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

Información técnica general

August 26, 2024

Citrix Secure Private Access local es una solución de acceso a la red de confianza cero (Zero Trust Network Access, ZTNA) administrada por el cliente que proporciona, además de una experiencia perfecta para el usuario final, acceso sin VPN a las aplicaciones web y SaaS internas con lo siguiente:

- Principio de mínimo privilegio
- Single Sign-On (SSO)
- Autenticación de varios factores
- Evaluación de la Device Posture
- Controles de seguridad en el nivel de aplicación
- Funciones de App Protection

La solución aprovecha la aplicación local StoreFront y Citrix Workspace para permitir una experiencia de acceso segura y sin problemas para acceder a las aplicaciones web y de SaaS en Citrix Enterprise Browser. Esta solución también aprovecha NetScaler Gateway para aplicar los controles de autenticación y autorización.

La solución local Citrix Secure Private Access mejora la postura general de seguridad y cumplimiento de una organización al ofrecer fácilmente acceso de red Zero Trust a las aplicaciones basadas en explorador (aplicaciones web y SaaS internas) mediante StoreFront como portal local de acceso unificado a las aplicaciones web y SaaS, junto con aplicaciones y escritorios virtuales como parte integrada de Citrix Workspace.

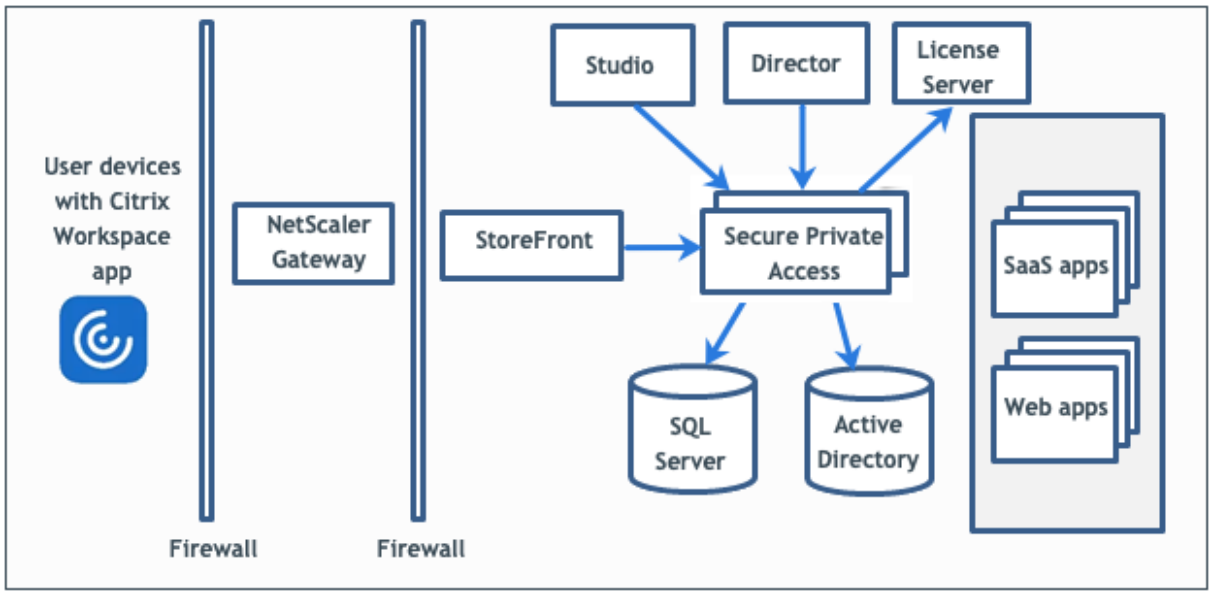
Citrix Secure Private Access combina los elementos de NetScaler Gateway y StoreFront para ofrecer una experiencia integrada a los usuarios finales y a los administradores.

Funcionalidad	Servicio/componente que proporciona la funcionalidad
IU coherente para acceder a las aplicaciones	Aplicación StoreFront On-Premies/Citrix Workspace
SSO a aplicaciones SaaS y web	NetScaler Gateway
Autenticación multifactorial (MFA) y Device Posture (también conocido como análisis de punto final)	NetScaler Gateway
Controles de seguridad y controles de protección de aplicaciones para aplicaciones web y SaaS	Citrix Enterprise Browser
Directivas de autorización	Secure Private Access

Funcionalidad	Servicio/componente que proporciona la funcionalidad
Cumplimiento del acceso	Clientes de NetScaler Gateway y Citrix Secure Access
Configuración y administración	Secure Private Access
Visibilidad, supervisión y solución de problemas	Secure Private Access, NetScaler Console (anteriormente ADM) y Citrix Director

Componentes

Esta ilustración muestra los componentes de una implementación típica de Secure Private Access.



Para obtener información sobre cada componente, consulte Componentes clave.

Novedades

August 26, 2024

Junio de 2024

Restricciones de acceso adicionales para las aplicaciones web internas y SaaS

Ahora hay restricciones de acceso adicionales disponibles para las aplicaciones web internas y SaaS. Los administradores pueden hacer cumplir estas restricciones a través de las directivas de acceso. Para obtener más información, consulta Restricciones de acceso disponibles.

Compatibilidad con sitios web no autorizados

El acceso a sitios web no autorizados ahora es compatible con el complemento Secure Private Access. Las aplicaciones (intranet o Internet) que no están configuradas en Secure Private Access se consideran "sitios web no autorizados". De forma predeterminada, Secure Private Access deniega el acceso a todas las aplicaciones web de la intranet si no hay aplicaciones ni directivas de acceso configuradas para esas aplicaciones. Para obtener más información, consulte Sitios web no autorizados.

Integración del plug-in Citrix Secure Private Access con los servicios SIEM

Citrix Secure Private Access ahora está integrado con la administración de eventos e información de seguridad (SIEM). Para obtener más información, consulte Integración con SIEM.

El nivel de registro de solución de problemas cambió de "Información"a "Error"

El nivel de registro de solución de problemas se cambia de "Información"a "Error"para reducir la carga de la base de datos. Para obtener más información sobre cómo cambiar el nivel de registro, consulte Cambiar el nivel de registro para los registros de solución de problemas.

Problemas resueltos

August 26, 2024

Los siguientes problemas se abordan en la versión 2402.

Configuración del controlador de dominio

El sufijo UPN alternativo no es compatible con la enumeración de aplicaciones de inicio de sesión e Internet/Extranet (puerta de enlace) de Secure Private Access for Intranet (StoreFront).

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).

Inicio de la aplicación

El inicio de la aplicación falla si se cumplen todas las condiciones siguientes:

- Se utilizan las versiones 13.0.x de Netscaler, 13.1 anterior a 13.1-48.47 y 14.1 anterior a 14.1—4.42.
- Los UPN de LDAP se configuran con un sufijo diferente al del dominio real.

Consola de administración

- La página **Editar aplicación** no se cierra automáticamente cuando la página **Editar aplicación** (**Secure Private Access > Aplicaciones > Editar aplicación**) de una aplicación publicada no se cierra después de modificar una entrada de dominio relacionada.

  Por ejemplo, si el dominio relacionado que ingresó al crear una aplicación era `www.example.com`. Una vez publicada la aplicación, sustituyes el dominio relacionado por el dominio `www.example.com`relacionado `abc.com`y haces clic en **Guardar**. La página **Editar aplicación** no se cierra, aunque la aplicación se actualiza correctamente.
- Al agregar una aplicación, si el nombre de la aplicación contiene una coma, se muestra una advertencia. No obstante, se crea la aplicación.
- Si la URL de una aplicación contiene www, la URL se guarda en la tabla de dominios de redirección (**Parámetros > Dominio de la aplicación**) sin el prefijo www.

Actualizaciones

Si se utiliza un certificado SSL personalizado para el servicio de administración de Secure Private Access, el certificado debe volver a vincularse al sitio "Citrix Access Security Admin"en Internet Information Service (IIS).

Problemas conocidos

August 26, 2024

Existen los siguientes problemas en la versión 2402.

Configuraciones del controlador de dominio

- No se admite la confianza unidireccional o bidireccional con el tipo de confianza "Bosque"entre dominios de diferentes bosques de AD.

  Por ejemplo, si los dominios.com y b.com se encuentran en dos bosques de AD diferentes y SPA está instalado en una máquina en la que el dominio está unido a a.com/b.com, los demás usuarios del dominio no podrán acceder a las aplicaciones publicadas en SPA.

- Si el dominio de la máquina en el que está instalado Secure Private Access for on-premise es diferente al dominio del administrador que inició sesión en Secure Private Access, debe hacer lo siguiente:

  Agregue una cuenta de servicio de dominio diferente como identidad en el grupo de aplicaciones de IIS para el servicio de administración y ejecución de Secure Private Access.

- Los grupos de distribución no son compatibles con Secure Private Access. Por lo tanto, las directivas no pueden buscar grupos de distribución para agregar condiciones de usuario y grupo.

- Secure Private Access no captura los detalles del dominio en la consola de administración o el servicio. Por lo tanto, depende completamente del dominio que proporcionó el usuario. Por lo tanto, si no se puede acceder al dominio correspondiente o si el nombre de dominio no es un nombre válido, ese dominio no es compatible.

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 inhabilite 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

RFWeb/Workspace para web no es compatible y, por lo tanto, las aplicaciones no se enumeran. Para obtener más información, consulte Cuando se usa la versión 2311 o posterior de StoreFront.

Inicio de la aplicación

El inicio de la aplicación falla si LDAP UPN y sAMAccountName son diferentes.

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. Para obtener información sobre la configuración de StoreFront, consulte StoreFront.
- Si utiliza las versiones 2308 o anteriores de StoreFront, la página **Almacenes > Administrar Delivery Controllers** muestra el tipo de plug-in 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.

El instalador aparece en la página Desinstalar o cambiar un programa

Al actualizar Secure Private Access de versiones anteriores a la 2405 mediante el archivo ISO, la página **Desinstalar o cambiar un programa** (**Panel de control > Programas > Programas y características**) muestra dos entradas para el instalador de Secure Private Access en lugar de reemplazar la entrada inicial.

Solución alternativa: desinstale el instalador de compilación anterior.

> **Nota:**
>
> Este problema no se observa cuando el instalador independiente de Secure Private Access se actualiza con el instalador independiente 2402.

Actualizar

- Después de actualizar a 2405 y editar una aplicación existente cuya URL comience por www, el campo **Conectividad de la aplicación** no rellena el estado anterior. Debes volver a seleccionar

el tipo de conectividad de la aplicación. Se trata de una acción que se realiza una sola vez después de la actualización, tras la cual la configuración se guarda y persiste.

- Tras actualizar a la versión 2405, aunque puede iniciar sesión en la consola de administración, no puede administrar las aplicaciones ni las directivas. Aparece un mensaje de error.

  Solución alternativa: Debe actualizar la base de datos mediante los scripts. Para obtener más información, consulte Actualizar la base de datos mediante scripts.

- Tras la actualización a la 2405, se produce un error en la enumeración y el inicio de la aplicación.

  Solución alternativa: Debe actualizar la base de datos mediante los scripts. Para obtener más información, consulte Actualizar la base de datos mediante scripts.

- No puede actualizar el plug-in Secure Private Access de la versión 2402 a la 2405 si el plug-in 2402 se instaló mediante el Delivery Controller.

Requisitos del sistema

August 26, 2024

Asegúrese de que su producto cumpla con los requisitos mínimos de versión.

- Aplicación Citrix Workspace
  - Windows: 2403 y versiones posteriores
  - macOS: 2402 y versiones posteriores
- Sistema operativo para el servidor de complementos Secure Private Access: Windows Server 2019 y versiones posteriores
- StoreFront: LTSR 2203 o CR 2212 y versiones posteriores
- NetScaler: 13.0, 13.1, 14.1 y versiones posteriores. Se recomienda utilizar las versiones más recientes de la versión 13.1 o 14.1 de NetScaler Gateway para optimizar el rendimiento.
- Director 2402 o posterior
- Puertos de comunicación: asegúrese de haber abierto los puertos necesarios para el plug-in Secure Private Access. Para obtener más información, consulte Puertos de comunicación.

> **Nota:**
>
> Secure Private Access para entornos locales no se admite en la aplicación Citrix Workspace para iOS y Android.

Requisitos previos

Para crear o actualizar un NetScaler Gateway existente, asegúrese de tener los siguientes detalles:

- Un servidor Windows con IIS en ejecución, configurado con un certificado SSL/TLS, en el que se instalará el plug-in Secure Private Access.
- URL de almacenamiento de StoreFront que se deben introducir durante la configuración.
- El almacén de StoreFront debe estar configurado y la URL del servicio de almacén debe estar disponible. El formato de la URL del servicio de almacén es `https://store.domain.com/Citrix/StoreSecureAccess`.
- Dirección IP de NetScaler Gateway, FQDN y URL de devolución de llamada de NetScaler Gateway.
- Dirección IP y FQDN de la máquina host del plug-in Secure Private Access (o un balanceador de carga si el plug-in Secure Private Access se implementa como un clúster).
- Nombre del perfil de autenticación configurado en NetScaler.
- Certificado de servidor SSL configurado en NetScaler.
- Nombre de dominio.
- Las configuraciones de los certificados están completas. Los administradores deben asegurarse de que las configuraciones de los certificados estén completas. El instalador de Secure Private Access configura un certificado autofirmado si no se encuentra ningún certificado en la máquina. Sin embargo, es posible que esto no siempre funcione.

> **Nota:**
>
> El servicio Runtime (aplicación SecureAccess en el sitio web predeterminado de IIS) requiere que la autenticación anónima esté habilitada, ya que no admite la autenticación de Windows. Esta configuración la establece el instalador de Secure Private Access de forma predeterminada y no se debe cambiar manualmente.

Requisitos de la cuenta de administrador

Se requieren las siguientes cuentas de administrador para configurar Secure Private Access.

- Instale Secure Private Access: debe iniciar sesión con una cuenta de administrador de la máquina local.
- Configurar el Secure Private Access: debe iniciar sesión en la consola de administración de Secure Private Access con un usuario de dominio que también sea el administrador local de la máquina en la que está instalado Secure Private Access.
- Administrar el Secure Private Access: debe iniciar sesión en la consola de administración de Secure Private Access con una cuenta de administrador de Secure Private Access.

Puertos de comunicación

En la siguiente tabla se enumeran los puertos de comunicación que utiliza el plug-in Secure Private Access.

Origen	Destino	Tipo	Puerto	Detalles
Estación de trabajo de administración	Plug-in Secure Private Access	HTTPS	4443	Plug-in Secure Private Access - Consola de administración
Plug-in Secure Private Access	Servicio NTP	TCP, UDP	123	Sincronización horaria
	Servicio de DNS	TCP, UDP	53	Búsqueda de DNS
	Active Directory	TCP, UDP	88	Kerberos
	Director	HTTP, HTTPS	80, 443	Comunicación con Director para la administración del rendimiento y la mejora de la solución de problemas
	Servidor de licencias	TCP	8083	Comunicación con el servidor de licencias para recopilar y procesar datos de licencias
		TCP	389	LDAP sobre texto plano (LDAP)
		TCP	636	LDAP sobre SSL (LDAPS)
	Microsoft SQL Server	TCP	1433	Plug-in Secure Private Access: comunicación con bases de datos
	StoreFront	HTTPS	443	Validación de autenticación

Origen	Destino	Tipo	Puerto	Detalles
	NetScaler Gateway	HTTPS	443	Retrollamada de NetScaler Gateway
StoreFront	Servicio NTP	TCP, UDP	123	Sincronización horaria
	Servicio de DNS	TCP, UDP	53	Búsqueda de DNS
	Active Directory	TCP, UDP	88	Kerberos
		TCP	389	LDAP sobre texto plano (LDAP)
		TCP	636	LDAP sobre SSL (LDAPS)
		TCP, UDP	464	Protocolo de autenticación nativo de Windows para permitir a los usuarios cambiar contraseñas caducadas
	Plug-in Secure Private Access	HTTPS	443	Autenticación y enumeración de aplicaciones
	NetScaler Gateway	HTTPS	443	Retrollamada de NetScaler Gateway
NetScaler Gateway	Plug-in Secure Private Access	HTTPS	443	Validación de autorización de aplicaciones
	StoreFront	HTTPS	443	Autenticación y enumeración de aplicaciones

Origen	Destino	Tipo	Puerto	Detalles
	Aplicaciones web	HTTP, HTTPS	80, 443	Comunicación de NetScaler Gateway con aplicaciones de Secure Private Access configuradas *(los puertos pueden diferir según los requisitos de la*aplicación)
Dispositivo de usuario	NetScaler Gateway	HTTPS	443	Comunicación entre el dispositivo del usuario final y NetScaler Gateway

Referencias

- Perfiles de autenticación.
- Cómo funcionan las directivas de autenticación.
- Enlazar un certificado SSL a un servidor virtual (SSL) en NetScaler.

Pautas de tallas

August 26, 2024

Requisitos de almacenamiento de bases de datos

Los registros consumen la mayor parte del almacenamiento de la base de datos. El consumo de espacio de almacenamiento de la configuración de directivas y aplicaciones es insignificante en comparación con los registros.

La siguiente figura muestra los requisitos de almacenamiento del servidor:

Number of users	Number of Secure Private Access server nodes	Secure Private Access node configuration			SQL Server (Secure Private Access Database only)			Active Directory		StoreFront	
		CPU	Memory (GB)	Storage (GB)	CPU	Memory (GB)	Storage (GB)	CPU	Memory (GB)	CPU	Memory (GB)
1000	3	8	16	80	4	16	250	4	16	4	16
5000	8	8	16	80	16	16	750	16	16	4	16

Nota:

- Las métricas se derivan partiendo del supuesto de que la limpieza de eventos del registro está inhabilitada y el período de retención del registro está establecido en 7 días.
- De forma predeterminada, los registros se conservan durante 90 días o se conservan hasta 100 000 eventos de registro, según los ajustes configurados. Estos ajustes están disponibles en el archivo appsettings.json del servicio Secure Private Access Runtime y se pueden modificar según sea necesario. Para obtener más información, consulte Parámetros para conservar los registros de eventos.

Configuración del servidor

En la siguiente tabla se muestran los detalles de configuración del servidor:

Configuración	Detalles
Número total de solicitudes	250
Número total de directivas	50
Número de aplicaciones por usuario	15
Configuración de AD	Los usuarios forman parte de 20 grupos, con hasta 20 niveles de anidación
Solución de problemas del período de retención de registros	7 días (predeterminado)
Nivel de registro de solución de problemas	Error (predeterminado)
Retención de registros del servidor de Secure Private Access	90 días o 600 archivos

Perfil de tráfico

En la siguiente tabla se muestran los detalles del perfil de tráfico por día y usuario.

Perfil	Detalles
Enumeraciones	10
Sincronización de directivas de exploradores empresariales	20
Inicio de la aplicación desde la aplicación Citrix Workspace	4
Acceso a aplicaciones desde Citrix Enterprise Browser	500
Solicitudes de solución de problemas del servicio de asistencia (por día), a través de Citrix Director	1000

Pautas de implementación

En la siguiente tabla, se muestran los requisitos de tamaño de la base de datos en función de parámetros como las sesiones de usuario de acceso simultáneo a las aplicaciones, la enumeración de aplicaciones por minuto y las CPU utilizadas por Secure Private Access:

Sesiones de usuario de acceso simultáneo a la aplicación	Enumeración de aplicaciones por minuto	Memoria de Secure Private Access en GB	CPU de Secure Private Access	Almacenamiento en GB	Notas
< 20 (para fines PoC)	2	4 GB	2	40 GB*	Para fines de PoC, SPA se puede implementar en la misma máquina que StoreFront sin ningún cambio en las especificaciones de las máquinas virtuales existentes.

Sesiones de usuario de acceso simultáneo a la aplicación	Enumeración de aplicaciones por minuto	Memoria de Secure Private Access en GB	CPU de Secure Private Access	Almacenamiento en GB	Notas
20	5	8 GB	4	60 GB	-
160**	18	16 GB	4***	60 GB	Se pueden implementar 2 o más nodos SPA para un mejor rendimiento

Nota:

- * El almacenamiento lo consumen principalmente los registros CDF. De forma predeterminada, Secure Private Access conserva 600 archivos de registro acumulados, cada uno de los cuales tiene un tamaño de 10 MB. Por lo tanto, si los servicios de administración y ejecución de Secure Private Access se ejecutan en la misma máquina, la utilización máxima de almacenamiento por parte de los registros es de 12 GB. Además, SQL express se puede instalar en la máquina virtual local con fines de PoC.
- ** Para este perfil de carga y superior, se recomienda implementar Secure Private Access en un servidor dedicado en lugar de hospedarlo conjuntamente con StoreFront, a menos que la versión de NetScaler Gateway sea inferior a la 13.0 o inferior a la 13.1-48.47.
- *** Se recomienda utilizar al menos 2 clústeres de nodos de Secure Private Access para dicha carga, ya que existen algunos problemas de rendimiento conocidos. Está previsto que estos problemas se aborden en las próximas versiones.

Configuración de otros componentes

Componente	vCPU	Memoria
Plug-in Secure Private Access	8	16 GB
Servidor SQL de Secure Private Access	8	16 GB
StoreFront	16	8 GB
Gateway	4	8 GB

Componente	vCPU	Memoria
Active Directory	8	14 GB
Cliente	4	8 GB

Instalación y configuración

August 26, 2024

El instalador de Secure Private Access está disponible como instalador independiente o como parte del instalador integrado de Citrix Virtual Apps and Desktops. Para obtener más información, consulte Instalación de componentes principales o Instalación desde la línea de comandos.

Una vez finalizada la instalación, la consola de administración de la configuración inicial se abre automáticamente en la ventana predeterminada del explorador. Puede hacer clic en **Continuar** para configurar Secure Private Access. También puede ver el acceso directo a Secure Private Access en el menú Inicio del escritorio (**Citrix > Citrix Secure Private Access**).

Requisitos de la cuenta de administrador para instalar y administrar Secure Private Access

- Para instalar Secure Private Access, debe iniciar sesión con una cuenta de administrador de la máquina local.
- Para configurar Secure Private Access, debe iniciar sesión en la consola de administración de Secure Private Access con un usuario de dominio que también sea el administrador local de la máquina en la que está instalado Secure Private Access.
- Una vez finalizada la configuración, ese usuario se convierte en el primer administrador de Secure Private Access y después puede agregar a otros administradores.
- Para administrar Secure Private Access después de la configuración, debe iniciar sesión en la consola de administración de Secure Private Access con una cuenta de administrador de Secure Private Access.

Configurar Secure Private Access

Para configurar el Secure Private Access, siga estos pasos:

- Configurar el Secure Private Access creando un sitio nuevo o Configurar el Secure Private Access uniéndose a un sitio existente

- Configurar bases de datos
- Integre StoreFront, NetScaler Gateway, Director y servidores de licencias

Configurar aplicaciones y directivas de acceso

Después de configurar el entorno de Secure Private Access, debe configurar las aplicaciones y las directivas de acceso para las aplicaciones.

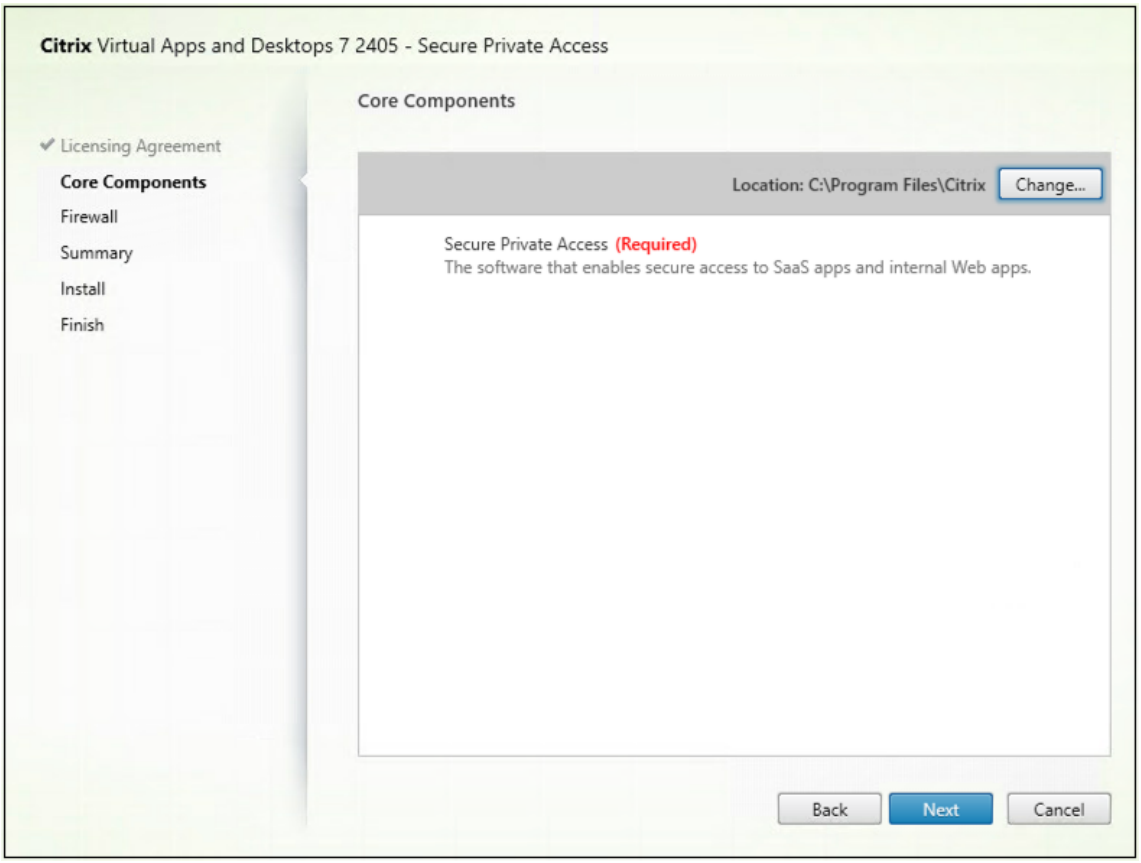
- Configurar aplicaciones
- Configurar directivas de acceso para las aplicaciones

Instalador de Secure Private Access

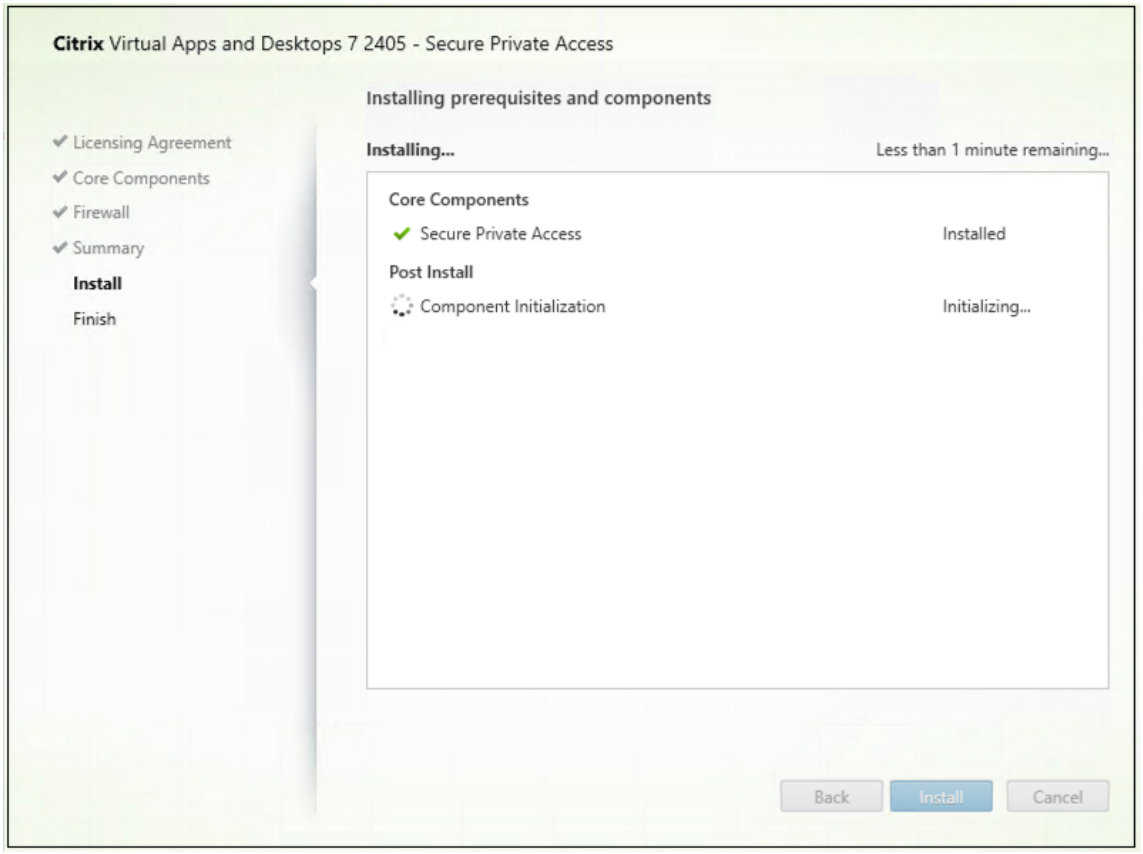
August 26, 2024

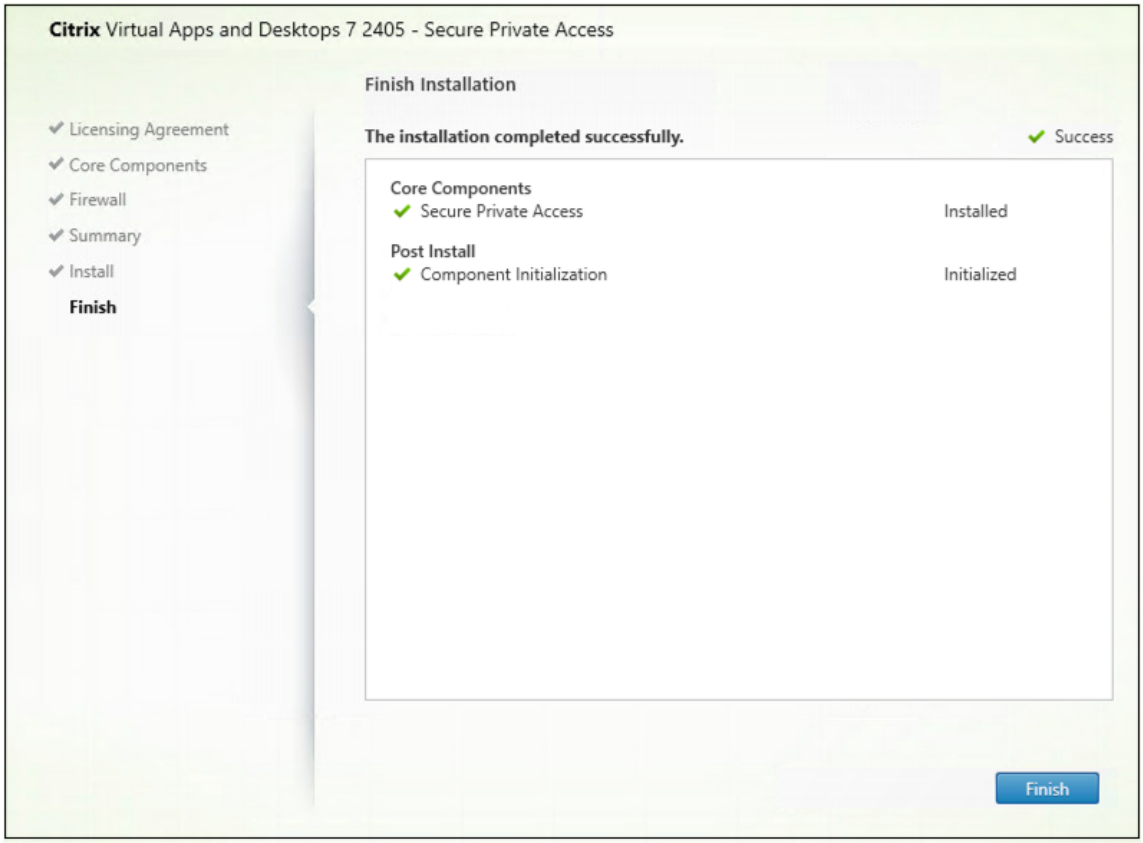
1. Descargue el instalador de Citrix Secure Private Access desde https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/.
2. Ejecute el archivo .exe como administrador en una máquina unida a un dominio.

