



Citrix Secure Private Access - 本地

Machine translated content

Disclaimer

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

Contents

新增功能	2
已知问题	2
Secure Private Access 安装程序	3
使用脚本升级数据库	8
设置 Secure Private Access	8
配置 NetScaler Gateway	15
配置应用程序	20
为应用程序配置访问策略	22
最终用户流程	25
通过 Web Studio 集成实现 Secure Private Access 集成	27
安装后管理设置	28
控制板概述	30
故障排除	32
卸载 Secure Private Access	37
Secure Private Access 2308 与传统版本的兼容性	38
第三方通知	40

新增功能

January 9, 2024

October 2023

适用于本地的 **Citrix Secure Private Access** —预览版

适用于本地的 Citrix Secure Private Access 现已推出预览版。Secure Private Access 访问解决方案包括全方位服务的管理员控制台用户界面，其外观和感觉与 Secure Private Access 服务类似。有关详细信息，请参阅[本地 Secure Private Access - 预览版](#)。

已知问题

February 20, 2024

适用于本地的 Citrix Secure Private Access 解决方案存在以下已知问题：

域控制器配置

- 不支持同一林内域之间或不同林间的域之间的单向信任。如果满足以下两个条件，则本地 Secure Private Access 解决方案不起作用。
 - 安装本地 Secure Private Access 的计算机域与登录到 Secure Private Access 的管理员的域不同。
 - 从计算机的域到用户的域都没有配置信任。
- 如果 sAMAccountName 和 UPN 不同，则枚举失败。

NetScaler Gateway

以下场景不支持带有 SSL 配置文件配置的 SSL 虚拟服务器。

- 客户使用的是 NetScaler Gateway 13.1—48.47 及更高版本或 14.1—4.42 及更高版本。
- `ns_vpn_enable_spa_onprem` 开关已启用。

解决方法：

将在 SSL 配置文件中配置的 SSL 参数直接绑定到 SSL 虚拟服务器或禁用 `ns_vpn_enable_spa_onprem` 开关。

有关开关的详细信息，请参阅 [对智能访问标签的支持](#)。

RfWeb/Workspace for Web

不支持 RfWeb /Workspace for Web。尽管对应用程序进行了枚举，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（注销或令牌到期）后才会反映出来。
- 管理员用户不得属于默认“域用户”AD 组，因为此类用户的身份验证失败。

升级

不支持按版本升级。本地 Secure Private Access 会提示您删除现有安装并在按版本升级中重新安装。

StoreFront

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

日志记录

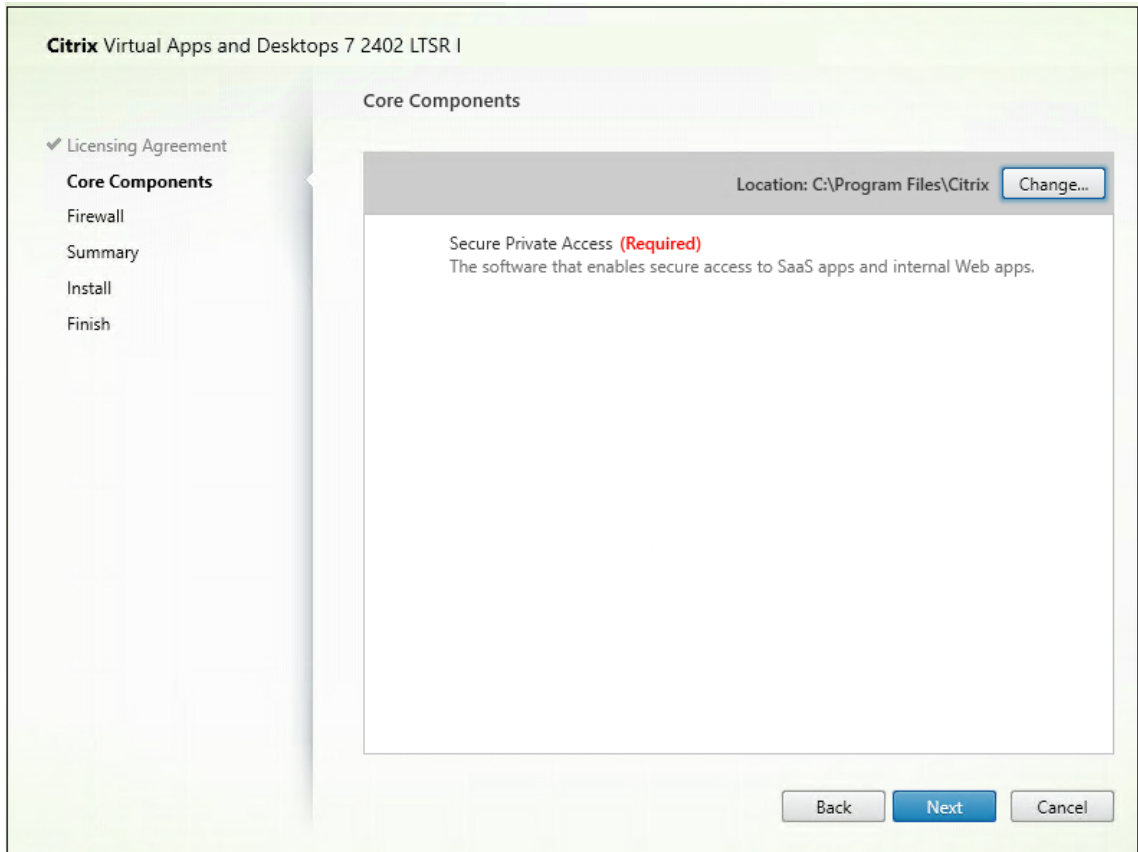
- 不支持为群集生成支持包。
- 不得删除管理员和运行时服务的日志文件夹。如果删除了这些文件夹，则无法重新创建 Secure Private Access 权限。

