



Citrix Secure Private Access - 本地

Contents

技术概况介绍	8
组成部分	9
新增功能	10
2024 年 12 月	10
2024 年 7 月	10
支持 TCP/UDP 应用程序	10
与 Citrix Scout 诊断和支持工具的集成	10
Web Studio 集成的增强功能	10
使用情况遥测报告的增强功能	11
已知问题	11
Domain Controller configurations	11
NetScaler® Gateway	11
RfWeb / 用于 Web 的工作区	12
应用程序启动	12
店面™	12
日志记录	12
启用 TCP/UDP 监控功能标志	13
升级	13
系统必备条件	14
先决条件	15
管理员帐户要求	15
通信端口要求	16
参考资料	18
调整大小指南	18
数据库存储空间要求	18
服务器配置	19

主机存储	19
流量配置文件	19
部署指导方针	20
其他组件的配置设置	21
安装安全私有访问	22
单点登录到管理控制台	22
后续步骤	23
组成部分	24
斯托弗，特朗	24
使用 StoreFront 2308 或更早版本时	25
使用 StoreFront 2311 或更高版本时	26
网思乐网关	26
与 ICA® 应用程序的兼容性	26
支持智能访问标签	27
配置安全专用访问切换开关	27
在 NetScaler 上保留安全私有访问插件设置	28
在 NetScaler Gateway 上启用安全私有访问插件	29
将公共网关证书上传	29
已知的限制	29
NetScaler Gateway 配置，用于网页/软件即服务应用程序	30
更新现有 NetScaler Gateway 网页和软件即服务应用程序配置	31
NetScaler 网关 虚拟服务器设置	32
NetScaler 网关会话策略设置	32
更多详细信息	34
NetScaler 网关 针对 TCP/UDP 应用程序的配置	35
更新现有 NetScaler 网关 的 TCP/UDP 应用程序配置	35
有关更多信息	38
上下文标签	38

使用 GUI 配置自定义标签	38
使用 CLI 配置自定义标签	39
添加新的上下文标签	40
参考资料	40
许可证服务器	40
思杰安全访问™ 客户端	41
导向器（可选）	41
使用 Director 配置工具来对 Director 进行配置，以使其能够与 Secure Private Access 功能进行集成	42
在 Director 中查看安全私有访问用户会话	42
将安全私有访问部署为集群（可选）	42
创建安全私有访问节点	42
负载均衡器配置	43
为安全私有访问创建监视器	44
配置安全私有访问插件	45
设置安全专用访问	45
先决条件	45
通过创建新站点设置安全专用访问	45
步骤 1：设置安全专用访问站点	45
步骤 2：配置数据库	46
步骤 3：集成服务器	47
步骤 4：配置摘要	48
通过加入现有站点设置安全私有访问	48
禁用 HTTP2 设置	49
多域环境的部署	49
如何配置服务帐户	50
后续步骤	50
配置 Web/SaaS 应用程序	50

后续步骤	52
配置 TCP/UDP 应用程序	52
配置 TCP/UDP 应用程序的访问策略	55
配置针对应用程序的访问策略	55
访问策略优先级	56
后续步骤	56
访问限制配置选项	56
剪贴板	56
复制	57
按文件类型下载限制	57
下载内容	58
不安全内容	58
键盘记录保护	58
麦克风	58
通知设置	59
粘贴	60
个人数据屏蔽	60
弹出窗口	61
打印	62
打印机管理	62
屏幕捕获	63
按文件类型限制上传	63
上传	64
水印功能	65
网络摄像头	65
针对安全组的剪贴板功能限制	65
最终用户流程	69
SaaS 应用程序	69

TCP/UDP 应用程序	69
升级	71
升级顺序	71
组件的升级	72
升级您的安全私有访问安装程序	72
后续步骤	72
使用脚本升级数据库	72
管理配置	74
管理未经批准的网站	74
管理安装完成后的各项设置	74
管理应用程序域的路由	74
管理管理员用户	74
修改集成配置的各项设置	75
管理应用程序和策略	75
编辑应用程序	75
编辑访问策略	75
未经批准的网站	76
未经批准的网站的工作原理	76
配置未经授权网站的规则	77
卸载安全私有访问	77
从 StoreFront 商店配置中删除安全私有访问插件	78
监控和故障排除	79
故障排除	79
Director 中的会话相关代码	79
参考资料	79
仪表板概览	79
从日志中查看上下文标记	80
基本故障排除	80

证书相关错误	81
数据库创建错误	81
思杰店面故障	82
公共网关/回调网关故障	84
安全私有访问服务器不可访问	84
数据库连接检查失败	84
网关连接性检查失败。未能成功获取公共证书	85
应用程序枚举失败	85
其他事项	85
首次设置未能成功完成	85
创建安全私有访问诊断支持捆绑包	85
安全私有访问的 SQL 数据库权限	86
更改故障排除日志的日志级别	87
应用程序启动问题或 Citrix Secure Access 登录失败	88
Director 中的安全私有访问会话代码	88
会话代码	88
应用程序枚举相关代码	89
应用程序启动消息代码	90
SIEM 集成	91
引用	92
斯科特集成	92
日志保留设置	93
自定义故障排除日志的保留设置	93
日志和遥测清理	94
遥测数据清理	94
CDF 日志清理	94
CDF 日志的自定义清理	94
第三方通知事项	96

技术概况介绍

Citrix Secure Private Access 本地部署版是一个客户管理的零信任网络访问 (ZTNA) 解决方案，它提供对内部 Web/SaaS 和 TCP/UDP 应用程序的安全访问，并具有以下功能以及无缝的最终用户体验：

- SaaS 和内部 Web 应用程序的无 VPN 访问
- 最小权限管理原则
- 单点登录 (SSO)
- 多因素身份验证
- 设备姿态评估功能
- 应用程序级安全控制
- 应用程序保护功能

该解决方案使用 StoreFront 本地部署版和 Citrix Workspace 应用程序，以实现在 Citrix Enterprise Browser 中访问内部 Web/SaaS 和 TCP/UDP 应用程序的无缝且安全的访问体验。此解决方案还使用 NetScaler Gateway 来强制执行身份验证和授权控制。

Citrix Secure Private Access 本地部署版解决方案通过使用 StoreFront 本地部署版门户作为统一访问门户，轻松地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）提供零信任访问，以及作为 Citrix Workspace 集成部分的虚拟应用程序和桌面，从而增强了组织的整体安全性和合规性态势。

Citrix 安全私有访问™ 结合了 网络加速器 网关 和 StoreFront 的各项功能，为最终用户和管理员提供集成式体验。

功能特性	负责提供此功能的服务/组件
访问应用程序的一致 UI	本地部署 StoreFront/思杰工作区应用程序
SaaS 和 Web 应用程序的单点登录	网络加速器® 网关
多重身份验证 (MFA) 和设备状态 (又称端点分析)	网思乐网关

功能特性	负责提供此功能的服务/组件
适用于 Web 和 SaaS 应用程序的安全控制和应用程序保护控制	Citrix 企业浏览器™
访问授权策略	安全私有访问
访问强制执行	网思乐网关和思杰安全访问客户端
配置与管理	安全私有访问
可见性、监控和故障排除	安全私有访问、NetScaler 控制台（原名 ADM）和 Citrix 导向器

组成部分

此图显示了典型的 Secure Private Access 部署的组件。



有关每个组件的信息，请参阅[主要组件](#)。

新增功能

2024 年 12 月

- 支持 FIPS 平台上的安全私有访问本地部署解决方案

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

2024 年 7 月

支持 TCP/UDP 应用程序

Secure Private Access 经过增强，除了 Web/SaaS 应用程序之外，还支持 TCP/UDP 应用程序。最终用户现在可以通过安装在其设备上的 Citrix Secure Access 客户端访问这些应用程序。

有关详细信息，请参阅以下主题：

- [Citrix 安全访问客户端](#)
- [配置 TCP/UDP 应用程序](#)
- [配置应用程序的访问策略](#)

与 Citrix Scout 诊断和支持工具的集成

Citrix Secure Private Access™ 现已与 Citrix Scout 集成。此集成有助于管理员收集日志和指标以进行故障排除。有关详细信息，请参阅[Scout 集成](#)。

Web Studio 集成的增强功能

Citrix Secure Private Access 与 Web Studio 控制台之间的集成功能现已得到显著增强，从而使得用户能够通过 Web Studio 无缝访问此项服务。有关详细信息，请参阅[将 Secure Private Access 与 Web Studio 集成](#)。

使用情况遥测报告的增强功能

遥测报告功能得到增强，可用于收集和分析客户管理的客户环境中 Citrix 产品、组件和功能的许可使用情况数据。此增强功能可确保 Citrix 产品部署符合许可协议。

要使用此功能，您必须更新到最新版本的许可证服务器。有关详细信息，请参阅以下主题：

- [思杰许可遥测](#)
- [所需的许可证服务器更新](#)
- [Citrix 许可证遥测常见问题解答](#)
- [Citrix 许可遥测数据元素](#)

已知问题

版本 2407 中存在以下问题。

注意：

某些问题仅出于内部参考目的分配了跟踪 ID，这些问题对客户没有任何影响。

Domain Controller configurations

- 不支持在不同 AD 林中的域之间建立信任类型为“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 安装在域已加入 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。
- 如果安装了本地 Secure Private Access 的计算机域与登录到 Secure Private Access 的管理员域不同，则必须执行以下操作：

为 Secure Private Access 管理员和运行时服务在 IIS 应用程序池中添加一个不同的域服务帐户作为身份。
- 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 不会在管理控制台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，如果相应的域不可访问或域名不是有效名称，则不支持该域。

NetScaler® Gateway

- 在以下场景中不支持带有 SSL 配置文件配置的 SSL 虚拟服务器。
 - 客户正在使用 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` 切换已启用。

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，或者禁用

`ns_vpn_enable_spa_onprem` 切换。

有关此切换的详细信息，请参阅[支持智能访问标签](#)。

RfWeb / 用于 Web 的工作区

- 不支持 RfWeb / Web 版 Workspace，因此未枚举应用程序。有关详细信息，请参阅[使用 StoreFront 2311 或更高版本时](#)。

应用程序启动

- 如果未启用 `ns_vpn_enable_spa_onprem` 和 `toggle_vpn_enable_securebrowse_client_mode` 旋钮，或者 NetScaler Gateway 不支持这些旋钮，则在 `CustomHeaderCryptoKey` 轮换后应用程序启动将失败。
`CustomHeaderCryptoKey` 轮换会在 30 天后自动发生。
- 如果 LDAP UPN 和 sAMAccountName 不同，则应用程序启动失败。

店面™

- 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，网站的默认接收器设置为空值，这不适用于 Secure Private Access。此外，客户端上会显示早期版本的 Receiver 用户界面。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 > 管理交付控制器** 页面会将 Secure Private Access 插件类型显示为 **XenMobile®**。这不影响功能。

日志记录

- 针对集群的支持包生成不受支持。
- 不得删除管理员和运行时服务的日志文件夹。如果这些文件夹被删除，Secure Private Access 无法重新创建它们。

启用 TCP/UDP 监控功能标志

- 在 2407 版本中，**SPAOP-3315-EnableZTNAApplications** 功能标志默认处于禁用状态。因此，TCP/UDP 监控数据未存储，导致 Director 集成失败。

解决方法：如果您正在使用 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。

升级

- 升级到 2407 后，如果您编辑一个 URL 以 `www` 开头的现有应用程序，则“应用程序连接”字段不会填充之前的状态。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，之后配置将被保存并持续存在。

- 升级到 2407 后，尽管您可以登录管理控制台，但无法管理应用程序和策略。此时会显示错误消息。

解决方法：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](#)。

- 升级到 2407 后，应用程序枚举和应用程序启动失败。

解决方法：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](#)。

- 如果插件是使用交付控制器安装的，则无法将安全私有访问插件从早期版本升级到 2407。

系统必备条件

请确保您的产品满足最低版本要求。

产品	最低版本
思杰工作区™ 应用	Windows – 2403 及更高版本
	macOS – 2402 及更高版本
思拓锋™	LTSR 2203 或 CR 2212 及更高版本
网思乐	13.1、14.1 及更高版本。建议使用 NetScaler Gateway 13.1 或 14.1 版本的最新版本以优化性能。
	对于 TCP/UDP 应用程序 - 14.1–25.56 及更高版本
网思乐 FIPS	13.1-37.219 及更高版本的 FIPS 版本
Citrix 安全访问客户端	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
监控器	2402 或更高版本
安全私有访问插件服务器的操作系统	Windows Server 2019 and later

通信端口： 确保已为 Secure Private Access 插件打开所需的端口。有关详细信息，请参阅[通信端口](#)。

注意：

- The Secure Private Access for on-premises is not supported on Citrix Workspace app for iOS and Android.
- 适用于 Linux、iOS 和 Android 的思杰安全访问客户端不支持本地部署的安全私有访问 TCP/UDP 应用程序。