> **Nota:**
>
> Para fines de POC, se recomienda instalar Secure Private Access en la misma máquina en la que está instalado StoreFront.

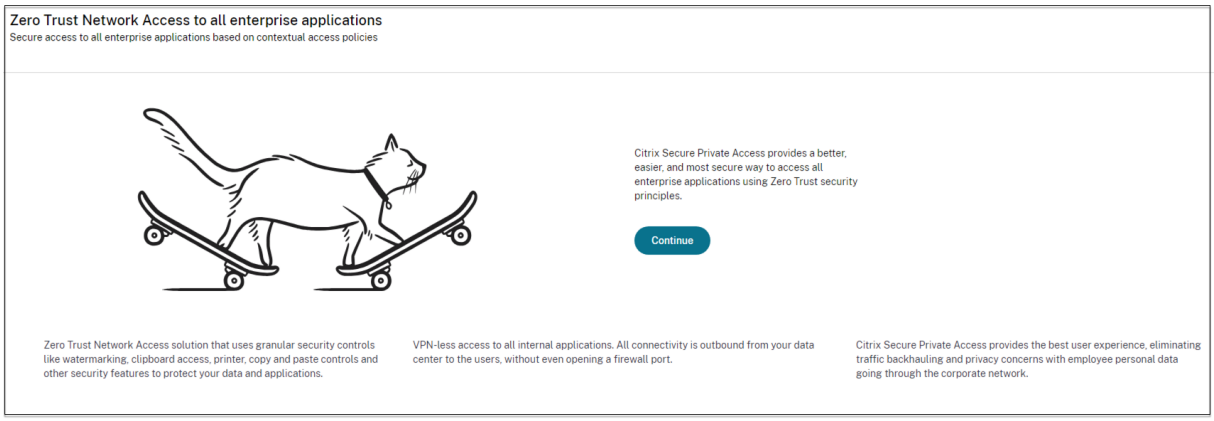


3. Siga las instrucciones que aparecen en pantalla para completar la instalación.

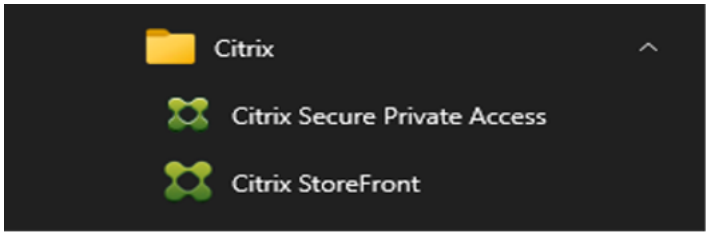




Una vez finalizada la instalación, la consola de administración de la configuración inicial se abre automáticamente en la ventana predeterminada del explorador. Puede hacer clic en **Continuar** para configurar Secure Private Access.



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



Para obtener más información, consulte estos temas:

- Instalar componentes principales
- Instalación desde la línea de comandos

SSO a la consola de administración

Se recomienda configurar la autenticación Kerberos para el explorador 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 explorador le pedirá que introduzca sus credenciales al acceder a la consola de administración de Secure Private Access.

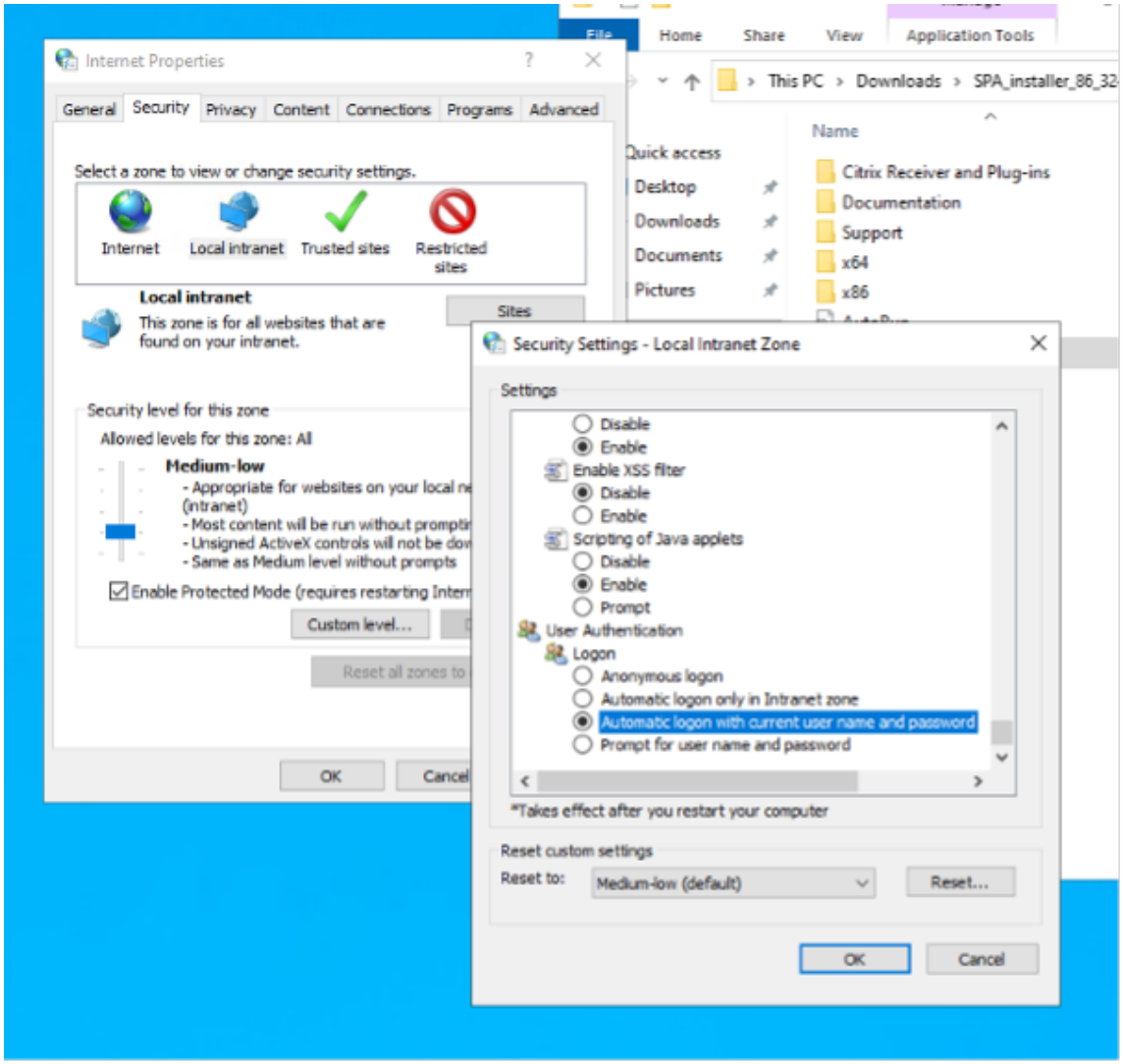
- Si introduce sus credenciales, habilita el inicio de sesión de la Autenticación integrada de Windows (IWA).
- Si no introduce sus credenciales, aparecerá la página de inicio de sesión de Secure Private Access.

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, si el usuario tiene privilegios de administrador local en la máquina de instalación.

Para los exploradores 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"`.
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 uss sesiones de incógnito de Chrome, cree una clave de registro DWORD Computer\HKEY_LOCAL_MACHINE y asígnele 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 exploradores, consulte la documentación del explorador específico sobre la autenticación Kerberos.

Siguientes pasos

- Configurar Secure Private Access
- Configurar NetScaler Gateway
- Configurar aplicaciones

- Configurar directivas de acceso para las aplicaciones

Configurar Secure Private Access

August 26, 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

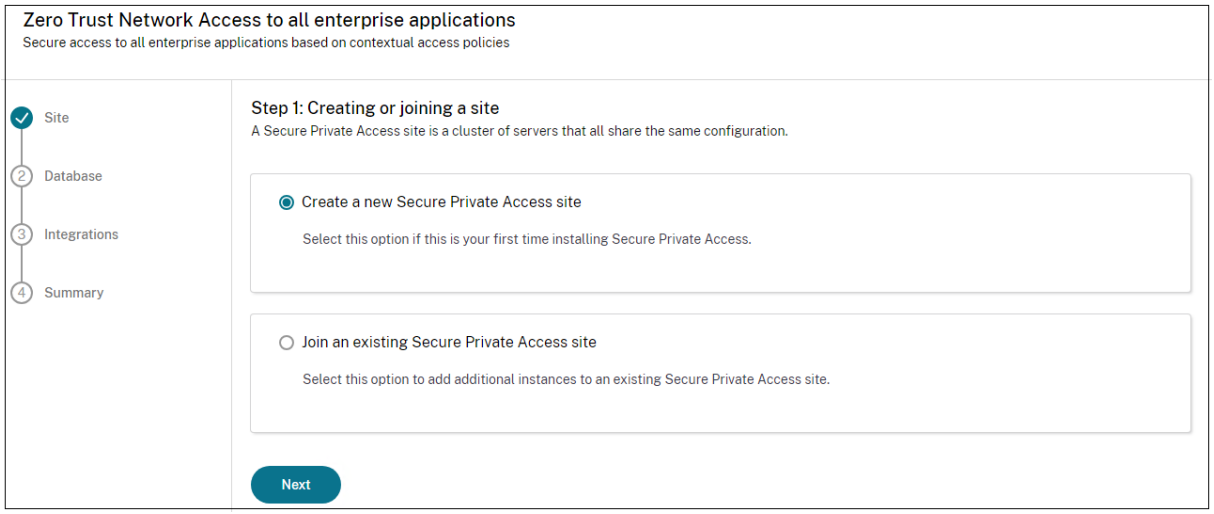
- Debe iniciar sesión en la consola de administración de Secure Private Access con un usuario de dominio que también sea el administrador local de la máquina en la que está instalado Secure Private Access.
- El servidor de base de datos SQL debe estar instalado antes de crear un sitio.

Configure Secure Private Access mediante la creación de un nuevo sitio

Paso 1: Configurar un sitio de Secure Private Access

Un sitio es el nombre de la implementación de Secure Private Access. Puede 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 automática 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.

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:

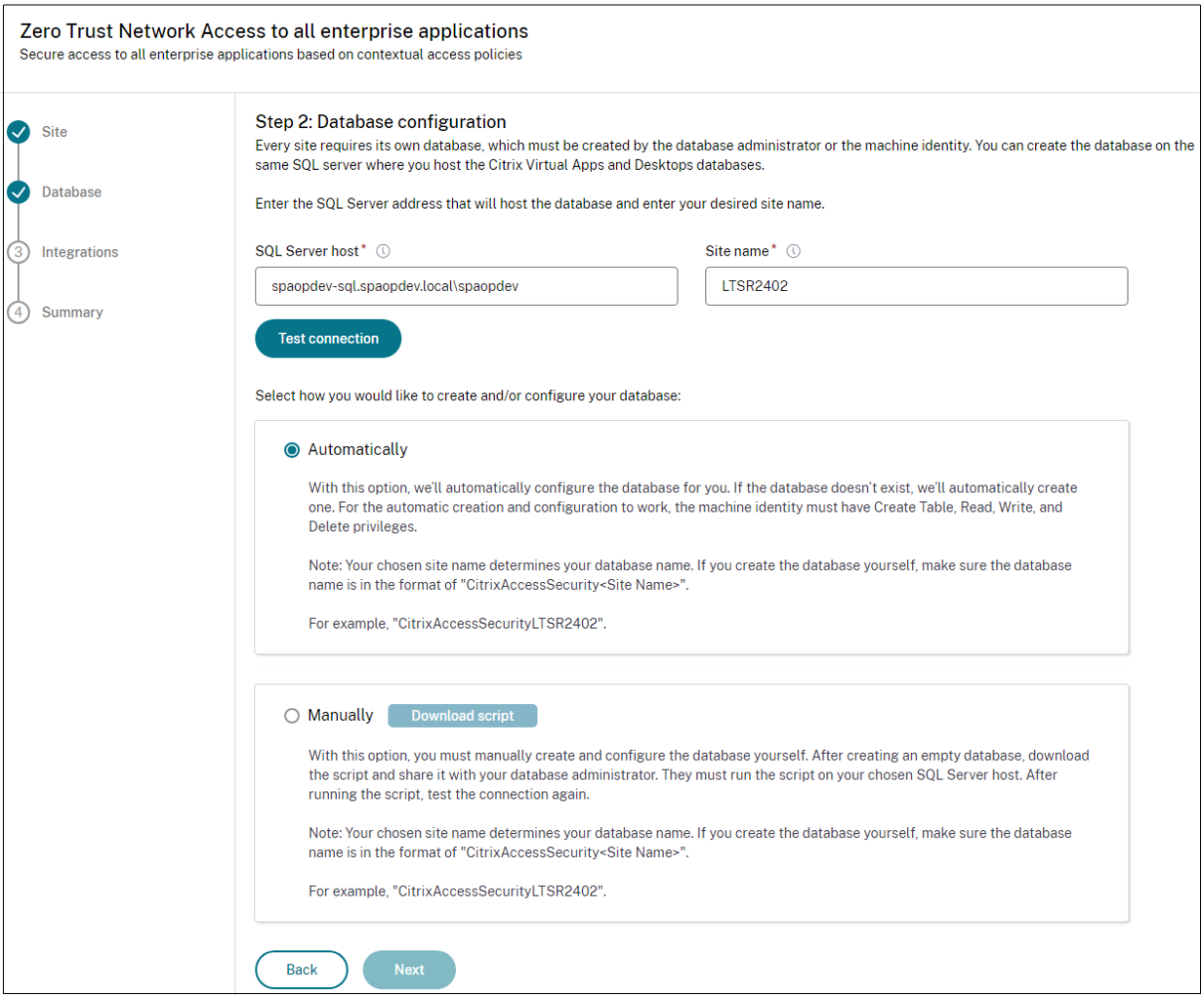
   - NombreServidor
   - NombreServidor\NombreInstancia
   - NombreServidor,NúmeroPuerto

   Para obtener más información, consulte Bases de datos.

2. En **Sitio**, escriba un nombre para el sitio de Secure Private Access.

   > **Nota:**
   >
   > El nombre del sitio que introduzca tiene el sufijo del nombre de la base de datos. El formato del nombre de la base de datos es `CitrixAccessSecurity<sitename>` y no se puede modificar. Si necesita personalizar el nombre de la base de datos, contacte con Citrix Support.

3. Haga clic en **Probar conexión** para comprobar que la instancia de SQL Server es válida y también para confirmar que la base de datos especificada existe para el sitio.



> **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.

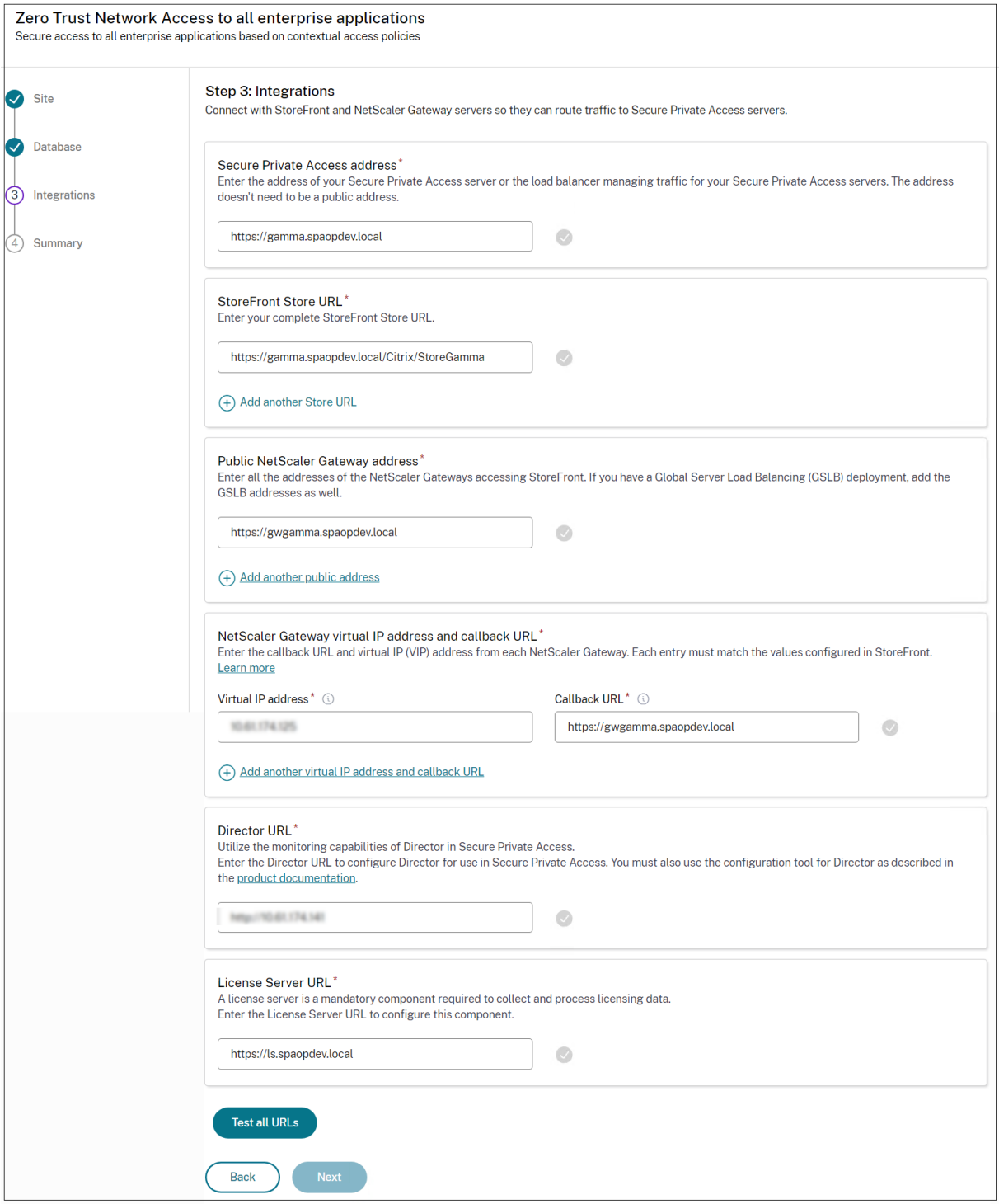
En la configuración manual, primero debe descargar los scripts y después ejecutarlos en el servidor de base de datos que haya especificado en el campo **Host de SQL Server**.

> **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 servidores

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. También debe especificar los detalles del servidor de Director y del servidor de licencias.

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 pública de NetScaler Gateway**: URL del NetScaler Gateway. Por ejemplo, `https://gateway.domain.com`.
    - **Dirección IP virtual**: esta dirección IP virtual debe ser la misma que la configurada en StoreFront para las devoluciones de llamadas.
    - **URL de devolución de llamada**: esta URL debe ser la misma que la configurada en StoreFront. Por ejemplo, `https://gateway.domain.com`.
    - **URL de Director:** - (Opcional) La dirección IP o el FQDN del servidor de Director para conectar Secure Private Access con Citrix Director.
    - **URL del servidor de licencias:** - La dirección IP del servidor de licencias para recopilar y procesar los datos de licencias.
2. Haga clic en **Validar todas las URL**
3. Haga clic en **Siguiente** y después seleccione **Guardar**.

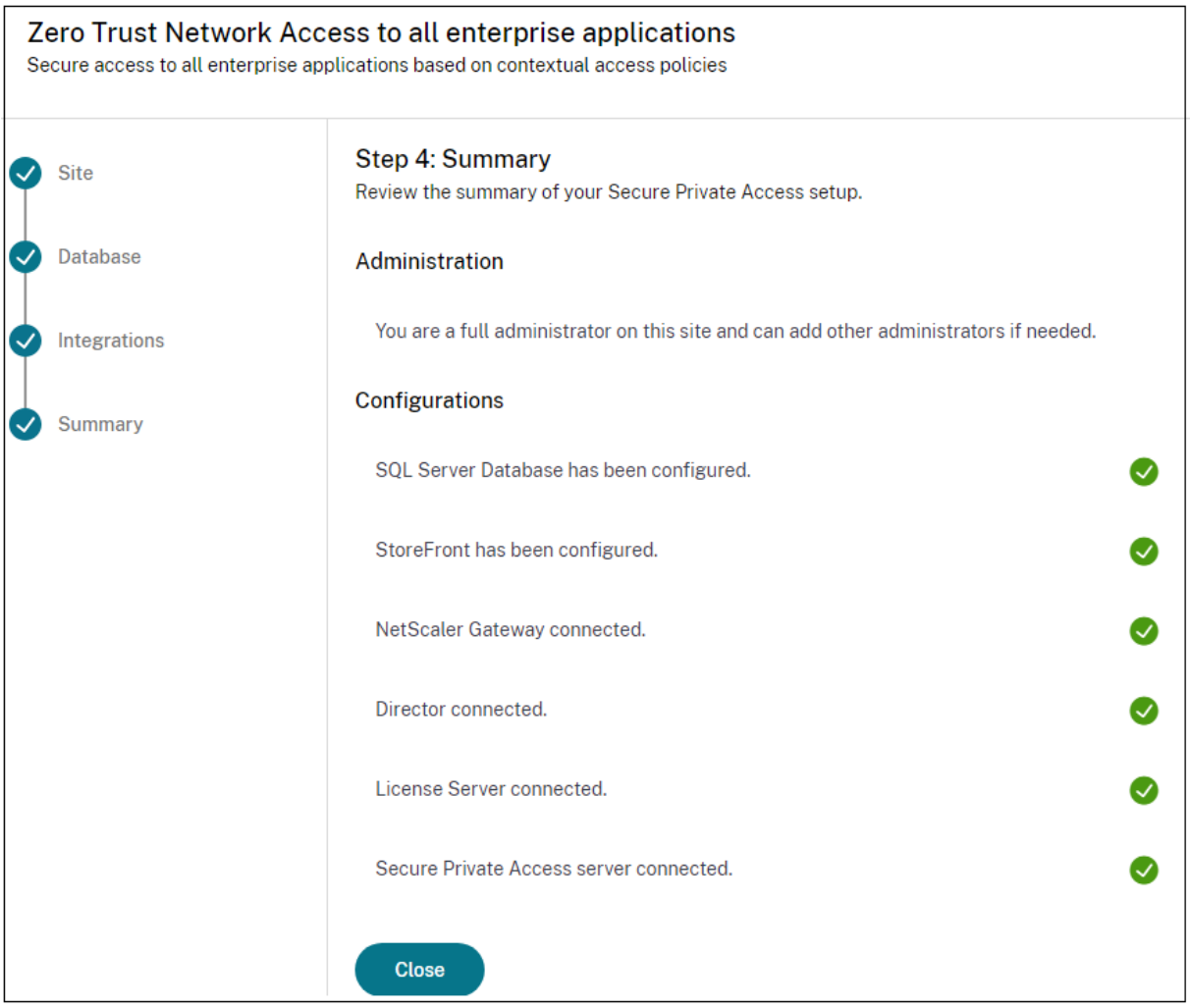


Paso 4: Resumen de la configuración

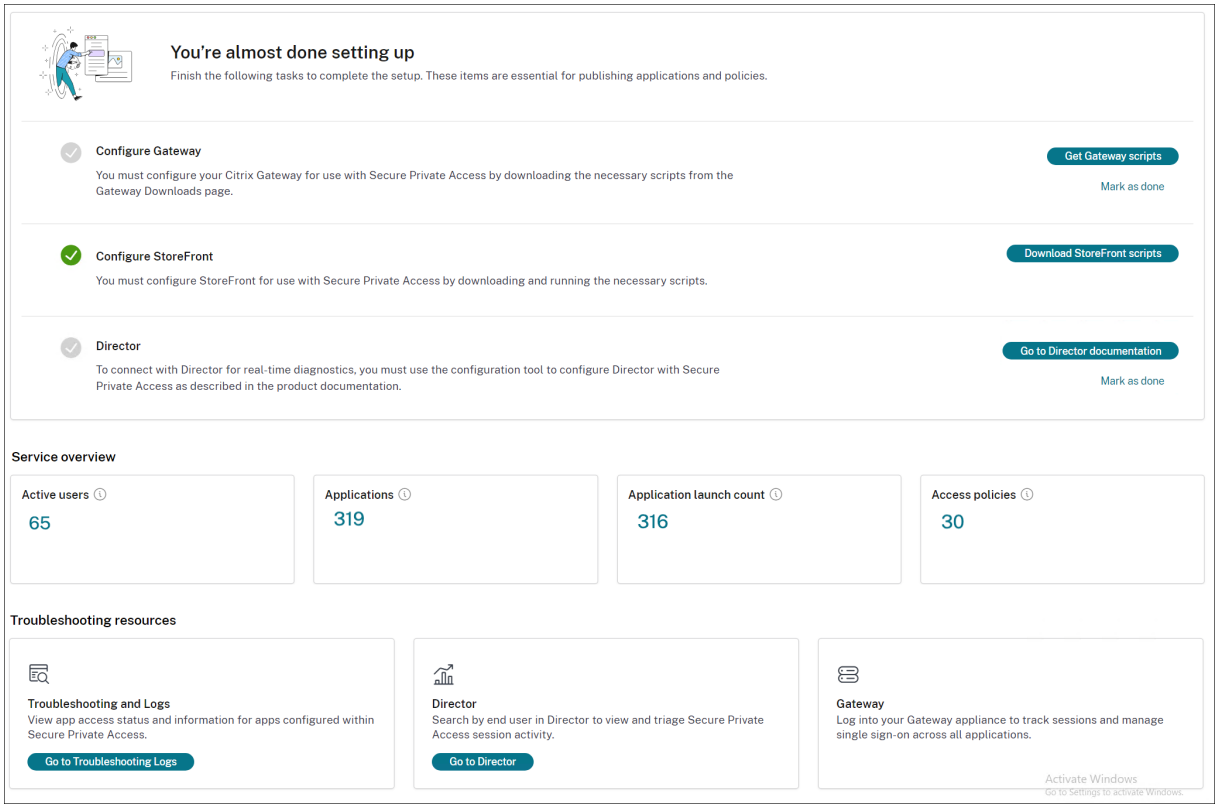
Una vez finalizada la configuración, se realiza la validación para garantizar que se pueda acceder a los servidores configurados. Además, se realiza una comprobación para garantizar que se pueda acceder

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, contacte con Citrix Support.