Secure Private Access 安装程序

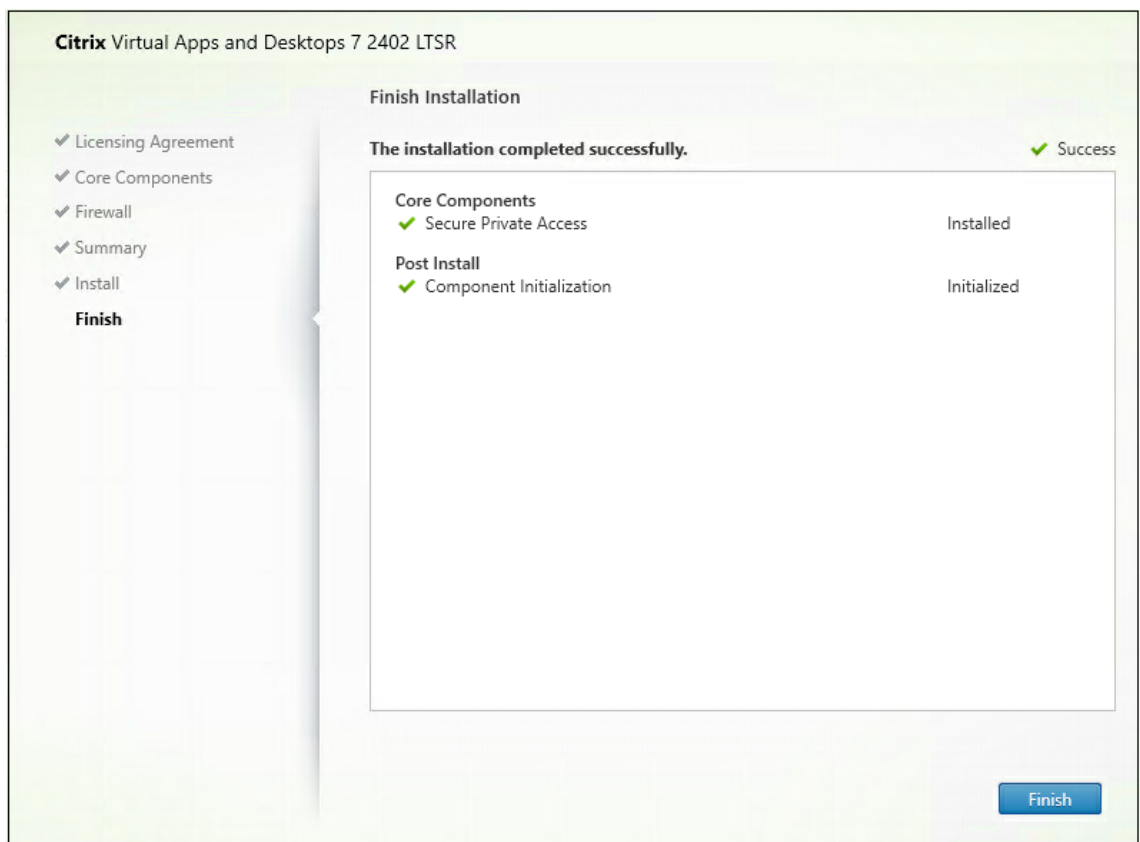
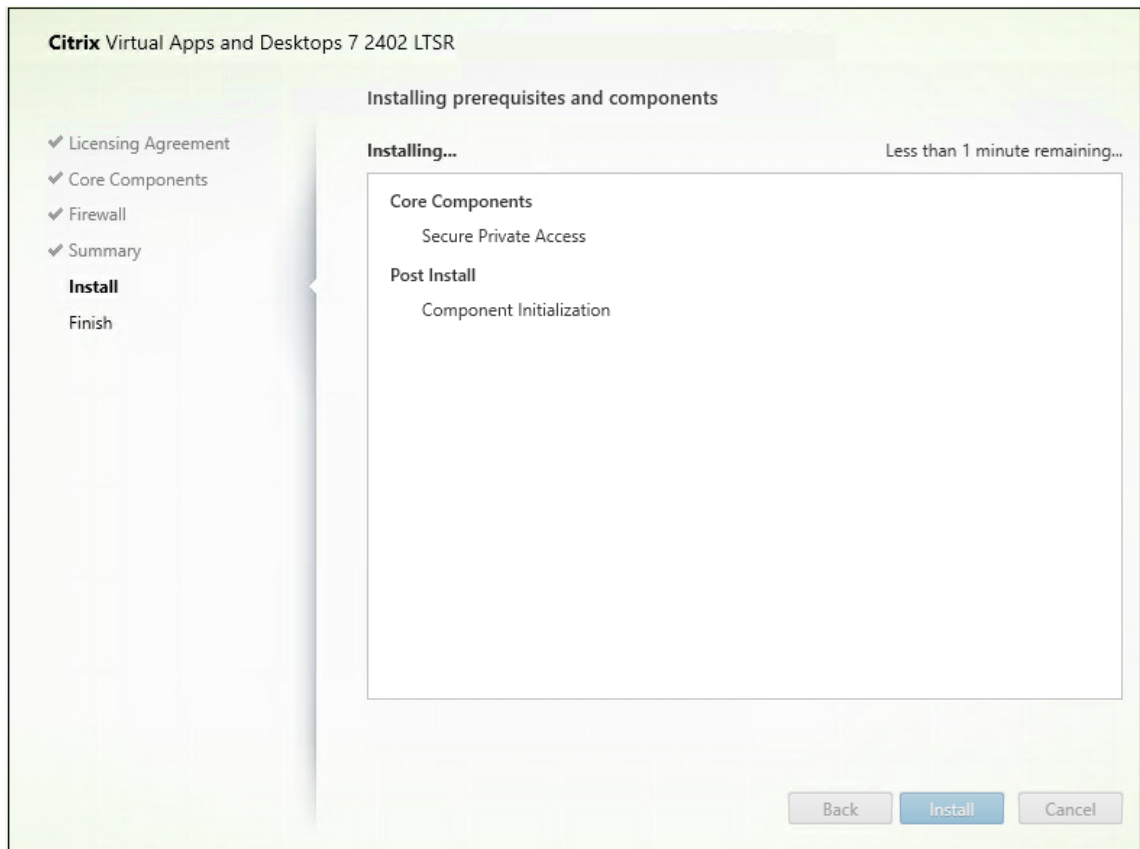
February 20, 2024

您可以使用 SecurePrivateAccessSetup_2308.exe 安装 Secure Private Access。

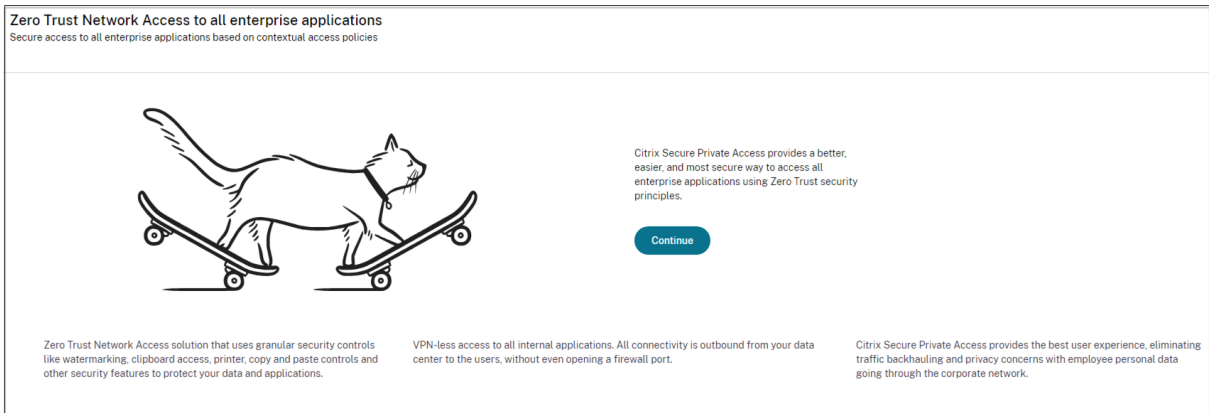
1. 从 <https://www.citrix.com/downloads/citrix-early-access-release/> 下载 Citrix Secure Private Access 安装程序。
2. 以管理员身份在加入域的计算机上运行.exe，最好在安装 StoreFront 的同一台计算机上运行。



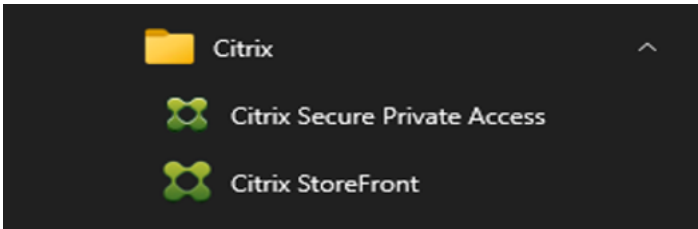
3. 按照屏幕上的说明完成安装。



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



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



SSO 到管理员控制台

建议您为用于 Secure Private Access 管理控制台的浏览器配置 Kerberos 身份验证。这是因为 Secure Private Access 使用集成 Windows 身份验证 (IWA) 进行管理员身份验证。

