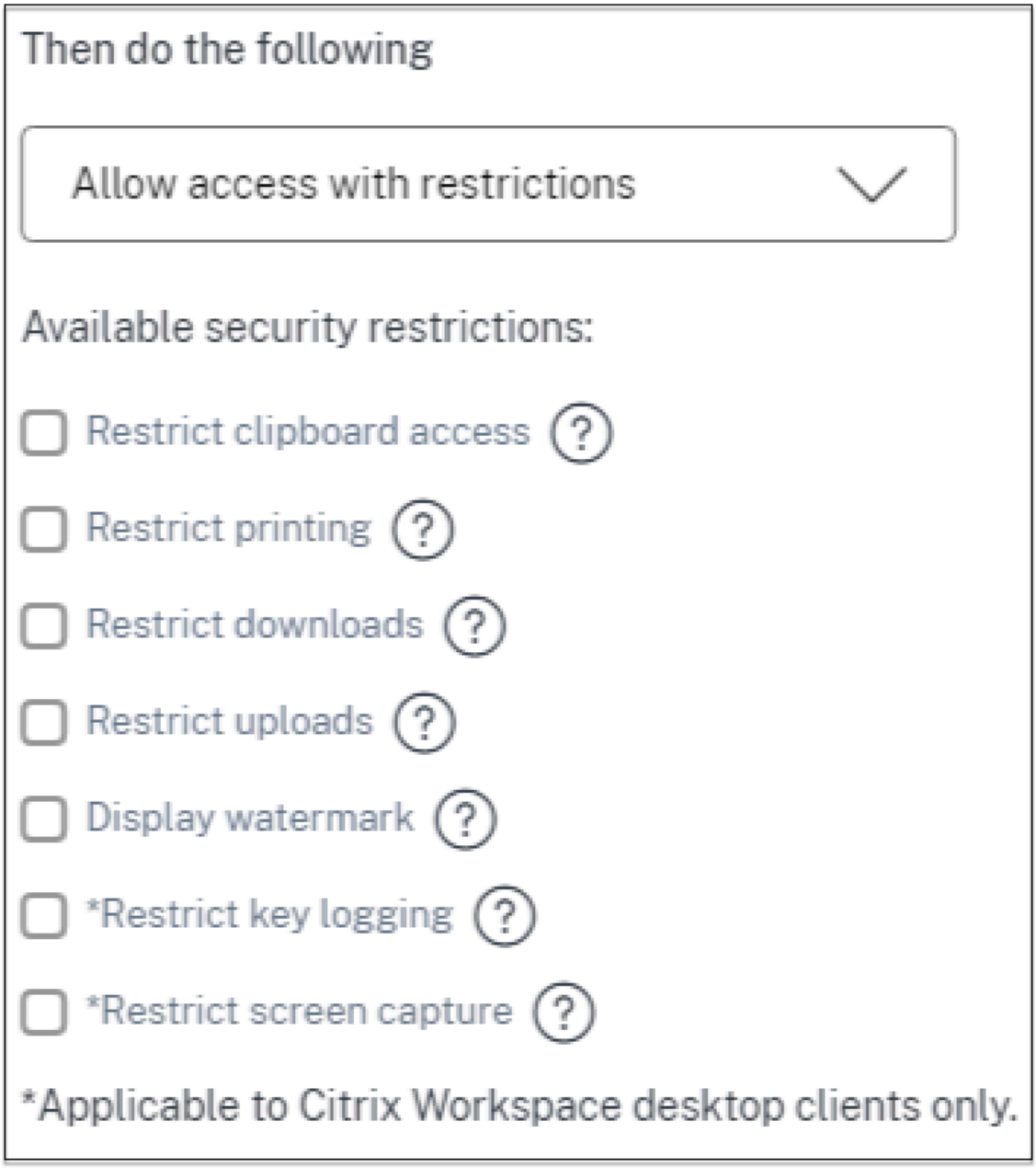
1. 在管理员控制台中，单击“访问策略”。
2. 单击创建策略。



3. 在 应用程序中，选择要强制执行访问策略的应用程序。
4. 在 用户/用户组 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。
5. 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。
6. 选择 条件标记，然后选择必须允许或拒绝应用程序访问所依据的条件。
7. 在“然后执行以下操作”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

选择“允许有限制的访问”时，可以选择以下限制。



- 限制剪贴板访问权限：禁用应用程序和系统剪贴板之间的剪切/复制/粘贴操作。
- 限制打印：禁用在 Citrix Enterprise Browser 中打印的功能。
- 限制下载：禁用用户从应用程序内下载的功能。
- 限制上载：禁用用户在应用程序内上载的权限。
- 显示水印：在用户屏幕上显示水印，显示用户计算机的用户名和 IP 地址。
- 限制按键记录：防范按键记录器。当用户尝试使用用户名和密码登录应用程序时，所有密钥都会在密钥记录器上加密。此外，用户在应用程序上执行的所有活动都受到密钥记录的保护。

例如，如果为 Office 365 启用了 App Protection 策略，并且用户编辑 Office 365 Word 文档，则所有按键记录器上的按键都经过加密。

- 限制屏幕截图：禁用使用任何屏幕捕获程序或应用程序捕获屏幕的功能。如果用户尝试捕获屏幕，则会捕获一个空白屏幕。

> 注意：
>
> 按键记录和屏幕截图限制仅适用于 Citrix Workspace 桌面客户端。

8. 在 策略名称中，输入策略的名称。
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。

配置验证示例

将 **Secure Private Access** 部署为群集

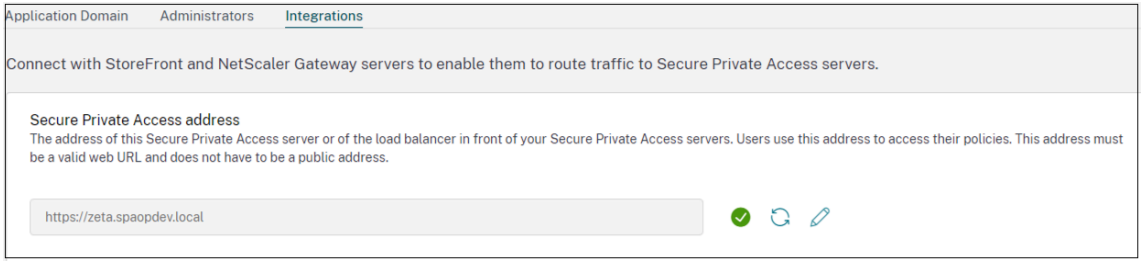
June 19, 2024

Secure Private Access 本地解决方案可以作为群集进行部署，以提供高可用性、高吞吐量和可扩展性。建议为大型部署（例如，超过 5000 名用户）部署独立的 Secure Private Access 节点。

