



Citrix Secure Private Access - 本地

Contents

新增功能	5
2023 年 10 月	5
思杰安全私有访问™ 本地部署版 — 预览	5
已知问题	6
域控制器配置相关问题	6
网思乐® 网关	6
Web 版接收器 / Web 版工作区	6
应用程序图标	6
管理员管理	7
升级	7
斯托弗 朗特™	7
日志记录	7
安全专用访问安装程序	8
管理控制台的 SSO	8
后续步骤	9
使用脚本升级数据库	10
设置安全私有访问	11
先决条件	11
通过创建新站点设置安全私有访问	11
步骤 1: 设置安全私有访问站点	11
步骤 2: 配置数据库	11
步骤 3: 对 StoreFront 和 NetScaler® 网关服务器进行集成	13
步骤 4: 配置摘要	13
通过加入现有站点设置安全私有访问	14
后续步骤	14
Configure NetScaler Gateway	15

在具有现有配置的 NetScaler 网关上配置安全私有访问	16
NetScaler Gateway 虚拟服务器上的相关配置设置	16
NetScaler 网关会话操作	17
与 ICA® 应用程序的兼容性	18
支持智能访问标签	18
已知限制和注意事项	19
上传公共网关的证书	19
配置应用程序	20
后续步骤	21
如何为应用程序配置访问策略	22
访问策略优先级	23
后续步骤	23
最终用户流程	24
安全私有访问与 Web Studio 集成	25
安装完成后管理设置	26
管理应用程序域的路由	26
管理安全私有访问的管理员	26
在设置完成后，更新 StoreFront™ 或 NetScaler Gateway 的服务器相关详细信息	26
仪表板概述	28
查看日志中的上下文标记	29
故障排除错误	30
证书相关错误	30
数据库创建错误	30
StoreFront™ 相关的故障和问题	31
公共网关/回调网关故障	32
安全私有访问服务器不可达	33
数据库连接检查失败	33
网关连接性检查失败。无法获取公共证书	33

身份验证问题	34
其他问题	34
创建安全私有访问诊断支持捆绑包	34
“安全专用访问”的 SQL 数据库权限	34
卸载 安全专用访问	36
从 StoreFront 商店配置中删除 安全私有访问 插件	36
安全私有访问 2308 与旧版本的兼容性	37
Citrix 虚拟应用和桌面™ 交付控制器清理	37
Citrix StoreFront cleanup	38
NetScaler 网关的清理工作	38
NetScaler 网关虚拟服务器	38
会话策略和操作	39
授权策略规则	39
第三方通知事项	40

新增功能

2023 年 10 月

思杰安全私有访问™ 本地部署版 — 预览

Citrix Secure Private Access 本地部署版现已推出预览版。Secure Private Access 本地部署解决方案包含一个功能齐全的管理控制台 UI，其外观和使用体验与 Secure Private Access 服务类似。有关详细信息，请参阅 [Secure Private Access 本地部署版 – 预览](#)。

已知问题

Citrix Secure Private Access™ 的本地部署解决方案存在以下已知问题：

域控制器配置相关问题

- 不支持同一林中或不同林之间域的单向信任。如果满足以下两个条件，则 Secure Private Access 本地解决方案将无法工作。
 - 安装了本地部署的 安全私有访问 的计算机的域与登录到 安全私有访问 的管理员的域不同。
 - 从计算机域到用户域之间尚未配置任何信任关系。
- 如果 SAM 账户名和用户主体名称不同，则枚举失败。

网思乐® 网关

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](#)。

Web 版接收器 / Web 版工作区

RfWeb / Workspace for web 不受支持。尽管应用程序已枚举，但应用程序启动可能会失败。

应用程序图标

仅支持 ICO 图标格式。不支持 PNG、JPEG 和其他格式。

管理员管理

- 管理员的 RBAC 角色更改仅在当前会话失效（通过注销或令牌过期）后才会反映。
- 管理员用户不得属于默认的 "Domain Users" AD 组，因为此类用户的身份验证会失败。

