Citrix Secure Private Access: en las instalaciones

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 Zero Trust Network Access (ZTNA) administrada por el cliente que proporciona acceso seguro a las aplicaciones Web/SaaS y TCP/UDP internas con lo siguiente, además de una experiencia perfecta para el usuario final:

- Acceso sin VPN para aplicaciones web internas y SaaS
- 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 utiliza la aplicación StoreFront local y Citrix Workspace para ofrecer una experiencia de acceso segura y sin problemas para acceder a las aplicaciones Web/SaaS y TCP/UDP internas en Citrix Enterprise Browser. Esta solución también usa 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 la organización al ofrecer fácilmente un acceso sin confianza a las aplicaciones basadas en explorador (aplicaciones web/SaaS internas) y a las aplicaciones cliente-servidor (aplicaciones TCP/UDP) mediante el portal local de StoreFront como portal de acceso unificado a las aplicaciones web/SaaS y TCP/UDP internas, junto con las aplicaciones y escritorios virtuales como parte integrada de Citrix Workspace.

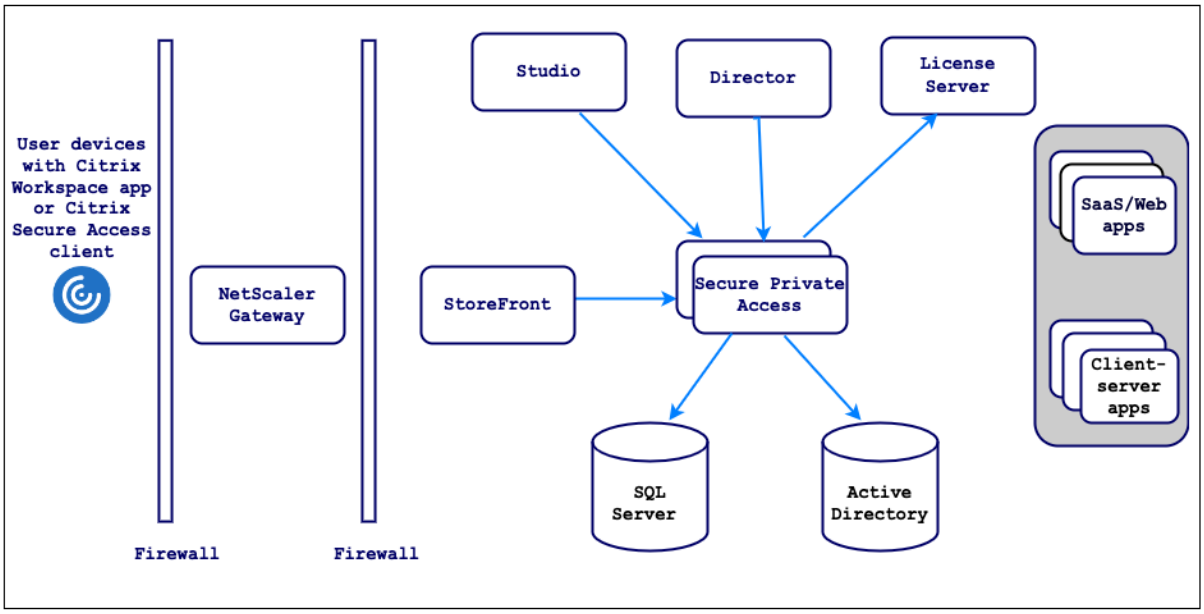
Citrix Secure Private Access combina los elementos de NetScaler Gateway y StoreFront para ofrecer una experiencia integrada a los usuarios finales y a los administradores.

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

Funcionalidad	Servicio/componente que proporciona la funcionalidad
Directivas de autorización	Secure Private Access
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

October 21, 2024

Agosto de 2024

Descubrimiento de aplicaciones

La función de descubrimiento de aplicaciones ayuda al administrador a obtener visibilidad de las aplicaciones privadas internas, como aplicaciones web y aplicaciones de servidor cliente (aplicaciones basadas en TCP y UDP) en su organización y los usuarios que acceden a esas aplicaciones. Los administradores pueden descubrir las aplicaciones especificando el alcance de los dominios (dominios comodín) o subredes IP. Para obtener más detalles, consulte Descubrir dominios o direcciones IP a los que acceden los usuarios finales.

Herramienta de modelado de políticas

La herramienta de modelado de políticas (**Políticas de acceso > Modelado de políticas**) ayuda a los administradores a analizar y solucionar problemas de configuración desde la consola de administración. Para obtener más detalles, consulte Herramienta de modelado de políticas.

Se agregó un nuevo tipo de aplicación para conexiones de servidor TCP/UDP a cliente

Secure Private Access ahora admite un nuevo tipo de aplicación **TCP/UDP - servidor a cliente** que se puede usar para los siguientes casos de uso.

- **Compatibilidad con direcciones IP de intranet:** - Las direcciones IP de intranet se pueden usar para asignar usuarios a direcciones IP para auditorías de seguridad, segmentación de red y cumplimiento. Para obtener más información sobre la dirección IP de la intranet, consulte Configurar grupos de direcciones.
- **Conexiones de servidor a cliente:** - Las conexiones de servidor a cliente se pueden utilizar para administrar y mantener un entorno de red como el siguiente:
  - Impulso de políticas basadas en dominios mediante políticas de grupo.
  - Distribución de software mediante Microsoft Endpoint Configuration Manager o soluciones similares.
  - Asistencia remota para solucionar problemas y depurar estaciones de trabajo de los usuarios.
- **Conexiones de cliente a cliente:** - Las conexiones de cliente a cliente permiten que dos computadoras remotas se comuniquen directamente entre sí para compartir y recibir datos en una red privada, compartida o pública sin comprometer la seguridad y la flexibilidad.

Para obtener detalles sobre cómo configurar una aplicación de servidor a cliente TCP/UDP, consulte Configurar aplicaciones de servidor a cliente TCP/UDP.

Problemas resueltos

October 21, 2024

Los siguientes problemas se abordan en la versión 2408.

Configuración del controlador de dominio

El sufijo UPN alternativo no es compatible con el acceso privado seguro para el inicio de sesión en Intranet (StoreFront) y la enumeración de aplicaciones de Internet/Extranet (puerta de enlace).

Gestión administrativa

Los cambios en el rol RBAC del administrador se reflejan solo después de que se invalida la sesión actual (por cierre de sesión o vencimiento del token).

Lanzamiento de la aplicación

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

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

Consola de administración

- La página **Editar aplicación** no se cierra automáticamente después de que la página **Editar aplicación** (**Acceso privado seguro> Aplicaciones > Editar aplicación**) de una aplicación publicada no se cierra después de que se modifica una entrada de dominio relacionada.

  Por ejemplo, si el dominio relacionado que ingresaste al crear una aplicación fue `www.example.com`. Después de publicar la aplicación, reemplace el dominio relacionado `www.example.com` con `abc.com`y haga 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. Sin embargo, la aplicación está creada.
- Si la URL de una aplicación contiene `www`, entonces la URL se guarda en la tabla de dominio de enrutamiento (**Configuración > Dominio de aplicación**) sin el prefijo `www`.

Actualizaciones

Si se utiliza un certificado SSL personalizado para el servicio de administración de acceso privado seguro, el certificado debe vincularse nuevamente al sitio "Citrix Access Security Admin"en Internet Information Service (IIS).

Problemas conocidos

October 21, 2024

Los siguientes problemas existen en la versión 2408.

> **Nota**
>
> A algunos problemas se les asigna un ID de seguimiento solo para referencia interna y estos no tienen ningún impacto en el cliente.

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 a.com y b.com están en dos bosques de AD diferentes, y SPA está instalado en una máquina donde el dominio está unido a a.com / b.com, entonces otros usuarios del dominio no pueden acceder a las aplicaciones publicadas de SPA.

  [SPAOP-2031]

- Si el dominio de la máquina donde está instalado Secure Private Access para instalaciones locales 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 tanto para el servicio de administración como para el servicio de tiempo de ejecución de Secure Private Access.

  [SPAOP-1558]

- Los grupos de distribución no son compatibles con Secure Private Access. Por lo tanto, las políticas 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 proporcionado por el usuario.

Por lo tanto, si el dominio correspondiente no es accesible o si el nombre de dominio no es un nombre válido, ese dominio no será compatible.

NetScaler Gateway

- El servidor virtual SSL con configuración de perfil SSL no es compatible en el siguiente escenario:
  - El cliente utiliza NetScaler Gateway 13.1–48.47 y posteriores o 14.1–4.42 y posteriores.
  - El interruptor `ns_vpn_enable_spa_onprem` está habilitado.

  Solución temporal:

  Vincule los parámetros SSL configurados en el perfil SSL directamente al servidor virtual SSL o deshabilite el interruptor `ns_vpn_enable_spa_onprem`.

  Para obtener detalles sobre el interruptor, consulte Compatibilidad con etiquetas de acceso inteligente.

RfWeb / Espacio de trabajo para la web

- RfWeb/Workspace para la web no es compatible y, por lo tanto, las aplicaciones no se enumeran. Para obtener más detalles, consulte Cuando se utiliza StoreFront versión 2311 o posterior.

  [SPAOP-2487]

Lanzamiento de la aplicación

- Si las perillas `ns_vpn_enable_spa_onprem` y `toggle_vpn_enable_securebrowse_client_mo` no están habilitadas o si estas perillas no son compatibles con su NetScaler Gateway, entonces el inicio de la aplicación falla después de la rotación `CustomHeaderCryptoKey`. La rotación `CustomHeaderCryptoKey` ocurre automáticamente después de 30 días.

  [SPAOP-4528]

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

  [SPAOP-1412]

StoreFront

- En **Tiendas > Configurar Experiencia Unificada**, el receptor predeterminado para el sitio web debe configurarse en /Citrix/<`StoreName`>Web. En versiones anteriores de StoreFront, el re-

ceptor predeterminado para el sitio web está configurado con un valor en blanco y eso no funciona para el acceso privado seguro. Además, la versión anterior de la interfaz de usuario del receptor se muestra en el cliente. Para obtener información sobre la configuración de StoreFront, consulte StoreFront.

- Si está utilizando las versiones 2308 o anteriores de StoreFront, la página **Tiendas > Administrar controladores de entrega** muestra el tipo de complemento Acceso privado seguro como **XenMobile**. Esto no afecta la funcionalidad.

Registros

- No se admite la generación de paquetes de soporte para el clúster.
- Las carpetas de registros de los servicios de administración y de tiempo de ejecución no se deben eliminar. El acceso privado seguro no se puede recrear si se eliminan estas carpetas.

Monitoreo TCP/UDP

- La función **SPAOP-3315-EnableZTNAApplications** está deshabilitada de manera predeterminada en 2408. Como resultado, los datos de monitoreo TCP/UDP no se almacenan y, por lo tanto, la integración de Director falla.

  Solución alternativa: si está utilizando aplicaciones TCP/UDP y desea habilitar la integración de Director, actualice manualmente la base de datos para habilitar esta función.

  [SPAOP-5587]

Actualización de versión

- Después de la actualización de la base de datos, las pestañas del módulo/sección en la interfaz de usuario no aparecen durante algún tiempo (aproximadamente una hora).

  Solución alternativa: reinicie manualmente el servicio IIS si desea que las pestañas de la interfaz de usuario sean visibles inmediatamente después de la actualización de la base de datos.

  [SPAOP-5331]

- Al intentar actualizar las versiones 2402 o 2407 a 2408 reemplazando el MSI, el mosaico Acceso privado seguro en el instalador de Citrix Virtual Apps and Desktops muestra **Actualización disponible**. Sin embargo, al hacer clic en el mosaico Secure Private Access para continuar con la actualización, Secure Private Access se desinstala en lugar de actualizarse. La página **Componentes principales** muestra el mensaje "**Se eliminará el acceso privado seguro**.

  [SPAOP-5495]

- Al actualizar de la versión 2405 o 2407 a la 2408, no puede configurar el acceso privado seguro si no se configuró en las versiones 2405 o 2407. El proceso de creación de la base de datos no puede continuar porque el botón **Siguiente** en la página **Configuración de la base de datos** está en gris.

  [SPAOP-5595]

- Después de actualizar a 2408 y editar una aplicación existente cuya URL comienza con www, el campo **Conectividad de la aplicación** no completa el estado anterior. Debes seleccionar nuevamente el tipo de conectividad de la aplicación. Esta es una acción única posterior a la actualización después de la cual la configuración se guarda y continúa persistiendo.

  [SPAOP-4216]

- Después de actualizar a 2408, aunque puede iniciar sesión en la consola de administración, no puede administrar aplicaciones ni políticas. Aparece un mensaje de error.

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

  [SPAOP-5255]

- Después de actualizar a 2408, la enumeración de aplicaciones y el inicio de aplicaciones fallan.

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

  [SPAOP-5255]

- No es posible actualizar el complemento Secure Private Access desde versiones anteriores a la 2408 si el complemento se instaló mediante el controlador de entrega.

  [SPAOP-4505]

Interfaz de usuario

- El contador de inicio de aplicaciones **** en la página Descripción general de acceso privado seguro ** >** no se incrementa para las aplicaciones TCP/UDP.

  [SPAOP-4201]

Requisitos del sistema

October 21, 2024

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

Producto	Versión mínima
Aplicación Citrix Workspace	Windows –2403 y posteriores macOS –2402 y posteriores
StoreFront	LTSR 2203 o CR 2212 y posteriores
NetScaler	13.1, 14.1 y posteriores. Se recomienda utilizar las últimas versiones de NetScaler Gateway versión 13.1 o 14.1 para un rendimiento optimizado. Para aplicaciones TCP/UDP: 14.1–25.56 y posteriores
Cliente de Citrix Secure Access	Cliente de Windows: 24.6.1.17 y posteriores Cliente macOS - 24.06.2 y posteriores
Director	2402 o posterior
Sistema operativo para el servidor de complementos de Secure Private Access	Windows Server 2019 y versiones posteriores

Puertos de comunicación: Asegúrese de haber abierto los puertos necesarios para el complemento de acceso privado seguro. Para obtener más detalles, consulte Puertos de comunicación.

Bases de datos: La siguiente es la lista de versiones de servidor Microsoft SQL compatibles con las bases de datos de configuración del sitio, registro de configuración y monitoreo:

```
- SQL Server 2022, ediciones Express, Standard y Enterprise.
- SQL Server 2019, ediciones Express, Standard y Enterprise.
- SQL Server 2017, ediciones Express, Standard y Enterprise.

Para instalaciones nuevas: De forma predeterminada, si no se detecta una instalación de SQL Server compatible existente, SQL Server Express 2017 con Cumulative Update 16 se instala al instalar el Controller.

Para la actualización de versiones, no se actualiza ninguna versión existente de SQL Server Express.

Se admiten las siguientes soluciones de alta disponibilidad de base de datos (excepto SQL Server Express, que solo admite el modo autónomo):

- Instancias de clúster de conmutación por error de SQL Server Always On
- Grupos de disponibilidad AlwaysOn de SQL Server (incluidos los grupos de disponibilidad básica)
- Crear reflejo de la base de datos de SQL Server
```



```
14
15 Se requiere la autenticación de Windows para las conexiones entre el
      Controller y la base de datos de SQL Server del sitio.
16
17 Para obtener más información sobre las bases de datos, consulte [Bases
      de datos](/es-es/citrix-virtual-apps-desktops/technical-overview/
      databases). > **Nota** > > -  El acceso privado seguro para
      instalaciones locales no es compatible con la aplicación Citrix
      Workspace para iOS y Android. > -  El cliente Citrix Secure Access
      para Linux, iOS y Android no admite aplicaciones TCP/UDP locales de
      Secure Private Access.
```

Requisitos previos

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

- Una máquina servidor Windows con IIS ejecutándose, configurada con un certificado SSL/TLS, en la que se instalará el complemento Secure Private Access.
- URL de la tienda StoreFront que se deben ingresar durante la configuración.
- La tienda en StoreFront debe estar configurada y la URL del servicio de la tienda debe estar disponible. El formato de la URL del servicio de la tienda 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 complemento Secure Private Access (o un equilibrador de carga si el complemento Secure Private Access se implementa como un clúster).
- Nombre del perfil de autenticación configurado en NetScaler.
- Certificado de servidor SSL configurado en NetScaler.
- Nombre del dominio.
- Las configuraciones del certificado están completas. Los administradores deben asegurarse de que las configuraciones del certificado estén completas. El instalador de Secure Private Access configura un certificado autofirmado si no se encuentra ningún certificado en la máquina. Sin embargo, esto podría no funcionar siempre.

> **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. Estas configuraciones las establece el instalador de Secure Private Access de forma predeterminada y no se deben cambiar manualmente.

Requisitos de la cuenta de administrador

Las siguientes cuentas de administrador son necesarias al configurar el acceso privado seguro.

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

Puertos de comunicación

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

Origen	Destino	Tipo	Puerto	Detalles
Puesto de trabajo de administración	Complemento de acceso privado seguro	HTTPS	4443	Complemento de acceso privado seguro: consola de administración
Complemento de acceso privado seguro	Servicio NTP	TCP, UDP	123	Sincronización horaria
	Servicio DNS	TCP, UDP	53	Búsqueda de DNS
	Active Directory	TCP, UDP	88	Kerberos
	Director	HTTP, HTTPS	80, 443	Comunicación con el Director para la gestión del desempeño y la resolución mejorada de problemas

Origen	Destino	Tipo	Puerto	Detalles
	Servidor de licencias	TCP	8083	Comunicación con el servidor de licencias para la recopilación y procesamiento de datos de licencias
		TCP	389	LDAP sobre texto simple (LDAP)
		TCP	636	LDAP sobre SSL (LDAPS)
	Microsoft SQL Server	TCP	1433	Plugin de acceso privado seguro: comunicación de bases de datos
	StoreFront	HTTPS	443	Validación de autenticación
	NetScaler Gateway	HTTPS	443	Devolución de llamada de NetScaler Gateway
StoreFront	Servicio NTP	TCP, UDP	123	Sincronización horaria
	Servicio DNS	TCP, UDP	53	Búsqueda de DNS
	Active Directory	TCP, UDP	88	Kerberos
		TCP	389	LDAP sobre texto simple (LDAP)
		TCP	636	LDAP sobre SSL (LDAPS)
		TCP, UDP	464	Protocolo de autenticación nativo de Windows que permite a los usuarios cambiar contraseñas vencidas

Origen	Destino	Tipo	Puerto	Detalles
	Complemento de acceso privado seguro	HTTPS	443	Autenticación y enumeración de aplicaciones
	NetScaler Gateway	HTTPS	443	Devolución de llamada de NetScaler Gateway
NetScaler Gateway	Complemento de acceso privado seguro	HTTPS	443	Validación de la autorización de la aplicación
	StoreFront	HTTPS	443	Autenticación y enumeración de aplicaciones
	Aplicaciones web	HTTP, HTTPS	80, 443	Comunicación de NetScaler Gateway con aplicaciones de acceso privado seguro 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 políticas de autenticación.
- Vincular un certificado SSL a un servidor virtual (SSL) en NetScaler.

Pautas de tallas

October 21, 2024

Acceso privado seguro a bases de datos locales

La base de datos local de Secure Private Access contiene información sobre las aplicaciones, políticas y material gráfico relacionado. También contiene información relacionada con la resolución de problemas y la telemetría.

Debido a su naturaleza dinámica, los registros de telemetría y resolución de problemas sufren cambios frecuentes y se conservan durante un período corto. Por lo tanto, se debe configurar una base de datos local de acceso privado seguro considerando la necesidad de actualizaciones frecuentes.

Durante las pruebas de escalabilidad interna, la siguiente configuración de la base de datos local de Secure Private Access pudo manejar una carga de 5000 usuarios.

Componente	Especificación
———————————————————-	——————
Procesador	8 vCPU
Memoria	16 GB
Red	10 GBP de trabajo en red
Almacenamiento de host	Tamaño: 127 GB
^^	IOPS: 500
^^	Rendimiento máximo: 100
Sistema operativo	Windows Server 2022
SQL Server	SQL Server 2022 CU12
Espacio de base de datos utilizado diariamente por 5000 usuarios	5 GB

> **Nota**
>
> - Las métricas se derivan asumiendo que la limpieza de eventos de registro está deshabilitada y el período de retención de registros 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 la configuración. Estas configuraciones están disponibles en el archivo appsettings.json del servicio de ejecución de acceso privado seguro y se pueden modificar según sea necesario. Para obtener más detalles, consulte Configuración para conservar registros de eventos.

Dimensionamiento del servidor de decisiones

La escalabilidad del servidor local de Secure Private Access depende de la base de datos utilizada. La base de datos almacena información de telemetría y resolución de problemas. La escala de la base de datos depende de la memoria, la velocidad del disco y la cantidad de CPU utilizadas para procesar la carga.

Durante las pruebas de escalabilidad interna, se confirmó que la siguiente configuración de 3 nodos locales de acceso privado seguro podía manejar una carga de 5000 usuarios.

Componente	Especificación
Procesador	4 CPU virtuales
Memoria	8 GB
Red	10 GBP
Almacenamiento de host	Unidad de estado sólido premium LRS Tamaño: 127 GB IOPS: 500 Rendimiento máximo: 100
Sistema operativo	Windows Server 2022

Instalar acceso privado seguro

October 21, 2024

El instalador seguro de acceso privado está disponible como instalador independiente o como parte del instalador integrado de Citrix Virtual Apps and Desktops.