先决条件

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

- 一台运行 IIS 并配置了 SSL/TLS 证书的 Windows 服务器，Secure Private Access 插件将安装在此服务器上。
- 设置期间要输入的 StoreFront 商店 URL。
- StoreFront 上的商店必须已配置，并且商店服务 URL 必须可用。商店服务 URL 的格式为 `https://store.domain.com/Citrix/StoreSecureAccess`。
- NetScaler Gateway IP address, FQDN, and NetScaler Gateway Callback URL.
- Secure Private Access 插件主机（或在 Secure Private Access 插件以群集形式部署时使用的负载均衡器）的 IP 地址和完全限定域名。
- 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已完成。如果在计算机中未找到证书，Secure Private Access 安装程序会配置自签名证书。但是，这可能并非总是有效。

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。这些设置由 Secure Private Access 安装程序默认设置，不得手动更改。

管理员帐户要求

在设置 Secure Private Access 期间，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，该域用户也是安装 Secure Private Access 的计算机的本地计算机管理员。
- 管理安全私有访问：您必须使用安全私有访问管理员帐户登录安全私有访问管理控制台。

通信端口要求

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

源	目的地	类型	端口	详细信息
管理员工作站	安全专用访问插件	超文本传输安全协议	4443	安全私有访问插件 - 管理控制台
安全私有访问插件	NTP 服务	TCP协议, UDP 协议	123	时间同步功能
	DNS 服务	TCP, UDP	53	DNS 查找
	活动目录	TCP, UDP	88	科尔贝罗斯协议
	监控器	HTTP, HTTPS	80, 443	与 Director 通信，用于性能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，用于收集和许可数据
		TCP	389	LDAP（通过明文传输）(LDAP)
		TCP	636	基于安全套接字层的LDAP (LDAPS)
	微软 SQL 服务器	TCP	1433	安全私有访问插件 - 数据库通信

源	目的地	类型	端口	详细信息
	思拓方	超文本传输安全协议	443	身份验证有效性验证
	纳思达网关	超文本传输安全协议	443	NetScaler Gateway Callback
思杰店面	NTP 服务	TCP, UDP	123	时间同步服务
	DNS 服务	TCP协议、UDP 协议	53	DNS 查找
	活动目录	TCP协议、UDP 协议	88	科尔贝罗斯
		TCP	389	使用明文协议进行的 LDAP 通信 (LDAP)
		TCP	636	使用 SSL 协议进行的 LDAP 通信 (LDAPS)
		TCP, UDP	464	允许用户更改过期密码的本机 Windows 身份验证协议
	安全专用访问插件	HTTPS (超文本传输安全协议)	443	身份验证和应用程序枚举
	NetScaler Gateway	安全超文本传输协议	443	应用交付网关回调
NetScaler Gateway	Secure Private Access plug-in	安全超文本传输协议	443	应用程序授权的有效性验证
	思拓方	超文本传输安全协议	443	身份验证和应用程序枚举

源	目的地	类型	端口	详细信息
	Web 应用程序	超文本传输协议、超文本传输安全协议	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	网标器 网关	超文本传输安全协议	443	最终用户设备与 NetScaler Gateway 之间的通信

参考资料

- [身份验证配置文件。](#)
- [身份验证策略的工作原理。](#)
- [在 NetScaler 上将 SSL 证书绑定到虚拟服务器 \(SSL\)。](#)

调整大小指南

数据库存储空间要求

大部分数据库存储空间被日志占用。与日志相比，应用程序和策略配置占用的存储空间可以忽略不计。

以下图示显示了服务器的存储要求：

服务器存储(/zh-cn/citrix-secure-private-access/media/spaop-sizing-guidelines.png)

注意：

- 这些指标是基于日志事件清理已禁用且日志保留期设置为 7 天的假设得出的。
- 默认情况下，日志会保留 90 天或最多 10 万个日志事件，具体取决于配置的设置。这些设置可在 Secure Private Access Runtime 服务 appsettings.json 文件中找到，并可根据需要进行修改。有关详细信息，请参阅[保留事件日志的设置](#)。

服务器配置

以下表格显示了服务器的配置详细信息：

配置信息	详细信息
应用程序总数量	250
策略的总数量	50
每个用户的应用程序数量	15
AD 配置	用户属于 20 个组，最多 20 层嵌套
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）
安全私有访问服务器日志保留	90 天或 600 个文件

主机存储

5000 个用户的基准主机存储详细信息如下：

大小 - 127 GB IOPS - 500 最大吞吐量 - 100

流量配置文件

下表显示了每个用户每天的流量配置文件详细信息。

配置文件	详细信息
枚举项	10

配置文件	详细信息
企业浏览器策略同步	20
从 思杰工作区™ 应用程序启动应用	4
从 思杰企业浏览器™ 访问应用	500
通过 Citrix Director 提交的帮助台故障排除请求 (每天)	1000

部署指导方针

下表显示了根据并发应用访问用户会话、每分钟应用枚举以及 Secure Private Access 使用的 CPU 等参数确定的数据库大小调整要求：

并发应用访问 用户会话	每分钟应用枚举数	安全私有访问 内存 (GB)	安全私有访问 CPU 数量	存储空间 (GB)	备注
< 20 (概念 验证用途)	2	4 GB	2	40 GB*	出于概念验证目的，SPA 可以部署在与 StoreFront™ 相同的计算机上，而无需更改现有 VM 规格。
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：

- ***** 存储主要由CDF日志占用。默认情况下，Secure Private Access保留600个滚动日志文件，每个文件大小为10 MB。因此，如果Secure Private Access管理服务和运行时服务都在同一台机器上运行，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VM上用于概念验证（PoC）目的。
- ****** 对于此负载配置文件及更高版本，建议将Secure Private Access部署在专用服务器上，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。
- ******* 建议为此类负载使用至少2个Secure Private Access节点集群，因为存在一些已知的性能问题。这些问题计划在即将发布的版本中解决。

其他组件的配置设置

组件名称	虚拟 CPU	内存
安全私有访问插件	8	16 GB
安全私有访问 SQL 服务器	8	16 GB
应用商店	16	8 GB
网关	4	8 GB
活动目录	8	14 GB
客户端	4	8 GB

安装安全私有访问

安全私有访问安装程序是集成式 Citrix 虚拟应用和桌面™ 安装程序的一部分。

执行以下步骤安装安全私有访问：

1. 从 <https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/> 下载 Citrix 虚拟应用和桌面 产品软件并启动向导。
2. 单击 **虚拟应用或虚拟应用和桌面** 旁边的**开始**。
3. 选择 **Secure Private Access** 并按照屏幕上的说明完成安装。



有关详细说明，请参阅以下主题：

- [安装核心组件](#)。
- [使用命令行安装](#)。

安装完成后，首次设置管理控制台会在默认浏览器窗口中自动打开。您可以单击**继续**以设置 Secure Private Access。



您还可以在桌面“开始”菜单中看到安全私有访问快捷方式（**思杰 > 思杰安全私有访问™**）。



单点登录到管理控制台

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。
- 如果您不输入凭据，您将看到 Secure Private Access 登录页面。

您必须登录管理控制台才能继续 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，则可以使用与安装计算机属于同一域的任何用户设置 Secure Private Access。

要为 谷歌 Chrome 浏览器和 微软 Edge 浏览器启用 Kerberos，请执行以下步骤。

1. 打开 **互联网选项**。
2. 选择“安全”选项卡，然后单击“**本地 Intranet 区域**”。
3. 单击 **站点** 并添加安全私有访问网址。

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

4. 单击“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：

- If using Chrome Incognito sessions, create a DWORD registry key `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\AmbientAuthenticationInPrivate` and set to value 1.
- 在为无痕模式启用 Kerberos 之前，您必须重新启动所有 Chrome 窗口（包括非无痕窗口）。
- 对于其他浏览器，请查阅特定浏览器关于 Kerberos 身份验证的文档。

后续步骤

- [设置 安全私有访问](#)
- [配置 网思乐网关](#)
- [配置应用程序](#)
- [配置应用程序的访问策略](#)

组成部分

以下是典型的本地部署 Secure Private Access 中的关键组件。

- **StoreFront**： - StoreFront 验证用户并管理用户访问的桌面和应用程序商店。它可以托管您的企业应用程序商店，为用户提供对其可用的桌面和应用程序的自助访问。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上获得一致的体验。有关 StoreFront 与 Secure Private Access 集成的详细信息，请参阅 [StoreFront](#)。
- **NetScaler 网关**： - NetScaler 网关通过企业防火墙提供单一安全访问点。有关 NetScaler 网关与安全私有访问集成的详细信息，请参阅 [NetScaler 网关](#)。
- **Director**：（可选）Director 使您能够进行有效的性能监控和故障排除。要将 Director 与安全私有访问集成，您必须输入必须在安全私有访问中注册的 Director 服务器的 FQDN 的 IP 地址。有关 Director 与安全私有访问集成的详细信息，请参阅 [安全私有访问与 Director 集成](#)。
- **许可证服务器**：许可证服务器收集并处理许可数据。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**: (Optional) Citrix Secure Private Access is integrated into the Web Studio console to enable users seamlessly access the service through Web Studio. For details about the Secure Private Access integration with Web Studio, see [Secure Private Access integration with Web Studio](#).

有关这些产品的最低版本要求的信息，请参阅 [System requirements](#)。

注意：

Director and License Server are integrated with Secure Private Access starting from release 2402.

斯托弗 特

如果 安全私有访问 与 店面 共同托管，则 店面 上的 安全私有访问 配置将由首次设置向导自动完成。

但是，如果 Secure Private Access 未与 StoreFront 共同托管，则必须手动完成某些配置更改。

执行以下步骤手动配置 StoreFront。

1. 从 Secure Private Access 管理控制台（**设置 > 集成**）下载脚本。
2. 单击与需要进行配置更改的 StoreFront 条目对应的**下载脚本**。

下载的 zip 文件包含一个配置脚本、一个 README 文件和一个配置清理脚本。如果 StoreFront 和 Secure Private Access 之间的集成要移除，则可以使用清理脚本。

3. 使用命令 `./ConfigureStorefront.ps1` 以管理员身份在 PowerShell 64 位实例上运行脚本
 - 不需要任何其他参数。
 - PowerShell 脚本执行策略必须设置为**无限制或绕过**才能运行 StoreFront 脚本。
 - 如果 StoreFront 配置为群集，该脚本还会将配置传播到其他 StoreFront 服务器。

一旦 StoreFront 完成了 Secure Private Access 相关设置的配置工作，Secure Private Access 插件的配置信息便会清晰地显示在 StoreFront 管理用户界面（**管理交付控制器屏幕**）中。

如果 Citrix Virtual Apps and Desktops™ 交付控制器也配置了相同的设置，则 StoreFront 脚本会自动配置 Secure Private Access 的聚合组设置。默认情况下，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**）。

重要提示：

- 建议仅使用从 Secure Private Access 管理**用户界面**下载的 StoreFront 脚本来为 Secure Private Access 配置 StoreFront。不要从 StoreFront 管理**用户界面**配置 Secure Private Access，因为**用户界面**不涵盖 StoreFront 上的所有必需配置。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 部署上配置（无论是在同一 StoreFront 上的另一个应用商店，还是在不同的 StoreFront 部署上）。可以从“**设置 > 集成**”页面添加 StoreFront。
- StoreFront 自动配置无法从“**设置 > 集成**”页面运行，即使 Secure Private Access 与 StoreFront 共同托管。自动配置仅在首次设置期间完成。如果从“**设置**”页面添加新的应用商店配置，则必须在相应的 StoreFront 计算机上下载并运行 StoreFront 脚本。

使用 StoreFront 2308 或更早版本时

如果您使用的是 StoreFront 2308 或更早版本，StoreFront 管理员 UI 存在以下已知问题：

- 安全私有访问插件类型显示为 XenMobile。
- 安全私有访问服务器 URL 未显示。

- 安全私有访问端口始终显示为 80。



使用 StoreFront 2311 或更高版本时

在 StoreFront 2311 及更高版本中，Citrix Workspace™ for Web 客户端不枚举安全私有访问应用程序。这是因为安全私有访问不支持在 Workspace for Web 平台上启动安全私有访问应用程序。

网思乐网关

NetScaler 网关配置支持 Web/SaaS 和 TCP/UDP 应用程序。您可以创建 NetScaler 网关或更新现有 NetScaler 网关配置以用于安全专用访问。建议您在应用这些更改之前创建 NetScaler 快照或保存 NetScaler 配置。