升级

版本到版本升级不受支持。内部部署的 Secure Private Access 会提示您在版本到版本升级中删除现有安装并重新安装。

斯托弗 特™

- 在 **应用商店 > 配置统一体验** 中，网站的默认接收方必须配置为 /Citrix/ <StoreName> Web。在早期版本的 StoreFront 中，网站的默认接收方设置为空值，这不适用于 Secure Private Access。此外，客户端上会显示早期版本的 Receiver UI。
- 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功能不受支持。
- 管理员和运行时服务的日志文件夹不得删除。如果这些文件夹被删除，Secure Private Access 无法重新创建。

安全专用访问安装程序

您可以通过运行 SecurePrivateAccessSetup_2308.exe 安装程序来安装安全私有访问。

1. 从 <https://www.citrix.com/downloads/citrix-early-access-release/> 下载 Citrix 安全专用访问安装程序。
2. 在已加入域的计算机上以管理员身份运行 .exe 文件，最好是在安装了 StoreFront™ 的同一台计算机上。
3. 请按照屏幕上显示的说明来完成安装。

安装完成后，首次设置管理控制台将在默认浏览器窗口中自动打开。您可以单击“继续”以设置安全专用访问。

您还可以在桌面“开始”菜单中看到安全专用访问快捷方式 (Citrix > Citrix Secure Private Access™)。

管理控制台的 SSO

建议您为您用于安全专用访问管理控制台的浏览器配置 Kerberos 身份验证。这是因为安全专用访问使用集成 Windows 身份验证 (IWA) 进行其管理员身份验证。

如果未设置 Kerberos 身份验证，在访问安全专用访问管理控制台时，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，则会显示 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。您可以使用与安装计算机属于同一域的任何用户来设置 Secure Private Access，前提是该用户在安装计算机上具有本地管理员权限。

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

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 Secure Private Access 统一资源定位符。

如果计划在多台计算机上安装安全私有访问，您也可以使用通配符。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：

- 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 思杰网关](#)
- [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

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. 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").
3. 运行以下命令：

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

设置安全私有访问

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 管理控制台来设置 Secure Private Access 环境。

- [通过创建新站点设置安全私有访问](#)
- [通过加入现有站点设置安全私有访问](#)

先决条件

在创建站点之前，必须安装 SQL 数据库服务器。

通过创建新站点设置安全私有访问

通过创建新站点设置安全私有访问

步骤 1: 设置安全私有访问站点

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

1. 启动安全私有访问 Web 管理控制台。
2. 在“创建或加入站点”页面上，“创建新的 Secure Private Access 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，必须自动或手动为新站点配置数据库，因为与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 站点创建一个数据库。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`。

您可以按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** 字段中，为 Secure Private Access 站点输入一个名称。
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：

- 如果站点没有可用的 SQL Server，连接性检查将失败。
- 如果 SQL Server 可用但数据库不存在，连接性检查将通过。但是，将显示警告消息。
- 安全私有访问使用计算机身份的 Windows 身份验证对 SQL Server 进行身份验证。

自动配置：

- 仅当计算机标识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，则会自动创建一个数据库。
- 创建数据库时，请确保其为空，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，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 Server 数据库中创建表所需的 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：对 StoreFront 和 NetScaler® 网关服务器进行集成

您必须指定 StoreFront 和 NetScaler 网关服务器详细信息，以将安全专用访问与 StoreFront 和 NetScaler 网关服务器连接。必须建立此连接才能使 StoreFront 和 NetScaler 网关将流量路由到安全专用访问。

1. 输入以下详细信息。

- **安全专用访问服务器地址。**例如， `https://secureaccess.domain.com`。
- **StoreFront 应用商店网址。**例如， `https://storefront.domain.com/Citrix/StoreMain`。
- **公共网关地址 – NetScaler Gateway 的统一资源定位符 (URL)。**例如， `https://gateway.domain.com`。
- **网关回调地址 –** 此 URL 必须与 StoreFront 中配置的 URL 相同。例如， `https://gateway.domain.com`。
- **网关 VIP –** 此虚拟 IP 地址必须与 StoreFront 中为回调配置的地址相同。