如果未设置 Kerberos 身份验证，则在访问 Secure Private Access 管理控制台时，浏览器会提示您输入凭据。

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

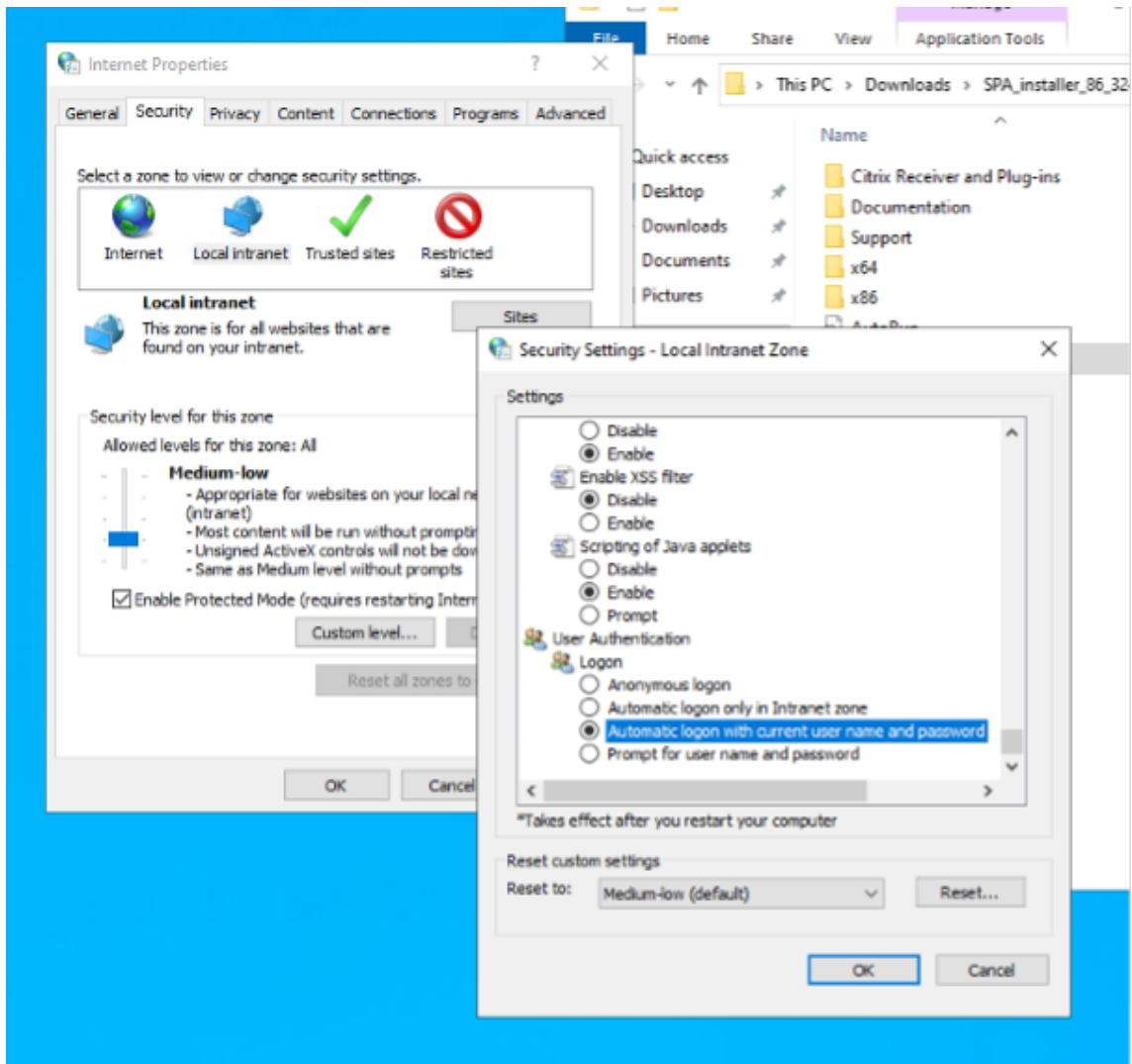
您必须登录管理员控制台才能继续进行 Secure Private Access 设置。只要用户在安装计算机上具有本地管理员权限，则可以为与安装计算机属于同一域的任何用户设置 Secure Private Access。

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

1. 打开“**Internet** 选项”。
2. 选择“安全”选项卡，然后单击“本地内联网区域”。
3. 单击“站点”，然后添加 Secure Private Access URL。

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

4. 单击“自定义级别”，然后在“用户身份验证” > “登录”中，选择“使用当前用户名和密码自动登录”。



注意：

- 如果使用 Chrome 隐身会话,请创建 DWORD 注册表项 Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Google\Chrome\DefaultContentSetting 并将值设置为 1。
- 在 Kerberos 启用隐身模式之前,您必须重新启动所有 Chrome 窗口(包括非隐身窗口)。
- 对于其他浏览器,请查看特定浏览器的 Kerberos 身份验证文档。

后续步骤

- [设置 Secure Private Access](#)
- [配置 NetScaler Gateway](#)
- [配置应用程序](#)
- [为应用程序配置访问策略](#)

使用脚本升级数据库

January 9, 2024

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

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

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

设置 **Secure Private Access**

June 19, 2024

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

- [通过创建新站点来设置 Secure Private Access](#)
- [通过加入现有站点来设置 Secure Private Access](#)

必备条件

在创建站点之前，必须安装 SQL 数据库服务器。

通过创建新站点来设置 Secure Private Access

通过创建新站点来设置 **Secure Private Access**

步骤 1: 设置 **Secure Private Access**

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

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

Zero Trust Network Access to all enterprise applications

Secure access to all enterprise applications based on contextual access policies

- 1 Site
- 2 Database
- 3 Integrations
- 4 Summary

Step 1: Creating or joining a site

A Secure Private Access site is a cluster of servers that all share the same configuration.

Create a new Secure Private Access site

Select this option if this is your first time installing Secure Private Access.

Join an existing Secure Private Access site

Select this option to add additional instances to an existing Secure Private Access site.

Next

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

步骤 2：配置数据库

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

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

可以使用以下格式之一指定数据库地址：

- ServerName
- ServerName\InstanceName
- ServerName,PortNumber

有关详细信息，请参阅[数据库](#)。

2. 在站点中，键入 Secure Private Access 站点的名称。
3. 单击“测试连接”以检查 SQL Server 实例是否有效，并确认该站点的指定数据库是否存在。

Zero Trust Network Access to all enterprise applications

Secure access to all enterprise applications based on contextual access policies

- 1 Site
- 2 Database
- 3 Integrations
- 4 Summary

Step 2: Database configuration

Every site requires its own database, which must be created by the database administrator or the machine identity. You can create the database on the same SQL server where you host the Citrix Virtual Apps and Desktops databases.

Enter the SQL Server address that will host the database and enter your desired site name.

SQL Server host* Site name*

Select how you would like to create and/or configure your database:

Automatically

With this option, we'll automatically configure the database for you. If the database doesn't exist, we'll automatically create one. For the automatic creation and configuration to work, the machine identity must have Create Table, Read, Write, and Delete privileges.

Note: Your chosen site name determines your database name. If you create the database yourself, make sure the database name is in the format of "CitrixAccessSecurity<Site Name>".

For example, "CitrixAccessSecurityLTSR2402".

Manually

With this option, you must manually create and configure the database yourself. After creating an empty database, download the script and share it with your database administrator. They must run the script on your chosen SQL Server host. After running the script, test the connection again.

Note: Your chosen site name determines your database name. If you create the database yourself, make sure the database name is in the format of "CitrixAccessSecurity<Site Name>".

For example, "CitrixAccessSecurityLTSR2402".

注意：

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

自动配置：

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

手动配置：

您可以使用“手动配置”选项来设置数据库。

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

注意：

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

第 3 步：整合 **StoreFront** 和 **NetScaler Gateway** 服务器

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

1. 输入以下详细信息。
 - **Secure Private Access** 服务器地址。例如，<https://secureaccess.domain.com>。
 - **StoreFront** 应用商店 **URL**。例如，<https://storefront.domain.com/Citrix/StoreMain>。
 - 公共网关地址—NetScaler Gateway 的 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 中为回调配置的虚拟 IP 地址相同。
2. 单击“验证所有 **URL**”。
3. 单击下一步，然后单击保存。

Zero Trust Network Access to all enterprise applications

Secure access to all enterprise applications based on contextual access policies

- Site
- Database
- 3 Integrations**
- 4 Summary

Step 3: Integrations

Connect with StoreFront and NetScaler Gateway servers so they can route traffic to Secure Private Access servers.

Secure Private Access address *
Enter the address of your Secure Private Access server or the load balancer managing traffic for your Secure Private Access servers. The address doesn't need to be a public address.

 ✓

StoreFront Store URL *
Enter your complete StoreFront Store URL.

 ✓
[+ Add another Store URL](#)

Public NetScaler Gateway address *
Enter all the addresses of the NetScaler Gateways accessing StoreFront. If you have a Global Server Load Balancing (GSLB) deployment, add the GSLB addresses as well.