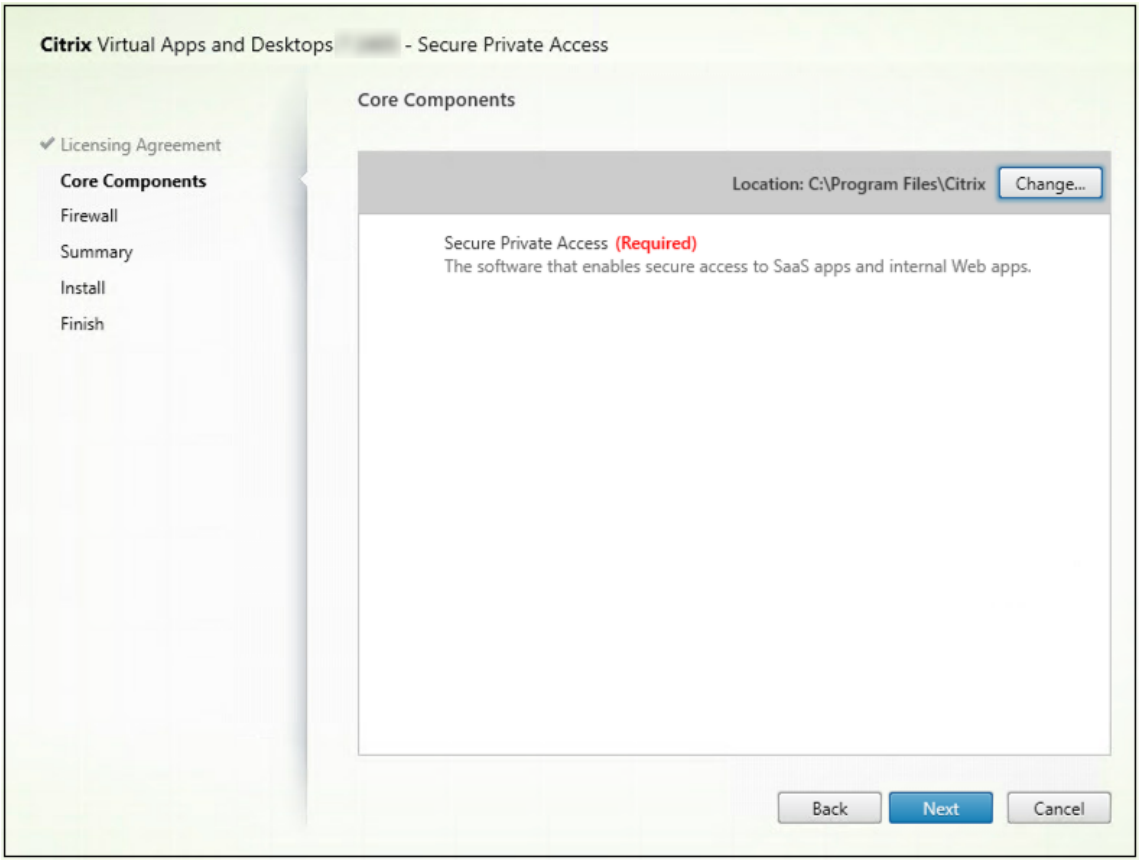
Requisitos de la cuenta de administrador para instalar y administrar Secure Private Access

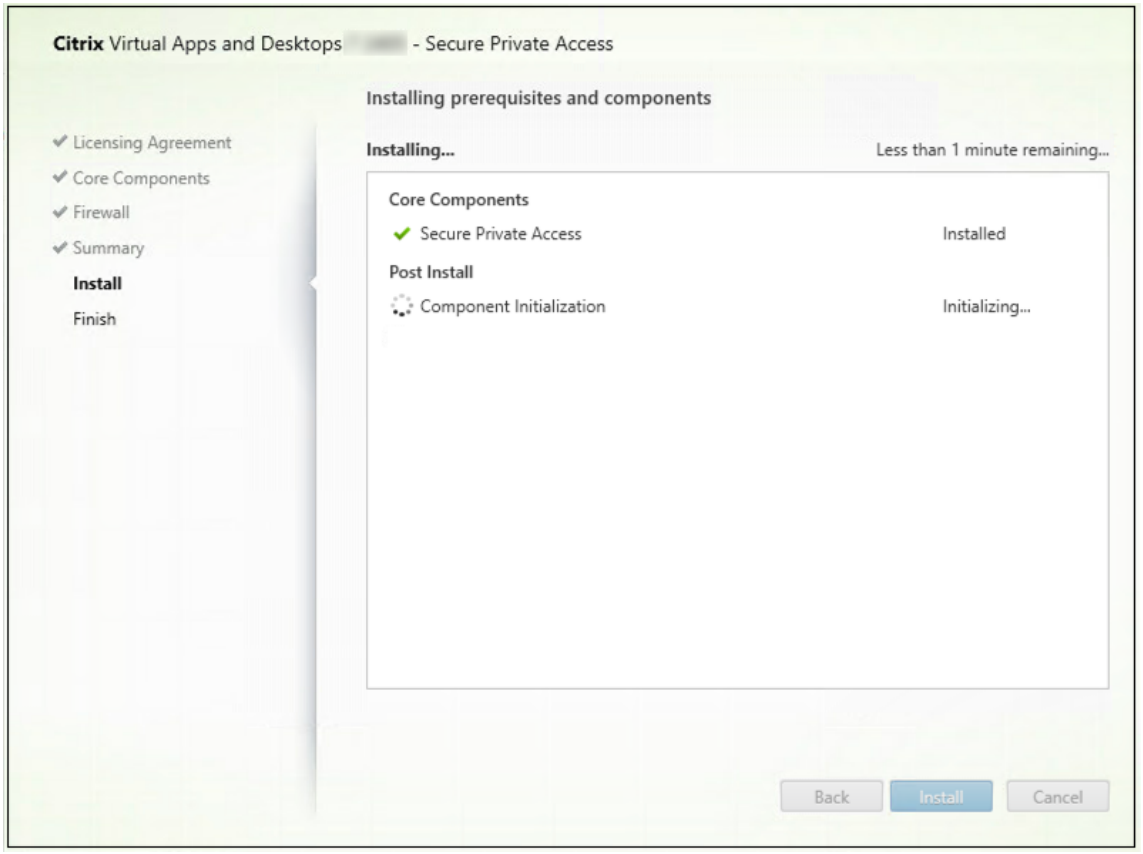
- Para instalar Secure Private Access, debe iniciar sesión con una cuenta de administrador de máquina local.
- Para configurar Secure Private Access, debe iniciar sesión en la consola de administración de Secure Private Access con un usuario de dominio que también sea administrador de la máquina local donde está instalado Secure Private Access.

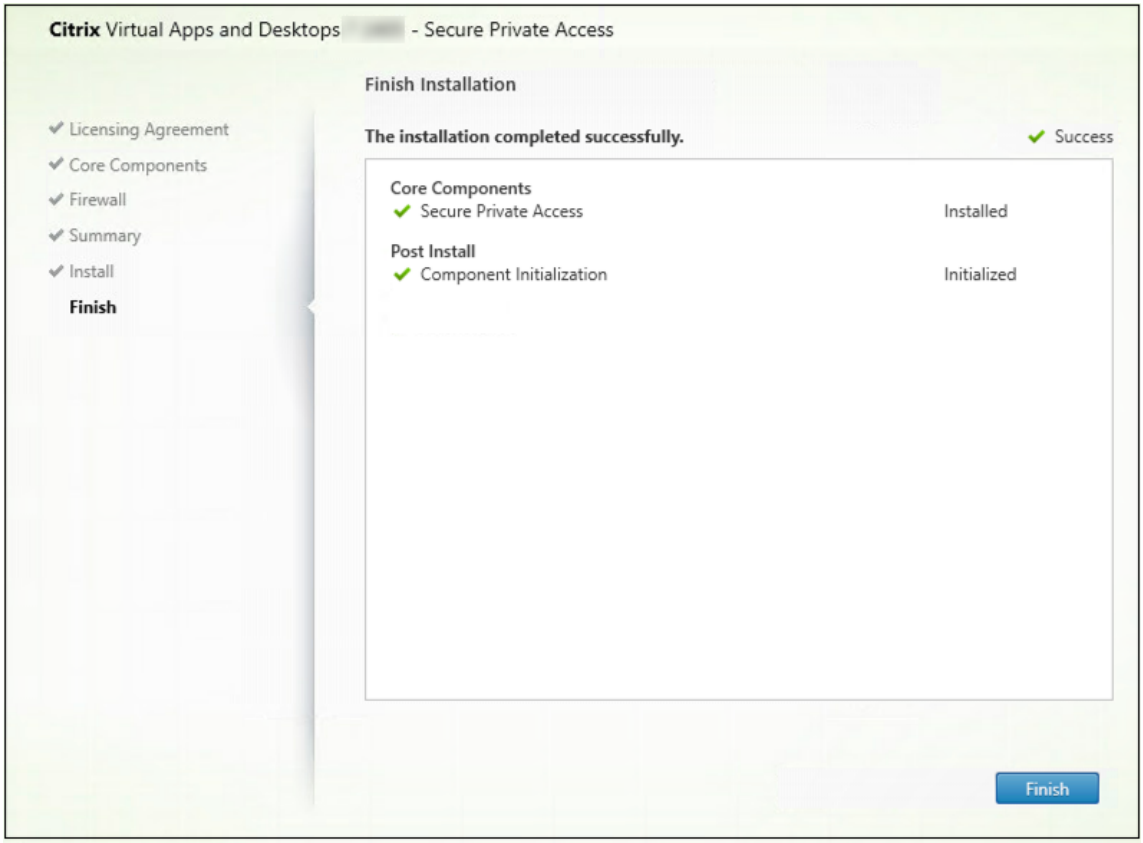
- Una vez completada la configuración, ese usuario se convierte en el primer administrador de Secure Private Access y luego puede agregar otros administradores.
- Para administrar Secure Private Access después de la configuración, debe iniciar sesión en la consola de administración de Secure Private Access con una cuenta de administrador de Secure Private Access.

Realice los siguientes pasos para instalar Secure Private Access:

1. Descargue el software del producto Citrix Virtual Apps and Desktops desde https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/ e inicie el asistente.
2. Haga clic en **Iniciar** situado junto al producto a instalar: Virtual Apps o Virtual Apps and Desktops.
3. Elija **Acceso privado seguro** y siga las instrucciones en pantalla para completar la instalación.

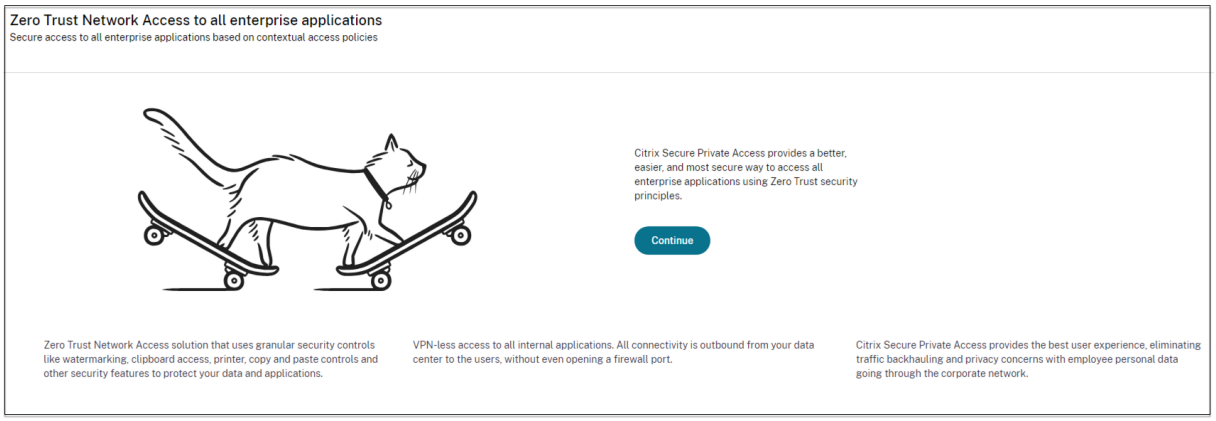




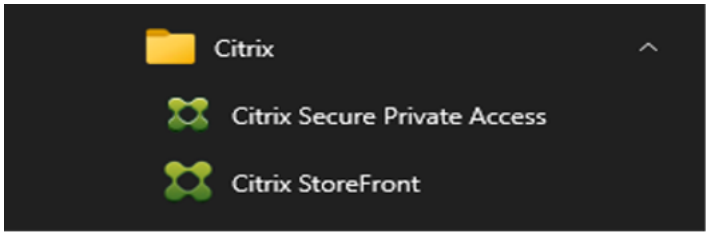


Para obtener instrucciones detalladas paso a paso, consulte Instalar componentes principales y Instalar usando la línea de comando.

Una vez completada la instalación, la consola de administración de configuración inicial se abre automáticamente en la ventana del navegador predeterminado. Puede hacer clic en **Continuar** para configurar el acceso privado seguro.



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



SSO a la consola de administración

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

Si la autenticación Kerberos no está configurada, el navegador le solicitará que ingrese sus credenciales cuando acceda a la consola de administración de Secure Private Access.

- Si ingresa sus credenciales, habilitará el inicio de sesión con Autenticación integrada de Windows (IWA).
- Si no ingresa sus credenciales, se le presentará la página de inicio de sesión de acceso privado seguro.

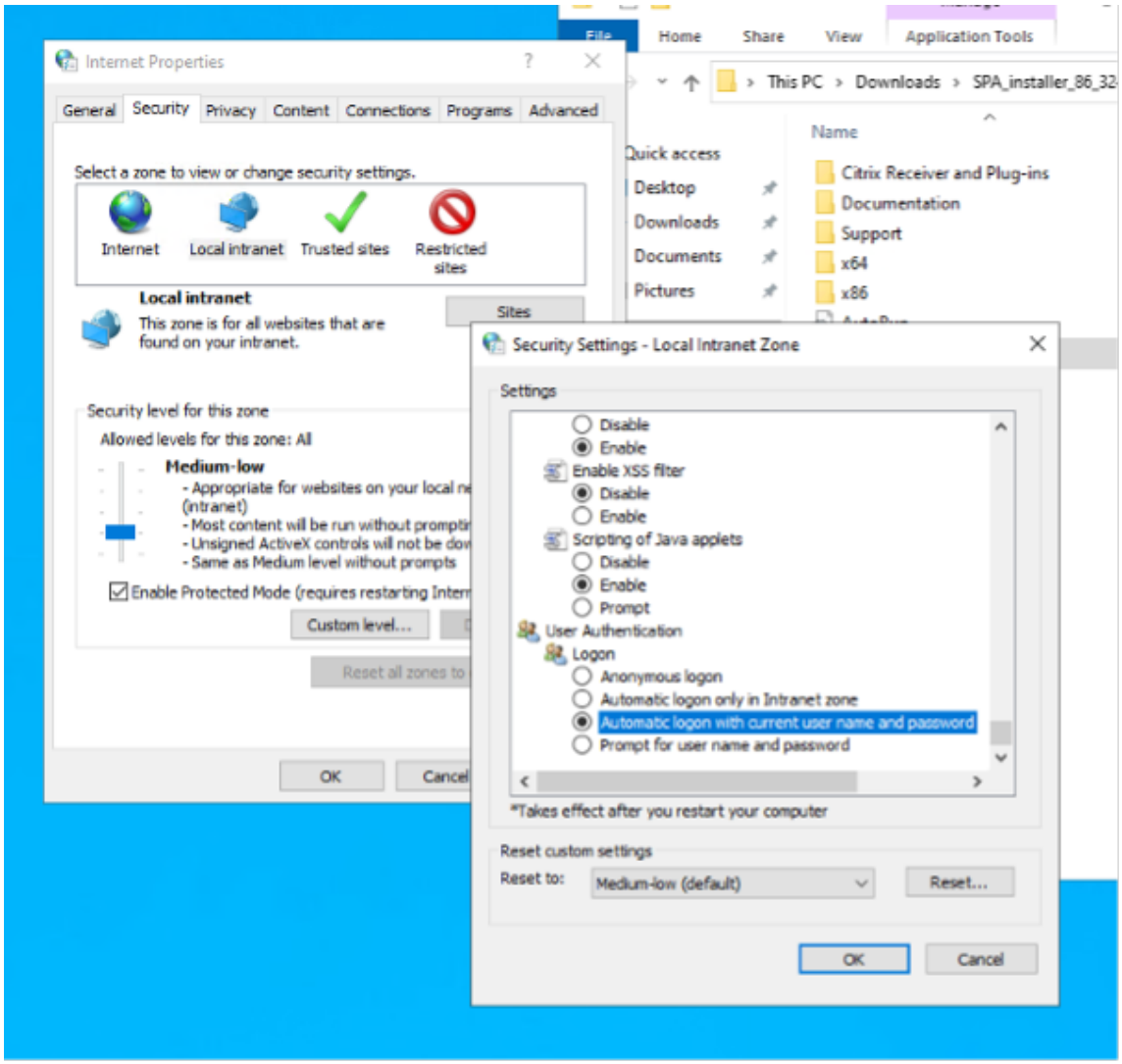
Debe iniciar sesión en la consola de administración para continuar con la configuración del acceso privado seguro. Puede configurar el acceso privado seguro con cualquier usuario que pertenezca al

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

Para los navegadores Google Chrome y Microsoft Edge, realice los siguientes pasos para habilitar Kerberos.

1. Abra **Opciones de Internet**.
2. Seleccione la pestaña **Seguridad** y haga clic en **Zona de Intranet Local**.
3. Haga clic en **Sitios** y agregue la URL de acceso privado seguro.

   También puede utilizar un comodín si planea instalar Secure Private Access en varias máquinas. Por ejemplo, `"https://*.fabrikam.local"`.
4. Haga clic en **Nivel personalizado**.
5. En **Autenticación de usuario > Inicio de sesión**, seleccione **Inicio de sesión automático con nombre de usuario y contraseña actuales**.



> **Nota**

- Si usa sesiones de incógnito de Chrome, cree una clave de registro DWORD Computer\HKEY_LOCAL_MACHINE y configúrela en el valor 1.
- Debes reiniciar todas las ventanas de Chrome (incluidas las ventanas que no son de incógnito) antes de que Kerberos se habilite para el modo de incógnito.
- Para otros navegadores, consulte la documentación del navegador específico sobre la autenticación Kerberos.

Siguientes pasos

- Configurar acceso privado seguro
- Configurar NetScaler Gateway
- Configurar aplicaciones
- Configurar políticas de acceso para las aplicaciones

Componentes

October 21, 2024

Los siguientes son los componentes clave en un acceso privado seguro típico para una implementación local.

- **StoreFront:** - StoreFront autentica a los usuarios y administra las tiendas de escritorios y aplicaciones a las 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 rastrea las suscripciones a aplicaciones de los usuarios, los nombres de accesos directos y otros datos. Gracias a ello, los usuarios tienen una experiencia similar, aunque utilicen varios dispositivos. Para obtener detalles 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 detalles sobre la integración de NetScaler Gateway con Secure Private Access, consulte NetScaler Gateway.
- **Director:** (Opcional) Director le permite realizar una supervisión del rendimiento y una resolución de problemas eficaces. Para integrar Director con Secure Private Access, debe ingresar la dirección IP del FQDN del servidor Director que debe estar registrado con Secure Private Access. Para obtener detalles 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 datos de licencias. Para obtener detalles 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 permitir que los usuarios accedan sin problemas al servicio a través de Web Studio. Para obtener detalles sobre la integración de Secure Private Access con Web Studio, consulte Integración de Secure Private Access con Web Studio.

Para obtener información sobre los requisitos de versiones mínimas de estos productos, consulte Requisitos del sistema.

> **Nota**
>
> Director y License Server están integrados con Secure Private Access a partir de la versión 2402.

StoreFront

June 19, 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**).

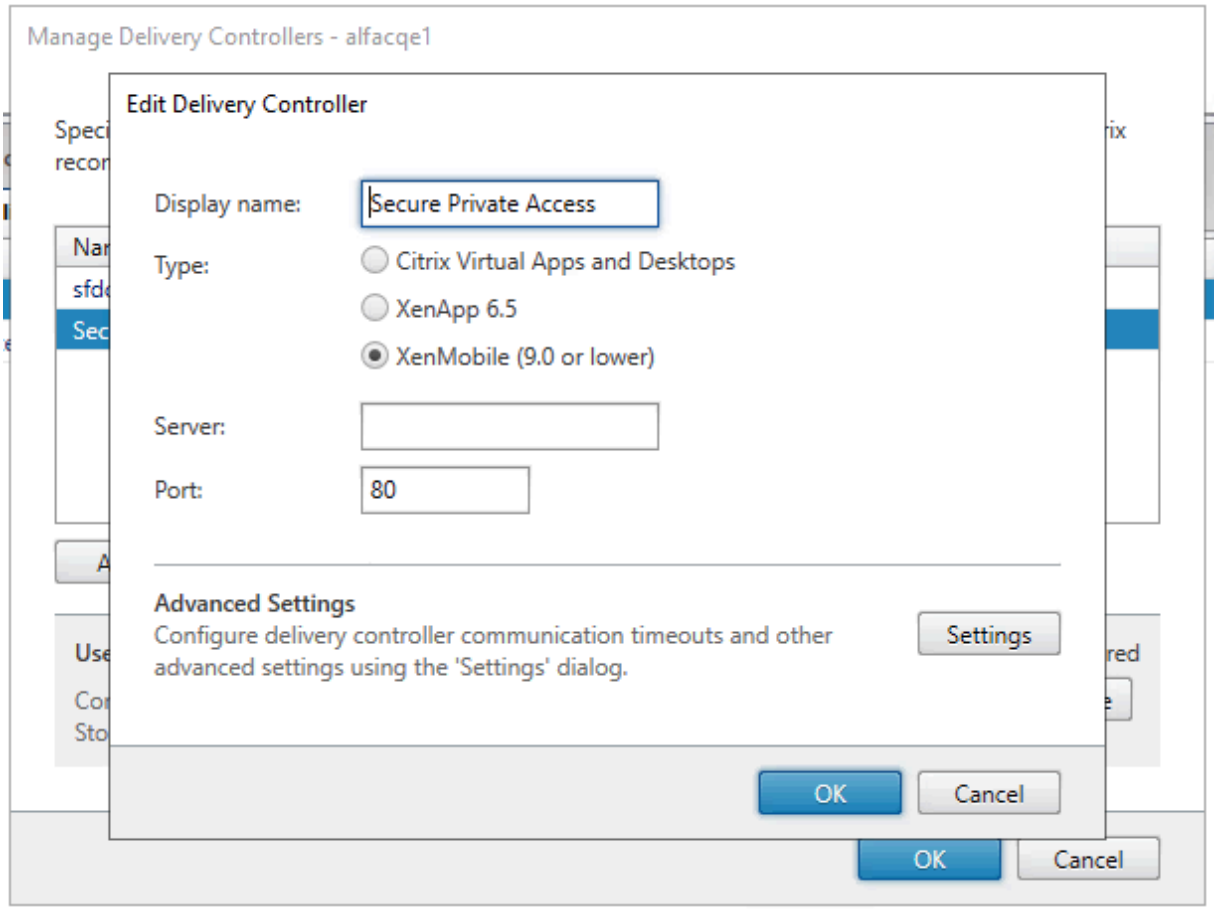
El script de StoreFront configura automáticamente la configuración del grupo de agregación para Secure Private Access si la misma está configurada para el Delivery Controller de Citrix Virtual Apps and Desktops. De forma predeterminada, el script configura el Secure Private Access para todos (**mapeo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

NetScaler Gateway

October 21, 2024

La configuración de NetScaler Gateway es compatible con aplicaciones Web/SaaS y TCP/UDP. Puede crear un NetScaler Gateway o actualizar una configuración de NetScaler Gateway existente para acceso privado seguro. Se recomienda crear instantáneas de NetScaler o guardar la configuración de NetScaler antes de aplicar estos cambios.

Para obtener detalles sobre las configuraciones de NetScaler Gateway para aplicaciones Web/SaaS y TCP/UDP, consulte los siguientes temas:

- Configuración de NetScaler Gateway para aplicaciones web/SaaS
- Configuración de NetScaler Gateway para aplicaciones TCP/UDP

Compatibilidad con las aplicaciones ICA

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

> **Nota**
>
> El servidor STA generalmente es parte de la implementación de Citrix Virtual Apps and Desktops.

Para obtener más detalles, consulte los siguientes temas:

- Configuración de la autoridad de tickets seguros en NetScaler Gateway
- Preguntas frecuentes: Autoridad de tickets seguros de Citrix Secure Gateway/NetScaler Gateway

Compatibilidad con etiquetas de acceso inteligente

> **Nota**
>
> - La información proporcionada en esta sección es aplicable solo si su versión de NetScaler Gateway es anterior a la 14.1-25.56.
> - Si su versión de NetScaler Gateway es 14.1–25.56 o posterior, puede habilitar el complemento Secure Private Access en NetScaler Gateway mediante la CLI o la GUI. Para obtener más detalles, consulte Habilitar el complemento de acceso privado seguro en NetScaler Gateway.

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 inteligente.

- 13.1–48.47 y posteriores
- 14.1–4.42 y posteriores

Las etiquetas de acceso inteligente se agregan como encabezado en la solicitud del complemento de acceso privado seguro.