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，将执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。



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 Secure Private Access 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。您可以从**设置 > 管理员**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”。

数据库配置(/zh-cn/citrix-secure-private-access/media/spaop-firsttime-select-site1a.png)

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，键入安全私有访问站点的名称。
4. 单击“测试连接”以检查 SQL Server 实例是否有效，并确认指定站点是否存在于数据库中。

数据库配置(/zh-cn/citrix-secure-private-access/media/spaop-databse-config-1a.png)

如果站点没有对应的数据库，则连接性检查将失败。

5. 单击“保存”。

将执行配置验证检查，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。

后续步骤

- [配置 网络加速器网关](#)
- [配置应用程序](#)
- [配置应用程序的访问策略](#)

Configure NetScaler Gateway

重要提示：

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-early-access-release/>` 下载脚本。

To create a new NetScaler Gateway, use `ns_gateway_secure_access.sh`. To update an existing NetScaler Gateway, use `ns_gateway_secure_access_update.sh`.

2. 将这些脚本上传到 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*`。

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 登录到 NetScaler 并切换到命令行界面（在 NetScaler 命令行界面中输入 '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 的命令行界面中运行上传的脚本。



6. 输入所需的参数。有关参数列表，请参阅 [Prerequisites](#)。

对于身份验证配置文件和 SSL 证书，您必须在 NetScaler 上提供名称。

将自动生成一个包含一组多个 NetScaler 命令的新文件（其默认路径为 `var/tmp/ns_gateway_secure_access`）。



7. 切换到 NetScaler CLI，并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 会逐一运行文件中的命令。如果某个命令失败，它会继续执行下一个命令。

如果资源已存在或在步骤 6 中输入的某个参数不正确，则命令可能会失败。

8. 确保所有命令都已成功完成。

注意：

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

在具有现有配置的 NetScaler 网关上配置安全私有访问

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 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对其进行审查，并创建网关配置的备份。

NetScaler Gateway 虚拟服务器上的相关配置设置

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。

tcpProfileName: nstcp_default_XA_XD_profile deploymentType: ICA_STOREFRONT icaOnly: OFF

示例：

要添加虚拟服务器：

```
`add vpn vserver _SecureAccess_Gateway SSL 333.333.333.333 443
-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：

```
`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 网关会话操作

会话操作通过会话策略绑定到网关虚拟服务器。创建会话操作时，请确保以下参数设置为定义的值。

- `transparentInterception` : 关闭
- `SSO` : ON
- `ssoCredential` : 主要
- `useMIP` : NS
- `useIIP` : 关闭
- `icaProxy` : 关闭
- `wihome` : "https://storefront.mydomain.com/Citrix/MyStoreWeb" - 替换为真实的商店 URL
- `ClientChoices` : 关闭
- `ntDomain` : mydomain.com - used for SSO
- `defaultAuthorizationAction` : 允许
- `authorizationGroup` : SecureAccessGroup (请确保已创建此组，它用于绑定安全私有访问的特定授权策略)
- `clientlessVpnMode` : 开启
- `clientlessModeUrlEncoding` : 透明
- `SecureBrowse` : 已启用
- `Storefronturl` : "https://storefront.mydomain.com"
- `sfGatewayAuthType` : 域