 ✓
[+ Add another public address](#)

NetScaler Gateway virtual IP address and callback URL *
Enter the callback URL and virtual IP (VIP) address from each NetScaler Gateway. Each entry must match the values configured in StoreFront. [Learn more](#)

Virtual IP address * ⓘ <input type="text" value="10.80.174.125"/>	Callback URL * ⓘ <input type="text" value="https://gwgamma.spaopdev.local"/> ✓
---	--

[+ Add another virtual IP address and callback URL](#)

Director URL *
Utilize the monitoring capabilities of Director in Secure Private Access. Enter the Director URL to configure Director for use in Secure Private Access. You must also use the configuration tool for Director as described in the [product documentation](#).

 ✓

License Server URL *
A license server is a mandatory component required to collect and process licensing data. Enter the License Server URL to configure this component.

 ✓

[Test all URLs](#)

[Back](#) [Next](#)

步骤 4：配置摘要

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

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

Zero Trust Network Access to all enterprise applications

Secure access to all enterprise applications based on contextual access policies

- ✓ Site
- ✓ Database
- ✓ Integrations
- ✓ Summary

Step 4: Summary

Review the summary of your Secure Private Access setup.

Administration

You are a full administrator on this site and can add other administrators if needed.

Configurations

- SQL Server Database has been configured. ✓
- StoreFront has been configured. ✓
- NetScaler Gateway connected. ✓
- Director connected. ✓
- License Server connected. ✓
- Secure Private Access server connected. ✓

Close

注意：

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

有关详细信息，请参阅 [安装后管理设置](#)。

通过加入现有站点来设置 **Secure Private Access**

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

The screenshot shows a configuration window titled "Zero Trust Network Access to all enterprise applications" with the subtitle "Secure access to all enterprise applications based on contextual access policies". On the left, a vertical navigation pane shows three steps: "Site" (checked), "Database" (selected with a purple circle), and "Summary" (circled in grey). The main content area is titled "Step 2: Database configuration" and includes the instruction: "Enter the database information for the existing Secure Private Access site. This machine identity must have Read and Write permissions for this database." There are two input fields: "SQL Server host*" with a help icon and a placeholder "i.e.: sql.example.com,1433", and "Site name*" with a help icon and a placeholder "i.e.: Site1". Below these is a "Test connection" button. A section titled "Select how you would like to create and/or configure your database:" contains two radio button options. The "Automatically" option is selected and includes a sub-button "Download script". The "Manually" option also includes a sub-button "Download script". At the bottom are "Back" and "Next" buttons.

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

- ServerName
- ServerName\InstanceName
- ServerName,PortNumber

有关详细信息，请参阅[数据库](#)。

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

Zero Trust Network Access to all enterprise applications
Secure access to all enterprise applications based on contextual access policies

1 Site
2 Database
3 Summary

Step 2: Database configuration

Enter the database information for the existing Secure Private Access site. This machine identity must have Read and Write permissions for this database.

SQL Server host* ⓘ Site name* ⓘ

Test connection

Select how you would like to create and/or configure your database:

Automatically

With this option, we'll automatically configure the database for you. For the automatic configuration to work, the machine identity must have Create Table, Read, Write, and Delete privileges.

Manually [Download script](#)

With this option, you must download the script to give Read and Write permissions to the machine. After downloading the script, share it with your database administrator. They must run the script on your chosen SQL Server host. After running the script, test the connection again.

[Back](#) [Next](#)

如果该站点没有相应的数据库，则连接检查失败。

5. 单击保存。

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

后续步骤

- [配置 NetScaler Gateway](#)
- [配置应用程序](#)
- [为应用程序配置访问策略](#)

配置 NetScaler Gateway

February 20, 2024

重要：

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

1. 从 <https://www.citrix.com/downloads/citrix-early-access-release/> 中下载脚本。

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

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

- 将这些脚本上载到 NetScaler 计算机。您可以使用 WinSCP 应用程序或 SCP 命令。例如，`*scp ns_gateway_secure_access.sh nsroot@nsalfa.fabrikam.local:/var/tmp*`。

注意：

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

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

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

- 在 NetScaler 外壳上运行上载的脚本。

```
root@nszeta# cd /var/tmp
root@nszeta# chmod +x ns_gateway_secure_access.sh
root@nszeta# ./ns_gateway_secure_access.sh
NetScaler Gateway vserver name (default: _SecureAccess_Gateway):
NetScaler Gateway IP: 192.168.1.100
NetScaler Gateway FQDN: gateway.yourdomain.com
SPA Plugin IP: 192.168.1.100
SPA Plugin FQDN: spa.yourdomain.com
StoreFront Store URL (including protocol http/https): https://storefront.yourdomain.com/Citrix/StoreSPA
NetScaler authentication profile name: auth_prof
NetScaler SSL server certificate name: star_yourdomain_com
Domain: yourdomain.com

***** Gateway configuration *****
NetScaler Gateway name: SecureAccess_Gateway
NetScaler Gateway IP: 192.168.1.100
NetScaler Gateway FQDN: gateway.yourdomain.com
SPA Plugin FQDN: spa.yourdomain.com
SPA Plugin IP: 192.168.1.100
StoreFront Store URL: https://storefront.yourdomain.com/Citrix/StoreSPA
NetScaler authentication profile name: auth_prof
NetScaler Gateway server certificate name: star_yourdomain_com
Domain: yourdomain.com
*****

Checking SPA Plugin support...
NetScaler supports SPA Plugin
Enabling SPA Plugin support.....SUCCESS
Enabling ns_vpn_securebrowse_client_mode enabled feature.....SUCCESS
Enabling ns_vpn_redirect_to_access_restricted_page_on_deny feature.....SUCCESS
Enabling ns_vpn_use_cdn_for_access_restricted_page feature.....SUCCESS
Persisting SPA Plugin setting nsapimgr -ys call=ns_vpn_enable_spa_onprem in /nsconfig/rc.netscaler file.
Persisting SPA Plugin setting nsapimgr -ys call=toggle_vpn_enable_securebrowse_client_mode in /nsconfig/rc.netscaler file.
Persisting SPA Plugin setting nsapimgr -ys call=toggle_vpn_redirect_to_access_restricted_page_on_deny in /nsconfig/rc.netscaler file.
Persisting SPA Plugin setting nsapimgr -ys call=toggle_vpn_use_cdn_for_access_restricted_page in /nsconfig/rc.netscaler file.

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

root@nszeta#
```

- 输入所需的参数。有关参数列表，请参阅 [必备条件](#)。

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

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

要添加虚拟服务器，请执行以下操作：

```
1 `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，请执行以下操作：

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

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

NetScaler Gateway 会话操作

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

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

示例：

要添加会话操作，请执行以下操作：

```
add vpn sessionAction AC_OS_SecureAccess_Gateway -transparentInterception  
  OFF -SSO ON -ssoCredential PRIMARY -useMIP NS -useIIP OFF -icaProxy  
  OFF -wihome "https://storefront.mydomain.com/Citrix/MyStoreWeb" -  
  ClientChoices OFF -ntDomain mydomain.com -defaultAuthorizationAction
```