Utilice el interruptor `ns_vpn_enable_spa_onprem` o `ns_vpn_disable_spa_onprem` para habilitar o deshabilitar esta función en estas versiones de NetScaler.

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

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

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

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

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

  ```
  nsapimgr -ys call=toggle_vpn_redirect_to_access_restricted_page_on_deny
  ```

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

  ```
  nsapimgr -ys call=toggle_vpn_use_cdn_for_access_restricted_page
  ```

- Para deshabilitarlo, ejecute el mismo comando nuevamente.
- Para verificar si el interruptor está activado o desactivado, ejecute el comando `nsconmsg` .
- Para configurar etiquetas de acceso inteligente en NetScaler Gateway, consulte Configurar etiquetas contextuales.

Persist Secure Private Access en la configuración del complemento NetScaler

Para conservar la configuración del complemento de acceso privado seguro en NetScaler, haga lo siguiente:

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

   ```
   nsapimgr -ys call=ns_vpn_enable_spa_onprem
   nsapimgr -ys call=toggle_vpn_enable_securebrowse_client_mode
   nsapimgr -ys call=toggle_vpn_redirect_to_access_restricted_page_on_deny

   nsapimgr -ys call=toggle_vpn_use_cdn_for_access_restricted_page
   ```

3. Guarde el archivo.

La configuración del complemento Secure Private Access se aplica automáticamente cuando se reinicia NetScaler.

Habilitar el complemento de acceso privado seguro en NetScaler Gateway

A partir de NetScaler Gateway 14.1–25.56 y versiones posteriores, puede habilitar el complemento Secure Private Access en NetScaler Gateway mediante la CLI o la GUI de NetScaler Gateway. Esta configuración reemplaza la perilla `nsapimgr_wr.sh -ys call=ns_vpn_enable_spa_onprem` utilizada en versiones anteriores a 2407.

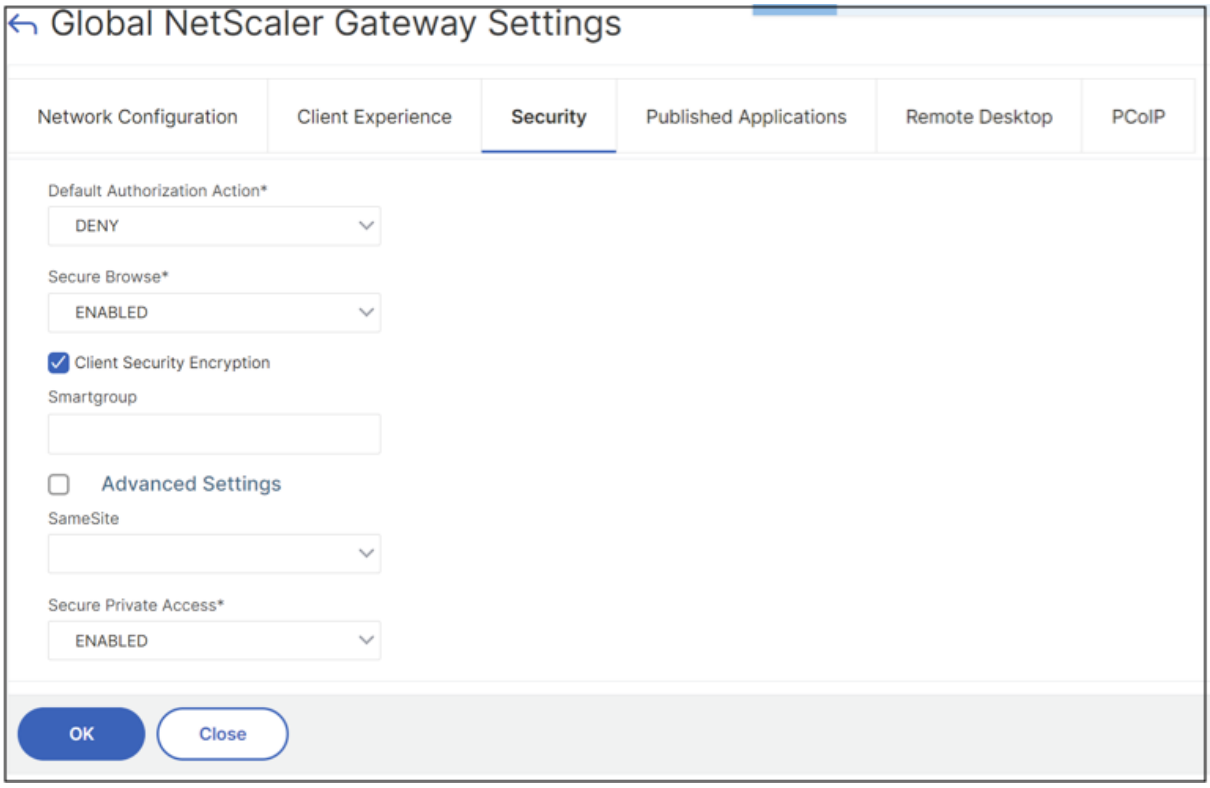
CLI:

En el símbolo del sistema, escriba el siguiente comando:

```
set vpn parameter -securePrivateAccess ENABLED
```

Interfaz gráfica de usuario:

1. Vaya a **NetScaler Gateway > Configuración global > Cambiar configuración global de NetScaler Gateway**.
2. Haga clic en la ficha **Seguridad**.
3. En **Acceso privado seguro**, seleccione **HABILITADO.**



Subir certificado de puerta de enlace pública

Si no se puede acceder a la puerta de enlace pública desde la máquina de acceso privado seguro, deberá cargar un certificado de puerta de enlace pública en la base de datos de acceso privado seguro.

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

1. Abra PowerShell o la ventana del símbolo del sistema con privilegios de administrador.
2. Cambie el directorio a la carpeta Admin\AdminConfigTool debajo de la carpeta de instalación de Secure Private Access (por ejemplo, cd "C:\Archivos de programa\Citrix\Citrix Access Security\Admin\AdminConfigTool")
3. Ejecute este comando:

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

Limitaciones conocidas

- Es posible actualizar un NetScaler Gateway existente mediante un script, pero puede haber una cantidad infinita de posibles configuraciones de NetScaler que no se puedan cubrir con un solo script.
- No utilice ICA Proxy en NetScaler Gateway. Esta función está deshabilitada cuando NetScaler Gateway está configurado.
- Si utiliza NetScaler implementado en la nube, deberá realizar cambios en la red. Por ejemplo, permitir comunicaciones entre NetScaler y otros componentes en determinados puertos.
- Si habilita SSO en NetScaler Gateway, asegúrese de que NetScaler se comunique con StoreFront mediante una dirección IP privada. Es posible que tengas que agregar un registro DNS de StoreFront a NetScaler con una dirección IP privada de StoreFront.

Configuración de NetScaler Gateway para aplicaciones web/SaaS

October 21, 2024

Para crear NetScaler Gateway para aplicaciones web/SaaS, realice los siguientes pasos:

1. Descargue el último script *`ns_gateway_secure_access.sh`*. desde https://www.citrix.com/downloads/citrix-secure-private-access/Shell-Script/.
2. Cargue estos scripts en la máquina NetScaler. Puede utilizar 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`*

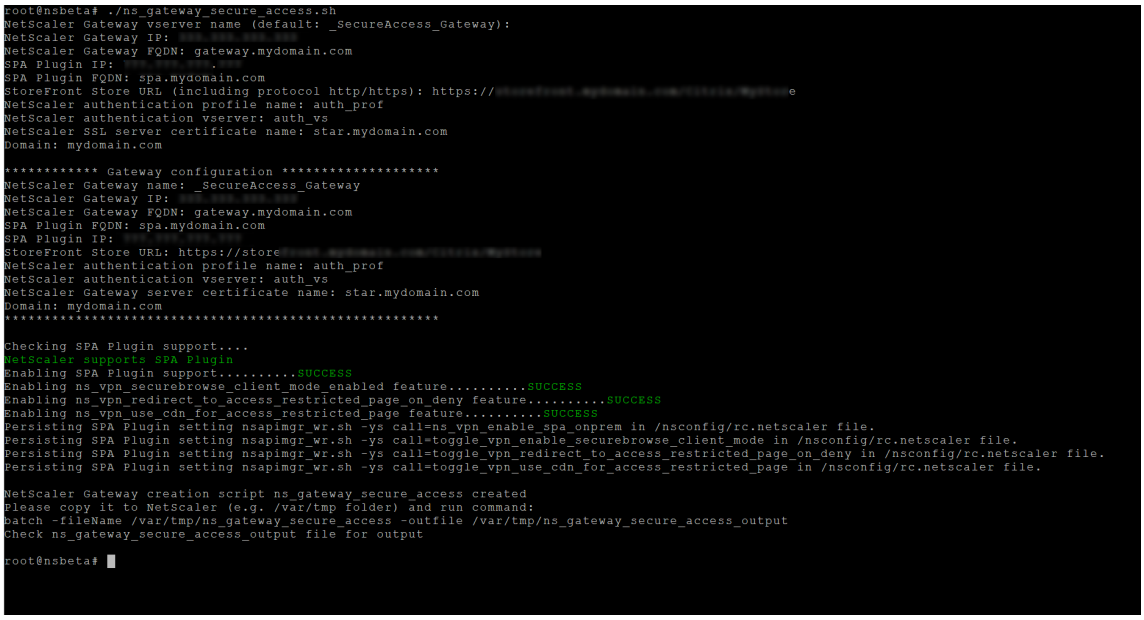
Nota

- Se recomienda utilizar la carpeta NetScaler /var/tmp para almacenar datos temporales.
- Asegúrese de que el archivo se guarde con 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 existe el archivo o directorio`, significa que los finales de línea son incorrectos. Puedes convertir el script utilizando cualquier editor de texto enriquecido, como Notepad++.

1. Acceda a NetScaler mediante SSH y cambie a shell (escriba 'shell'en la CLI de NetScaler).
2. Hacer que el script cargado sea ejecutable. Utilice el comando chmod para hacerlo.

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

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



4. Ingrese **N** para el parámetro **Habilitar compatibilidad con tipos de aplicaciones TCP/UDP** si desea configurar la puerta de enlace solo para aplicaciones web y SaaS.
5. 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 múltiples comandos 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 complemento Secure Private Access, el script habilita las funciones de NetScaler para admitir etiquetas de acceso inteligente que envían mejoras y redireccionan a una nueva página de denegación cuando se restringe el acceso a un recurso. Para obtener detalles sobre las etiquetas inteligentes, consulte Compatibilidad con etiquetas de acceso inteligente.
>
> Las características del complemento Secure Private Access persisten en el archivo /nsconfig/rc.netscaler y permiten mantenerlas habilitadas después de reiniciar NetScaler.

```
1 ![Configuración 2 de NetScaler](/en-us/citrix-secure-private-access/
     media/spaop-configure-netscaler2-old.png)
```

1. Cambie a la CLI de NetScaler y ejecute los comandos de NetScaler resultantes desde el nuevo archivo con el comando por lotes. 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 uno de los parámetros ingresados en el paso 6 es incorrecto.

2. Asegúrese de que todos los comandos se completen correctamente.

> **Nota**
>
> Si hay un error, NetScaler aún ejecuta los comandos restantes y crea/actualiza/vincula parcialmente los recursos. Por lo tanto, si ve un error inesperado debido a que uno de los parámetros es incorrecto, se recomienda rehacer la configuración desde el principio.

Actualizar la configuración existente de NetScaler Gateway para aplicaciones web y SaaS

Puede usar el script `ns_gateway_secure_access_update.sh`en un NetScaler Gateway existente para actualizar la configuración de las aplicaciones web y SaaS. Sin embargo, si desea actualizar la configuración existente (NetScaler Gateway versión 14.1–4.42 y posteriores) manualmente, utilice los comandos de ejemplo para actualizar una configuración existente de NetScaler Gateway. Además, debe actualizar la configuración de acciones de sesión y del servidor virtual NetScaler Gateway.

> **Nota**
>
> A partir de NetScaler Gateway 14.1–25.56 y versiones posteriores, puede habilitar el complemento Secure Private Access en NetScaler Gateway mediante la CLI o la GUI de NetScaler Gateway. Para obtener más detalles, consulte Habilitar el complemento de acceso privado seguro en NetScaler Gateway.

También puede utilizar los scripts en un NetScaler Gateway existente para admitir el acceso privado seguro. Sin embargo, el script no actualiza lo siguiente:

- Servidor virtual NetScaler Gateway existente
- Acciones de sesión existentes y políticas de sesión vinculadas a NetScaler Gateway

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

Configuración del servidor virtual NetScaler Gateway

Al agregar o actualizar el servidor virtual NetScaler Gateway existente, asegúrese de que los siguientes parámetros estén configurados en los valores definidos. Para ver comandos de muestra, consulte Comandos de ejemplo para actualizar una configuración existente de NetScaler Gateway.

Agregar un servidor virtual:

- Nombre de perfil tcp: nstcp_default_XA_XD_profile
- deploymentType: ICA_STOREFRONT (disponible solo con el comando `add vpn vserver`)
- icaOnly: DESACTIVADO

Actualizar un servidor virtual:

- Nombre de perfil tcp: nstcp_default_XA_XD_profile
- icaOnly: DESACTIVADO

Configuración de acciones de sesión de NetScaler Gateway

La acción de la sesión está vinculada a un servidor virtual de puerta de enlace con políticas de sesión. Al crear o actualizar una acción de sesión, asegúrese de que los siguientes parámetros estén configurados con los valores definidos. Para ver comandos de muestra, consulte Comandos de ejemplo para actualizar una configuración existente de NetScaler Gateway.

- `Intercepción transparente`: DESACTIVADO
- `SSO`: ACTIVADO
- `ssoCredential`: PRIMARIO

- usoMIP: NS
- useIIP: DESACTIVADO
- icaProxy: DESACTIVADO
- wihome: "https://storefront.mydomain.com/Citrix/MyStoreWeb" - reemplazar con la URL de la tienda real. La ruta a la tienda /Citrix/MyStoreWeb es opcional.
- Opciones del cliente: DESACTIVADO
- ntDomain: mydomain.com - utilizado para SSO (opcional)
- acción de autorización predeterminada: PERMITIR
- authorizationGroup: SecureAccessGroup (Asegúrese de que este grupo esté creado, se usa para vincular políticas de autorización específicas de Secure Private Access)
- modo VPN sin cliente: ACTIVADO
- clientlessModeUrlEncoding: TRANSPARENTE
- SecureBrowse: HABILITADO
- Storefronturl: "https://storefront.mydomain.com"
- sfGatewayAuthType: dominio

Comandos de ejemplo para actualizar una configuración existente de NetScaler Gateway

Agregar/actualizar 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
- set vpn vserver SecureAccess_Gateway -icaOnly OFF

Agregar una acción de sesión.

- add vpn sessionAction AC_OSspaonprem -transparentInterception OFF -defaultAuthorizationAction ALLOW -authorizationGroup SecureAccessGroup -SSO ON -ssoCredential PRIMARY -useMIP NS -useIIP OFF -icaProxy OFF -wihome "https://storefront.example.corp/Citrix/SPAWeb"-ClientChoices OFF -ntDomain example.corp -clientlessVpnMode ON -clientlessModeUrlEncoding TRANSPARENT -SecureBrowse ENABLED -storefronturl "https://storefront.example.corp"-sfGatewayAuthType domain
- add vpn sessionAction AC_WBspaonprem -transparentInterception OFF -defaultAuthorizationAction ALLOW -authorizationGroup SecureAccessGroup -SSO ON -ssoCredential PRIMARY -useMIP NS -useIIP OFF -icaProxy OFF -wihome "https://storefront.example.corp/Citrix/SPAWeb"-ClientChoices OFF -ntDomain example.corp -


```
clientlessVpnMode ON -clientlessModeUrlEncoding TRANSPARENT -
SecureBrowse ENABLED -storefronturl "https://storefront.example.
corp"-sfGatewayAuthType domain
```

Agregar una política de sesión.

- `add vpn sessionPolicy PL_OSspaonprem "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\")"AC_OSspaonprem`
- `add vpn sessionPolicy PL_WBspaonprem "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\").NOT && HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"plugin\").NOT"AC_WBspaonprem`

Vincula la política de sesión al servidor virtual VPN.

- `bind vpn vserver SecureAccess_Gateway -policy PL_OSspaonprem -priority 111 -gotoPriorityExpression NEXT -type REQUEST`
- `bind vpn vserver SecureAccess_Gateway -policy PL_WBspaonprem -priority 110 -gotoPriorityExpression NEXT -type REQUEST`

Vincula el complemento de acceso privado seguro al servidor virtual VPN.

- `bind vpn vserver spaonprem -appController "https://spa.example.corp"`

Para obtener detalles sobre los parámetros de acción de la sesión, vpn-sessionAction.

Información adicional

Para obtener información adicional sobre NetScaler Gateway for Secure Private Access, consulte los siguientes temas:

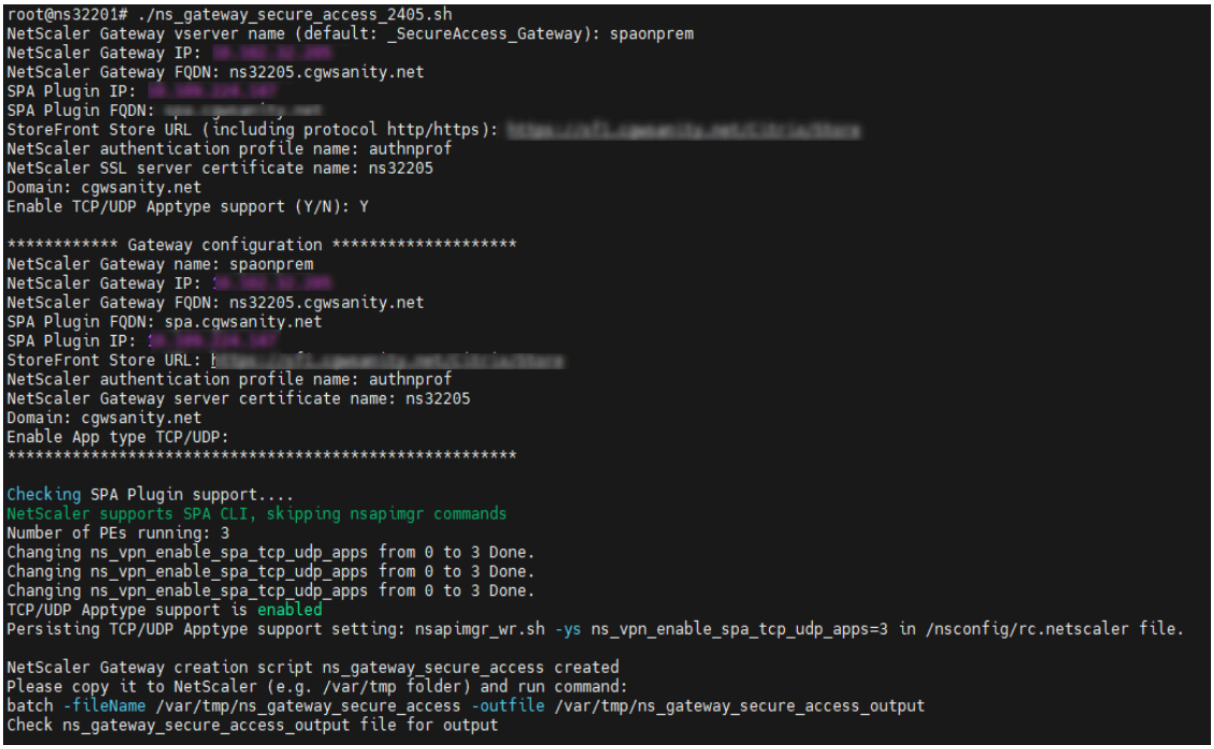
- Compatibilidad con las aplicaciones ICA
- Compatibilidad con etiquetas de acceso inteligente
- Persist Secure Private Access en la configuración del complemento NetScaler
- Habilitar el complemento de acceso privado seguro en NetScaler Gateway
- Subir certificado de puerta de enlace pública
- Limitaciones conocidas

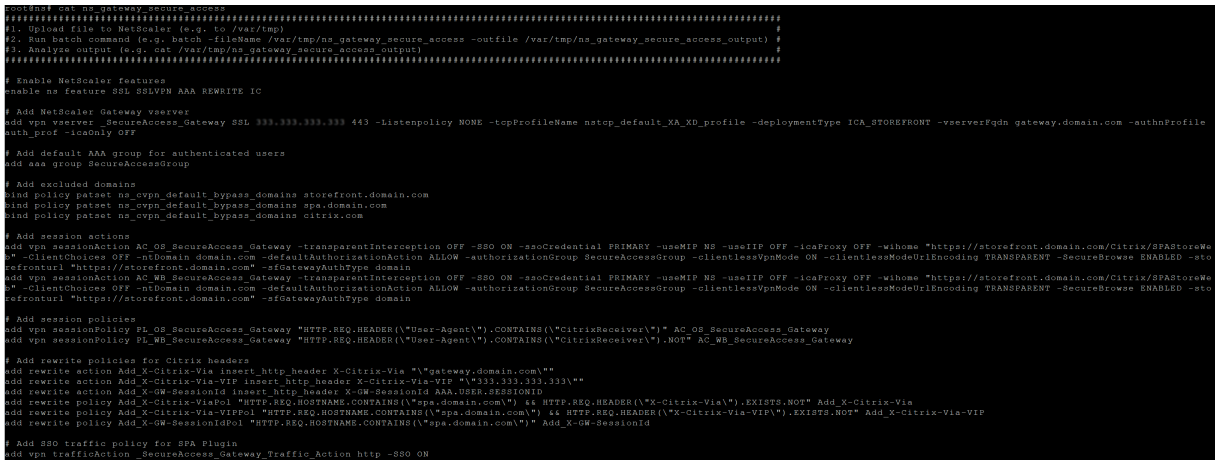
Configuración de NetScaler Gateway para aplicaciones TCP/UDP

October 21, 2024

Puede utilizar el procedimiento descrito en Configuración de NetScaler Gateway para aplicaciones web/SaaS para configurar aplicaciones TCP/UDP. Para configurar la puerta de enlace para aplicaciones TCP/UDP, debe habilitar la compatibilidad con TCP/UDP ingresando **Y** para el parámetro **Habilitar compatibilidad con tipos de aplicaciones TCP/UDP** en el script.

La siguiente figura muestra el parámetro **Habilitar compatibilidad con tipos de aplicaciones TCP/UDP** habilitado para compatibilidad con TCP/UDP.





Actualizar la configuración existente de NetScaler Gateway para aplicaciones TCP/UDP

Si está actualizando la configuración de versiones anteriores a 2407, se recomienda que actualice la configuración manualmente. Para obtener más detalles, consulte Comandos de ejemplo para actualizar una configuración de NetScaler Gateway existente. Además, debe actualizar la configuración de acciones de sesión y del servidor virtual NetScaler Gateway.

Configuración del servidor virtual NetScaler Gateway

Al agregar o actualizar el servidor virtual NetScaler Gateway existente, asegúrese de que los siguientes parámetros estén configurados en los valores definidos. Para ver comandos de muestra, consulte Comandos de ejemplo para actualizar una configuración existente de NetScaler Gateway. Además, debe actualizar la configuración de acciones de sesión y del servidor virtual NetScaler Gateway.

