



# Citrix Secure Private Access: local

**Machine translated content**

## **Disclaimer**

La versión oficial de este contenido está en inglés. Para mayor comodidad, parte del contenido de la documentación de Cloud Software Group solo tiene traducción automática. Cloud Software Group no puede controlar el contenido con traducción automática, que puede contener errores, imprecisiones o un lenguaje inadecuado. No se ofrece ninguna garantía, ni implícita ni explícita, en cuanto a la exactitud, la fiabilidad, la idoneidad o la precisión de las traducciones realizadas del original en inglés a cualquier otro idioma, o que su producto o servicio de Cloud Software Group se ajusten a cualquier contenido con traducción automática, y cualquier garantía provista bajo el contrato de licencia del usuario final o las condiciones de servicio, o cualquier otro contrato con Cloud Software Group, de que el producto o el servicio se ajusten a la documentación no se aplicará en cuanto dicha documentación se ha traducido automáticamente. Cloud Software Group no se hace responsable de los daños o los problemas que puedan surgir del uso del contenido traducido automáticamente.

## Contents

|  |           |
|--|-----------|
| <b>Novedades</b>   | <b>2</b>  |
| <b>Problemas conocidos</b>   | <b>2</b>  |
| <b>Instalador de Secure Private Access</b>                                   | <b>4</b>  |
| <b>Actualice la base de datos mediante scripts</b>                           | <b>9</b>  |
| <b>Configurar Secure Private Access</b>                                      | <b>9</b>  |
| <b>Configurar NetScaler Gateway</b>  | <b>17</b> |
| <b>Configurar aplicaciones</b>   | <b>23</b> |
| <b>Configurar directivas de acceso para las aplicaciones</b>                 | <b>26</b> |
| <b>Flujo de usuarios finales</b>   | <b>29</b> |
| <b>Integración de Secure Private Access con la integración de Web Studio</b> | <b>32</b> |
| <b>Administrar la configuración después de la instalación</b>                | <b>33</b> |
| <b>Descripción general del panel</b>   | <b>35</b> |
| <b>Solución de errores</b>   | <b>37</b> |
| <b>Desinstalar Secure Private Access</b>                                     | <b>44</b> |
| <b>Compatibilidad de Secure Private Access 2308 con versiones antiguas</b>   | <b>45</b> |
| <b>Notificaciones de terceros</b>  | <b>47</b> |

## Novedades

December 27, 2023

### Octubre de 2023

#### **Citrix Secure Private Access para entornos locales: versión preliminar**

Citrix Secure Private Access para entornos locales ya está en versión preliminar. La solución local de Secure Private Access incluye una interfaz de usuario de consola de administración de servicio completo con una apariencia similar a la del servicio Secure Private Access. Para obtener más información, consulte [Secure Private Access para entornos locales: versión preliminar](#).

## Problemas conocidos

February 16, 2024

La solución Citrix Secure Private Access for on-premise presenta los siguientes problemas conocidos:

### Configuraciones del controlador de dominio

- No se admite la confianza unidireccional entre dominios del mismo bosque o entre bosques diferentes. La solución Secure Private Access for on-premise no funciona si se cumplen las dos condiciones siguientes.
  - El dominio de la máquina en el que está instalado Secure Private Access for on-premise es diferente del dominio del administrador que inició sesión en Secure Private Access.
  - No hay confianza configurada desde el dominio de la máquina al dominio del usuario.
- Si SAMAccountName y UPN son diferentes, se produce un error en la enumeración.

### NetScaler Gateway

El servidor virtual SSL con configuración de perfil SSL no se admite en el siguiente escenario.

- El cliente usa NetScaler Gateway 13.1—48.47 y versiones posteriores o 14.1—4.42 y versiones posteriores.

- La opción `ns_vpn_enable_spa_onprem` está habilitada.

Solución temporal:

Enlace los parámetros SSL configurados en el perfil SSL directamente al servidor virtual SSL o inhabilita la opción `ns_vpn_enable_spa_onprem`.

Para obtener más información sobre el conmutador, consulte [Compatibilidad con etiquetas de acceso inteligentes](#).

## RFweb/ Workspace para web

No se admite RFWeb/Workspace para web. Aunque las aplicaciones están enumeradas, es posible que no se inicie correctamente.

## Iconos de aplicaciones

Solo se admite el formato de ícono ICO. No se admiten los formatos PNG, JPEG y otros.

## Administración de administradores

- Los cambios en las funciones de RBAC del administrador se reflejan solo después de invalidar la sesión actual (al cerrar sesión o al caducar el token).
- Los usuarios administradores no deben formar parte del grupo AD predeterminado “Usuarios de dominio” porque la autenticación de dichos usuarios falla.

## Actualizaciones

No se admite la actualización de compilación a compilación. Secure Private Access para entornos locales le solicita que elimine la instalación existente y la vuelva a instalar en una actualización de compilación a compilación.

## StoreFront

- En **Almacenes > Configurar Unified Experience**, el receptor predeterminado para el sitio web debe configurarse en `/Citrix/<StoreName>Web`. En versiones anteriores de StoreFront, el receptor predeterminado para el sitio web estaba configurado en un valor en blanco y eso no funcionaba para Secure Private Access. Además, en el cliente se muestra la versión anterior de la interfaz de usuario de Receiver.

- Si utiliza las versiones 2308 o anteriores de StoreFront, la página **Tiendas > Administrar Delivery Controllers** muestra el tipo de complemento Secure Private Access como **XenMobile**. Esto no afecta a la funcionalidad.

## Registros

- No se admite la generación de paquetes de soporte para el clúster.
- No se deben eliminar las carpetas de registros de los servicios de administración y tiempo de ejecución. Secure Private Access no puede volver a crear si se eliminan estas carpetas.

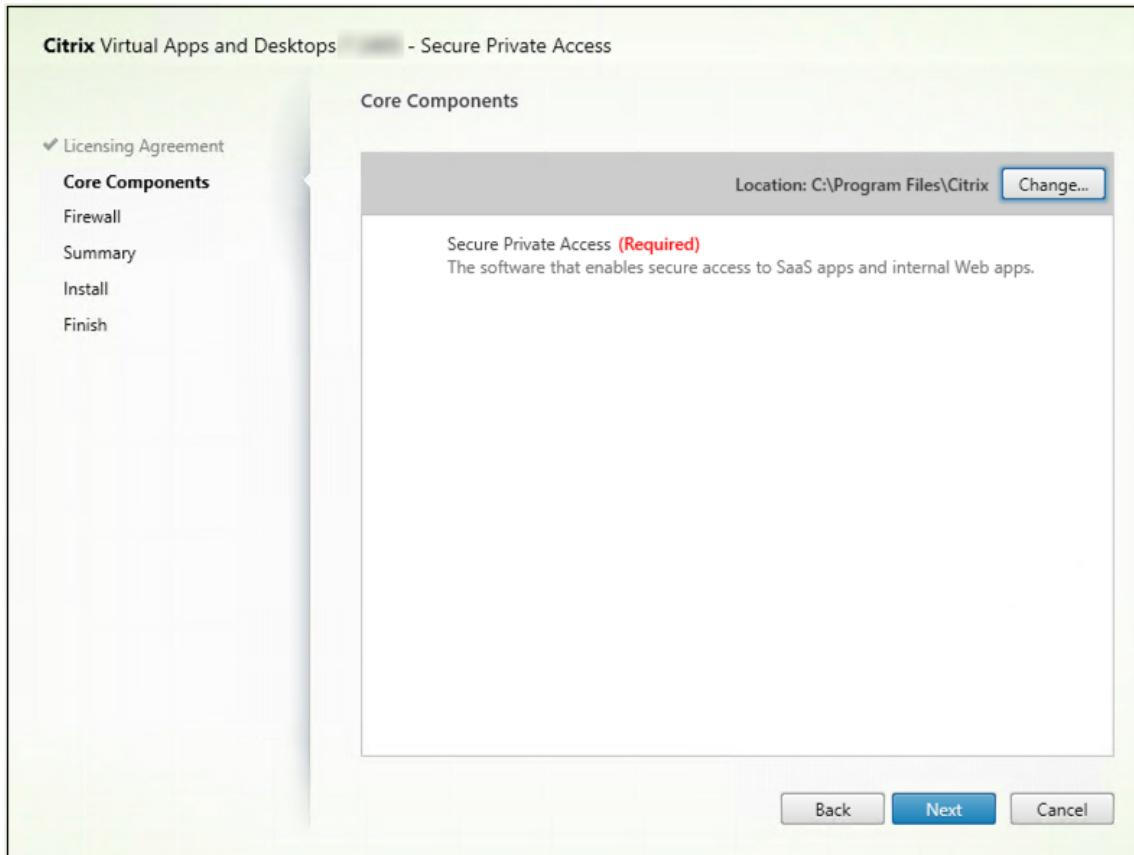
## Instalador de Secure Private Access

February 16, 2024

Puede instalar Secure Private Access mediante SecurePrivateAccessSetup\_2308.exe.

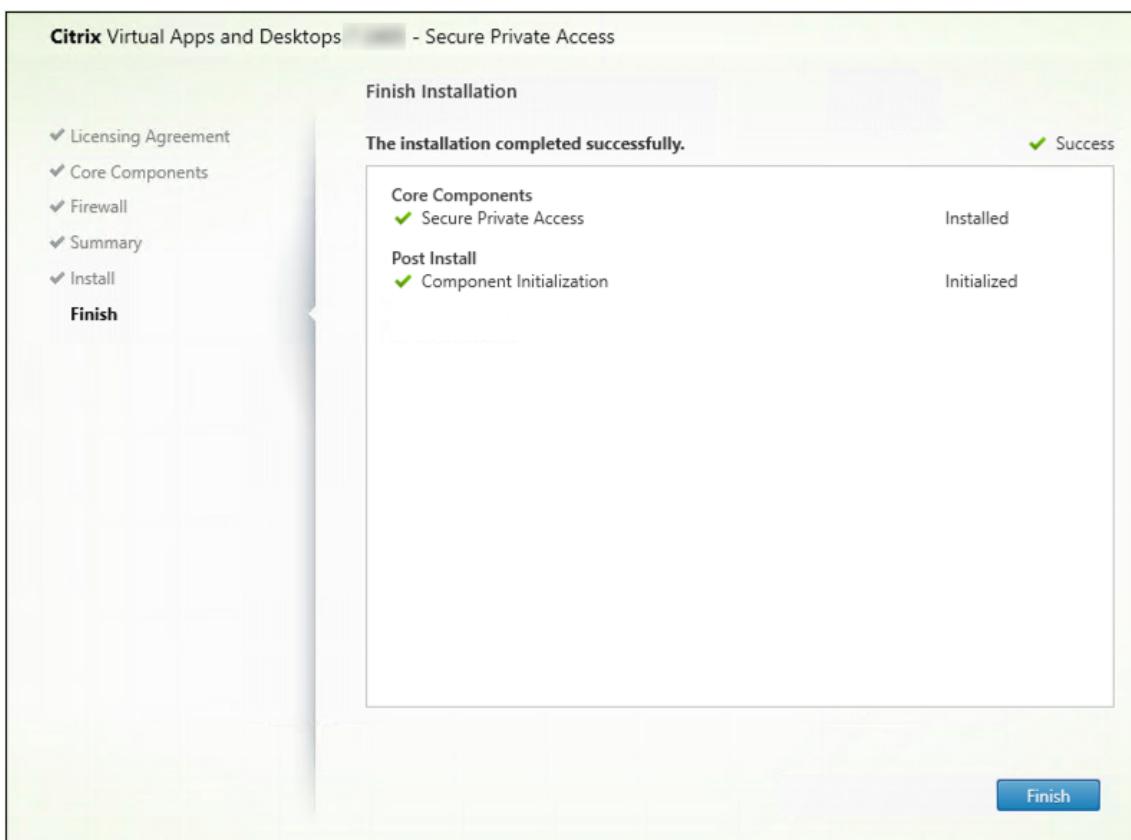
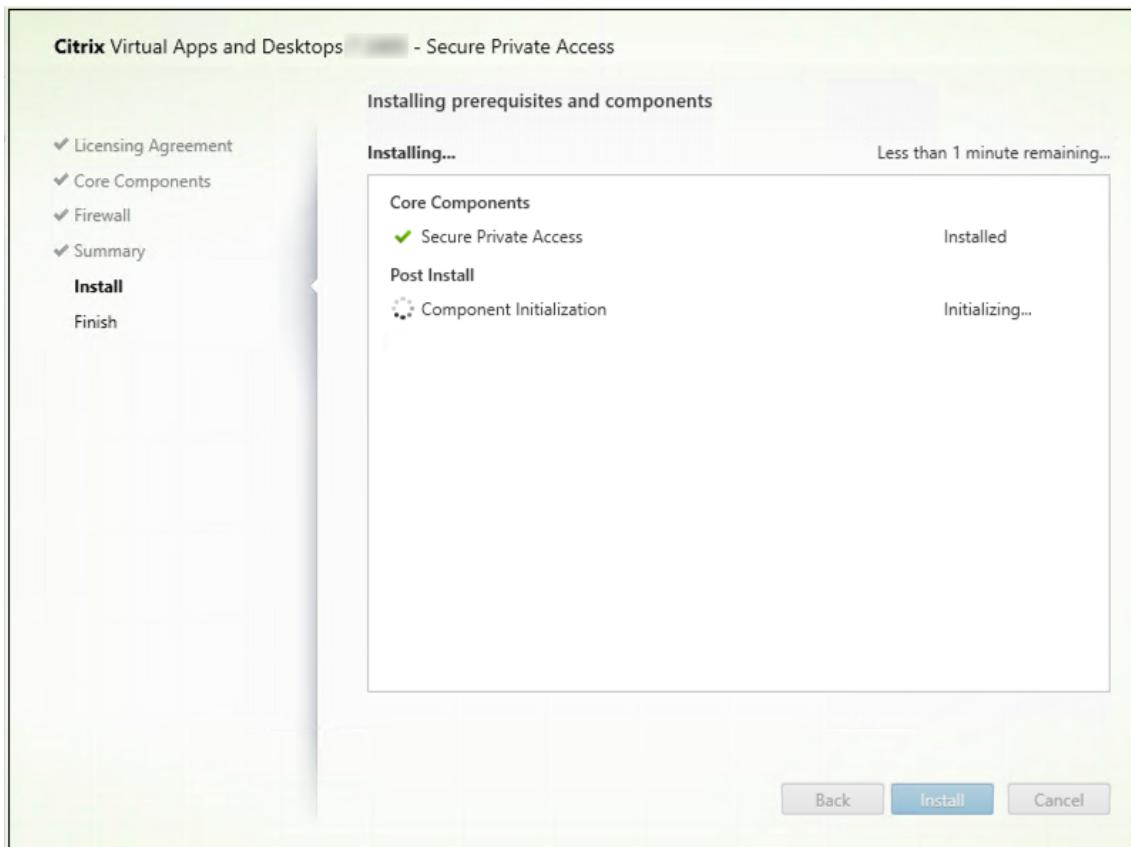
1. Descargue el instalador de Citrix Secure Private Access desde <https://www.citrix.com/downloads/citrix-early-access-release/>.
2. Ejecute el .exe como administrador en un equipo unido a un dominio, preferiblemente en el mismo equipo en el que está instalado StoreFront.

