新增功能

2023 年 12 月

思杰安全私有访问™ 本地部署版 – 正式发布

Citrix Secure Private Access 本地部署版现已作为 Citrix Virtual Apps and Desktops 2311 版本的一部分正式发布。Citrix Secure Private Access 本地部署解决方案通过能够轻松地为基于浏览器的应用程序（内部 Web 应用程序和 SaaS 应用程序）提供零信任网络访问，从而增强了组织的整体安全性和合规性态势，同时使用 StoreFront 作为 Web 和 SaaS 应用程序的统一访问门户，以及作为 Citrix Workspace 集成部分的虚拟应用程序和桌面。该解决方案与现有版本的 NetScaler 和 StoreFront 兼容，无需更改版本。有关详细信息，请参阅 Secure Private Access 本地部署版。

与 思杰虚拟应用和桌面™ 集成的安全私有访问安装程序

Secure Private Access 安装程序已与 Desktop Delivery Controller (DDC) 集成，现在可以使用命令行和 GUI 进行安装。有关详细信息，请参阅 安装核心组件。

已知问题

Citrix Secure Private Access™ 本地部署解决方案存在以下已知问题，这些问题计划在未来版本中解决。

域控制器配置设置

- 不支持不同 AD 林之间域的信任类型为“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 Secure Private Access 本地部署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：

  - 在 IIS 应用程序池中，为 Secure Private Access Admin 和 Runtime 服务添加一个不同的域服务帐户作为标识。

- Secure Private Access 不支持用于内网 (StoreFront) 登录和互联网/外网 (网关) 应用程序枚举的备用 UPN 后缀。
- Secure Private Access 不支持分布式组。因此，策略无法搜索分布式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。

网思乐® 网关

在以下场景中不支持具有 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 / 网络版工作区

不支持 RfWeb / Web 版 Workspace。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）后才会生效。

升级

不支持从 2308 升级到 2311 及更高版本。您必须卸载 2308 并重新安装所需版本（2311 及更高版本）。

思拓方™

- 在 **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。在早期版本的 StoreFront 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 UI。
- 如果您使用的是 StoreFront 2308 或更早版本，则 **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

- 针对群集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。

安装安全私有访问的管理员帐户要求

- 要安装 Secure Private Access，您必须使用本地计算机管理员帐户登录。
- 要设置 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。
- 设置完成后，该用户将成为第一个 Secure Private Access 管理员，然后可以添加其他管理员。

- 设置完成后，要管理安全私有访问，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。

安全限制规定

如果最初发布的关联域被替换为不同的域，则与应用程序相关的安全限制将无法生效。

例如，您创建一个应用程序，其关联域为 `edition.test.com`，并对该应用程序强制执行打印限制和水印。当访问应用程序 URL 时，将强制执行安全限制。但是，如果您编辑同一应用程序并将关联域 `edition.test.com` 替换为 `*.1800flowers.com`，则当访问新的应用程序 URL 时，将不强制执行安全限制。

管理控制台

发布应用程序的“**编辑应用程序**”页面（**Secure Private Access > 应用程序 > 编辑应用程序**）在关联域条目修改后不会自动关闭。

例如，如果您在创建应用程序时输入的关联域是 `www.example.com`。应用程序发布后，您将关联域 `www.example.com` 替换为 `abc.com`，然后单击“**保存**”。“**编辑应用程序**”页面不会关闭，尽管应用程序已成功更新。

“卸载或更改程序”页面中的安装程序显示

当您使用 ISO 文件将 Secure Private Access 从 2308 升级到 2311 时，“**卸载或更改程序**”页面（**控制面板 > 程序 > 程序和功能**）会显示 Secure Private Access 安装程序的两个条目，而不是替换初始条目。

- **Citrix 虚拟应用和桌面™ 7 2311**
- **Citrix 虚拟应用和桌面 7 2308 - 安全专用访问**

您可以卸载预览版安装程序，方法是选择 **Citrix Virtual Apps and Desktops 7 2308 - 安全专用访问**。

> **注意：**
>
> 当使用 2311 独立安装程序升级 Secure Private Access 2308 独立安装程序时，未观察到此问题。

安全私有访问安装程序

1. 从 `<https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/>` 下载思杰安全私有访问安装程序。
2. 在已加入域的计算机上以管理员身份运行 .exe 文件。

> **注意：**
>
> 出于 POC 目的，建议您将 Secure Private Access 安装在与 StoreFront™ 安装在同一台计算机上。
>
> 