示例：

添加会话操作：

```
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
```

更新会话操作：

```
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/zh-cn/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，您必须配置安全票证颁发机构 (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

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。

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

- 您可以使用命令（FreeBSD shell）进行切换：

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

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

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

- 要禁用，请再次运行相同的命令。
- 要验证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《在 NetScaler Gateway 上配置自定义标签（智能访问标签）》。

已知限制和注意事项

- 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。
- 请勿在 NetScaler 网关上使用 ICA 代理。配置 NetScaler 网关时，此功能将被禁用。
- 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 与其他组件在特定端口上进行通信。
- 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.

上传公共网关的证书

要将公共网关证书上传到 Secure Private Access 数据库，请执行以下步骤：

1. 以管理员权限打开 PowerShell 或命令提示符窗口。
2. 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"`)
3. 运行以下命令：

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

配置应用程序

1. 选择应用程序所在的位置。

- 对于外部应用程序，选择**我的公司网络外部**。
- 对于内部应用程序，选择**我的公司网络内部**。

2. 在“应用程序详细信息”部分输入以下详细信息，然后单击**下一步**。



- **应用程序名称** – 应用程序的名称。
- **应用程序描述** - 应用程序的简要描述。此描述将显示在用户的工作区中。您还可以按 **KEYWORDS: <keyword_name>** 格式为应用程序输入关键字。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，也可以使用 Citrix Workspace UI 中的现有类别。为 Web 或 SaaS 应用程序指定类别后，该应用程序将显示在 Workspace UI 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”字段中错误地将“业务和生产力”类别输入为“业务和生产”，则除了“业务和生产力”类别之外，Citrix Workspace UI 中还会列出一个名为“业务和生产”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。 **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作为收藏应用程序添加到 Citrix Workspace 应用程序中。

- **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带挂锁的星形图标。

如果从 Secure Private Access 控制台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”。

3. 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](#)

如何为应用程序配置访问策略

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，您还可以通过添加安全限制来启用对应用程序的受限访问。

1. 单击 **创建策略**。



2. 在 **应用程序** 中，选择要强制执行访问策略的应用程序。
3. 在 **用户/用户组** 中 – 选择条件以及用户或用户组，以确定是否允许或拒绝应用程序访问。
 - **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被允许访问。
 - **不匹配以下任意项**：除了字段中列出的用户或组之外，所有用户或组都允许访问。
4. 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。
5. 选择 **条件标签**，然后选择基于此允许或拒绝应用程序访问的条件。
6. 在 **然后执行以下操作** 中，选择基于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**

当您选择 **允许受限访问** 时，您可以选择以下限制。



- **限制剪贴板访问**：禁用应用程序与系统剪贴板之间的剪切/复制/粘贴操作。
- **限制打印**：禁用从 Citrix Enterprise Browser 内部进行打印的功能。
- **限制下载**：禁用用户从应用程序内部进行下载的功能。
- **限制上传**：禁用用户在应用程序内部进行上传的功能。
- **显示水印**：在用户屏幕上显示水印，其中包含用户的用户名和用户计算机的 IP 地址。
- **限制键盘记录**：防止键盘记录器。当用户尝试使用用户名和密码登录应用程序时，所有按键都会在键盘记录器上加密。此外，用户在应用程序上执行的所有活动都受到键盘记录保护。例如，如果为 Office 365 启用了应用程序保护策略，并且用户编辑 Office 365 Word 文档，则所有击键都会在键盘记录器上加密。

- **限制屏幕捕获**：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，则会捕获空白屏幕。

注意：

键盘记录和屏幕捕获限制仅适用于 Citrix Workspace™ 桌面客户端。

7. 在“策略名称”中，输入策略的名称。
8. 选择“保存时启用策略”。如果未选择此选项，则只会创建策略，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，默认情况下会为该访问策略分配一个优先级编号。您可以在“访问策略”主页上查看优先级。

值越低的优先级具有最高的偏好，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。

示例

最终用户流程

假设管理员已为最终用户配置了带有水印和打印限制的 Office365 应用程序。现在，当最终用户访问 Office365 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 Office365 应用程序：

1. 从 思杰工作区™ 应用程序访问 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。

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



注意：

管理员必须向用户提供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](#)。

安全私有访问与 Web Studio 集成

Citrix Secure Private Access™ is also integrated into the Web Studio console to enable users seamlessly access the service through Web Studio.

您必须安装 Web Studio 2308 或更高版本。

执行以下步骤以启用 Web Studio 集成：

1. Install Citrix Web Studio by using the Citrix Virtual Apps and Desktops™ installer or integrated DDC installer.
2. 按照屏幕上的说明完成安装。当系统提示输入控制器地址时，输入 DDC FQDN 作为控制器地址。