## Citrix Secure Private Access: local



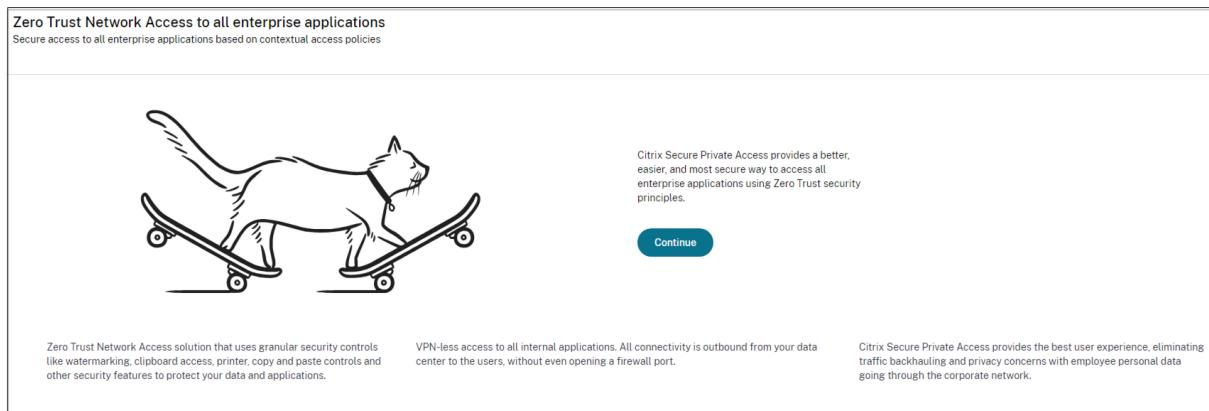
3. Siga las instrucciones que aparecen en pantalla para completar la instalación.

## Citrix Secure Private Access: local

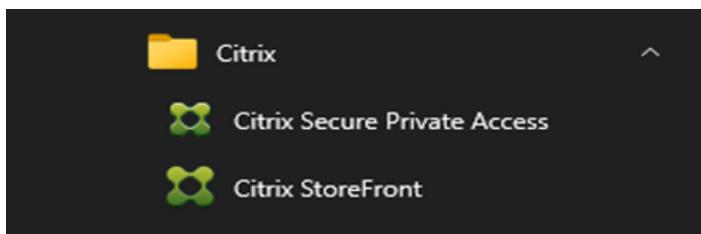


## Citrix Secure Private Access: local

Una vez finalizada la instalación, la consola de administración de la configuración inicial se abre automáticamente en la ventana predeterminada del navegador. Puede hacer clic en **Continuar** para configurar Secure Private Access.



También puede ver el acceso directo de Secure Private Access en el menú Inicio del escritorio (**Citrix > Citrix Secure Private Access**).



## SSO a la consola de administración

Se recomienda configurar la autenticación Kerberos para el navegador que utilice para la consola de administración de Secure Private Access. Esto se debe a que Secure Private Access utiliza la autenticación integrada de Windows (IWA) para su autenticación de administrador.

Si la autenticación Kerberos no está configurada, el navegador le pedirá que introduzca sus credenciales al acceder a la consola de administración de Secure Private Access.

- Si introduce sus credenciales, habilita el inicio de sesión de la Autenticación integrada de Windows (IWA).
- Si no introduce sus credenciales, aparecerá la página de inicio de sesión de Secure Private Access.

Debe iniciar sesión en la consola de administración para continuar con la configuración de Secure Private Access. Puede configurar Secure Private Access con cualquier usuario que pertenezca al mismo dominio que la máquina de instalación, siempre que el usuario tenga privilegios de administrador local en la máquina de instalación.

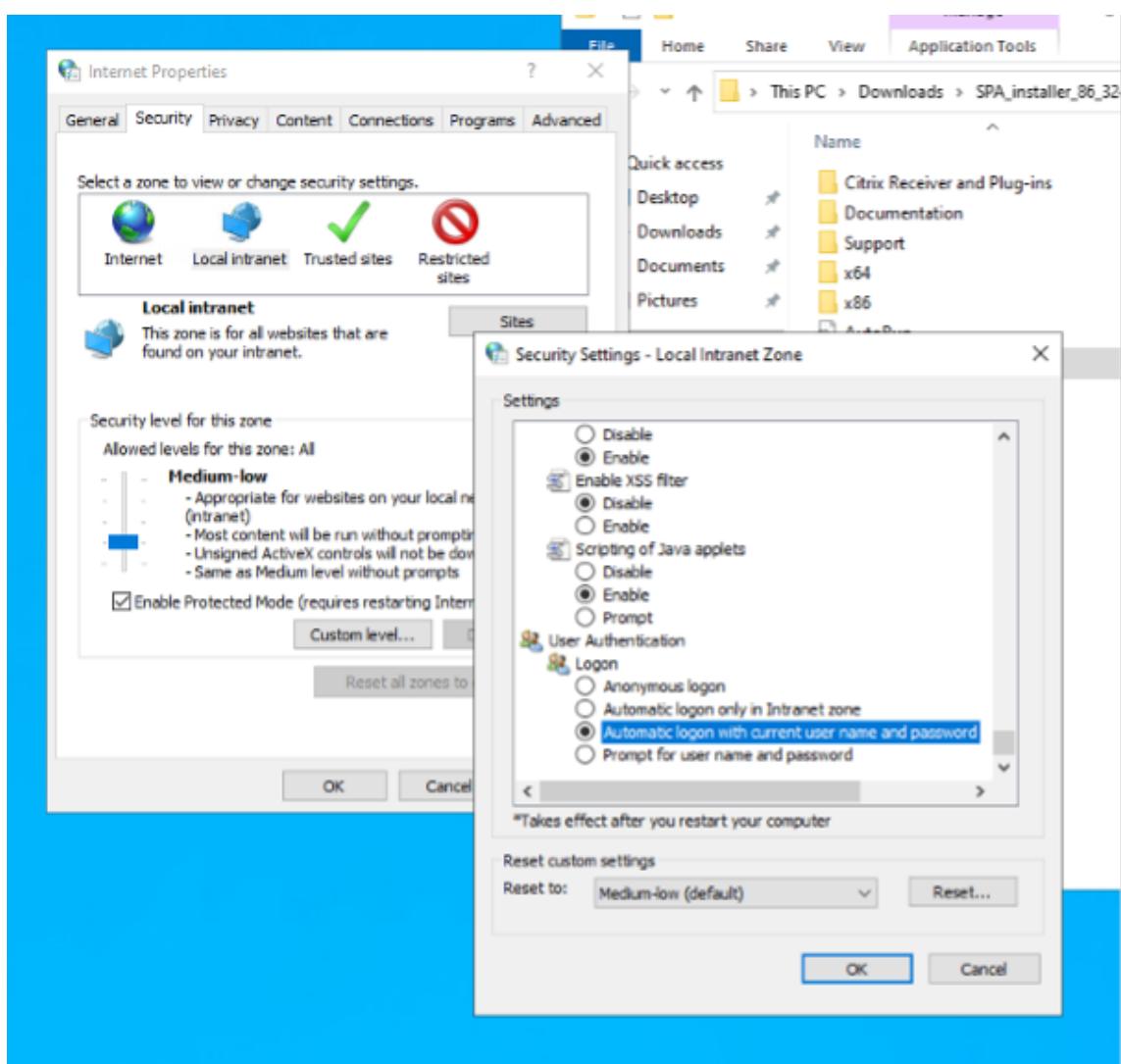
## Citrix Secure Private Access: local

Para los navegadores Google Chrome y Microsoft Edge, lleve a cabo los siguientes pasos para habilitar Kerberos.

1. Abre **Opciones de Internet**.
2. Seleccione la ficha **Seguridad** y haga clic en **Zona de intranet local**.
3. Haga clic en **Sitios** y agregue la URL de Secure Private Access.

También puede usar un comodín si planea instalar Secure Private Access en varios equipos. Por ejemplo, “[https://\\*.fabrikam.local](https://*.fabrikam.local)”.

4. Haga clic en **Nivel personalizado** y, en **Autenticación de usuario > Inicio de sesión**, seleccione **Inicio de sesión automático con el nombre de usuario y la contraseña actuales**.



### Nota:

- Si utilizas sesiones de incógnito de Chrome, crea una clave de registro DWORD Computer\

HKEY\_LOCAL\_MACHINE\ SOFTWARE\ Policies\ Google\ Chrome\ AmbientAuthenticationInPrivateModesEnabled y ponla en el valor 1.

- Debes reiniciar todas las ventanas de Chrome (incluidas las que no sean de incógnito) antes de habilitar Kerberos para el modo incógnito.
- Para otros navegadores, consulte la documentación del navegador específico sobre la autenticación Kerberos.

## Siguientes pasos

- [Configurar Secure Private Access](#)
- [Configurar NetScaler Gateway](#)
- [Configurar aplicaciones](#)
- [Configurar directivas de acceso para las aplicaciones](#)

## Actualice la base de datos mediante scripts

December 27, 2023

Puede usar la herramienta de configuración de administración para descargar los scripts de actualización de la base de datos para el complemento Secure Private Access.

1. Abra PowerShell o la ventana de línea de comandos con privilegios de administrador.
2. Cambie el directorio a la carpeta Admin\ AdminConfigTool en la carpeta de instalación de Secure Private Access (por ejemplo, cd “C:\Program Files\ Citrix\ Citrix Access Security\ Admin\ AdminConfigTool”).
3. Ejecute este comando:

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

## Configurar Secure Private Access

February 16, 2024

Puede configurar Secure Private Access creando un sitio nuevo o uniéndose a un sitio existente. En ambos casos, puede usar la consola de administración web para configurar el entorno de Secure Private Access.

- Configure Secure Private Access mediante la creación de un nuevo sitio
- Configure Secure Private Access uniéndose a un sitio existente

## Requisitos previos

El servidor de base de datos SQL debe estar instalado antes de crear un sitio.