Agregar un servidor virtual:

- Nombre de perfil tcp: nstcp_default_XA_XD_profile
- deploymentType: ICA_STOREFRONT (disponible solo con el comando `add vpn vserver`)
- icaOnly: DESACTIVADO

Actualizar un servidor virtual:

- Nombre de perfil tcp: nstcp_default_XA_XD_profile
- icaOnly: DESACTIVADO

Para obtener detalles sobre los parámetros del servidor virtual, consulte vpn-sessionAction.

Configuración de la política de sesión de NetScaler Gateway

La acción de la sesión está vinculada a un servidor virtual de puerta de enlace con políticas de sesión. Al crear o actualizar una acción de sesión, asegúrese de que los siguientes parámetros estén configurados con los valores definidos. Para ver comandos de muestra, consulte Comandos de ejemplo para actualizar una configuración existente de NetScaler Gateway. Además, debe actualizar la configuración de acciones de sesión y del servidor virtual NetScaler Gateway.

- `Intercepción transparente`: ACTIVADO
- `SSO`: ACTIVADO
- `ssoCredential`: PRIMARIO
- `usoMIP`: NS
- `useIIP`: DESACTIVADO
- `icaProxy`: DESACTIVADO
- `Opciones del cliente`: ACTIVADO

- ntDomain: mydomain.com - utilizado para SSO (opcional)
- acción de autorización predeterminada: PERMITIR
- grupo de autorización: grupo de acceso seguro
- modo VPN sin cliente: DESACTIVADO
- clientlessModeUrlEncoding: TRANSPARENTE
- SecureBrowse: HABILITADO

Comandos de ejemplo para actualizar una configuración existente de NetScaler Gateway

> **Nota**
>
> Si está actualizando manualmente la configuración existente, además de los siguientes comandos, debe actualizar el archivo /nsconfig/rc.netscaler con el comando `nsapimgr_wr.sh -ys ns_vpn_enable_spa_tcp_udp_apps=3`.

- Agregue una acción de sesión VPN para admitir conexiones basadas en Citrix Secure Access.

```
add vpn sessionAction AC_AG_PLGspaonprem -splitDns BOTH -splitTunnel
 ON -transparentInterception ON -defaultAuthorizationAction ALLOW
 -authorizationGroup SecureAccessGroup -SSO ON -ssoCredential
PRIMARY -useMIP NS -useIIP OFF -icaProxy OFF -ClientChoices ON -
ntDomain example.corp -clientlessVpnMode OFF -clientlessModeUrlEncoding
 TRANSPARENT -SecureBrowse ENABLED
```

- Agregue una política de sesión VPN para admitir conexiones basadas en Citrix Secure Access.

```
add vpn sessionPolicy PL_AG_PLUGINspaonprem "HTTP.REQ.HEADER
(\"User-Agent\").CONTAINS(\"CitrixReceiver\").NOT && (HTTP.REQ
.HEADER(\"User-Agent\").CONTAINS(\"plugin\")|| HTTP.REQ.HEADER(\"
User-Agent\").CONTAINS(\"CitrixSecureAccess\"))"AC_AG_PLGspaonprem
```

- Vincula la política de sesión al servidor virtual VPN para admitir conexiones basadas en Citrix Secure Access.

```
bind vpn vserver spaonprem -policy PL_AG_PLUGINspaonprem -priority
 105 -gotoPriorityExpression NEXT -type REQUEST
```

- Agregue una política de llamada HTTP para admitir la validación de autorización para conexiones basadas en TCP/UDP.

> **Nota**
>
> Este paso solo es necesario si su versión de NetScaler Gateway es inferior a 14.1-29.x.


```
`add policy httpCallout SecureAccess_httpCallout_TCP -IPAddress
   192.0.2.24 -port 443  -returnType BOOL -httpMethod POST -hostExpr "
   \"spa.example.corp\"" -urlStemExpr "\"/secureAccess/authorize\"" -
   headers Content-Type("application/json") X-Citrix-SecureAccess-Cache
   ("dstip="+HTTP.REQ.HEADER("CSIP").VALUE(0)+"&sessid="+aaa.user.
   sessionid) -bodyExpr q/"{
 "+"\"userName\":\""+aaa.USER.NAME.REGEX_REPLACE(re#\\#,"\\\\",ALL)+"
    \","+"\"domain\":\""+aaa.USER.DOMAIN+"\","+"\"customTags\":\""+http
    .REQ.HEADER("X-Citrix-AccessSecurity").VALUE(0)+"\","+"\"
    gatewayAddress\":\"ns224158.example.corp\","+"\"userAgent\":\"
    CitrixSecureAccess\","+"\"applicationDomain\":\""+http.REQ.HEADER("
    CSHOST").VALUE(0)+"\","+"\"smartAccessTags\":\""+aaa.user.attribute
    ("smartaccess_tags")+"\",\"applicationType\":\"ztna\",\"
    applicationDetails\":{
 \"destinationIp\":\""+HTTP.REQ.HEADER("CSIP").VALUE(0)+"\",\"
    destinationPort\":\""+HTTP.REQ.HEADER("PORT").VALUE(0)+"\",\"
    protocol\":\"TCP\" }
  }
 "/ -scheme https -resultExpr "http.RES.HEADER(\"X-Citrix-SecureAccess-
    Decision\").contains(\"ALLOW\")"`

donde
-  **192.0.2.24** es la dirección IP del complemento de acceso privado
   seguro
-  **spa.example.corp** es el FQDN del complemento Secure Private
   Access
-  **ns224158.example.corp** es el FQDN del servidor virtual VPN de la
   puerta de enlace
```

- Agregue una política de autorización para admitir conexiones basadas en TCP/UDP.

  ```
  add authorization policy SECUREACCESS_AUTHORIZATION_TCP "HTTP.REQ
  .URL.EQ(\"/cs\")&& HTTP.REQ.HEADER(\"PRTCL\").EQ(\"TCP\")&& sys.
  HTTP_CALLOUT(SecureAccess_httpCallout_TCP)"ALLOW
  ```

- Vincula la política de autorización al grupo de autenticación y autorización para admitir aplicaciones basadas en TCP/UDP.

  ```
  bind aaa group SecureAccessGroup -policy SECUREACCESS_AUTHORIZATION_TCP
   -priority 1010 -gotoPriorityExpression END
  ```

- Vincula el complemento de acceso privado seguro al servidor virtual VPN.

  ```
  bind vpn vserver spaonprem -appController "https://spa.example.
  corp"
  ```

Información adicional

Para obtener información adicional sobre NetScaler Gateway para acceso privado seguro, consulte los siguientes temas:

Etiquetas contextuales

October 21, 2024

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

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

El complemento de acceso privado seguro puede recibir etiquetas de acceso inteligente como encabezado (nueva lógica) o realizando devoluciones de llamadas a Gateway. Para obtener más detalles, consulte Etiquetas de acceso inteligente.

> **Nota**
>
> - A partir de NetScaler Gateway 14.1-25.x y versiones posteriores, se admiten las políticas de EPA de nFactor.
> - Si su versión de NetScaler Gateway es inferior a 14.1-25.x, solo se podrán configurar políticas de preautenticación de puerta de enlace clásica en NetScaler Gateway.

Configurar etiquetas personalizadas mediante la GUI

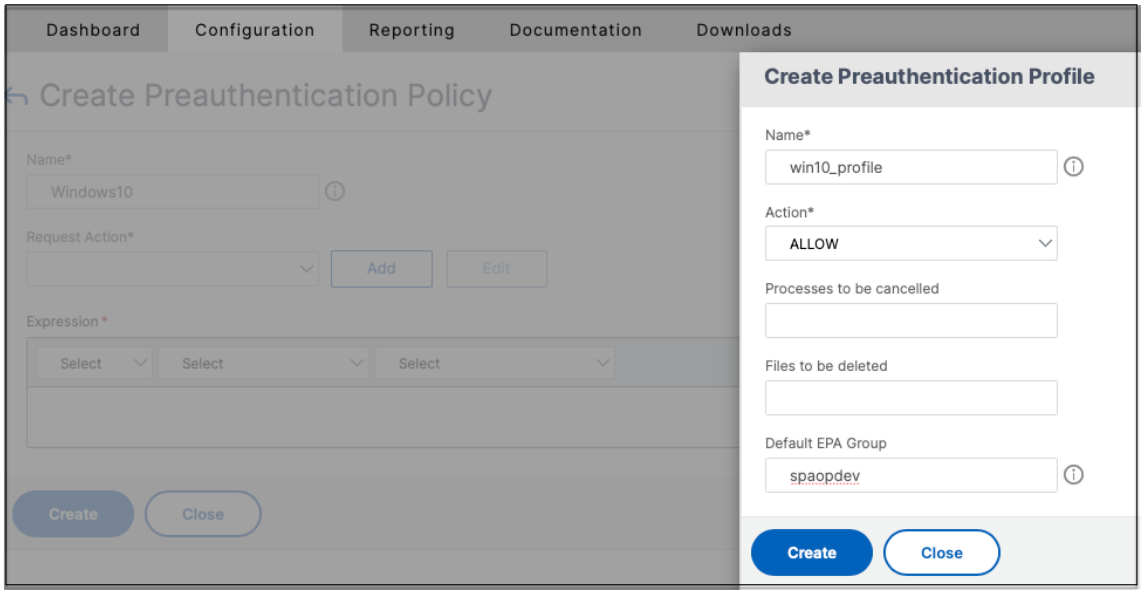
Los siguientes pasos de alto nivel están involucrados en la configuración de etiquetas contextuales.

1. Configurar una política de preautenticación de puerta de enlace clásica
2. Vincular la política de preautenticación clásica al servidor virtual de puerta de enlace

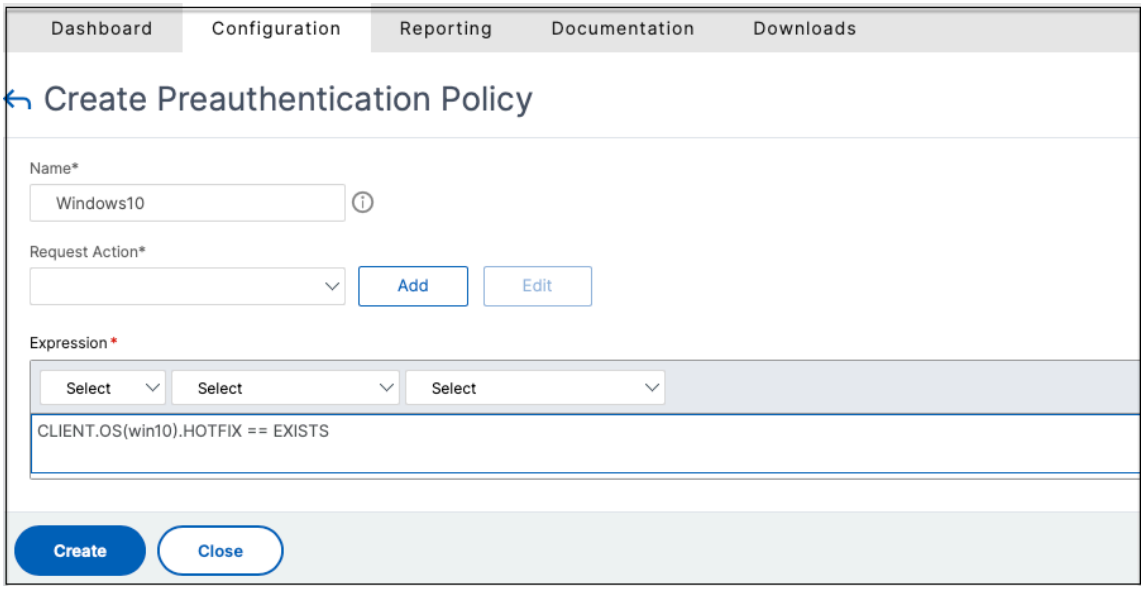
Configurar una política de preautenticación de puerta de enlace clásica

1. Vaya a **NetScaler Gateway > Políticas > Preautenticación** y luego haga clic en **Agregar**.

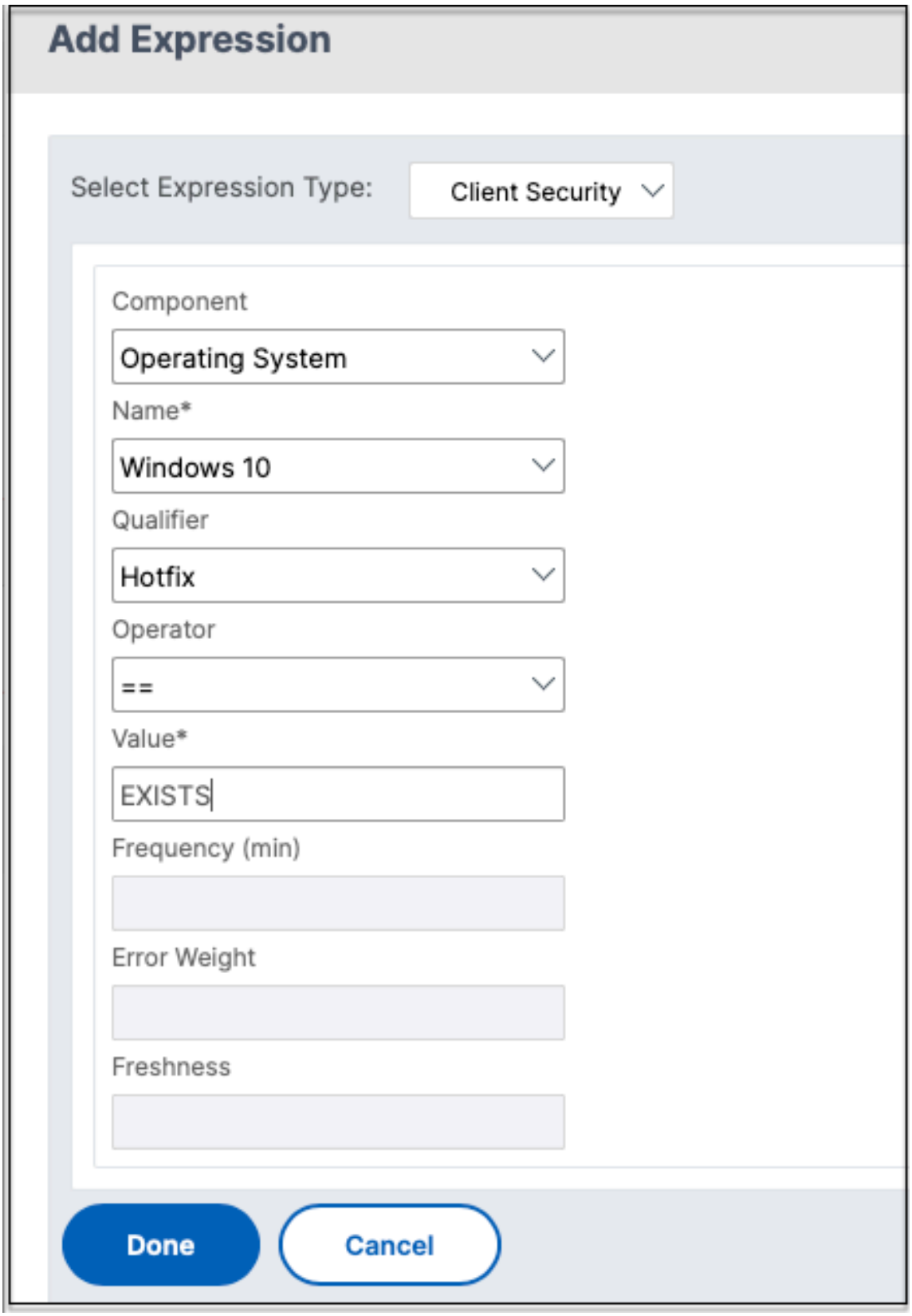
2. Seleccione una política existente o agregue un nombre para la política. Este nombre de política se utiliza como valor de etiqueta personalizada.
3. En **Solicitar acción**, haga clic en **Agregar** para crear una acción. Puede reutilizar esta acción para múltiples políticas, por ejemplo, utilizar una acción para permitir el acceso y otra para denegarlo.



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



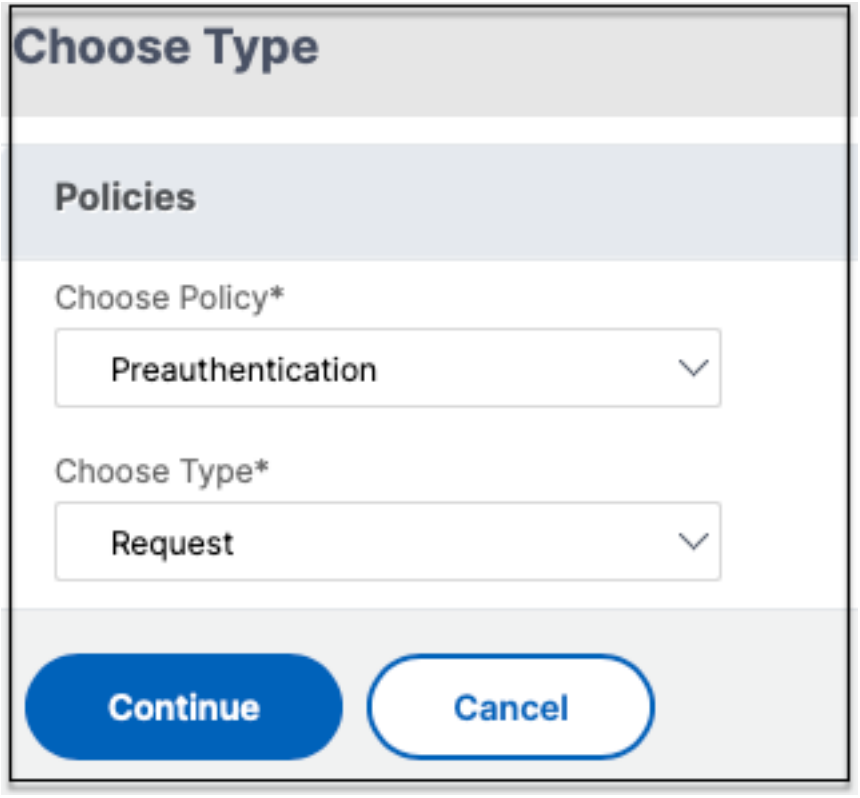
La siguiente figura muestra una expresión de muestra construida para verificar el sistema operativo Windows 10.



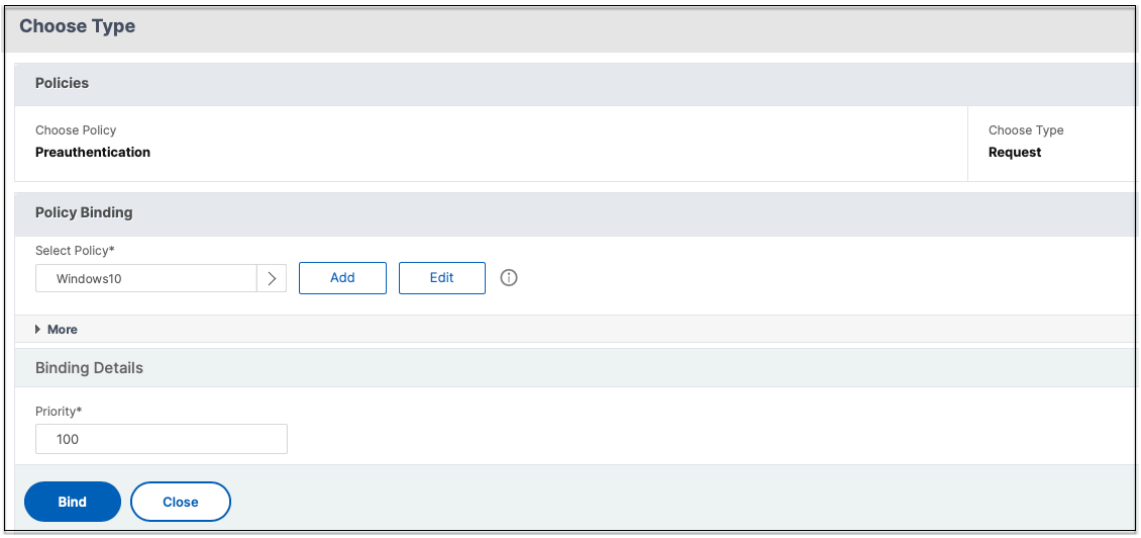
6. Haga clic en **Create**.

Vincular la etiqueta personalizada a NetScaler Gateway

1. Vaya a **NetScaler Gateway**> Servidores virtuales.
2. Seleccione el servidor virtual para el cual se vinculará la política de preautenticación y luego haga clic en **Editar**.
3. En la sección **Políticas** , haga clic en **+** para vincular la política.
4. En **Elija Política**, seleccione la política de preautenticación y seleccione **Solicitud** en **Elija Tipo**.



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



Configurar etiquetas personalizadas mediante la CLI

Ejecute los siguientes comandos de muestra en la CLI de NetScaler para crear y vincular una política de preautenticación:

- `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`

Ejecute el siguiente comando de muestra en la CLI de NetScaler para configurar la política de EPA de nFactor:

- `add authentication epaAction epaallowact -csecexpr "sys.client_expr(\"proc_0_notepad.exe\")"-defaultEPAGroup allow_app -quarantineGroup deny_app`
- `add authentication Policy epaallow -rule true -action epaallowact`

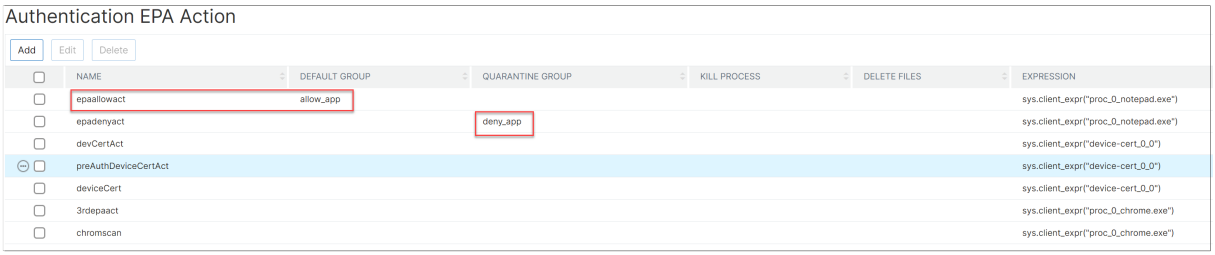
Agregar una nueva etiqueta contextual

1. Abra la consola de administración de Secure Private Access y haga clic en **Políticas de acceso**.
2. Crear una nueva política o editar una política existente.
3. En la sección **Condición** , haga clic en **Agregar condición** y seleccione **Etiquetas contextuales**, **Coincide con todos los**y luego ingrese el nombre de la etiqueta contextual (por ejemplo, `Windows10`).

Nota sobre las etiquetas de la EPA enviadas al complemento Secure Private Access

El nombre de la acción de EPA configurado en la política de nFactor EPA y el nombre del grupo asociado como etiquetas de acceso inteligente al complemento de acceso privado seguro. Sin embargo, las etiquetas que se envían dependen del resultado de la evaluación de acciones de la EPA.