3. After successful installation, navigate to the folder C:\Program Files\Citrix\Web Studio\Site\assets\json and modify the content of the spa-config.json file. If a non-default location was used for the Web Studio installation, replace the default installation location in C:\Program Files\Citrix with the correct location.



1. 将“SpaServer”替换为您的安全私有访问插件的 FQDN。
2. 登录到 Web 工作室。



1. 在左侧导航菜单中，单击 **Secure Private Access** **<Preview>** 以从 Web Studio 访问安全私有访问管理控制台。

安装完成后管理设置

安装 Secure Private Access 后，您可以从“设置”页面修改设置。

管理应用程序域的路由

您可以查看 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。

管理安全私有访问的管理员

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

在设置完成后，更新 StoreFront™ 或 NetScaler Gateway 的服务器相关详细信息

在完成 Secure Private Access 的部署和配置后，您可以前往“**集成**”选项卡，对 StoreFront 和 NetScaler® Gateway 的相关条目进行修改或更新操作。

1. 单击 **设置 > 集成**。
2. 单击您要修改的设置所在行中的编辑图标，然后更新该条目。
3. 单击刷新图标，以确保这些设置是有效的。

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。

安装后的设置([/zh-cn/citrix-secure-private-access/media/spaop-manage-settings-dayn.png](#))

仪表板概述

Secure Private Access 故障排除日志仪表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线的日志。您可以通过单击“+”号向图表添加列，具体取决于您希望在仪表板中看到的信息。您可以将用户日志导出为 CSV 格式。

您可以使用筛选器（类别和结果）来优化搜索结果。



您还可以依据下列参数，并结合搜索字段中提供的运算符，对您的搜索进行细化。

- 用户名
- 类别
- 事件类型
- 结果
- 事务 ID
- 详细信息

以下是您可以在“用户日志”和“按强制执行划分的顶级访问策略”图表中用于优化搜索的搜索运算符。

- =：用于搜索与搜索条件完全匹配的日志/策略。
- !=：用于搜索不包含指定条件的日志/策略。
- ~：搜索部分匹配搜索条件的日志/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”。

同样地，要搜索部分包含术语“operator”的用户，请使用字符串 **User-Name ~ 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 关联了访问请求的所有 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记

详细信息列中的[显示详细信息](#)链接会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。



故障排除错误

本主题列出了在设置 Secure Private Access 时可能会遇到的一些错误。

[证书错误](#) [数据库创建错误](#) [StoreFront 故障](#) [公共网关/回调网关故障](#) [Secure Private Access 服务器不可达](#)

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。 **解决方法：**按照更新 Citrix Virtual Apps and Desktops 网关证书的相同方式更新网关证书。

数据库创建错误

- **错误消息：**创建数据库失败

解决方案：对于自动情况 - 计算机必须具有在 SQL 服务器上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。

此错误消息可能在以下任何情况下发生。

- 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，则该数据库必须是空数据库。如果数据库不是空数据库，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，之前安装的数据库可能未被删除。

解决方案：您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，在运行脚本时，已创建了一个同名数据库。

解决方案：您必须重命名站点，然后再次运行脚本。

- 该计算机没有在 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：**创建数据库失败：连接失败

解决方案：

- 检查您的计算机与数据库的网络连接。确保 SQL Server 端口在防火墙上已打开。
- 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 Server，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 Server（非安装程序），请检查 NT AUTHORITY\SYSTEM 用户是否必须创建登录名。

StoreFront™ 相关的故障和问题

- **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：

- a. 单击“**设置**”，然后单击“**集成**”选项卡。
- b. 在 **StoreFront 商店 URL** 中，如果 StoreFront 条目未显示，请将其添加。

- **错误消息：**未能配置 StoreFront 条目，原因： <Store URL>

解决方案：

- a. 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。
- b. 如果受到限制，您必须绕过此限制并手动运行 StoreFront 配置脚本。
- c. 单击 **设置**，然后单击 **集成** 选项卡。
- d. 在 **StoreFront 商店网址** 中，识别发生错误的 StoreFront 网址条目。
- e. 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。

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，原因： <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。您必须在安装了 StoreFront 的计算机上手动运行 StoreFront 配置。

- a. 单击 **设置**，然后单击 **集成** 选项卡。
- b. In **StoreFront Store URL**, identify the StoreFront URL entry for which the error occurred.
- c. 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。

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).

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达

错误消息：未能更新 IIS 池。未能重新启动 IIS 池

解决方案：

1. 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
- 安全私有访问管理池

还要检查默认的 IIS 站点 `"Default Web Site"` 是否正常运行。

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，Secure Private Access 插件主机无法访问数据库服务器。
****解决方案：****检查数据库端口（默认端口 1433）是否在防火墙上打开。
- 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。无法获取公共证书

****错误消息：****安装后配置失败，出现错误“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>
```