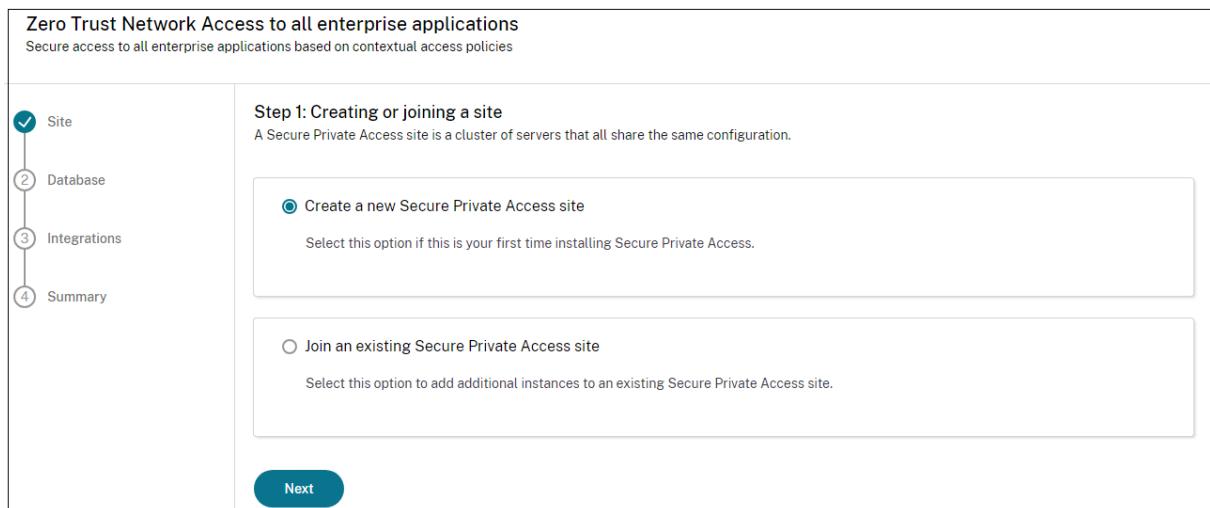
Configure Secure Private Access mediante la creación de un nuevo sitio

## Configure Secure Private Access mediante la creación de un nuevo sitio

### Paso 1: Configurar un sitio de Secure Private Access

Un sitio es el nombre de la implementación de Secure Private Access. Puedes crear un sitio o unirte a uno existente.

1. Inicie la consola de administración web de Secure Private Access.
2. En la página **Crear o unirse a un sitio**, la opción **Crear un nuevo sitio de Secure Private Access** está seleccionada de forma predeterminada.
3. Haga clic en **Siguiente**.



Cuando decide crear un sitio, debe configurar automáticamente o manualmente una base de datos para el nuevo sitio, ya que es posible que la base de datos correspondiente al nombre del sitio no esté disponible en la configuración.

### Paso 2: Configurar bases de datos

Debe crear una base de datos para el nuevo sitio de Secure Private Access. Esto se puede hacer de forma manual o automática.

## Citrix Secure Private Access: local

1. En **SQL Server Host**, introduzca el nombre del host del servidor. Por ejemplo:.sql1.fabrikam.local\citrix

Puede especificar una dirección de base de datos de una de las siguientes formas:

- NombreServidor
- NombreServidor\NombreInstancia
- NombreServidor,NúmeroPuerto

Para obtener más información, consulte [Bases de datos](#).

2. En **Sitio**, escriba un nombre para el sitio de Secure Private Access.
3. Haga clic en **Probar conectividad** para comprobar que la instancia de SQL Server es válida y también para confirmar que la base de datos especificada existe para el sitio.

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

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\* ⓘ

spaopdev-sql.spaopdev.local\spaopdev LTSR2402

**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. 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 **Download script**

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".

**Back** **Next**

### Nota:

- Si no hay un servidor SQL disponible para el sitio, se produce un error en la comprobación de conectividad.

- Si hay un servidor SQL disponible pero la base de datos no existe, se aprueba la comprobación de conectividad. Sin embargo, aparece un mensaje de advertencia.
- Secure Private Access usa la autenticación de Windows mediante la identidad de la máquina para autenticarse en un servidor SQL.

#### **Configuración automática:**

- Puede usar la opción **Configuración automática** solo si la identidad de la máquina tiene los privilegios de base de datos necesarios.
- Si no existe una base de datos en la dirección especificada, se crea automáticamente una base de datos.
- Al crear una base de datos, asegúrese de que esté vacía pero que tenga los privilegios de base de datos necesarios. Para obtener más información sobre los privilegios, consulte [Permisos necesarios para configurar bases de datos](#).

#### **Configuración manual:**

Puede utilizar la opción **Configuración manual** para configurar las bases de datos.

En la configuración manual, primero debe descargar los scripts y, a continuación, ejecutarlos en el servidor de base de datos que haya especificado en el campo **Host de SQL Server**.

##### **Nota:**

La creación de la base de datos puede fallar si la máquina no tiene los permisos READ, WRITE O UPDATE para crear tablas dentro de la base de datos del servidor SQL. Debe habilitar los permisos apropiados en la máquina. Para obtener más información, consulte [Permisos necesarios para configurar bases de datos](#).

### **Paso 3: Integrar los servidores StoreFront y NetScaler Gateway**

Debe especificar los detalles de los servidores de StoreFront y NetScaler Gateway para conectar Secure Private Access con los servidores de StoreFront y NetScaler Gateway. Esta conexión se debe establecer para permitir que StoreFront y NetScaler Gateway enruten el tráfico a Secure Private Access.

#### 1. Introduzca los siguientes detalles.

- **Dirección del servidor de Secure Private Access.** Por ejemplo:<https://secureaccess.domain.com>
- URL del almacén de**StoreFront**. Por ejemplo:<https://storefront.domain.com/Citrix/StoreMain>
- **Dirección de gateway pública** : URL de NetScaler Gateway. Por ejemplo:<https://gateway.domain.com>

- **Dirección de devolución de llamada de la puerta de enlace:** esta URL debe ser la misma que la configurada en **StoreFront**. Por ejemplo:<https://gateway.domain.com>
  - **Gateway VIP**: esta dirección IP virtual debe ser la misma que la configurada en StoreFront para las devoluciones de llamadas.
2. Haga clic en **Validar todas las URL**.
  3. Haga clic en **Siguiente** y, a continuación, seleccione **Guardar**.

## Citrix Secure Private Access: local

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

Site Database Integrations 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\*

Callback URL\*

[+ 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**

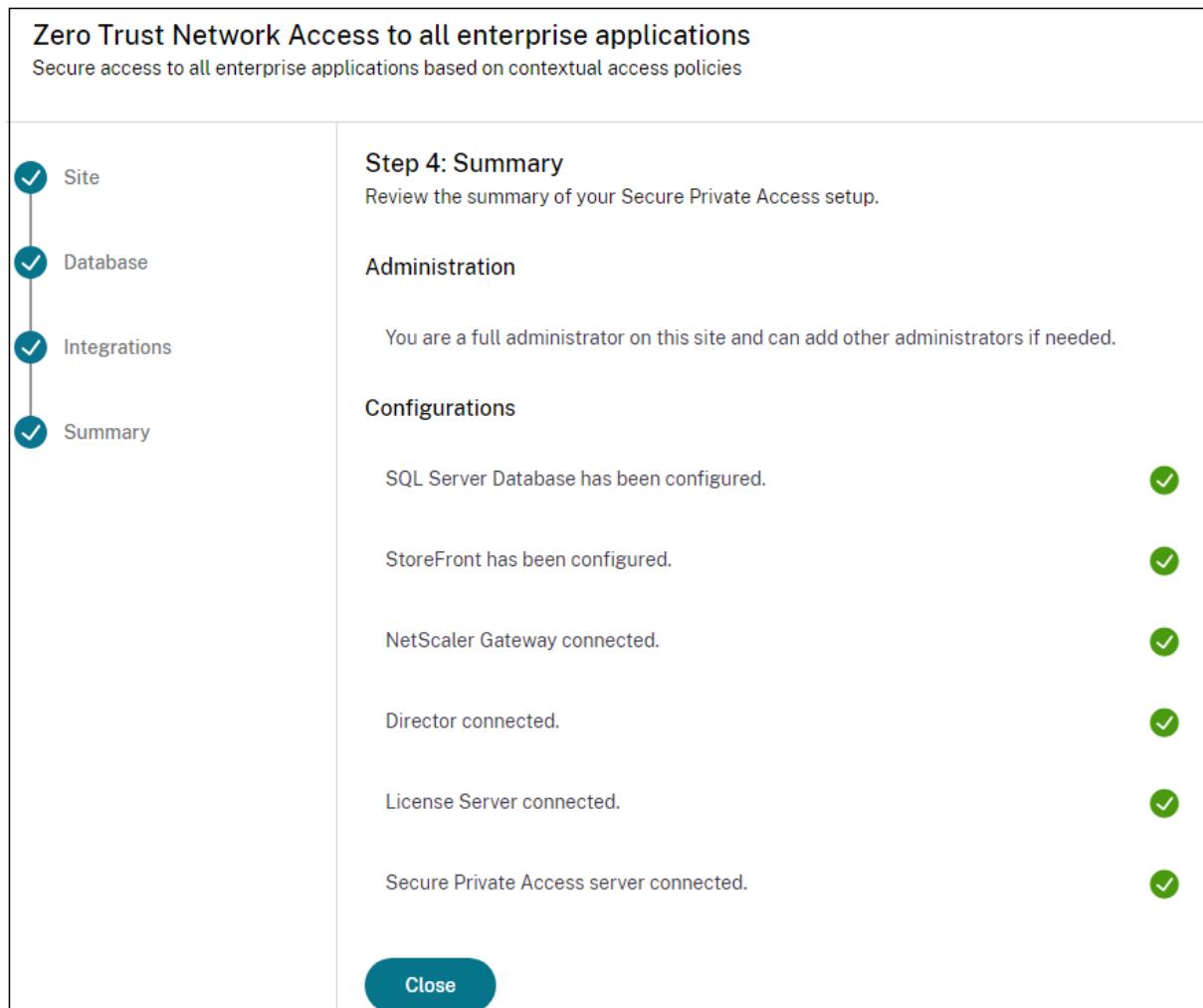
**Back** **Next**

### Paso 4: Resumen de la configuración

Una vez finalizada la configuración, se realiza la validación para garantizar que se pueda acceder a los servidores configurados. Además, se realiza una comprobación para garantizar que se pueda acceder

al servidor de Secure Private Access.

Si la página de resumen de la configuración muestra algún error, consulte [Solución de errores](#) para obtener más información. Si esto no resuelve el problema, póngase en contacto con el soporte de Citrix.



**Nota:**

- Una vez que haya configurado el entorno, puede modificar la configuración desde Configuración > Integraciones en la consola de administración web.
- Al administrador que instale Secure Private Access por primera vez se le concederá el permiso completo. A continuación, este administrador puede agregar otros administradores a la configuración. Puede ver la lista de administradores en **Configuración > Administradores**.
- También puede agregar grupos de administradores para que se habilite el acceso para todos los administradores de ese grupo.

Para obtener más información, consulte [Administrar la configuración después de la instalación](#).

## Configure Secure Private Access uniéndose a un sitio existente

1. En la página **Crear o unirse a un sitio**, seleccione **Unirse a un sitio existente**, a continuación, haga clic en **Siguiente**.

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

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.

Site

Database

Summary

SQL Server host\* ⓘ  
i.e.: sql.example.com,1433

Site name\* ⓘ  
i.e.: Site1

**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**

2. En **SQL Server Host**, introduzca el nombre del host del servidor. Asegúrese de que la base de datos correspondiente al nombre del sitio que introduzca ya esté presente en el servidor SQL que ha seleccionado. Puede especificar una dirección de base de datos de una de las siguientes formas:

- NombreServidor
- NombreServidor\NombreInstancia
- NombreServidor,NúmeroPuerto

Para obtener más información, consulte [Bases de datos](#).

3. En **Sitio**, escriba un nombre para el sitio de Secure Private Access.
4. Haga clic en **Probar conectividad** para comprobar que la instancia de SQL Server es válida y también para confirmar que el sitio especificado existe en la base de datos.

## Citrix Secure Private Access: local

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

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\* ⓘ

xa03-spa.training.local\SQLEXPRESS SPAopv2308

**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**

Si no hay una base de datos correspondiente para el sitio, se produce un error en la comprobación de conectividad.

### 5. Haga clic en **Guardar**.

La comprobación de validación de la configuración se realiza para garantizar que el servidor de base de datos SQL esté configurado y para comprobar que se puede acceder al servidor de Secure Private Access.

## Próximos pasos

- [Configurar NetScaler Gateway](#)
- [Configurar aplicaciones](#)
- [Configurar directivas de acceso para las aplicaciones](#)

## Configurar NetScaler Gateway

August 26, 2024

### Importante:

Se recomienda crear instantáneas de NetScaler o guardar la configuración de NetScaler antes de

## Citrix Secure Private Access: local

---

aplicar estos cambios.

1. Descargue el script desde <https://www.citrix.com/downloads/citrix-early-access-release/>.

Para crear otro dispositivo NetScaler Gateway, utilice `ns_gateway_secure_access.sh`.

Para actualizar un NetScaler Gateway existente, utilice `ns_gateway_secure_access_update.sh`.

2. Cargue estos scripts en la máquina NetScaler. Puede usar la aplicación WinSCP o el comando SCP. Por ejemplo, `*scp ns_gateway_secure_access.sh nsroot@nsalfa.fabrikam.local:/var/tmp*`.