Una vez finalizada la configuración, aparece la siguiente página al hacer clic en **Cerrar** en la página **Resumen**.



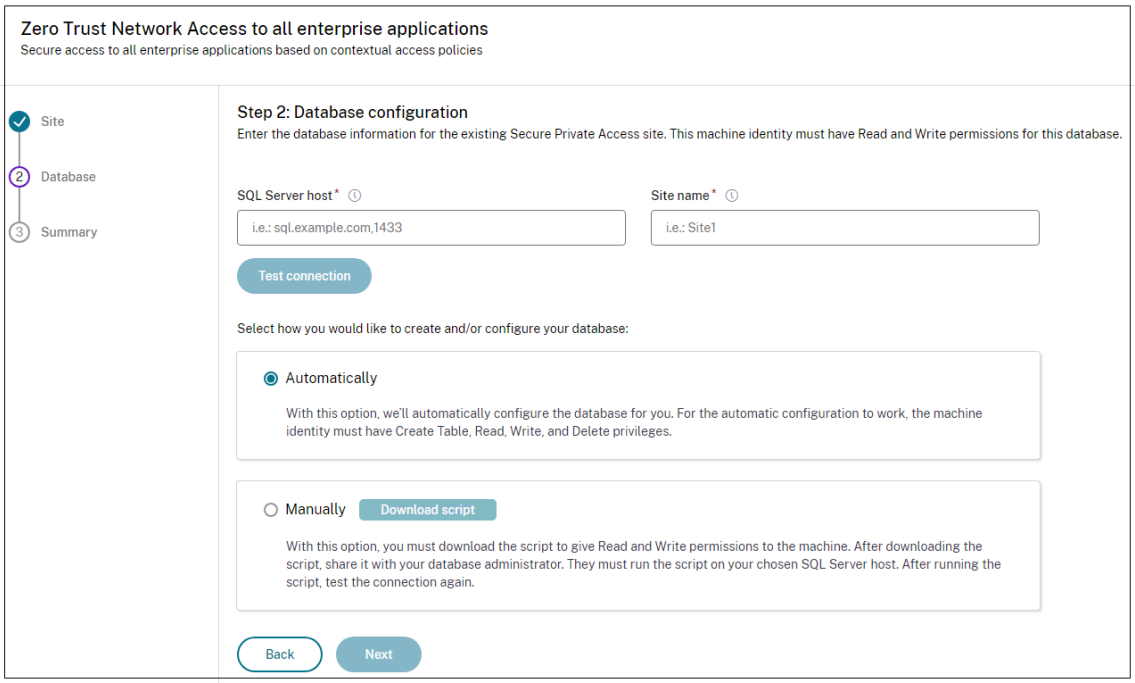
Nota:

- Después de configurar el entorno, puede modificar la configuración en **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 **Parámetros > 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**y, a continuación, haga clic en **Siguiente**.



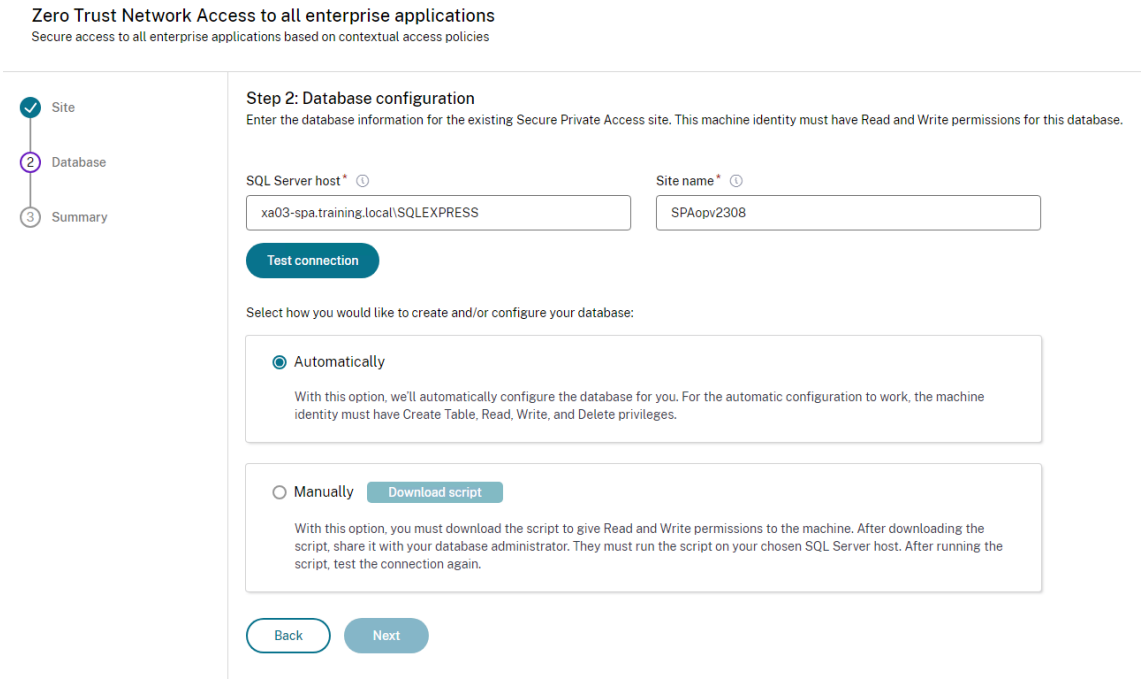
2. En **SQL Server Host**, introduzca el nombre del host del servidor. Asegúrese de que la base de datos correspondiente al nombre del sitio que introduzca ya esté presente en el servidor SQL que ha seleccionado. Puede especificar una dirección de base de datos de una de las siguientes formas:

   - 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 conexión** para comprobar que la instancia de SQL Server es válida y también para confirmar que el sitio especificado existe en la base de datos.



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

5. Haga clic en **Save**.

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.

Siguientes pasos

- Configurar NetScaler Gateway
- Configurar aplicaciones
- Configurar directivas de acceso para las aplicaciones

Componentes

August 26, 2024

Los siguientes son los componentes clave de un Secure Private Access típico para una implementación local.

- **StoreFront**: - StoreFront autentica a los usuarios y administra los almacenes de escritorios y aplicaciones a los que acceden los usuarios. Puede alojar el almacén de las aplicaciones de su empresa, lo que da a los usuarios acceso cada vez que quieran a los escritorios y las aplicaciones que quiera poner a su disposición. También realiza un rastreo de las suscripciones de aplicaciones que tengan los usuarios, los nombres de los accesos directos y otros datos. Gracias a ello, los usuarios tienen una experiencia similar, aunque utilicen varios dispositivos. Para obtener más información sobre la integración de StoreFront con Secure Private Access, consulte StoreFront.
- **NetScaler Gateway:** - NetScaler Gateway proporciona un único punto de acceso seguro a través del firewall corporativo. Para obtener más información sobre la integración de NetScaler Gateway con Secure Private Access, consulte NetScaler Gateway.
- **Director:** (opcional) Director le permite supervisar el rendimiento y solucionar problemas de forma eficaz. Para integrar Director con Secure Private Access, debe introducir la dirección IP del FQDN del servidor de Director que debe estar registrado en Secure Private Access. Para obtener más información sobre la integración de Director con Secure Private Access, consulte Integración de Secure Private Access con Director.
- **Servidor de licencias:** el servidor de licencias recopila y procesa los datos de licencias. Para obtener más información sobre la integración del servidor de licencias con Secure Private Access, consulte Integración del servidor de licencias con Secure Private Access.
- **Web Studio:** Citrix Secure Private Access está integrado en la consola de Web Studio para que los usuarios puedan acceder sin problemas al servicio a través de Web Studio. Para obtener más información sobre la integración de Secure Private Access con Web Studio, consulte Integración de Secure Private Access con Web Studio.

> **Nota:**
>
> Director y el servidor de licencias se integran con Secure Private Access a partir de la versión 2402.

NetScaler Gateway

August 26, 2024

> **Importante:**
>
> Se recomienda crear instantáneas de NetScaler o guardar la configuración de NetScaler antes de aplicar estos cambios.

1. Descargue el script desde https://www.citrix.com/downloads/citrix-secure-private-access/Shell-Script/Shell-Script-for-Gateway-Configuration.html.

   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*`.

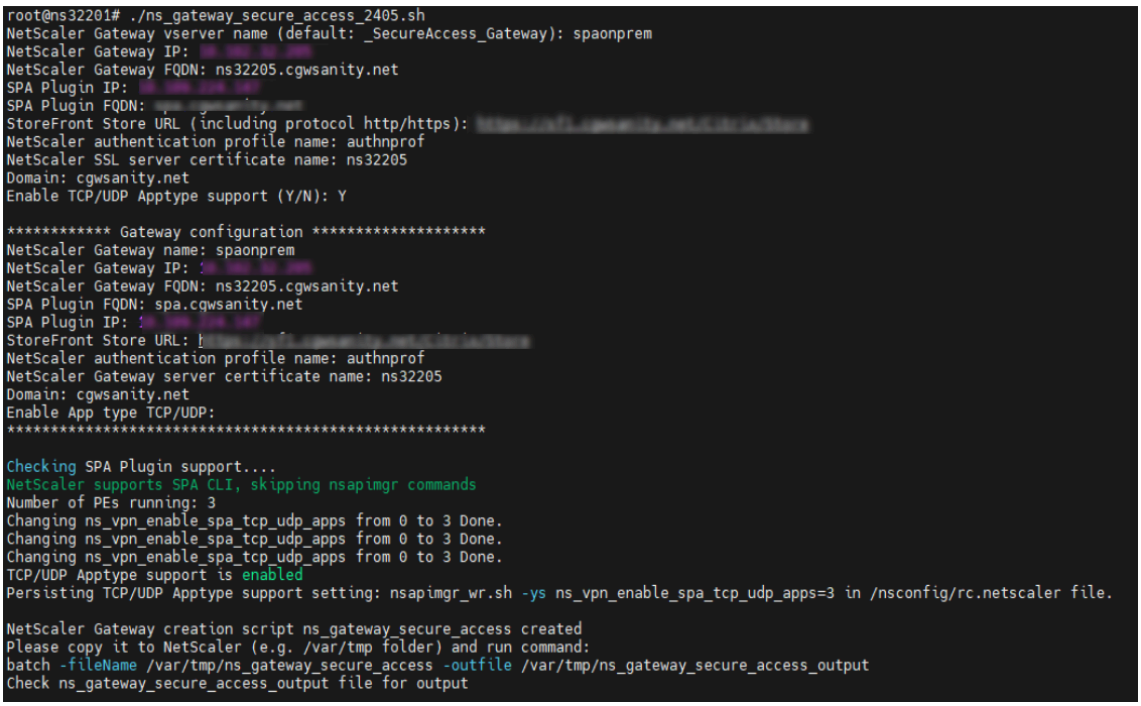
   Por ejemplo, `*scp ns_gateway_secure_access.sh nsroot@nsalfa.fabrikam.local:/var/tmp*`

   > **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.

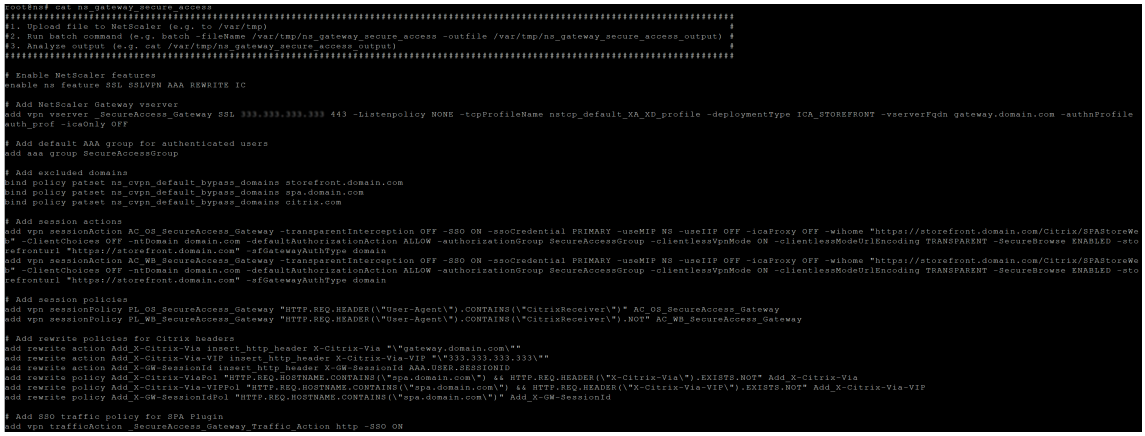


6. Introduzca los parámetros requeridos. Para ver la lista de parámetros, consulte Requisitos previos.

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

   Se genera un nuevo archivo con varios comandos de NetScaler (el predeterminado es var/tmp/ns_gateway_secure_access).

   > **Nota:**
   >
   > Durante la ejecución del script, se comprueba la compatibilidad de los complementos NetScaler y Secure Private Access. Si NetScaler admite el plug-in Secure Private Access, el script permite que las funciones de NetScaler admitan el envío de mejoras mediante etiquetas de acceso inteligente y la redirección a una nueva página de denegación cuando el acceso al recurso está restringido. Para obtener más información sobre las etiquetas inteligentes, consulte Compatibilidad con etiquetas de acceso inteligentes.
   >
   > Las funciones del plug-in Secure Private Access que persisten en el archivo /nsconfig/rc.netscaler permiten mantenerlas habilitadas después de reiniciar NetScaler.



7. 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.

8. 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.

Agregue un servidor virtual:

- tcpProfileName: nstcp_default_XA_XD_profile
- DeploymentType: ICA_STOREFRONT (disponible solo con el comando `add vpn vserver`)
- icaOnly: DESACTIVADO

Actualizar un servidor virtual:

- tcpProfileName: nstcp_default_XA_XD_profile
- icaOnly: DESACTIVADO

Ejemplos:

Para agregar un servidor virtual:

```
add vpn vserver _SecureAccess_Gateway SSL 999.999.999.999 443 -
Listenpolicy NONE -tcpProfileName nstcp_default_XA_XD_profile -
deploymentType ICA_STOREFRONT -vserverFqdn gateway.mydomain.com -
authnProfile auth_prof_name -icaOnly OFF
```

Para actualizar un servidor virtual:


```
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" - reemplazar con la URL real del almacén. La ruta al almacén /Citrix/MyStoreWeb es opcional.
- ClientChoices: OFF
- ntDomain: mydomain.com: se usa para el inicio de sesión único (opcional)
- 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

Soporte 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
  ```


- Habilite la redirección a la página "Acceso restringido"si se deniega el acceso.

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

- Utilice la página de "Acceso restringido"alojada en CDN.

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

- Para inhabilitarlo, vuelva a ejecutar el mismo comando.
- Para comprobar si la opción está activada o desactivada, ejecute el comando `nsconmsg`.
- Para configurar las etiquetas de acceso inteligente en NetScaler Gateway, consulte Configurar etiquetas contextuales.

Conservar la configuración del plug-in Secure Private Access en NetScaler

Para conservar la configuración del plug-in Secure Private Access en NetScaler, haga lo siguiente:

1. Cree o actualice el archivo /nsconfig/rc.netscaler.
2. Agregue los siguientes comandos al archivo.

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

   nsapimgr_wr.sh -ys call=toggle_vpn_redirect_to_access_restricted_page_on_d

   nsapimgr_wr.sh -ys call=toggle_vpn_use_cdn_for_access_restricted_page
   ```

3. Guarde el archivo.

La configuración del plug-in Secure Private Access se aplica automáticamente cuando se reinicia NetScaler.

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

Si no se puede acceder a la puerta de enlace pública desde la máquina de Secure Private Access, debe cargar un certificado de puerta de enlace pública a la base de datos de Secure Private Access.

Realice los siguientes pasos para cargar un certificado de puerta de enlace pública:

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 etiquetas contextuales

August 26, 2024

El plug-in Secure Private Access proporciona acceso contextual (acceso inteligente) a aplicaciones web o SaaS en función del contexto de la sesión del usuario, como la plataforma y el sistema operativo del dispositivo, el software instalado y la geolocalización.

Los administradores pueden agregar condiciones con etiquetas contextuales a la directiva de acceso. La etiqueta contextual del plug-in Secure Private Access es el nombre de una directiva de NetScaler Gateway (sesión, autenticación previa, EPA) que se aplica a las sesiones de los usuarios autenticados.

El plug-in Secure Private Access puede recibir etiquetas de acceso inteligentes como encabezado (nueva lógica) o haciendo llamadas a Gateway. Para obtener más información, consulte Etiquetas de acceso inteligentes.

> **Nota:**
>
> El plug-in Secure Private Access solo admite las directivas clásicas de autenticación previa a las puertas de enlace que se pueden configurar en NetScaler Gateway.

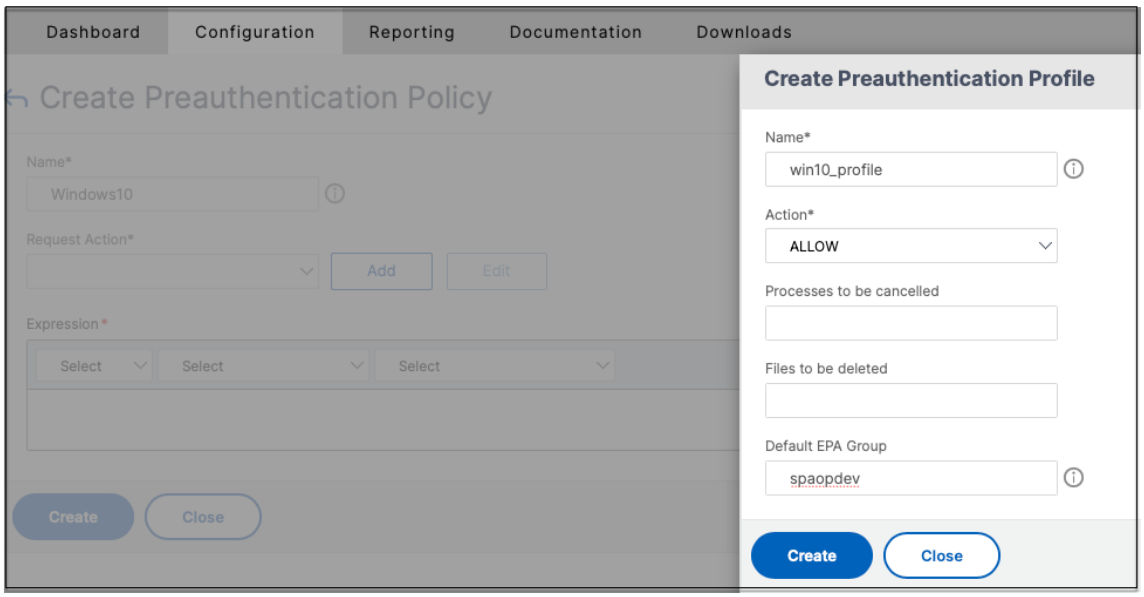
Configurar etiquetas personalizadas mediante la GUI

Los siguientes pasos de alto nivel están relacionados con la configuración de las etiquetas contextuales.

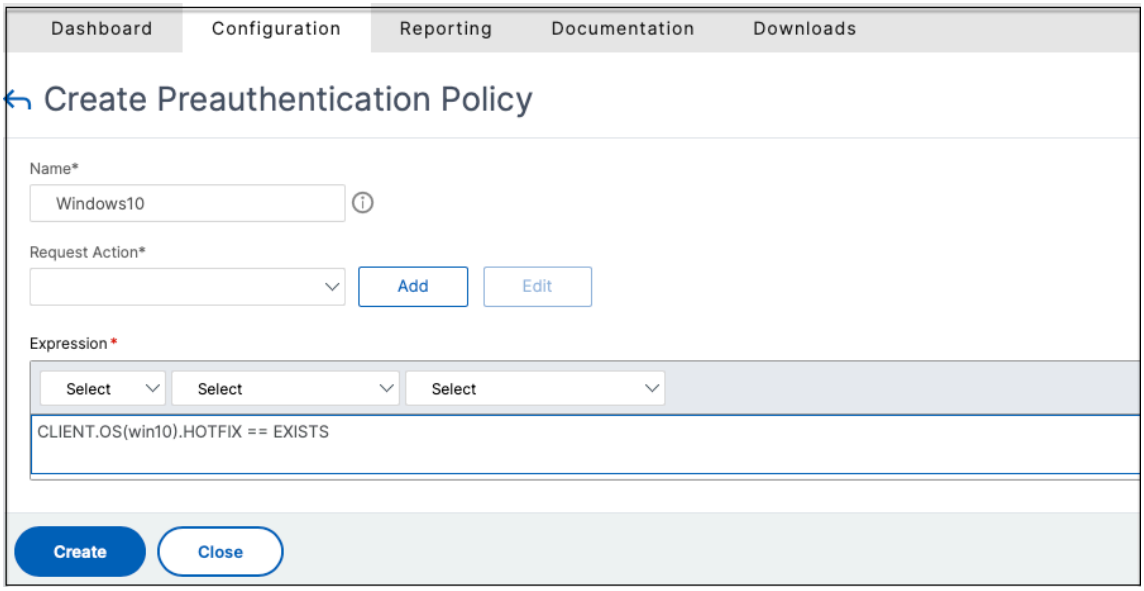
1. Configurar una directiva de autenticación previa de gateway clásica
2. Enlazar la directiva de autenticación previa clásica al servidor virtual de puerta de enlace

Configurar una directiva de autenticación previa de gateway clásica

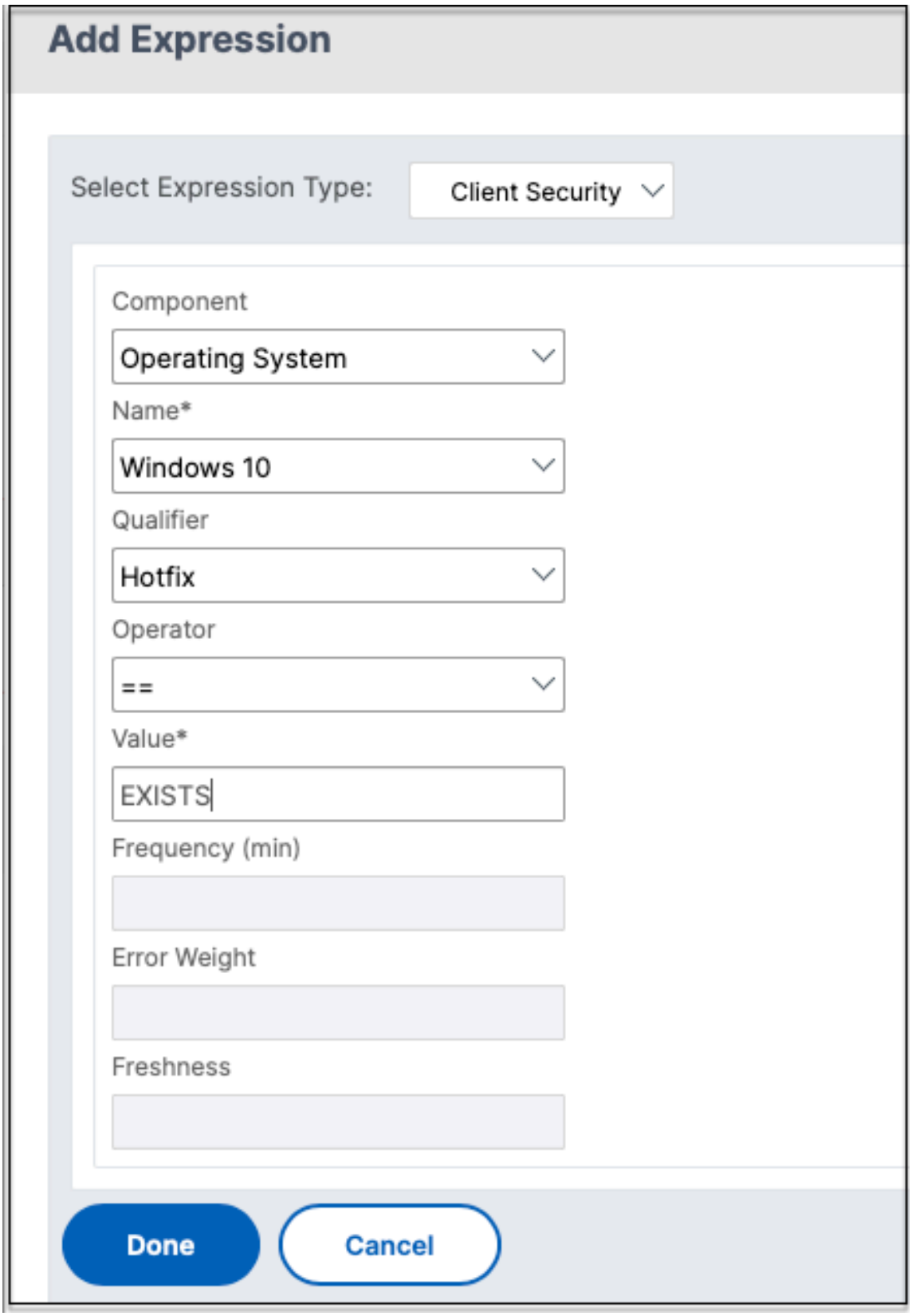
1. Vaya a **NetScaler Gateway > Directivas >** Autenticación previa y después haga clic en **Agregar**.
2. Seleccione una directiva existente o añada un nombre para la directiva. Este nombre de directiva se usa como valor de etiqueta personalizado.
3. En **Solicitar acción**, haga clic en **Agregar** para crear una acción. Puede reutilizar esta acción para varias directivas, por ejemplo, usar una acción para permitir el acceso y otra para denegar el acceso.



4. Complete los detalles en los campos obligatorios y haga clic en **Crear**.
5. En **Expresión**, introduzca la expresión manualmente o utilice el editor de expresiones para crear una expresión para la directiva.



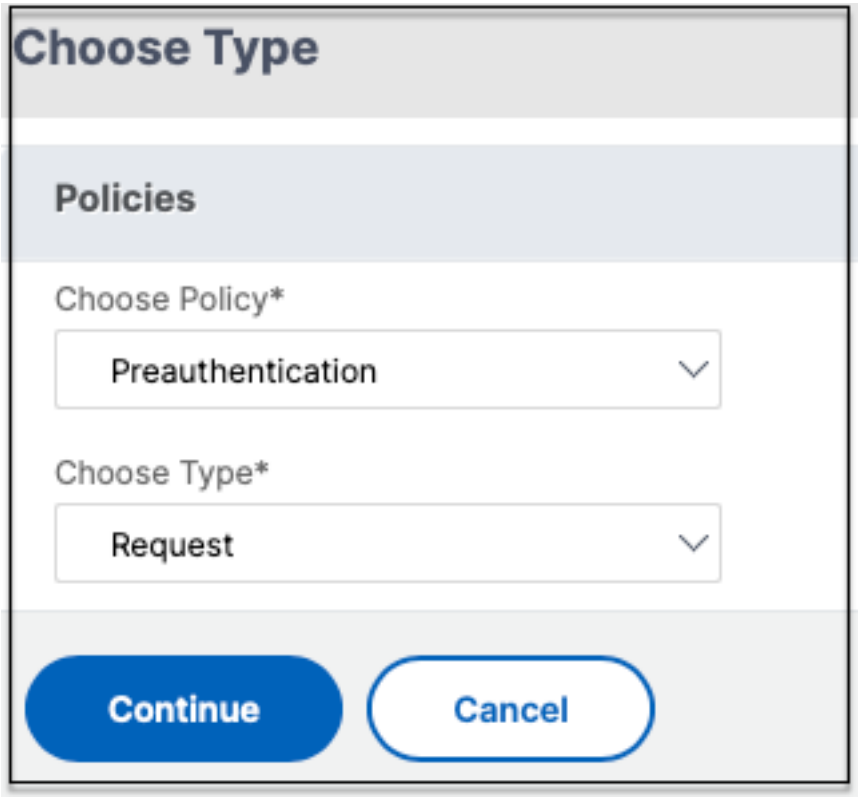
La siguiente figura muestra una expresión de ejemplo creada para comprobar el sistema operativo Windows 10.



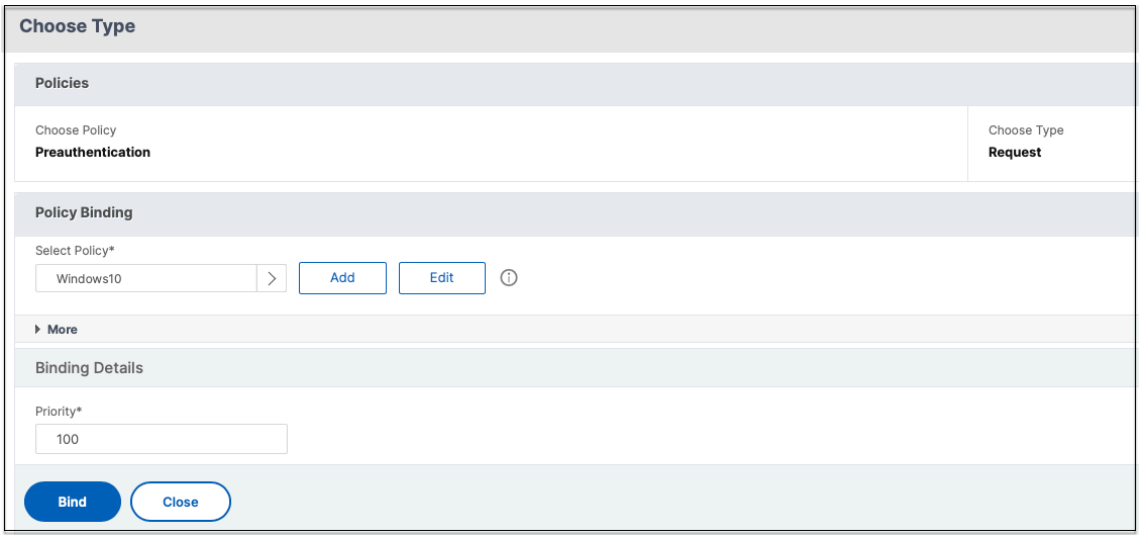
6. Haga clic en **Crear**.

Enlazar la etiqueta personalizada a NetScaler Gateway

1. Vaya a **NetScaler Gateway**> Servidores virtuales.
2. Seleccione el servidor virtual al que se vinculará la directiva de autenticación previa y después haga clic en **Editar**.
3. En la sección **Directivas**, haga clic en **+** para vincular la directiva.
4. En **Elegir directiva**, seleccione la directiva de autenticación previa y seleccione **Solicitud** en **Elegir tipo**.



5. Seleccione el nombre de la directiva y la prioridad para la evaluación de la directiva.
6. Haga clic en **Bind**.



Configurar etiquetas personalizadas mediante la CLI

Ejecute los siguientes comandos en la CLI de NetScaler para crear y vincular una directiva de autenticación previa:

Ejemplo:

- `add aaa preauthenticationaction win10_prof ALLOW`
- `add aaa preauthenticationpolicy Windows10 "CLIENT.OS(win10)EXISTS "win10_prof`
- `bind vpn vserver _SecureAccess_Gateway -policy Windows10 -priority 100`

Agregar una nueva etiqueta contextual

1. Abra la consola de administración de Secure Private Access y haga clic en **Directivas** de acceso.
2. Cree una directiva nueva o seleccione una directiva existente.
3. En la sección **Si se cumple la siguiente condición**, haga clic en **Agregar condición** y seleccione **Etiquetas** contextuales, coincide con **todas y después introduzca el nombre de** la etiqueta contextual (por ejemplo, `Windows10`).

Referencias

- Configure las directivas de acceso para las aplicaciones.
- Soporte para etiquetas de acceso inteligentes.

StoreFront

August 26, 2024

Si Secure Private Access se aloja conjuntamente con StoreFront, la configuración de Secure Private Access en StoreFront la realiza automáticamente el asistente de configuración por primera vez.

Sin embargo, si Secure Private Access no está hospedado conjuntamente con StoreFront, algunos cambios de configuración se deben realizar manualmente.

Realice los siguientes pasos para configurar StoreFront manualmente.

1. Descargue el script desde la consola de administración de Secure Private Access (**Parámetros > Integraciones**).
2. Haga clic en **Descargar el script** correspondiente a la entrada de StoreFront para la que se deben realizar los cambios de configuración.

   El archivo zip descargado contiene un script de configuración, un archivo README y un script de limpieza de la configuración. El script de limpieza se puede usar en caso de que se vaya a eliminar la integración entre StoreFront y Secure Private Access.
3. Ejecute el script como administrador en una instancia de PowerShell de 64 bits mediante el comando `./ConfigureStorefront.ps1`.

   - No se requieren otros parámetros.
   - La directiva de ejecución de scripts de PowerShell se debe establecer en **Sin restricciones** o en **Omitir** para ejecutar el script de StoreFront.
   - El script también propaga la configuración a otros servidores StoreFront si StoreFront está configurado como un clúster.

Una vez que StoreFront esté configurado con los parámetros de Secure Private Access, la configuración del plug-in Secure Private Access se podrá ver en la interfaz de usuario de administración de StoreFront (pantalla **Administrar Delivery Controllers**).

El script de StoreFront configura automáticamente la configuración del grupo de agregación para Secure Private Access si la misma está configurada para el Delivery Controller de Citrix Virtual Apps and Desktops. De forma predeterminada, el script configura el Secure Private Access para todos (**mapeo de usuarios y configuración de agregación multisitio > Configurado**).

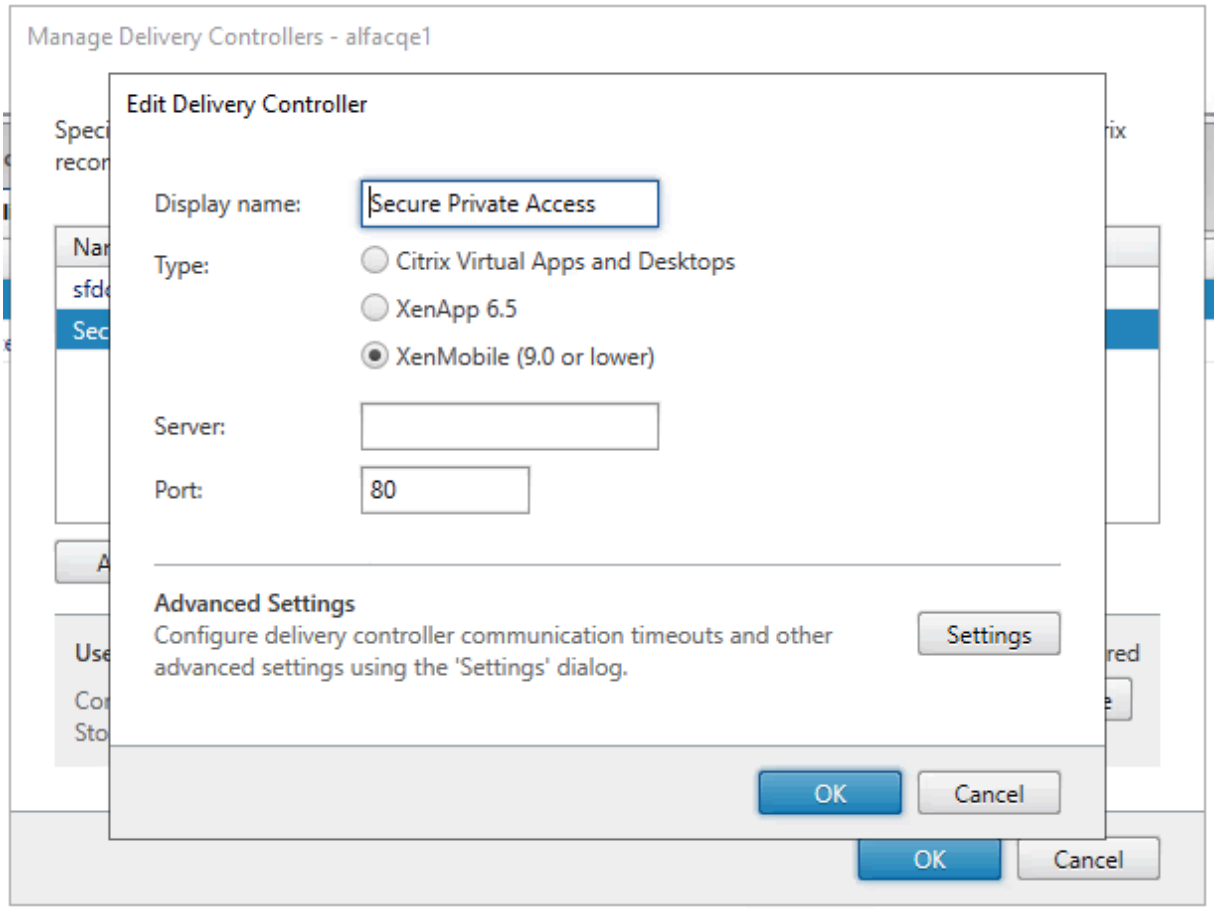
> **Importante:**
>
> - Se recomienda usar el script de StoreFront descargado de la interfaz de usuario de administración de Secure Private Access para configurar StoreFront únicamente para Secure Private Access. No configure Secure Private Access desde la interfaz de usuario de adminis-

> tración de StoreFront, ya que la interfaz de usuario no cubre toda la configuración requerida en StoreFront. El script debe ejecutarse para completar todas las configuraciones necesarias.
>
> - También se puede configurar un sitio de Secure Private Access en varias implementaciones de StoreFront (en otro almacén del mismo StoreFront o en una implementación de StoreFront diferente).
>   StoreFront se puede agregar desde la página **Parámetros > Integraciones**.
> - La configuración automática de StoreFront no funciona desde la página Parámetros **> Integración**, incluso si Secure Private Access se aloja conjuntamente con StoreFront. La configuración automática solo se realiza durante la primera configuración. Si se agrega una nueva configuración de almacén desde la **página**de configuración, el script de StoreFront debe descargarse y ejecutarse en la máquina StoreFront correspondiente.

Cuando se usa la versión 2308 de StoreFront o anterior

Si utiliza la versión 2308 de StoreFront o una anterior, la interfaz de usuario de administración de StoreFront presenta los siguientes problemas conocidos:

- El tipo de plug-in Secure Private Access se muestra como XenMobile.
- No se muestra la URL del servidor de Secure Private Access.
- El puerto de Secure Private Access siempre se muestra como 80.



Al usar StoreFront versión 2311 o posterior

En la versión 2311 y posteriores de StoreFront, el cliente Citrix Workspace para Web no enumera las aplicaciones de Secure Private Access. Esto se debe a que Secure Private Access no admite el inicio de la aplicación Secure Private Access en la plataforma Workspace for Web.

Director

August 26, 2024

La integración de Director con Secure Private Access permite una supervisión eficaz del rendimiento y la solución de problemas. Para integrar Director con Secure Private Access, debe introducir la dirección IP del FQDN del servidor de Director que debe estar registrado en Secure Private Access. Para obtener más información, consulte Integrar servidores.

El registro de Director con Secure Private Access es una configuración obligatoria para los clientes locales de la versión 2402 de Secure Private Access. Si no tiene Director configurado, debe instalar la

versión más reciente de Director, LTSR 2402 o posterior. Si ya tiene Director configurado, debe actualizarlo a la versión más reciente, LTSR 2402 o posterior. La configuración de Secure Private Access no se puede completar sin registrar un Director. La validación también falla en los siguientes casos.

- Director no está registrado en Secure Private Access.
- La dirección IP de Director o el FQDN que ha introducido no existen.

Para obtener más información sobre el registro de Director con Secure Private Access, consulte Integrar servidores de StoreFront y NetScaler Gateway y Administrar la configuración después de la instalación.

> **Nota:**
>
> - El registro o inicio de sesión de Director no admite la autenticación integrada de Windows (IWA). Si el administrador ha iniciado sesión en la consola de Secure Private Access mediante IWA, se le pedirá que introduzca las credenciales para registrarse como Director.
> - Si el administrador ha iniciado sesión manualmente en la consola de Secure Private Access, esos detalles se aprovechan para autenticarse en el servidor de Director. Si esto no funciona, se le pide al administrador que introduzca las credenciales.
> - Si el administrador tiene que agregar un Director diferente una vez finalizada la configuración, registre el nuevo Director desde la página **Administrar ajustes**. Al actualizar los detalles de Director después de la configuración, los administradores deben introducir las credenciales para realizar los cambios. No se admite el inicio de sesión único para editar la URL de Director IPv6, SSLv3.

Configure Director con Secure Private Access mediante la herramienta de configuración de Director

La configuración de Director con Secure Private Access mediante la herramienta de configuración es un paso obligatorio para completar la integración. Para obtener más información, consulte Integración de Secure Private Access con Director.

Ver las sesiones de usuario de Secure Private Access en Director

Puede ver las sesiones de usuario de Secure Private Access en Director Para obtener más información, consulte Ver una sesión de Secure Private Access por usuario.

Servidor de licencias

August 26, 2024

Un servidor de licencias para el plug-in Secure Private Access es un componente obligatorio necesario para recopilar y procesar los datos de licencias. Un servidor de licencias se puede registrar en Secure Private Access durante la configuración inicial o también se puede configurar o actualizar una vez finalizada la configuración. Para obtener más información sobre el registro de un servidor de licencias con Secure Private Access, consulte Integrar los servidores de StoreFront y NetScaler Gateway y Administrar la configuración después de la instalación.

Debe especificar la URL del servidor de licencias para conectar Secure Private Access con el servidor de licencias. El plug-in Secure Private Access se registra automáticamente en el servidor de licencias.

> **Nota:**
>
> - Debe instalar al menos una licencia de intermediario de Citrix Virtual Apps and Desktops en el servidor de licencias para registrar el plug-in Secure Private Access en el servidor de licencias.
> - El servidor de licencias para el plug-in Secure Private Access es compatible a partir de la versión 11.17.2, compilación 45000 y posteriores. Si ya tiene un servidor de licencias, debe actualizarlo a la versión 11.17.2 build 45000 o posterior.

Para obtener más información sobre el servidor de licencias, consulte Servidor de licencias.

Web Studio

August 26, 2024

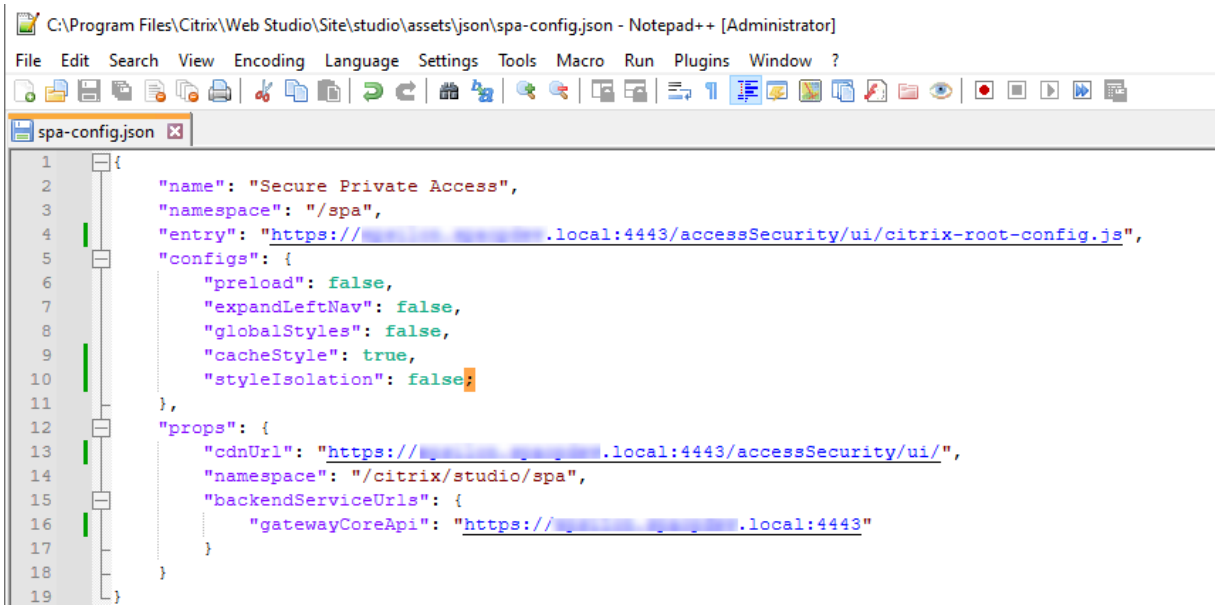
Citrix Secure Private Access también está integrado en la consola de Web Studio para permitir a los usuarios acceder sin problemas al servicio a través de Web Studio.

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 de 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\studio\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.



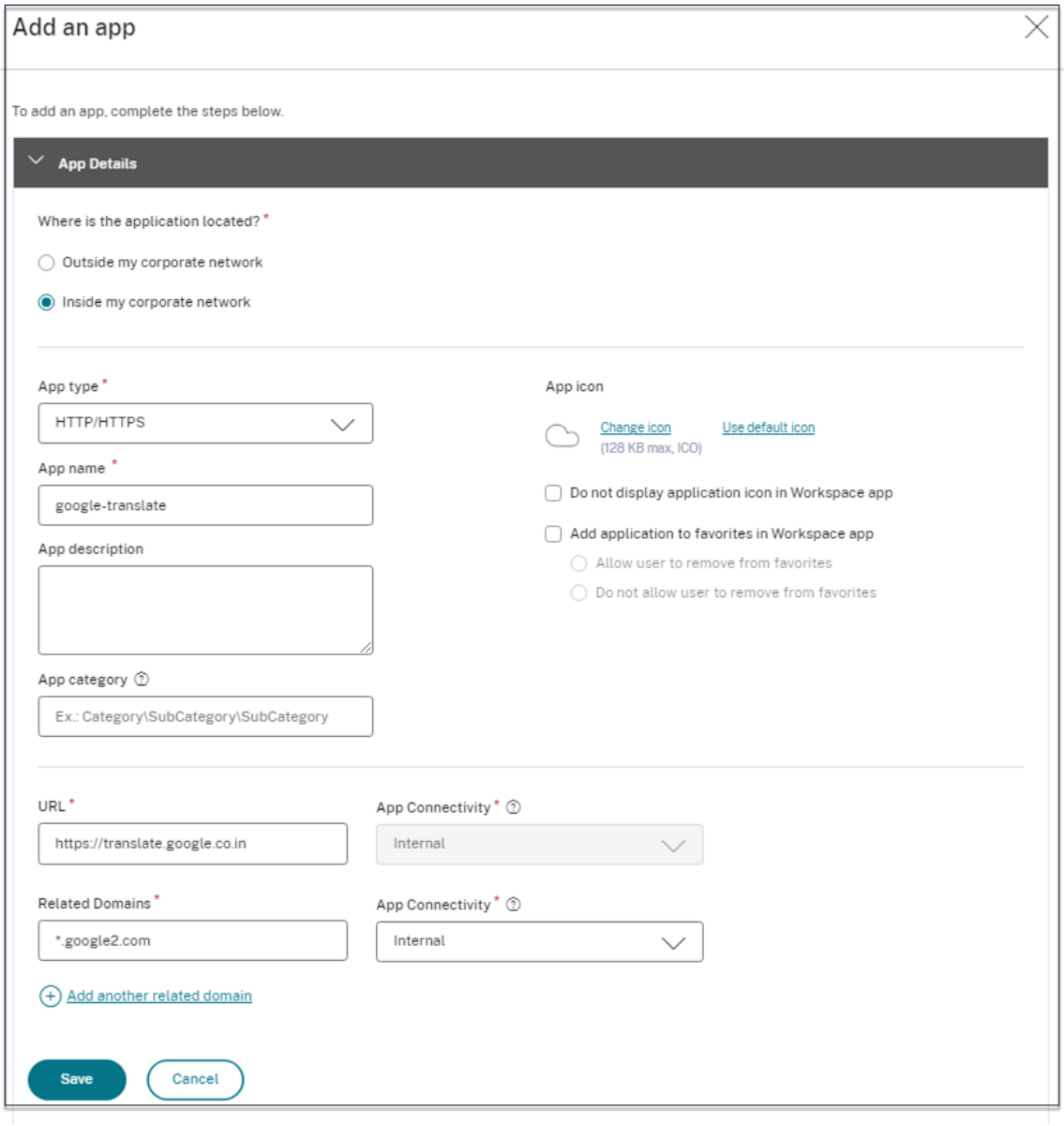
1. Sustituya "SpaServer"por el FQDN de su complemento de Secure Private Access.
2. Inicie sesión en Web Studio.
3. En el menú de navegación de la izquierda, haga clic en **Secure Private Access** para acceder a la consola de administración de Secure Private Access desde Web Studio.

Configurar aplicaciones HTTP/HTTPS

August 26, 2024

Después de configurar Secure Private Access, puede configurar las aplicaciones y las directivas de acceso desde la consola de administración.

1. En la consola de administración, haga clic en **Aplicaciones**.
2. Haga clic en **Agregar una aplicación**.
3. 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.
4. Introduzca los siguientes detalles en la sección Detalles de la aplicación y haga clic en **Siguiente**.



- **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, consulte 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 icono** para cambiar el icono 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 icono, se muestra el icono 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.

  > **Nota:**
  >
  > - Asegúrese de que el dominio relacionado de una aplicación no se superponga con el dominio relacionado de otra aplicación. Si esto ocurre, elimine el dominio relacionado de todas las aplicaciones y cree una nueva aplicación con este dominio y, a continuación, defina el acceso según corresponda en la directiva de acceso. También puede considerar si desea mostrar esta aplicación en StoreFront u ocultarla. Puede ocultar la aplicación en StoreFront mediante la opción **No mostrar la aplicación a los usuarios** al publicar la aplicación.
  > - Del mismo modo, la URL de una aplicación publicada no se debe agregar como dominio relacionado de otra aplicación.
  > - Para obtener más información, consulte Prácticas recomendadas para configuraciones de aplicaciones web y SaaS.

- **Agregar aplicación a favoritos automáticamente**: haga clic en esta opción para agregar esta aplicación como favorita en la aplicación Citrix Workspace. Al seleccionar esta opción, aparece un icono de estrella con un candado en la esquina superior izquierda de 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 eliminen la aplicación de la lista de aplicaciones favoritas de la aplicación Citrix Workspace.
    Al seleccionar esta opción, aparece un icono 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 eliminen la aplicación de la lista de aplicaciones favoritas 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.

5. Haga clic en **Guardar**y, a continuación, en **Finalizar**.

Puede ver todos los dominios de la aplicación que están configurados en **Parámetros > Dominio de la aplicación**. Para obtener más información, consulte Administrar la configuración después de la instalación.

Siguientes pasos

Configurar directivas de acceso para las aplicaciones

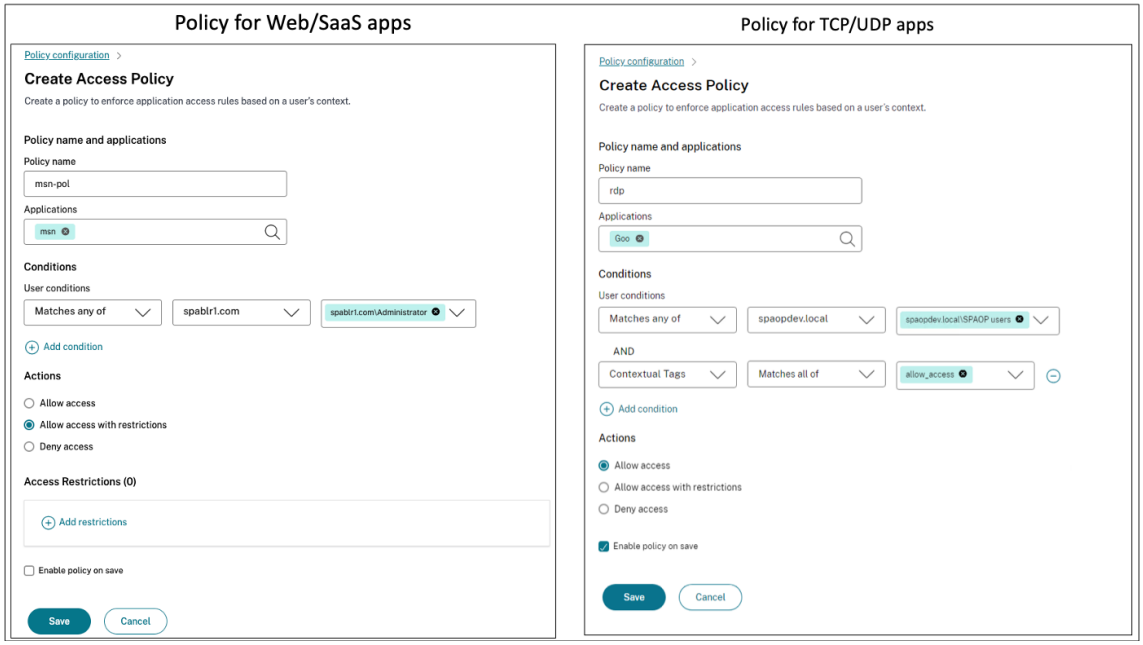
Configurar directivas de acceso para las aplicaciones

August 26, 2024

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 (HTTP/HTTPS) agregando las restricciones de seguridad.

1. En la consola de administración, haga clic en **Directivas de acceso**.

2. Haga clic en **Crear directiva**.



3. a) En **Nombre de la directiva**, introduzca un nombre para la directiva.
4. En **Aplicaciones**, seleccione las aplicaciones para las que desea aplicar las directivas de acceso.
5. En **Condiciones de usuario**: seleccione las condiciones y los usuarios o grupos de usuarios según 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.

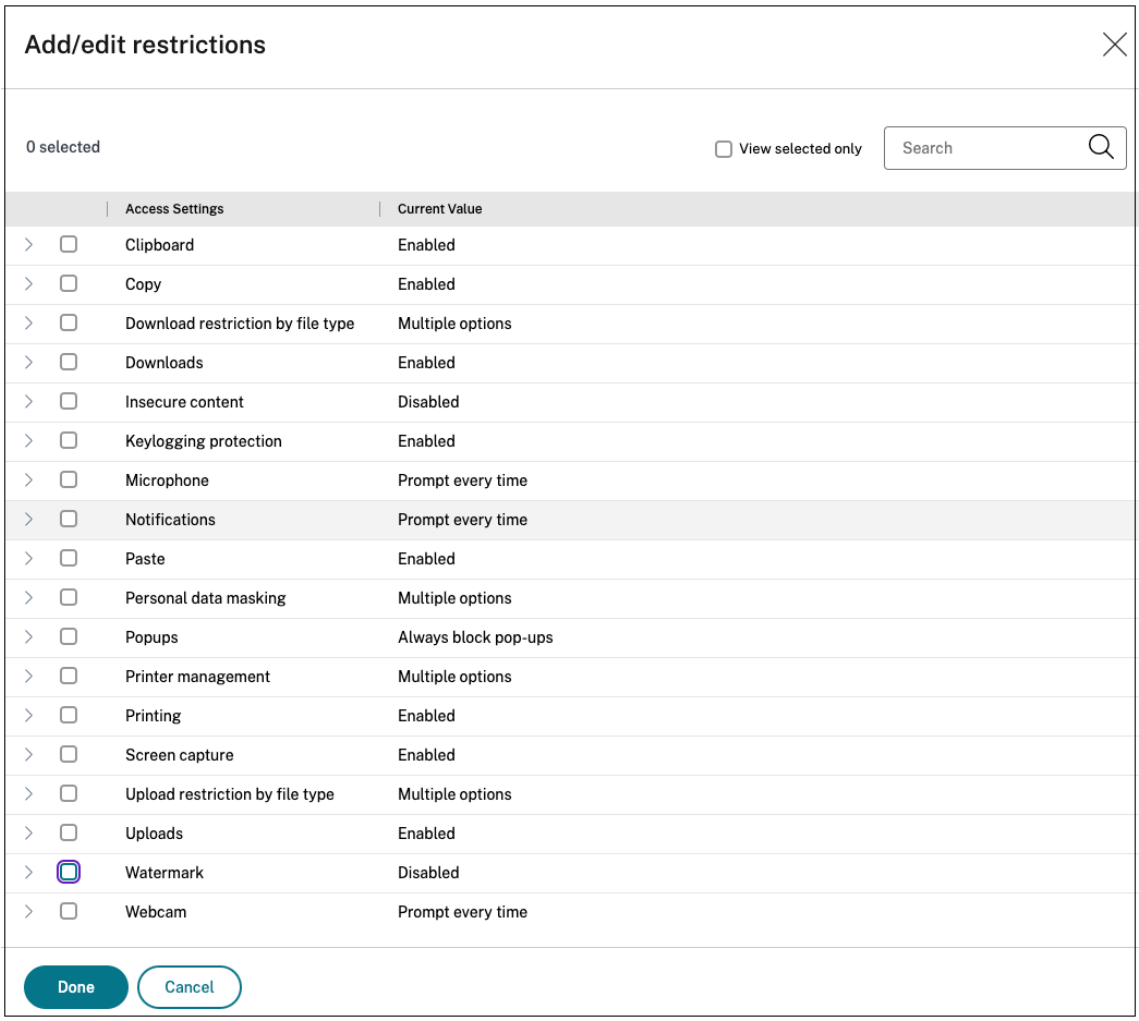