重要提示：

有关适用于 Web/SaaS 和 TCP/UDP 应用程序的 NetScaler Gateway 配置的详细信息，请参阅以下部分：

- 适用于网页/软件即服务应用程序的 NetScaler Gateway 配置(/zh-cn/citrix-secure-private-access/2407/spa-onprem-netscaler-gateway-web-saas-config.html)
- 适用于传输控制协议/用户数据报协议应用程序的 NetScaler Gateway 配置(/zh-cn/citrix-secure-private-access/current-release/spa-onprem-netscaler-gateway-tcp-udp-config.html)

与 ICA® 应用程序的兼容性

为支持安全私有访问插件而创建或更新的网思乐网关也可用于枚举和启动 ICA 应用程序。在这种情况下，您必须配置安全票证颁发机构 (STA) 并将其绑定到网思乐网关。

注意：

STA 服务器通常是 Citrix 虚拟应用和桌面™ 部署的一部分。

有关详细信息，请参阅以下主题：

- 在 NetScaler Gateway 上配置安全票证颁发机构
- 常见问题：Citrix 安全网关/ NetScaler 网关 安全票证颁发机构

支持智能访问标签

注意：

- 本节提供的信息仅适用于您的 NetScaler Gateway 版本低于 14.1-25.56 的情况。
- 如果您的 NetScaler 网关版本为 14.1–25.56 或更高版本，那么您可以通过使用命令行界面 (CLI) 或图形用户界面 (GUI) 的方式，在 NetScaler 网关上启用 Secure Private Access 插件。有关详细信息，请参阅[在 NetScaler 网关上启用 Secure Private Access 插件](#)。

在以下版本中，NetScaler Gateway 会自动发送标签。您无需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。

配置安全专用访问切换开关

下表列出了在本地部署中支持智能访问标签所需使用的切换开关：

切换开关名称	详细说明
<code>nsapimgr_wr.sh -ys</code> <code>call=ns_vpn_enable_spa_onprem</code>	启用针对本地部署的安全私有访问功能
<code>nsapimgr_wr.sh -ys</code> <code>call=ns_vpn_disable_spa_onprem</code>	禁用针对本地部署的安全私有访问功能
<code>nsapimgr_wr.sh -ys</code> <code>ns_vpn_enable_spa_tcp_udp_apps=3</code>	启用 TCP/UDP 应用程序
<code>nsapimgr_wr.sh -ys</code> <code>ns_vpn_enable_spa_tcp_udp_apps=0</code>	禁用 TCP/UDP 应用程序
<code>nsapimgr_wr.sh -ys</code> <code>call=toggle_vpn_enable_securebrowse_client_mode</code>	为 HTTP 回调配置启用 SecureBrowse 客户端模式

切换开关名称	详细说明
<pre>nsapimgr -ys call=toggle_vpn_redirect_to_access_restricted_page_on_deny</pre>	如果访问被拒绝，则启用重定向到“访问受限”页面。
<pre>nsapimgr -ys call=toggle_vpn_use_cdn_for_access_restricted_page</pre>	使用 CDN 上托管的“访问受限”页面。

注意：

- 要禁用没有单独禁用命令的切换开关，请再次运行相同的命令。这仅适用于命令中包含“toggle”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[配置上下文标签](#)。

在 NetScaler 上保留安全私有访问插件设置

要在 NetScaler 上保留安全私有访问插件设置，请执行以下操作：

1. Create or update the file `/nsconfig/rc.netscaler`.
2. 将以下命令添加到文件中。

```
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_deny
```

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

3. 保存文件。

NetScaler 重新启动后，安全专用访问插件设置将自动应用。

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 命令行界面或图形用户界面在 NetScaler Gateway 上启用安全私有访问插件。此配置取代了 2407 之前版本中使用的 `nsapimgr_wr.sh -ys call=ns_vpn_enable_spa_onprem` 按钮。

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 > 更改全局 NetScaler 网关 设置**。
2. 单击**安全**选项卡。
3. 在 **安全私有访问** 中，选择 **已启用**。



将公共网关证书上传

如果公共网关无法从 Secure Private Access 计算机访问，则必须将公共网关证书上传到 Secure Private Access 数据库。

请执行以下步骤来上传公共网关证书：

1. 以管理员权限打开 PowerShell 或命令提示符窗口。
2. 将目录更改为 安全私有访问 安装文件夹下的 管理\配置工具 文件夹（例如，`cd "C:\程序文件\Citrix\Citrix 访问安全\管理\配置工具"`）
3. 运行以下命令：

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

已知的限制

- 现有 NetScaler Gateway 可以通过脚本更新，但可能存在无限数量的 NetScaler 配置，这些配置无法通过单个脚本覆盖。
- 我们建议您在启用 Secure Private Access 的 VPN 虚拟服务器中将 **ICA 代理** 设置为 OFF。
- 如果您使用部署在云中的 NetScaler，则必须对网络进行一些更改。例如，允许 NetScaler 和其他组件在某些端口上进行通信。有关端口的详细信息，请参阅[通信端口](#)。

- If you enable SSO on NetScaler Gateway, make sure that NetScaler communicates to StoreFront™ using a private IP address. You might have to add a new StoreFront DNS record to NetScaler with a StoreFront private IP address.

NetScaler Gateway 配置，用于网页/软件即服务应用程序

要创建用于 Web/SaaS 应用程序的 NetScaler Gateway，请执行以下步骤：

1. 从 `<https://www.citrix.com/downloads/citrix-secure-private-access/Shell-Script/Shell-Script-for-Gateway-Configuration.html>` 下载最新脚本 `*ns_gateway_secure_access.sh*`。
2. 将这些脚本上传到 NetScaler 设备。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`，这意味着行结尾不正确。您可以使用任何富文本编辑器（例如 Notepad++）转换脚本。

3. 通过 SSH 连接到 NetScaler，并切换到命令行（在 NetScaler 命令行界面上输入 'shell'）。
4. 使上传的脚本可执行。使用 `chmod` 命令执行此操作。

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

5. 在 NetScaler 命令行界面上运行上传的脚本。



6. 如果仅打算为 Web 和 SaaS 应用程序配置网关，请为“启用 TCP/UDP 应用程序类型支持”参数输入 **N**。
7. 输入所需的参数。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。

将生成一个包含多个 NetScaler 命令的新文件（默认情况下，文件路径为 `var/tmp/ns_gateway_secure_access`）。

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，脚本将启用 NetScaler 功能，以支持智能访问标签发送改进，并在资源访问受限时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](#)。

The Secure Private Access plug-in features persisted in the `/nsconfig/rc.netscaler` file allow to keep them enabled after NetScaler is restarted.



8. 切换到 NetScaler CLI，并使用批处理命令运行新文件中生成的 NetScaler 命令。例如；

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

```
/var/tmp/ns_gateway_secure_access_output
```

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

如果资源已存在或步骤 6 中输入的某个参数不正确，则命令可能会失败。

9. 请确保所有命令都已成功完成。

注意：

如果出现错误，NetScaler 仍会运行剩余命令并部分创建/更新/绑定资源。因此，如果您因某个参数不正确而看到意外错误，建议从头开始重新配置。

更新现有 NetScaler Gateway 网页和软件即服务应用程序配置

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，如果您想手动更新现有配置（NetScaler Gateway 版本 14.1–4.42 及更高版本），请使用 [更新现有 NetScaler Gateway 配置的示例命令](#)。此外，您必须更新 NetScaler Gateway 虚拟服务器和会话操作设置。

注意：

Starting from NetScaler Gateway 14.1–25.56 and later, you can enable the Secure Private Access plug-in on NetScaler Gateway by using the NetScaler Gateway CLI or the GUI. For details, see [Enable Secure Private Access plug-in on NetScaler Gateway](#).

您还可以使用现有 NetScaler Gateway 上的脚本来支持 Secure Private Access。但是，该脚本不会更新以下内容：

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

请确保在执行每个命令之前进行审查，并创建网关配置的备份。

NetScaler 网关 虚拟服务器设置

当您添加或更新现有 NetScaler Gateway 虚拟服务器时，请确保以下参数设置为定义的值。有关示例命令，请参阅 [更新现有 NetScaler Gateway 配置的示例命令](#)。

添加虚拟服务器：

- tcpProfileName: nstcp_default_XA_XD_profile
- 部署类型: ICA_STOREFRONT（仅适用于 `add vpn vserver` 命令）
- 仅限ICA: 关闭

更新虚拟服务器：

- tcpProfileName: nstcp_default_XA_XD_profile
- 仅限ICA: 关闭

NetScaler 网关会话策略设置

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，请确保以下参数设置为定义的值。有关示例命令，请参阅 [更新现有 NetScaler Gateway 配置的示例命令](#)。

- `transparentInterception` : 关闭
- `SSO` : ON
- `ssoCredential` : 主要
- `useMIP` : NS
- `useIIP` : 关闭

- `icaProxy` : 关闭
- `wihome` : "https://storefront.mydomain.com/Citrix/MyStoreWeb" - 替换为真实的 Store URL。Store `/Citrix/MyStoreWeb` 的路径是可选的。
- `ClientChoices` : 关闭
- `ntDomain` : 您的域名.com - 用于 SSO (可选)
- `defaultAuthorizationAction` : 允许
- `authorizationGroup` : SecureAccessGroup (确保已创建此组, 它用于绑定安全私有访问特定的授权策略)
- `clientlessVpnMode` : 开启
- `clientlessModeUrlEncoding` : 透明
- `SecureBrowse` : 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 安全私有访问 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](#)。

更多详细信息

有关 NetScaler Gateway 的安全私有访问的更多信息，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 网关上启用安全私有访问插件](#)
- [上传公共网关证书](#)
- [已知限制](#)

NetScaler 网关 针对 TCP/UDP 应用程序的配置

您可以使用 (/zh-cn/citrix-secure-private-access/2407/spa-onprem-netscaler-gateway-web-saas-config.html) 中概述的步骤来配置 TCP/UDP 应用程序。要为 TCP/UDP 应用程序配置网关，您必须通过在脚本中为 **Enable TCP/UDP App type support** 参数输入 Y 来启用 TCP/UDP 支持。

下图显示了为 TCP/UDP 支持而启用的“启用 TCP/UDP 应用程序类型支持”参数。

NetScaler 的配置界面示意图 1(/zh-cn/citrix-secure-private-access/media/spaop-configure-netscaler1.png)

NetScaler 的配置界面示意图 2(/zh-cn/citrix-secure-private-access/media/spaop-configure-netscaler2.png)

更新现有 NetScaler 网关的 TCP/UDP 应用程序配置

如果您正在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 (/zh-cn/citrix-secure-private-access/2407/spa-onprem-netscaler-gateway-tcp-udp-config#example-commands-to-update-an-existing-netscaler-gateway-configuration)。此外，您必须更新 NetScaler Gateway 虚拟服务器和会话操作设置。

NetScaler Gateway virtual server settings

当您添加或更新现有 NetScaler Gateway 虚拟服务器时，请确保以下参数设置为定义的值。有关示例命令，请参阅 (/zh-cn/citrix-secure-private-access/2407/spa-onprem-netscaler-gateway-tcp-udp-config#example-commands-to-update-an-existing-netscaler-gateway-configuration)。此外，您必须更新 NetScaler Gateway 虚拟服务器和会话操作设置。

添加虚拟服务器：

- tcpProfileName: nstcp_default_XA_XD_profile
- deploymentType: ICA_STOREFRONT (available only with the `add vpn vserver` command)
- 仅限 ICA: 关闭

更新虚拟服务器：

- tcpProfileName: nstcp_default_XA_XD_profile
- 仅限 ICA: 关闭

有关虚拟服务器参数的详细信息，请参阅 [vpn-sessionAction](#)。

NetScaler 网关会话策略设置

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，请确保以下参数设置为定义的值。有关示例命令，请参阅 [更新现有 NetScaler Gateway 配置的示例命令](#)。此外，您必须更新 NetScaler Gateway 虚拟服务器和会话操作设置。

- `transparentInterception` : ON
- `SSO` : ON
- `ssoCredential` : 主要
- `useMIP` : NS
- `useIIP` : 关闭
- `icaProxy` : 关闭
- `ClientChoices` : ON
- `ntDomain` : mydomain.com - 用于单点登录（可选）
- `defaultAuthorizationAction` : 允许
- `authorizationGroup` : 安全访问组
- `clientlessVpnMode` : 关闭
- `clientlessModeUrlEncoding` : 透明
- `SecureBrowse` : 已启用

更新现有 NetScaler Gateway 配置的示例命令

注意：

如果您正在手动更新现有配置，则除了以下命令之外，您还必须使用命令 `nsapimgr_wr.sh -ys ns_vpn_enable_spa_tcp_udp_apps=3` 更新 `/nsconfig/rc.netscaler` 文件。

- 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\")" 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 115 -gotoPriorityExpression NEXT -type REQUEST
```

- 添加 HTTP 回调策略以支持基于 TCP/UDP 的连接的授权验证。