**Nota:**

- Se recomienda utilizar la carpeta /var/tmp de NetScaler para almacenar datos temporales.
- Asegúrese de que el archivo esté guardado con los finales de línea LF. FreeBSD no admite CRLF.
- Si ve el error `-bash: /var/tmp/ns_gateway_secure_access.sh: /bin/sh^M: bad interpreter: No such file or directory`, significa que los finales de línea son incorrectos. Puede convertir el script con cualquier editor de texto enriquecido, como Notepad++.

3. Utilice SSH a NetScaler y cambie a shell (escriba ‘shell’ en la CLI de NetScaler).

4. Haga que el script cargado sea ejecutable. Use el comando chmod para hacerlo.

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

5. Ejecute el script cargado en el shell de NetScaler.

```
root@ns32201# ./ns_gateway_secure_access_2405.sh
NetScaler Gateway vserver name (default: _SecureAccess_Gateway): spaonprem
NetScaler Gateway IP: [REDACTED]
NetScaler Gateway FQDN: ns32205.cgwsanity.net
SPA Plugin IP: [REDACTED]
SPA Plugin FQDN: [REDACTED]
StoreFront Store URL (including protocol http/https): [REDACTED]
NetScaler authentication profile name: authnprof
NetScaler SSL server certificate name: ns32205
Domain: cgwsanity.net
Enable TCP/UDP Apptype support (Y/N): Y

***** Gateway configuration *****
NetScaler Gateway name: spaonprem
NetScaler Gateway IP: [REDACTED]
NetScaler Gateway FQDN: ns32205.cgwsanity.net
SPA Plugin FQDN: spa.cgwsanity.net
SPA Plugin IP: [REDACTED]
StoreFront Store URL: [REDACTED]
NetScaler authentication profile name: authnprof
NetScaler Gateway server certificate name: ns32205
Domain: cgwsanity.net
Enable App type TCP/UDP:
*****



Checking SPA Plugin support....
NetScaler supports SPA CLI, skipping nsapimgr commands
Number of PEs running: 3
Changing ns_vpn_enable_spa_tcp_udp_apps from 0 to 3 Done.
Changing ns_vpn_enable_spa_tcp_udp_apps from 0 to 3 Done.
Changing ns_vpn_enable_spa_tcp_udp_apps from 0 to 3 Done.
TCP/UDP Apptype support is enabled
Persisting TCP/UDP Apptype support setting: nsapimgr_wr.sh -ys ns_vpn_enable_spa_tcp_udp_apps=3 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
```

## Citrix Secure Private Access: local

- Introduzca los parámetros requeridos. Para ver la lista de parámetros, consulte [Requisitos previos](#).

Para el perfil de autenticación y el certificado SSL, debe proporcionar nombres en NetScaler.

Se genera un nuevo archivo con varios comandos de NetScaler (el predeterminado es var/tmp/ns\_gateway\_secure\_access).

```
Content] cat ns_gateway_secure.access
#####
# Upload file to NetScaler (e.g. -w /var/tmp)
# 2. Run batch command (e.g. batch -fileName /var/tmp/ns_gateway_secure.access -outfile /var/tmp/ns_gateway_secure.access_output)
# 3. Analyze output (e.g. cat /var/tmp/ns_gateway_secure.access_output)
#####

# Enable NetScaler features
enable ns feature SSL SSLV2V3 AAA REWRITE IC

# Add NetScaler Gateway vserver
add vpx vserver _SecureAccess_Gateway SSL 333.333.333.333 443 -listenpolicy NONE -tcpProfileName nstop_default_XA_XD_profile -deploymentType ICA_STOREFRONT -vserverFqdn gateway.domain.com -authnProfile
authn_gprof -icdonly OFF

# Add default AAA group for authenticated users
add aaa group SecureAccessGroup

# Add excluded domains
add vpx sessionaction ns_cvpn_default_bypass domain storefront.domain.com
bind policy patset ns_cvpn_default_bypass domain spa.domain.com
bind policy patset ns_cvpn.default_bypass domain citrix.com

# Add session actions
add vpx sessionaction AC_OSSecureAccess_Gateway -transparentInterception OFF -SSO ON -ssoCredential PRIMARY -useUIP NS -useIIP OFF -icaProxy OFF -whome "https://storefront.domain.com/Citrix/SFAStoreWebClientchoices OFF -ntdomain domain.com -defaultAuthorizationAction ALLOW -authorizationGroup SecureAccessGroup -clientlessVmMode ON -clientlessModeUrlEncoding TRANSPARENT -SecureBrowse ENABLED -addToSessionCookie OFF -ntdomain domain.com -defaultAuthorizationAction ALLOW -authorizationGroup SecureAccessGroup -clientlessVmMode ON -clientlessModeUrlEncoding TRANSPARENT -SecureBrowse ENABLED -addToSessionCookie https://storefront.domain.com -selectedKeyAndValue Group

# Add session policies
add vpx sessionpolicy AC_WB_SecureAccess_Gateway "HTTP.REQ.HEADER["User-Agent"]".CONTAINS("CitrixReceiver")* AC_OSSecureAccess_Gateway
add vpx sessionpolicy AC_WB_SecureAccess_Gateway "HTTP.REQ.HEADER["User-Agent"]".CONTAINS("CitrixReceiver").NOT* AC_WB_SecureAccess_Gateway

# Add rewrite policies for Citrix Headers
add rewrite action Add_X-Citrix-Via insert http_header X-Citrix-Via "gateway.domain.com"
add rewrite action Add_X-Citrix-Via-VIP insert http_header X-Citrix-Via-VIP "33.333.333.333"
add rewrite action Add_X-GW-SessionId insert http_header X-GW-SessionId ANDER_SESSIONID
add rewrite action Add_X-GM-SessionId insert http_header X-GM-SessionId ANDER_SESSIONID
add rewrite policy Add_X-Citrix-Via-VIPFor1 "HTTP.REQ.HEADER["X-Citrix-Via"]".EXISTS.NOT* Add_X-Citrix-Via
add rewrite policy Add_X-Citrix-Via-VIPFor1 "HTTP.REQ.HOSTNAME.CONTAINS("spa.domain.com")" && "HTTP.REQ.HEADER["X-Citrix-Via-VIP"]".EXISTS.NOT* Add_X-Citrix-Via-VIP

# Add SSO traffic policy for SPA Plugin
add vpx trafficaction _SecureAccess_Gateway_Traffic Action http -SSO ON
```

- Cambie a la CLI de NetScaler y ejecute los comandos de NetScaler resultantes desde el nuevo archivo con el comando batch. Por ejemplo,

```
batch -fileName /var/tmp/ns_gateway_secure.access -outfile /var/tmp/ns_gateway_secure.access_output
```

NetScaler ejecuta los comandos del archivo uno por uno. Si un comando falla, continúa con el siguiente comando.

Un comando puede fallar si existe un recurso o si uno de los parámetros introducidos en el paso 6 es incorrecto.

- Asegúrese de que todos los comandos se hayan completado correctamente.

### Nota:

Si se produce un error, NetScaler sigue ejecutando los comandos restantes y crea/actualiza/enlaza parcialmente los recursos. Por lo tanto, si aparece un error inesperado debido a que uno de los parámetros es incorrecto, se recomienda volver a realizar la configuración desde el principio.

## Configurar Secure Private Access en un NetScaler Gateway con la configuración existente

También puede usar los scripts en un NetScaler Gateway existente para admitir Secure Private Access. Sin embargo, el script no actualiza lo siguiente:

- Servidor virtual NetScaler Gateway existente

- Acciones de sesión y directivas de sesión existentes vinculadas a NetScaler Gateway

Asegúrese de revisar cada comando antes de ejecutarlo y cree copias de seguridad de la configuración de la puerta de enlace.

### Parámetros del servidor virtual NetScaler Gateway

Al agregar o actualizar el servidor virtual de NetScaler Gateway existente, asegúrese de que los siguientes parámetros estén configurados en los valores definidos.

tcpProfileName: nstcp\_default\_XA\_XD\_profile

deploymentType: ICA\_STOREFRONT

icaOnly: DESACTIVADO

Ejemplos:

Para agregar un servidor virtual:

```
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`
```

Para actualizar un servidor virtual:

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

Para obtener más información sobre los parámetros del servidor virtual, consulte [VPN-SessionAction](#).

### Acciones de sesión de NetScaler Gateway

La acción de sesión está enlazada a un servidor virtual de puerta de enlace con directivas de sesión. Al crear una acción de sesión, asegúrese de que los siguientes parámetros estén configurados en los valores definidos.

- transparentInterception: OFF
- SSO: ON
- ssoCredential: PRIMARY
- useMIP: NS
- useIIP: OFF
- icaProxy: OFF
- wihome: "<https://storefront.mydomain.com/Citrix/MyStoreWeb>" - Reemplázelo por la URL de almacén real
- ClientChoices: OFF
- ntDomain: mydomain.com: se utiliza para el inicio de sesión único

- `defaultAuthorizationAction`: PERMITIR
- `authorizationGroup`: SecureAccessGroup (asegúrese de crear este grupo, se usa para vincular directivas de autorización específicas de Secure Private Access)
- `clientlessVpnMode`: ON
- `clientlessModeUrlEncoding`: TRANSPARENT
- `SecureBrowse`: ENABLED
- `Storefronturl`: "<https://storefront.mydomain.com>"
- `sfGatewayAuthType`: dominio

Ejemplos:

Para agregar una acción de sesión:

```
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
```

Para actualizar una acción de sesión:

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

Para obtener más información sobre los parámetros de acción de la sesión, consulte <https://developer-docs.netscaler.com/en-us/adc-command-reference-int/13-1/vpn/vpn-sessionaction>.

## Compatibilidad con las aplicaciones ICA

NetScaler Gateway creado o actualizado para admitir el plug-in Secure Private Access también se puede usar para enumerar e iniciar aplicaciones ICA. En este caso, debe configurar Secure Ticket Authority (STA) y vincularla a NetScaler Gateway.

Nota: El servidor STA suele formar parte de la implementación de DDC de Citrix Virtual Apps and Desktops.

Para obtener más información, consulte los siguientes temas:

- [Configurar Secure Ticket Authority en NetScaler Gateway](#)
- [Preguntas frecuentes: Citrix Secure Gateway/ NetScaler Gateway Secure Ticket Authority](#)

## Suporte para etiquetas de acceso inteligentes

En las siguientes versiones, NetScaler Gateway envía las etiquetas automáticamente. No es necesario utilizar la dirección de devolución de llamada de la puerta de enlace para recuperar las etiquetas de acceso inteligentes.

- 13.1.48.47 y versiones posteriores
- 14.1—4.42 y versiones posteriores

Las etiquetas de acceso inteligente se agregan como encabezado en la solicitud del plug-in Secure Private Access.

Utilice la opción `ns_vpn_enable_spa_onprem` o `ns_vpn_disable_spa_onprem` para habilitar o inhabilitar esta función en estas versiones de NetScaler.

- Puede alternar con el comando (shell de FreeBSD):

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

- Habilite el modo cliente SecureBrowse para la configuración de llamadas HTTP ejecutando el siguiente comando (shell de FreeBSD).

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

- Para inhabilitarlo, vuelva a ejecutar el mismo comando.
- Para comprobar si la opción está activada o desactivada, ejecute el comando `nsconmsg`.
- Para configurar etiquetas de acceso inteligente en NetScaler Gateway, consulte Configuración de etiquetas personalizadas (etiquetas SmartAccess) en NetScaler Gateway.

## Limitaciones conocidas

- El NetScaler Gateway existente se puede actualizar con un script, pero puede haber un número infinito de posibles configuraciones de NetScaler que no se pueden cubrir con un solo script.
- No utilice ICA Proxy en NetScaler Gateway. Esta función está inhabilitada cuando se configura NetScaler Gateway.
- Si usa NetScaler implementado en la nube, debe realizar algunos cambios en la red. Por ejemplo, permita la comunicación entre NetScaler y otros componentes en determinados puertos.
- Si habilita el SSO en NetScaler Gateway, asegúrese de que NetScaler se comunique con StoreFront mediante una dirección IP privada. Puede que tenga que agregar un nuevo registro DNS de StoreFront a NetScaler con una dirección IP privada de StoreFront.

## Cargar certificado de puerta de enlace pública

Para cargar un certificado de puerta de enlace pública en la base de datos de Secure Private Access, lleve a cabo los siguientes pasos:

1. Abra PowerShell o la ventana de línea de comandos con los privilegios de administrador.
2. Cambie el directorio a la carpeta Admin\AdminConfigTool en la carpeta de instalación de Secure Private Access (por ejemplo, cd “C:\Program Files\Citrix\Citrix Access Security\Admin\AdminConfigTool”)
3. Ejecute este comando:

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

## Configurar aplicaciones

February 16, 2024

1. Seleccione la ubicación en la que reside la aplicación.
  - **Fuera de mi red corporativa** para aplicaciones externas.
  - **Dentro de mi red corporativa** para aplicaciones internas.
2. Introduzca los siguientes detalles en la sección Detalles de la aplicación y haga clic en **Siguiente**.