- Si todas las acciones de EPA en una política de EPA de nFactor dan como resultado la acción **DENY** y se configura un grupo de cuarentena en la última acción, el nombre del grupo de cuarentena se envía como acceso inteligente.
- Si una acción de EPA en una política de EPA de nFactor da como resultado la acción **ALLOW**, los nombres de la política de EPA asociados con la acción y el nombre del grupo predeterminado (si está configurado) se envían como etiquetas de acceso inteligente.



En este ejemplo, cuando se niega la acción, se envía *deny_app* como etiqueta de acceso inteligente al complemento de acceso privado seguro. Cuando se permite la acción, *epaallowact* y *allow_app*se envían como etiquetas de acceso inteligente al complemento de acceso privado seguro.

Referencias

- Configurar políticas de acceso para las aplicaciones.
- Soporte para etiquetas de acceso inteligente.

Servidor de licencias

October 21, 2024

Un servidor de licencias para el complemento Secure Private Access es un componente obligatorio necesario para recopilar y procesar datos de licencias. Se puede registrar un servidor de licencias con Secure Private Access durante la configuración inicial o también se puede configurar o actualizar una vez completada la configuración. Para obtener detalles sobre cómo registrar un servidor de licencias con Secure Private Access, consulte Integrar servidores StoreFront y NetScaler Gateway.

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

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

Parámetros de la herramienta de configuración

Los siguientes parámetros de la herramienta de configuración están disponibles para el servidor de licencias:

- Hash - `.\AdminConfigTool.exe LICENSE_SERVER_ENABLE_HASHING <true|false>`
- Descarga de datos PII - `.\AdminConfigTool.exe DOWNLOAD_PII_DATA <filename>`

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

Cliente de Citrix Secure Access

October 21, 2024

Con el cliente Citrix Secure Private Access ahora puede acceder a todas las aplicaciones privadas, incluidas las aplicaciones TCP/UDP y HTTPS/HTTP, ya sea mediante un navegador nativo o una aplicación cliente nativa a través del cliente Citrix Secure Access que se ejecuta en su máquina.

Con el soporte adicional de aplicaciones TCP/UDP dentro de Citrix Secure Private Access, ahora puede eliminar la dependencia de una solución VPN tradicional para brindar acceso a todas las aplicaciones privadas para usuarios remotos.

Funcionamiento

Los usuarios finales pueden acceder fácilmente a todas sus aplicaciones privadas autorizadas simplemente instalando el cliente Citrix Secure Access en sus dispositivos cliente.

- Para Windows, la versión del cliente (24.6.1.17 y posteriores) se puede descargar desde https://www.citrix.com/downloads/citrix-gateway/plug-ins/citrix-secure-access-client-for-windows.html.
- Para macOS, la versión del cliente (24.06.2 y posteriores) se puede descargar desde la aplicación

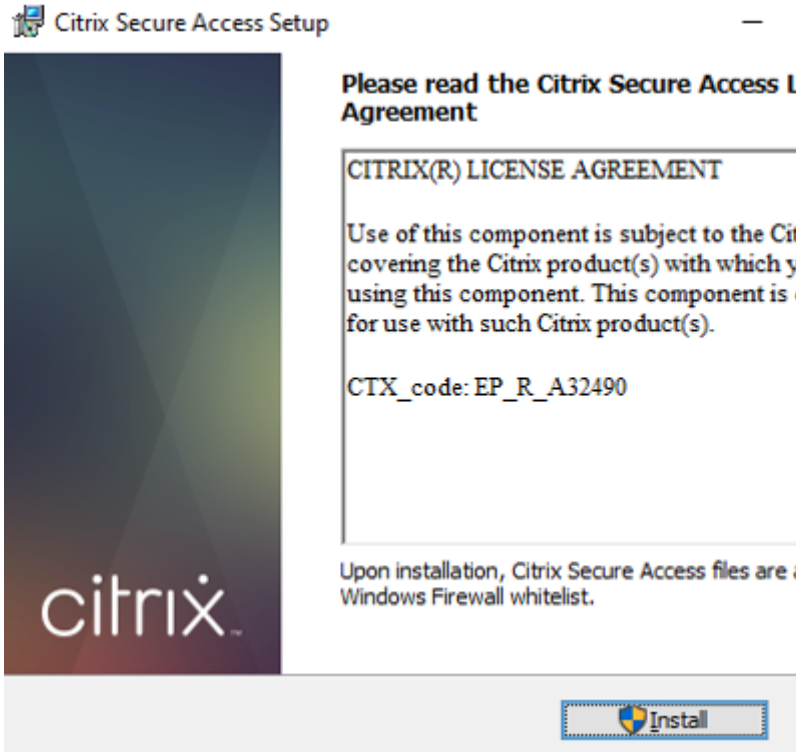
Instalar el cliente Citrix Secure Access en una máquina Windows

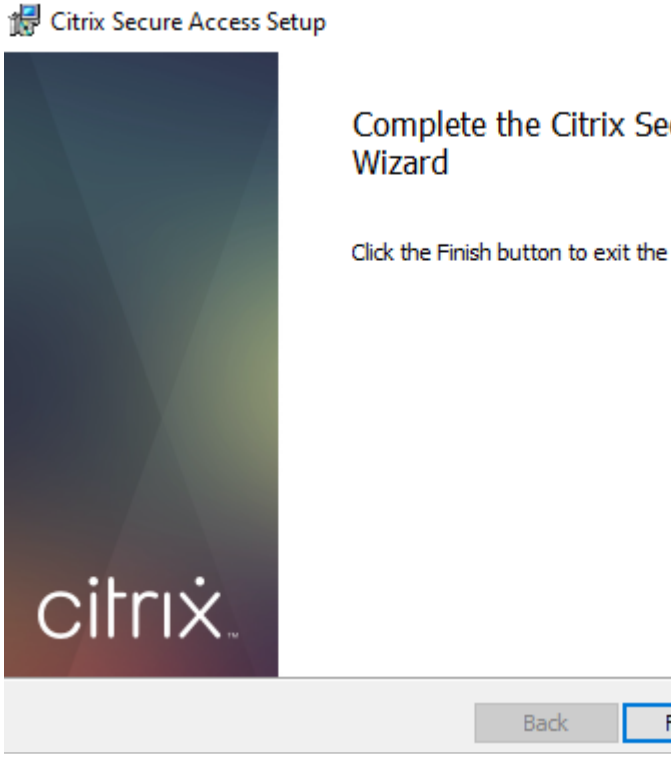
Versiones de sistema operativo compatibles:

Ventanas: Windows 11, Windows 10, Windows Server 2016 y Windows Server 2019.

A continuación se muestran los pasos para instalar el cliente Citrix Secure Access en una máquina Windows.

1. Descargue el cliente Citrix Secure Access desde https://www.citrix.com/downloads/citrix-gateway/plug-ins/citrix-secure-access-client-for-windows.html.
2. Haga clic en **Instalar** para instalar el cliente en su máquina Windows. Si tiene un cliente Citrix Gateway existente, el mismo se actualiza.





3. Haga clic en **Finalizar** para completar la instalación.

> **Nota**
>
> No se admiten sesiones multiusuario en Windows.

Instalar el cliente Citrix Secure Access en una máquina macOS

1. Descargue el cliente Citrix Secure Access para macOS desde la App Store.
2. Haga clic en **Abrir** una vez que se complete la descarga.

> **Nota**
>
> - El cliente Citrix Secure Access para macOS está disponible a partir de macOS 10.15 (Catalina) y versiones posteriores.
> - Las versiones preliminares están disponibles en la aplicación TestFlight solo para macOS Monterey (12.x).
> - Si cambia entre la aplicación App Store y la aplicación de vista previa TestFlight, debe volver a crear el perfil que desea usar con la aplicación Citrix Secure Access. Por ejemplo, si ha estado utilizando un perfil de conexión con `blr.abc.company.com`, elimine el perfil VPN y vuelva a crear el mismo perfil.

Versiones de sistema operativo compatibles:

macOS - 14.x (Sonoma), 13.x (Ventura), 12.x (Monterey)

Funciones no disponibles

Las siguientes funciones no son compatibles con la solución Secure Private Access para instalaciones locales.

- Siempre encendido antes del inicio de sesión de Windows (túnel de la máquina)
- DNS-TCP

Plataformas de cliente no compatibles

Las siguientes plataformas no son compatibles con la solución Secure Private Access para instalaciones locales.

- Linux
- iOS
- Android

Director

October 21, 2024

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

El registro de Director con acceso privado seguro es una configuración obligatoria para el acceso privado seguro para los clientes de la versión 2402 en las instalaciones. Si no tiene Director configurado, debe instalar la última versión de Director, LTSR 2402 o posterior. Si ya tiene Director configurado, debe actualizarlo a la última versión, LTSR 2402 o posterior. La configuración del acceso privado seguro no se puede completar sin registrar un Director. La validación también falla en los siguientes casos.

- El director no está registrado en Secure Private Access.
- La dirección IP del Director o el FQDN que ha ingresado no existe.

Para obtener detalles sobre cómo registrar Director con Secure Private Access, consulte Integrar servidores StoreFront y NetScaler Gateway y Administrar configuraciones después de la instalación.

Nota

- A partir de Secure Private Access 2407 o posterior, las sesiones TCP/UDP también se muestran además de las aplicaciones web/SaaS en el panel de Director.
- El registro o inicio de sesión del director no es compatible con la autenticación integrada de Windows (IWA). Si el administrador ha iniciado sesión en la consola de acceso privado seguro mediante IWA, se le solicitará que ingrese las credenciales para el registro del Director.
- Si el administrador ha realizado un inicio de sesión manual en la consola de acceso privado seguro, esos detalles se utilizan para autenticarse en el servidor Director. Si esto no tiene éxito, se le solicitará al administrador que ingrese las credenciales.
- Si el administrador tiene que agregar un Director diferente después de completar la configuración, registre al nuevo Director desde la página **Administrar configuraciones** . Al actualizar los detalles del Director después de la configuración, los administradores deben ingresar las credenciales para realizar los cambios. El inicio de sesión único no es compatible para editar la URL del Director IPv6, SSLv3.

Configurar Director con acceso privado seguro mediante la herramienta de configuración de Director

Configurar Director con acceso privado seguro mediante la herramienta de configuración es un paso obligatorio para que la integración se complete. Para obtener más detalles, consulte Integración de acceso privado seguro con Director.

Ver sesiones de usuario de Secure Private Access en Director

Puede ver las sesiones de usuario de Ver acceso privado seguro en Director. Para obtener más detalles, consulte Ver una sesión de acceso privado seguro por el usuario.

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.

Para habilitar esta integración, debe instalar Web Studio versión 2308 o posterior.

Para obtener más información, consulte Integración de Secure Private Access con Web Studio.

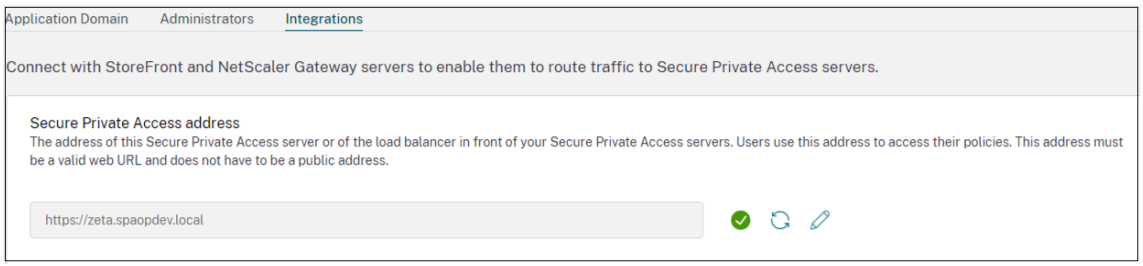
Implementar Secure Private Access como un clúster

October 21, 2024

La solución local Secure Private Access se puede implementar como un clúster para lograr alta disponibilidad, alto rendimiento y escalabilidad. Para implementaciones grandes (por ejemplo, más de 5000 usuarios), se pueden implementar múltiples nodos de acceso privado seguro separados para distribuir la carga de trabajo y mejorar la escalabilidad.

Crear nodos de acceso privado seguro

- Crear un nuevo sitio de acceso privado seguro. Para obtener más detalles, consulte Configurar un sitio de acceso privado seguro.
- Agregue la cantidad necesaria de nodos de clúster al sitio de acceso privado seguro. Para obtener más detalles, consulte Configurar acceso privado seguro uniéndose a un sitio existente.
- En cada nodo de acceso privado seguro, configure los mismos certificados de servidor. El nombre común del sujeto del certificado o el nombre alternativo del sujeto debe coincidir con el FQDN del equilibrador de carga.
- Al configurar el primer nodo en Secure Private Access, utilice los nombres del balanceador de carga. Para agregar los nodos subsiguientes, especifique la dirección de la base de datos en la pestaña Integraciones y ejecute manualmente el script de la base de datos. Para obtener detalles sobre cómo actualizar 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 acceso privado seguro. Si utiliza NetScaler como equilibrador de carga, 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 está utilizando 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 un acceso privado seguro, es suficiente configurar un balanceador de carga. Para obtener más detalles, consulte Equilibrio de carga con NetScaler. Antes de configurar el acceso privado seguro, se debe configurar la tienda StoreFront. Si utiliza un balanceador de carga, configure la URL base con el nombre del balanceador de carga y utilice HTTPS para una comunicación segura. Para obtener más detalles, consulte Cómo proteger StoreFront con HTTPS.

- Se recomienda que los servicios de acceso privado seguro se ejecuten como HTTPS, pero esto no es un requisito obligatorio. Los servicios de acceso privado seguro también se pueden implementar como HTTP.
- Se admite la descarga SSL o el puente SSL, por lo que se puede utilizar cualquier configuración de equilibrador de carga. Al utilizar el puente SSL, asegúrese de configurar los mismos certificados de servidor en cada nodo de acceso privado seguro. Además, el nombre común del sujeto del certificado o el nombre alternativo del sujeto (SAN) debe coincidir con el FQDN del equilibrador de carga. Además, SAN debe configurarse en el servicio Load Balancer.
- El certificado SSL correcto está vinculado al servidor IIS y a NetScaler.
- Se utilizan cifrados seguros.
- Los servicios de acceso privado seguro (tanto de administración como de tiempo de ejecución) no tienen estado, por lo que no se requiere persistencia.
- Los balanceadores de carga (por ejemplo, NetScaler) tienen monitores (sondas) integrados predeterminados para servidores back-end. Si debe configurar un monitor (sonda) personalizado basado en HTTP para servidores locales de Secure Private Access, se puede utilizar el siguiente punto final:

  `/secureAccess/health`

  Respuesta esperada:

```
1    Http status code: 200 OK
2
3    Payload:
4
5    {
6  "status":"OK","details":{
7  "duration":"00:00:00.0084206","status":"OK" }
8   }
```

  Para obtener detalles sobre cómo configurar un balanceador de carga NetScaler, consulte Configurar el balanceo de carga básico.

Crear un monitor para el acceso privado seguro

Utilice el siguiente comando CLI para crear un monitor para acceso privado seguro.


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

Después de crear un monitor, vincule el certificado al monitor.

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

Configurar el complemento de acceso privado seguro

October 21, 2024

Después de instalar el complemento Citrix Secure Access, puede configurar el entorno de acceso privado seguro y luego configurar aplicaciones y políticas de acceso para las aplicaciones. Secure Private Access admite aplicaciones Web/SaaS y TCP/UDP. Las políticas de acceso le permiten habilitar o deshabilitar el acceso a las aplicaciones según el usuario o los grupos de usuarios. Además, puedes habilitar el acceso restringido a las aplicaciones (HTTP/HTTPS y TCP/UDP) habilitando las restricciones de seguridad adecuadas.

- Configurar aplicaciones HTTP/HTTPS
- Configurar aplicaciones TCP/UDP
- Configurar TCP/UDP: aplicaciones de servidor a cliente
- Configurar políticas de acceso para las aplicaciones
- Opciones de restricción de acceso

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.

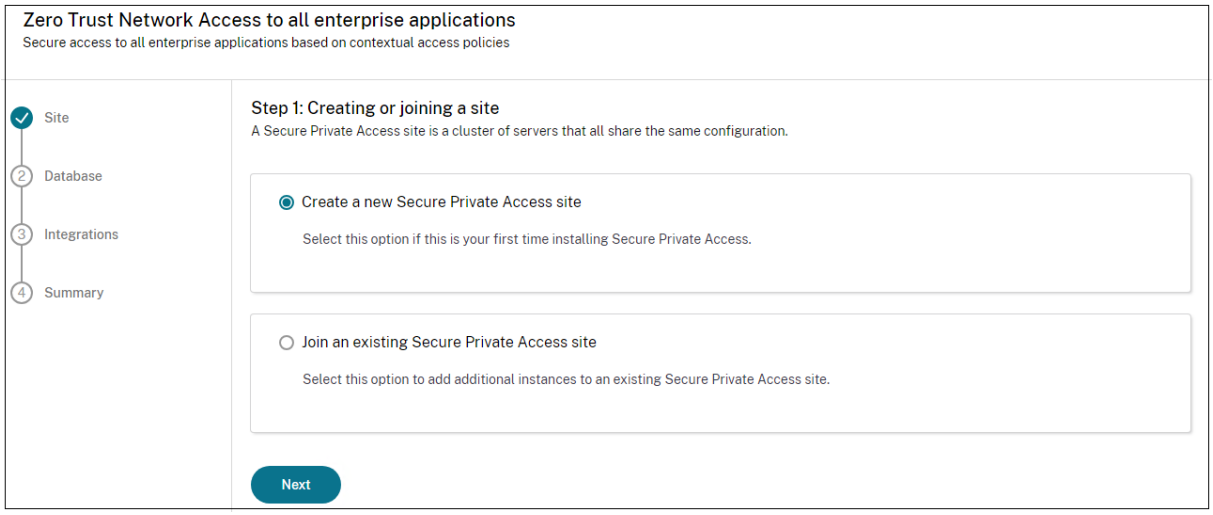
- El servidor de base de datos SQL debe estar instalado antes de crear un sitio.

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

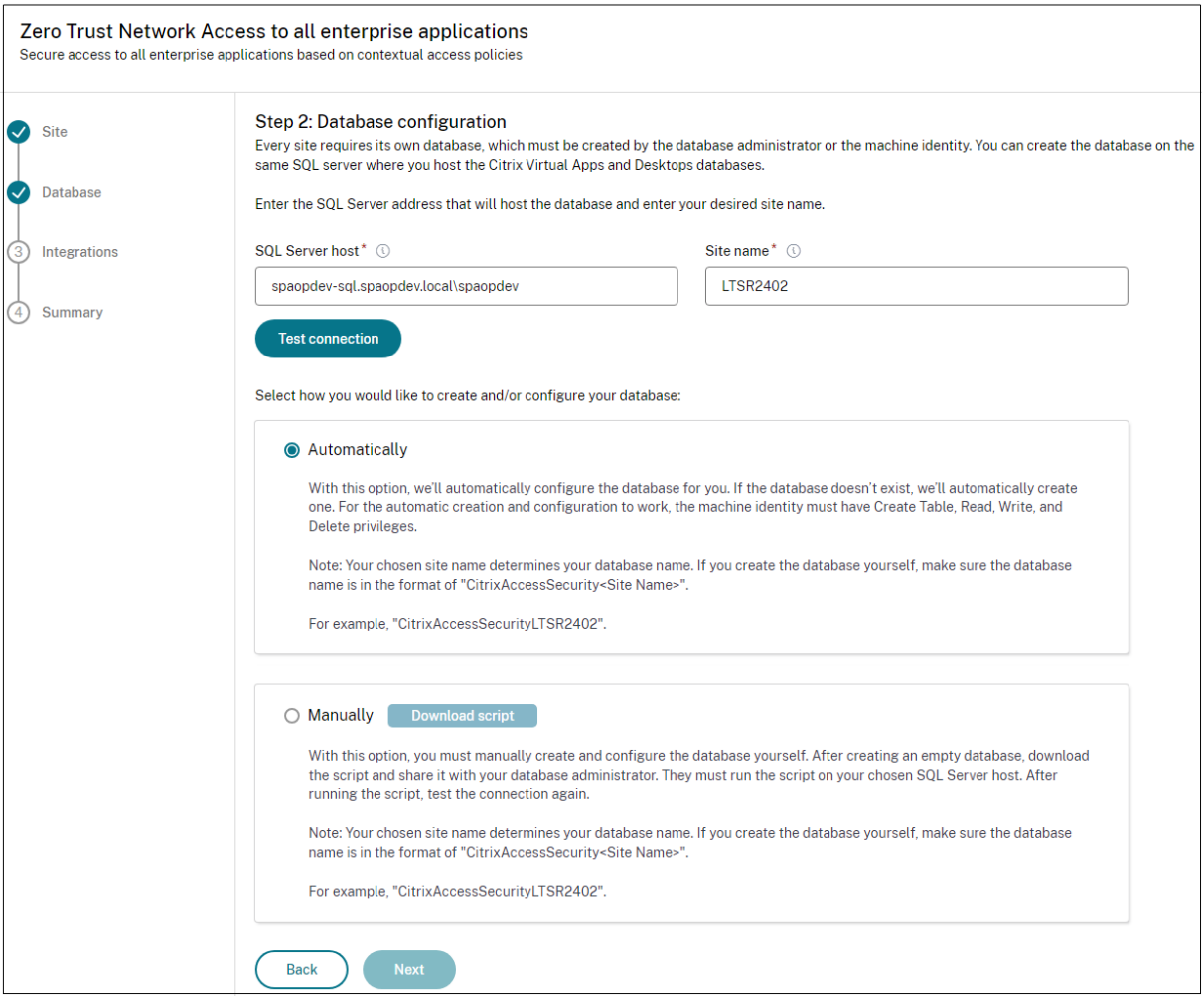
- NombreServidor\NombreInstancia
- NombreServidor,NúmeroPuerto

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.