创建 **Secure Private Access** 节点

- 创建一个新的 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。证书使用者常用名称或主题备用名称必须与负载平衡器 FQDN 相匹配。
- 在 Secure Private Access 中配置第一个节点时，使用负载平衡器名称。要添加后续节点，请在“集成”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。



负载平衡器配置

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 作为负载平衡器，请注意以下几点：

- 用于访问 StoreFront 的 FQDN 作为主题备用名称 (SAN) 包含在 DNS 字段中。如果您使用负载平衡器，则同时包括单个服务器的 FQDN 和负载平衡器 FQDN。这适用于 SSL 证书。对于 Secure Private Access，配置负载平衡器就足够了。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 应用商店。如果使用负载平衡器，请使用负载平衡器名称配置基本 URL，并使用 HTTPS 进行安全通信。有关详情，请参阅使用 HTTPS 保护 StoreFront。
- 建议使用 HTTPS 运行 Secure Private Access 服务，但这不是强制性要求。Secure Private Access 服务也可以作为 HTTP 部署。
- 支持 SSL 卸载或 SSL 桥接，因此可以使用任何负载平衡器配置。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，证书使用者公用名称或使用者备用名称 (SAN) 必须与负载平衡器 FQDN 相匹配。此外，必须在负载平衡器服务中配置 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（包括管理员和运行时）是无状态的，因此不需要持久性。
- 负载平衡器（例如 NetScaler）具有用于后端服务器的默认内置监视器（探测器）。如果您必须为 Secure Private Access 本地服务器配置基于 HTTP 的自定义监视器（探测器），则可以使用以下端点：

  `/secureAccess/health`

  预期回应：

```
Http status code: 200 OK

```



```
Payload:

{
"status":"OK","details":{
"duration":"00:00:00.0084206","status":"OK" }
 }

<!--NeedCopy-->
```

有关配置 NetScaler 负载平衡器的详细信息，请参见设置基本负载平衡。

为 **Secure Private Access** 创建监视器

使用以下 CLI 命令为 Secure Private Access 创建监视器。

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

创建监视器后，将证书绑定到显示器。

有关使用 NetScaler 用户界面创建监视器的详细信息，请参阅创建监视器。

卸载 **Secure Private Access**

June 19, 2024

您可以从“控制面板”**>**“程序”**>**“程序和功能”中卸载“Secure Private Access”。

1. 选择 **Citrix Virtual Apps and Desktops 7 2402 —Secure Private Access**。
2. 单击卸载。
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，请从管理控制台下载 StoreFrontScripts.zip 文件，从 StoreFront 应用商店配置中删除 Secure Private Access 插件。

要下载 StoreFrontScripts 压缩文件，请按照以下步骤操作：

1. 登录到 Secure Private Access 管理控制台。
2. 单击“设置”，然后单击“集成”选项卡。
3. 在 StoreFront 应用商店 URL 部分单击下载脚本。

从 **StoreFront** 应用商店配置中移除 **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 StoreFront 计算机。
2. 下载 StoreFrontScripts.zip 文件。
3. 将 StoreFrontScripts.zip 解压到一个文件夹。
4. 使用管理员权限打开 PowerShell 窗口。
5. 运行以下命令：

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

升级

June 19, 2024

您可以将 Secure Private Access 部署升级到更新的版本，而无需先设置新的计算机或站点。在升级之前，我们建议您创建快照或保存配置。要开始升级，您需要从新版本运行安装程序来升级之前安装的 Secure Private Access 插件。

升级顺序

升级顺序如下所示：

1. 您可以通过 Delivery Controller 升级 Secure Private Access，也可以根据最初安装 Secure Private Access 的方式通过安装程序用户界面中的专用“Secure Private Access”图块升级。
   - 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 图块安装了 Secure Private Access，则可以单独对其进行升级。有关详细信息，请参阅升级您的 Secure Private Access 安装程序。

   > 注意：
   >
   > 我们建议您通过适用于 POC 环境的 Delivery Controller 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，以便您可以调整新特性或功能。

2. 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。
3. 再次运行 StoreFront 配置。从“设置”**>**“配置”下载 StoreFront 脚本，然后在相应的 StoreFront 计算机上运行这些脚本。有关详细信息，请参阅修改集成设置。