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 type \*  
HTTP/HTTPS

App name \*  
google-translate

App description

App icon

Change icon     Use default icon  
(128 KB max, ICO)

Do not display application icon in Workspace app  
 Add application to favorites in Workspace app  
 Allow user to remove from favorites  
 Do not allow user to remove from favorites

App category ⓘ  
Ex.: Category\SubCategory\SubCategory

URL \*  
https://translate.google.co.in

App Connectivity \* ⓘ  
Internal

Related Domains \*  
\* google2.com

App Connectivity \* ⓘ  
Internal

[+ Add another related domain](#)

Save     Cancel

- **Nombre de la aplicación:** Nombre de la aplicación.
- **Descripción de la aplicación :** una breve descripción de la aplicación. Esta descripción se muestra a los usuarios en el espacio de trabajo. También puede introducir palabras clave para las solicitudes en el formato **KEYWORDS**: <keyword\_name>. Puede usar las palabras clave para filtrar las aplicaciones. Para obtener más información, consulta [Filtrar recursos por palabras clave incluidas](#).
- **Categoría de aplicación :** agregue la categoría y el nombre de la subcategoría (si corresponde) con los que debe aparecer la aplicación que va a publicar en la interfaz de usuario de Citrix Workspace. Puede agregar una nueva categoría para cada aplicación o usar las categorías existentes de la interfaz de usuario de Citrix Workspace. Una vez que especi-

fiques una categoría para una aplicación web o SaaS, la aplicación aparecerá en la interfaz de usuario de Workspace en la categoría específica.

- La categoría/subcategoría se puede configurar por el administrador y los administradores pueden agregar una nueva categoría para cada aplicación.
- Los nombres de las categorías o subcategorías deben estar separados por una barra invertida. Por ejemplo, Negocios y productividad\ Ingeniería . Además, en este campo se distingue entre mayúsculas y minúsculas. Los administradores deben asegurarse de definir la categoría correcta. Si hay una discrepancia entre el nombre de la interfaz de usuario de Citrix Workspace y el nombre de la categoría introducido en el campo Categoría de aplicaciones, la categoría aparece como una categoría nueva.

Por ejemplo, si introduce la categoría Empresa y productividad de forma incorrecta como Empresa y productividad en el campo Categoría de aplicaciones , aparecerá una nueva categoría denominada Empresa y productividad en la interfaz de usuario de Citrix Workspace, además de la categoría Empresa y productividad .

- **Icono de la aplicación:** Haga clic en **Cambiar ícono** para cambiar el ícono de la aplicación. El tamaño del archivo de iconos debe ser de 128 x 128 píxeles y solo se admite el formato Ico. Si no cambia el ícono, se muestra el ícono predeterminado.
  - **No mostrar la aplicación a los usuarios :** seleccione esta opción si no desea mostrar la aplicación a los usuarios.
  - **URL :** URL de la aplicación.
  - **Dominios relacionados :** el dominio relacionado se rellena automáticamente en función de la URL de la aplicación. Los administradores pueden agregar más dominios internos o externos relacionados.
- Agregar la aplicación a favoritos automáticamente :** haga clic en esta opción para agregar esta aplicación como favorita en la aplicación Citrix Workspace.
- **Permitir que el usuario la elimine de los favoritos :** haga clic en esta opción para permitir que los suscriptores de la aplicación eliminan la aplicación de la lista de aplicaciones favoritas de la aplicación Citrix Workspace.
- Al seleccionar esta opción, aparece un ícono de estrella amarilla en la esquina superior izquierda de la aplicación Citrix Workspace.
- **No permitir que el usuario la elimine de los favoritos :** haga clic en esta opción para evitar que los suscriptores eliminan la aplicación de la lista de aplicaciones favoritas de la aplicación Citrix Workspace.

Al seleccionar esta opción, aparece un ícono de estrella con un candado en la esquina superior izquierda de la aplicación Citrix Workspace.

Si quita las aplicaciones marcadas como favoritas de la consola de Secure Private Access, estas aplicaciones deben eliminarse manualmente de la lista de favoritos de Citrix Workspace. Las aplicaciones no se eliminan automáticamente de StoreFront si se eliminan de la consola de Secure Private Access.

Conectividad de aplicaciones: seleccione Interna para aplicaciones web y Externa para aplicaciones SaaS.

3. Haga clic en **Guardary**, a continuación, en **Finalizar**.

Puede ver todos los dominios de la aplicación que están configurados en **Configuración > Dominio de la aplicación**. Para obtener más información, consulte [Administrar la configuración después de la instalación](#).

## Próximos pasos

[Configurar directivas de acceso para las aplicaciones](#)

## Configurar directivas de acceso para las aplicaciones

December 27, 2023

Las directivas de acceso le permiten habilitar o inhabilitar el acceso a las aplicaciones en función del usuario o los grupos de usuarios. Además, puede habilitar el acceso restringido a las aplicaciones agregando las restricciones de seguridad.

1. Haga clic en **Crear directiva**.

## Citrix Secure Private Access: local

The image displays two side-by-side screenshots of the Citrix Secure Private Access policy configuration interface. Both screenshots show the 'Create Access Policy' screen.

**Policy for Web/SaaS apps:** This section shows a policy named 'msn-pol' that applies to the application 'msn'. The user condition is set to 'Matches any of' for 'spabrl.com' and 'spabrl.com\Administrator'. The action selected is 'Allow access with restrictions'. There are no access restrictions listed. A checkbox for 'Enable policy on save' is checked. Buttons for 'Save' and 'Cancel' are at the bottom.

**Policy for TCP/UDP apps:** This section shows a policy named 'rdp' that applies to the application 'Goo'. The user condition is set to 'Matches any of' for 'spaopdev.local' and 'spaopdev.local\SPAOP users'. The action selected is 'Allow access with restrictions'. A conditional tag 'allow\_access' is selected under 'AND'. A checkbox for 'Enable policy on save' is checked. Buttons for 'Save' and 'Cancel' are at the bottom.

2. En **Aplicaciones**, seleccione las aplicaciones para las que desea aplicar las directivas de acceso.
3. En **Usuarios/grupos de usuarios**: seleccione las condiciones y los usuarios o grupos de usuarios en función de los cuales se debe permitir o denegar el acceso a la aplicación.
  - **Coincide con cualquiera de**: Solo se permite el acceso a los usuarios o grupos que coincidan con alguno de los nombres que figuran en el campo.
  - **No coincide con ninguno**: se permite el acceso a todos los usuarios o grupos, excepto los que figuran en el campo.
4. Haga clic en **Agregar condición** para agregar otra condición basada en etiquetas contextuales. Estas etiquetas se derivan de NetScaler Gateway.
5. Seleccione **Etiquetas condicionales** y, a continuación, seleccione las condiciones en función de las cuales se debe permitir o denegar el acceso a la aplicación.
6. En **Luego, haga lo siguiente**, seleccione una de las siguientes acciones que se deben aplicar en la aplicación en función de la evaluación de la condición.
  - **Permitir el acceso**
  - **Permitir el acceso con restricción**
  - **Denegar el acceso**

Al seleccionar **Permitir el acceso con restricciones**, puede seleccionar las siguientes restricciones.

**Add/edit restrictions**

| Access Settings            |                       | Current Value    |
|----------------------------|-----------------------|------------------|
| > <input type="checkbox"/> | Clipboard             | Allowed          |
| > <input type="checkbox"/> | Copy                  | Allowed          |
| > <input type="checkbox"/> | Download MIME types   | Multiple options |
| > <input type="checkbox"/> | Downloads             | Allowed          |
| > <input type="checkbox"/> | Insecure content      | Prohibited       |
| > <input type="checkbox"/> | Keylogging protection | Allowed          |
| > <input type="checkbox"/> | Microphone            | Ask every time   |
| > <input type="checkbox"/> | Notifications         | Ask every time   |
| > <input type="checkbox"/> | Paste                 | Allowed          |
| > <input type="checkbox"/> | Personal data masking | Multiple options |
| > <input type="checkbox"/> | Popups                | Block            |
| > <input type="checkbox"/> | Printing              | Allowed          |
| > <input type="checkbox"/> | Printing options      | Multiple options |
| > <input type="checkbox"/> | Screen capture        | Allowed          |
| > <input type="checkbox"/> | Upload MIME types     | Multiple options |
| > <input type="checkbox"/> | Uploads               | Allowed          |
| > <input type="checkbox"/> | Watermark             | Disabled         |
| > <input type="checkbox"/> | Webcam                | Ask every time   |

**Done** **Cancel**

- **Restringir el acceso al portapapeles:** inhabilita las operaciones de cortar/copiar/pegar entre la aplicación y el portapapeles del sistema.
- **Restringir la impresión:** inhabilita la capacidad de imprimir desde el navegador Citrix Enterprise.
- **Restringir descargas:** inhabilita la capacidad del usuario de descargar desde la aplicación.
- **Restringir las subidas:** inhabilita la capacidad del usuario de subir contenido desde la aplicación.
- **Mostrar marca de agua:** muestra una marca de agua en la pantalla del usuario que muestra el nombre de usuario y la dirección IP de la máquina del usuario.
- **Restringir el registro de claves:** protege contra los registradores de claves. Cuando un usuario intenta iniciar sesión en la aplicación con el nombre de usuario y la contraseña, todas las claves se cifran en los registradores de claves. Además, todas las actividades

que el usuario realiza en la aplicación están protegidas contra el registro de claves.

Por ejemplo, si las directivas de protección de aplicaciones están habilitadas para Office 365 y el usuario edita un documento de Word de Office 365, todas las pulsaciones de teclas se cifran en los registradores de teclas.

- **Restringir la captura de pantalla:** desactiva la capacidad de capturar las pantallas mediante cualquiera de los programas o aplicaciones de captura de pantalla. Si un usuario intenta capturar la pantalla, se captura una pantalla en blanco.

**Nota:**

Las restricciones de registro de teclas y captura de pantalla solo se aplican a los clientes de escritorio de Citrix Workspace.

7. En **Nombre de la directiva**, introduzca un nombre para la directiva.
8. Seleccione **Habilitar la directiva al guardar**. Si no selecciona esta opción, la directiva solo se crea y no se aplica a las aplicaciones. Como alternativa, también puede habilitar la directiva desde la página Directivas de acceso mediante la opción de cambio.

### Prioridad de la directiva de acceso

Después de crear una directiva de acceso, se asigna un número de prioridad a la directiva de acceso de forma predeterminada. Puede ver la prioridad en la página de inicio de las directivas de acceso.

Una prioridad con un valor inferior tiene la preferencia más alta y se evalúa primero. Si esta directiva no cumple con las condiciones definidas, se evalúa la siguiente directiva con el número de prioridad más bajo y así sucesivamente.

Puede cambiar el orden de prioridad moviendo las directivas hacia arriba o hacia abajo mediante el icono de arriba a abajo de la columna **Prioridad**.

### Siguientes pasos

Valide su configuración desde las máquinas cliente (Windows y macOS).

[Example](#)

## Flujo de usuarios finales

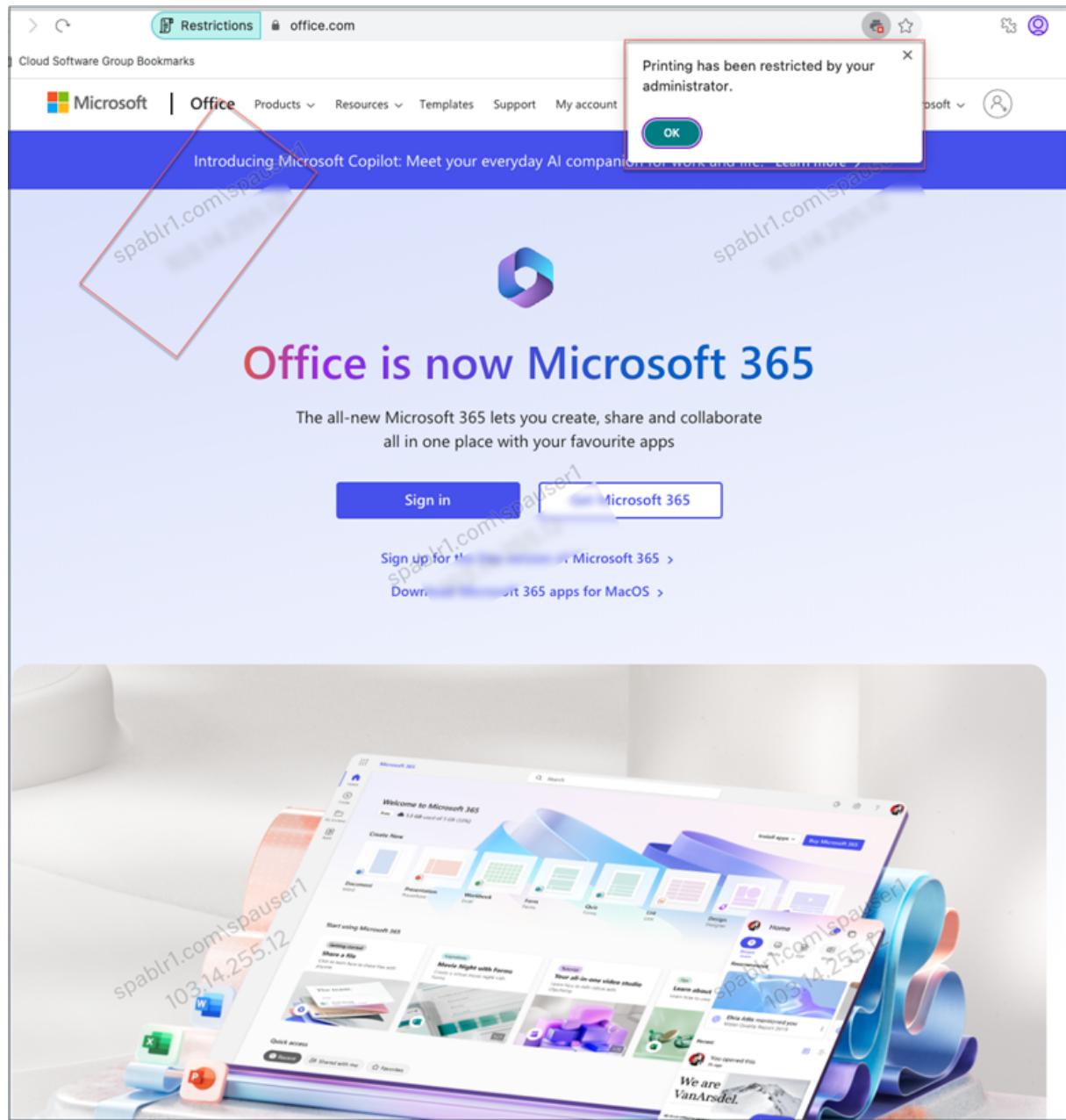
August 26, 2024

Supongamos que un administrador ha configurado la aplicación Office365 con la restricción de marca de agua e impresión para el usuario final. Ahora, cuando el usuario final acceda a la aplicación Office365, se deben aplicar las restricciones de marca de agua e impresión en la aplicación.