```
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/{"{"+\"userName\": \"\"+aaa.USER.NAME.REGEX_REPLACE(re#\&num; , \"\\\", 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** 是安全私有访问插件的 IP 地址
- **spa.example.corp** 是安全私有访问插件的完全限定域名
- **ns224158.example.corp** 是网关 VPN 虚拟服务器的完全限定域名。
- 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
```

- 将安全私有访问插件绑定到 VPN 虚拟服务器。

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

有关更多信息

有关适用于安全私有访问的 NetScaler 网关的更多信息，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](#)

上下文标签

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、已安装软件、地理位置）为 Web 或 SaaS 应用程序提供上下文访问（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 插件上的上下文标签是应用于已认证用户会话的 NetScaler® Gateway 策略（会话、预认证、EPA）的名称。

Secure Private Access 插件可以通过标头（新逻辑）或通过回调到 Gateway 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：

安全私有访问插件仅支持可在 NetScaler 网关上配置的经典网关预认证策略。

使用 GUI 配置自定义标签

在配置上下文标签时，需要执行以下高级步骤。

1. 配置一个经典网关预认证策略
2. 将经典预认证策略绑定到网关虚拟服务器

配置一个经典网关预认证策略

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



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

表达式示例(/zh-cn/citrix-secure-private-access/media/spaop-expression-sample.png)

下图显示了为检查 Windows 10 操作系统而构建的示例表达式。

表达式编辑器(/zh-cn/citrix-secure-private-access/media/spaop-policy-exp-editor.png)

6. 单击“**创建**”。

将自定义标签绑定到 NetScaler 网关

1. 导航到 **NetScaler 网关 > 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“**+**”以绑定策略。
4. 在“**选择策略**”中，选择预身份验证策略，并在“**选择类型**”中选择“**请求**”。

策略类型(/zh-cn/citrix-secure-private-access/media/spaop-request-type.png)

5. 请选择策略的名称，并确定该策略在评估时的优先级。
6. 单击“**绑定**”。

策略绑定(/zh-cn/citrix-secure-private-access/media/spaop-preauth-policy-binding.png)

使用 CLI 配置自定义标签

在 NetScaler CLI 上运行以下命令以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`

添加新的上下文标签

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

关于发送到 Secure Private Access 插件的 EPA 标签的注意事项

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

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



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。当操作被允许时，`epaallowact` 和 `allow_app` 作为智能访问标签发送到 Secure Private Access 插件。

参考资料

- [配置应用程序的访问策略。](#)
- [支持智能访问标签。](#)

许可证服务器

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强制组件。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进行配置或更新。有关将许可证服务器注册到 Secure Private Access 的详细信息，请参阅 ([/zh-cn/citrix-secure-private-access/2407/spa-onprem-setup-spa#step-3-integrate-storefront-and-netscaler-gateway-servers](#))。

您必须指定许可证服务器 URL，才能将 Secure Private Access 连接到许可证服务器。Secure Private Access 插件会自动在许可证服务器上注册。

注意：

- 您必须在许可证服务器上安装至少一个 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。
- Secure Private Access 插件的许可证服务器支持版本 11.17.2 build 45000 及更高版本。如果您已有许可证服务器，则必须将许可证服务器升级到版本 11.17.2 build 45000 或更高版本。

有关许可服务器的更多信息，请参阅 (</zh-cn/licensing/current-release>)。

思杰安全访问™ 客户端

您现在可以通过在您的机器上运行的 Citrix Secure Access 客户端，使用原生浏览器或原生客户端应用程序访问所有私有应用程序，包括 TCP/UDP 和 HTTPS/HTTP 应用程序。

随着 Citrix Secure Private Access 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，从而为远程用户提供对所有私有应用程序的访问。欲了解更多信息，请参阅 [Citrix Secure Access](#) 文档。

导向器（可选）

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，您必须输入需要注册到 Secure Private Access 的 Director 服务器的完全限定域名 (FQDN) 的 IP 地址。有关详细信息，请参阅 [集成服务器](#)。

对于本地版本 2402 的 Secure Private Access 客户，将 Director 注册到 Secure Private Access 是一项强制性配置。如果您尚未配置 Director，则必须安装最新版本的 Director，即 LTSR 2402 或更高版本。如果您已配置 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 未注册到 Citrix 安全专用访问。
- 您输入的 Director IP 地址或 FQDN 不存在。

有关将 Director 注册到 Citrix 安全专用访问 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：

- Director 注册或登录不支持集成 Windows 身份验证 (IWA)。如果管理员使用 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。
- 如果管理员需要在设置完成后添加其他 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。单点登录不支持编辑 Director URL IPv6、SSLv3。

使用 Director 配置工具来对 Director 进行配置，以使其能够与 Secure Private Access 功能进行集成

使用配置工具配置 Director，使其与 Secure Private Access 集成，这是完成此集成的强制步骤。有关详细信息，请参阅 [安全专用访问与 Director 集成](#)。

在 Director 中查看安全私有访问用户会话

您可以在 Director 中查看安全私有访问用户会话。有关详细信息，请参阅 [按用户查看安全私有访问会话](#)。

将安全私有访问部署为集群（可选）

Secure Private Access 本地解决方案可以作为集群部署，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），可以部署多个独立的 Secure Private Access 节点来分发工作负载并增强可扩展性。

创建安全私有访问节点

- 创建新的安全私有访问站点。有关详细信息，请参阅[设置安全私有访问站点](#)。
- 将所需数量的集群节点添加到 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。证书主题公用名或主题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“集成”选项卡中指定数据库地址并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 集群设置没有特定的负载均衡配置要求。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。如果您使用负载均衡器，则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 进行负载均衡](#)。在配置 Secure Private Access 之前，必须配置 StoreFront 存储。如果使用负载均衡器，请使用负载均衡器名称配置基本 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](#)。
- 建议安全私有访问服务以 HTTPS 运行，但这并非强制要求。安全私有访问服务也可以部署为 HTTP。
- 支持 SSL 卸载或 SSL 桥接，因此可以使用任何负载均衡器配置。使用 SSL 桥接时，请确保在每个 Secure Private Access 节点中配置相同的服务器证书。此外，证书主题公用名或主题备用名称 (SAN) 必须与负载均衡器 FQDN 匹配。此外，SAN 必须在负载均衡器服务中配置。
- 正确的 SSL 证书已绑定到 IIS 服务器和 NetScaler。
- 使用安全密码。
- Secure Private Access 服务（包括管理和运行时）是无状态的，因此不需要持久性。
- 负载均衡器（例如 NetScaler）为后端服务器提供了默认的内置监视器（探测器）。如果必须为本地 Secure Private Access 服务器配置基于 HTTP 的自定义监视器（探测器），可以使用以下端点：

`/secureAccess/health`

预期响应：