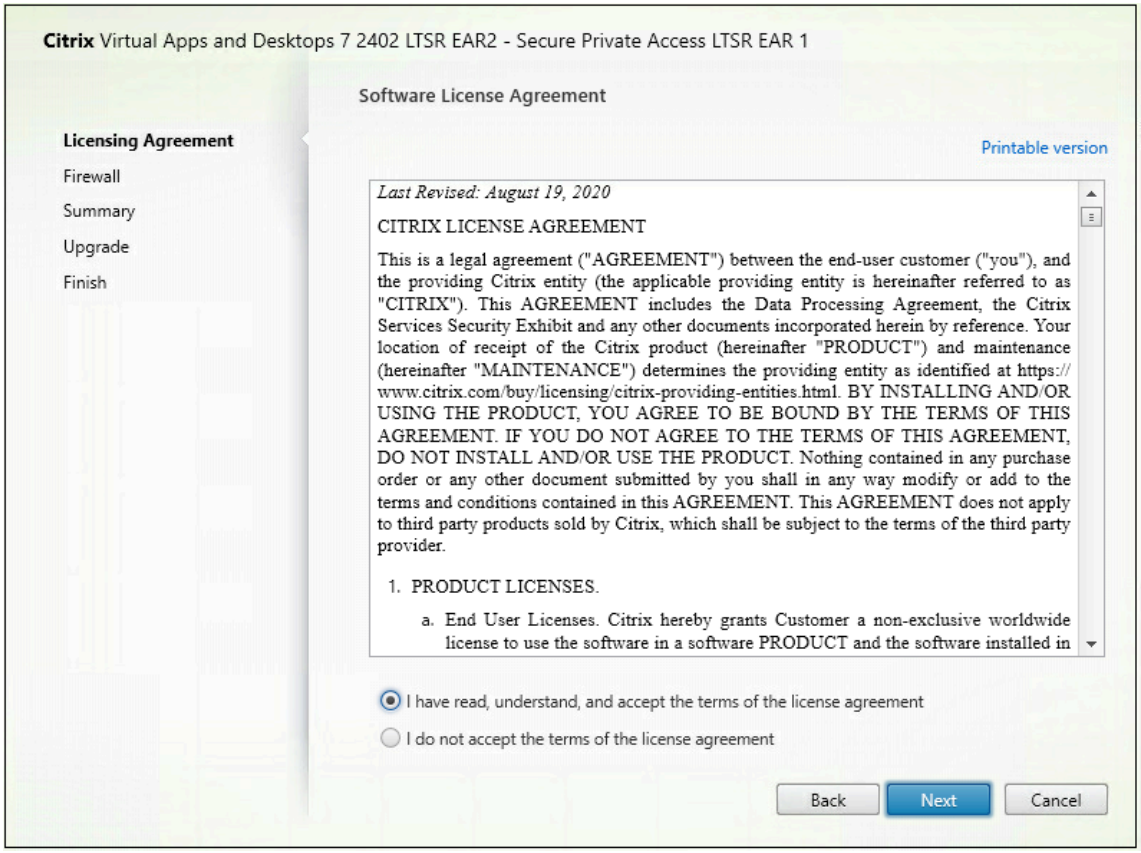
> 注意：
>
> 如果您不运行脚本，则不会触发端点。

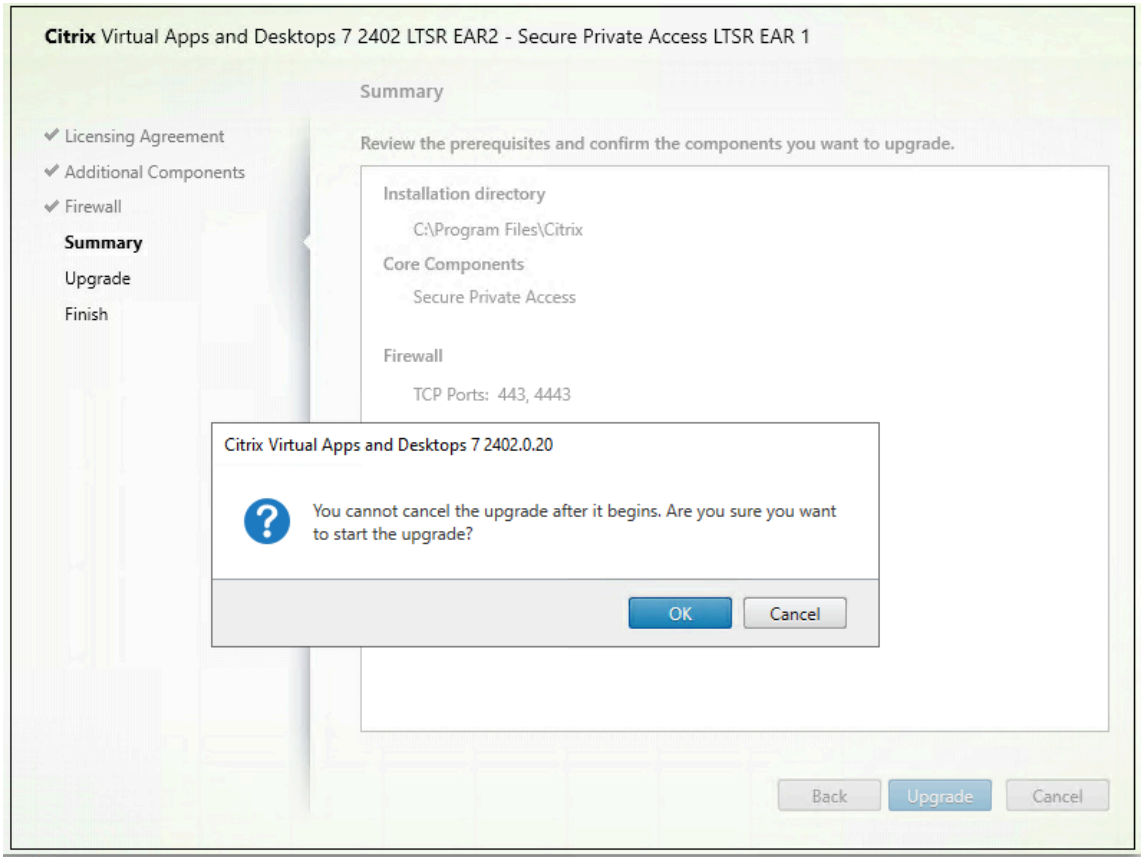
4. （可选）运行 NetScaler Gateway 脚本。有关详细信息，请参阅 NetScaler Gateway。