6. Haga clic en **Agregar condición** para agregar otra condición basada en etiquetas contextuales. Estas etiquetas se derivan de NetScaler Gateway.
7. En **Acciones**, seleccione una de las siguientes acciones que se deben aplicar en la aplicación en función de la evaluación de la condición.

   - **Permitir el acceso**
   - **Permitir el acceso con restricción**
   - **Denegar el acceso**

   Al seleccionar **Permitir acceso con restricciones**, debe hacer clic en **Agregar restricciones** para seleccionar las restricciones. Para obtener más información sobre cada restricción, consulte Restricciones de acceso disponibles

   Seleccione las restricciones y, a continuación, haga clic en **Listo**.

> **Nota:**
>
> La acción **Permitir el acceso con restricciones** no se aplica a las aplicaciones TCP/UDP.



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

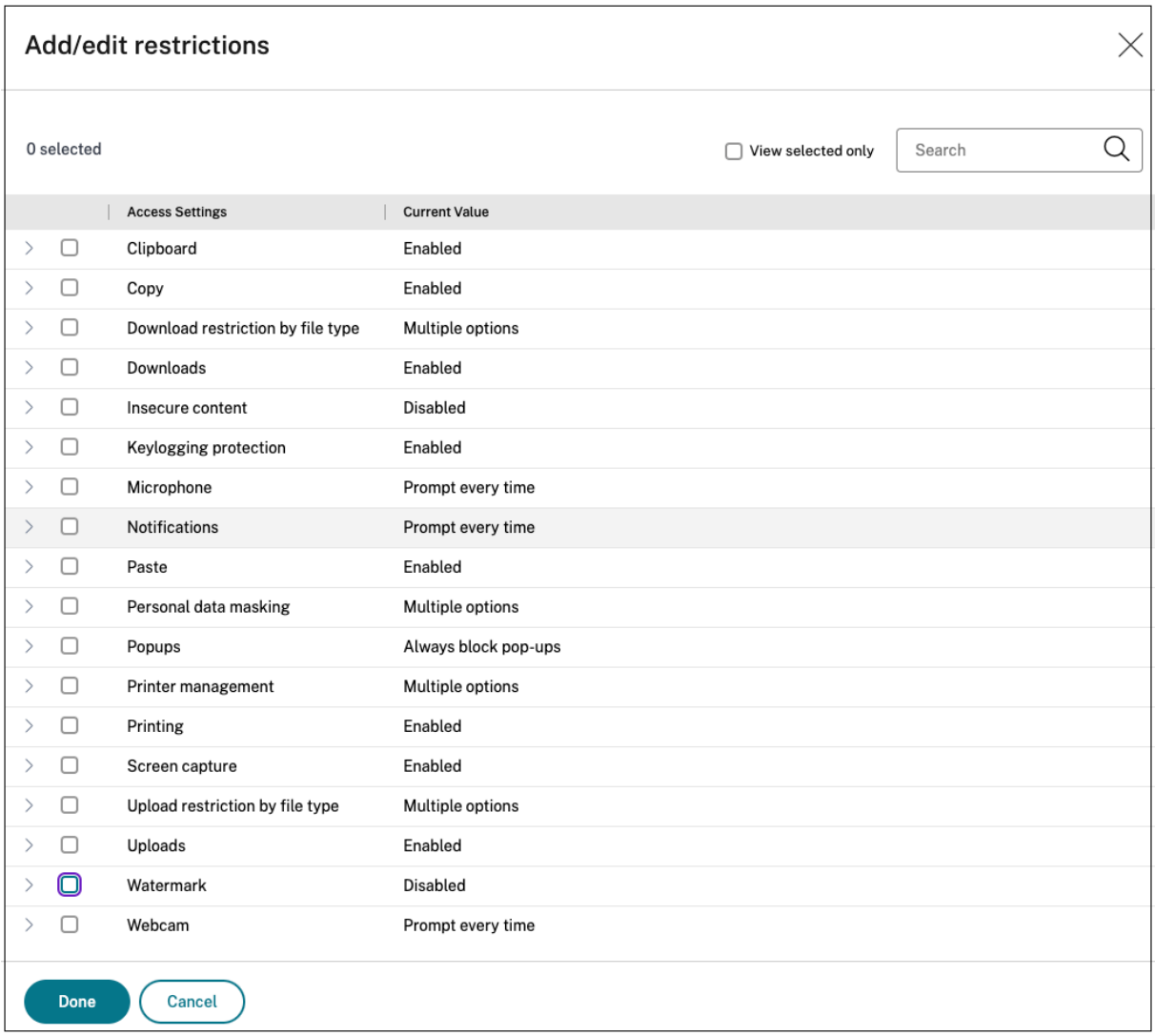
- Valide su configuración desde las máquinas cliente (Windows y macOS).
- Para las aplicaciones TCP/UDP, valide la configuración desde las máquinas cliente (Windows y macOS) iniciando sesión en el cliente Citrix Secure Access.

Ejemplo de validación de configuración

Opciones de restricción de acceso

August 27, 2024

Al seleccionar la acción **Permitir el acceso con restricciones**, puede seleccionar las restricciones de seguridad según el requisito. Estas restricciones de seguridad están predefinidas en el sistema. Los administradores no pueden modificar ni agregar otras combinaciones.



Portapapeles

Habilite o inhabilite las operaciones de cortar/copiar/pegar en una aplicación web interna o SaaS con esta directiva de acceso cuando se acceda a través de Citrix Enterprise Browser. Valor predeterminado: Habilitado.

Copiar

Habilite o inhabilite la copia de datos de una aplicación web interna o SaaS con esta directiva de acceso cuando se acceda a través de Citrix Enterprise Browser. Valor predeterminado: Habilitado.

> **Nota:**
>
> - Si las restricciones del **portapapeles** y de **copia** están habilitadas en una directiva, la restricción del **portapapeles** tiene prioridad sobre la restricción de **copia**.
> - Los usuarios finales deben usar la versión 126 o posterior de Citrix Enterprise Browser para acceder a las aplicaciones para las que está habilitada esta restricción. De lo contrario, el acceso a la aplicación está restringido.
> - Para un control detallado de las operaciones de copia dentro de las aplicaciones, los administradores pueden usar la restricción de **grupos de seguridad**. Para obtener más información, consulte Restricción del portapapeles para grupos de seguridad.

Restricción de descarga por tipo de archivo

Habilite o inhabilite la capacidad del usuario para descargar un tipo de MIME (archivo) específico desde la aplicación SaaS o web interna con esta directiva cuando acceda a través de Citrix Enterprise Browser.

> **Nota:**
>
> - La **restricción de descarga por tipo de archivo** está disponible además de la restricción de **descarga**.
> - Si tanto la **descarga** como la **restricción de descarga por tipo de archivo** están habilitadas en una directiva, la restricción de **descarga** tiene prioridad sobre la **restricción de descarga por tipo de archivo**.
> - Los usuarios finales deben usar la versión 126 o posterior de Citrix Enterprise Browser para acceder a las aplicaciones para las que está habilitada esta restricción. De lo contrario, el acceso a la aplicación está restringido.

Para habilitar la descarga de tipos MIME, lleve a cabo los siguientes pasos:

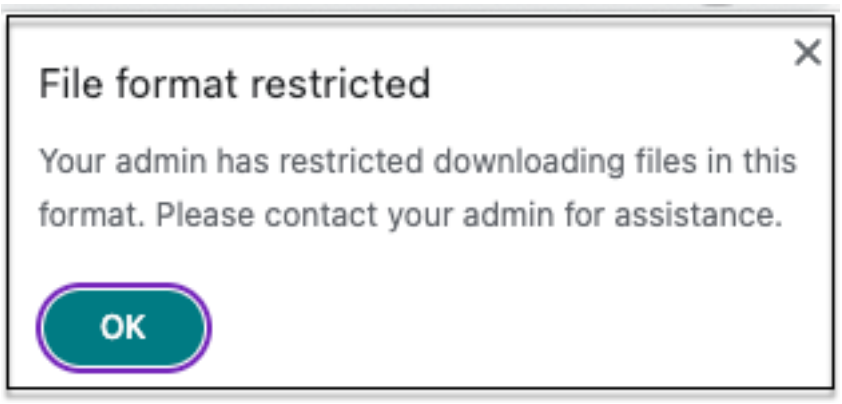
1. Cree o modifique una directiva de acceso. Para obtener más información sobre la creación de una directiva de acceso, consulte Configurar directivas de acceso.
2. En **Acciones**, seleccione **Permitir con restricciones**.
3. Haga clic en **Restricción de descarga por tipo de archivo** y, a continuación, en **Modificar**.
4. En la página de **parámetros de restricción de descargas por tipo de archivo**, seleccione una de las siguientes opciones:
    - **Permitir todas las descargas con excepciones**: seleccione los tipos que deben bloquearse y permita todos los demás tipos.
    - **Bloquear todas las descargas con excepciones**: seleccione solo los tipos que se pueden cargar y bloquee todos los demás tipos.

5. Si el tipo de archivo no existe en la lista, haga lo siguiente:

    a) Haga clic en **Agregar tipos MIME personalizados**.
    b) En **Agregar tipos MIME**, introduzca el tipo MIME en el formato `category`/`subcategory` <`extension`>. Por ejemplo, image/png.
    c) Haga clic en **Listo**.

    El tipo MIME ahora aparece en la lista de excepciones.

Cuando un usuario final intenta descargar un tipo de archivo restringido, Citrix Enterprise Browser muestra el siguiente mensaje de advertencia:



Descargas

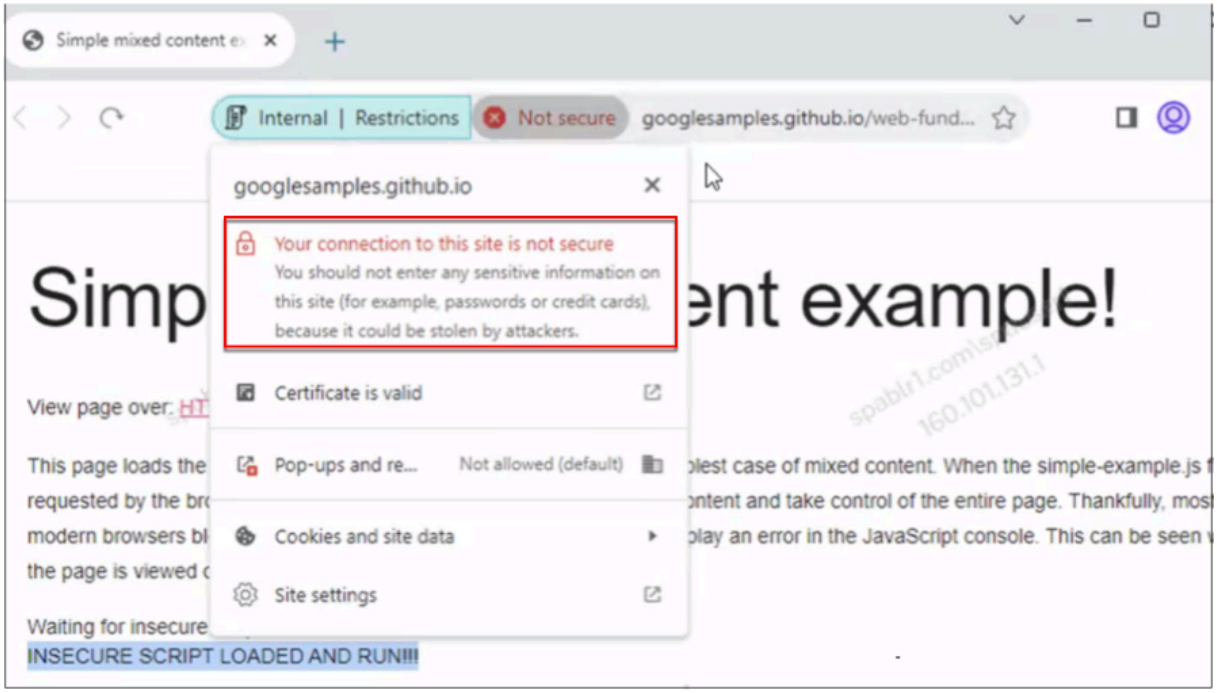
Habilite o inhabilite la capacidad del usuario para descargar desde la aplicación web interna o SaaS con esta directiva cuando acceda a través de Citrix Enterprise Browser. Valor predeterminado: Habilitado.

> **Nota:**
>
> Si tanto las **descargas** como la **restricción de descargas por tipo de archivo** están habilitadas en una directiva, la restricción de **descargas** tiene prioridad sobre la **restricción de descargas por tipo de archivo**.

Contenido no seguro

Habilite o inhabilite que los usuarios finales accedan a contenido no seguro dentro de la aplicación web interna o SaaS configurada con esta directiva cuando acceden a través de Citrix Enterprise Browser. El contenido no seguro es cualquier archivo enlazado desde una página web mediante un enlace HTTP en lugar de un enlace HTTPS. Valor predeterminado: Habilitado.

En la siguiente figura se muestra un ejemplo de notificación cuando se accede a contenido no seguro.



Protección contra registro de tecleo

Habilite o inhabilite los registradores de teclas para que no capturen las pulsaciones de teclas desde la aplicación web interna o SaaS con esta directiva de acceso cuando se accede a través de Citrix Enterprise Browser. Valor predeterminado: Habilitado.

Micrófono

Pregunte o no a los usuarios cada vez que accedan al micrófono en la aplicación web interna o SaaS configurada con esta directiva cuando accedan a través de Citrix Enterprise Browser. Valor predeterminado: Preguntar siempre.

Los usuarios finales deben usar la versión 126 o posterior de Citrix Enterprise Browser para acceder a las aplicaciones para las que está habilitada la restricción del **micrófono**.

Para permitir el micrófono en todo momento sin que se le pregunte, lleve a cabo los siguientes pasos:

1. Cree o modifique una directiva de acceso. Para obtener más información, consulte Configurar directivas de acceso.
2. En **Acciones**, seleccione **Permitir con restricciones**.
3. Haga clic en **Micrófono** y, a continuación, en **Modificar**.
4. En la página **Parámetros del micrófono**, haga clic en **Permitir siempre el acceso**.
5. Haga clic en **Guardar**y, a continuación, en **Listo**.

> **Nota:**
>
> - Si la restricción de **micrófono** está habilitada en la directiva de Secure Private Access, Citrix Enterprise Browser mostrará la configuración **Permitir**.
> - Si la opción es **Preguntar siempre** en la directiva de Secure Private Access, la configuración aplicada en Citrix Enterprise Browser varía en función de si se utiliza o no Global App Configuration Service (GACS) para administrar Citrix Enterprise Browser.
>
> - Si se usa GACS, la configuración de GACS se aplica en Citrix Enterprise Browser.
> - Si no se usa GACS, Citrix Enterprise Browser muestra el parámetro **Preguntar**.
>
> - Actualmente, Secure Private Access no admite el bloqueo del micrófono. Si necesita bloquear el micrófono, debe hacerlo a través de GACS.

Para obtener más información acerca de GACS, consulte Administrar Citrix Enterprise Browser mediante Global App Configuration Service.

Notificaciones

Pregunte o no a los usuarios cada vez para ver las notificaciones en la aplicación web interna o SaaS configurada con esta directiva cuando accedan a través de Citrix Enterprise Browser. Valor predeterminado: Preguntar siempre.

Los usuarios finales deben usar la versión 126 o posterior de Citrix Enterprise Browser para acceder a las aplicaciones para las que está habilitada esta restricción.

Para bloquear la visualización de notificaciones sin preguntar, lleve a cabo los siguientes pasos.

1. Cree o modifique una directiva de acceso. Para obtener más información, consulte Configurar directivas de acceso.
2. En **Acciones**, seleccione **Permitir con restricciones**.
3. Haga clic en **Notificaciones** y, a continuación, en **Modificar**.
4. En la página **Parámetros de notificaciones**, haga clic en **Bloquear siempre las notificaciones**.
5. Haga clic en **Guardar**y, a continuación, en **Listo**.

Pegar

Habilite o inhabilite el pegado de datos copiados en la aplicación web interna o SaaS con esta directiva de acceso cuando se acceda a través de Citrix Enterprise Browser. Valor predeterminado: Habilitado.

> **Nota:**
>
> - Si las restricciones del **portapapeles** y **pegado** están habilitadas en una directiva, la restricción del **portapapeles** tiene prioridad sobre la restricción de **pegado**.
> - Los usuarios finales deben usar la versión 126 o posterior de Citrix Enterprise Browser para acceder a las aplicaciones para las que está habilitada esta restricción. De lo contrario, el acceso a la aplicación está restringido.
> - Para un control detallado de las operaciones de pegado dentro de las aplicaciones, los administradores pueden usar la restricción **de grupos de seguridad**. Para obtener más información, consulte Restricción del portapapeles para grupos de seguridad.

Enmascaramiento de datos personales

Habilite o inhabilite la redacción o el enmascaramiento de la información de identificación personal (PII) en la aplicación web interna o SaaS con esta directiva cuando se acceda a través de Citrix Enterprise Browser.

> **Nota:**
>
> Los usuarios finales deben usar la versión 126 o posterior de Citrix Enterprise Browser para acceder a las aplicaciones para las que está habilitada esta restricción. De lo contrario, el acceso a la aplicación está restringido.

Para redactar o enmascarar la información de identificación personal, lleve a cabo los siguientes pasos:

1. Cree o modifique una directiva de acceso. Para obtener más información, consulte Configurar directivas de acceso.
2. En **Acciones**, seleccione **Permitir con restricciones**.
3. Haga clic en **Enmascaramiento de datos personales** y, a continuación, en **Modificar**.
4. Seleccione el tipo de información que desea ocultar o enmascarar y, a continuación, haga clic en **Agregar**.

   Si el tipo de información no aparece en la lista predefinida, puede agregar un tipo de información personalizado. Para obtener más información, consulte Agregar un tipo de información personalizado.
5. Seleccione el tipo de máscara.

   - **Enmascaramiento completo**: cubre completamente la información confidencial para que sea ilegible.

- **Enmascaramiento parcial**: cubre parcialmente la información confidencial. Solo se cubren las secciones relevantes, dejando el resto intacto.

  Al seleccionar **Enmascaramiento parcial**, debe seleccionar los caracteres empezando por el principio o el final del documento. Debe introducir los números en los campos **Primeros caracteres enmascarados** y **Últimos caracteres enmascarados**.

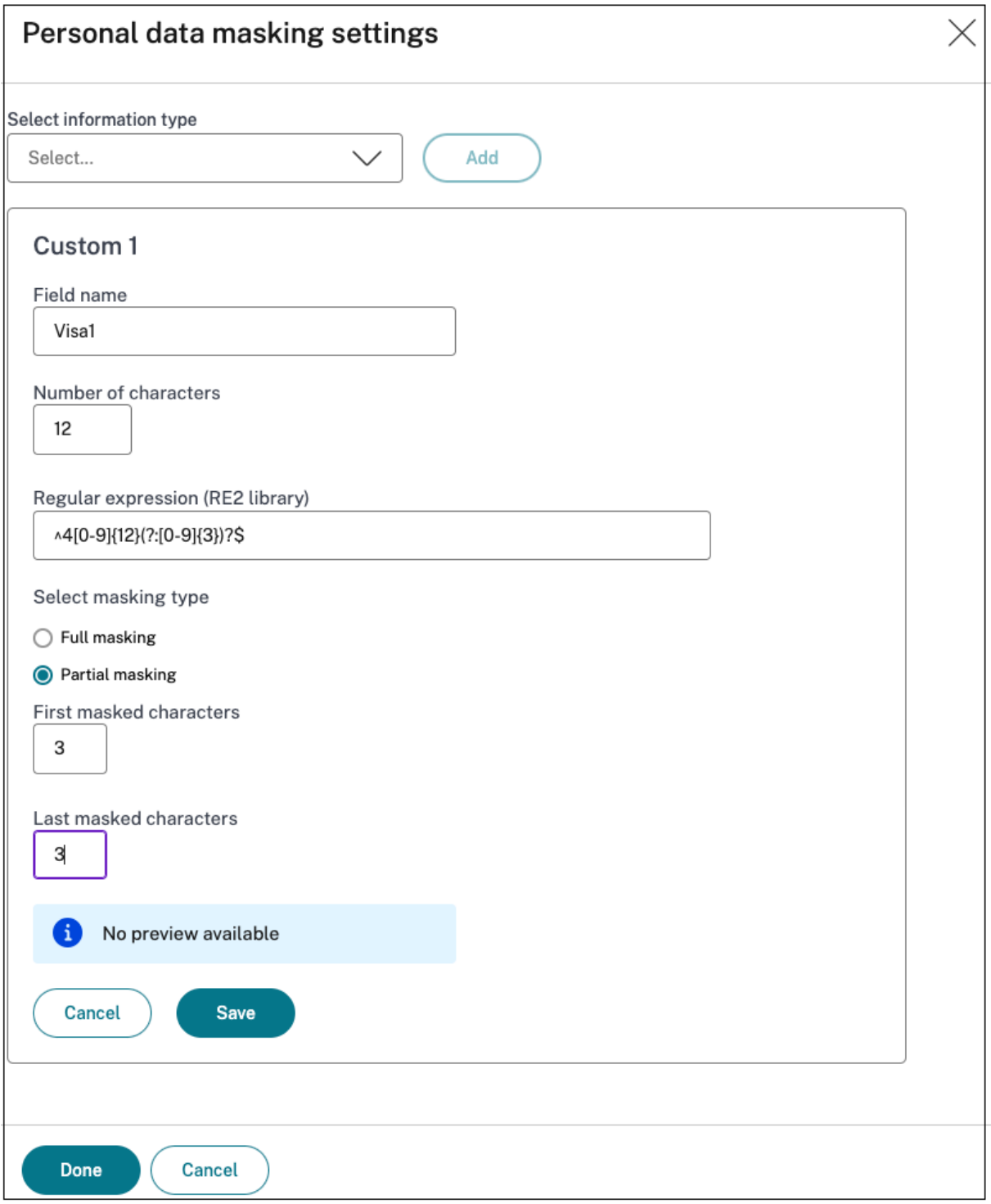
  El campo **Vista previa** muestra el formato de máscara. Esta vista previa no está disponible para las directivas personalizadas.

6. Haga clic en **Guardar** y, a continuación, en **Listo**.

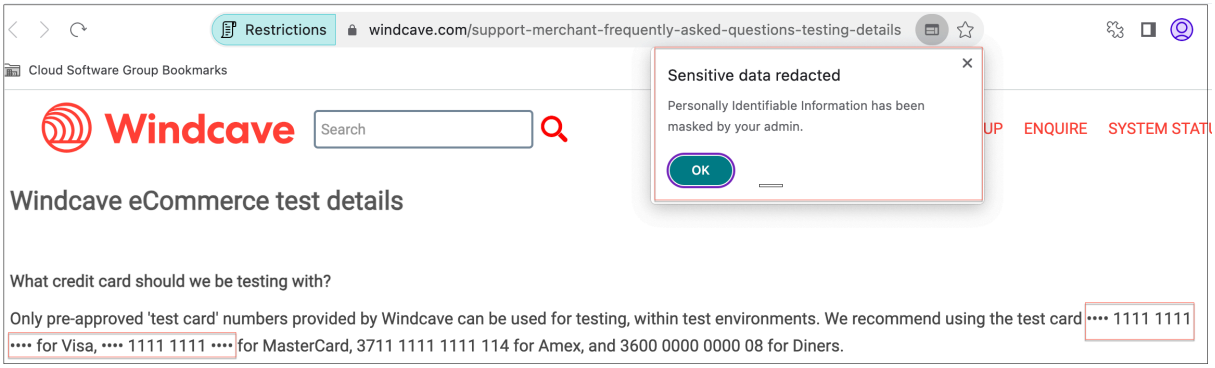
Agregar un tipo de información personalizado

Puede agregar un tipo de información personalizado agregando la expresión regular del tipo de información.

1. En **Seleccionar tipo de información**, seleccione **Personalizado** y, a continuación, haga clic en **Agregar**.
2. En **Nombre de campo**, introduzca el nombre del tipo de información que desea enmascarar.
3. En **Número de caracteres**, introduzca el número de caracteres del tipo de información.
4. En **Expresión regular (biblioteca RE2)**, introduzca la expresión del tipo de información personalizado. Por ejemplo, `^4[0-9]{ 12 } (?:[0-9]{ 3 } )?$`.
5. Seleccione el tipo de máscara si desea enmascarar la información completa o los primeros o últimos caracteres.
6. Haga clic en **Guardar**y, a continuación, en **Listo**.



En la siguiente figura se muestra una aplicación de ejemplo en la que la PII está enmascarada. La figura también muestra la notificación relacionada con el enmascaramiento de la PII.



Ventanas emergentes

Habilite o inhabilite la visualización de ventanas emergentes en la aplicación web interna o SaaS configurada con esta directiva cuando se accede a través de Citrix Enterprise Browser. De forma predeterminada, las ventanas emergentes están inhabilitadas en las páginas web. Valor predeterminado: bloquear siempre las ventanas emergentes.

Los usuarios finales deben usar la versión 126 o posterior de Citrix Enterprise Browser para acceder a las aplicaciones para las que está habilitada esta restricción.

Para habilitar la visualización de ventanas emergentes, lleve a cabo los siguientes pasos:

1. Cree o modifique una directiva de acceso. Para obtener más información, consulte Configurar directivas de acceso.
2. En **Acciones**, seleccione **Permitir con restricciones**.
3. Haga clic en **Ventanas emergentes** y, a continuación, en **Modificar**.
4. En la página **Parámetros de ventanas emergentes**, haga clic en **Permitir siempre las ventanas emergentes**.
5. Haga clic en **Guardar**y, a continuación, en **Listo**.

Impresión

Habilite o inhabilite la impresión de datos desde las aplicaciones web internas o SaaS configuradas con esta directiva cuando se acceda a través de Citrix Enterprise Browser. Valor predeterminado: Habilitado.

El siguiente mensaje aparece cuando un usuario final intenta imprimir contenido desde la aplicación para la que está habilitada la restricción de impresión.

> **Nota:**
>
> Si las restricciones de **impresión** y **administración de impresoras** están habilitadas en una directiva, la restricción de **impresión** tiene prioridad sobre la restricción de **administración de impresoras**.

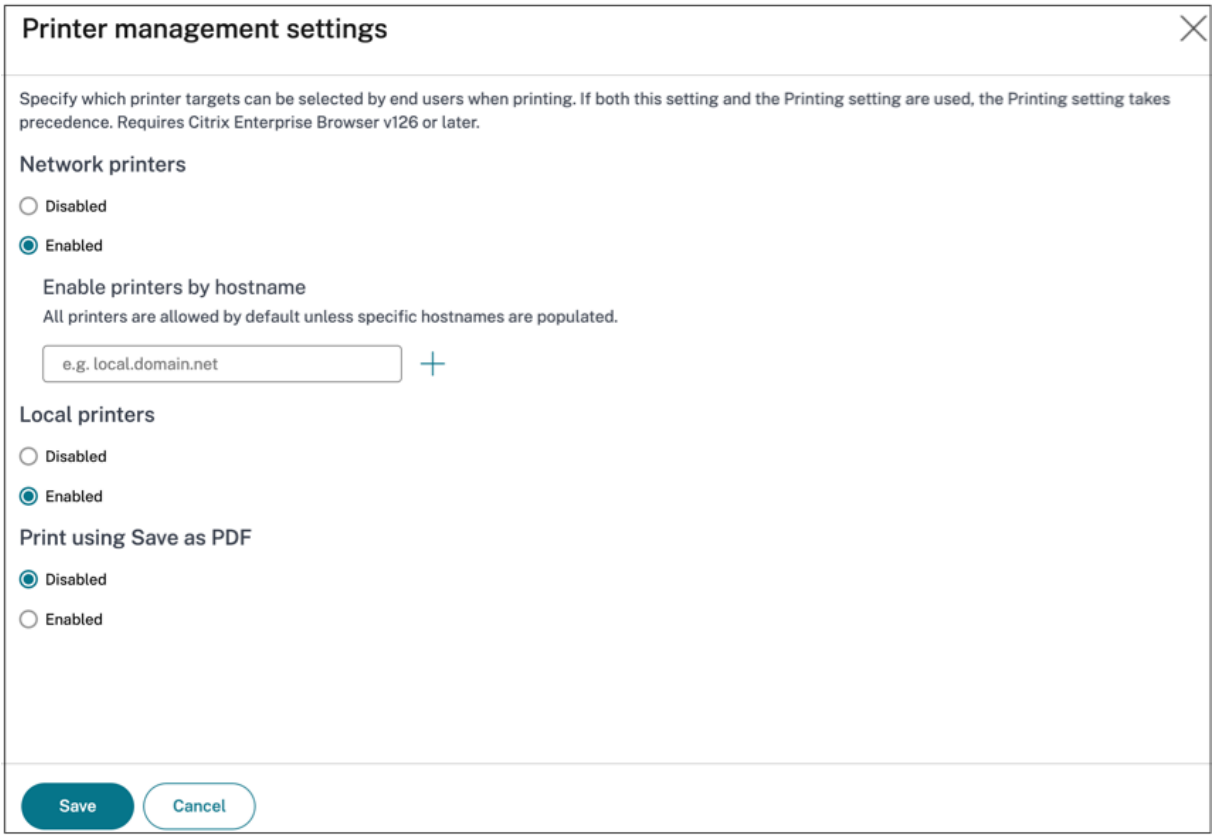
Administración de la impresora

Habilite o inhabilite la impresión de datos mediante las impresoras configuradas por el administrador desde las aplicaciones web internas o SaaS configuradas con esta directiva cuando se acceda a través de Citrix Enterprise Browser.

> **Nota:**
>
> - La restricción **de administración de impresoras** está disponible además de la restricción de **impresión** cuando la impresión está habilitada o inhabilitada.
>   Si las restricciones de **impresión** y **administración de impresoras** están habilitadas en una directiva de acceso, la restricción de **impresión** tiene prioridad sobre la restricción de **administración de impresoras**.
> - Los usuarios finales deben usar la versión 126 o posterior de Citrix Enterprise Browser para acceder a las aplicaciones para las que está habilitada esta restricción. De lo contrario, el acceso a la aplicación está restringido.

Para habilitar o inhabilitar las restricciones de impresión, lleve a cabo los siguientes pasos:

1. Cree o modifique una directiva de acceso. Para obtener más información sobre la creación de una directiva de acceso, consulte Configurar directivas de acceso.
2. En **Acciones**, seleccione **Permitir con restricciones**.
3. Haga clic en **Administración de impresoras** y, a continuación, en **Modificar**.



1. Seleccione las excepciones según sus requisitos.

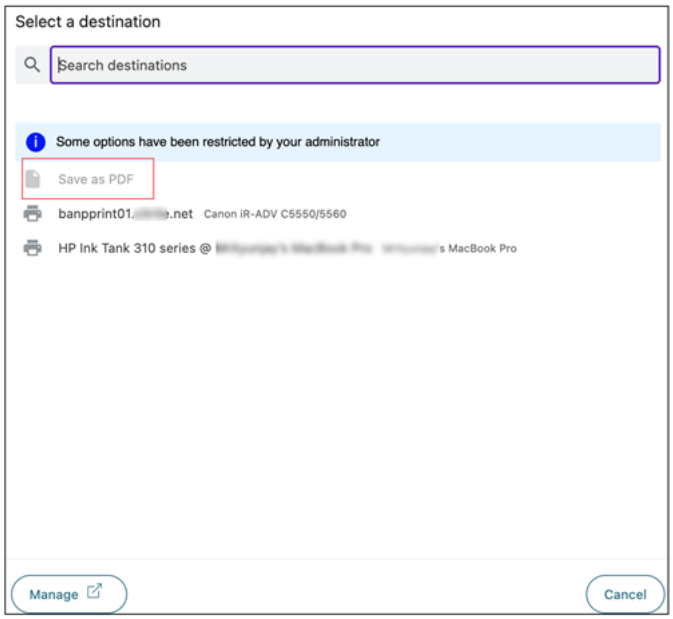
   - **Impresoras de red**: una impresora de red es una impresora que puede conectarse a una red y ser utilizada por varios usuarios.
     - **Inhabilitado:** la impresión desde cualquier impresora de la red está inhabilitada.
     - **Habilitado:** La impresión desde todas las impresoras de la red está habilitada. Si se especifican los nombres de host de las impresoras, se bloquean todas las demás impresoras de la red, excepto las especificadas.

     Nota: Las impresoras de red se identifican por sus nombres de host.
   - **Impresoras locales**: una impresora local es un dispositivo conectado directamente a un equipo individual a través de una conexión por cable. Esta conexión normalmente se facilita a través de USB, puertos paralelos u otras interfaces directas.
     - **Inhabilitado:** la impresión desde todas las impresoras locales está inhabilitada.
     - **Habilitado:** la impresión desde todas las impresoras locales está habilitada.
   - **Imprimir con Guardar como PDF**
     - **Inhabilitado**: guardar el contenido de la aplicación en formato PDF está inhabilitado.
     - **Habilitado:** el almacenamiento del contenido de la aplicación en formato PDF está habilitado.