El usuario final debe realizar los siguientes pasos para acceder a la aplicación Office365:

1. Acceder al almacén de StoreFront desde la aplicación Citrix Workspace.
2. Iniciar sesión en el almacén.
3. Hacer clic en la ficha **Aplicaciones** y, a continuación, en la aplicación **Office365**.

El usuario final ahora debe observar que la aplicación de Office365 se ha iniciado y contiene la marca de agua. Además, si el usuario final intenta imprimir algunos datos desde la aplicación Office365, se le debe mostrar el mensaje de restricción de impresión.



**Nota:**

Los administradores deben proporcionar a los usuarios la información de cuenta que necesitan para acceder a los escritorios y aplicaciones virtuales. Para obtener más información, consulte [Agregar la URL del almacén a la aplicación Citrix Workspace](#).

## **Integración de Secure Private Access con la integración de Web Studio**

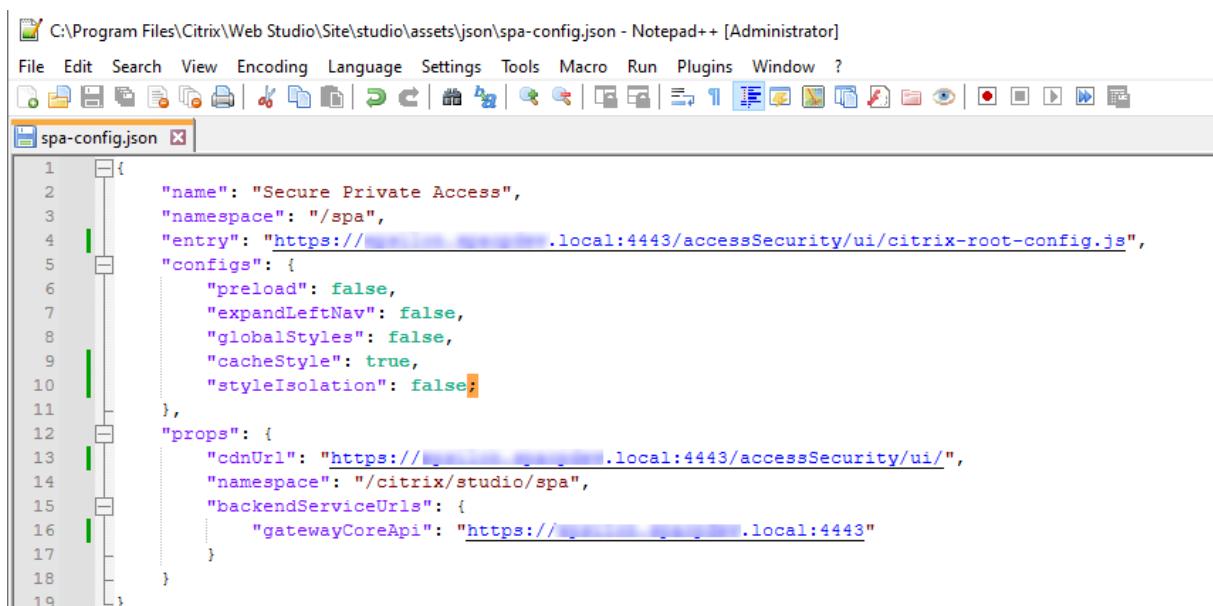
June 19, 2024

Citrix Secure Private Access también está integrado en la consola de Web Studio para permitir a los usuarios acceder sin problemas al servicio a través de Web Studio.

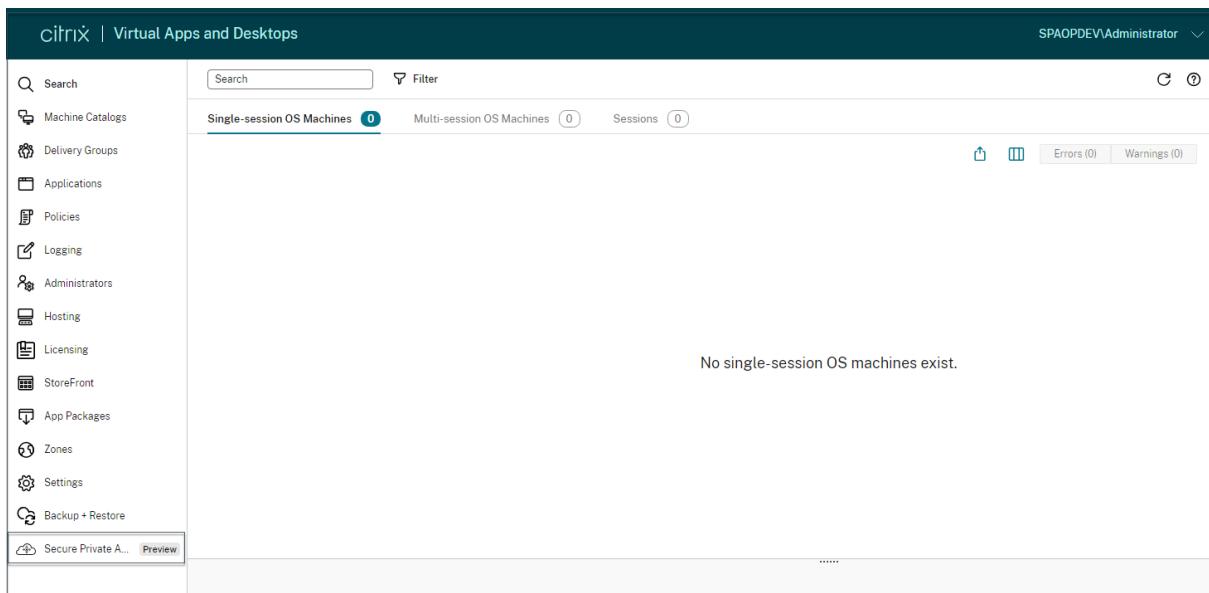
Debe instalar Web Studio versión 2308 o posterior.

Realice los siguientes pasos para habilitar la integración con Web Studio:

1. Instale Citrix Web Studio mediante el instalador de Citrix Virtual Apps and Desktops o el instalador DDC integrado.
  2. Siga las instrucciones que aparecen en pantalla y complete la instalación. Cuando se le pida una dirección del controlador, introduzca el FQDN del DDC como dirección del controlador.
  3. Tras una instalación correcta, vaya a la carpeta C:\Program Files\Citrix\Web Studio\Site\assets\json y modifique el contenido del archivo spa-config.json.  
Si se utilizó una ubicación no predeterminada para la instalación de Web Studio, sustituya la ubicación de instalación predeterminada en C:\Program Files\Citrix por la ubicación correcta.



1. Sustituya “SpaServer”por el FQDN de su complemento de Secure Private Access.
  2. Inicie sesión en Web Studio.



1. En el menú de navegación de la izquierda, haga clic en **Secure Private Access <Preview>** para acceder a la consola de administración de Secure Private Access desde Web Studio.

## Administrar la configuración después de la instalación

December 27, 2023

Una vez que haya instalado Secure Private Access, puede modificar la configuración desde la página Configuración.

### Gestione el enrutamiento de los dominios de las aplicaciones

Puede ver una lista de los dominios de aplicaciones agregados en la configuración de Secure Private Access. En la tabla de dominios de la aplicación se enumeran todos los dominios relacionados y cómo se enruta el tráfico de la aplicación (externa o internamente).

1. Haga clic en **Configuración > Dominio de la aplicación**.
2. Puede hacer clic en el icono de edición y cambiar el tipo de ruta, si es necesario.

### Administrar administradores para un Secure Private Access

Puede ver la lista de administradores y también agregar administradores desde la página **Configuración > Administradores**. El administrador que instala Secure Private Access por primera vez recibe

el permiso completo. A continuación, este administrador puede agregar otros administradores a la configuración.

También puedes agregar grupos de administradores para que se habilite el acceso para todos los administradores de ese grupo.

1. En la página **Administradores**, haga clic en **Agregar**.
2. En **Dominio**, seleccione el dominio al que debe agregarse este administrador.
3. En **Usuarios o grupo de usuarios**, seleccione el usuario o los grupos a los que pertenece este usuario.
4. En **Tipo de administrador**, seleccione el tipo de permiso que debe asignarse a este usuario.

### **Actualice los detalles del servidor StoreFront o NetScaler Gateway después de la configuración**

Una vez que haya configurado Secure Private Access, puede modificar o actualizar las entradas de StoreFront y NetScaler Gateway desde la ficha **Integraciones**.

1. Haga clic en **Configuración > Integraciones**.
2. Haga clic en el ícono de edición en línea con la configuración que desee modificar y actualizar la entrada.
3. Haga clic en el ícono de actualización para asegurarse de que la configuración es válida.

#### **Nota:**

Si Secure Private Access está instalado en un equipo diferente al de StoreFront, descargue el script de StoreFront y ejecútelo en StoreFront.

## Citrix Secure Private Access: local

The screenshot shows the 'Integrations' tab of the Citrix Secure Private Access configuration interface. On the left, a sidebar lists 'Overview', 'Applications', 'Access Policies', 'Settings', and 'Troubleshooting'. The main area contains several configuration sections:

- Secure Private Access address:** Set to <https://gamma.spaopdev.local>. Action buttons: checkmark, refresh, edit.
- StoreFront Store URL:** Set to <https://gamma.spaopdev.local/Citrix/StoreGamma>. Action buttons: checkmark, refresh, edit, 'Download Script' button.
- Public NetScaler Gateway address:** Set to <https://gwgamma.spaopdev.local>. Action buttons: checkmark, refresh, edit, 'Refresh Certificate' button. Sub-link: 'Get Gateway scripts'.
- NetScaler Gateway virtual IP address and callback URL:** Gateway VIP set to <https://gwgamma.spaopdev.local>, Callback URL set to <https://gwgamma.spaopdev.local>. Action buttons: checkmark, refresh, edit. Sub-link: '+ Add another virtual IP address and callback URL'.
- Director URL:** Set to <https://director.spaopdev.local>. Action buttons: checkmark, refresh, edit.
- License Server URL:** Set to <https://ls.spaopdev.local>. Action buttons: checkmark, refresh, edit.

## Descripción general del panel

December 27, 2023

El panel de registros de solución de problemas de Secure Private Access muestra los registros relacionados con el inicio de la aplicación, la enumeración de las aplicaciones y sus estados.

Puede ver los registros de la hora preestablecida o de una línea de tiempo personalizada. Puede agregar columnas al gráfico haciendo clic en el signo +, según la información que quiera ver en el panel. Puede exportar los registros de usuario a formato CSV.