```
Http status code: 200 OK
```

```
Payload:
```

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

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](#)。

为安全私有访问创建监视器

使用以下 CLI 命令为安全私有访问创建监视器。

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

创建监视器后，将证书绑定到监视器。

有关使用 NetScaler UI 创建监视器的详细信息，请参阅 [创建监视器](#)。

配置安全私有访问插件

安装 Citrix Secure Access 插件后，您可以设置安全私有访问环境，然后配置应用程序及其访问策略。安全私有访问支持 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，您可以通过启用相应的安全限制来启用对应用程序（HTTP/HTTPS 和 TCP/UDP）的受限访问。

- [配置基于 HTTP/HTTPS 的应用程序](#)
- [配置 TCP/UDP 应用程序](#)
- [配置应用程序的访问策略](#)
- [访问限制选项](#)

设置安全专用访问

您可以通过创建新站点或加入现有站点来设置安全专用访问。在这两种情况下，您都可以使用 Web 管理控制台来设置安全专用访问环境。

- [通过创建新站点设置安全专用访问](#)
- [通过加入现有站点设置安全专用访问](#)

先决条件

- 您必须使用域用户登录安全专用访问管理控制台，该域用户也是安装安全专用访问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。
- 如果您有多个域环境，请确保在位于不同林的 Active Directory 域之间建立域信任。有关详细信息，请参阅[多域环境](#)。

通过创建新站点设置安全专用访问

步骤 1：设置安全专用访问站点

站点是您的安全专用访问部署的名称。您可以创建站点或加入现有站点。

1. 启动安全专用访问 Web 管理控制台。

2. 在“创建或加入站点”页面上，“创建新的安全专用访问站点”默认处于选中状态。
3. 单击“下一步”。



当您选择创建站点时，您必须自动或手动为新站点配置数据库，因为设置中可能没有与站点名称对应的数据库。

步骤 2：配置数据库

您必须为新的 Secure Private Access 站点创建数据库。这可以通过手动或自动方式完成。

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

您可以通过以下任一形式指定数据库地址：

- 服务器名称
- 服务器名称\实例名称
- 服务器名称,端口号

有关详细信息，请参阅[数据库](#)。

2. 在 **站点** 中，键入安全私有访问站点的名称。

注意：

您输入的站点名称将作为数据库名称的后缀。数据库名称格式为

`CitrixAccessSecurity<sitename>`，无法修改。如果必须自定义数据库名称，请联系 Citrix 支持。

3. 单击 **测试连接** 以检查 SQL Server 实例是否有效，并确认站点存在指定的数据库。



注意：

- 如果站点的 SQL 服务器不可用，则连接性检查将失败。
- 如果 SQL 服务器可用但数据库不存在，则连接性检查将通过。但是，会显示一条警告消息。
- Secure Private Access 使用 Windows 身份验证（通过计算机身份）对 SQL 服务器进行身份验证。

自动配置：

- 仅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。

- 如果指定地址处不存在数据库，则会自动创建一个数据库。
- 创建数据库时，请确保它是空的，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，您必须首先下载脚本，然后在您在**SQL Server 主机**字段中指定的数据库服务器上运行这些脚本。

注意

如果计算机没有在 SQL 服务器上的数据库中创建表的 READ、WRITE、UPDATE 权限，则数据库创建可能会失败。您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

您必须指定 StoreFront 和 NetScaler® Gateway 服务器详细信息，以将安全私有访问与 StoreFront 和 NetScaler Gateway 服务器连接。必须建立此连接，才能使 StoreFront 和 NetScaler Gateway 将流量路由到安全私有访问。您还必须指定 Director 服务器和许可证服务器详细信息。

1. 输入以下详细信息。

- **安全私有访问服务器地址。**例如， `https://secureaccess.domain.com`。
- **店面商店网址。**例如， `https://storefront.domain.com/Citrix/StoreMain`。
- **公共 NetScaler Gateway 地址** – 其统一资源定位符。例如， `https://gateway.domain.com`。
- **虚拟 IP 地址** – 此虚拟 IP 地址必须与 StoreFront 中为回调配置的地址相同。
- **回调 URL** – 此 URL 必须与 StoreFront 中配置的 URL 相同。例如， `https://gateway.domain.com`。
- **导向器 URL**： - （可选）用于将 Secure Private Access 连接到 Citrix Director 的导向器服务器 IP 地址或完全限定域名。
- **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，将进行验证以确保所配置的服务器可访问。此外，还会检查以确保 Secure Private Access 服务器可访问。

如果配置摘要页面显示任何错误，请参阅[故障排除错误](#)了解详细信息。如果这不能解决问题，请联系 Citrix 支持。



设置完成后，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，您可以在 Web 管理控制台中通过[设置 > 集成](#)修改设置。
- 首次安装安全私有访问的管理员将获得完全权限。此管理员随后可以将其他管理员添加到设置中。您可以通过[设置 > 管理员](#)查看管理员列表。
- 您还可以添加管理员组，以便该组中的所有管理员都获得访问权限。

有关详细信息，请参阅[安装后管理设置](#)。

通过加入现有站点设置安全私有访问

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。确保您输入的站点名称对应的数据库已存在于您选择的 SQL Server 中。您可以采用以下任一形式指定数据库地址：
 - 服务器名称
 - 服务器名称\实例名称
 - 服务器名称,端口号

有关详细信息，请参阅[数据库](#)。

3. 在[站点](#)中，为安全私有访问站点键入一个名称。
4. 单击[测试连接](#)以检查 SQL 服务器实例是否有效，并确认数据库中存在指定的站点。



如果站点没有对应的数据库，连接性检查将失败。

5. 单击**保存**。

执行配置验证检查，以确保 SQL 数据库服务器已配置，并检查 Secure Private Access 服务器是否可访问。

禁用 HTTP2 设置

本地部署的 Secure Private Access 在 Internet Information Services (IIS) 环境中运行。因此，Microsoft 会直接解决并修补 IIS 中影响 HTTP/2 的任何潜在常见漏洞。在此期间，客户可以通过直接在 IIS 中手动修改 HTTP/2 设置来缓解此漏洞，从而确保本地部署的 Secure Private Access 解决方案在官方补丁发布之前也受到保护。

执行以下步骤以禁用每个站点的 HTTP2。

1. 打开 Internet 信息服务 (IIS) 管理器。
2. 在导航窗格中，展开**站点**并选择**默认网站**。
3. 在**操作**窗格中，单击**绑定**，并通过选中**禁用 HTTP/2**复选框来修改 HTTPS 绑定。
4. 保存并重新启动 IIS 管理器。

禁用 HTTP2 设置(/zh-cn/citrix-secure-private-access/media/disable-http2.png)

多域环境的部署

本地部署的 Secure Private Access 支持多域环境，其中计算机服务器和用户帐户服务器位于不同的 Active Directory 域中。这种跨域部署功能为管理基础架构和用户身份提供了灵活性。但是，要使此环境成功运行，必须在位于不同林的 Active Directory 域之间建立至少单向信任关系。



为了在多域环境中为本地部署的 Secure Private Access 建立域信任，必须满足以下先决条件：

- 用于初始配置的计算机域（例如，域 B）中的服务帐户必须在用户帐户域（例如，域 A）中进行预配。

注意：

必须在 IIS 中为 Citrix Access Security Runtime Service Pool 添加服务帐户。该服务帐户不需要管理员权限。有关详细信息，请参阅 [配置服务帐户的步骤](#)。

- 如果安装服务器（在域 A 中，称为“服务器域 a”）也位于域 A 中，则必须将服务帐户创建为数据库用户，并在相关数据库实例中拥有“db owner”权限。

如何配置服务帐户

请按照以下步骤操作，以完成服务帐户的配置：

1. 启动互联网信息服务 (IIS) 管理器。
2. 在站点服务器下，选择 **应用程序池 > Citrix 访问安全运行时池 > 高级设置**。



3. 请点击位于 **标识 > ApplicationPoolIdentity** 选项旁边的编辑图标。



4. 在 **自定义帐户：** 中，单击 **设置**。



5. 为用户设置凭据。

6. 单击 **确定**。



后续步骤

- [配置 NetScaler 网关 的设置](#)
- [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

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

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

配置应用程序(/zh-cn/citrix-secure-private-access/media/spaop-add-app.png)

- **应用程序名称** – 应用程序的名称。

- **应用程序描述** - 应用程序的简要说明。此说明将显示给工作区中的用户。您还可以按 `KEYWORDS: <keyword_name>` 格式输入应用程序的关键字。您可以使用关键字筛选应用程序。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** - 添加您发布的应用程序必须在 Citrix Workspace™ UI 中显示的类别和子类别名称（如果适用）。您可以为每个应用程序添加新类别，或使用 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/子类别可由管理员配置，管理员可以为每个应用程序添加新类别。
 - 类别/子类别名称必须用反斜杠分隔。例如，Business And Productivity\Engineering。此外，此字段区分大小写。管理员必须确保定义正确的类别。如果 Citrix Workspace UI 中的名称与“应用程序类别”字段中输入的类别名称不匹配，则该类别将作为新类别列出。

例如，如果您在应用程序类别字段中将“业务与生产力”类别错误地输入为“业务和生产力”，则 Citrix Workspace UI 中除了“业务与生产力”类别之外，还会列出名为“业务和生产力”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。如果您不更改图标，则会显示默认图标。
- **不向用户显示应用程序** - 如果您不想向用户显示应用程序，请选择此选项。
- **URL** - 应用程序的 URL。
- **相关域** - 相关域会根据应用程序 URL 自动填充。管理员可以添加更多相关的内部或外部域。

注意：

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

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

如果您从 Secure Private Access 控制台中删除标记为收藏的应用程序，则必须从 Citrix Workspace 中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** - Web 应用程序选择**内部**，SaaS 应用程序选择**外部**。

5. 单击**保存**，然后单击**完成**。

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

后续步骤

配置应用程序的访问策略(/zh-cn/citrix-secure-private-access/2407/spa-onprem-configure-access-policies.html)

配置 TCP/UDP 应用程序

先决条件：

- 安全私有访问设置已完成。有关详细信息，请参阅 [设置安全私有访问](#)。
- Citrix 安全访问™ 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

有关思杰安全访问客户端的详细信息，请参阅 思杰安全访问客户端。

执行以下步骤以从管理控制台配置 TCP/UDP 应用程序。

1. 在管理控制台中，单击“**应用程序**”，然后单击“**添加应用程序**”。
2. 选择位置“**在我的公司网络中**”。



3. 输入以下详细信息：

- **应用程序类型** – 选择 TCP/UDP。

注意：

如果 SPAOP-3315-EnableZTNAApplications 功能标志被禁用，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。

- **应用程序名称** – 应用程序的名称。
- **应用程序描述** – 您正在添加的应用程序的描述。此字段是可选的。
- **目标** – 位于资源位置的后端计算机的 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** – 举个例子：10.106.90.0/24
 - **机器的完全限定域名 (FQDN) 或其对应的域名** – 单个域名或通配符域名。例如，您可以输入以下内容：ex.destination.domain.com, *.domain.com

重要提示：

- 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。这是因为 Citrix Secure Access 客户端可以将 FQDN 解析为真实的 IP 地址。

下表提供了各种目标的示例以及如何使用这些目标访问应用程序：

目的地输入	如何访问应用程序
10.10.10.1-10.10.10.100	最终用户应仅通过此范围内的 IP 地址访问应用程序。
10.10.10.0/24	最终用户应仅通过在 IP CIDR 中配置的 IP 地址访问应用程序。

目的地输入	如何访问应用程序
10.10.10.101	最终用户应仅通过 10.10.10.101 访问应用程序。
.info.citrix.com	最终用户应访问 info.citrix.com 的子域以及 info.citrix.com（父域）。例如，info.citrix.com, sub1.info.citrix.com, level1.sub1.info.citrix.com 注意： 通配符必须始终是域的起始字符，并且只允许一个。
info.citrix.com	最终用户应仅访问 info.citrix.com，而不访问任何子域。例如，sub1.info.citrix.com 无法访问。

目标 IP 地址在所有资源位置中必须是唯一的。如果存在冲突配置，则在应用程序域表（**设置 > 应用程序域**）中特定 IP 地址旁边会显示警告符号。



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

以下表格提供了可针对某个目标进行配置的端口示例。

端口输入	功能描述
*	默认情况下，端口字段设置为 "*"（任何端口）。目标支持 1 到 65535 之间的端口号。
1300–2400	目标支持 1300 到 2400 的端口号。
38389	目标仅支持端口号 38389。
22,345,5678	目标支持端口 22、345、5678。
1300–2400, 42000-43000,22,443	目标支持端口号范围 1300 到 2400、42000 到 43000，以及端口 22 和 443。

注意：

通配符端口 (*) 不能与端口号或端口范围共存。

- **Protocol** – TCP/UDP

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

- **编辑应用程序**
- **删除**

配置 TCP/UDP 应用程序的访问策略

为了授予用户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](#)。

配置针对应用程序的访问策略

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

创建策略(/zh-cn/citrix-secure-private-access/media/spaop-add-policy.png)

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 – 选择允许或拒绝应用程序访问所依据的条件以及用户或用户组。
 - **匹配以下任意项**：只有与字段中列出的任何名称匹配的用户或组才允许访问。
 - **不匹配任何项**：除字段中列出的用户或组外，所有用户或组都允许访问。
6. 单击 **添加条件** 以添加基于上下文标签的另一个条件。这些标签源自 NetScaler® Gateway。
7. 在 **操作** 中，选择根据条件评估必须对应用程序强制执行的以下操作之一。
 - **允许访问**
 - **允许受限访问**
 - **拒绝访问**

注意：

- 操作**允许受限访问**不适用于 TCP/UDP 应用程序。
- 选择**允许受限访问**后，必须单击**添加限制**以选择限制。有关每个限制的更多信息，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**。如果未选择此选项，则策略仅创建，而不会在应用程序上强制执行。或者，您也可以通过使用切换开关从“访问策略”页面启用策略。

访问策略优先级

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

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

您可以通过使用**优先级**列中的上下箭头图标来向上或向下移动策略，从而更改优先级顺序。

后续步骤

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

示例配置验证

访问限制配置选项

当您选择操作 **允许受限访问** 时，可以根据要求选择安全限制。这些安全限制在系统中是预定义的。管理员无法修改或添加其他组合。



剪贴板

通过 Citrix Enterprise Browser 访问 SaaS 或内部 Web 应用程序时，使用此访问策略启用/禁用剪切/复制/粘贴操作。默认值：已启用。

复制

通过 Citrix Enterprise Browser 访问 SaaS 或内部 Web 应用程序时，使用此访问策略启用/禁用数据复制。默认值：已启用。

注意：

- 如果策略中同时启用了 **剪贴板** 和 **复制** 限制，则 **剪贴板** 限制优先于 **复制** 限制。
- 最终用户必须使用 Citrix Enterprise Browser™ 126 或更高版本才能访问已启用此限制的应用程序。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细粒度控制，管理员可以使用 **安全组** 限制。有关详细信息，请参阅 [针对安全组的剪贴板限制](#)。

按文件类型下载限制

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

注意：

- **按文件类型下载限制** 除了 **下载** 限制之外还可用。
- 如果策略中同时启用了“**下载**”和“**按文件类型限制下载**”限制，“**下载**”限制优先于“**按文件类型限制下载**”限制。
- 最终用户必须使用 Citrix Enterprise Browser 126 或更高版本才能访问已启用此限制的应用程序。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“**操作**”中，选择“**允许（带限制）**”。
3. 单击“**按文件类型限制下载**”，然后单击“**编辑**”。
4. 在“**按文件类型限制下载设置**”页面中，选择以下选项之一：
 - “**允许所有下载（带例外）**” – 选择必须阻止的类型，并允许所有其他类型。
 - “**阻止所有下载（带例外）**” – 仅选择可以上传的类型，并阻止所有其他类型。

5. 如果文件类型不在列表中，请执行以下操作：

- a. 单击“**添加自定义 MIME 类型**”。
- b. 在“**添加 MIME 类型**”中，以 `category/subcategory<extension>` 格式输入 MIME 类型。
例如，`image/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文件类型时，Citrix Enterprise Browser 会显示以下警告消息：