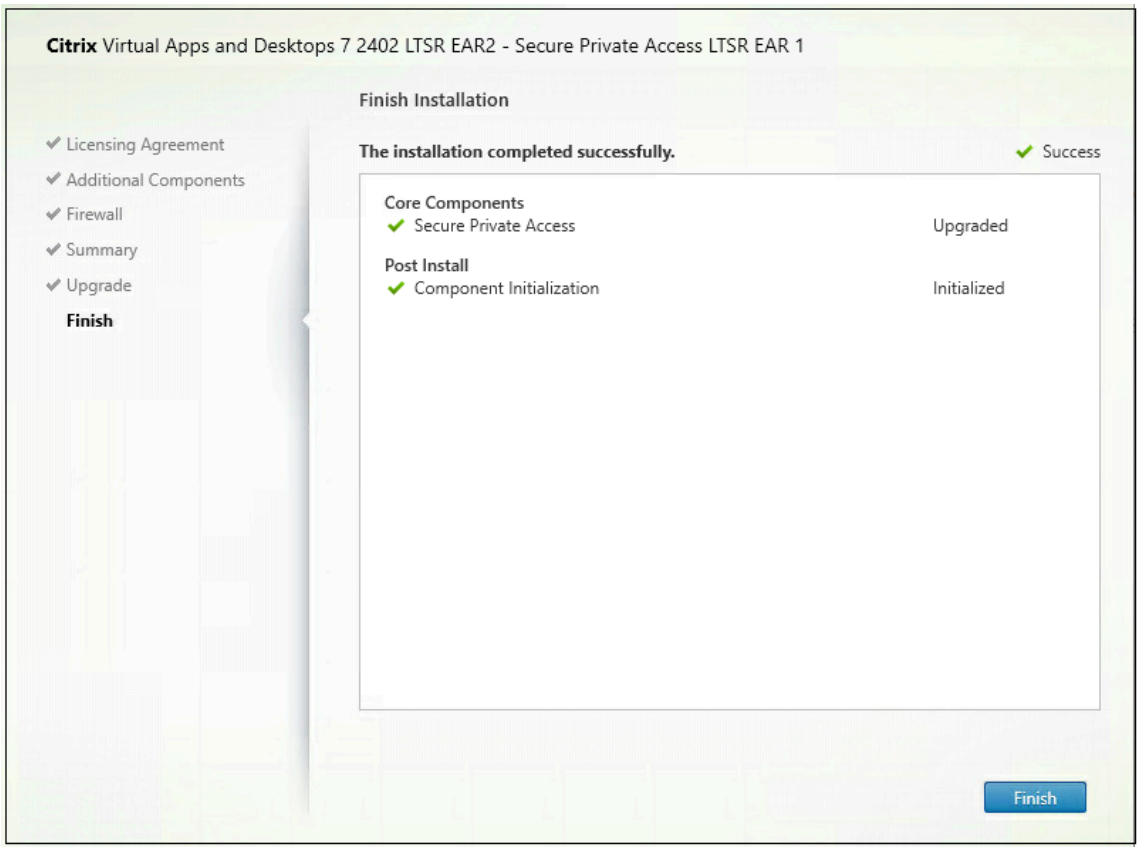
升级您的 **Secure Private Access** 安装程序

June 19, 2024

1. 从 https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/中下载 Citrix Secure Private Access 2402 安装程序。
2. 在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：
>
> 将安装程序升级到版本 2402 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 Secure Private Access
- 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

June 19, 2024

安装 Secure Private Access 后，可以从“设置”页面修改设置。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，必须使用 Secure Private Access 管理员帐户登录 Secure Private Access 管理员控制台。

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

安装后管理设置

June 19, 2024

管理应用程序域的路由

您可以查看在 Secure Private Access 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的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 Secure Private Access 权限的管理员将被授予完全权限。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，以便为该组中的所有管理员启用访问权限。

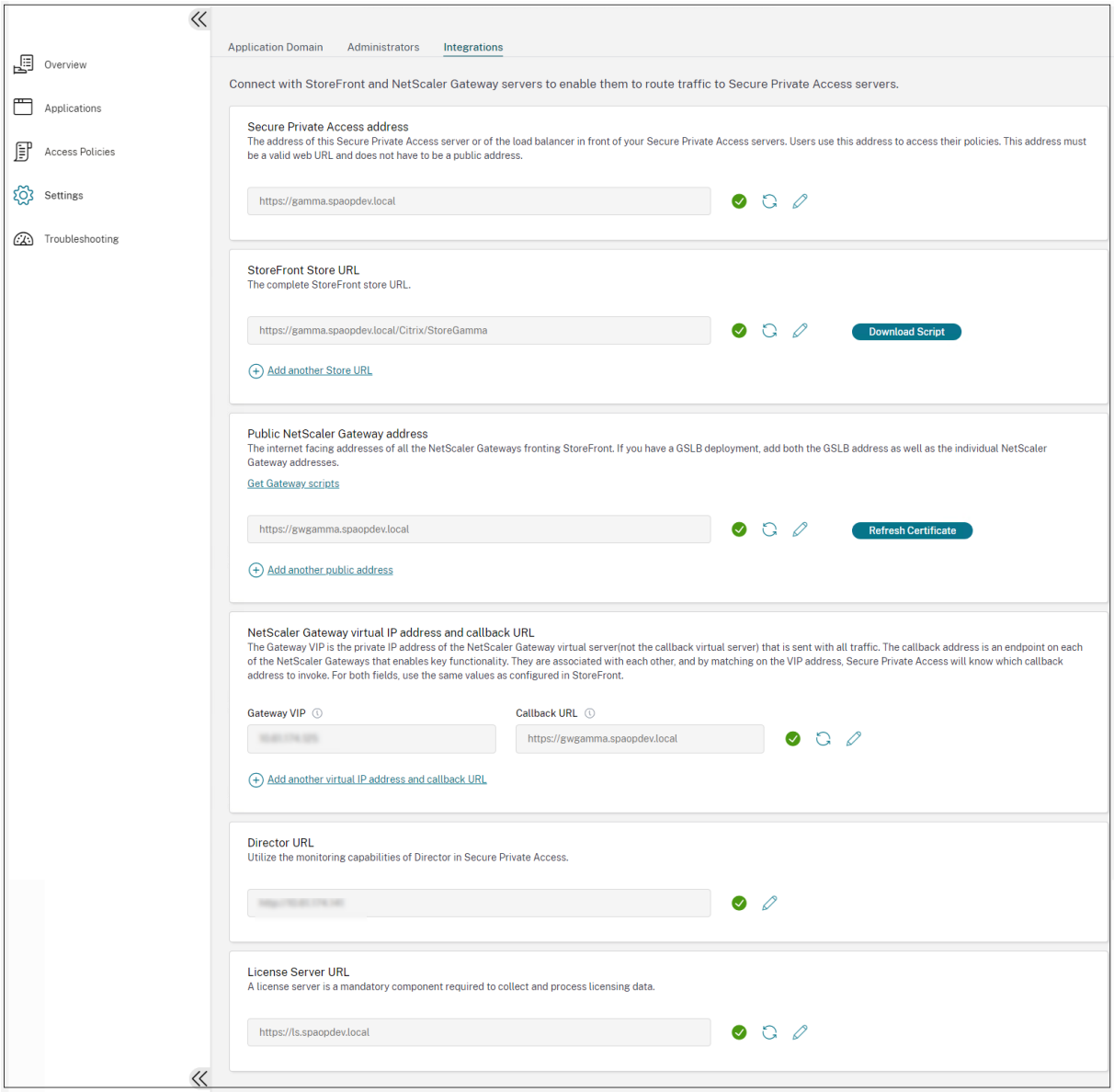
1. 在管理员页面中，单击添加。
2. 在 域中，选择必须将该管理员添加到的域。
3. 在用户或用户组中，选择该用户所属的用户或组。
4. 在 管理员类型中，选择必须分配给该用户的权限类型。