身份验证问题

Secure Private Access 运行时服务 IIS 身份验证配置可能无法正常工作，因为不支持集成 Windows 身份验证 (IWA)。

其他问题

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。
- 请将您的当前工作目录切换到安全私有访问产品的安装文件夹中名为 Admin\AdminConfigTool 的子文件夹。例如，您可以通过在命令行界面中输入并执行以下命令来完成此操作：cd "C:\Program Files\Citrix\Citrix Access Security\Admin\AdminConfigTool"。
- 运行以下命令：

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

“安全专用访问”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和创建数据库架构的权限。

远程数据库：

请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 虚拟机创建机器身份的 SQL Server 登录名。例如，如果您的 Secure Private Access 代理计算机名称是 HOST1，计算机域是 DOMAIN1，则机器身份是“DOMAIN1\HOST1\$”。如果登录名已创建，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 角色分配给机器身份。

```
USE CitrixAccessSecurity<SiteName>
```

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

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

本地数据库：

请执行以下步骤，为本地数据库设置权限。

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 `NT AUTHORITY\SYSTEM` 用户创建 SQL 服务器登录。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. Assign the db_owner role to the “NT AUTHORITY\SYSTEM” user.

```
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。

卸载 安全专用访问

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 2308 – 安全专用访问**。
2. 单击“**卸载**”。
3. 按照屏幕上的说明进行操作，并完成卸载。

注意：

如果 安全专用访问 的安装后设置已完成，则在卸载 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. 登录到安全专用访问管理控制台。
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

卸载 安全私有访问 后，您必须从 StoreFront 商店配置中删除 安全私有访问 插件。

1. 登录到安装了 StoreFront 的计算机。
2. Download the StoreFrontScripts.zip file.
3. 请将 StoreFrontScripts.zip 文件解压到任意一个文件夹中。
4. 以管理员权限打开 PowerShell 窗口。
5. 运行以下命令：

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

安全私有访问 2308 与旧版本的兼容性

安全私有访问 2308 与旧版本（本地部署版安全私有访问 V1.0 和 V1.5）不兼容。必须使用新脚本配置 NetScaler 网关，具体方法如之前在 [配置 NetScaler 网关](#) 中所述。对于安全私有访问 2308，Citrix 虚拟应用和桌面交付控制器中无需进行任何配置。

从本地部署的 Secure Private Access 旧版本（1.0 和 1.5）迁移到 2308 的最佳方法是清理以下内容：

- Citrix 虚拟应用和桌面 交付控制器，用于 Web/软件即服务应用程序
- 将 Citrix StoreFront™ 更新为默认配置或在 StoreFront 上创建新应用商店
- 网思乐® 网关

Citrix 虚拟应用和桌面™ 交付控制器清理

在 Citrix 虚拟应用和桌面 交付控制器上创建的 安全私有访问 应用程序可以手动删除或使用 PowerShell 脚本删除。

手动：

1. Open Citrix Studio or Citrix WebStudio.
2. 单击“应用程序”。
3. 选择应用程序，右键单击，然后选择“删除”。

使用脚本：

1. 通过运行以下命令获取当前的 Secure Private Access 应用程序：