下载内容

通过此策略，当用户通过 Citrix Enterprise Browser 访问 SaaS 或内部 Web 应用程序时，启用/禁用其下载功能。默认值：已启用。

注意：

如果策略中同时启用了“**下载**”和“**按文件类型限制下载**”限制，则“**下载**”限制优先于“**按文件类型限制下载**”。

不安全内容

通过此策略，当最终用户通过 Citrix Enterprise Browser 访问 SaaS 或内部 Web 应用程序时，启用/禁用其访问不安全内容的功能。不安全内容是指通过 HTTP 链接而非 HTTPS 链接从网页链接到的任何文件。默认值：已启用。

下图展示了当您访问不安全内容时的一个通知示例。



键盘记录保护

通过此访问策略，当用户通过 Citrix Enterprise Browser 访问 SaaS 或内部 Web 应用程序时，启用/禁用键盘记录器捕获击键的功能。默认值：已启用。

麦克风

通过此策略，当用户通过 Citrix Enterprise Browser 访问 SaaS 或内部 Web 应用程序时，每次访问麦克风时提示/不提示用户。默认值：每次都提示。

最终用户必须使用 Citrix Enterprise Browser 126 或更高版本才能访问已启用“**麦克风**”限制的应用程序。

若要每次都允许麦克风而不进行提示，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[Configure access policies](#)。
2. 在“**操作**”中，选择“**允许（带限制）**”。
3. 单击“**麦克风**”，然后单击“**编辑**”。
4. 在“**麦克风设置**”页面中，单击“**始终允许访问**”。
5. 单击“**保存**”，然后单击“**完成**”。

注意：

- 如果在 **安全私有访问** 策略中启用了 **麦克风** 限制，则 **Citrix 企业浏览器** 会显示设置 **允许**。
- 如果 **安全私有访问** 策略中的选项为 **每次提示**，则 **Citrix 企业浏览器** 上应用的设置会因是否使用 **全局应用程序配置服务 (GACS)** 来管理 **Citrix 企业浏览器** 而异。
- 如果使用 GACS，则 GACS 设置将应用于 **Citrix 企业浏览器**。
- 如果不使用 GACS，则 **Citrix 企业浏览器** 会显示设置 **询问**。
- 目前，Secure Private Access 不支持阻止麦克风。如果必须阻止麦克风，则必须通过 GACS 进行操作。

有关 GACS 的更多信息，请参阅 [通过全局应用配置服务管理 Citrix Enterprise Browser](#)。

通知设置

允许/每次提示用户通过 Citrix Enterprise Browser 访问使用此策略配置的 SaaS 或内部 Web 应用程序时查看通知。默认值：每次提示。

最终用户必须使用 Citrix Enterprise Browser 126 或更高版本才能访问已启用此限制的应用程序。

要阻止通知而不进行提示，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[Configure access policies](#)。
2. 在**操作**中，选择**允许（带限制）**。
3. 单击**通知**，然后单击**编辑**。
4. 在**通知设置**页面中，单击**始终阻止通知**。
5. 单击**保存**，然后单击**完成**。

粘贴

启用/禁用通过 Citrix Enterprise Browser 访问 SaaS 或内部 Web 应用程序时，使用此访问策略将复制的数据粘贴到其中。默认值：已启用。

注意：

- 如果策略中同时启用了**剪贴板**和**粘贴**限制，则**剪贴板**限制优先于**粘贴**限制。
- 最终用户必须使用 Citrix Enterprise Browser 版本 126 或更高版本才能访问已启用此限制的应用程序。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

启用/禁用通过 Citrix Enterprise Browser 访问 SaaS 或内部 Web 应用程序时，使用此策略编辑或屏蔽个人身份信息 (PII)。个人身份信息可以是信用卡号、社会安全号、日期等。您还可以定义自定义规则来检测特定类型的敏感信息并进行相应的屏蔽。**个人数据屏蔽**限制还提供完全或部分屏蔽信息的选项。

注意：

最终用户必须使用 Citrix Enterprise Browser 版本 126 或更高版本才能访问已启用此限制的应用程序。否则，应用程序访问将受到限制。

要编辑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 **操作** 中，选择 **允许受限访问**。
3. 单击 **个人数据掩码**，然后单击 **编辑**。
4. 选择要模糊或屏蔽的信息类型，然后单击 **Add**。

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. 选择屏蔽类型。

- **Full masking** – 完全覆盖敏感信息，使其无法读取。
- **Partial masking** – 部分覆盖敏感信息。仅覆盖相关部分，其余部分保持不变。

当您选择 **部分掩码** 时，您必须选择从文档开头或结尾开始的字符。您必须在 **第一个掩码字符** 和 **最后一个掩码字符** 字段中输入数字。

Preview 字段显示屏蔽格式。此预览不适用于自定义策略。

6. 单击 **Save**，然后单击 **Done**。

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** 中，选择 **自定义**，然后单击 **添加**。
2. 在 **Field name** 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. 选择一种掩码类型，如果您想掩盖完整信息或前几个或后几个字符。
6. 单击 **保存**，然后单击 **完成**。



下图显示了一个示例应用程序，其中 PII 已被掩码。该图还显示了与 PII 掩码相关的通知。



弹出窗口

当通过 Citrix Enterprise Browser 访问时，启用/禁用在此策略中配置的 SaaS 或内部 Web 应用程序中弹出窗口的显示。默认情况下，网页中的弹出窗口是禁用的。默认值：始终阻止弹出窗口。

最终用户必须使用 Citrix Enterprise Browser 126 或更高版本才能访问已启用此限制的应用程序。

要启用弹出窗口显示，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 **操作** 中，选择 **允许（带限制）**。
3. 单击 **弹出窗口**，然后单击 **编辑**。
4. 在 **弹出窗口设置** 页面中，单击 **始终允许弹出窗口**。
5. 单击 **保存**，然后单击 **完成**。

打印

通过 Citrix Enterprise Browser 访问时，使用此策略启用/禁用来自配置的 SaaS 或内部 Web 应用程序的打印数据。默认值：已启用。

当最终用户尝试打印已启用打印限制的应用程序中的内容时，将显示以下消息。



注意：

如果策略中同时启用了**打印**和**打印机管理**限制，则**打印**限制优先于**打印机管理**限制。

打印机管理

通过 Citrix Enterprise Browser 访问时，使用此策略启用/禁用通过使用管理员配置的打印机从配置的 SaaS 或内部 Web 应用程序打印数据。

注意：

- **打印机管理**限制除了**打印**限制（其中打印功能已启用或禁用）之外还可用。如果访问策略中同时启用了**打印**和**打印机管理**限制，则**打印**限制优先于**打印机管理**限制。
- 最终用户必须使用 Citrix Enterprise Browser 版本 126 或更高版本才能访问已启用此限制的应用程序。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. 在操作中，选择**允许受限访问**。
3. 点击“**打印机管理**”，然后点击“**编辑**”。



1. 根据您的要求选择例外项。

- **网络打印机** - 网络打印机是可以连接到网络并供多个用户使用的打印机。
 - **已禁用**：禁止从网络中的任何打印机进行打印。
 - **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，则除指定的打印机之外的所有其他网络打印机都将被阻止。

注意：网络打印机通过其主机名进行识别。

- **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。此连接通常通过 USB、并行端口或其他直接接口实现。
 - **已禁用：**禁止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**
 - **已禁用：**禁止将应用程序中的内容保存为 PDF 格式。
 - **已启用：**允许将应用程序中的内容保存为 PDF 格式。

2. 点击“保存”。

如果网络打印机被禁用，则当最终用户尝试在“**目标**”字段中选择打印机时，该特定打印机名称将显示为灰色。

此外，如果禁用了**使用另存为 PDF 打印**，则当最终用户单击**目标**字段中的**查看更多**链接时，**另存为 PDF** 选项将显示为灰色。

如果最终用户重命名网络打印机，则他们无法使用该网络打印机。



屏幕捕获

当通过 Citrix Enterprise Browser 使用任何屏幕捕获程序或应用程序访问 SaaS 或内部 Web 应用程序时，此策略可启用/禁用捕获屏幕的能力。如果用户尝试捕获屏幕，则捕获到的是空白屏幕。默认值：已启用。

按文件类型限制上传

当通过 Citrix Enterprise Browser 访问 SaaS 或内部 Web 应用程序时，此策略可启用/禁用用户下载特定 MIME（文件）类型的能力。

注意：

- **按文件类型限制上传限制**除了上传限制之外还可用。
- 如果策略中同时启用了**上传**和**按文件类型限制上传限制**，则**上传限制**优先于**按文件类型限制上传限制**。
- 最终用户必须使用 Citrix Enterprise Browser 版本 126 或更高版本才能访问已启用此限制的应用程序。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**操作中**，选择**允许（带限制）**。
3. 单击**按文件类型限制上传**，然后单击**编辑**。
4. 在**按文件类型设置上传限制**页面中，选择以下选项之一：

允许所有上传（有例外） – 上传所有文件，但选定类型除外。 **阻止所有上传（有例外）** – 阻止所有文件类型上传，但选定类型除外。

5. 如果列表中不存在该文件类型，请执行以下操作：
 - a. 单击**添加自定义 MIME 类型**。
 - b. 在**添加 MIME 类型**中，以 `category/subcategory<extension>` 格式输入 MIME 类型。例如，`image/png`。
 - c. 单击**完成**。

MIME 类型现在显示在例外列表中。

当最终用户尝试上传受限文件类型时，Citrix Enterprise Browser 会显示警告消息。



上传

启用/禁用用户通过 Citrix Enterprise Browser 访问此策略配置的 SaaS 或内部 Web 应用程序时上传的能力。默认值：已启用。

注意：

如果策略中同时启用了**上传**和**按文件类型上传限制**，则**上传限制**优先于**按文件类型上传限制**。

水印功能

启用/禁用用户屏幕上的水印，该水印显示用户的用户名和用户计算机的 IP 地址。默认值：已禁用。

网络摄像头

每次都提示/不提示用户访问通过 Citrix Enterprise Browser 访问的、在此策略配置的 SaaS 或内部 Web 应用程序中的网络摄像头。默认值：每次都提示。

最终用户必须使用 Citrix Enterprise Browser 126 或更高版本，才能访问已启用 **Webcam** 限制的应用程序。

若要每次都允许网络摄像头访问而不进行提示，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“操作”中，选择“允许受限”。
3. 单击 **Webcam**（网络摄像头），然后单击 **Edit**（编辑）。
4. 在“网络摄像头设置”页面中，单击“始终允许访问”。
5. 单击 **Save**（保存），然后单击 **Done**（完成）。

注意：

- 如果在安全私有访问策略中启用了网络摄像头限制，则 Citrix 企业浏览器会显示允许设置。
- 如果在安全私有访问策略中启用了每次都提示选项，则 Citrix 企业浏览器上应用的设置会因是否使用全局应用程序配置服务 (GACS) 来管理 Citrix 企业浏览器而异。
- 如果使用 GACS，则 GACS 设置将应用于 Citrix 企业浏览器。
- 如果不使用 GACS，则 Citrix 企业浏览器会显示询问设置。
- 目前，Secure Private Access 不支持阻止网络摄像头。如果必须阻止网络摄像头，则必须通过 GACS 进行操作。

有关 GACS 的更多信息，请参阅 [通过全局应用程序配置服务管理 Citrix Enterprise Browser](#)。

针对安全组的剪贴板功能限制

您可以将剪贴板访问权限限制到任何指定的应用程序组。这些指定的应用程序组被创建为安全组，以便最终用户只能在该安全组内复制和粘贴内容。要在安全组中的应用程序内启用剪贴板访问，您只需配置一个访问策略，其操作为 **允许** 或 **允许受限**，而不选择任何访问设置。

- 启用 **安全组** 限制后，您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”，即使两个组都启用了 **复制 / 粘贴** 限制，您也无法将内容从“Edocs”复制/粘贴到“ProdDocs”。
- 对于不属于安全组的应用程序，您可以创建一个访问策略，其操作为 **允许受限**，并选择限制（**复制、粘贴** 或 **剪贴板**）。在这种情况下，应用程序不属于安全组，因此可以对该应用程序应用 **复制 / 粘贴** 限制。

注意：

您还可以通过全局应用程序配置服务 (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，则使用 **启用沙盒剪贴板** 选项来管理剪贴板访问。当您通过 GACS 限制剪贴板访问时，它适用于通过 Citrix Enterprise Browser 访问的所有应用程序。有关 GACS 的更多信息，请参阅 [通过全局应用程序配置服务管理 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 **应用程序**，然后单击 **安全组**。
2. 单击 **添加新安全组**。



1. 输入安全组的名称。
2. 在 **添加 Web 或 SaaS 应用程序** 中，选择您要分组以后启用复制和粘贴控制的应用程序。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/粘贴控制](#)。

当最终用户从 Citrix Workspace 启动这些应用程序（Wikipedia、Pinterest 和 Dribble）时，他们必须能够在安全组内的一个应用程序与其他应用程序之间共享数据（复制/粘贴）。复制/粘贴的发生不受已为应用程序启用的其他安全限制的影响。

但是，最终用户无法将其机器上的本地应用程序或未发布的应用程序中的内容复制并粘贴到这些指定应用程序，反之亦然。当内容从指定应用程序复制到另一个应用程序时，将显示以下通知：

粘贴错误(/zh-cn/citrix-secure-private-access/media/spa-pasting-blocked.png)

注意：

您可以使用**高级剪贴板设置**中的选项，在安全组中的应用程序与计算机上的其他本地应用程序或未发布的Web应用程序之间复制和粘贴内容。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/粘贴控制](#)。

启用精细级别复制/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。您可以通过为应用程序创建访问策略并根据您的要求启用**复制/粘贴**限制来实现此目的。

注意：

请务必确保您为精细级别剪贴板访问而专门创建的特定访问策略，其优先级必须高于您为安全组所创建的策略。

示例：

假设您创建了一个包含三个应用程序（即维基百科、Pinterest 和 Dribbble）的安全组。

现在，您希望限制将内容从维基百科或 Dribbble 粘贴到 Pinterest。为此，请执行以下步骤：

1. 创建或编辑分配给应用程序 **Pinterest** 的访问策略。有关创建访问策略的详细信息，请参阅[配置访问策略](#)。
2. 在操作中，选择**允许（带限制）**。
3. 选择**粘贴**。

尽管 Pinterest 是一个安全组的一部分，该安全组也包含维基百科和 Dribbble，但用户无法将内容从维基百科或 Dribbble 复制到 Pinterest，因为与 Pinterest 关联的访问策略已启用**粘贴**限制。

粘贴错误2(/zh-cn/citrix-secure-private-access/media/spa-printing-block-example.png)

为本机应用程序和未发布的应用程序启用复制/粘贴控制

您可以使用“**高级剪贴板设置**”中的选项，在安全组中的应用程序与计算机上的其他本地应用程序或未发布的 Web 应用程序之间复制和粘贴内容。

1. 创建一个安全组。有关详细信息，请参阅[用于复制和粘贴限制的剪贴板安全组](#)。
2. 展开“**高级剪贴板设置**”。



3. 请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** – 启用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** - 启用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** – 启用将数据从未通过 Secure Private Access 发布的应用程序复制到安全组中的应用程序。
- **允许将数据从本机应用程序复制到安全组** - 启用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 > 应用程序域) 中的路由表会保留已删除应用程序的域。因此，这些应用程序在 Secure Private Access 中也被视为已发布的应用程序。如果直接从 Citrix Enterprise Browser 访问这些域，则无论您在“高级剪贴板设置”中选择了哪些选项，都将禁用从这些应用程序复制/粘贴。

例如，请假设以下场景：

- 您已删除名为 Jira2 (<https://test.citrite.net>) 的应用程序，该应用程序曾是某个安全组的一部分。
- 您已启用选项“允许将数据从安全组复制到未发布的域”。

在此场景下，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，粘贴控件将被禁用。系统会向用户显示相关通知。

- 对于 SaaS 应用程序，如果应用程序配置了操作为 **拒绝访问** 的访问策略，则应用程序访问可能会被拒绝。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，则安全组设置将不被遵守，因此您无法从该应用程序复制/粘贴内容。

最终用户流程

SaaS 应用程序

假设管理员已为最终用户配置了带有水印和打印限制的 Office 365 应用程序。现在，当最终用户访问 Office 365 应用程序时，水印和打印限制必须应用于该应用程序。

最终用户必须执行以下步骤才能访问 Office 365 应用程序：

1. 从 Citrix 工作区™ 应用访问店面™ 商店。
2. 登录到商店。
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 Office 365 应用程序已启动并包含水印。此外，如果最终用户尝试从 Office 365 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[将商店 URL 添加到 Citrix Workspace 应用程序](#)。

TCP/UDP 应用程序

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

1. 登录到 Citrix 安全访问™ 客户端。
2. 在安全访问会话已成功建立之后，您可以启动远程桌面连接。



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

现已建立远程桌面连接，最终用户可与远程计算机进行交互。

升级

您可以将 Secure Private Access 部署升级到新版本，而无需首先设置新机器或站点。在升级之前，我们建议您创建快照或保存配置。要开始升级，请运行新版本的安装程序以升级以前安装的 Secure Private Access 插件。

升级顺序

升级顺序如下所示：

1. Secure Private Access 的升级方式取决于您最初的安装方式：您可以通过 Delivery Controller™ 进行升级，也可以通过安装程序 UI 中的专用 Secure Private Access 磁贴进行升级。
 - 如果您通过 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](#)。
 - 如果您通过专用 安全私有访问 磁贴安装了 安全私有访问，则可以独立升级它。有关详细信息，请参阅 [升级您的 安全私有访问 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，以便您可以适应新功能。