修改集成设置

设置 Secure Private Access 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. 单击符合您要修改的设置的编辑图标，然后更新条目。
3. 单击“刷新”图标以确保设置有效。

> 注意：
>
> 如果 Secure Private Access 安装在与 StoreFront 不同的计算机上，请下载 StoreFront 脚本并在 StoreFront 上运行。



管理应用程序和策略

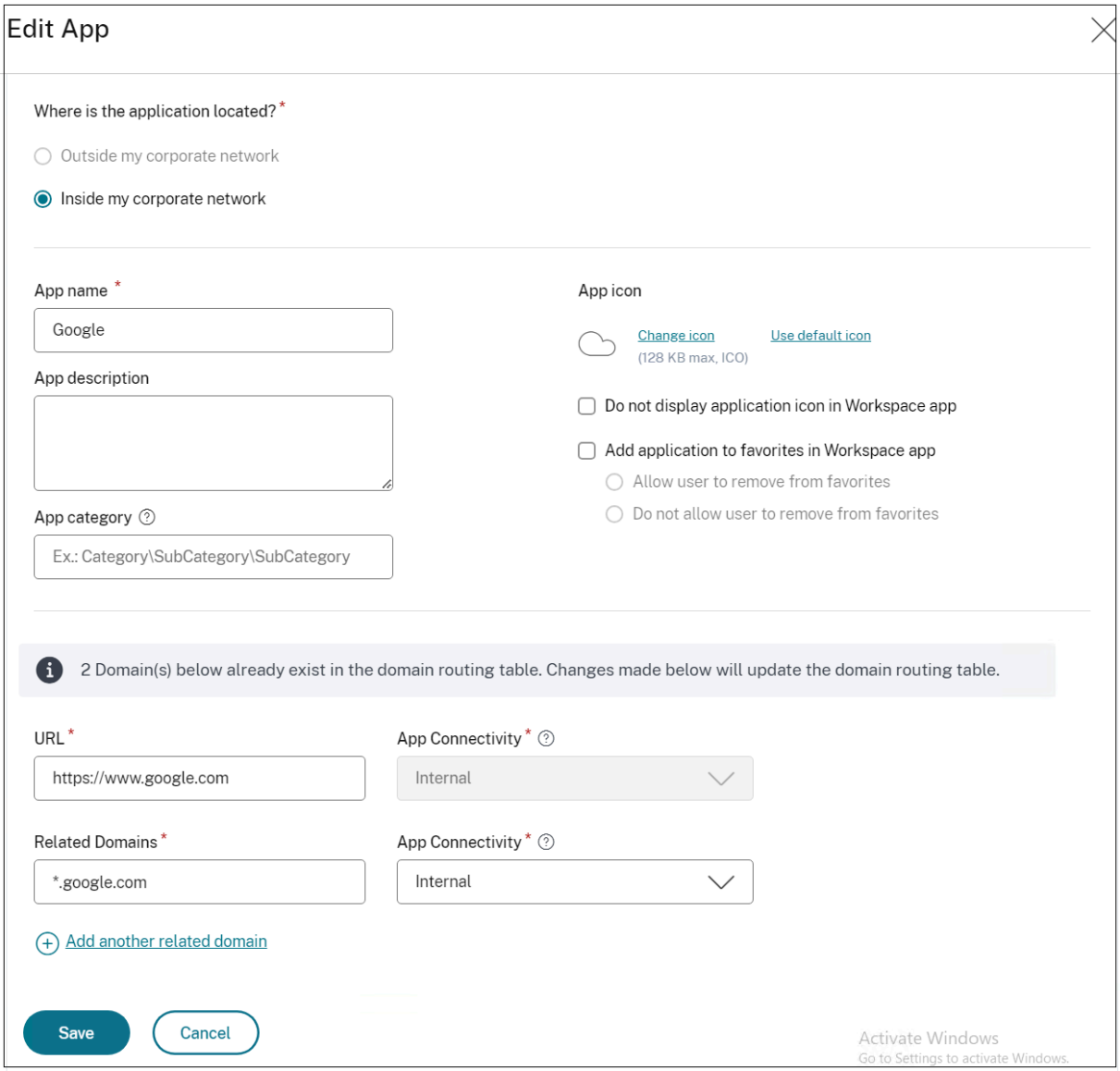
June 19, 2024