2. Haga clic en **Save**.

Si una impresora de red está inhabilitada, el nombre específico de la impresora aparecerá atenuado cuando intente seleccionar la impresora en el campo **Destino**.

Además, si la opción **Imprimir con Guardar como PDF** está desactivada, al hacer clic en el enlace **Ver más** del campo **Destino**, la opción **Guardar como PDF** aparece atenuada.



Captura de pantalla

Habilite o inhabilite la capacidad de capturar las pantallas desde la aplicación web interna o SaaS con esta directiva cuando se acceda a través de Citrix Enterprise Browser mediante cualquiera de los programas o aplicaciones de captura de pantalla. Si un usuario intenta capturar la pantalla, se captura una pantalla en blanco. Valor predeterminado: Habilitado.

Restricción de carga por tipo de archivo

Habilite o inhabilite la capacidad del usuario para descargar un tipo de MIME (archivo) específico desde la aplicación web interna o SaaS con esta directiva cuando acceda a través de Citrix Enterprise Browser.

> **Nota:**
>
> - La **restricción de carga por tipo de archivo** está disponible además de la restricción de **carga**.
> - Si tanto la **carga** como la **restricción de carga por tipo de archivo** están habilitadas en

> una directiva, la restricción de **carga** tiene prioridad sobre la **restricción de carga por tipo de archivo**.
> - Los usuarios finales deben usar la versión 126 o posterior de Citrix Enterprise Browser para acceder a las aplicaciones para las que está habilitada esta restricción. De lo contrario, el acceso a la aplicación está restringido.

Para habilitar o inhabilitar la carga de tipos MIME, lleve a cabo los siguientes pasos:

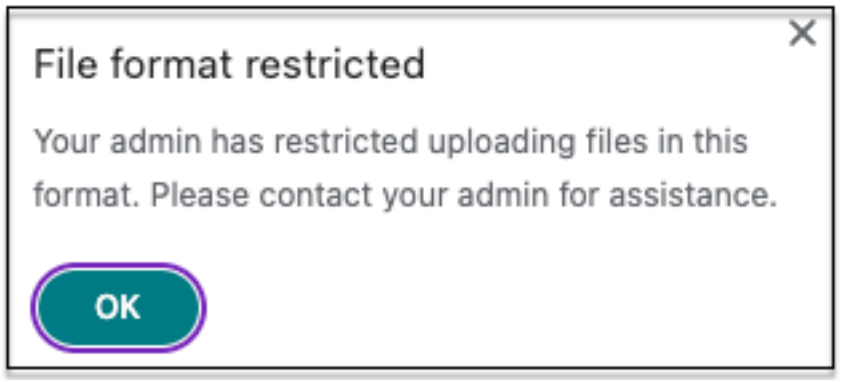
1. Cree o modifique una directiva de acceso. Para obtener más información, consulte Crear directivas de acceso.
2. En **Acciones**, seleccione **Permitir con restricciones**.
3. Haga clic en **Restricción de carga por tipo de archivo** y, a continuación, en **Modificar**.
4. En la página de **configuración de restricción de carga por tipo de archivo**, seleccione una de las siguientes opciones:

   Permitir todas las cargas con excepciones: carga todos los archivos excepto los tipos seleccionados.
   Bloquear todas las cargas con excepciones: bloquea la carga de todos los tipos de archivos, excepto los seleccionados.
5. Si el tipo de archivo no existe en la lista, haga lo siguiente:

   a) Haga clic en **Agregar tipos MIME personalizados**.
   b) En **Agregar tipos MIME**, introduzca el tipo MIME en el formato `category/subcategory <extension>`. Por ejemplo, image/png.
   c) Haga clic en **Listo**.

   El tipo MIME ahora aparece en la lista de excepciones.

Cuando un usuario final intenta cargar un tipo de archivo restringido, Citrix Enterprise Browser muestra un mensaje de advertencia.



Cargas

Habilite o inhabilite la capacidad del usuario de cargar contenido en la aplicación web interna o SaaS configurada con esta directiva cuando acceda a través de Citrix Enterprise Browser. Valor predeterminado: Habilitado.

> **Nota:**
>
> Si tanto la **carga** como la **restricción de carga por tipo de archivo** están habilitadas en una directiva, la restricción de **carga** tiene prioridad sobre la **restricción de carga por tipo de archivo**.

Marca de agua

Habilite o inhabilite la marca de agua en la pantalla del usuario que muestra el nombre de usuario y la dirección IP de la máquina del usuario. Valor predeterminado: Inhabilitado.

Cámara web

Pregunte o no a los usuarios cada vez que accedan a la cámara web en la aplicación web interna o SaaS configurada con esta directiva cuando accedan a través de Citrix Enterprise Browser. Valor predeterminado: Preguntar siempre.

Los usuarios finales deben usar la versión 126 o posterior de Citrix Enterprise Browser para acceder a las aplicaciones para las que está habilitada la restricción de **cámara web**.

Para permitir la cámara web en todo momento sin que se le pregunte, lleve a cabo los siguientes pasos:

1. Cree o modifique una directiva de acceso. Para obtener más información, consulte Configurar directivas de acceso.
2. En **Acciones**, seleccione **Permitir con restricciones**.
3. Haga clic en **Cámara web** y, a continuación, en **Modificar**.
4. En la página **Parámetros de cámara web**, haga clic en **Permitir siempre el acceso**.
5. Haga clic en **Guardar**y, a continuación, en **Listo**.

> **Nota:**
>
> - Si la restricción de cámara web está habilitada en la directiva de Secure Private Access, Citrix Enterprise Browser mostrará la configuración **Permitir**.
> - Si la opción es **Preguntar siempre** en la directiva de Secure Private Access, la configuración aplicada en Citrix Enterprise Browser varía en función de si se utiliza o no Global App Configuration Service (GACS) para administrar Citrix Enterprise Browser.

  - Si se usa GACS, la configuración de GACS se aplica en Citrix Enterprise Browser.
  - Si no se usa GACS, Citrix Enterprise Browser muestra el parámetro **Preguntar**.

- Actualmente, Secure Private Access no admite el bloqueo de la cámara web. Si necesita bloquear la cámara web, debe hacerlo a través de GACS.

Para obtener más información acerca de GACS, consulte Administrar Citrix Enterprise Browser mediante Global App Configuration Service.

Restricción del portapapeles para grupos de seguridad

Puede habilitar el acceso al portapapeles para un grupo de aplicaciones designado mediante la restricción de **grupos de seguridad (Aplicaciones > Grupos de seguridad)**. A los grupos de seguridad se les asigna un conjunto de aplicaciones en las que se pueden realizar las operaciones de copiar y pegar. Para habilitar el acceso al portapapeles dentro de las aplicaciones de un grupo de seguridad, solo debe tener una directiva de acceso configurada con la acción **permitir** o **permitir con restricciones** sin seleccionar ninguna configuración de acceso.

- Cuando la restricción de **grupos de seguridad** está habilitada, no puede copiar ni pegar datos entre aplicaciones de diferentes grupos de seguridad. Por ejemplo, si la aplicación "ProdDocs" pertenece al grupo de seguridad "SG1"y la aplicación "Edocs"pertenece al grupo de seguridad "SG2", no puede copiar ni pegar contenido de "Edocs"en "ProdDocs"aunque la restricción de **copiar**/**pegar** esté habilitada para ambos grupos.
- Para las aplicaciones que no forman parte de un grupo de seguridad, puede crear una directiva de acceso con la acción **permitir con restricciones** y seleccionar las restricciones (**copiar**, **pegar**o **portapapeles**). En este caso, la aplicación no forma parte de un grupo de seguridad y, por lo tanto, la restricción de **copiar** y **pegar** se puede aplicar a esa aplicación.

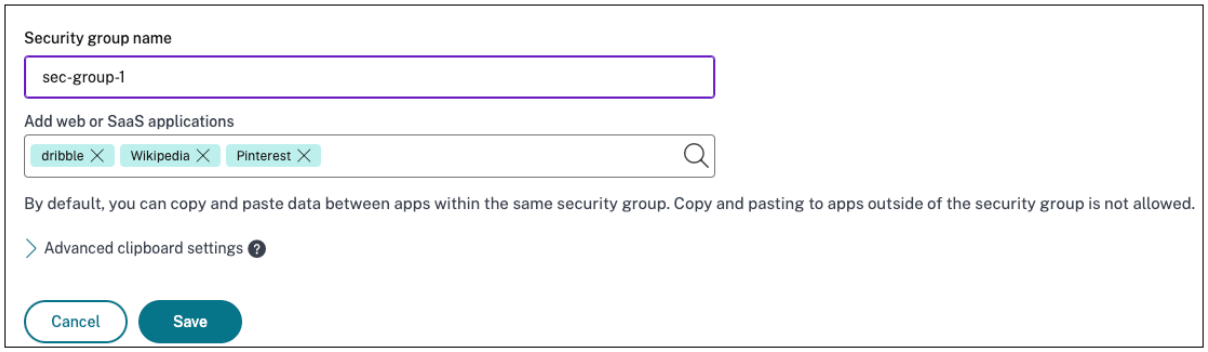
Nota:

También puede restringir el acceso al portapapeles para las aplicaciones a las que se accede mediante Citrix Enterprise Browser a través de Global App Configuration Service (GACS). Si utiliza el GACS para administrar Citrix Enterprise Browser, utilice la opción **Habilitar portapapeles de espacio aislado** para administrar el acceso al portapapeles. Cuando se restringe el acceso al portapapeles a través de GACS, se aplica a todas las aplicaciones a las que se accede mediante Citrix Enterprise Browser. Para obtener más información acerca de GACS, consulte Administrar Citrix Enterprise Browser mediante Global App Configuration Service.

Para crear un grupo de seguridad, lleve a cabo los siguientes pasos:

1. En la consola de Secure Private Access, haga clic en **Aplicaciones** y, a continuación, en **Grupos de seguridad**.

2. Haga clic en **Agregar un nuevo grupo de seguridad**.

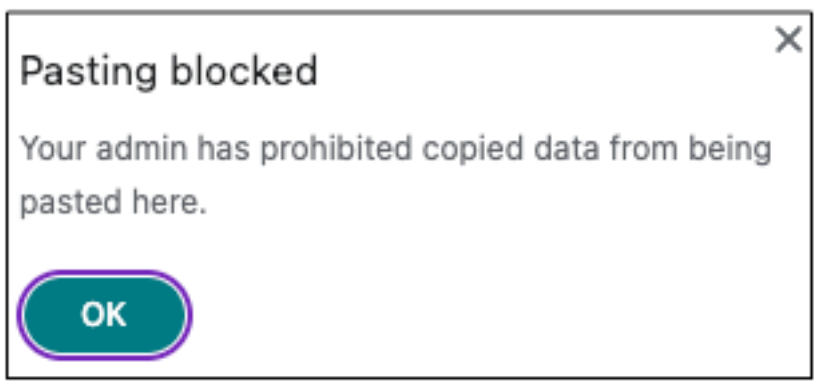


1. Introduzca un nombre para el grupo de seguridad.
2. En **Agregar aplicaciones web o SaaS**, elija las aplicaciones que desea agrupar para habilitar el control de copiar y pegar. Por ejemplo, Wikipedia, Pinterest y Dribble.
3. Haga clic en **Save**.

Para obtener más información sobre la configuración avanzada del portapapeles, consulte Habilitar los controles de copiar y pegar para aplicaciones nativas y aplicaciones no publicadas.

Cuando los usuarios finales inician estas aplicaciones (Wikipedia, Pinterest y Dribble) desde Citrix Workspace, deben poder compartir datos (copiar y pegar) de una aplicación con las demás aplicaciones del grupo de seguridad. La operación de copiar y pegar se produce independientemente de otras restricciones de seguridad que ya estén habilitadas para las aplicaciones.

Sin embargo, los usuarios finales no pueden copiar y pegar el contenido de sus aplicaciones locales en sus máquinas o aplicaciones no publicadas en estas aplicaciones designadas y viceversa. La siguiente notificación aparece cuando el contenido se copia de las aplicaciones designadas en otra aplicación:



> **Nota:**
>
> Puede habilitar los controles de copiar/pegar contenido de aplicaciones locales en las máquinas de los usuarios o aplicaciones no publicadas mediante las opciones de la sección **Configuración**

> **avanzada del portapapeles**. Para obtener más información, consulte Habilitar los controles de copiar y pegar para aplicaciones nativas y aplicaciones no publicadas.

Habilitar copiar/pegar a nivel granular

Puede habilitar el acceso al portapapeles a nivel granular dentro de las aplicaciones de un grupo designado. Puede hacerlo creando directivas de acceso para las aplicaciones y habilitando la restricción de **copiar**/**pegar** según sus necesidades.

> **Nota:**
>
> Asegúrese de que la directiva de acceso específica que ha creado para el acceso al portapapeles de nivel granular tenga una prioridad más alta que la directiva que ha creado para los grupos de seguridad.

Ejemplo:

Tenga en cuenta que ha creado un grupo de seguridad con tres aplicaciones, a saber, Wikipedia, Pinterest y Dribble.

Ahora, quiere restringir el pegado de contenido de Wikipedia o Dribble en Pinterest. Para hacerlo, lleve a cabo los siguientes pasos:

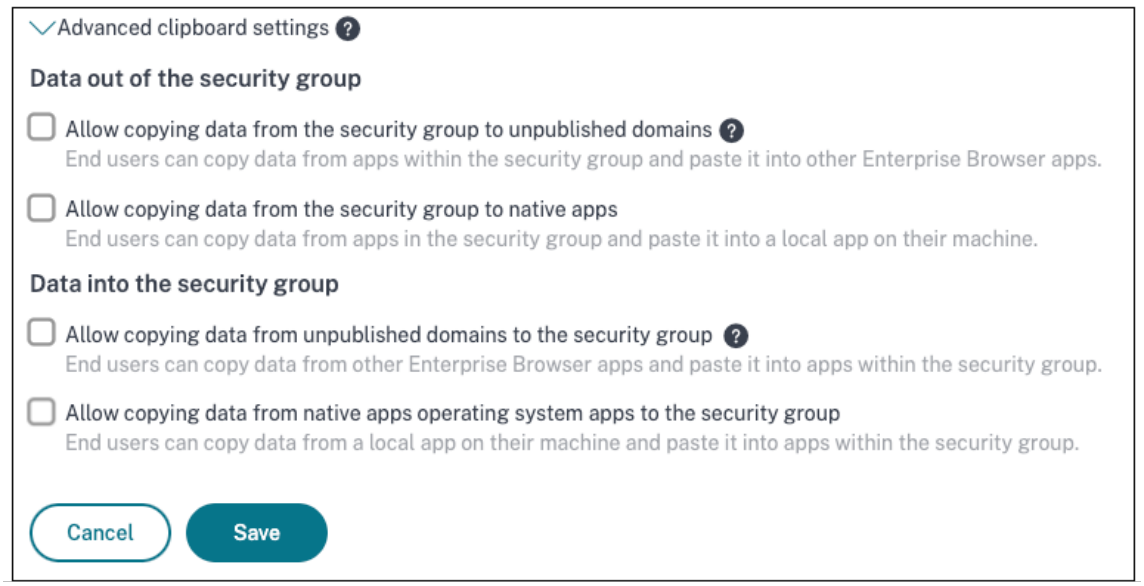
1. Cree o modifique una directiva de acceso asignada a la aplicación `Pinterest`. Para obtener más información sobre la creación de una directiva de acceso, consulte Configurar directivas de acceso.
2. En **Acciones**, seleccione **Permitir con restricciones**.
3. Seleccione **Pegar**.

Aunque Pinterest forma parte de un grupo de seguridad que también incluye Wikipedia y Dribble, los usuarios no pueden copiar contenido de Wikipedia o Dribble en Pinterest debido a la directiva de acceso asociada a Pinterest en la que está habilitada la restricción de **pegar**.

Habilitar los controles de copiar/pegar para aplicaciones nativas y aplicaciones no publicadas

1. Cree un grupo de seguridad. Para obtener más información, consulte Grupos de seguridad del portapapeles para restricciones de copiar y pegar.

2. Amplíe la **configuración avanzada del portapapeles**.



3. Seleccione las siguientes opciones según sus necesidades:

   - **Permitir la copia de datos del grupo de seguridad a dominios no publicados**: habilite la copia de datos de las aplicaciones de los grupos de seguridad en las aplicaciones que no están publicadas en Secure Private Access.
   - **Permitir la copia de datos del grupo de seguridad a las aplicaciones nativas**: habilite la copia de datos de las aplicaciones de los grupos de seguridad en las aplicaciones locales de sus máquinas.
   - **Permitir la copia de datos de los dominios no publicados al grupo de seguridad**: habilite la copia de datos de las aplicaciones no publicadas a través de Secure Private Access en las aplicaciones de los grupos de seguridad.
   - **Permitir la copia de datos de las aplicaciones nativas, el sistema operativo y el grupo de seguridad**: habilite la copia de datos de las aplicaciones locales de las máquinas en las aplicaciones.

Problemas conocidos

- La tabla de redirección de (**Parámetros > Dominio de la aplicación**) conserva los dominios de una aplicación eliminada. Por lo tanto, estas aplicaciones también se consideran aplicaciones publicadas en Secure Private Access. Si se accede a estos dominios directamente desde Citrix Enterprise Browser, se inhabilita la función de copiar y pegar en estas aplicaciones, independientemente de las opciones que haya seleccionado en la **configuración avanzada del portapapeles**.

  Por ejemplo, supongamos el siguiente escenario:

  - Ha eliminado una aplicación llamada Jira2 (`https://test.citrite.net`) que formaba parte de un grupo de seguridad.
  - Ha habilitado la opción **Permitir la copia de datos del grupo de seguridad en dominios no publicados**.

  En este escenario, si el usuario intenta copiar datos de esta aplicación en otra aplicación del mismo grupo de seguridad, se inhabilita el control de pegado. Se muestra al usuario una notificación sobre lo mismo.

- En el caso de una aplicación SaaS, se puede denegar el acceso a la aplicación si la aplicación está configurada con una directiva de acceso con la acción **Denegar acceso.** Los usuarios finales aún pueden acceder a la aplicación porque el tráfico de la aplicación no se canaliza a través de Secure Private Access. Además, si la aplicación forma parte del grupo de seguridad, la configuración del grupo de seguridad no se respeta y, por lo tanto, no puede copiar ni pegar contenido de la aplicación.

Implemente el Secure Private Access como un clúster

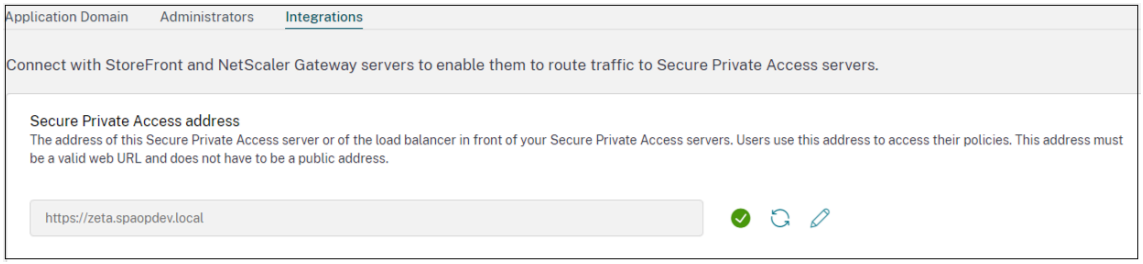
August 26, 2024

La solución local Secure Private Access se puede implementar como un clúster para proporcionar alta disponibilidad, alto rendimiento y escalabilidad. Se recomienda implementar nodos de Secure Private Access independientes para despliegues grandes (por ejemplo, más de 5000 usuarios).

Creación de nodos de Secure Private Access

- Cree un nuevo sitio de Secure Private Access. Para obtener más información, consulte Configurar un sitio de Secure Private Access.
- Agregue la cantidad requerida de nodos del clúster al sitio de Secure Private Access. Para obtener más información, consulte Configurar el Secure Private Access uniéndose a un sitio existente.
- En cada nodo de Secure Private Access, configure los mismos certificados de servidor. El nombre común o el nombre alternativo del sujeto del certificado deben coincidir con el FQDN del balanceador de cargas.
- Al configurar el primer nodo en Secure Private Access, utilice los nombres del balanceador de cargas. Para agregar los nodos siguientes, especifique la dirección de la base de datos en la

ficha Integraciones y ejecute manualmente el script de la base de datos. Para obtener más información sobre la actualización de la base de datos mediante scripts, consulte Actualizar la base de datos mediante scripts.



Configuración del balanceador de carga

No hay requisitos de configuración de equilibrio de carga específicos para la configuración del clúster de Secure Private Access. Si utiliza NetScaler como balanceador de cargas, tenga en cuenta lo siguiente:

- Los FQDN utilizados para acceder a StoreFront se incluyen en el campo DNS como nombre alternativo del sujeto (SAN). Si usa un balanceador de carga, incluya tanto el FQDN del servidor individual como el FQDN del balanceador de carga. Esto se aplica a los certificados SSL. Para Secure Private Access, basta con configurar el balanceador de cargas. Para obtener más información, consulte Equilibrio de carga con NetScaler.
  Antes de configurar Secure Private Access, se debe configurar el almacén de StoreFront. Si usa un balanceador de carga, configure la URL base con el nombre del balanceador de carga y use HTTPS para una comunicación segura. Para obtener más información, consulte Proteger StoreFront con HTTPS.
- Se recomienda que los servicios de Secure Private Access se ejecuten como HTTPS, pero este no es un requisito obligatorio. Los servicios de Secure Private Access también se pueden implementar como HTTP.
- Se admite la descarga SSL o el puente SSL, por lo que se puede usar cualquier configuración de balanceador de cargas. Cuando utilice un puente SSL, asegúrese de configurar los mismos certificados de servidor en cada nodo de Secure Private Access. Además, el nombre común o el nombre alternativo del sujeto (SAN) del sujeto del certificado deben coincidir con el FQDN del balanceador de cargas. Además, la SAN debe configurarse en el servicio Load Balancer.
- El certificado SSL correcto está enlazado al servidor IIS y a NetScaler.
- Se utilizan sistemas de cifrado seguros.
- Los servicios de Secure Private Access (tanto de administración como de ejecución) no tienen estado, por lo que no es necesaria la persistencia.

- Los balanceadores de carga (por ejemplo, NetScaler) tienen monitores integrados predeterminados (sondas) para los servidores back-end. Si debe configurar un monitor (sonda) basado en HTTP personalizado para los servidores locales de Secure Private Access, se puede usar el siguiente punto final:

  `/secureAccess/health`

  Respuesta esperada:

  ```
  Http status code: 200 OK

  Payload:

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

  Para obtener más información sobre la configuración de un balanceador de cargas de NetScaler, consulte Configurar el balanceo de cargas básico.

Cree un monitor para un Secure Private Access

Utilice el siguiente comando de la CLI para crear un monitor para el Secure Private Access.

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

Tras crear un monitor, vincule el certificado al monitor.

Para obtener más información sobre la creación de monitores mediante la interfaz de usuario de NetScaler, consulte Crear monitores.

Desinstalar Secure Private Access

August 26, 2024

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

1. Seleccione **Citrix Virtual Apps and Desktops 7 2405 —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 plug-in 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 **Parámetros** y después en la ficha **Integraciones**.
3. Haga clic en **Descargar script** en la sección URL del almacén de StoreFront.

Eliminar el plug-in Secure Private Access de la configuración del almacén de StoreFront

Tras desinstalar Secure Private Access, debe eliminar el plug-in 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
```

Actualizar

August 26, 2024

Puede actualizar sus implementaciones de Secure Private Access a una versión más reciente sin tener que configurar primero máquinas o sitios nuevos. Antes de actualizar, le recomendamos que cree las instantáneas o guarde las configuraciones. Para iniciar una actualización, ejecute el instalador desde la nueva versión para actualizar el plug-in Secure Private Access previamente instalado.

Secuencia de actualización

La secuencia de actualización es la siguiente:

1. Puede actualizar Secure Private Access a través del Delivery Controller o mediante el icono de Secure Private Access dedicado de la interfaz de usuario del instalador en función de cómo instaló Secure Private Access originalmente.

    - Si ha instalado Secure Private Access mediante Delivery Controller, no podrá actualizar el componente Secure Private Access por sí solo. En su lugar, debe actualizar todos los componentes. Para obtener información más detallada, consulte Actualizar una implementación.
    - Si ha instalado Secure Private Access a través del icono de Secure Private Access dedicado, puede actualizarlo de forma independiente. Para obtener más información, consulte Actualizar el instalador de Secure Private Access.

    > **Nota:**
    >
    > Se recomienda instalar Secure Private Access a través del Delivery Controller para los entornos POC. Sin embargo, para los entornos de producción, se recomienda utilizar el instalador dedicado para poder adaptar las nuevas funciones o características.

2. Ejecute los scripts de la base de datos. Para obtener más información, consulte Actualizar la base de datos mediante scripts.
3. Vuelva a ejecutar la configuración de StoreFront. Descargue los scripts de StoreFront desde **Parámetros > Configuración** y ejecute los scripts en las máquinas de StoreFront correspondientes. Para obtener más información, consulte Modificar la configuración de integración.

    > **Nota:**
    >
    > Si no ejecuta los scripts, los puntos finales no se activan.

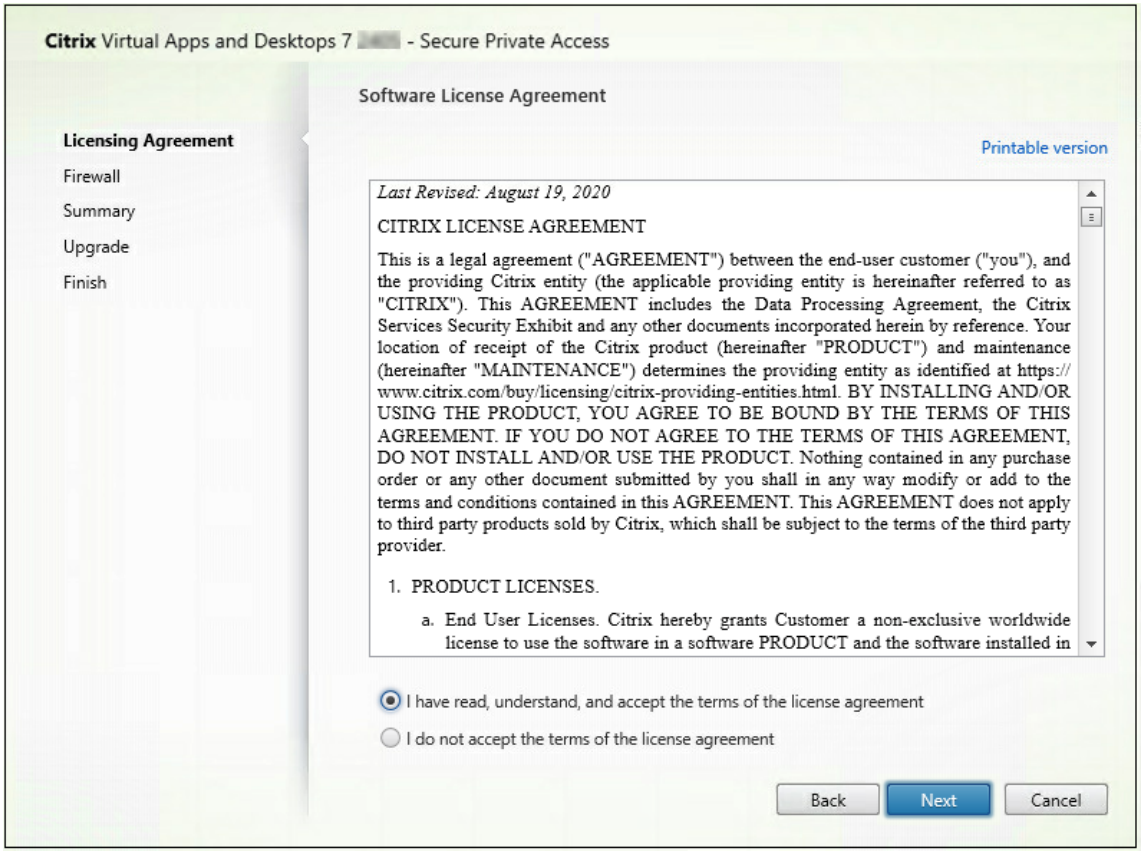
4. (Opcional) Ejecute el script de NetScaler Gateway. Para obtener más información, consulte NetScaler Gateway.

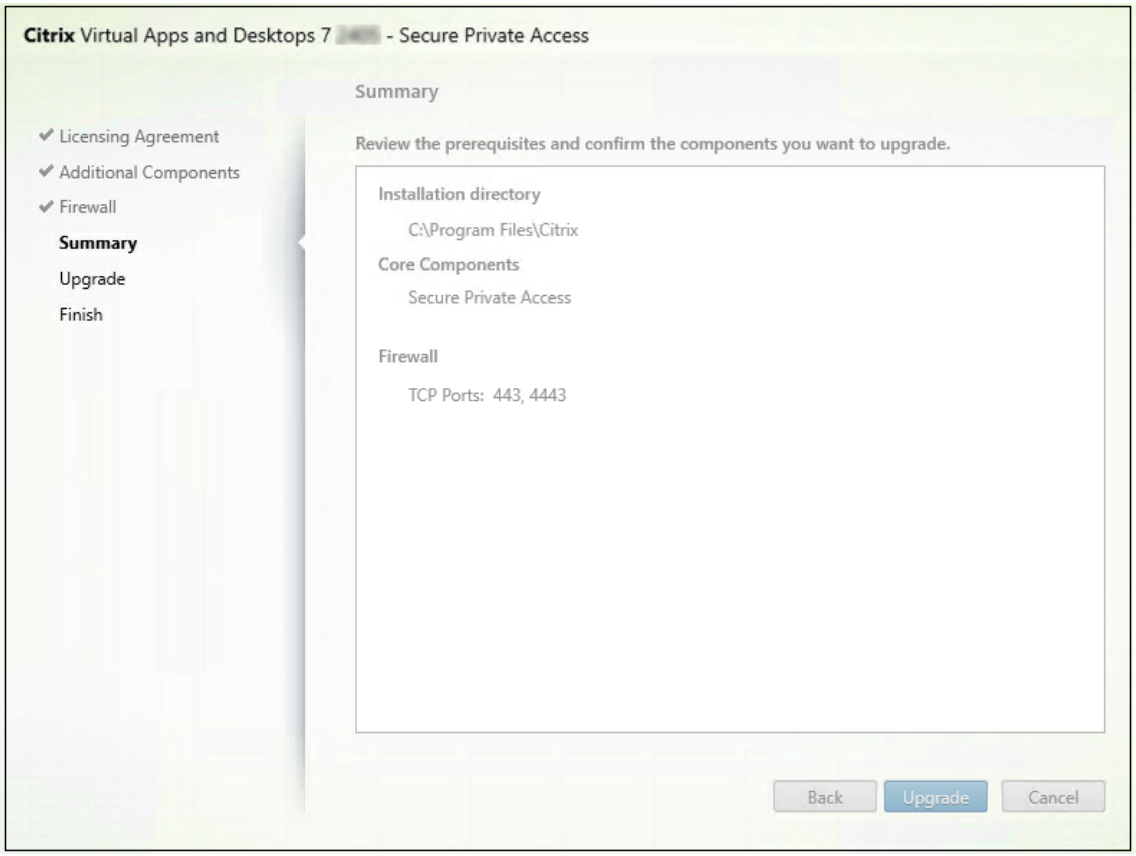
Actualice su instalador de Secure Private Access

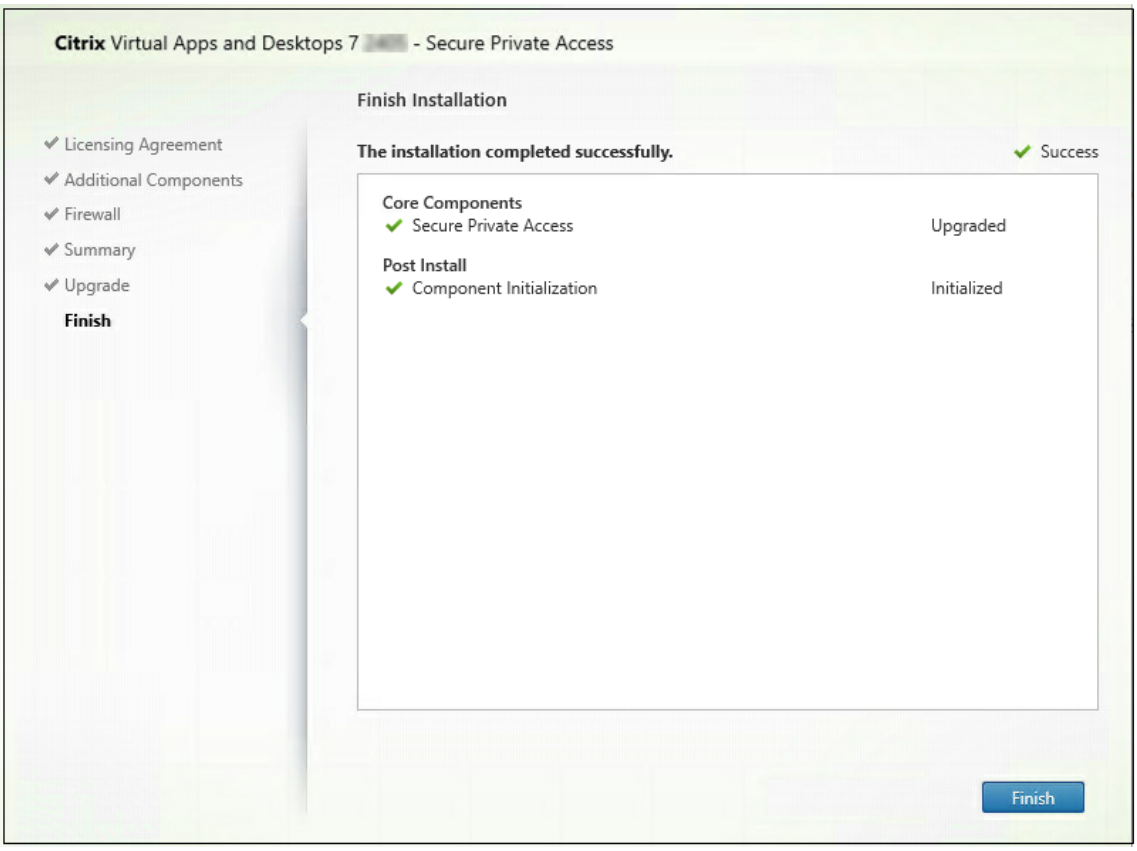
August 26, 2024

1. Descargue el instalador de Citrix Secure Private Access 2405 desde https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/.

2. Ejecute el archivo .exe como administrador en una máquina unida a un dominio.
3. Siga las instrucciones que aparecen en pantalla para completar la instalación.







> **Importante:**
>
> Tras actualizar el instalador a la versión 2405, debe volver a ejecutar el script de StoreFront para que los detalles del nuevo punto final estén disponibles.

Siguientes pasos

- Configurar Secure Private Access
- Configurar NetScaler Gateway
- Configurar aplicaciones
- Configurar directivas de acceso para las aplicaciones

Actualizar la base de datos mediante scripts

August 26, 2024

Puede usar la herramienta de configuración de administración para descargar los scripts de actualización de la base de datos para el plug-in 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>
   ```

Administrar

August 26, 2024

Después de instalar Secure Private Access, puede modificar la configuración en la página Parámetros. Puede administrar el enrutamiento de los dominios de aplicaciones y los administradores y modificar la configuración de integración.

Para modificar la configuración, debe iniciar sesión en la consola de administración de Secure Private Access con una cuenta de administrador de Secure Private Access.

Para obtener más información sobre cómo actualizar o modificar la configuración, consulte los siguientes temas:

- Administrar el enrutamiento de los dominios de las aplicaciones
- Administrar administradores
- Modificar la configuración de integración

Administrar la configuración después de la instalación

August 26, 2024

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

Administrar administradores

Puede ver la lista de administradores y también agregar administradores desde la página **Parámetros > 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 puede agregar grupos de administradores para que se habilite el acceso para todos los administradores de ese grupo.

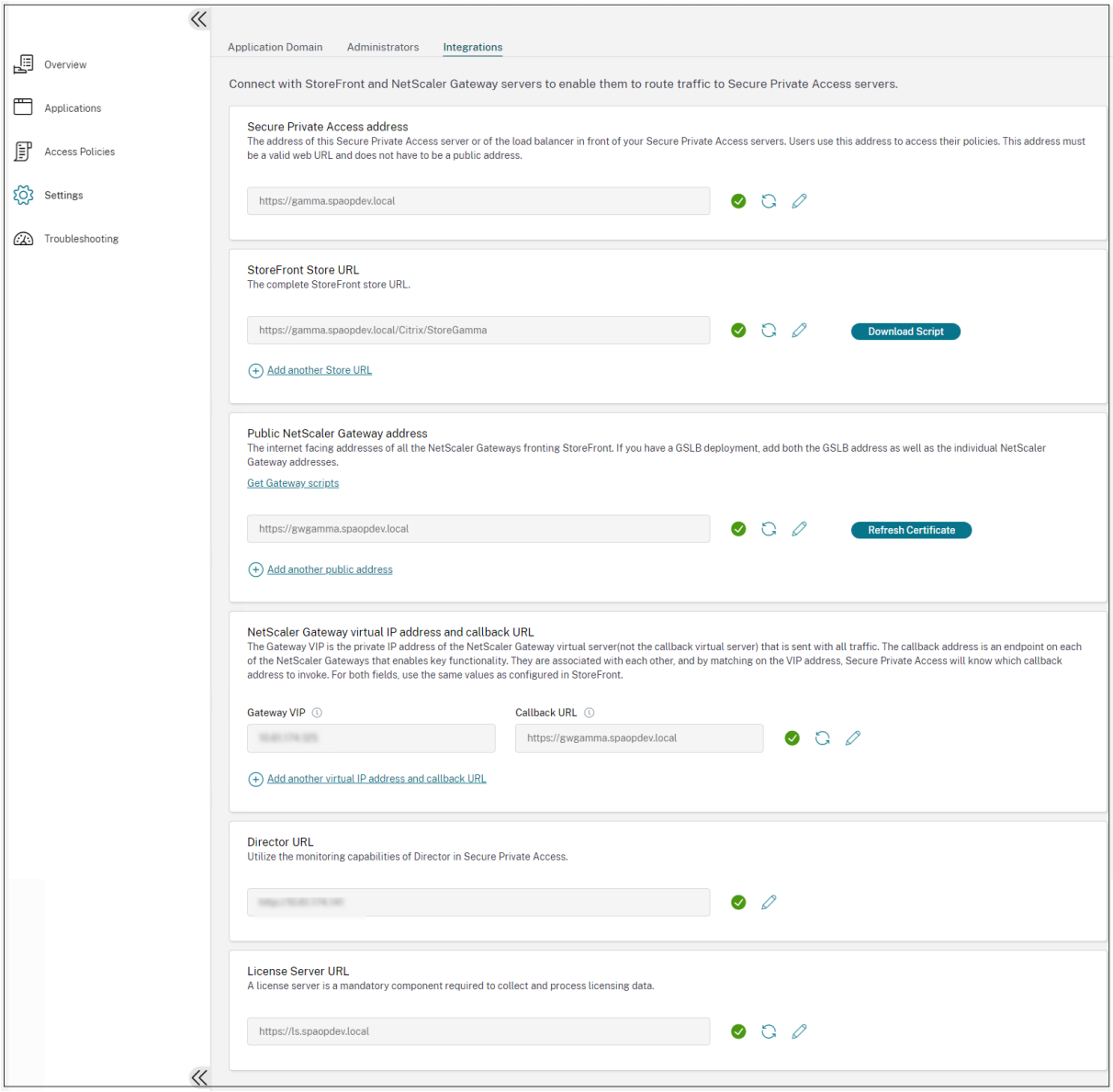
1. En la página **Administradores**, haga clic en **Agregar**.
2. En **Dominio**, seleccione el dominio al que debe agregarse este administrador.
3. En **Usuarios o grupo de usuarios**, seleccione el usuario o grupo al que pertenece este usuario.
4. En **Tipo de administrador**, seleccione el tipo de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

Modificar la configuración de integración

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 **Parámetros > Integraciones**.
2. Haga clic en el icono de edición en línea con la configuración que desee modificar y actualizar la entrada.
3. Haga clic en el icono 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.



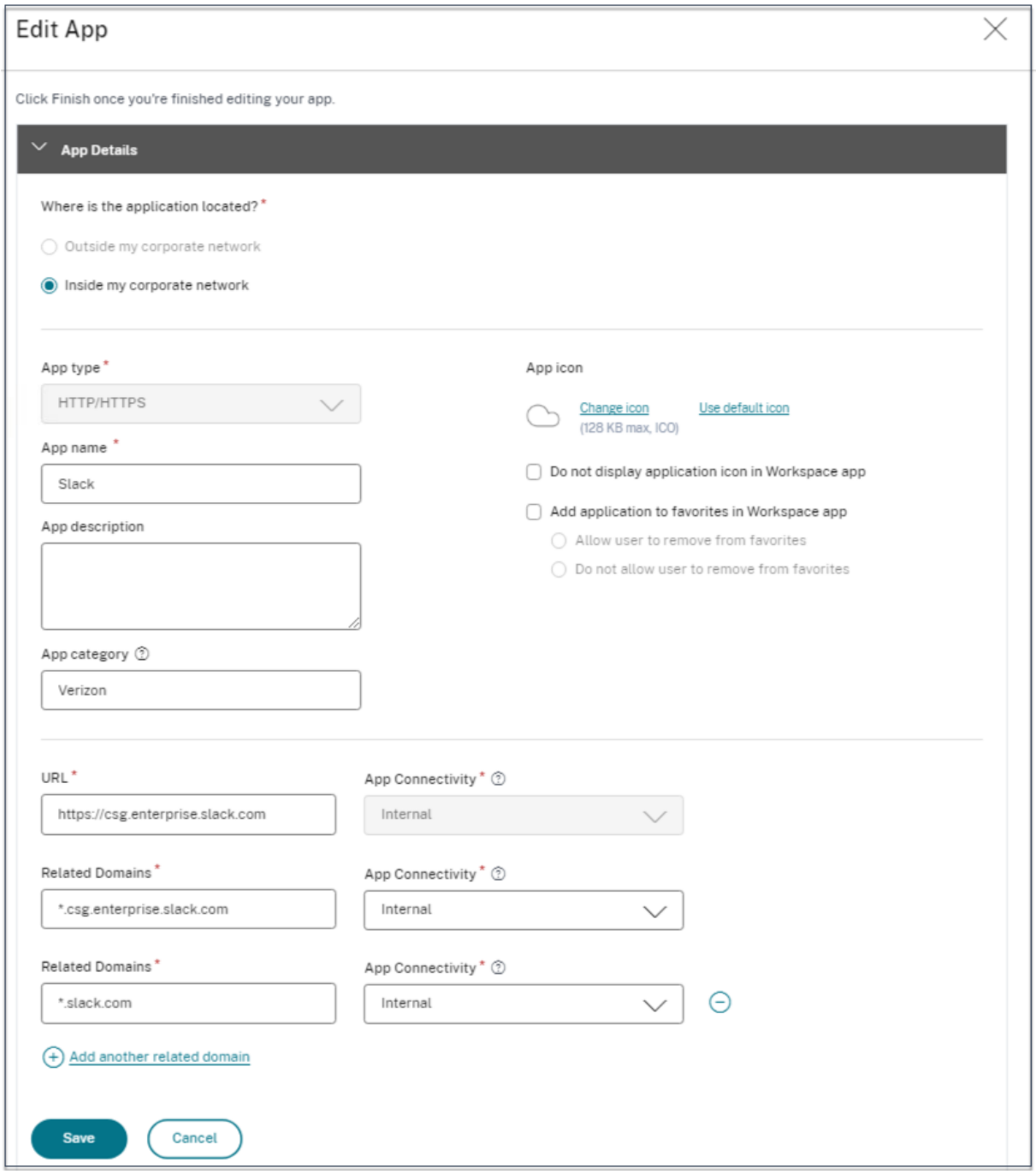
Administrar aplicaciones y directivas

August 26, 2024

Tras configurar las aplicaciones y las directivas de acceso, puede editarlas si es necesario.

Modificar una aplicación

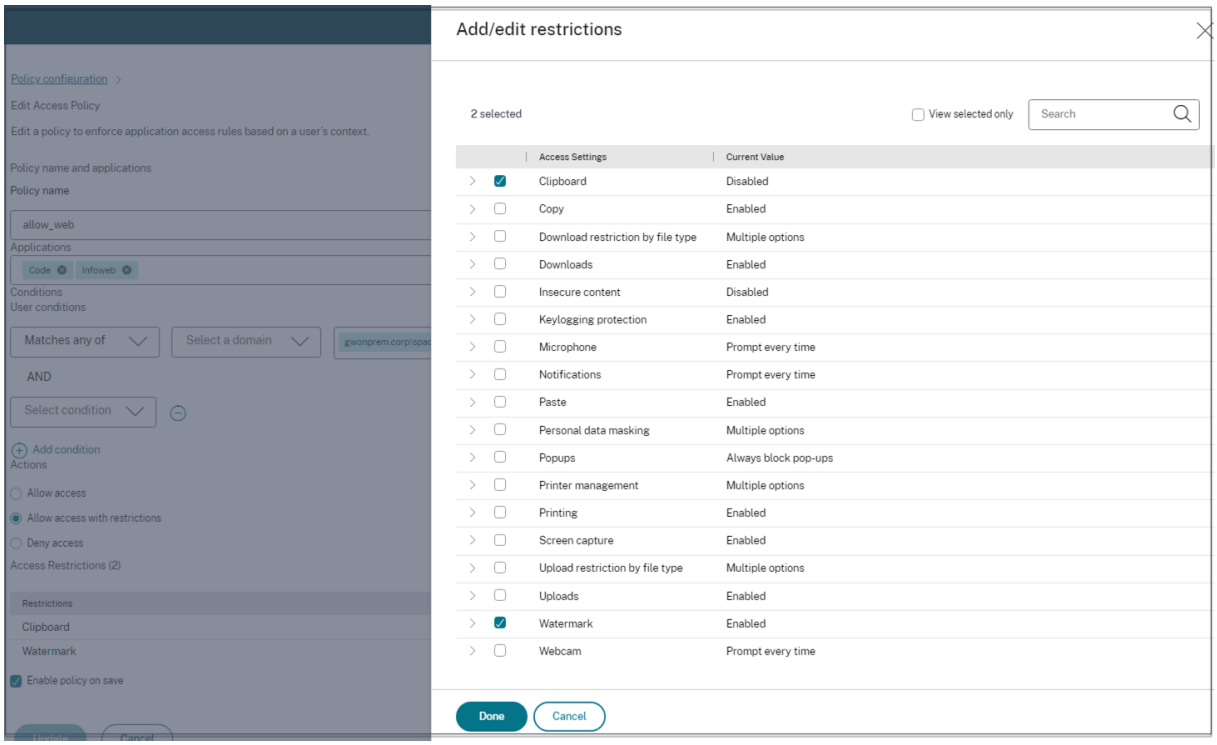
1. En la consola de administración de Secure Private Access, haga clic en **Aplicaciones**.
2. Haga clic en el botón de puntos suspensivos en la línea de la aplicación que desea modificar y después haga clic en **Editar aplicación**.
3. Edita los detalles de la aplicación.
4. Haga clic en **Save**.



Editar una directiva de acceso

1. En la consola de administración de Secure Private Access, haga clic en **Directivas de acceso**.
2. Haga clic en el botón de puntos suspensivos correspondiente a la directiva que desea modificar y después haga clic en **Editar directiva de acceso**.
3. Edite los detalles de la directiva.

4. Haga clic en **Update**.



Sitios web no autorizados

August 26, 2024

Las aplicaciones (intranet o Internet) que no están configuradas en Secure Private Access se consideran "sitios web no autorizados". De forma predeterminada, Secure Private Access deniega el acceso a todas las aplicaciones web de la intranet si no hay aplicaciones ni directivas de acceso configuradas para esas aplicaciones.

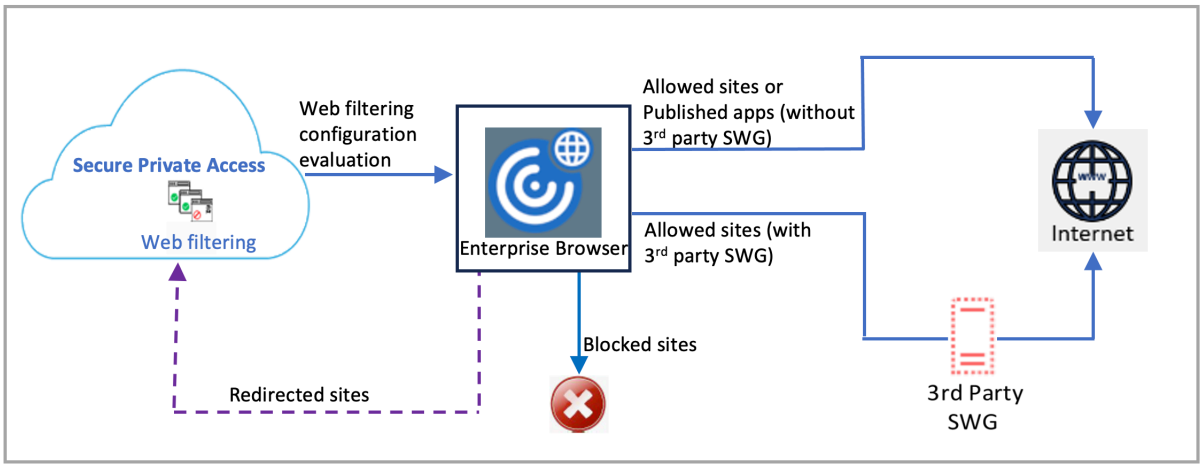
Para todas las demás URL de Internet o aplicaciones SaaS que no tengan una aplicación configurada, los administradores pueden usar la ficha **Parámetros > Sitios web no autorizados** de la consola de administración para permitir o denegar el acceso a través de Citrix Enterprise Browser.