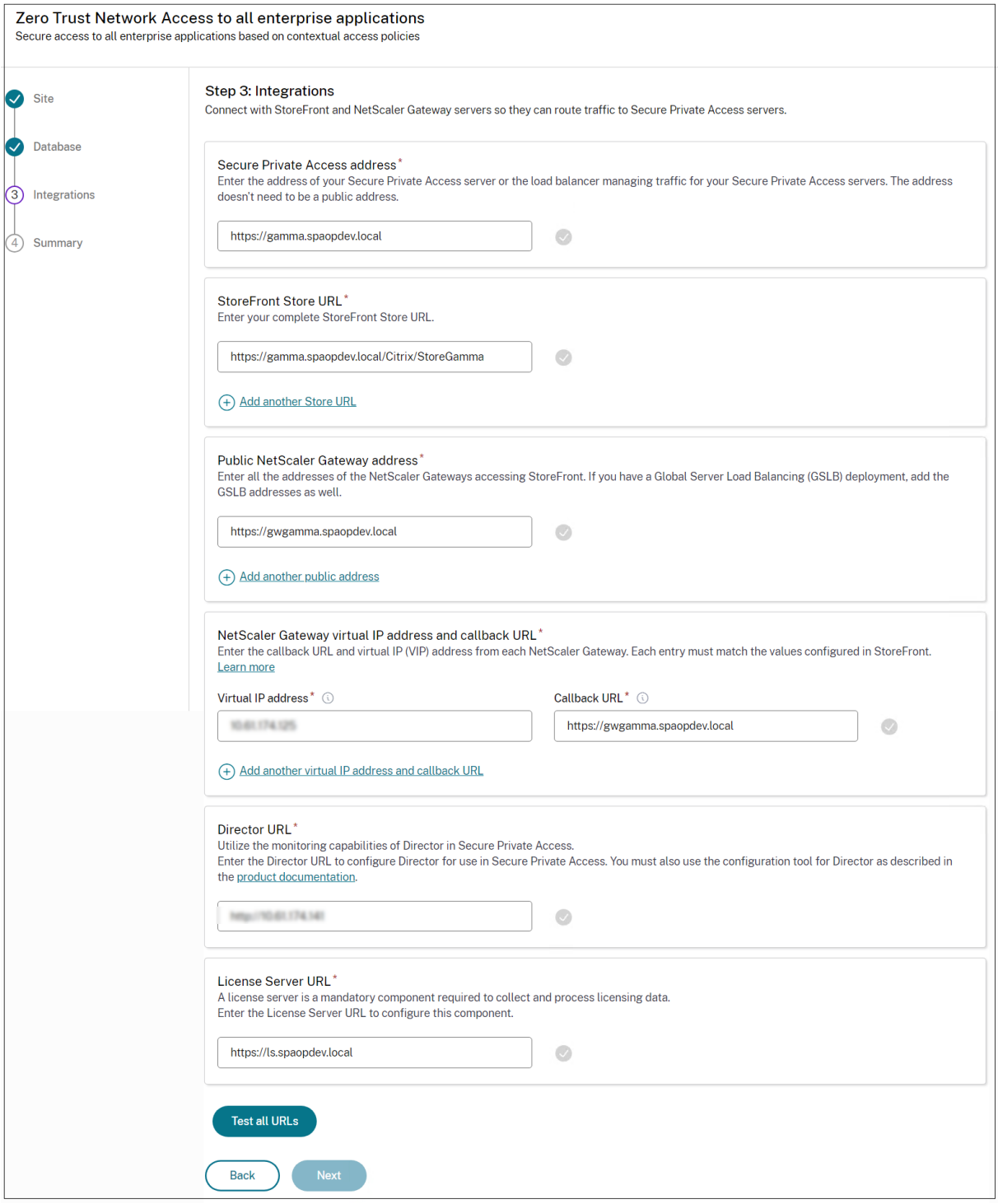
Paso 3: Integrar servidores

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**.

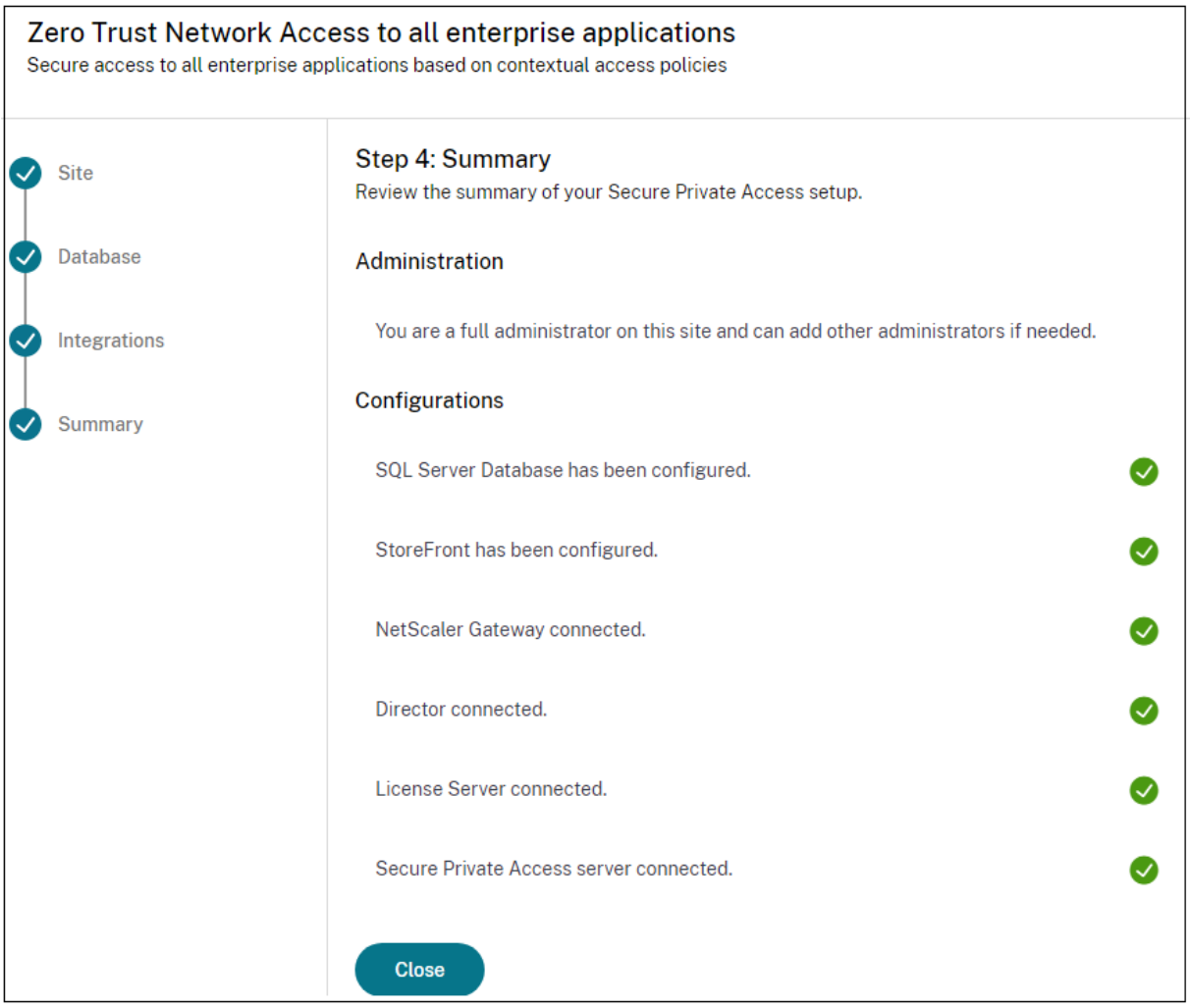


Paso 4: Resumen de la configuración

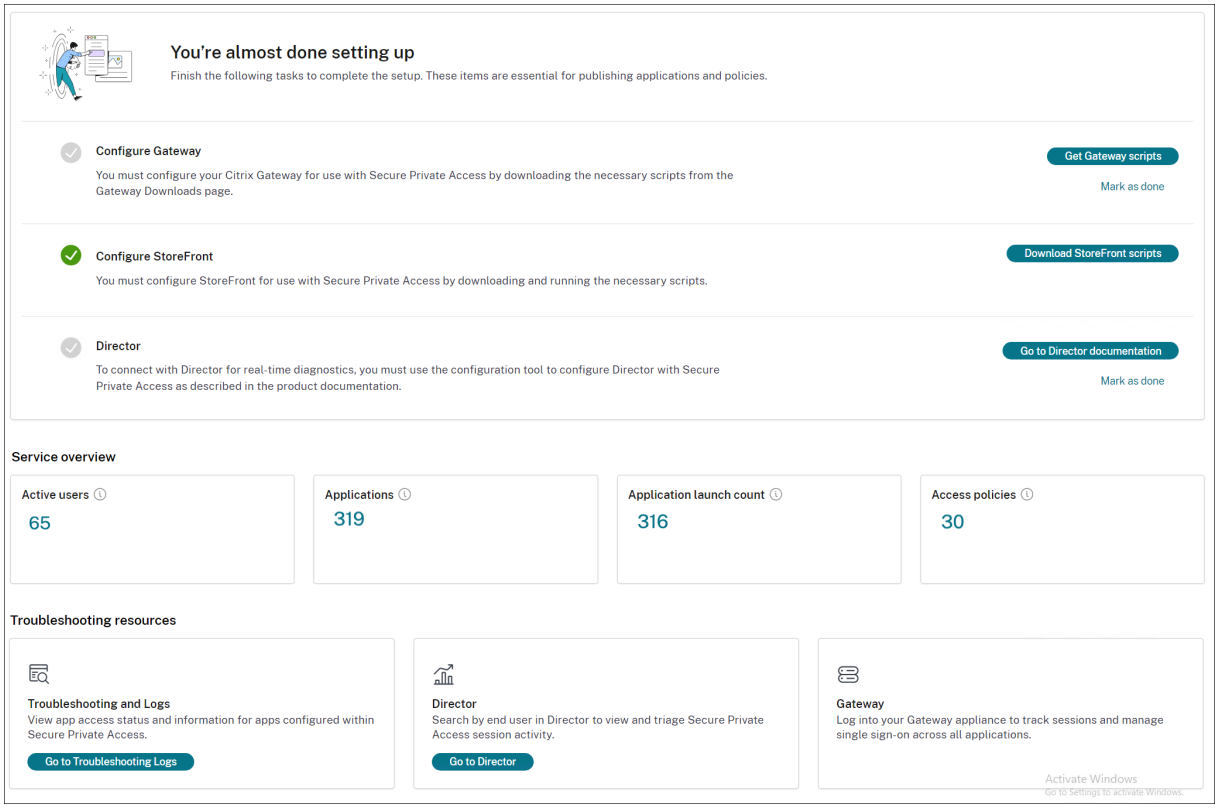
Una vez finalizada la configuración, se realiza la validación para garantizar que se pueda acceder a los servidores configurados. Además, se realiza una comprobación para garantizar que se pueda acceder

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**.



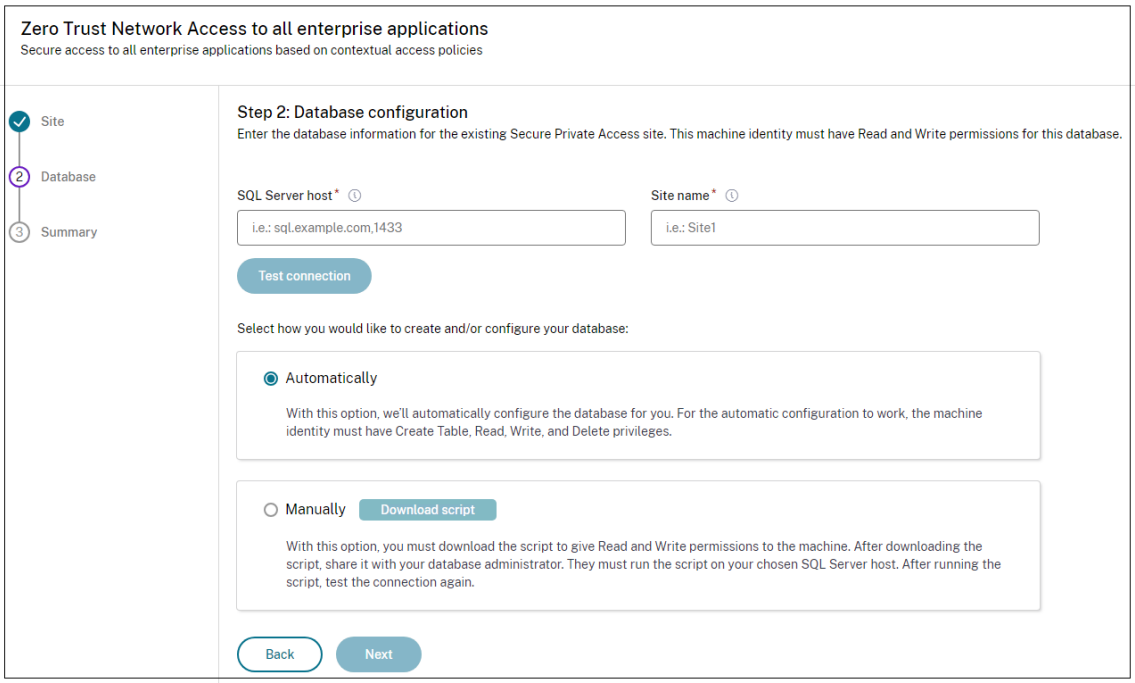
Nota:

- 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**.



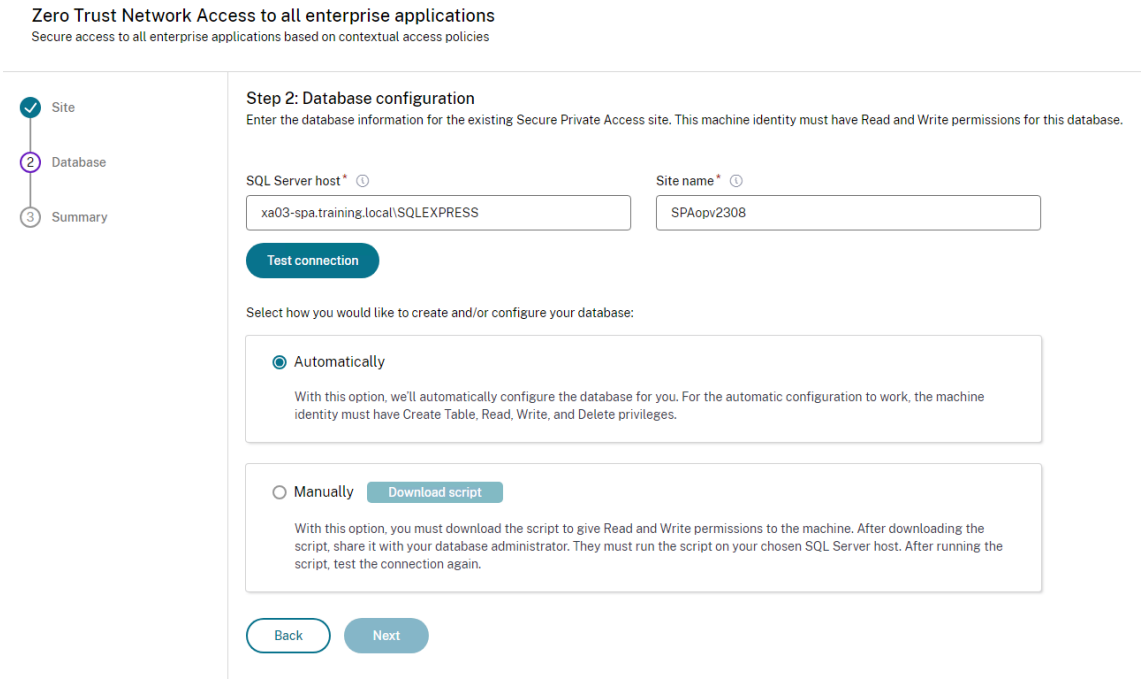
2. En **SQL Server Host**, introduzca el nombre del host del servidor. Asegúrese de que la base de datos correspondiente al nombre del sitio que introduzca ya esté presente en el servidor SQL que ha seleccionado. Puede especificar una dirección de base de datos de una de las siguientes formas:

   - 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

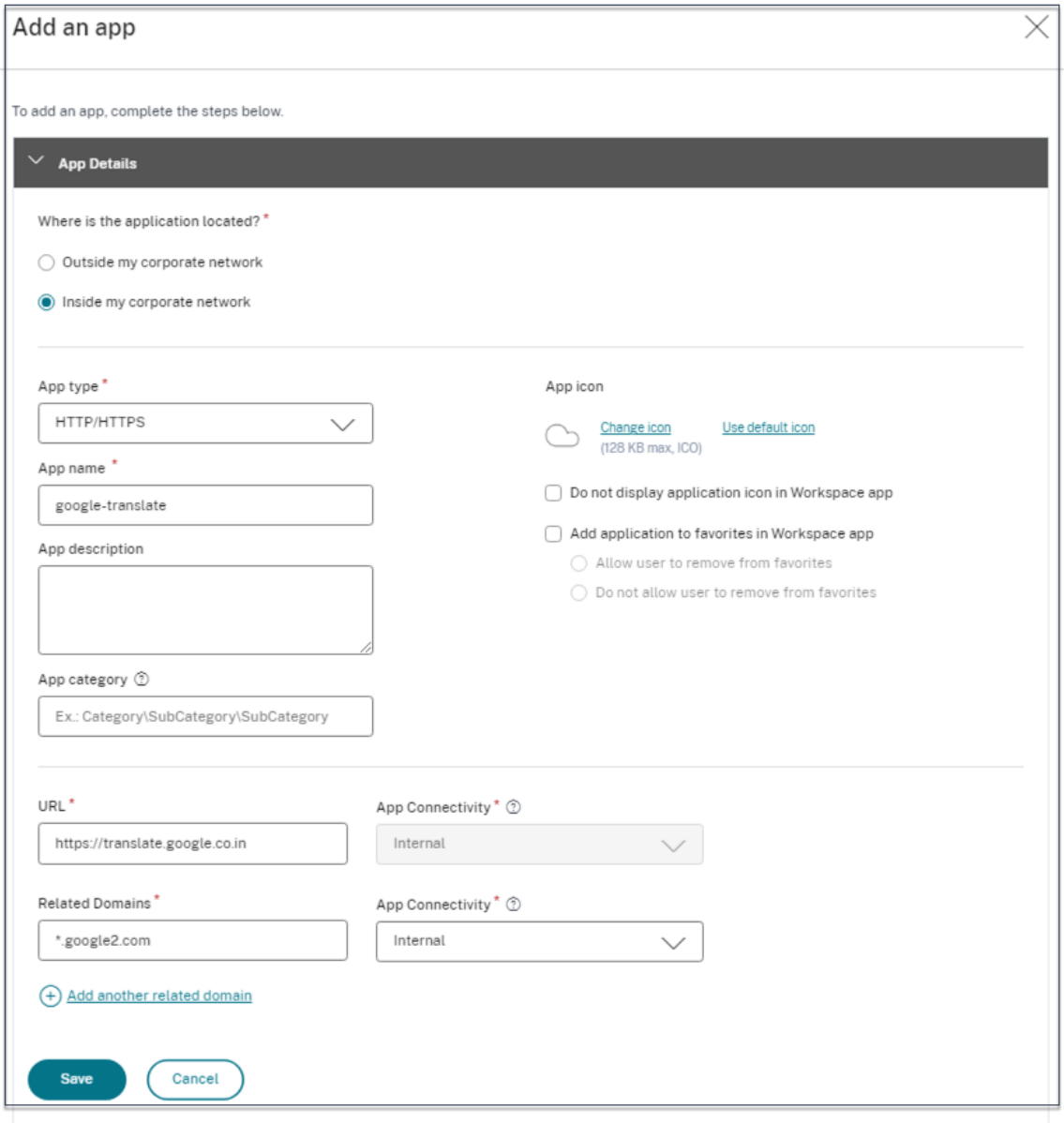
Configurar aplicaciones web/SaaS

October 21, 2024

Después de configurar el acceso privado seguro, puede configurar aplicaciones y políticas 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 donde reside la aplicación.
   - **Fuera de mi red corporativa** para aplicaciones externas.
   - **Dentro de mi red corporativa** para aplicaciones internas.
4. Ingrese 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 sus usuarios en el espacio de trabajo. También puede ingresar palabras clave para las aplicaciones en el formato `PALABRAS CLAVE: <keyword_name>`. Puede uti-

lizar las palabras clave para filtrar las aplicaciones. Para obtener más detalles, consulte Filtrar recursos por palabras clave incluidas.

- **Categoría de la aplicación** : agregue la categoría y el nombre de la subcategoría (si corresponde) bajo la cual debe aparecer la aplicación que está publicando en la interfaz de usuario de Citrix Workspace. Puede agregar una nueva categoría para cada aplicación o utilizar categorías existentes en la interfaz de usuario de Citrix Workspace. Una vez que especifica una categoría para una aplicación web o SaaS, la aplicación aparece en la interfaz de usuario del espacio de trabajo bajo la categoría específica.
  - Las categorías y subcategorías son configurables por el administrador y los administradores pueden agregar una nueva categoría para cada aplicación.
  - Los nombres de categorías y subcategorías deben estar separados por una barra invertida. Por ejemplo, Negocios y Productividad\Ingeniería. Además, este campo distingue entre mayúsculas y minúsculas. Los administradores deben asegurarse de definir la categoría correcta. Si hay una discrepancia entre el nombre en la interfaz de usuario de Citrix Workspace y el nombre de la categoría ingresado en el campo Categoría de la aplicación, la categoría aparece como una nueva categoría.

    Por ejemplo, si ingresa incorrectamente la categoría Negocios y productividad como Negocios y productividad en el campo Categoría de aplicación, entonces aparece una nueva categoría llamada Negocios y productividad en la interfaz de usuario de Citrix Workspace además de la categoría Negocios y productividad.
- **Ícono de la aplicación** –Haga clic en **Cambiar ícono** para cambiar el ícono de la aplicación. El tamaño del archivo del icono debe ser de 128x128 píxeles y solo se admite el formato Ico. Si no cambia el icono, se mostrará 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 completa automáticamente según 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. If this occurs, remove the related domain from all apps and create a new app with this domain and then set access accordingly in the access policy. You can also consider if you want to display this app in StoreFront or hide it. You can hide the app in StoreFront using the option

> **Do not display application to users** while publishing the app.
>
> – De manera similar, la URL de una aplicación publicada no debe agregarse como dominio relacionado de otra aplicación.
>
> – Para obtener más detalles, consulte Mejores prácticas para configuraciones de aplicaciones web y SaaS.

- **Agregar aplicación a favoritos automáticamente** –Haga clic en esta opción para agregar la aplicación como favorita en la aplicación Citrix Workspace. Cuando selecciona esta opción, aparece un ícono de estrella con un candado en la esquina superior izquierda de la aplicación Citrix Workspace.
  - **Permitir que el usuario elimine de favoritos** –Haga clic en esta opción para permitir que los suscriptores de la aplicación eliminen la aplicación de la lista de aplicaciones favoritas en la aplicación Citrix Workspace. Cuando selecciona esta opción, aparece un ícono de estrella amarilla en la esquina superior izquierda de la aplicación en la aplicación Citrix Workspace.
  - **No permitir que el usuario elimine de favoritos** –Haga clic en esta opción para evitar que los suscriptores eliminen la aplicación de la lista de aplicaciones favoritas en la aplicación Citrix Workspace.

  Si elimina las aplicaciones marcadas como favoritas de la consola de Secure Private Access, dichas aplicaciones deberán eliminarse manualmente de la lista de favoritos en Citrix Workspace. Las aplicaciones no se eliminan automáticamente de StoreFront si se eliminan de la consola de acceso privado seguro.
- **Conectividad de aplicaciones** - Seleccione **Interna** para aplicaciones web y **Externa** para aplicaciones SaaS.