```
ALLOW -authorizationGroup SecureAccessGroup -clientlessVpnMode
ON -clientlessModeUrlEncoding TRANSPARENT -SecureBrowse ENABLED -
storefronturl "https://storefront.mydomain.com"-sfGatewayAuthType
domain
```

要更新会话操作，请执行以下操作：

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

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

与 ICA 应用程序的兼容性

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

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

有关详细信息，请参阅以下主题：

- [在 NetScaler Gateway 上配置 Secure Ticket Authority](#)
- [常见问题解答：Citrix Secure Gateway/NetScaler Gateway Secure Ticket Authority](#)

支持智能访问标签

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

- 13.1.48.47 及更高版本
- 14.1—4.42 及更高版本

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

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

- 您可以使用命令进行切换（FreeBSD shell）：

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

- 运行以下命令（FreeBSD shell），为 HTTP 标注配置启用 SecureBrowse 客户端模式。

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

- 要禁用，请再次运行相同的命令。

- 要验证开关处于开启还是关闭状态，请运行 `nsconmsg` 命令。
- 要在 NetScaler Gateway 上配置智能访问标签，请参阅在 NetScaler Gateway 上配置自定义标签（SmartAccess 标签）。

已知限制

- 现有的 NetScaler Gateway 可以使用脚本进行更新，但可能有无限数量的 NetScaler 配置，单个脚本无法涵盖。
- 请勿在 NetScaler Gateway 上使用 ICA 代理。配置 NetScaler Gateway 时，此功能将被禁用。
- 如果您使用部署在云端的 NetScaler，则必须在网络中进行一些更改。例如，允许 NetScaler 与其他组件在特定端口上进行通信。
- 如果您在 NetScaler Gateway 上启用 SSO，请确保 NetScaler 使用私有 IP 地址与 StoreFront 通信。您可能需要使用 StoreFront 私有 IP 地址向 NetScaler 添加一条新的 StoreFront DNS 记录。

上载公共网关证书

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

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

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

配置应用程序

February 20, 2024

1. 选择应用程序所在的位置。
 - 在我的公司网络 之外供外部应用程序使用。
 - 在我的公司网络 中，用于内部应用程序。
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”。

Add an app ✕

To add an app, complete the steps below.

▼ App Details

Where is the application located? *

Outside my corporate network

Inside my corporate network

App name *

App icon

[Change icon](#)
[Use default icon](#)

(128 KB max, ICO)

App description

App category ?

URL *

App Connectivity * ?

Related Domains *

[+ Add another related domain](#)

App Connectivity * ?

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

- 类别/子类别名称必须用反斜杠分隔。例如，业务与生产力\工程。此外，此字段区分大小写。管理员必须确保他们定义了正确的类别。如果 Citrix Workspace 用户界面中的名称与在应用程序类别字段中输入的类别名称不匹配，则该类别将列为新类别。

例如，如果您在应用程序类别字段中错误地将业务和工作效率类别输入为业务和工作效率类别，则除业务和工作效率类别外，Citrix Workspace UI 中还会列出一个名为业务和工作效率的新类别。

- 应用程序图标—单击更改图标以更改应用程序图标。图标文件大小必须为 128x128 像素，并且仅支持 lco 格式。如果不更改图标，则会显示默认图标。
- 不向用户显示应用程序 -如果您不想向用户显示应用程序，请选择此选项。
- **URL** —应用程序的 URL。
- 相关域 -根据应用程序 URL 自动填充相关域。管理员可以添加更多相关的内部或外部域。
自动将应用程序添加到收藏夹 -单击此选项可将此应用添加为 Citrix Workspace 应用程序中的常用应用程序。
- 允许用户从收藏夹中删除 -单击此选项可允许应用程序订阅者从 Citrix Workspace 应用程序的收藏夹应用程序列表中删除该应用程序。
选择此选项时，在 Citrix Workspace 应用程序中，该应用程序的左上角会出现一个黄色星形图标。
- 不允许用户从收藏夹中删除 -单击此选项可防止订阅者从 Citrix Workspace 应用程序的收藏夹应用程序列表中删除该应用程序。

选择此选项时，带挂锁的星形图标会显示在 Citrix Workspace 应用程序的应用程序的左上角。

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

应用程序连接：对于 Web 应用程序，选择“内部”，为 SaaS 应用程序选择“外部”。

3. 单击“保存”，然后单击“完成”。

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

后续步骤

[为应用程序配置访问策略](#)

为应用程序配置访问策略

January 9, 2024

访问策略允许您根据用户或用户组启用或禁用对应用程序的访问权限。此外，您可以通过添加安全限制来启用对应用程序的限制访问。

1. 单击创建策略。

Create a policy to enforce application access rules based on a user's context.

Applications

Google

If the following condition is met

User/user groups*

Matches any of

spaopdev.local

SPAOP users

+ Add condition

Then do the following

Allow access

Policy name

Google-Win11

Enable policy on save

Save Cancel

Activate Windows
Go to Settings to activate Windows.

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-选择必须允许或拒绝应用程序访问的条件和用户或用户组。

- 匹配以下任一项：仅允许与字段中列出的任何名称相匹配的用户或组进行访问。
- 与任何用户或组都不匹配：允许除字段中列出的用户或组之外的所有用户或组进行访问。

4. 单击“添加条件”，根据上下文标签添加另一个条件。这些标签源自 NetScaler Gateway。


5. 选择 条件标记，然后选择必须允许或拒绝应用程序访问所依据的条件。

6. 在“然后执行以下操作”中，选择必须根据条件评估在应用程序上强制执行的以下操作之一。








- 允许访问
- 允许有限的访问
- 拒绝访问

选择“允许有限制的访问”时，可以选择以下限制。

Then do the following

Allow access with restrictions 

Available security restrictions:

- Restrict clipboard access 
- Restrict printing 
- Restrict downloads 
- Restrict uploads 
- Display watermark 
- *Restrict key logging 
- *Restrict screen capture 

***Applicable to Citrix Workspace desktop clients only.**

- 限制剪贴板访问权限：禁用应用程序和系统剪贴板之间的剪切/复制/粘贴操作。
- 限制打印：禁用从 Citrix Enterprise Browser 中打印的功能。
- 限制下载：禁用用户从应用程序内下载的权限。
- 限制上载：禁用用户在应用程序内上载的功能。
- 显示水印：在用户屏幕上显示水印，显示用户计算机的用户名和 IP 地址。
- 限制按键记录：防范按键记录器。当用户尝试使用用户名和密码登录应用程序时，所有密钥都会在密钥记录器上加密。此外，用户在应用程序上执行的所有活动都受到密钥记录的保护。
例如，如果为 Office 365 启用了 App Protection 策略，并且用户编辑 Office 365 Word 文档，则所有

按键记录器上的按键都经过加密。

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

注意：

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

7. 在 策略名称中，输入策略的名称。

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

访问策略优先级