> **Nota:**
>
> De forma predeterminada, los parámetros están configurados para PERMITIR el acceso a todas las URL de Internet o aplicaciones SaaS a través de Citrix Enterprise Browser.

Cómo funcionan los sitios web no autorizados

1. La comprobación del análisis de URL se realiza para determinar si la URL es una URL de servicio Citrix.
2. A continuación, se comprueba la URL para determinar si se trata de una URL de aplicación SaaS o web empresarial.
3. A continuación, se comprueba la URL para determinar si está identificada como una URL bloqueada o si se puede permitir el acceso a la URL.

En la siguiente ilustración, se explica el flujo de tráfico del usuario final.



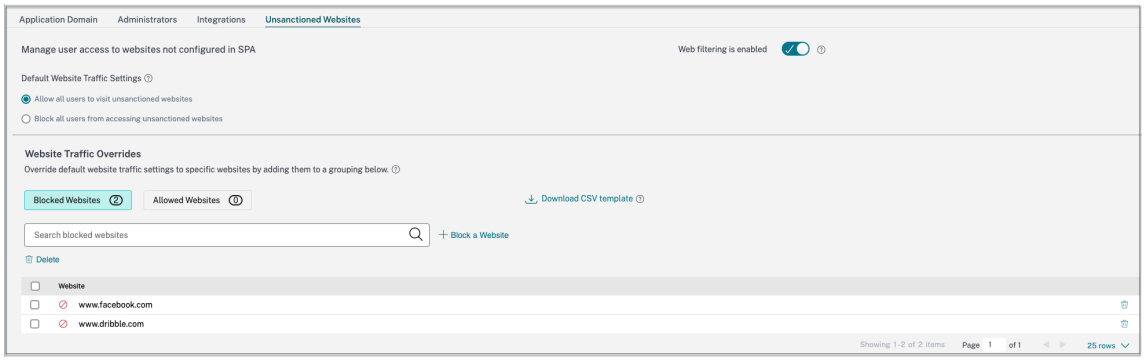
Cuando llega una solicitud, se llevan a cabo las comprobaciones siguientes y se toman las medidas correspondientes:

1. ¿La solicitud corresponde a alguna entrada de la lista global de sitios permitidos?
    a) Si corresponde, el usuario puede acceder al sitio web solicitado.
    b) Si no corresponde, se consultan las listas de sitios web.
2. ¿La solicitud corresponde a alguna entrada de la lista de sitios web configurados?
    a) Si corresponde, la secuencia siguiente determina la acción a realizar.
        i. Bloquear
        ii. Permitir
    b) Si no corresponde, se aplica la acción predeterminada (PERMITIR). La acción predeterminada no se puede cambiar.

Configurar reglas para sitios web no autorizados

1. En la consola de administración de Secure Private Access, haga clic en **Parámetros > Sitios web no autorizados**.

   > **Nota:**
   >
   > - La función de filtrado web está habilitada de forma predeterminada y se permite el acceso a todas las URL de Internet no autorizadas.
   > - Puede cambiar la configuración para **Impedir que todos los usuarios accedan a sitios web no autorizados** para bloquear el acceso a cualquier URL de Internet a través de Citrix Enterprise Browser para todos los usuarios.

   También puede cambiar los parámetros de URL específicas agregándolas a sitios web bloqueados o sitios web permitidos.

   Por ejemplo, si has bloqueado el acceso a todas las URL no autorizadas de forma predeterminada y solo quieres permitir el acceso a unas cuantas URL de Internet específicas, puede hacerlo siguiendo estos pasos:

   a) Haga clic en la ficha **Sitios web permitidos** y después haga clic en **Permitir un sitio web**.

   b) Agregue la dirección del sitio web a la que se debe permitir el acceso. Puede agregar manualmente la dirección del sitio web o arrastrar y soltar un archivo CSV que contenga la dirección del sitio web.

   c) Haga clic en **Agregar una URL** y después en **Guardar**.

      La URL se añade a la lista de sitios web permitidos.

Flujo de usuarios finales

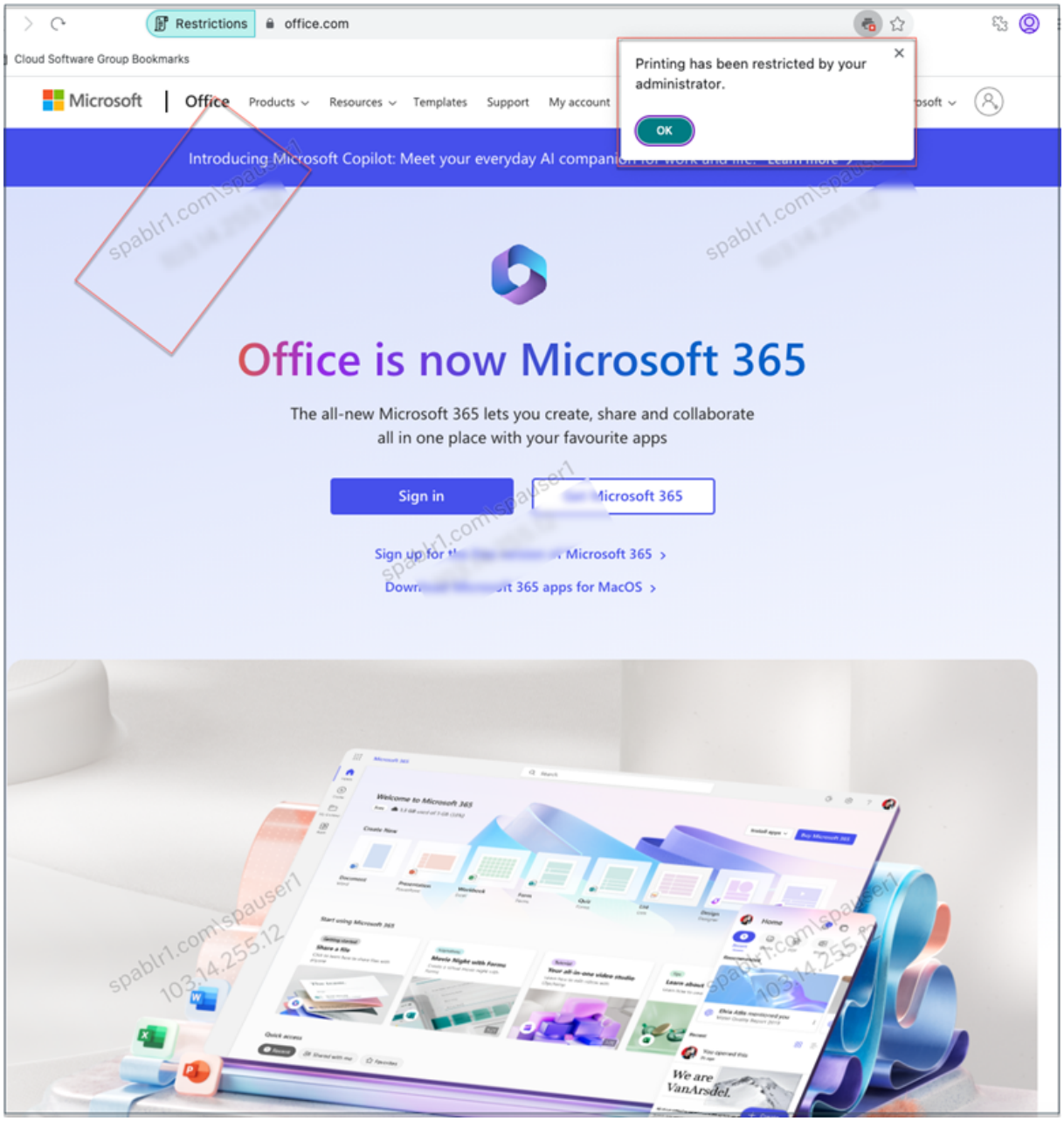
August 26, 2024

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.

Supervisión y solución de problemas

August 26, 2024

El panel 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. Para obtener más información, consulte Descripción general del panel de control.

Solución de problemas

Es posible que se encuentre con problemas relacionados con lo siguiente mientras configura Secure Private Access o después de configurar Secure Private Access:

- Errores certificados
- Errores de creación de bases de datos
- Fallos de StoreFront
- Fallos en la puerta de enlace pública/puerta de enlace de devolución de llamada
- No se puede acceder al servidor de Secure Private Access

Para obtener más información sobre cómo solucionar estos problemas, consulte Solución de problemas básicos.

Códigos relacionados con la sesión en Director

La integración de Director con Secure Private Access permite una supervisión eficaz del rendimiento y la resolución de problemas, ya que los problemas de todos los componentes de una configuración de Secure Private Access se capturan en Director. Se recomienda resolver los problemas de errores o excepciones examinando los registros. Si esto no resuelve el problema, ponte en contacto con el servicio de asistencia.

Referencias

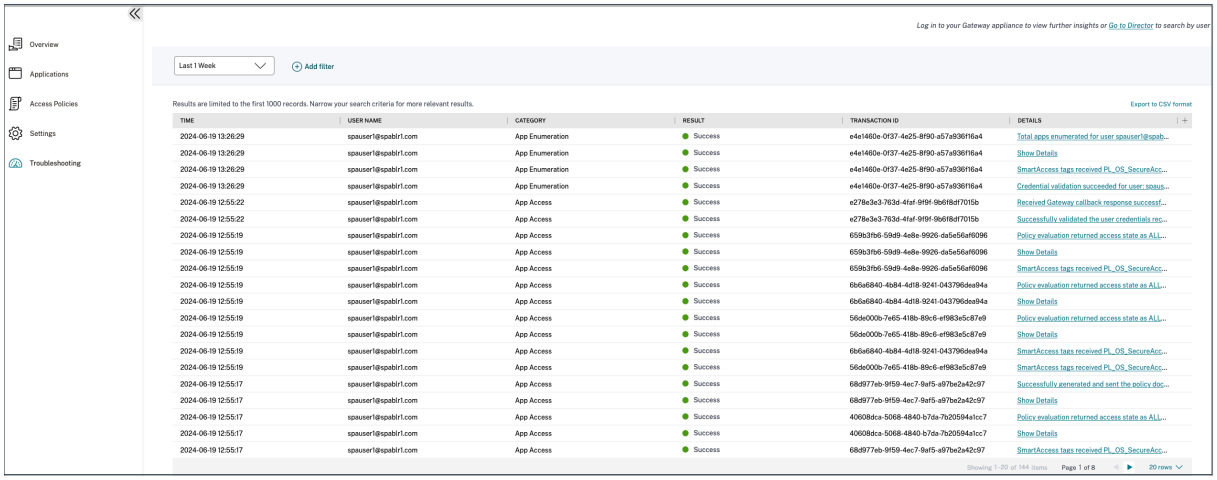
- Configurar Director con Secure Private Access
- Ver una sesión de Secure Private Access en Director
- Lista de códigos de sesión de Secure Private Access en Director.
- Director.

Descripción general del panel

August 26, 2024

El panel de solución de problemas muestra los registros relacionados con el inicio de la aplicación, la enumeración de las aplicaciones y el estado. Puede ver los registros de la hora preestablecida o de una línea de tiempo personalizada. Puedes usar la opción **Agregar filtro** para refinar la búsqueda en función de varios criterios, como la categoría de la aplicación, el nombre de usuario, el identificador de la transacción, etc. Por ejemplo, en los campos de búsqueda, puede seleccionar Transaction-ID, = (igual a algún valor) e introducir 7456c0fb-a60d-4bb9-a2a2-edab8340bb15 en esta secuencia para buscar todos los registros relacionados con este ID de transacción.

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.



Puede usar los siguientes operadores de búsqueda para refinar la búsqueda mediante la opción **Agregar filtro**:

- **= (equivale a algún valor)**: para buscar los registros o directivas que coincidan exactamente con los criterios de búsqueda.
- **! = (no es igual a algún valor)**: para buscar los registros o directivas que no contienen los criterios especificados.
- **~ (contiene algún valor)**: para buscar los registros o directivas que coincidan parcialmente con los criterios de búsqueda.
- **!~ (no contiene ningún valor)**: para buscar los registros o directivas que no contienen algunos de los criterios especificados.

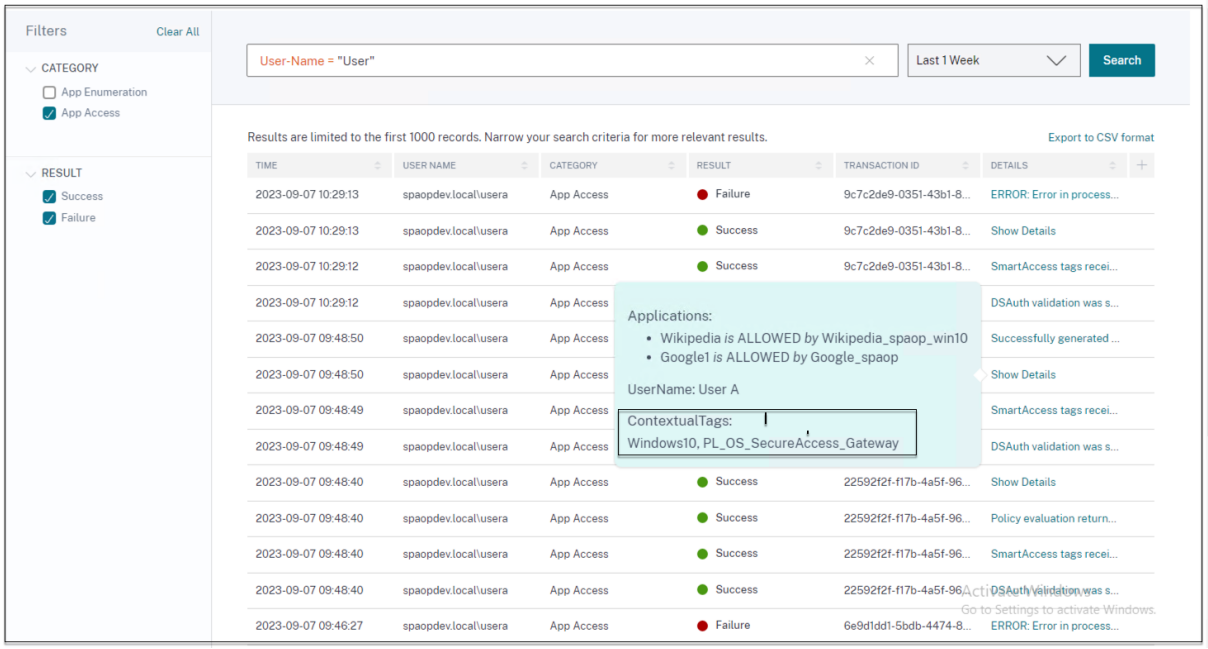
Por ejemplo, puede buscar un evento del tipo "Enumeración"utilizando la cadena **Event-Type > = (igual a algún valor) > Enumeration** en el campo de búsqueda.

Del mismo modo, para buscar usuarios que contengan parcialmente el término "operador", utilice la cadena **UserName > ~ (contiene algún valor) > operador**. 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. 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. Puede filtrar los registros mediante el ID de transacción para encontrar todos los registros relacionados con una solicitud de acceso a una aplicación concreta.

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.



Solución de problemas básicos

August 26, 2024

En este tema se enumeran algunos de los errores que puede encontrar durante o después de configurar Secure Private Access.

Errores certificados

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

Este mensaje de error aparece cuando intenta agregar una dirección pública de NetScaler Gateway y se produce un problema al obtener el certificado. Este problema puede producirse al configurar el Secure Private Access o al actualizar la configuración una vez finalizada la configuración.

Soluciónalternativa : actualice el certificado de puerta de enlace de la misma manera que lo haría para Citrix Virtual Apps and Desktops.

Errores de creación de bases de datos

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

  Solución: 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 siguientes escenarios.

  - 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.
  - Desinstale Secure Private Access y vuelva 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.

    Solución: 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 después 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 después 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

  Solución:

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

  Solución:

  1. Haga clic en **Parámetros** y después en la ficha **Integraciones**.
  2. En la **URL del almacén** 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>`

  Solución:

  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 **Parámetros** y después 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 este almacén y ejecute este script de PowerShell con privilegios de administrador en la máquina en la que se encuentra la instalación de StoreFront correspondiente. Este script debe ejecutarse en todas las máquinas StoreFront.

> **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 Parámetros > 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 Parámetros. Anote la URL del almacén de StoreFront en la que se produjo este error.

  Solución:

  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 **Parámetros** y después 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 se encuentra la instalación de StoreFront correspondiente. Este script debe ejecutarse en todas las máquinas StoreFront.

  > **Nota:**
  >
  > Para ejecutar el script de PowerShell de StoreFront, abra la ventana de PowerShell compat-

> ible con Windows x64 con privilegios de administrador y después ejecute ConfigureStore-Front.ps1. El script de StoreFront no es compatible con Windows PowerShell (x86).

- **Mensaje de error**: "Get-STFStoreService: Se produjo una excepción del tipo 'Citrix.DeliveryServices.Framew . "mientras se ejecuta el script de StoreFront con PowerShell.

  Este error se produce cuando el script de StoreFront se ejecuta en una ventana de PowerShell compatible con x86.

  Solución:

  Para ejecutar el script PowerShell de StoreFront, abra la ventana de PowerShell compatible con Windows x64 con privilegios de administrador y después ejecute`ConfigureStorefront.ps1`.

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`>

Solución:

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 **Parámetros**.

1. Haga clic en **Parámetros** y después 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

Solución:

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 Secure Private Access
- Grupo de administradores de Secure Private Access

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 plug-in 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 plug-in 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>
```

Fallo en la enumeración de la aplicación

La enumeración de aplicaciones se interrumpe si la URL de StoreFront o la URL de NetScaler Gateway contienen una barra diagonal final (/).

Solución:

Elimine la barra diagonal final de la URL del almacén de StoreFront o de la URL de NetScaler Gateway. Para obtener más información, consulte Actualizar los detalles del servidor StoreFront o NetScaler Gateway después de la configuración.

Otros

No se puede completar la configuración inicial

Es posible que no pueda volver a configurar el servidor de licencias si la configuración de Director falló durante la configuración por primera vez.

Solución:

Limpia manualmente la tabla license_server.

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 plug-in Secure Private Access debe tener los permisos para conectarse a la base de datos y crear el esquema de la 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.

Cambiar el nivel de registro para los registros de solución de problemas

Los registros de solución de problemas son el nivel de registro de errores predeterminado.

Para cambiar el nivel de registro de los registros de solución de problemas, en el servicio de tiempo de ejecución appsettings.json (C:\Program Files\Citrix\Citrix Access Security\Runtime\RuntimeService) actualice `restrictedToMinimumLevel` para `TroubleshootingSql` a uno de los valores siguientes:

```
-  Information
-  Debug
-  Warning
-  Error

"TroubleshootingSql": {

  "restrictedToMinimumLevel": "Error",
  "batchPostingLimit": 50,
  "batchPeriod": "00:00:05" // 5 seconds
 }
```

Solución de problemas mediante Director

August 26, 2024

La integración de Director con Secure Private Access permite una supervisión eficaz del rendimiento y la resolución de problemas, ya que los problemas de todos los componentes de una configuración de Secure Private Access se capturan en Director. En las tablas siguientes se enumeran los distintos códigos de error y las condiciones asociadas que se muestran en Director.

Para obtener más información, consulte los siguientes temas.

- Configurar Director con Secure Private Access
- Ver una sesión de Secure Private Access en Director

> **Nota:**
>
> - Los códigos que contienen “0”en el segundo dígito representan un flujo de ejecución normal. Por ejemplo, 1000 representa que la enumeración de aplicaciones se ha realizado correctamente.
> - Los códigos que contienen “1”en el segundo dígito representan un error o una excepción. Por ejemplo, 2101 representa un error de sesión. En caso de error o excepción, se recomienda que resuelva estos problemas examinando los registros. Si esto no resuelve el problema, ponte en contacto con el servicio de asistencia.

Códigos relacionados con la enumeración

Código	Estado	Descripción
1101	fallo	Se produjo un error interno durante la enumeración.
1102	fallo	Se enumeraron algunas aplicaciones, pero falló al menos una evaluación de la aplicación.
1103	fallo	No se enumeró ninguna aplicación y falló al menos una evaluación de la aplicación.
1000	Correcto	La enumeración se realizó correctamente. Se enumeró al menos una aplicación.
1001	Correcto	No se enumeró ninguna aplicación porque las directivas las rechazaron todas.
1002	Correcto	No se enumeró ninguna aplicación porque no coincidió ninguna directiva.
1003	Correcto	No se enumeró ninguna aplicación porque algunas fueron rechazadas y, en otras, ninguna directiva coincidió.
1004	Correcto	No se enumeró ninguna aplicación porque no hay directivas que evaluar.

Códigos relacionados con la sesión

Código	Estado	Descripción
2101	Fallo	Fallo de sesión.
2102	activo/inactivo/fallido	La sesión está activa o ha terminado o se ha producido un error al iniciar al menos una aplicación en la sesión.
2000	Active	La sesión está activa.

Código	Estado	Descripción
2001	Inactivo	La sesión ha finalizado o está inactiva.

Códigos de mensajes de enumeración de aplicaciones

Código	Estado	Descripción
3101	Fallo	Enumeración de aplicaciones: se ha producido un error interno (no se utiliza actualmente).
3102	Fallo	La aplicación no se enumeró porque hubo una excepción durante la evaluación de la directiva.
3103	Fallo	El estado de enumeración de la aplicación es nulo: se produjo un error interno durante la evaluación de la directiva.
3104	Permitir/denegar/fallo	Error al recuperar los detalles de la directiva de la aplicación.
3000	Permitir	Se permite la enumeración de aplicaciones.
3001	Negar	La directiva deniega la enumeración de aplicaciones.
3002	Negar	La aplicación no se enumeró porque no coincidió ninguna directiva.
3003	Desconocido	Se desconoce el estado de enumeración de la aplicación.
3004	Inicio de la aplicación desde CEB	Intento de inicio de la aplicación desde Citrix Enterprise Browser.

Códigos de mensajes de inicio de aplicaciones

Código	Estado	Descripción
4101	Fallo	Error de inicio de la aplicación: se produjo un error interno durante el inicio de la aplicación
4102	Fallo	Error al iniciar la aplicación (interno)
4103	Permitir/denegar/fallo	Error al recuperar los detalles de la directiva de la aplicación
4000	Permitir	Se permite el inicio de la aplicación.
4001	Negar	Se denegó el inicio de la aplicación debido a una directiva.
4002	Negar	Se denegó el inicio de la aplicación porque no coincidía ninguna directiva.

Integración con SIEM

August 26, 2024

El plug-in Secure Private Access admite la integración con los servicios de gestión de eventos e información de seguridad (SIEM). Los eventos de seguridad se almacenan en tiempo real en el registro de eventos de Windows (Visor de eventos\Registros de aplicaciones y servicios\Citrix Access Security) y pueden recopilarse y analizarse con herramientas de terceros.

En la siguiente tabla se enumeran los eventos de seguridad del plug-in Secure Private Access:

ID de suceso	Resumen	Descripción	Origen
4624	Se inició sesión correctamente en una cuenta	Evento creado cuando el administrador de Secure Private Access inició sesión en la consola de administración de Secure Private Access	Citrix Access Security Admin Service
4625	No se pudo iniciar sesión en una cuenta	Evento creado cuando el administrador de Secure Private Access no pudo iniciar sesión en la consola de administración de Secure Private Access	Citrix Access Security Admin Service
4634	Se cerró la sesión de una cuenta	Evento creado cuando el administrador de Secure Private Access cerró sesión en la consola de administración de Secure Private Access	Citrix Access Security Admin Service
4720	Se creó una cuenta de usuario	Evento creado al agregar un nuevo administrador de Secure Private Access	Citrix Access Security Admin Service
4738	Se cambió una cuenta de usuario	Evento creado cuando se actualizó el nuevo administrador de Secure Private Access	Citrix Access Security Admin Service
4726	Se ha eliminado una cuenta de usuario	Evento creado al eliminar al nuevo administrador de Secure Private Access	Citrix Access Security Admin Service

ID de suceso	Resumen	Descripción	Origen
8001	Sesión de acceso seguro de usuario	Evento creado cuando la sesión de usuario se inició o finalizó en el dispositivo de punto final. Contiene detalles del usuario, la sesión y el dispositivo, y los dominios internos y externos visitados durante la sesión	Citrix Access Security Admin Service
8002	Solicitud de autorización de acceso de usuario	Evento creado cuando el complemento Secure Private Access autoriza el acceso al recurso. Contiene el FQDN del recurso y la decisión de autorización	Citrix Access Security Admin Service

Referencias

- Integración de gestión de información y eventos de seguridad (SIEM)
- Acerca de compartir registros en soluciones SIEM

Configuración de retención de registros

August 26, 2024

Los registros se almacenan en la base de datos de Secure Private Access durante siete días. Si el recuento total de registros es demasiado grande (por ejemplo, más de 100 000), puede eliminar los registros más antiguos que tengan menos de 90 días. La tarea de limpieza, de forma predeterminada, se ejecuta cada 12 horas. El trabajo también se ejecuta cada vez que se reinicia el servicio de ejecución.

Personalización de la configuración de retención de registros para la solución de problemas

La limpieza de los registros se puede configurar mediante el archivo appsettings.json de la carpeta de instalación del servicio Runtime. Puede configurar la limpieza en función de la antigüedad de los registros y del número de registros que se pueden almacenar en la base de datos. Modifique las siguientes entradas en el archivo appsettings.json, según sea necesario:

Ejemplo de archivo appsettings.json:

```
"TroubleshootingLogs": {

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

Para inhabilitar la limpieza, configure los siguientes ajustes según sea necesario:

- Para conservar los registros solo durante 7 días, establézcalo `CleanupDataOlderThanDays` en 7.
- Para inhabilitar la limpieza basada en días, establézcala `CleanupDataOlderThanDays`en 0.
- Para inhabilitar la limpieza basada en el recuento, establézcala `CleanupOldestDataIfEntriesCount` en 0.
- Si ambas configuraciones se establecen en 0 o si `CleanupPeriodInHours`se establece en 0, los registros se conservan para siempre.
  - No se recomienda establecer ambos `CleanupDataOlderThanDays`valores `CleanupOldestDataIfEntriesCountAbove`en 0 o en `CleanupPeriodInHours` 0, ya que podría provocar un problema de uso del disco al 100%.
  - La frecuencia de limpieza de los registros también se puede cambiar modificando la `CleanupPeriodInHours`entrada.

> **Nota:**
>
> Si Secure Private Access se implementa como un clúster, esta configuración se debe modificar en cada nodo del clúster. Si hay una discrepancia en la configuración del nodo, la instancia que se limpia con más frecuencia tiene prioridad.

Limpieza de registros y telemetría

August 26, 2024

Limpieza de datos de telemetría

Los datos de telemetría se almacenan en la base de datos de Secure Private Access durante 3 meses. Las comprobaciones para identificar los datos de telemetría que deben limpiarse se realizan cada 30 segundos.

> **Nota:**
>
> El servicio de ejecución debe estar en ejecución para activar la limpieza de datos de telemetría.

Limpieza de registros CDF

Los registros CDF se almacenan en la máquina de instalación de Secure Private Access, dentro de las carpetas de instalación del servicio de administración y ejecución. Los registros CDF se colocan en archivos.csv con un límite de tamaño de 10 MB aplicado a cada archivo.
El servicio de administración puede retener hasta 90 archivos de registro CDF a la vez, después de lo cual elimina los archivos más antiguos para liberar espacio para la creación de los nuevos archivos de registro CDF.
El servicio Runtime funciona de la misma manera que el servicio Admin, pero puede retener una mayor cantidad de archivos a la vez, hasta 600.

Limpieza personalizada de registros de CDF

La limpieza de los registros de CDF se puede configurar a través de los archivos appsettings.json de las carpetas de instalación de los servicios de administración y ejecución. Para cambiar el tamaño del archivo y el límite de recuento de los archivos, actualiza las siguientes entradas en el archivo appsettings.json:

```
"CdfFile": {

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

> **Nota:**
>
> Si hay varias instancias de Secure Private Access configuradas en el sitio, actualice los archivos

> appsettings.json para la limpieza de CDF en cada máquina de instalación de Secure Private Access.

Notificaciones de terceros

August 26, 2024

Citrix Secure Private Access para entornos locales