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

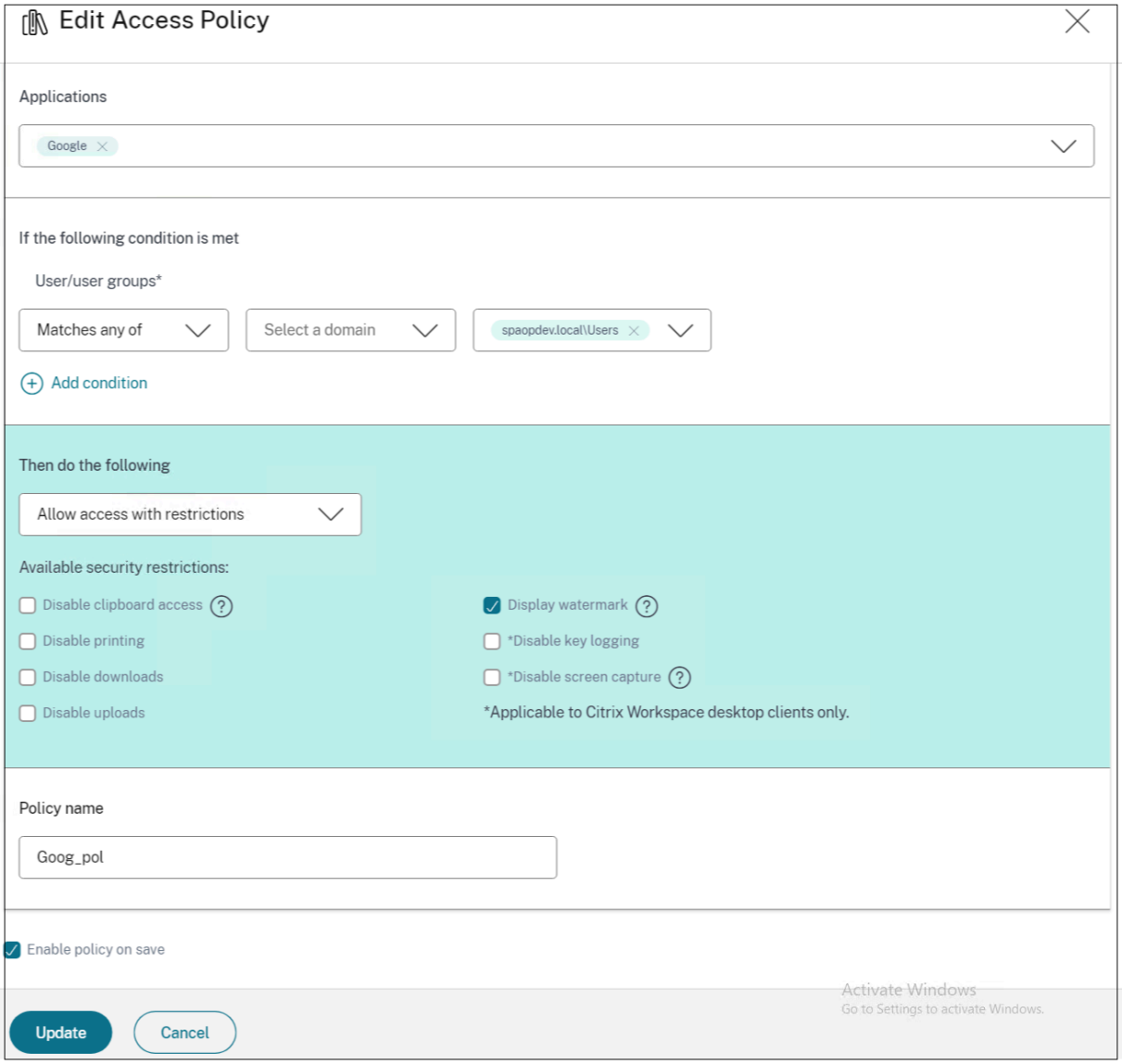
1. 在 Secure Private Access 管理员控制台中，单击“应用程序”。

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

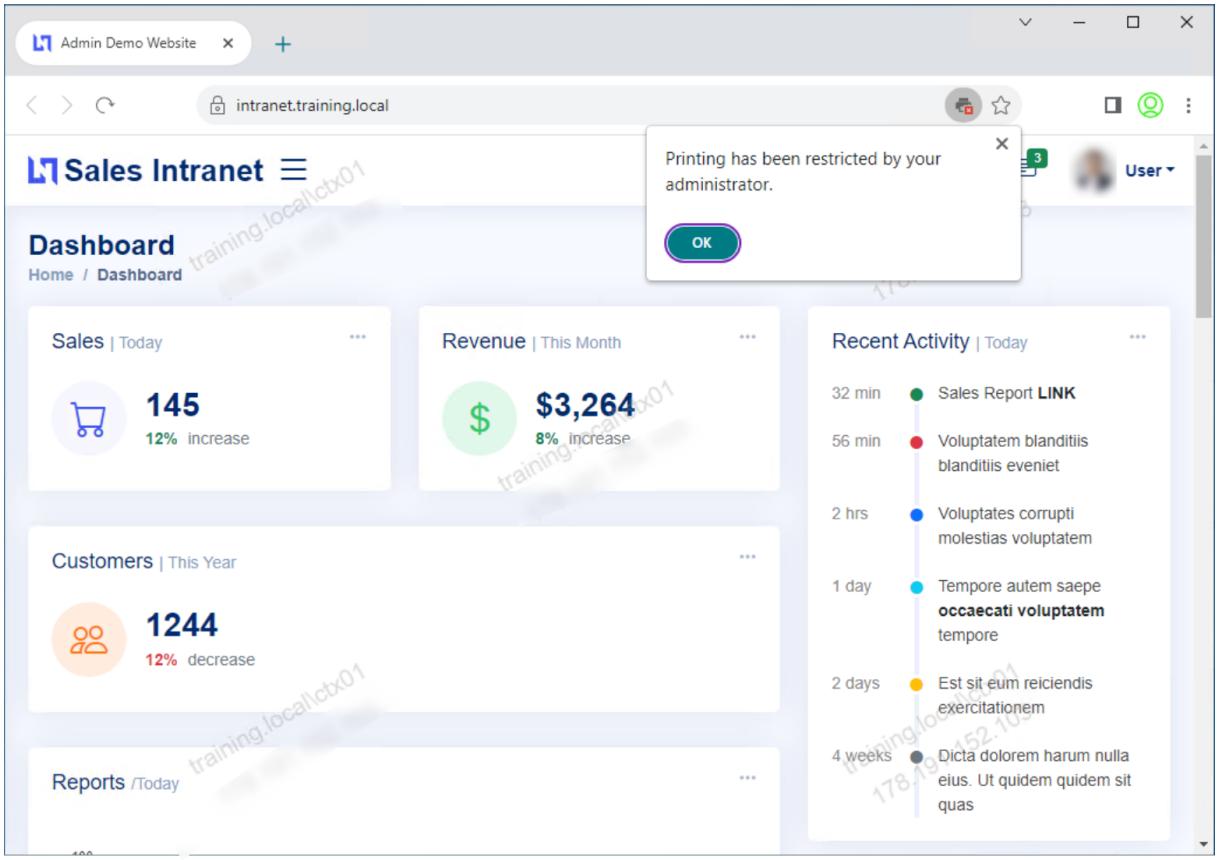
1. 在“Secure Private Access”管理员控制台中，单击“访问策略”。
2. 单击与要修改的策略对应的省略号按钮，然后单击“编辑访问策略”。
3. 编辑策略详情。
4. 单击更新。