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. 在 **Internet 信息服务 (IIS) 管理器** 控制台上重新启动 **默认网站** 和 **Citrix 访问安全管理站点** 以应用更改。
4. 再次运行 StoreFront 配置。从 **Settings > Configuration** 下载 StoreFront 脚本，并在相应的 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。

5. （可选）运行 NetScaler 网关脚本。有关详细信息，请参阅 [NetScaler 网关](#)。

组件的升级

有关本地部署的 Secure Private Access 中涉及的组件升级，请参阅以下主题。

- [云连接器](#)
- [应用商店](#)
- [网思网关](#)
- [许可证服务器](#)
- [Web 工作室](#)
- [导向器](#)

升级您的安全私有访问安装程序

1. 从 <https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/> 下载 Citrix 安全私有访问 2407 安装程序。
2. 在已加入域的计算机上以管理员身份运行 .exe 文件。
3. 请遵循屏幕上的指示，以完成安装过程。



重要提示：

将安装程序升级到 2407 版本后，您必须重新运行 StoreFront™ 脚本，以便新的端点详细信息可用。

后续步骤

- [设置 安全专用访问](#)
- [对 NetScaler 网关进行配置](#)
- [配置应用程序](#)
- [配置应用程序的访问策略](#)

使用脚本升级数据库

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

1. 以管理员权限打开 PowerShell 或命令提示符窗口。
2. 将目录更改为 安全专用访问 安装文件夹下的 管理员\AdminConfigTool 文件夹（例如，cd "C:\程序文件\Citrix\Citrix 访问安全\Admin\AdminConfigTool"）。
3. 运行以下命令：

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

管理配置

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](#)

管理安装完成后的各项设置

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。

管理管理员用户

您可以从 **设置 > 管理员** 页面查看管理员列表并添加管理员。首次安装 Secure Private Access 的管理员被授予完全权限。此管理员随后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能获得访问权限。

1. 在 **管理员** 页面中，单击 **添加**。

2. 在 **域** 中，选择必须添加此管理员的域。
3. 在 **用户或用户组** 中，选择用户或此用户所属的组。
4. 在 **管理员类型** 中，选择必须分配给此用户的权限类型。

修改集成配置的各项设置

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 网关条目。

1. 单击 **设置 > 集成**。
2. 点击与您要修改的设置在同一行的编辑图标，并更新条目。
3. 点击刷新图标，以确保各项设置均有效。

注意：

如果安全私有访问安装在与 StoreFront 不同的计算机上，则下载 StoreFront 脚本并在 StoreFront 上运行它。



管理应用程序和策略

配置应用程序和访问策略后，您可以根据需要对其进行编辑。

编辑应用程序

1. 在 Secure Private Access 管理控制台中，单击“**应用程序**”。
2. 单击要修改的应用程序所在行中的省略号按钮，然后单击“**编辑应用程序**”。
3. 编辑应用程序详细信息。
4. 单击“**保存**”。



编辑访问策略

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



未经批准的网站

未在 Secure Private Access 中配置的应用程序（内网或互联网）被视为“未经批准的网站”。默认情况下，如果未配置任何应用程序和访问策略，Secure Private Access 将拒绝访问所有内网 Web 应用程序。

对于所有其他未配置应用程序的互联网 URL 或 SaaS 应用程序，管理员可以使用管理控制台中的“**设置 > 未经批准的网站**”选项卡，以通过 Citrix Enterprise Browser 允许或拒绝访问。

注意：

默认情况下，设置配置为允许通过 Citrix Enterprise Browser 访问所有互联网 URL 或 SaaS 应用程序。

未经批准的网站的工作原理

1. 执行 URL 分析检查以确定该 URL 是否为 Citrix® 服务 URL。
2. 然后检查该 URL 以确定它是否为企业 Web 或 SaaS 应用程序 URL。
3. 然后检查该 URL 以确定它是否被识别为被阻止的 URL，或者该 URL 是否可以被允许访问。

下图说明了最终用户流量的传输过程。

最终用户流量流(/zh-cn/citrix-secure-private-access/media/website-filtering-onprem.png)

当请求抵达时，系统会执行以下检查，并采取相应的措施：

1. 请求是否与全局允许列表匹配？
 - a. 如果匹配，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，以下序列将决定操作。
 - i. 阻止
 - ii. 允许
 - b. 如果不匹配，则应用默认操作（允许）。默认操作无法更改。

配置未经授权网站的规则

1. 在 Secure Private Access 管理控制台中，单击 **设置 > 非授权网站**。

注意：

- Web 过滤功能默认启用，允许访问所有非授权互联网 URL。
- 您可以将设置更改为 **阻止所有用户访问非授权网站**，以通过 Citrix Enterprise Browser 阻止所有用户访问任何互联网 URL。



您还可以通过将特定 URL 添加到阻止网站或允许网站来更改其设置。

例如，如果您默认阻止了所有非授权 URL 的访问，并且只想允许访问少数几个特定的互联网 URL，则可以执行以下步骤：

- a. 单击 **允许的网站** 选项卡，然后单击 **允许网站**。
- 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，也可以拖放包含网站地址的 CSV 文件。
- c. 单击 **添加 URL**，然后单击 **保存**。

该 URL 已添加到允许的网站列表。

卸载安全私有访问

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

1. 选择 **Citrix 虚拟应用和桌面™ 7 2408 – 安全私有访问**。
2. 单击“**卸载**”。
3. 请按照屏幕上的说明操作，并完成卸载过程。

注意：

如果安全专用访问的安装后设置已完成，那么在卸载安全专用访问之前，请从管理控制台下载 StoreFrontScripts.zip 文件，以从 StoreFront 商店配置中删除安全专用访问插件。

要下载 StoreFrontScripts zip 文件，请按照以下步骤操作：

1. 登录安全私有访问管理控制台。

2. 单击“**设置**”，然后单击“**集成**”选项卡。
3. 在“StoreFront 商店 URL”部分中单击“**下载脚本**”。

从 StoreFront 商店配置中删除安全私有访问插件

在您完成 Secure Private Access 的卸载操作之后，您必须从 StoreFront 的商店配置中移除其插件。

1. 登录 StoreFront 所在的计算机。
2. Download the StoreFrontScripts.zip file.
3. Unzip StoreFrontScripts.zip to a folder.
4. 以管理员权限打开 PowerShell 窗口。
5. 运行以下命令：

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

监控和故障排除

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 期间或之后，您可能会遇到与以下方面相关的问题：

- 证书相关的错误
- 数据库创建错误
- 思杰店面故障
- 公共网关/回调网关故障
- 安全私有访问服务器不可达

有关解决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控和故障排除，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。如果这不能解决问题，请联系支持人员。

参考资料

- [使用 安全私有访问 配置 Director](#)
- [在 Director 中查看安全私有访问会话](#)
- [Director 中的安全私有访问会话代码。](#)
- [管理控制台。](#)

仪表板概览

故障排除仪表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线的日志。您可以使用“[添加筛选器](#)”选项，根据应用程序类别、用户名、事务 ID 等各种条

件优化搜索。例如，在搜索字段中，您可以按此顺序选择“事务 ID”、“=（等于某个值）”，然后输入 7456c0fb-a60d-4bb9-a2a2-edab8340bb15，以搜索与此事务 ID 相关的所有日志。

您可以根据要在仪表板中查看的信息，通过单击“+”号向图表添加列。您可以将用户日志导出为 CSV 格式。



您可以使用以下搜索运算符，通过“**添加筛选器**”选项优化搜索：

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

例如，您可以在搜索字段中使用字符串“**事件类型 > =（等于某个值） > 枚举**”来搜索事件类型“枚举”。

同样，要搜索部分包含术语“operator”的用户，请使用字符串“**用户名 > ~（包含某个值） > operator**”。此搜索会列出所有包含术语“operator”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，最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，以查找与特定应用程序访问请求相关的所有日志。

从日志中查看上下文标记

“详细信息”列中的“显示详细信息”链接显示与特定访问策略关联的应用程序列表以及与该策略关联的上下文标记。如果配置了 nFactor 身份验证，则为当前用户验证的 nFactor EPA 操作名称也会作为上下文标记的一部分进行捕获。



基本故障排除

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

证书错误

数据库创建错误

店面故障

公共网关/回调网关故障

安全私有访问服务器不可达

杂项

证书相关错误

错误消息：无法自动从一个或多个网关服务器获取证书。

当您尝试添加公共 NetScaler® Gateway 地址并且在获取证书时出现问题时，会出现此错误消息。此问题可能在设置 Secure Private Access 时或在设置完成后更新设置时发生。

解决方法：以与 Citrix 虚拟应用和桌面 相同的方式更新网关证书。

数据库创建错误

- **错误消息：**未能创建数据库

解决方案：对于自动情况 - 计算机必须具有在 SQL Server 上的数据库中创建表的读取、写入、更新权限。

- **错误消息：**创建数据库失败：数据库已存在。

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，则该数据库必须为空。如果数据库为非空数据库，则可能会出现此错误消息。

解决方案：您必须创建一个空数据库。

- 您卸载 Secure Private Access 并使用相同的站点名称重试设置。在这种情况下，以前安装的数据库将不会被删除。

解决方案：您必须手动删除数据库。

- 您选择通过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，运行脚本时已创建同名数据库。

解决方案：您必须重命名站点，然后再次运行脚本。

- 计算机没有在 SQL Server 上的数据库中创建表的 READ、WRITE、UPDATE 权限。

解决方案：在计算机上启用适当的权限。有关详细信息，请参阅[设置数据库所需的权限](#)。

- **错误消息：**创建数据库失败：连接失败

解决方案：

- 检查计算机与数据库的网络连接。确保防火墙上已打开 SQL Server 端口。
- 如果使用远程 SQL 服务器，请检查 SQL 服务器是否已使用 Secure Private Access 计算机身份 Domain\hostname\$ 创建登录名。
- 如果使用远程 SQL 服务器，请确认计算机身份已分配正确的角色，即系统管理员角色。
- 如果使用本地 SQL 服务器（非安装程序自带），请检查 NT AUTHORITY\SYSTEM 用户是否必须创建登录名。

思杰店面故障

- **错误消息：**未能为 <Store URL> 创建 StoreFront 条目

如果 StoreFront 条目不可见，请从**设置**选项卡更新它们。使用向导设置 Secure Private Access 后，您可以从**设置**选项卡编辑 StoreFront 条目。记下发生此错误的 StoreFront 商店 URL。

解决方案：

- 单击**设置**，然后单击**集成**选项卡。
- 在**StoreFront 商店 URL**中，如果 StoreFront 条目不可见，请添加该条目。

- **错误消息：**未能为 <Store URL> 配置 StoreFront 条目

解决方案：

- 可能存在 PowerShell 执行策略限制。运行 PowerShell 脚本命令 `Get-ExecutionPolicy` 以获取详细信息。
- 如果受到限制，您必须绕过此限制并手动运行 StoreFront 配置脚本。
- 单击**设置**，然后单击**集成**选项卡。
- 在**思杰店面商店 URL**中，识别发生错误的思杰店面 URL 条目。
- 单击此商店 URL 旁边的**下载脚本**按钮，并在安装了相应 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

If you are retrying the installation after uninstalling, ensure that you don't have an entry with the name "Secure Private Access" in the StoreFront configuration (**StoreFront > store> Delivery Controller™ -> Secure Private Access**). If Secure Private Access is present, delete this entry. Manually download and run the script from the Settings > Integrations page.

- **错误消息：**StoreFront 配置不是本地的： <Store URL>

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

解决方案：

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

- 单击“**设置**”，然后单击“**集成**”选项卡。
- In **StoreFront Store URL**, identify the StoreFront URL entry for which the error occurred.
- 单击此商店 URL 旁边的“下载脚本”按钮，并在安装了相应 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

To run the StoreFront PowerShell script, open the Windows x64 compatible PowerShell window with admin privileges and then run ConfigureStorefront.ps1. StoreFront script is not compatible with Windows PowerShell (x86).

- **Error message:** "Get-STFStoreService : Exception of type 'Citrix.DeliveryServices.Framework.Feature.Exceptions.RegistryKeyNotFoundException' was thrown." while running StoreFront script using PowerShell.

当在 x86 兼容的 PowerShell 窗口中运行 StoreFront 脚本时，会出现此错误。

解决方案：

若要运行 StoreFront PowerShell 脚本，您需要以管理员权限打开兼容 Windows x64 的 PowerShell 窗口，然后执行 `ConfigureStorefront.ps1`。

公共网关/回调网关故障

错误消息：未能为 `<Gateway URL>` 创建网关条目 或 未能为 `<Callback Gateway URL>` 创建回调网关条目

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，您可以从“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. 更新发生故障的公共网关地址或回调网关地址以及虚拟 IP 地址。

安全私有访问服务器不可访问

错误消息：未能更新 IIS 池。未能重新启动 IIS 池

解决方案：

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

- 安全私有访问运行时池
- 安全私有访问管理员池

另请检查默认 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

数据库连接检查失败可能有多种原因：

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

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 插件主机没有连接到数据库的权限。

解决方案：请参阅 [安全私有访问的 SQL 数据库权限](#)。

网关连接性检查失败。未能成功获取公共证书

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传到 Secure Private Access 数据库。
- 以管理员权限打开 PowerShell 或命令提示符窗口。
- Change the directory to the Admin\AdminConfigTool folder under the Secure Private Access installation folder (for example, 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 (/)，则应用程序的枚举功能将无法正常工作。

解决方案：

删除 StoreFront 商店网址或 NetScaler Gateway 网址中的尾部斜杠。有关详细信息，请参阅 [设置后更新 StoreFront 或 NetScaler Gateway 服务器详细信息](#)。

其他事项

首次设置未能成功完成

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

解决方案：

手动清理 license_server 表中的数据。

创建安全私有访问诊断支持捆绑包

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

- 以管理员权限打开 PowerShell 或命令提示符窗口。

- Change the directory to the Admin\AdminConfigTool folder under the Secure Private Access installation folder (for example, cd "C:\Program Files\Citrix\Citrix Access Security\Admin\AdminConfigTool").
- 运行以下命令：

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

安全私有访问的 SQL 数据库权限

对于自动数据库创建，Secure Private Access 插件主机必须具有连接到数据库并创建数据库架构的权限。

远程数据库：

要设置远程数据库的权限，请执行以下步骤。

1. 使用名称语法 `CitrixAccessSecurity<Site Name>` 创建一个空数据库。其中 `<Site Name>` 是安全私有访问站点名称。（例如：CitrixAccessSecuritySPA）。

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

2. 为 Secure Private Access 虚拟机的计算机标识创建 SQL Server 登录名。例如，如果您的 Secure Private Access 代理计算机名称为 HOST1 且计算机域为 DOMAIN1，则计算机标识为“DOMAIN1\HOST1\$”。如果已创建登录名，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 角色分配给计算机标识。