3. 请按照屏幕上的指示完成安装过程。




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



您还可以在桌面“开始”菜单（**Citrix > Citrix Secure Private Access™**）上看到 安全私有访问 快捷方式。



有关详细信息，请参阅以下主题：

- 安装核心组件
- 使用命令行安装(/zh-cn/citrix-virtual-apps-desktops/install-configure/install-core/install-command)

管理控制台的 SSO

建议您为您用于 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) 进行其管理员身份验证。

如果未设置 Kerberos 身份验证，当您访问 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，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。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来设置 Secure Private Access。

对于 谷歌浏览器 和 Microsoft 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 安全私有访问 URL。

   如果计划在多台计算机上安装 Secure Private Access，也可以使用通配符。例如，`"https://*.fabrikam.local"`。
4. 单击“**自定义级别**”，然后在“**用户身份验证 > 登录**”中，选择“**使用当前用户名和密码自动登录**”。



> **注意：**

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

后续步骤

- 设置 安全私有访问
- 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\管理员配置工具 文件夹（例如，cd "C:\Program Files\Citrix\Citrix 访问安全\管理员\管理员配置工具"）。
3. 运行以下命令：

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

大小调整指南

数据库所需存储空间

大部分数据库存储空间被日志消耗。与日志相比，应用程序和策略配置的存储空间消耗可以忽略不计。

下表显示了基于用户会话、日志、每用户每天的应用枚举等参数的服务器存储要求。

用户会话	每用户每天的应用枚举	每用户每天的应用访问量	每天总应用访问量	每天消耗的存储空间	日志保留期（天）	日志保留期内的总存储使用量（7 天）
1000	20	100	100000	2.5 GB	7	17.5 GB
1000	10	50	50000	1.27 GB	7	9 GB

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，或者最多保留 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。

部署指导方针

下表显示了根据并发应用程序访问用户会话、每分钟应用程序枚举以及 Secure Private Access 使用的 CPU 等参数确定的数据库大小要求。

CITRIX SECURE PRIVATE ACCESS - 本地

并发应用程序访问用户会话	每分钟应用程序枚举	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，可以在与 StoreFront ™ 相同的计算机上部署 SPA，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。

其他组件的配置说明

组件	虚拟CPU	内存
SQL 服务器	4	16 GB

思拓方	4	8 GB
活动目录	8	16 GB

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

- 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。
- 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

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 Databases。

2. 在 **站点** 中，键入安全专用访问站点的名称。
3. 单击 **测试连接** 以检查 SQL Server 实例是否有效，并确认指定数据库是否存在于该站点。



> **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。
- Secure Private Access 使用通过计算机身份的 Windows 身份验证来对 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**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：集成 店面 和 NetScaler® 网关服务器

您必须指定 StoreFront 和 NetScaler Gateway 服务器的详细信息，以便将安全专用访问连接到这些服务器。必须建立此连接，以使 StoreFront 和 NetScaler Gateway 能够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 网关的网址。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，还会执行检查以确保 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，您可以从 Web 管理控制台中的“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。您可以采用以下形式之一指定数据库地址：

   - 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 Secure Private Access 站点键入一个名称。
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，连接性检查将失败。

5. 单击“**保存**”。

配置验证检查旨在确保 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 网思乐 网关(/zh-cn/citrix-secure-private-access/2311/spa-onprem-netscaler-gateway-config)
- 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-secure-private-access/Shell-Script/Shell-Script-for-Gateway-Configuration.html>` 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 协议连接到 NetScaler 设备并切换到命令行界面（在 NetScaler 命令行接口键入 '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 命令行界面上运行已上传的脚本。

   NetScaler 配置的第一个图示(/zh-cn/citrix-secure-private-access/media/spaop-configure-netscaler1.png)

6. 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，您必须在 NetScaler 上提供名称。

系统将自动生成一个包含多个 NetScaler 命令的新文件，该文件的默认路径为 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。