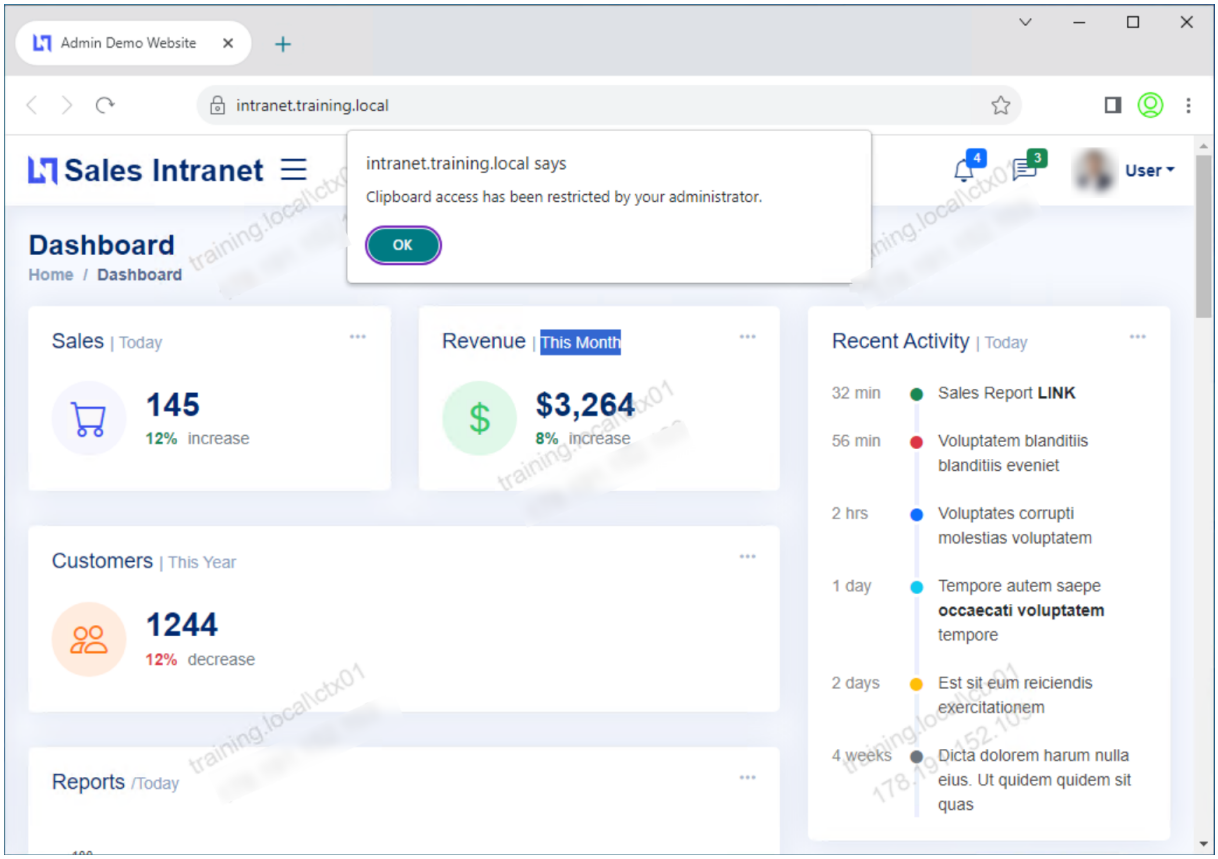
最终用户流程

June 19, 2024

假设您已经为具有剪贴板访问和打印限制的应用程序创建了访问策略。现在，当最终用户从 StoreFront 访问该应用时，该应用会在 Citrix Enterprise Browser 中打开，用户可以使用该应用。但是，如果用户尝试从应用程序打印，则会显示以下消息。



同样，如果用户尝试访问剪贴板，则会显示以下消息。



> 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。

监视和故障排除

June 19, 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。

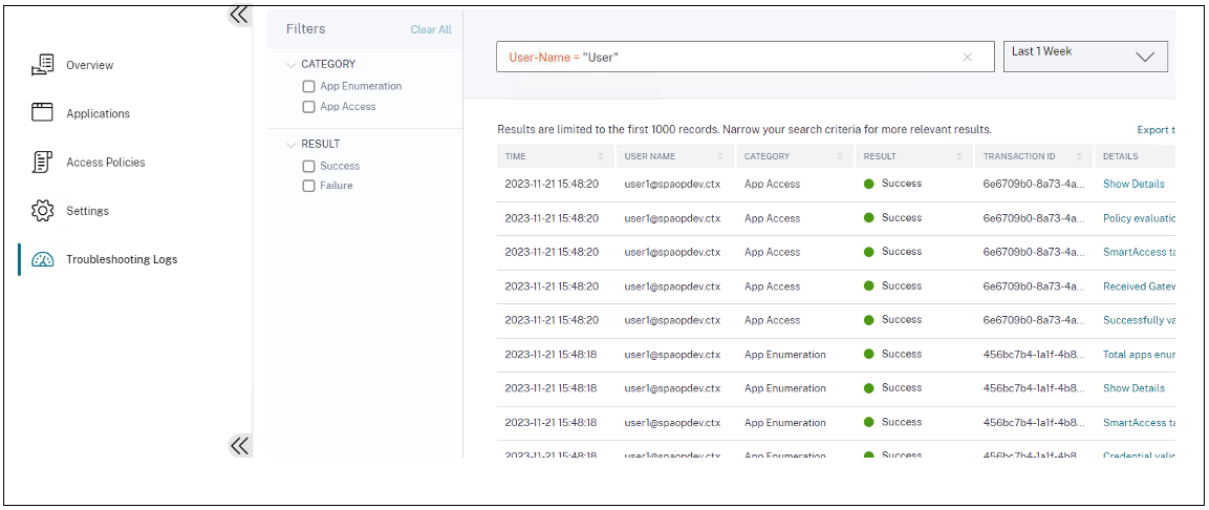
控制板概述

June 19, 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。

您可以查看预设时间或自定义时间轴的日志。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。

您可以使用过滤器（类别和结果）来优化搜索结果。



您还可以根据以下参数以及搜索字段中的运算符来细化搜索。

- 用户名称
- 类别
- 事件类型
- 结果
- Transaction-ID
- 详细信息

以下是搜索运算符，您可以使用这些运算符在用户日志和按强制执行的顶级访问策略图表中细化搜索范围。

- =：搜索与搜索条件完全匹配的日志/策略。
- !=：搜索不包含指定条件的日志/策略。
- ~：搜索与搜索条件部分匹配的日志/策略。
- !~：搜索不包含某些指定条件的日志/策略。