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

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

您可以通过使用“优先级”列中的向上或向下移动策略来更改 优先级 顺序。

后续步骤

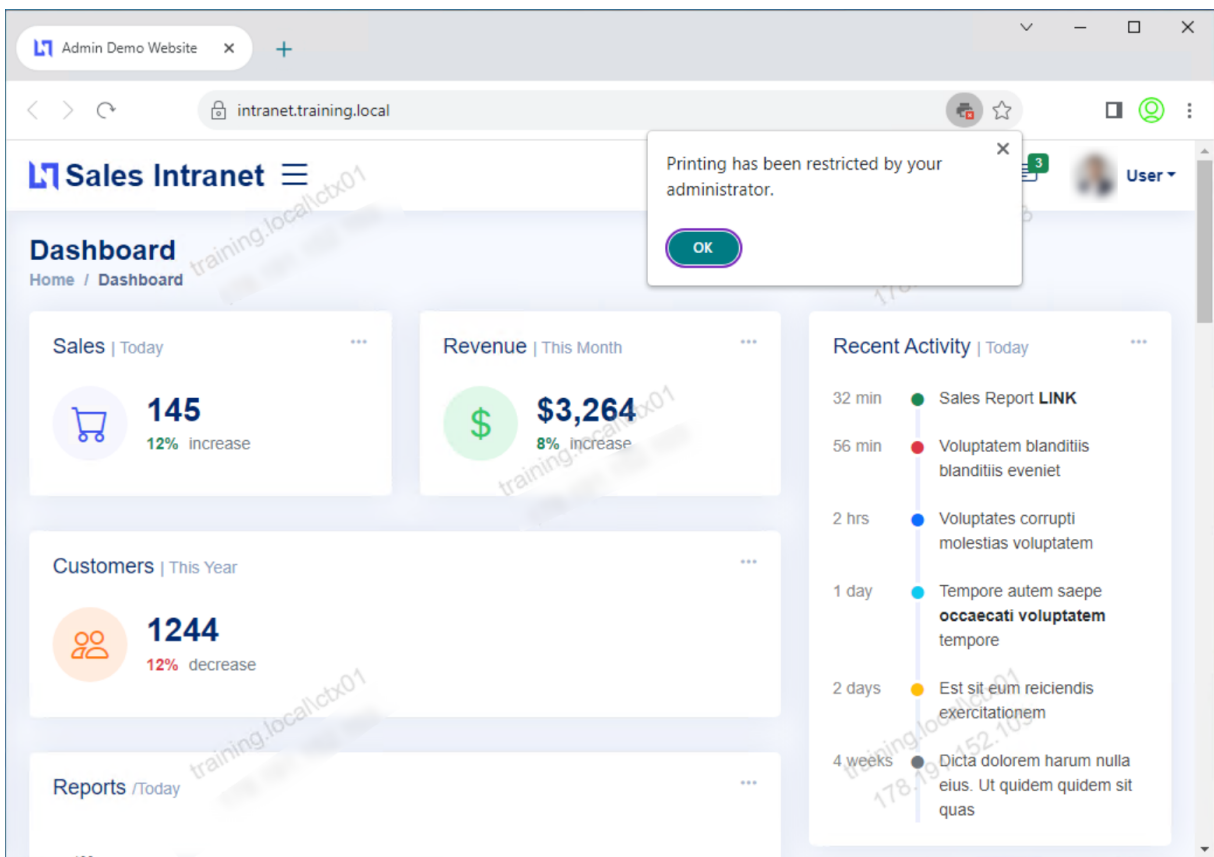
在客户端（Windows 和 macOS）上验证您的配置。

Example

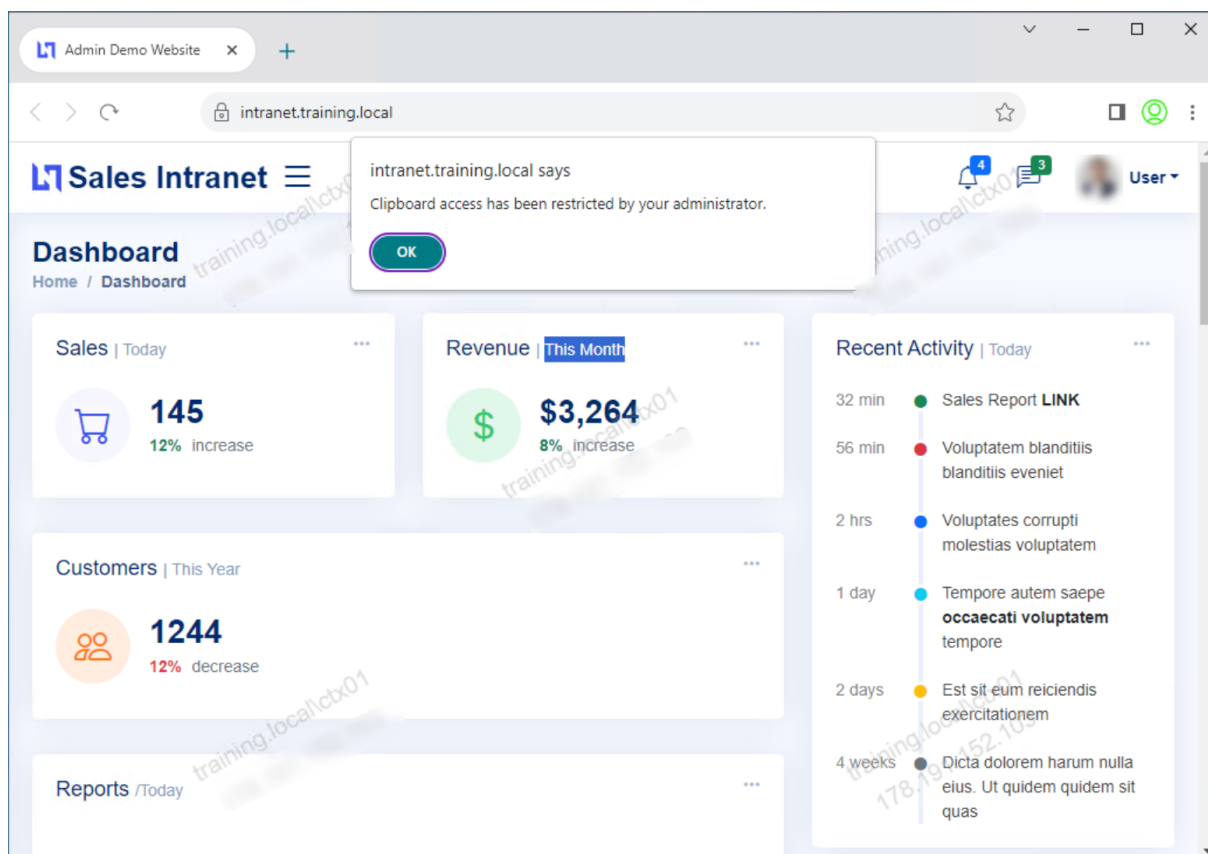
最终用户流程

June 19, 2024

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



同样，如果用户尝试访问剪贴板，则会显示以下消息。



注意：

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

通过 Web Studio 集成实现 Secure Private Access 集成

June 19, 2024

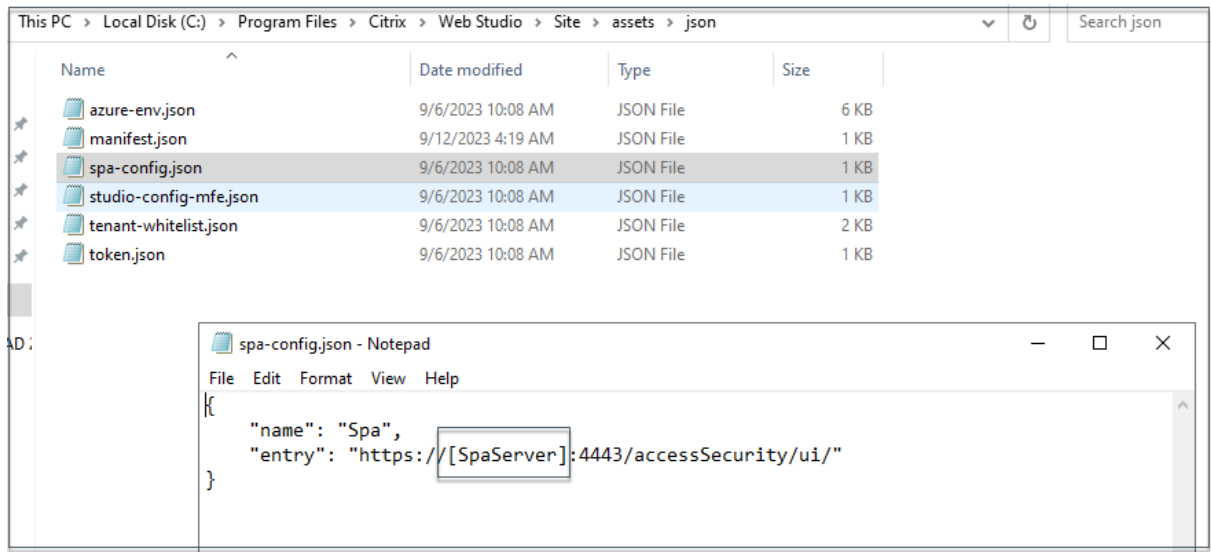
Citrix Secure Private Access 还集成到 Web Studio 控制台中，使用户能够通过 Web Studio 无缝访问该服务。

您必须安装 Web Studio 版本 2308 或更高版本。

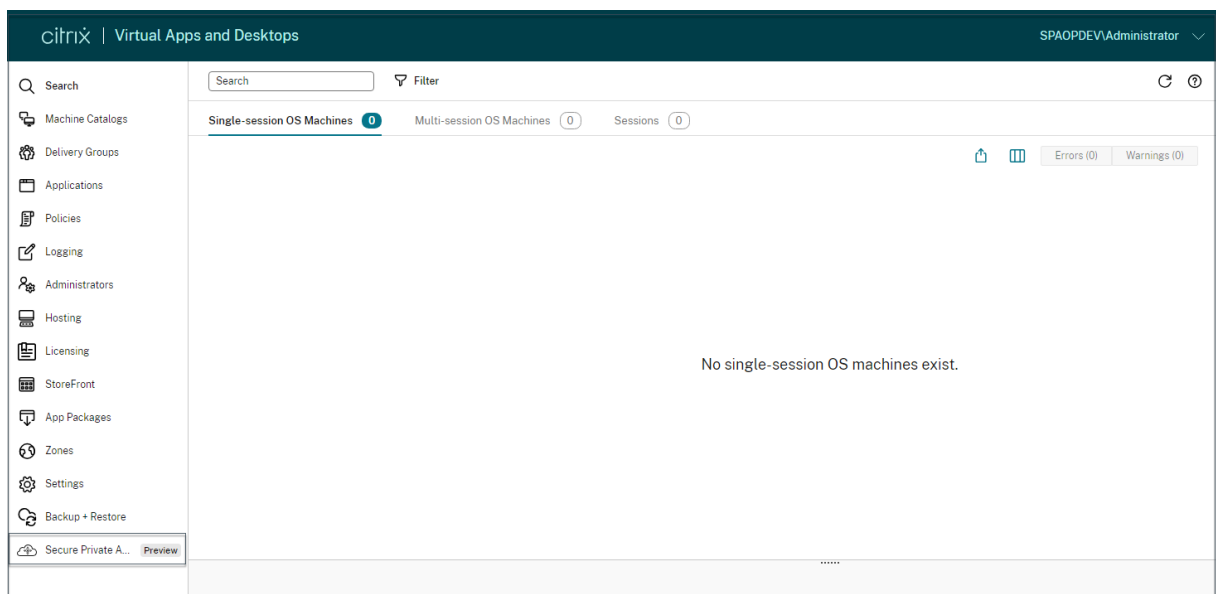
执行以下步骤以启用 Web Studio 集成：

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

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



1. 将“SpaServer”替换为您的 Secure Private Access 插件的 FQDN。
2. 登录到 Web Studio。



1. 在左侧导航菜单上，单击“**Secure Private Access<Preview>**”，从 Web Studio 访问 Secure Private Access 管理控制台。

安装后管理设置

January 9, 2024

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

管理应用程序域的路由

您可以查看在 Secure Private Access 设置中添加的应用程序域列表。应用程序域表列出了所有相关的域以及应用程序流量的路由方式（外部或内部）。

1. 单击“设置” > “应用程序域”。
2. 如果需要，您可以单击编辑图标并更改路由类型。

管理 **Secure Private Access** 的管理员

您可以查看管理员列表，也可以从“设置” > “管理员”页面添加管理员。首次安装 Secure Private Access 权限的管理员将被授予完全权限。然后，该管理员可以将其他管理员添加到设置中。

您还可以添加管理员组，以便为该组中的所有管理员启用访问权限。

1. 在“管理员”页面中，单击“添加”。
2. 在域中，选择必须将该管理员添加到的域。
3. 在用户或用户组中，选择该用户所属的一个或多个用户组。
4. 在管理员类型中，选择必须分配给该用户的权限类型。

设置完成后更新 **StoreFront** 或 **NetScaler Gateway** 服务器详情

设置 Secure Private Access 后，您可以从“集成”选项卡修改或更新 StoreFront 和 NetScaler Gateway 条目。

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

注意：

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

Application Domain Administrators **Integrations**

Connect with StoreFront and NetScaler Gateway servers to enable them to route traffic to Secure Private Access servers.

Secure Private Access address
The address of this Secure Private Access server or of the load balancer in front of your Secure Private Access servers. Users use this address to access their policies. This address must be a valid web URL and does not have to be a public address.

✓ ↻ ✎

StoreFront Store URL
The complete StoreFront store URL.

✓ ↻ ✎ [Download Script](#)

[+ Add another Store URL](#)

Public NetScaler Gateway address
The internet facing addresses of all the NetScaler Gateways fronting StoreFront. If you have a GSLB deployment, add both the GSLB address as well as the individual NetScaler Gateway addresses.
[Get Gateway scripts](#)

✓ ↻ ✎ [Refresh Certificate](#)

[+ Add another public address](#)

NetScaler Gateway virtual IP address and callback URL
The Gateway VIP is the private IP address of the NetScaler Gateway virtual server(not the callback virtual server) that is sent with all traffic. The callback address is an endpoint on each of the NetScaler Gateways that enables key functionality. They are associated with each other, and by matching on the VIP address, Secure Private Access will know which callback address to invoke. For both fields, use the same values as configured in StoreFront.

Gateway VIP Callback URL ✓ ↻ ✎

[+ Add another virtual IP address and callback URL](#)

Director URL
Utilize the monitoring capabilities of Director in Secure Private Access.

✓ ✎

License Server URL
A license server is a mandatory component required to collect and process licensing data.

✓ ↻ ✎

控制板概述

January 9, 2024

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

您可以使用过滤器（类别和结果）来优化搜索结果。

The screenshot shows the Citrix Secure Private Access console interface. On the left is a navigation menu with options: Overview, Applications, Access Policies, Settings, and Troubleshooting Logs. The main area displays search filters and a table of logs. The search criteria is 'User-Name = "User"' and the time range is 'Last 1 Week'. The table shows results limited to the first 1000 records. The table columns are: TIME, USER NAME, CATEGORY, RESULT, TRANSACTION ID, and DETAILS. The table contains 10 rows of logs, all with a 'Success' result. The categories include 'App Access' and 'App Enumeration'.

TIME	USER NAME	CATEGORY	RESULT	TRANSACTION ID	DETAILS
2023-11-21 15:48:20	user1@spaopdev.ctx	App Access	Success	6e6709b0-8a73-4a...	Show Details
2023-11-21 15:48:20	user1@spaopdev.ctx	App Access	Success	6e6709b0-8a73-4a...	Policy evaluatic
2023-11-21 15:48:20	user1@spaopdev.ctx	App Access	Success	6e6709b0-8a73-4a...	SmartAccess tr
2023-11-21 15:48:20	user1@spaopdev.ctx	App Access	Success	6e6709b0-8a73-4a...	Received Gatev
2023-11-21 15:48:20	user1@spaopdev.ctx	App Access	Success	6e6709b0-8a73-4a...	Successfully ve
2023-11-21 15:48:18	user1@spaopdev.ctx	App Enumeration	Success	456bc7b4-1a1f-4b8...	Total apps enur
2023-11-21 15:48:18	user1@spaopdev.ctx	App Enumeration	Success	456bc7b4-1a1f-4b8...	Show Details
2023-11-21 15:48:18	user1@spaopdev.ctx	App Enumeration	Success	456bc7b4-1a1f-4b8...	SmartAccess tr