   如果资源已存在或在步骤 6 中输入的参数之一不正确，则命令可能会失败。

8. 确保所有命令都已成功完成。

> **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。

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

确保您在执行每个命令之前进行审查，并创建网关配置的备份。

NetScaler 网关虚拟服务器上的设置

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：

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`
```

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 - 此域名主要用于实现单点登录 (SSO) 功能。
- `defaultAuthorizationAction`: 允许
- `authorizationGroup`: SecureAccessGroup (请务必确保此组已成功创建，因为它将用于绑定与 Secure Private Access 相关的特定授权策略。)
- `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：思杰安全网关/ 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。

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

- 您可以使用命令（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）》。

已知的限制

- 现有 NetScaler Gateway 可以通过脚本更新，但可能存在无数种 NetScaler 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 网关后，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.

上传公共网关证书文件

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。

执行以下步骤上传公共网关证书文件：

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。Secure Private Access 插件上的上下文标签是应用于已验证用户会话的 NetScaler® Gateway 策略（会话、预身份验证、EPA）的名称。

Secure Private Access 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身份验证策略。

使用 GUI 配置自定义标签

配置上下文标签的流程中包含以下几个高级步骤。

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

配置经典网关预身份验证策略

1. 导航到 **NetScaler 网关 > 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。您可以将此操作用于多个策略，例如，使用一个操作允许访问，使用另一个操作拒绝访问。

   

4. 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-polcy-exp-editor.png)

6. 单击“**创建**”。

将自定义标记绑定到 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. 选择策略名称以及用于策略评估的优先级。
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**”，然后选择“**上下文标签**”、“**全部匹配**”，然后输入上下文标签名称（例如，`Windows10`）。

参考文献

- 为应用程序配置访问策略。
- 支持智能访问标签。

Configure StoreFront

If Secure Private Access is co-hosted with StoreFront, then the Secure Private Access configuration on StoreFront is done automatically by the first time setup wizard.

但是，如果 Secure Private Access 未与 StoreFront 共同托管，则必须手动进行某些配置更改。

执行以下步骤以手动配置 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。如果需要移除 StoreFront 和 Secure Private Access 之间的集成，可以使用清理脚本。
3. 使用命令 `./ConfigureStorefront.ps1.` 在 PowerShell 64 位实例上以管理员身份运行脚本。

   - 不需要其他任何参数。
   - 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。

StoreFront 配置了安全私有访问设置后，可以在 StoreFront 管理用户界面（**管理交付控制器**屏幕）中看到安全私有访问插件配置。

如果为 Citrix Virtual Apps and Desktops™ 交付控制器配置了相同的设置，StoreFront 脚本会自动为 Secure Private Access 配置聚合组设置。默认情况下，该脚本会为所有人配置 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 脚本来配置 StoreFront 以实现 Secure Private Access。请勿从 StoreFront 管理用户界面配置 Secure Private Access，因为该用户界面未涵盖 StoreFront 上的所有必需配置。必须运行脚本才能完成所有必要的配置。

- 一个 Secure Private Access 站点也可以配置在多个 StoreFront 部署上（无论是同一 StoreFront 上的另一个应用商店，还是不同的 StoreFront 部署）。 StoreFront 可以从“**设置 > 集成**”页面添加。
- 即使 Secure Private Access 与 StoreFront 共同托管，StoreFront 自动配置也无法从“**设置 > 集成**”页面运行。自动配置仅在首次设置期间完成。如果从“**设置**”页面添加新的应用商店配置，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。

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**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**。
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，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。管理员必须确保他们定义了正确的类别。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“Business And productivity”，则 Citrix Workspace 用户界面中除了“业务和生产力”类别之外，还会列出一个名为“Business and productivity”的新类别。
   - **应用程序图标** – 单击**更改图标**以更改应用程序图标。图标文件大小必须为 128x128 像素，并且仅支持 Ico 格式。如果您不更改图标，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，应用程序的左上角会在 Citrix Workspace 应用程序中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，应用程序的左上角会在 Citrix Workspace 应用程序中显示一个带挂锁的星形图标。

如果您从 Secure Private Access 控制台删除标记为收藏的应用程序，则必须从 Citrix Workspace 中的收藏列表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

为应用程序配置访问策略

针对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，据此必须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。
4. 单击 **添加条件** 以根据上下文标签添加另一个条件。这些标签源自 NetScaler® Gateway。
5. 选择 **条件标签**，然后选择必须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**

   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保护，以防止键

盘记录。 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，则所有按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**。如果您不选择此选项，则策略只会创建，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。

您可以通过在**优先级**列中使用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，必须在该应用程序上应用水印和打印限制。

最终用户必须执行以下步骤才能访问 Office365 应用程序：

1. 最终用户可以通过 Citrix Workspace™ 应用程序来成功访问 StoreFront™ 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 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 的集成

Citrix 安全私有访问™ 也已集成到 Web Studio 控制台中，以使用户能够通过 Web Studio 无缝访问该服务。

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. 登录到网络工作室。
3. 在左侧导航菜单中，点击 **安全专用访问** 以从网络工作室访问安全专用访问管理控制台。

将安全私有访问部署为群集

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

如果您正在使用 NetScaler 网关 13.0 或 13.1 版本，其内部版本号为 48.47 或更早，建议您将安全私有访问与 StoreFront 共同进行托管。

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。