```
USE CitrixAccessSecurity<SiteName>
```

```
EXEC sys.sp_addrolemember [db_owner], 'DOMAIN1\HOST1$'
```

```
ALTER USER [DOMAIN1\HOST1$] WITH DEFAULT_SCHEMA = dbo;
```

本地数据库：

要设置本地数据库的权限，请执行以下步骤。

1. 创建一个空数据库，其命名语法为 `CitrixAccessSecurity<Site Name>`。其中 `<Site Name>` 是安全私有访问 站点名称。（例如，`CitrixAccessSecuritySPA`）。

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

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

```
USE CitrixAccessSecurity<SiteName>
```

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

3. 将数据库所有者角色分配给“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。

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。

To change the log level for the troubleshooting logs, in the runtime service appsettings.json (C:\Program Files\Citrix\Citrix Access Security\Runtime\RuntimeService) update

`restrictedToMinimumLevel` for `TroubleshootingSql` to one of the following values:

- Information
- Debug
- Warning
- Error

```
"TroubleshootingSql": {
  "restrictedToMinimumLevel": "Error",
  "batchPostingLimit": 50,
```

```
"batchPeriod": "00:00:05" // 5 seconds

}
```

应用程序启动问题或 Citrix Secure Access 登录失败

如果 Netscaler Gateway 证书轮换，则应用程序的启动或 Citrix Secure Access 的登录将无法进行。

解决方案： 在 Secure Private Access 管理控制台中刷新证书。

1. 导航到 **设置 > 集成**。
2. 在 **公共 NetScaler Gateway 地址**部分中，单击 **刷新证书**。

刷新过程可能需要几分钟才能完成。

有关详细信息，请参阅修改集成设置。

Director 中的安全私有访问会话代码

Director 与安全私有访问集成，实现了有效的性能监控和故障排除，因为安全私有访问设置中所有组件的问题都会在 Director 中捕获。以下表格列出了 Director 中显示的不同错误代码和相关条件。

有关详细信息，请参阅以下主题。

- [配置 Director 与安全私有访问](#)
- [在 Director 中查看安全私有访问会话](#)

注意：

- 第二位数字包含“0”的代码表示正常的执行流程。例如，1000 表示应用程序枚举成功。
- 第二位数字包含“1”的代码表示失败或异常。例如，2101 表示会话失败。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。

会话代码

代码	状态	详细说明
2101	失败	会话失败。

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

应用程序枚举相关代码

代码	状态	描述信息
1101	失败	在枚举过程中发生了一个内部错误。
1102	失败	枚举了一些应用程序，但至少有一个应用程序评估失败。
1103	失败	没有枚举任何应用程序，并且至少有一个应用程序评估失败。
1000	成功	枚举成功。至少枚举了一个应用程序。
1001	成功	没有枚举任何应用程序，因为它们都被策略拒绝了。
1002	成功	未枚举任何应用程序，因为没有策略匹配。
1003	成功	未枚举任何应用程序，因为某些应用程序被拒绝，而其他应用程序没有策略匹配。
1004	成功	未枚举任何应用程序，因为没有要评估的策略。
3101	失败	应用程序枚举 - 发生内部错误（当前未使用）。

代码	状态	描述信息
3102	失败	未枚举应用程序，因为在策略评估期间发生异常。
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	检索应用程序策略详细信息时出错。
3000	允许	允许应用程序枚举。
3001	拒绝	策略拒绝应用程序枚举。
3002	拒绝	未枚举应用程序，因为没有策略匹配。
3003	未知	应用程序枚举状态未知。
3004	从 CEB 启动应用程序	由 Citrix Enterprise Browser 所进行的应用程序启动的尝试性操作行为。

应用程序启动消息代码

代码	状态	详细说明
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	检索应用程序策略详细信息时出错。
4104	失败	应用程序启动错误 - 未找到应用程序配置。
4000	允许	允许应用程序启动。
4001	拒绝	由于策略原因，应用程序启动被拒绝。

代码	状态	详细说明
4002	拒绝	由于没有匹配的策略，应用程序启动被拒绝。

SIEM 集成

安全私人访问插件支持与安全信息和事件管理 (SIEM) 服务的集成。安全事件实时存储到 Windows 事件日志（事件查看器\应用程序和服务日志\Citrix Access Security），并可通过第三方工具进行收集和分析。

下表列出了安全私人访问插件安全事件：

事件 ID	总结	说明	源
4624	帐户已成功登录	当 Secure Private Access 管理员登录 Secure Private Access 管理控制台时创建的事件	Citrix Access 安全管理服务
4625	帐户登录失败	当 Secure Private Access 管理员无法登录 Secure Private Access 管理控制台时创建事件	Citrix Access 安全管理服务
4634	帐户已注销	当 Secure Private Access 管理员从 Secure Private Access 管理控制台注销时创建事件	Citrix Access Security 管理服务
4720	已创建用户帐户	添加新的安全私人访问管理员时创建的事件	Citrix Access Security 管理服务
4738	用户帐户已更改	当新的安全私人访问管理员更新时创建事件	Citrix Access Security 管理服务

事件 ID	总结	说明	源
4726	用户帐户已被删除	当新的安全私人访问管理员被删除时创建事件	Citrix Access Security 管理服务
8001	用户安全访问会话	当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 管理服务
8002	用户访问授权请求	当安全私人访问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 管理服务

引用

- [安全信息和事件管理 \(SIEM\) 集成](#)
- [关于将日志共享至 SIEM 解决方案](#)

斯科特集成

Citrix Scout 与 Secure Private Access 集成，以帮助管理员收集日志和指标进行故障排除。有关收集的信息，请参阅 [收集了哪些信息](#)。

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

1. 选择一台安全私有访问计算机以开始收集。
2. 单击 **继续**。

您可以随时单击 **停止收集** 以停止收集。

Citrix Scout 还会检索以下日志。这些日志以捆绑包的形式存储在本地计算机中，并可以上传到 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

日志在 Secure Private Access 数据库中存储七天。如果日志总数变得过大（例如超过 100,000 条），您可以删除早于 90 天的最旧日志。清理作业默认每 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的保留设置

日志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。您可以根据日志的保留时间和数据库中可存储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：

以下是 `appsettings.json` 文件的示例内容：

```
"TroubleshootingLogs": {  
  
  "CleanupPeriodInHours": 12,  
  
  "CleanupDataOlderThanDays": 7,  
  
  "CleanupOldestDataIfEntriesCountAbove": 0  
  
}
```

要禁用清理，请根据需要配置以下设置：

- 要仅保留 7 天的日志，请将 `CleanupDataOlderThanDays` 设置为 7。
- 要禁用基于天数的清理，请将 `CleanupDataOlderThanDays` 设置为 0。
- 要禁用基于数量的清理，请将 `CleanupOldestDataIfEntriesCountAbove` 设置为 0。
- 如果这两个设置都设置为 0，或者如果 `CleanupPeriodInHours` 设置为 0，则日志将永久保留。
 - 不建议将 `CleanupDataOlderThanDays` 或 `CleanupOldestDataIfEntriesCountAbove` 都设置为 0，或者将 `CleanupPeriodInHours` 设置为 0，因为这可能会导致 100% 的磁盘使用问题。
 - 日志清理频率也可以通过修改 `CleanupPeriodInHours` 条目来更改。

注意：

如果 Secure Private Access 作为群集部署，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，则清理最频繁的实例将优先。

日志和遥测清理

遥测数据清理

遥测数据在 Secure Private Access 数据库中存储 3 个月。每 30 秒执行一次检查，以识别需要清理的遥测数据。

注意：

运行时服务必须运行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 Admin 和运行时服务的安装文件夹中。CDF 日志以 .csv 文件形式存储，每个文件的大小限制为 10MB。Admin 服务一次最多可保留 90 个 CDF 日志文件，之后会删除最旧的文件，为创建新的 CDF 日志文件腾出空间。运行时服务的工作方式与 Admin 服务相同，但一次可以保留更多文件，最多 600 个。

CDF 日志的自定义清理

CDF 日志清理可通过 Admin 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计数限制，请更新 appsettings.json 文件中的以下条目：

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

注意：

如果您的站点配置了多个 Secure Private Access 实例，则需要更新每台 Secure Private Access 安装机器上的 appsettings.json 配置文件，以便进行 CDF 日志清理操作。

第三方通知事项

思杰安全私有访问 适用于本地部署