## Citrix Secure Private Access: local

Puede utilizar los filtros (CATEGORÍA y RESULTADO) para refinar los resultados de la búsqueda.

| TIME                | USER NAME          | CATEGORY        | RESULT  | TRANSACTION ID                       | DETAILS  |
|---------------------|--------------------|-----------------|---------|--------------------------------------|--|
| 2024-06-19 13:26:29 | spouser@spabrl.com | App Enumeration | Success | e4e1460e-0f57-4e25-8f90-a57a936f18a4 | Total apps enumerated for user spouser@spabrl...   |
| 2024-06-19 13:26:29 | spouser@spabrl.com | App Enumeration | Success | e4e1460e-0f57-4e25-8f90-a57a936f18a4 | Show Details                                       |
| 2024-06-19 13:26:29 | spouser@spabrl.com | App Enumeration | Success | e4e1460e-0f57-4e25-8f90-a57a936f18a4 | SmartAccess tags received PL_OS_SecureAcc...       |
| 2024-06-19 13:26:29 | spouser@spabrl.com | App Enumeration | Success | e4e1460e-0f57-4e25-8f90-a57a936f18a4 | Credential validation succeeded for user spous...  |
| 2024-06-19 13:55:22 | spouser@spabrl.com | App Access      | Success | e278e3e3-763d-4ef1-9f91-0e6f8d7015b  | Received Gateway callback response successf...     |
| 2024-06-19 12:55:22 | spouser@spabrl.com | App Access      | Success | e278e3e3-763d-4ef1-9f91-0e6f8d7015b  | Successfully validated the user credentials re...  |
| 2024-06-19 12:55:19 | spouser@spabrl.com | App Access      | Success | 65963fb6-59d9-4e8b-9920-d5e5fa9af098 | Policy evaluation returned access state as ALL...  |
| 2024-06-19 12:55:19 | spouser@spabrl.com | App Access      | Success | 65963fb6-59d9-4e8b-9920-d5e5fa9af098 | Show Details                                       |
| 2024-06-19 12:55:19 | spouser@spabrl.com | App Access      | Success | 65963fb6-59d9-4e8b-9920-d5e5fa9af098 | SmartAccess tags received PL_OS_SecureAcc...       |
| 2024-06-19 12:55:19 | spouser@spabrl.com | App Access      | Success | 65963fb6-59d9-4e8b-9920-d5e5fa9af098 | Policy evaluation returned access state as ALL...  |
| 2024-06-19 12:55:19 | spouser@spabrl.com | App Access      | Success | 65963fb6-59d9-4e8b-9920-d5e5fa9af098 | Show Details                                       |
| 2024-06-19 12:55:19 | spouser@spabrl.com | App Access      | Success | 65963fb6-59d9-4e8b-9920-d5e5fa9af098 | SmartAccess tags received PL_OS_SecureAcc...       |
| 2024-06-19 12:55:19 | spouser@spabrl.com | App Access      | Success | 65963fb6-59d9-4e8b-9920-d5e5fa9af098 | Policy evaluation returned access state as ALL...  |
| 2024-06-19 12:55:19 | spouser@spabrl.com | App Access      | Success | 65963fb6-59d9-4e8b-9920-d5e5fa9af098 | Show Details                                       |
| 2024-06-19 12:55:19 | spouser@spabrl.com | App Access      | Success | 65963fb6-59d9-4e8b-9920-d5e5fa9af098 | SmartAccess tags received PL_OS_SecureAcc...       |
| 2024-06-19 12:55:19 | spouser@spabrl.com | App Access      | Success | 65963fb6-59d9-4e8b-9920-d5e5fa9af098 | Policy evaluation returned access state as ALL...  |
| 2024-06-19 12:55:19 | spouser@spabrl.com | App Access      | Success | 65963fb6-59d9-4e8b-9920-d5e5fa9af098 | Show Details                                       |
| 2024-06-19 12:55:17 | spouser@spabrl.com | App Access      | Success | 68d977eb-9f59-4ec7-9ef5-a97bd242c97  | Successfully enumerated and sent the policy doc... |
| 2024-06-19 12:55:17 | spouser@spabrl.com | App Access      | Success | 68d977eb-9f59-4ec7-9ef5-a97bd242c97  | Show Details                                       |
| 2024-06-19 12:55:17 | spouser@spabrl.com | App Access      | Success | 40068d8a-5068-4840-b7a5-7b20594a1cc7 | Policy evaluation returned access state as ALL...  |
| 2024-06-19 12:55:17 | spouser@spabrl.com | App Access      | Success | 40068d8a-5068-4840-b7a5-7b20594a1cc7 | Show Details                                       |
| 2024-06-19 12:55:17 | spouser@spabrl.com | App Access      | Success | 68d977eb-9f59-4ec7-9ef5-a97bd242c97  | SmartAccess tags received PL_OS_SecureAcc...       |

También puede refinar la búsqueda en función de los siguientes parámetros junto con los operadores del campo de búsqueda.

- User-Name
- Categoría
- Event-Type
- Resultado
- ID de transacción
- Detalles

Los siguientes son los operadores de búsqueda que puede utilizar para refinar la búsqueda en los gráficos Registros de usuarios y Directivas de acceso principales por aplicación de directiva.

- =: Para buscar los registros o directivas que coincidan exactamente con los criterios de búsqueda.
- !=: Para buscar los registros o directivas que no contienen los criterios especificados.
- ~: Para buscar los registros o directivas que coincidan parcialmente con los criterios de búsqueda.
- !~: Para buscar los registros o directivas que no contienen algunos de los criterios especificados.

Por ejemplo, puede buscar un tipo de evento “DSAuth” utilizando la cadena **Event-Type = DSAuth** en el campo de búsqueda.

Del mismo modo, para buscar usuarios que contengan parcialmente el término “operador”, utilice la cadena **User-Name ~ operator**. Esta búsqueda muestra todos los nombres de usuario que contienen el término “operador”. Por ejemplo, “operador local”, “operador administrador”

Puede buscar todos los registros relacionados con un solo evento mediante el ID de transacción. El ID de transacción correlaciona todos los registros de Secure Private Access de una solicitud de acceso.

## Citrix Secure Private Access: local

En una solicitud de acceso a la aplicación se pueden generar varios registros, empezando por la autenticación, la enumeración de la aplicación y, por último, el acceso a la propia aplicación. Todos estos eventos generan sus propios registros. El ID de transacción se utiliza para correlacionar todos estos registros. Puedes filtrar los registros de solución de problemas con el ID de transacción para buscar todos los registros relacionados con una solicitud de acceso a una aplicación en particular.

### Ver etiquetas contextuales de los registros

El enlace **Mostrar detalles** de la columna **Detalles** muestra la lista de aplicaciones asociadas a la directiva de acceso específica y también las etiquetas contextuales asociadas a la directiva.

| TIME                | USER NAME            | CATEGORY   | RESULT  | TRANSACTION ID           | DETAILS                     |
|---------------------|----------------------|------------|---------|--------------------------|-----------------------------|
| 2023-09-07 10:29:13 | spaopdev.local\usera | App Access | Failure | 9c7cde9-0351-43b1-8...   | ERROR: Error in process...  |
| 2023-09-07 10:29:13 | spaopdev.local\usera | App Access | Success | 9c7cde9-0351-43b1-8...   | Show Details                |
| 2023-09-07 10:29:12 | spaopdev.local\usera | App Access | Success | 9c7cde9-0351-43b1-8...   | SmartAccess tags recei...   |
| 2023-09-07 10:29:12 | spaopdev.local\usera | App Access |         |                          | DSAAuth validation was s... |
| 2023-09-07 09:48:50 | spaopdev.local\usera | App Access |         |                          | Successfully generated ...  |
| 2023-09-07 09:48:50 | spaopdev.local\usera | App Access |         |                          | Show Details                |
| 2023-09-07 09:48:49 | spaopdev.local\usera | App Access |         |                          | SmartAccess tags recei...   |
| 2023-09-07 09:48:49 | spaopdev.local\usera | App Access |         |                          | DSAAuth 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... | DSAAuth validation was s... |
| 2023-09-07 09:46:27 | spaopdev.local\usera | App Access | Failure | 6e9d1dd1-5bdb-4474-8...  | ERROR: Error in process...  |

## Solución de errores

February 16, 2024

En este tema se enumeran algunos de los errores que pueden surgir al configurar Secure Private Access.

### Errores de certificado

[de creación de bases de datos Errores](/es-es/citrix-secure-private-access/2308/spa-onprem-troubleshooting#database-creation-errors)

de[StoreFront Errores](/es-es/citrix-secure-private-access/2308/spa-onprem-troubleshooting#storefront-failures)

de puerta de enlace[pública/puerta de enlace de devolución de llamada No se puede acceder al servidor de acceso privado](/es-es/citrix-secure-private-access/2308/spa-onprem-troubleshooting#public-gateway-callback-gateway-failures) seguro

## Errores certificados

**Mensaje de error:** no se pueden obtener los certificados automáticamente de uno o más servidores de Gateway.

**Solución alternativa:** actualice el certificado de gateway de la misma manera que lo haría con Citrix Virtual Apps and Desktops.

## Errores de creación de bases de datos

- **Mensaje de error:** no se pudo crear la base de datos

**Resolución:** en caso automático: la máquina debe tener permisos de LECTURA, ESCRITURA Y ACTUALIZACIÓN para crear tablas en la base de datos del servidor SQL.

- **Mensaje de error:** No se pudo crear la base de datos: ya existe una base de datos.

Este mensaje de error puede aparecer en cualquiera de los escenarios siguientes.

- Si se selecciona la opción **Configuración automática** al configurar las bases de datos.
- Si el administrador está creando una base de datos, debe ser una base de datos vacía. Este mensaje de error puede aparecer si la base de datos no está vacía.

**Solución:** Debe crear una base de datos vacía.

- Desinstala Secure Private Access y vuelve a intentar la configuración con el mismo nombre de sitio. En este caso, la base de datos de la instalación anterior no se habría eliminado.

**Resolución:** debe eliminar manualmente la base de datos.

- Elija configurar la base de datos manualmente (seleccionando Configuración manual en la página Configuración de bases de datos) mediante el script y, a continuación, cambie a la opción Configuración automática pero utilice el mismo nombre de sitio. En este caso, ya se ha creado una base de datos con el mismo nombre mientras se ejecuta el script.

**Solución:** debe cambiar el nombre del sitio y, a continuación, volver a ejecutar el script.

- La máquina no tiene los permisos de LECTURA, ESCRITURA NI ACTUALIZACIÓN para crear tablas en la base de datos del servidor SQL.

**Solución:** habilite los permisos apropiados en la máquina. Para obtener más información, consulte [Permisos necesarios para configurar bases de datos](#).

- **Mensaje de error:** No se pudo crear la base de datos: no se pudo conectar

**Resolución:**

- Compruebe la conectividad de la red de la base de datos desde su máquina. Asegúrese de que el puerto de SQL Server esté abierto en el firewall.
- Si usa un servidor SQL remoto, compruebe si el servidor SQL ha creado un inicio de sesión con la identidad de la máquina de Secure Private Access, Domain\ hostname\$.
- Si usa un servidor SQL remoto, confirme que la identidad de la máquina tenga asignada la función correcta, la función de administrador del sistema.
- Si utiliza un servidor SQL local (no desde el instalador), compruebe si el usuario de NT AUTHORITY\ SYSTEM debe tener un inicio de sesión creado.

## Fallos de StoreFront

- **Mensaje de error:** No se pudo crear una entrada de StoreFront para: <Store URL>

Actualice las entradas de StoreFront desde la ficha **Configuración** si no está visible. Una vez que haya configurado Secure Private Access con el asistente, puede editar las entradas de StoreFront desde la ficha **Configuración**. Anote la URL del almacén de StoreFront en la que se produjo este error.

**Resolución:**

1. Haga clic en **Configuración** y, a continuación, en la ficha **Integraciones**.
2. En la **URL de la tienda** de StoreFront , añada la entrada de StoreFront si no está visible.

- **Mensaje de error:** no se pudo configurar la entrada de StoreFront para: <Store URL>

**Resolución:**

1. Es posible que haya una restricción en la directiva de ejecución de PowerShell. Ejecute el comando de script de PowerShell Get-ExecutionPolicy para obtener más información.
2. Si está restringido, debe omitirlo y ejecutar manualmente un script de configuración de StoreFront.
3. Haga clic en **Configuración** y, a continuación, en la ficha **Integraciones**.
4. En la URL del almacén de **StoreFront**, identifique la entrada URL de StoreFront en la que se produjo el error.
5. Haga clic en el botón **Descargar script** situado junto a la URL de esta tienda y ejecute este script de PowerShell con privilegios de administrador en la máquina en la que se encuentra la instalación de StoreFront correspondiente.

**Nota:**

Si vuelve a intentar la instalación después de la desinstalación, asegúrese de no tener ninguna entrada con el nombre “Secure Private Access” en la configuración de StoreFront (StoreFront> **store**> **Delivery Controller**-> Secure Private Access). Si existe Secure Private Access, elimine esta entrada. Descargue y ejecute manualmente el script desde la página Configuración > Integraciones.

- **Mensaje de error:** la configuración de StoreFront no es local para: <[Store URL](#)>

Una vez que haya configurado Secure Private Access mediante el asistente, puede editar las entradas de la puerta de enlace desde la ficha Configuración . Anote la URL del almacén de StoreFront en la que se produjo este error.

**Resolución:**

Este problema se produce si StoreFront no está instalado en el mismo equipo que Secure Private Access. Debe ejecutar manualmente la configuración de StoreFront en la máquina en la que ha instalado StoreFront.