- 将所需数量的群集节点添加到 Secure Private Access 站点。有关详细信息，请参阅 通过加入现有站点设置 Secure Private Access。
- 在每个 Secure Private Access 节点中，配置相同的服务器证书。证书主题公用名或主题备用名称必须与负载均衡器 FQDN 匹配。

负载均衡器配置

Secure Private Access 群集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：

- 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。
- 建议安全私有访问服务以 HTTPS 运行，但这并非强制性要求。它们也可以部署为 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，必须在负载均衡器服务中配置 SAN。
- 负载均衡器（例如 NetScaler）具有用于后端服务器的默认内置监视器（探测器）。如果您必须为本地 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。

安装后管理各项设置

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

要修改设置，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。

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，以便为该组中的所有管理员启用访问权限。

1. 在 **管理员** 页面中，单击 **添加**。
2. 在 **域** 中，选择必须添加此管理员的域。
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。

Update StoreFront™ or the NetScaler Gateway server details after the setup

After you have set up Secure Private Access, you can modify or update the StoreFront and NetScaler® Gateway entries from the **Integrations** tab.

1. 单击**设置 > 集成**。
2. 单击要修改的设置旁边的编辑图标，然后更新条目。
3. 点击刷新图标，以确保所有设置均已正确生效。

注意：

如果 Secure Private Access 部署在与 StoreFront 不同的服务器或计算机设备上，那么请务必下载 StoreFront 提供的脚本文件，并将其在 StoreFront 环境中运行。



仪表板概述

安全私有访问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范围内的日志。您可以根据要在仪表板中查看的信息，通过单击“+”号向图表中添加列。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。



除了搜索字段中的运算符之外，您还可以依据以下参数来进一步细化您的搜索。

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

以下是您可以用于优化用户日志和按强制执行图表划分的顶级访问策略中的搜索的运算符。

- =：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。
- ~: 用于搜索部分匹配搜索条件的日志/策略。
- !~: 用于搜索不包含某些指定条件的日志/策略。

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

同样，要搜索部分包含术语“操作员”的用户，请使用字符串 **User-Name ~ operator**。此搜索会列出所有包含术语“操作员”的用户名。例如，“本地操作员”、“管理员操作员”

您可以使用事务 ID 搜索与单个事件相关的所有日志。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 筛选故障排除日志，以查找与特定应用程序访问请求相关的所有日志。

查看日志中的上下文标签

详细信息列中的**显示详细信息**链接显示了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签。



对一些常见错误进行故障排除

本主题列出了您在设置 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

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

证书相关的错误

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**：创建数据库失败

  解决方案：对于自动情况 - 计算机必须具有 READ、WRITE、UPDATE 权限才能在 SQL Server 上的数据库中创建表。

- **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。

- 您卸载了 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，运行脚本时已创建了同名数据库。

  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 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。

StoreFront™ 故障及解决方案

- **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. In **StoreFront Store URL**, add the StoreFront entry if it is not visible.

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

  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. 如果受限，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. In **StoreFront Store URL**, identify the StoreFront URL entry for which the error occurred.

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。此脚本必须在所有 StoreFront 计算机上运行。

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

- **错误消息**：StoreFront 配置不是本地的，适用于：`<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。

a. 单击“**设置**”，然后单击“**集成**”选项卡。

b. 在**StoreFront 应用商店 URL**中，识别发生错误的 StoreFront 地址条目。

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。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，会发生此错误。

  解决方案：

  To run the StoreFront PowerShell script, open the Windows x64 compatible PowerShell window with admin privileges and then run `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无法访问

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

数据库连接检查可能因多种原因而失败：

- 数据库服务器由于防火墙原因无法从 Secure Private Access 插件主机访问。

  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 (/)，则应用程序枚举功能将无法正常工作。

解决方案：

Delete the trailing slash in the StoreFront store URL or the NetScaler Gateway URL. For details, see Update StoreFront or the NetScaler Gateway server details after the setup.

其他问题

创建安全私有访问故障诊断支持包

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：

请执行以下步骤，以配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>` 是安全私有访问的站点名称。（例如：CitrixAccessSecuritySPA）。

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

2. 为 Secure Private Access 虚拟机的计算机身份创建 SQL Server 登录名。例如，如果您的 Secure Private Access 代理计算机名称是 HOST1，计算机域是 DOMAIN1，则计算机身份是 "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：

请执行以下步骤，以配置本地数据库的权限。

1. 请创建一个空数据库，其命名应遵循 `CitrixAccessSecurity<Site Name>` 所定义的语法。在此处，`<Site Name>` 指代的是 Secure Private Access 的站点名称。（例如：CitrixAccessSecuritySPA）。

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

2. 为 `NT AUTHORITY\SYSTEM` 用户创建 SQL Server 登录名。如果登录名已创建，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。

保留故障排除日志

故障排除日志页面中的日志在 Secure Private Access 数据库中存储 90 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 天的旧日志。默认情况下，清理作业每 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 Runtime 服务的安装文件夹中的 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：

示例应用程序设置文件：