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

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

Siguientes pasos

Configurar políticas de acceso para las aplicaciones

Configurar aplicaciones TCP/UDP

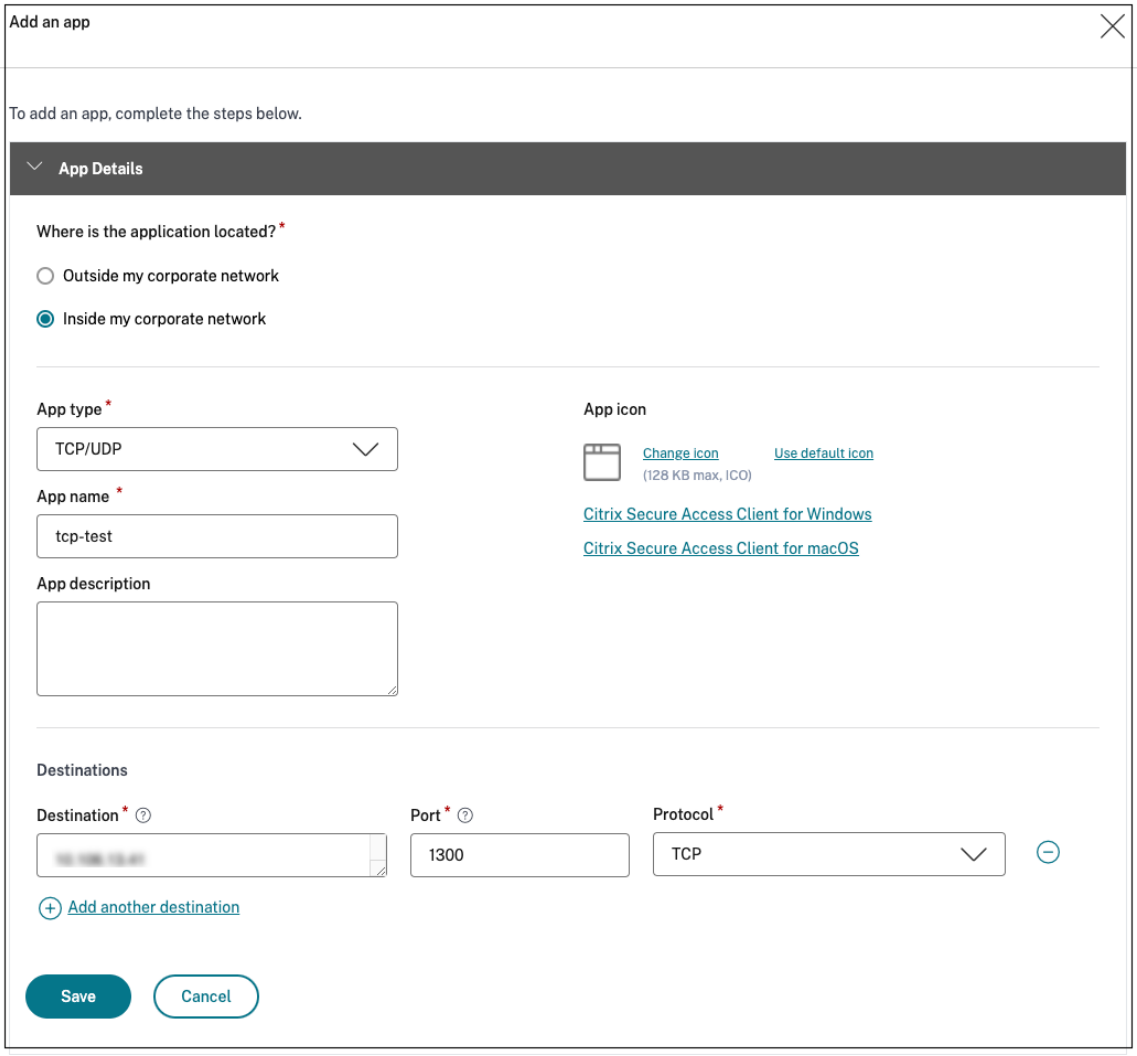
October 21, 2024

Requisitos previos:

- La configuración del acceso privado seguro está completa.
- Las versiones de cliente cumplen los siguientes requisitos:
  - Windows - 24.6.1.17 y posteriores
  - macOS - 24.06.2 y posteriores

Realice los siguientes pasos para configurar aplicaciones TCP/UDP desde la consola de administración:

1. En la consola de administración, haga clic en **Aplicaciones** y luego haga clic en **Agregar una aplicación**.
2. Seleccione la ubicación **Dentro de mi red corporativa**.



3. Introduzca los siguientes detalles:

   - **Tipo de aplicación** –Seleccione **TCP/UDP** para iniciar conexiones con los servidores back-end que residen en el centro de datos.

> **Nota**
>
> La opción TCP/UDP aparece en gris si el indicador de función SPAOP-3315-EnableZTNAApplications está deshabilitado. Debe actualizar manualmente la base de datos para habilitar esta función.

```
- **Nombre de la aplicación** – Nombre de la aplicación.
- **Descripción de la aplicación** – Descripción de la aplicación que estás agregando. Este campo es opcional.
- **Destinos** – Direcciones IP o FQDN de las máquinas back-end que residen en el centro de datos. Se pueden especificar uno o más destinos de la siguiente manera.
  - **Dirección IP v4**
  - **Rango de direcciones IP** – Ejemplo: 10.68.90.10-10.68.90.99
```



```
6       - **CIDR** – Ejemplo: 10.106.90.0/24
7       - **FQDN de las máquinas o nombre de dominio** – Dominio único o
           comodín. Ejemplo: ex.destino.dominio.com, *.dominio.com > **Nota
           ** > > - Los usuarios finales pueden acceder a las aplicaciones
            mediante FQDN incluso si el administrador ha configurado las
           aplicaciones utilizando la dirección IP. Esto es posible porque
           el cliente Citrix Secure Access puede resolver un FQDN en la
           dirección IP real.
8
9       La siguiente tabla proporciona ejemplos de varios destinos y cómo
           acceder a las aplicaciones con estos destinos:
10
11      | Entrada de destino      | Cómo acceder a la aplicación
              |
12      | ----------------------- |
           ------------------------------------------------------------------------
            |
13      | 10.10.10.1-10.10.10.100 | Se espera que el usuario final acceda a
            la aplicación solo a través de direcciones IP en este rango.
              |
14      | 10.10.10.0/24           | Se espera que el usuario final acceda a
            la aplicación solo a través de direcciones IP configuradas en
           el CIDR IP.
              |
15      | 10.10.10.101            | Se espera que el usuario final acceda a
            la aplicación solo a través de 10.10.10.101
              |
16      | `*.info.citrix.com`     | Se espera que el usuario final acceda a
            los subdominios de `info.citrix.com` y también a `info.citrix.
           com` \(el dominio principal). Por ejemplo, `info.citrix.com,
           sub1.info.citrix.com, level1.sub1.info.citrix.com` \*\*Nota:\*\*
            El comodín siempre debe ser el carácter inicial del dominio y
           solo un \*. está permitido |
17      | información.citrix.com  | Se espera que el usuario final acceda ú
           nicamente a `info.citrix.com` y no a ningún subdominio. Por
           ejemplo, `sub1.info.citrix.com` no es accesible.
              |
18
19      La dirección IP de destino debe ser única en todas las ubicaciones
           de recursos. Si existe una configuración conflictiva, se muestra
            un símbolo de advertencia junto a la dirección IP específica en
            la tabla Dominio de aplicación (**Configuración > Dominio de
           aplicación**).
20
21      ![Conflicto](/en-us/citrix-secure-private-access/media/spaop-
           warning-conflict-config.png)
22
23  -       **Port** – The destination port on which the app is running.
```



```
          Admins can configure multiple ports or port ranges per
      destination.
24
25            The following table provides examples of ports that can be
                 configured for a destination.
26
27            |Port input|Description|
28            |---|---|
29            |\*|By default, the port field is set to ` “ *” ` \(any port).
                    The port numbers from 1 to 65535 are supported for the
                 destination.|
30            |1300 – 2400|The port numbers from 1300 to 2400 are supported
                 for the destination.|
31            |38389|Only the port number 38389 is supported for the
                 destination.|
32            |22,345,5678|The ports 22, 345, 5678 are supported for the
                 destination.|
33            |1300 – 2400, 42000-43000,22,443|The port number range from
                 1300 to 2400, 42000 – 43000, and ports 22 and 443 are
                 supported for the destination.|
34
35          >**Nota:**
36          >
37          >El puerto comodín (*) no puede coexistir con números de puerto
                o rangos.
38
39  -         **Protocol** – TCP/UDP
```

1. Haga clic en **Agregar** para agregar destinos o servidores adicionales según corresponda.
2. Haga clic en **Guardar**. La aplicación se agrega a la página **Configuración de la aplicación** . Puede editar o eliminar una aplicación desde la página **Aplicaciones** después de haber configurado la aplicación. Para ello, haga clic en el botón de puntos suspensivos en línea con la aplicación y seleccione las acciones correspondientes.
   - **Editar aplicación**
   - **Eliminar**

Configurar políticas de acceso para aplicaciones TCP/UDP

Para permitir el acceso a las aplicaciones para los usuarios, los administradores deben crear políticas de acceso. Para obtener más detalles, consulte Configurar políticas de acceso.

Referencias

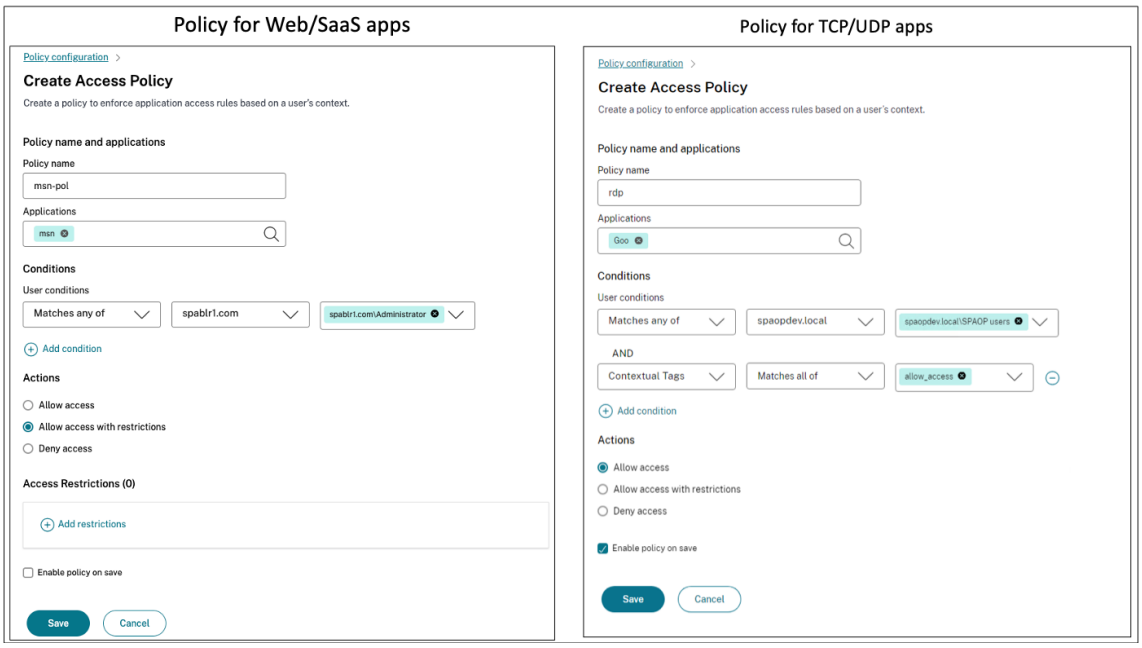
Cliente de acceso seguro de Citrix.

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 y TCP/UDP) agregando las restricciones de seguridad.

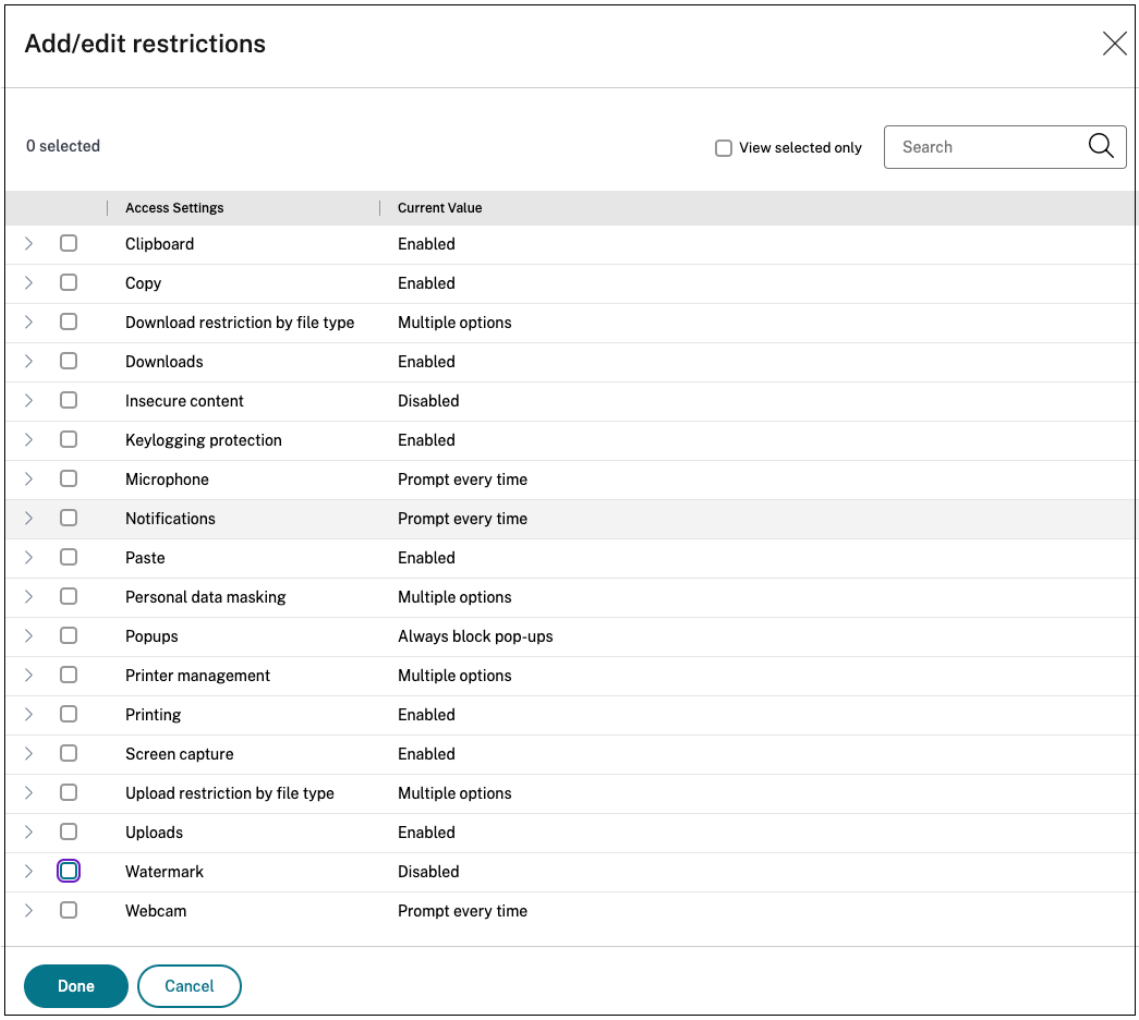
1. En la consola de administración, haga clic en **Directivas de acceso**.
2. Haga clic en **Crear directiva**.



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**

> **Nota:**
>
> - La acción **Permitir el acceso con restricciones** no es aplicable a las aplicaciones TCP/UDP.
> - 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.



8. Seleccione las restricciones y, a continuación, haga clic en **Listo**.
9. 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

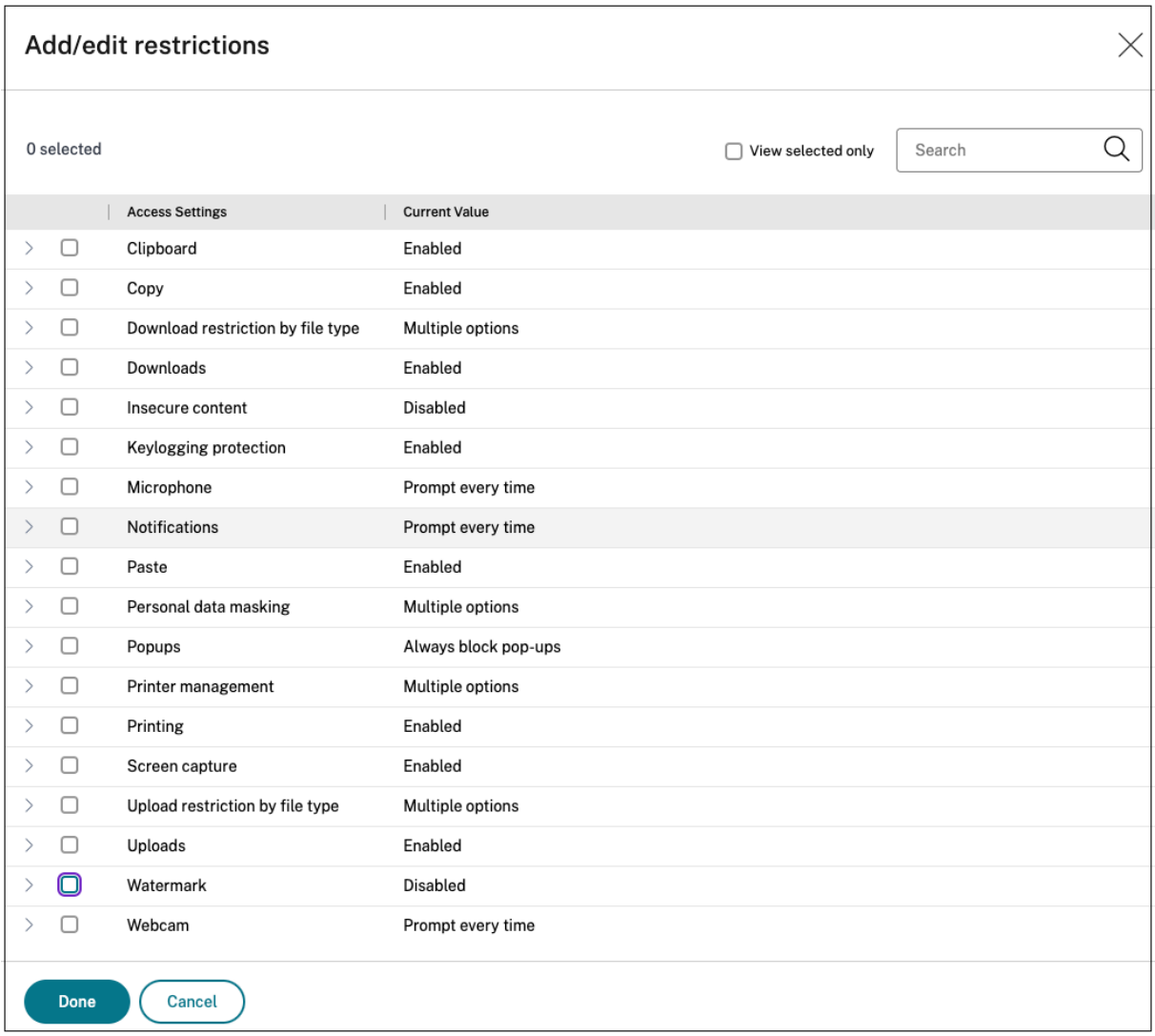
- Valide su configuración desde las máquinas cliente (Windows y macOS).
- Para las aplicaciones TCP/UDP, valide la configuración desde las máquinas cliente (Windows y macOS) iniciando sesión en el cliente Citrix Secure Access.

Ejemplo de validación de configuración

Opciones de restricción de acceso

October 21, 2024

Cuando selecciona la acción **Permitir 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 deshabilite las operaciones de cortar, copiar y pegar en una aplicación web interna o SaaS con esta política de acceso cuando acceda a través de Citrix Enterprise Browser. Valor predeterminado: habilitado.

Copiar

Habilite o deshabilite la copia de datos desde una aplicación web interna o SaaS con esta política de acceso cuando se accede a través del navegador Citrix Enterprise. Valor predeterminado: habilitado.

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

Descargas

Habilite o deshabilite la capacidad del usuario para descargar desde dentro del SaaS o la aplicación web interna con esta política cuando se accede a través de Citrix Enterprise Browser. Valor predeterminado: habilitado.

> **Nota**
>
> - Si ha deshabilitado la restricción **Descargar** para el usuario final, los usuarios finales pueden solicitar acceso de descarga desde la aplicación cuando acceden a través de Citrix Enterprise Browser. Para obtener más detalles, consulte Acceso de descarga por solicitud.
> - Si las restricciones **Descargas** y **Restricción de descargas por tipo de archivo** están habilitadas en una política, la restricción **Descargas** tiene prioridad sobre la restricción **Restricción de descargas por tipo de archivo**.

Restricción de descarga por tipo de archivo

Habilite o deshabilite la capacidad del usuario para descargar un tipo de MIME (archivo) específico desde dentro de la aplicación web interna o SaaS con esta política cuando se accede a través de Citrix Enterprise Browser.

> **Nota**
>
> - La restricción de descarga **por tipo de archivo** está disponible además de la restricción de descarga ** .
> - Si las restricciones **Descargas** y **Restricción de descargas por tipo de archivo** están habilitadas en una política, la restricción **Descargas** tiene prioridad sobre la restricción **Restricción de descargas por tipo de archivo** .
> - Los usuarios finales deben utilizar Citrix Enterprise Browser versión 126 o posterior para acceder a las aplicaciones para las que está habilitada esta restricción. De lo contrario, el

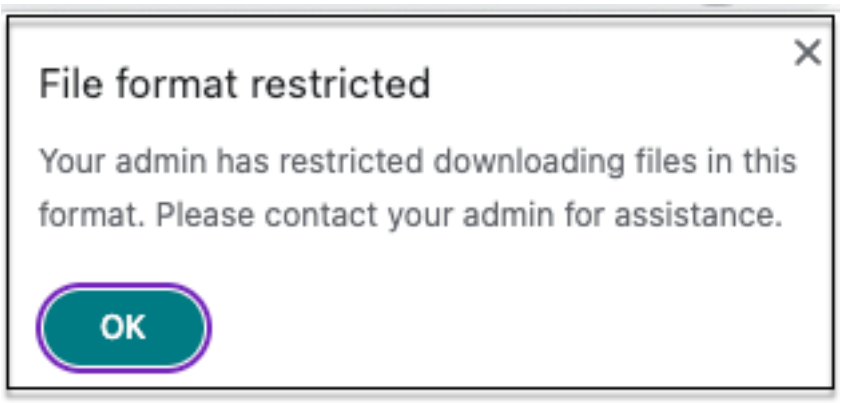
> acceso a la aplicación estará restringido.