```
Get-BrokerApplication -Description "KEYWORDS:SPAENABLED"
```

For details, see [Remove-BrokerApplication](#).

2. 验证应用程序后，运行以下命令将其删除：

```
Get-BrokerApplication -Description "KEYWORDS:SPAENABLED" | Remove-BrokerApplication
```

Citrix StoreFront cleanup

您可以创建新的 StoreFront 商店，也可以清理现有商店。

- 创建新的 StoreFront 商店：您必须为 Secure Private Access 2308 创建新的 StoreFront 商店，因为为旧版本创建的现有 StoreFront 商店与 2308 不兼容。这是避免配置相关问题的推荐选项。
- 清理现有 StoreFront 商店：StoreFront 上的现有商店可以手动清理，也可以使用脚本清理。但是，将本地 Secure Private Access 迁移到 2308 的最佳选择是在 StoreFront 上创建新商店。

手动：

1. Find and remove policy.json (e.g C:
\\inetpub\\wwwroot\\Citrix\\Store\\Resources\\SecureBrowser\\policy.json)
2. Find and remove folders SecureBrowser (for example C:
\\inetpub\\wwwroot\\Citrix\\Store\\Resources\\SecureBrowser) and Resources (for example C:
\\inetpub\\wwwroot\\Citrix\\Store\\Resources)
3. Remove the "route" node from web.config (you can find it in C:\\inetpub\\wwwroot\\Citrix\\Store\\
with the name "webSecurePolicy" routing to the URL "Resources\\SecureBrowser\\policy.json"
4. 重新启动 **Internet 信息服务 (IIS) 管理器** 上的默认网站 控制台以应用更改。

使用脚本：

1. 从 <https://www.citrix.com/downloads/citrix-secure-private-access/> 下载脚本。
2. 将脚本上传到 StoreFront 计算机。
3. 在 PowerShell 上以管理员身份运行脚本。
4. 输入应用商店名称。

该脚本会删除位于 C:\\inetpub\\wwwroot\\Citrix\\Store\\Resources 的文件夹、其所有子文件夹以及其中的文件，并对 web.config 文件进行更新。

5. 重新启动 **Internet 信息服务 (IIS) 管理器** 中的默认网站 控制台以应用更改。

NetScaler 网关的清理工作

NetScaler 网关虚拟服务器

为旧版本（1.0 和 1.5）创建的 NetScaler 网关虚拟服务器可用于安全私有访问 2308。

- 要更新现有的 NetScaler 网关，请参阅。
- 要配置新的 NetScaler 网关，请参阅。

会话策略和操作

为旧版本（1.0 和 1.5）创建的会话策略和操作可由 Secure Private Access 2308 重复使用。

- 要更新现有的 NetScaler 网关 会话策略/操作，请参阅 [NetScaler 网关 会话操作](#)。
- 要配置新的 NetScaler 网关，请参阅 [配置 NetScaler 网关](#)

脚本还会创建完全配置的会话策略/操作。

授权策略规则

在 NetScaler Gateway 上为旧版本（1.0 和 1.5）创建的授权策略可能会干扰 Secure Private Access 2308 策略并中断流程。

您可以执行以下操作来清理授权策略。

- 手动解除授权策略与在 NetScaler Gateway 上用作默认组的身份验证和授权组的绑定。在这种情况下，策略可以重复使用。
- 对授权策略进行移除。

第三方通知事项

Citrix 本地安全专用访问