1. Haga clic en **Configuración** y, a continuación, en la ficha **Integraciones** .
2. En la URL del almacén de **StoreFront**, identifique la entrada URL de StoreFront en la que se produjo el error.
3. Haga clic en el botón Descargar script situado junto a la URL de este almacén y ejecute este script de PowerShell con privilegios de administrador en la máquina en la que esté presente la instalación de StoreFront correspondiente.

**Nota:**

Para ejecutar el script de PowerShell de StoreFront, abra la ventana de PowerShell compatible con Windows x64 con privilegios de administrador y, a continuación, ejecute ConfigureStoreFront.ps1. El script de StoreFront no es compatible con Windows PowerShell (x86).

## Fallos en la puerta de enlace pública/puerta de enlace de devolución de llamada

**Mensaje de error:** No se pudo crear la entrada de puerta de enlace para: <[Gateway URL](#)> O BIEN No se pudo crear la entrada de puerta de enlace de devolución de llamada para: <[Callback Gateway URL](#)>

**Resolución:**

Anote la URL de la puerta de enlace pública o de la puerta de enlace de devolución de llamada en la que se produjo el error. Una vez que haya configurado Secure Private Access mediante el asistente, puede editar las entradas de la puerta de enlace desde la ficha **Configuración** .

1. Haga clic en **Configuración** y, a continuación, en la ficha **Integraciones**.
2. Actualice la dirección de la puerta de enlace pública o la dirección de la puerta de enlace de devolución de llamada y la dirección IP virtual en la que se produjo el error.

### **No se puede acceder al servidor de Secure Private Access**

**Mensaje de error:** no se pudo actualizar el grupo de IIS. No se pudo reiniciar el grupo de IIS

**Resolución:**

1. Vaya a los grupos de aplicaciones de Internet Information Services (IIS) y compruebe que los siguientes grupos de aplicaciones se hayan iniciado y estén en ejecución:
  - Pool de tiempo de ejecución de acceso privado seguro
  - Grupo de administradores de acceso privado seguro

Compruebe también que el sitio predeterminado de IIS "[Default Web Site](#)" esté en funcionamiento.

### **Fallos en la comprobación de conectividad de bases**

**Mensaje de error:** error en la comprobación de conectividad

La comprobación de conectividad de la base de datos puede fallar debido a varios motivos:

- No se puede acceder al servidor de base de datos desde la máquina host del complemento Secure Private Access debido a un firewall.
- Solución:** compruebe si el puerto de la base de datos (el puerto predeterminado 1433) está abierto en el firewall.
- La máquina host del complemento Secure Private Access no tiene permiso para conectarse a la base de datos.

**Solución:** consulte [Permisos de bases de datos SQL para Secure Private Access](#).

### **Falló la comprobación de conectividad de la pasarela. No se puede obtener el certificado público**

**Mensaje de error:** La configuración posterior a la instalación falla con el error “Falló la comprobación de conectividad de la puerta de enlace. No se puede obtener un certificado público...”

**Solución:**

- Cargue el certificado público de la puerta de enlace a la base de datos de Secure Private Access manualmente mediante la herramienta de configuración.
- Abra PowerShell o la ventana de línea de comandos con privilegios de administrador.
- Cambie el directorio a la carpeta Admin\ AdminConfigTool en la carpeta de instalación de Secure Private Access (por ejemplo, cd “C:\Program Files\ Citrix\ Citrix Access Security\ Admin\ AdminConfigTool”)
- Ejecute este comando:  
`.\AdminConfigTool.exe /UPLOAD_PUBLIC_GATEWAY_CERTIFICATE <PublicGatewayUrl> <PublicGatewayCertificatePath>`

## Problemas de autenticación

Es posible que la configuración de autenticación IIS del servicio de ejecución de Secure Private Access no funcione, ya que no se admite la autenticación integrada de Windows (IWA).

## Otros

### Cree un paquete de soporte de diagnóstico de Secure Private Access

Realice los siguientes pasos para crear un paquete de soporte de diagnóstico de Secure Private Access:

- Abra PowerShell o la ventana de línea de comandos con privilegios de administrador.
- Cambie el directorio a la carpeta Admin\ AdminConfigTool en la carpeta de instalación de Secure Private Access (por ejemplo, cd “C:\Program Files\ Citrix\ Citrix Access Security\ Admin\ AdminConfigTool”).
- Ejecute este comando:  
`.\AdminConfigTool.exe /SUPPORTBUNDLE <output folder>`

### Permisos de bases de datos SQL para Secure Private Access

Para la creación automática de bases de datos, la máquina host del complemento Secure Private Access debe tener los permisos para conectarse a la base de datos y crear un esquema de base de datos.

#### Base de datos remota:

Realice los siguientes pasos para configurar los permisos de una base de datos remota.

1. Cree una base de datos vacía con la sintaxis del nombre `CitrixAccessSecurity<Site Name>`. Este `<Site Name>` es el nombre del sitio de Secure Private Access. (por ejemplo, `CitrixAccessSecuritySPA`).

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

2. Cree un inicio de sesión de SQL Server para la identidad de la máquina virtual de Secure Private Access. Por ejemplo, si el nombre de la máquina intermediaria de Secure Private Access es HOST1 y el dominio de la máquina es DOMAIN1, la identidad de la máquina es “`DOMAIN1\HOST1$`”. Si el inicio de sesión ya está creado, puede ignorar este paso.

```
USE CitrixAccessSecurity<SiteName>
```

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

El nombre de dominio se puede encontrar mediante la siguiente consulta:

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

3. Asigne la función `db_owner` a la identidad de la máquina.

```
USE CitrixAccessSecurity<SiteName>
```

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

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

### Base de datos local:

Realice los siguientes pasos para configurar los permisos de una base de datos local.

1. Cree una base de datos vacía con la sintaxis del nombre `CitrixAccessSecurity<Site Name>`. Este `<Site Name>` es el nombre del sitio de Secure Private Access. (por ejemplo, `CitrixAccessSecuritySPA`).

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

2. Cree un inicio de sesión de SQL Server para el usuario `NT AUTHORITY\SYSTEM`. Si el inicio de sesión ya está creado, puede ignorar este paso.

```
USE CitrixAccessSecurity<SiteName>
```

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

3. Asigne la función `db_owner` al usuario “`NT AUTHORITY\ SYSTEM`”.

```
USE CitrixAccessSecurity<SiteName>
```

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

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

Al crear manualmente la base de datos, el script de base de datos descargado agrega los permisos a la identidad de la máquina.

## Desinstalar Secure Private Access

December 27, 2023

Puede desinstalar Secure Private Access desde **Panel de control > Programas > Programas y características.**

1. Seleccione **Citrix Virtual Apps and Desktops 7 2308 —Secure Private Access.**
2. Haga clic en **Desinstalar.**
3. Siga las instrucciones que aparecen en pantalla y complete la desinstalación.

**Nota:**

Si la configuración posterior a la instalación de Secure Private Access ha finalizado, antes de desinstalar Secure Private Access, descargue el archivo StoreFrontScripts.zip de la consola de administración para eliminar el complemento Secure Private Access de la configuración del almacén de StoreFront.

Para descargar el archivo zip de StoreFrontScripts, siga estos pasos:

1. Inicie sesión en la consola de administración de Secure Private Access.
2. Haga clic en **Configuración** y, a continuación, en la ficha **Integraciones**.
3. Haga clic en **Descargar script** en la sección URL del almacén de StoreFront.

### Eliminar el complemento Secure Private Access de la configuración del almacén de StoreFront

Tras desinstalar Secure Private Access, debe eliminar el complemento Secure Private Access de la configuración del almacén de StoreFront.

1. Inicie sesión en la máquina StoreFront.
2. Descargue el archivo StoreFrontScripts.zip.
3. Descomprima StoreFrontScripts.zip en una carpeta.
4. Abra una ventana de PowerShell con los privilegios de administrador.
5. Ejecute este comando:

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

## Compatibilidad de Secure Private Access 2308 con versiones antiguas

February 16, 2024

Secure Private Access 2308 no es compatible con las versiones anteriores (Secure Private Access para V1.0 y V1.5 locales). NetScaler Gateway debe configurarse con el nuevo script, tal como se describió anteriormente en [Configurar NetScaler Gateway](#). No se requiere ninguna configuración en el controlador de entrega de Citrix Virtual Apps and Desktops para Secure Private Access 2308.

La mejor manera de migrar de las versiones antiguas locales de Secure Private Access (1.0 y 1.5) a la 2308 es eliminar lo siguiente:

- Controlador de entrega de Citrix Virtual Apps and Desktops desde aplicaciones web/SaaS
- Actualizar Citrix StoreFront a la configuración predeterminada o crear otro almacén en StoreFront
- NetScaler Gateway

### Limpieza de Citrix Virtual Apps and Desktops Delivery Controller

Las aplicaciones de Secure Private Access creadas en Citrix Virtual Apps and Desktops Delivery Controller se pueden eliminar manualmente o mediante el script de PowerShell.

#### Manual:

1. Abra Citrix Studio o Citrix WebStudio.
2. Haga clic en **Aplicaciones**.
3. Selecciona la aplicación, haga clic con el botón derecho y, a continuación, selecciona **Eliminar**.

#### Uso de un script:

1. Obtenga las aplicaciones actuales de Secure Private Access ejecutando el siguiente comando:

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

Para obtener más información, consulte [Remove-BrokerApplication](#).

2. Después de verificar las aplicaciones, ejecuta el siguiente comando para eliminarlas:

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

### Limpieza de Citrix StoreFront

Puede crear otro almacén de StoreFront o limpiar el almacén existente.

- Crear otro almacén de StoreFront: Debe crear otro almacén de StoreFront para Secure Private Access 2308, ya que los almacenes de StoreFront existentes creados para las versiones anteriores no son compatibles con la 2308. Esta es la opción recomendada para evitar problemas relacionados con la configuración.
- Limpiar un almacén de StoreFront existente: El almacén existente en StoreFront se puede limpiar manualmente o mediante el script. Sin embargo, la mejor opción para migrar Secure Private Access local a 2308 es crear otro almacén en StoreFront.

**Manual:**

1. Busque y elimine policy.json (por ejemplo, C:\inetpub\wwwroot\Citrix\Store\Resources\SecureBrowser\policy.json)
2. Buscar y eliminar las carpetas SecureBrowser (por ejemplo C:\inetpub\wwwroot\Citrix\Store\Resources\SecureBrowser y Resources (por ejemplo C:\inetpub\wwwroot\Citrix\Store\Resources))
3. Elimine el nodo “route”de web.config (lo encontrará en C:\inetpub\wwwroot\Citrix\Store) con el nombre “WebSecurePolicy”y diríjase a la URL “Resources\ SecureBrowser\ policy.json”
4. Reinicie el **sitio web predeterminado en la consola de administrador de Internet Information Service (IIS)** para aplicar los cambios.

**Uso de un script:**

1. Descargue el script desde <https://www.citrix.com/downloads/citrix-secure-private-access/>.
2. Cargue el script en una máquina StoreFront.
3. Ejecute el script como administrador en PowerShell.
4. Introduce el nombre del almacén.

El script elimina la carpeta, la subcarpeta y los archivos C:\inetpub\wwwroot\Citrix\Store\Resources y actualiza el archivo web.config.

5. Reinicie el **sitio web predeterminado en la consola de administrador de Internet Information Service (IIS)** para aplicar los cambios.

## Limpieza de NetScaler Gateway

### Servidor virtual NetScaler Gateway

El servidor virtual NetScaler Gateway creado para las versiones antiguas (1.0 y 1.5) se puede reutilizar para Secure Private Access 2308.

- Para actualizar un NetScaler Gateway existente, consulte [Actualizar un NetScaler Gateway existente].
- Para configurar un nuevo NetScaler Gateway, consulte [Configurar NetScaler Gateway].

## **Directivas y acciones de la sesión**

Secure Private Access 2308 puede reutilizar las directivas y acciones de sesión creadas para las versiones antiguas (1.0 y 1.5).

- Para actualizar las directivas o acciones de una sesión de NetScaler Gateway existente, consulte [Acciones de sesión de NetScaler Gateway](#).
- Para configurar un nuevo NetScaler Gateway, consulte [Configurar NetScaler Gateway](#).

El script también crea directivas y acciones de sesión completamente configuradas.

## **Directivas de autorización**

Las directivas de autorización creadas en NetScaler Gateway para las versiones antiguas (1.0 y 1.5) pueden interferir con las directivas 2308 de Secure Private Access e interrumpir el flujo.

Puede hacer lo siguiente para limpiar las directivas de autorización.

- Desvincula manualmente las directivas de autorización de los grupos de autenticación y autorización que se utilizan como grupos predeterminados en NetScaler Gateway. En este caso, las directivas se pueden reutilizar.
- Elimine las directivas de autorización.

## **Notificaciones de terceros**

December 27, 2023

[Citrix Secure Private Access para entornos locales](#)



© 2024 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at <https://www.cloud.com/legal>. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (<https://www.cloud.com/legal>) for more information.