2023-11-21 15:48:18	user1@spaopdev.ctx	App Enumeration	Success	456bc7b4-1a1f-4b8...	Credential valr

您还可以根据以下参数以及搜索字段中的运算符来细化搜索。

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

以下是搜索运算符，您可以使用这些运算符在用户日志和执行图表中的热门访问策略中优化搜索。

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

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

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

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

查看日志中的上下文标签

详细信息列中的显示详细信息链接显示与特定访问策略相关的应用程序列表以及与该策略相关的上下文标签。

TIME	USER NAME	CATEGORY	RESULT	TRANSACTION ID	DETAILS
2023-09-07 10:29:13	spaopdev.local\usera	App Access	Failure	9c7c2de9-0351-43b1-8...	ERROR: Error in process...
2023-09-07 10:29:13	spaopdev.local\usera	App Access	Success	9c7c2de9-0351-43b1-8...	Show Details
2023-09-07 10:29:12	spaopdev.local\usera	App Access	Success	9c7c2de9-0351-43b1-8...	SmartAccess tags recei...
2023-09-07 10:29:12	spaopdev.local\usera	App Access	Success	9c7c2de9-0351-43b1-8...	DSAuth validation was s...
2023-09-07 09:48:50	spaopdev.local\usera	App Access	Success	9c7c2de9-0351-43b1-8...	Successfully generated ...
2023-09-07 09:48:50	spaopdev.local\usera	App Access	Success	9c7c2de9-0351-43b1-8...	Show Details
2023-09-07 09:48:49	spaopdev.local\usera	App Access	Success	9c7c2de9-0351-43b1-8...	SmartAccess tags recei...
2023-09-07 09:48:49	spaopdev.local\usera	App Access	Success	9c7c2de9-0351-43b1-8...	DSAuth validation was s...
2023-09-07 09:48:40	spaopdev.local\usera	App Access	Success	22592f2f-f17b-4a5f-96...	Show Details
2023-09-07 09:48:40	spaopdev.local\usera	App Access	Success	22592f2f-f17b-4a5f-96...	Policy evaluation return...
2023-09-07 09:48:40	spaopdev.local\usera	App Access	Success	22592f2f-f17b-4a5f-96...	SmartAccess tags recei...
2023-09-07 09:48:40	spaopdev.local\usera	App Access	Success	22592f2f-f17b-4a5f-96...	DSAuth validation was s...
2023-09-07 09:46:27	spaopdev.local\usera	App Access	Failure	6e9d1dd1-5bdb-4474-8...	ERROR: Error in process...

故障排除

June 19, 2024

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

[证书错误](#)

[数据库创建错误](#)

[StoreFront 故障](#)

[公共网关/回调网关故障](#)

[无法访问 Secure Private Access 服务器](#)

证书错误

错误消息：无法自动从一台或多台 Gateway 服务器获取证书。

解决办法：更新网关证书的方式与更新 Citrix Virtual Apps and Desktops 的方法相同。

数据库创建错误

- 错误消息：无法创建数据库

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

- 错误消息：无法创建数据库：数据库已经存在。

在以下任何情况下都可能出现此错误消息。

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

解决方案：必须创建一个空数据库。

- 您卸载了 Secure Private Access，然后使用相同的站点名称重试设置。在这种情况下，先前安装的数据库不会被删除。

解决方案：必须手动删除数据库。

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

解决方案：您必须重命名该站点，然后再次运行脚本。

- 计算机没有读取、写入、更新权限，无法在 SQL 服务器的数据库中创建表。

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

- 错误消息：无法创建数据库：连接失败

解决方案：

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

StoreFront 故障

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

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

解决方案：

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

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

解决方案：

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

注意：

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

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

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

解决方案：

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

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

注意：

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

公共网关/回调网关故障

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

解决方案：

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

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

无法访问 **Secure Private Access** 服务器

错误消息：更新 IIS 池失败。无法重新启动 IIS 池

解决方案：

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

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

还要检查默认 IIS 站点 "[Default Web Site](#)" 是否已启动并正在运行。

数据库连接检查失败

错误消息：连接检查失败

数据库连接检查可能由于多种原因而失败：

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

解决方案：检查防火墙上是否打开了数据库端口（默认端口 1433）。

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

解决方案：请参阅 [Secure Private Access 的 SQL 数据库权限](#)。

网关连接检查失败。无法获取公共证书

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

解决方案：

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

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

身份验证问题

Secure Private Access 运行时服务 IIS 身份验证配置可能不起作用，因为不支持集成 Windows 身份验证 (IWA)。

其他

创建 **Secure Private Access** 诊断支持包

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

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

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

Secure Private Access 的 SQL 数据库权限

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

远程数据库：

执行以下步骤来设置远程数据库的权限。

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

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

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