```
"TroubleshootingLogs": {

  "CleanupPeriodInHours": 12,

  "CleanupDataOlderThanDays": 90,

  "CleanupOldestDataIfEntriesCountAbove": 100000

}
```

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。
- 要禁用基于计数的清理，请将 `CleanupOldestDataIfEntriesCountAbove` 设置为 0。
- 如果这两个设置都设置为 0，或者如果 `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，或将 `CleanupPeriodInHours` 设置为 0，因为这可能会导致 100% 的磁盘使用率问题。

- 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。

日志和遥测数据清理

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 Runtime 服务的安装文件夹中。CDF 日志以 .csv 文件形式存放，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。 Runtime 服务的工作方式与 Admin 服务相同，但一次可保留更多文件，最多 600 个。

CDF 日志的自定义清理

CDF 日志清理可通过 Admin 和 Runtime 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：**

> 如果为站点设置了多个安全私有访问实例，请在每台安全私有访问安装机器上更新用于 CDF 清理的 appsettings.json 文件。

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 2308 – 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。

> **注意：**
>
> 如果安全私有访问的安装后设置已完成，则在卸载安全私有访问之前，请从管理控制台下载 StoreFrontScripts.zip 文件，以从 StoreFront 存储配置中删除安全私有访问插件。
>
> 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 存储 URL 部分中单击**下载脚本**。

从 StoreFront 商店配置中移除安全私有访问插件

卸载安全私有访问后，您必须从 StoreFront 商店配置中移除安全私有访问插件。

1. 登录 StoreFront 所在的计算机。
2. 请务必下载名为 StoreFrontScripts.zip 的文件，此文件是后续操作所必需的。
3. 将 StoreFrontScripts.zip 文件解压缩到您选择的某个文件夹中。
4. 打开一个具有管理员权限的 PowerShell 窗口。
5. 运行以下命令：

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

Secure Private Access 2311 compatibility with legacy versions

Secure Private Access 2311 is incompatible with the legacy versions. NetScaler Gateway must be configured using the new script as described earlier in Configure NetScaler Gateway. No configuration is required in the Citrix Virtual Apps and Desktops delivery controller for Secure Private Access legacy versions.

从旧版本迁移到 2311 的最佳方法是清理以下内容：

- 来自 Web/SaaS 应用程序的 思杰虚拟应用和桌面 交付控制器
- 将 Citrix StoreFront™ 更新为默认配置，或在 StoreFront 上创建新应用商店
- 网标器网关

思杰虚拟应用和桌面交付控制器清理

在 Citrix Virtual Apps and Desktops 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. 打开 Citrix **管理工作室** 或 Citrix Web **管理工作室**。
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 存储，也可以清理现有存储。

- 创建新的 StoreFront 存储：您必须为 Secure Private Access 2311 创建新的 StoreFront 存储，因为为旧版本创建的现有 StoreFront 存储与 2311 不兼容。这是避免配置相关问题的推荐选项。
- 清理现有 StoreFront 存储：StoreFront 上的现有存储可以手动清理或使用脚本清理。但是，将本地 Secure Private Access 迁移到 2311 的最佳选项是在 StoreFront 上创建新存储。

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 中以管理员身份运行脚本。
4. 输入应用商店名称。

   The Script removes the C:\inetpub\wwwroot\Citrix\Store\Resources folder, subfolder and files, and updates the web.config file.
5. 重新启动 **互联网信息服务 (IIS) 管理器上的默认网站** 控制台以应用更改。

奈思开勒网关清理

NetScaler 网关虚拟服务器

为旧版本创建的 NetScaler 网关虚拟服务器可重复用于 Secure Private Access 2311。

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

会话策略和操作

为旧版本创建的会话策略和操作可以由 Secure Private Access 2311 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

该脚本还会创建完全配置的会话策略/操作。

授权相关的策略

在 NetScaler Gateway 上为旧版本创建的授权策略可能会干扰 Secure Private Access 2311 策略并中断流程。

您可以执行以下操作来清理授权策略。

- 手动解除绑定 NetScaler Gateway 上用作默认组的身份验证和授权组中的授权策略。在这种情况下，策略可以重复使用。
- 删除这些授权策略。

第三方通知信息

Citrix 安全私有访问（本地部署版）