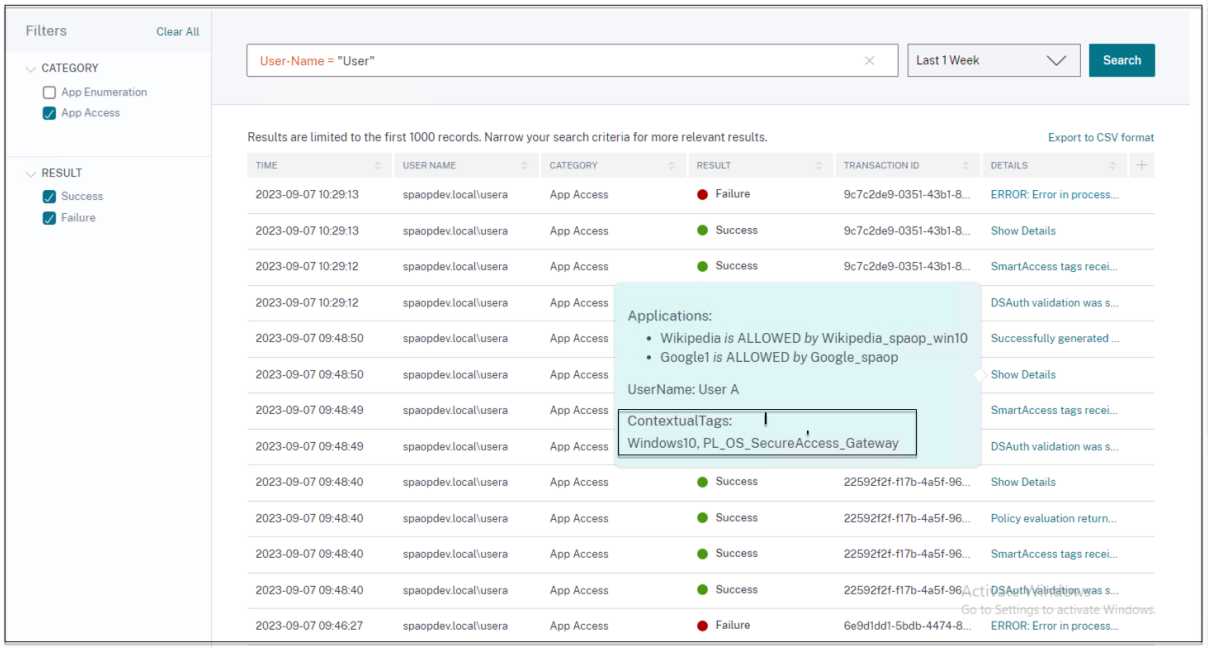
例如，您可以通过在搜索字段中使用字符串 **Event-Type = DSAuth** 来搜索事件类型“DSAuth”。

同样，要搜索部分包含“运算符”一词的用户，请使用字符串 **User-Name ~ operator**。此搜索列出了所有包含“操作员”一词的用户名。例如，“本地操作员”、“管理员操作员”

您可以使用事务 ID 搜索与单个事件相关的所有日志。交易 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 筛选故障排除日志，以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。



基本故障排除

June 19, 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** 解决问题

June 19, 2024

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。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 Secure Private Access 会话

> 注意：
>
> - 第二位数字中包含“0”的代码表示正常的执行流程。例如，1000 表示成功的应用程序枚举。
> - 第二位数字中包含“1”的代码表示失败或异常。例如，2101 表示会话失败。对于故障或异常，建议您通过检查日志来解决此类问题。如果仍无法解决问题，请联系支持人员。

与枚举相关的代码

代码	状态	说明
1101	失败	枚举期间出现内部错误。
1102	失败	一些应用程序已枚举，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，并且至少有一个应用程序评估失败。
1000	成功	枚举成功。至少列举了一个应用程序。
1001	成功	没有列举任何应用程序，因为它们都被策略拒绝。
1002	成功	没有列举任何应用程序，因为没有匹配的策略。
1003	成功	没有列举任何应用程序，因为有些应用程序被拒绝，而对于另一些应用程序，则没有匹配的策略。
1004	成功	没有列举任何应用程序，因为没有可供评估的策略。

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/处于非活动状态。

应用程序枚举消息代码

代码	状态	说明
3101	失败	应用程序枚举 - 出现内部错误（当前未使用）。
3102	失败	由于在策略评估期间出现异常，因此未枚举应用程序。

代码	状态	说明
3103	失败	应用程序枚举状态为空-策略评估期间出现内部错误。
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	拒绝	应用程序枚举被策略拒绝。
3002	拒绝	应用程序未枚举，因为没有匹配的策略。
3003	未知	应用程序枚举状态未知。
3004	CEB 推出应用程序	尝试从 Citrix Enterprise Browser 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-应用程序启动期间出现内部错误
4102	失败	应用程序启动错误（内部）
4103	允许/拒绝/失败	检索应用程序的策略详细信息时出错
4000	允许	允许启动应用程序。
4001	拒绝	由于策略原因，应用程序启动被拒绝。
4002	拒绝	应用程序启动被拒绝，因为没有匹配的策略。

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：

```
  "TroubleshootingLogs": {

    "CleanupPeriodInHours": 12,
    "CleanupDataOlderThanDays": 7,
    "CleanupOldestDataIfEntriesCountAbove": 0
   }

<!--NeedCopy-->
```

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
      }

<!--NeedCopy-->
```

> 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