```
USE CitrixAccessSecurity<SiteName>
```

```
CREATE LOGIN [DOMAIN1\HOST1$] FROM WINDOWS
```

可以使用以下查询找到域名：

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

3. 将 `db_owner` 角色分配给计算机身份。

```
USE CitrixAccessSecurity<SiteName>
```

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

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

本地数据库：

执行以下步骤来设置本地数据库的权限。

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

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

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

```
USE CitrixAccessSecurity<SiteName>
```

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

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

```
USE CitrixAccessSecurity<SiteName>
```

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

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

当您手动创建数据库时，下载的数据库脚本会将权限添加到计算机标识中。

卸载 Secure Private Access

January 9, 2024

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

1. 选择 **Citrix Virtual Apps and Desktops 7 2308 – Secure Private Access**。
2. 单击卸载。
3. 按照屏幕上的说明完成卸载。

注意：

如果 Secure Private Access 安装后设置已完成，则在卸载 Secure Private Access 之前，请从管理控制台下载 `StoreFrontScripts.zip` 文件，从 StoreFront 应用商店配置中删除 Secure Private Access 插件。

要下载 `StoreFrontScripts` 压缩文件，请按照以下步骤操作：

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

从 **StoreFront** 应用商店配置中移除 **Secure Private Access** 插件

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

1. 登录 StoreFront 计算机。
2. 下载 StoreFrontScripts.zip 文件。
3. 将 StoreFrontScripts.zip 解压到一个文件夹。
4. 使用管理员权限打开 PowerShell 窗口。
5. 请运行以下命令：

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

Secure Private Access 2308 与传统版本的兼容性

February 20, 2024

Secure Private Access 2308 与传统版本（本地 V1.0 和 V1.5 的 Secure Private Access）不兼容。如前面[配置 NetScaler Gateway](#) 中所述，必须使用新脚本配置 NetScaler Gateway。无需在 Citrix Virtual Apps and Desktops Delivery Controller 中对 Secure Private Apps 2308 进行任何配置。

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

- 来自 Web/SaaS 应用程序的 Citrix Virtual Apps and Desktops Delivery Controller
- 将 Citrix StoreFront 更新为默认配置或在 StoreFront 上创建新应用商店
- NetScaler Gateway

Citrix Virtual Apps and Desktops Delivery Controller 清理

可以手动删除在 Citrix Virtual Apps and Desktops Delivery Controller 上创建的 Secure Private Access 应用程序，也可以使用 PowerShell 脚本删除。

手动：

1. 打开 Citrix Studio 或 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"
```

有关详细信息，请参阅 [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 清理

您可以创建新的 StoreFront 应用商店或清理现有应用商店。

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

手动：

1. 查找并移除 policy.json(例如 C:\inetpub\wwwroot\Citrix\Store\Resources\SecureBrowser\policy.json)
2. 查找并删除文件夹 SecureBrowser(例如 C:\inetpub\wwwroot\Citrix\Store\Resources\SecureBrowser) 和资源 (例如 C:\inetpub\wwwroot\Citrix\Store\Resources)
3. 从 web.config (您可以在 C:\inetpub\wwwroot\Citrix\Store 中找到) 中移除名为 “webSecurePolicy” 的 “route” 节点，该节点路由到 RUL “Resources\SecureBrowser\policy.json”
4. 重新启动 **Internet Information Services (IIS)** 管理器控制台上的默认 **Web** 站点以应用更改。

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。

该脚本删除 C:\inetpub\wwwroot\Citrix\Store\Resources 文件夹、子文件夹和文件，并更新 web.config 文件。

5. 重新启动 **Internet Information Services (IIS)** 管理器控制台上的默认 **Web** 站点以应用更改。

NetScaler Gateway 清理

NetScaler Gateway 虚拟服务器

为传统版本 (1.0 和 1.5) 创建的 NetScaler Gateway 虚拟服务器可以重复使用于 Secure Private Access 2308。

- 要更新现有 NetScaler Gateway，请参阅 [更新现有 NetScaler Gateway]。
- 要配置新的 NetScaler Gateway，请参阅 [配置 NetScaler Gateway]。

会话策略和操作

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

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

该脚本还创建了完全配置的会话策略/操作。

授权策略

在 NetScaler Gateway 上为传统版本（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。

- 手动取消授权策略与 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，可以重复使用这些策略。
- 移除授权策略。

第三方通知

January 9, 2024

[适用于本地的 Citrix Secure Private Access](#)



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).