Para habilitar la descarga de tipos MIME, realice los siguientes pasos:

1. Crear o editar una política de acceso. Para obtener detalles sobre cómo crear una política de acceso, consulte Configurar políticas de acceso.
2. En **Acciones**, seleccione **Permitir con restricciones**.
3. Haga clic en **Restricción de descarga por tipo de archivo** y luego haga clic en **Editar**.
4. En la página **Configuración de restricción de descarga por tipo de archivo** , seleccione una de las siguientes opciones:
   - **Permitir todas las descargas con excepciones** –Seleccionar los tipos que deben bloquearse y permitir todos los demás tipos.
   - **Bloquear todas las descargas con excepciones** –Seleccionar solo los tipos que se pueden cargar y bloquear 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**, ingrese el tipo MIME en el formato `categoría/subcategoría<extension>`. Por ejemplo, `imagen/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:



Contenido inseguro

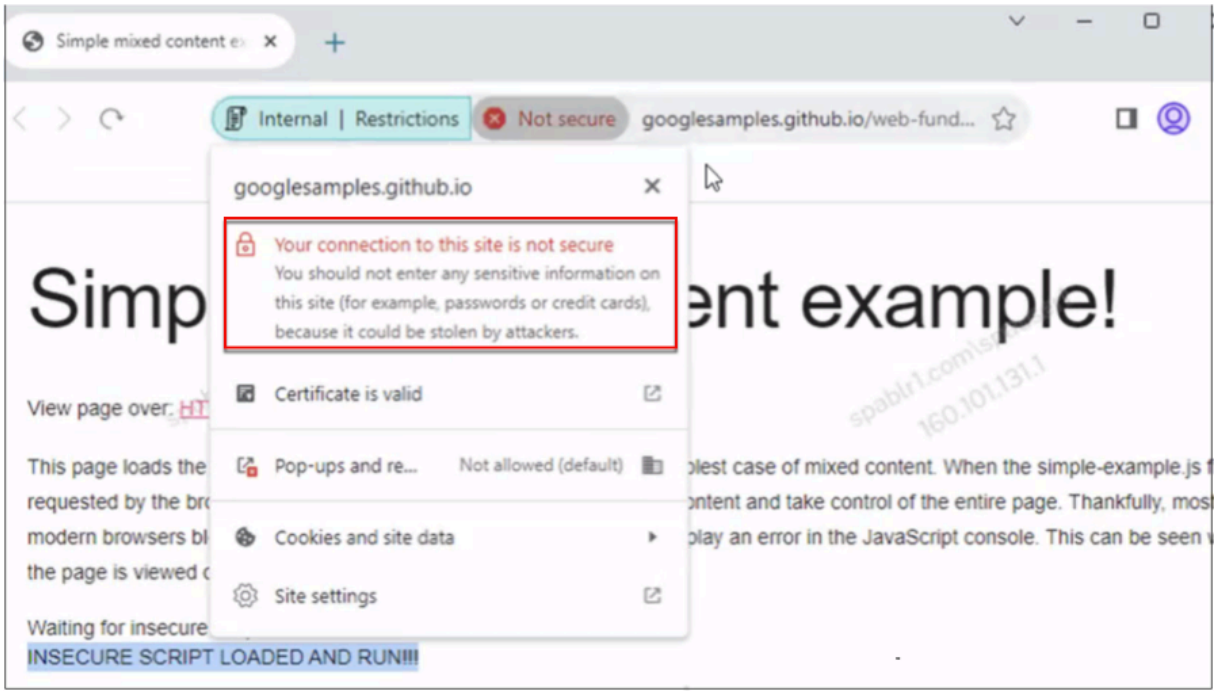
Habilite o deshabilite a los usuarios finales para que no accedan a contenido inseguro dentro del SaaS o la aplicación web interna configurada con esta política cuando accedan a través de Citrix Enterprise

Browser. El contenido inseguro es cualquier archivo vinculado desde una página web mediante un enlace HTTP en lugar de un enlace HTTPS. Valor predeterminado: Inhabilitada.

Para habilitar la visualización de contenido inseguro, realice los siguientes pasos:

1. Crear o editar una política de acceso. Para obtener detalles sobre cómo crear una política de acceso, consulte Configurar políticas de acceso.
2. En **Acciones**, seleccione **Permitir con restricciones**.
3. Haga clic en **Contenido inseguro**.
4. Haga clic en **Guardar**y, a continuación, haga clic en **Listo**.

La siguiente figura muestra una notificación de muestra cuando accede a un contenido inseguro.



Protección contra registro de teclas

Habilite o deshabilite los keyloggers para que no capturen pulsaciones de teclas desde la aplicación web interna o SaaS con esta política de acceso cuando se acceda a través de Citrix Enterprise Browser. Valor predeterminado: habilitado.

Micrófono

Solicitar/no solicitar a los usuarios cada vez que accedan al micrófono dentro de la aplicación web interna o SaaS configurada con esta política cuando accedan a través de Citrix Enterprise Browser. Valor predeterminado: Preguntar cada vez.

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

Para habilitar el micrófono cada vez sin que se le solicite, realice los siguientes pasos:

1. Crear o editar una política de acceso. Para obtener más detalles, consulte Configurar políticas de acceso.
2. En **Acciones**, seleccione **Permitir con restricciones**.
3. Haga clic en **Micrófono** y luego haga clic en **Editar**.
4. En la página **Configuración del micrófono** , haga clic en **Permitir siempre el acceso**.
5. Haga clic en **Guardar**y, a continuación, haga clic en **Listo**.

> **Nota**
>
> - Si la restricción **Micrófono** está habilitada en la política de Acceso privado seguro, entonces Citrix Enterprise Browser muestra la configuración **Permitir**.
> - Si la opción **Preguntar cada vez** en la política de acceso privado seguro, entonces la configuración aplicada en Citrix Enterprise Browser varía dependiendo de si se utiliza el servicio de configuración global de aplicaciones (GACS) para administrar Citrix Enterprise Browser.
> - Si se utiliza GACS, la configuración de GACS se aplica en Citrix Enterprise Browser.
> - Si no se utiliza GACS, Citrix Enterprise Browser muestra la configuración **Preguntar**.
> - Actualmente, Secure Private Access no admite el bloqueo del micrófono. Si debe bloquear un micrófono, debe hacerlo a través de GACS.

Para obtener más información sobre GACS, consulte Administrar Citrix Enterprise Browser a través del servicio de configuración global de aplicaciones.

Notificaciones

Permitir/preguntar a los usuarios cada vez que quieran ver las notificaciones dentro de la aplicación web interna o SaaS configurada con esta política cuando accedan a través de Citrix Enterprise Browser. Valor predeterminado: Preguntar cada vez.

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

Para bloquear la visualización de notificaciones sin previo aviso, realice los siguientes pasos.

1. Crear o editar una política de acceso. Para obtener más detalles, consulte Configurar políticas de acceso.
2. En **Acciones**, seleccione **Permitir con restricciones**.
3. Haga clic en **Notificaciones** y luego haga clic en **Editar**.
4. En la página **Configuración de notificaciones** , haga clic en **Bloquear siempre las notificaciones**.

5. Haga clic en **Guardar**y, a continuación, haga clic en **Listo**.

Pegar

Habilite o deshabilite el pegado de datos copiados en la aplicación web interna o SaaS con esta política de acceso cuando se accede a través de Citrix Enterprise Browser. Valor predeterminado: habilitado.

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

Enmascaramiento de datos personales

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

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

Para redactar o enmascarar información de identificación personal, realice los siguientes pasos:

1. Crear o editar una política de acceso. Para obtener más detalles, consulte Configurar políticas de acceso.
2. En **Acciones**, seleccione **Permitir con restricciones**.
3. Haga clic en **Enmascaramiento de datos personales** y luego haga clic en **Editar**.
4. Seleccione el tipo de información que desea ocultar o enmascarar y luego 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 detalles, consulte Agregar tipo de información personalizada.

5. Seleccione el tipo de enmascaramiento.

    - **Enmascaramiento completo** –Cubre completamente la información confidencial para hacerla ilegible.
    - **Enmascaramiento parcial** –Cubre parcialmente la información confidencial. Se cubren únicamente las secciones relevantes dejando el resto intacto.

      Cuando selecciona **Marcado parcial**, debe seleccionar caracteres comenzando desde el principio o el final del documento. Debes ingresar los números en los campos **Primeros caracteres enmascarados** y **Últimos caracteres enmascarados** .

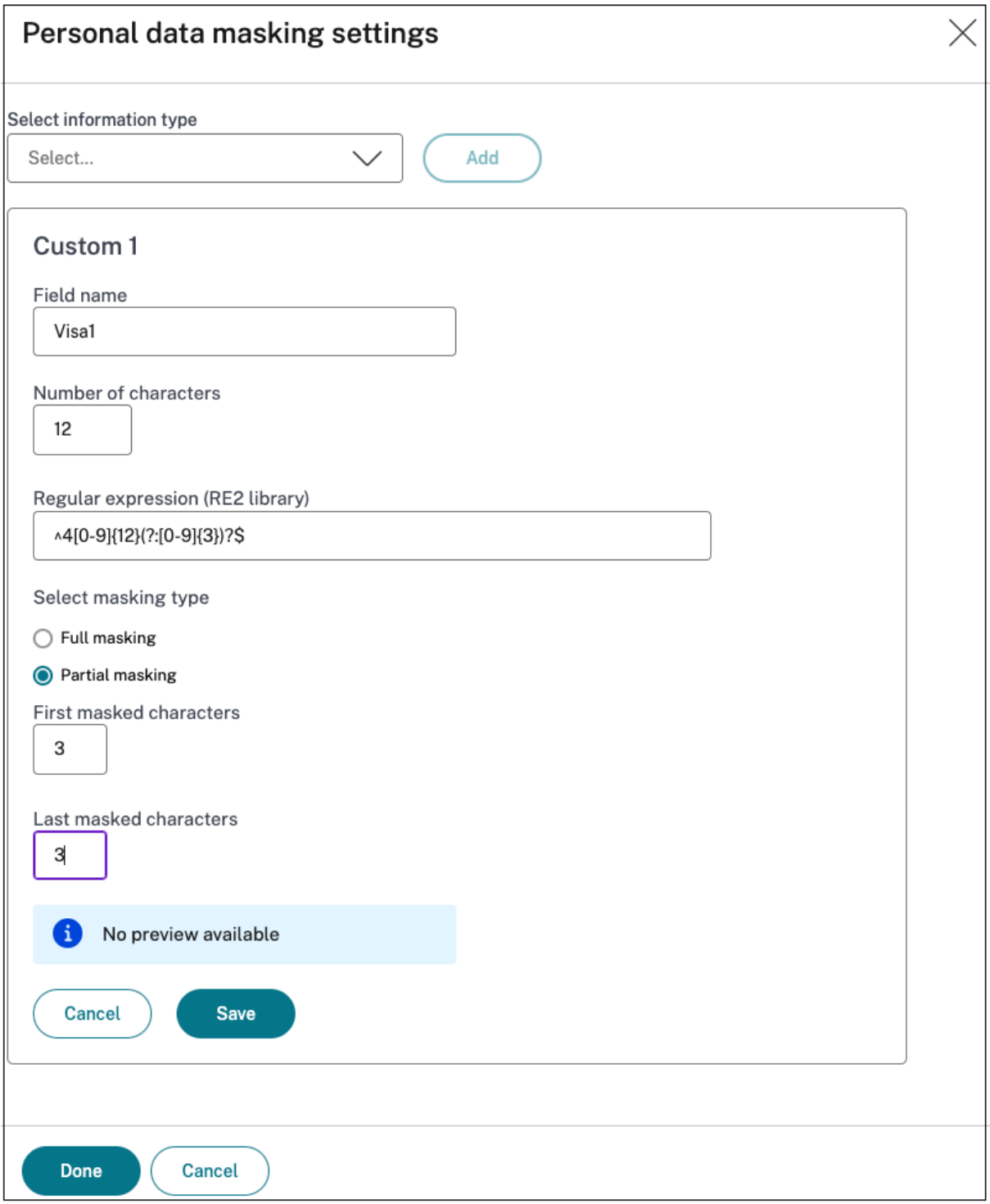
      El campo **Vista previa** muestra el formato de enmascaramiento. Esta vista previa no está disponible para políticas personalizadas.

6. Haga clic en **Guardar** y luego haga clic en **Listo**.

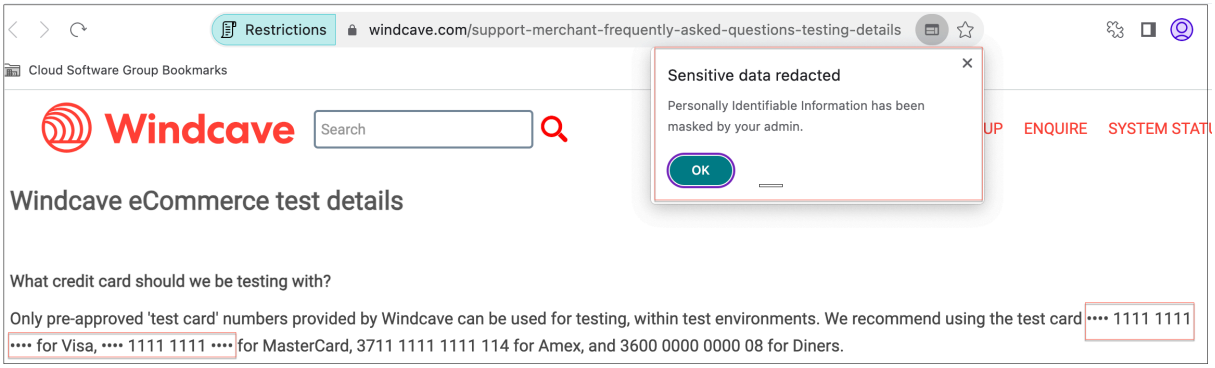
Agregar tipo de información personalizada

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

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



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



Ventanas emergentes

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

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

Para habilitar la visualización de ventanas emergentes, realice los siguientes pasos:

1. Crear o editar una política de acceso. Para obtener más detalles, consulte Configurar políticas de acceso.
2. En **Acciones**, seleccione **Permitir con restricciones**.
3. Haga clic en **Ventanas emergentes** y luego haga clic en **Editar**.
4. En la página **Configuración de ventanas emergentes** , haga clic en **Permitir siempre ventanas emergentes**.
5. Haga clic en **Guardar**y, a continuación, haga clic en **Listo**.

Impresión

Habilite o deshabilite los datos de impresión desde las aplicaciones web internas o SaaS configuradas con esta política cuando se acceda a ellas a través del navegador Citrix Enterprise. 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 ha deshabilitado la opción de impresión para el usuario final, los usuarios finales pueden solicitar acceso a la impresión desde la aplicación cuando accedan a través de Citrix Enterprise Browser. Para obtener más detalles, consulte Acceso de impresión por solicitud.
- Si las restricciones **Impresión** y **Administración de impresoras** están habilitadas en una política, la restricción **Impresión** tiene prioridad sobre la restricción **Administración de impresoras** .

Administración de la impresora

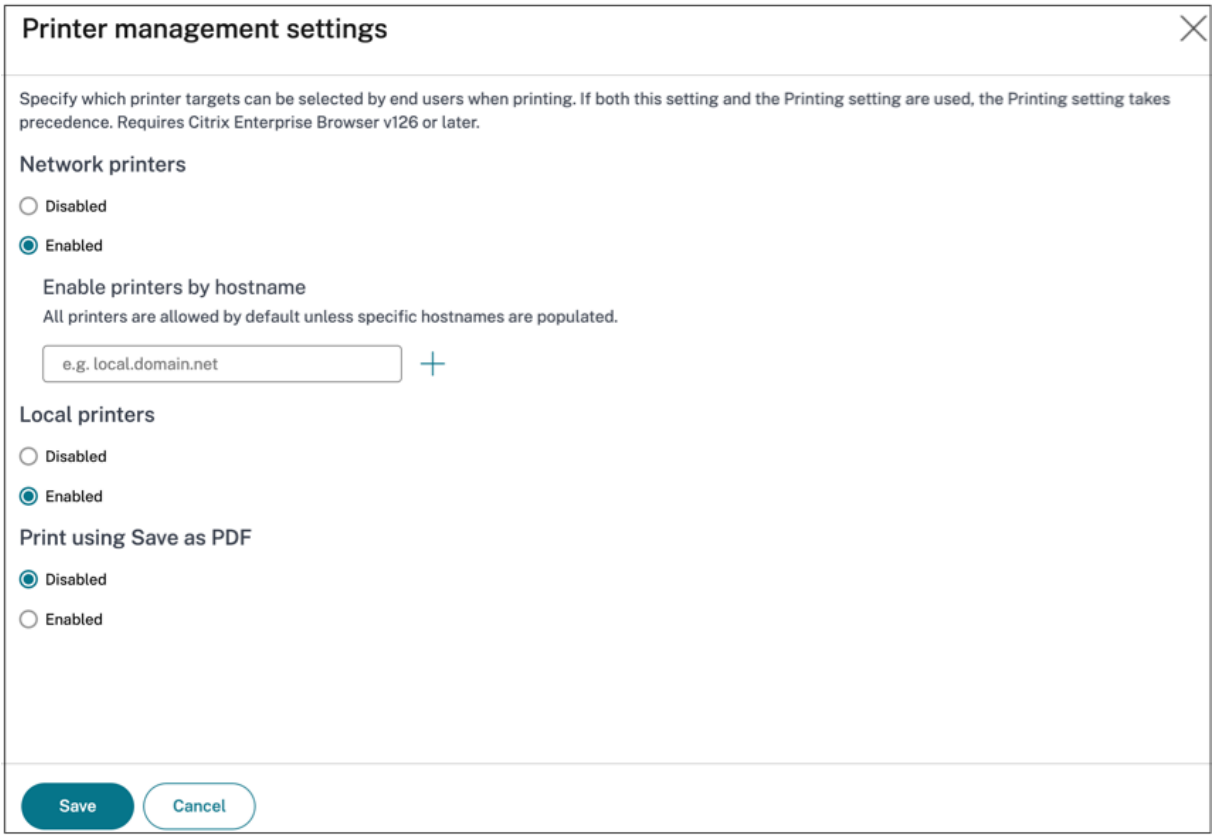
Habilite o deshabilite la impresión de datos mediante el uso de impresoras configuradas por el administrador desde las aplicaciones web internas o SaaS configuradas con esta política cuando se acceda a ellas a través de Citrix Enterprise Browser.

Nota

- La restricción **Administración de impresora** está disponible además de la restricción **Impresión** donde la impresión está habilitada o deshabilitada. Si las restricciones **Impresión** y **Administración de impresoras** están habilitadas en una política de acceso, la restricción **Impresión** tiene prioridad sobre la restricción **Administración de impresoras** .
- Los usuarios finales deben utilizar Citrix Enterprise Browser versión 126 o posterior para acceder a las aplicaciones para las que está habilitada esta restricción. De lo contrario, el acceso a la aplicación estará restringido.

Para habilitar o deshabilitar las restricciones de impresión, realice los siguientes pasos:

1. Crear o editar una política de acceso. Para obtener detalles sobre cómo crear una política de acceso, consulte Configurar políticas de acceso.
2. En **Acciones**, seleccione **Permitir con restricciones**.
3. Haga clic en **Administración de impresoras** y luego haga clic en **Editar**.



1. Seleccione las excepciones según sus necesidades.

   - **Impresoras de red** - Una impresora de red es una impresora que puede conectarse a una red y ser utilizada por varios usuarios.

     - **Deshabilitado:** La impresión desde cualquier impresora en la red está deshabilitada.
     - **Habilitado:** La impresión desde todas las impresoras de la red está habilitada. Si se especifican nombres de host de impresora, se bloquearán todas las demás impresoras de 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 una computadora 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.

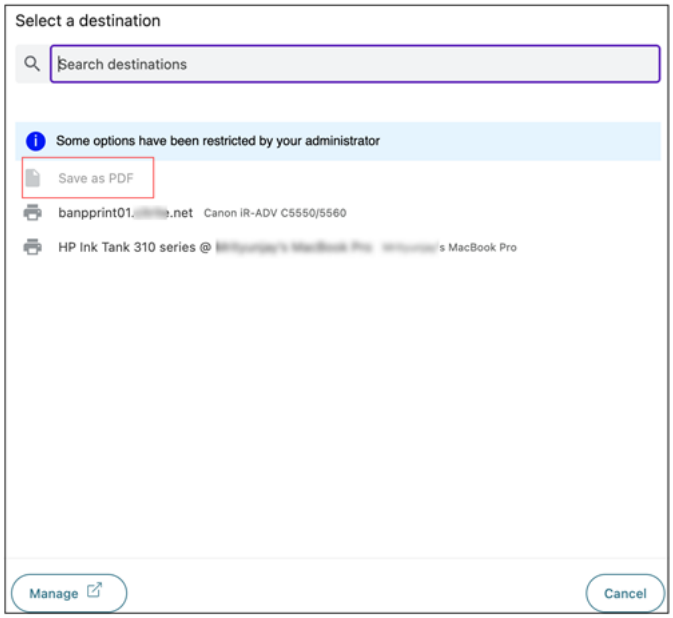
   - **Imprimir con Guardar como PDF**

     - **Deshabilitado**: Guardar el contenido de la aplicación en formato PDF está deshabilitado.
     - **Habilitado:** Está habilitado guardar el contenido de la aplicación en formato PDF.

2. Haga clic en **Guardar**.

Si una impresora de red está deshabilitada, el nombre específico de la impresora aparece en gris cuando intenta seleccionar la impresora en el campo **Destino** .

Además, si **Imprimir usando Guardar como PDF** está deshabilitado, entonces cuando hace clic en el enlace **Ver más** en el campo **Destino** , la opción **Guardar como PDF** aparece en gris.



Captura de pantalla

Habilite o deshabilite la capacidad de capturar pantallas desde la aplicación web interna o SaaS con esta política cuando se acceda a través de Citrix Enterprise Browser usando 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 deshabilite la capacidad del usuario para descargar un tipo de MIME (archivo) específico desde la aplicación web interna o SaaS con esta política cuando se accede a través de Citrix Enterprise Browser.

> **Nota**
>
> - La restricción de carga **por tipo de archivo** está disponible además de la restricción de carga ** .
> - Si las restricciones **Cargar** y **Cargar por tipo de archivo** están habilitadas en una política,

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

Para habilitar o deshabilitar la carga de tipos MIME, realice los siguientes pasos:

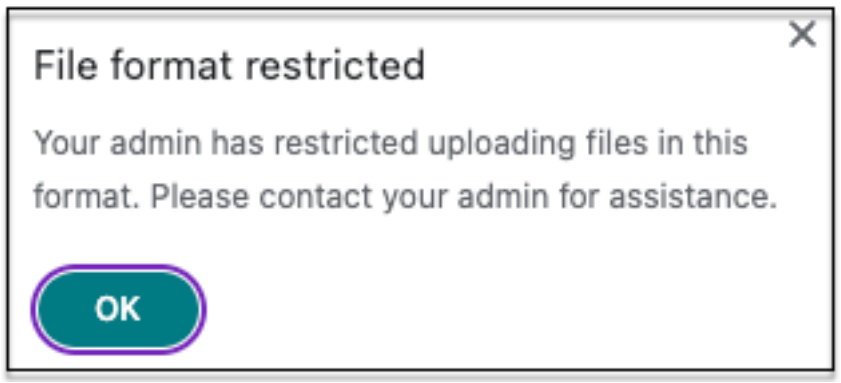
1. Crear o editar una política de acceso. Para obtener más detalles, consulte Crear políticas de acceso.
2. En **Acciones**, seleccione **Permitir con restricciones**.
3. Haga clic en **Restricción de carga por tipo de archivo** y luego haga clic en **Editar**.
4. En la página **Configuración de restricción de carga por tipo de archivo** , seleccione una de las siguientes opciones:

   Permitir todas las cargas con excepciones –Cargar todos los archivos excepto los tipos seleccionados. **Bloquea todas las cargas con excepciones** –Bloquea la carga de todos los tipos de archivos, excepto los tipos 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**, ingrese el tipo MIME en el formato `categoría/subcategoría<extension>`. Por ejemplo, `imagen/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.



Subidas

Habilite o deshabilite la capacidad del usuario para cargar dentro de la aplicación web interna o SaaS configurada con esta política cuando se accede a través de Citrix Enterprise Browser. Valor predeterminado: habilitado.

> **Nota**
>
> Si las restricciones **Cargas** y **Restricción de carga por tipo de archivo** están habilitadas en una política, la restricción **Cargas** tiene prioridad sobre la restricción **Restricción de carga por tipo de archivo** .

Marca de agua

Habilitar/deshabilitar la marca de agua en la pantalla del usuario mostrando el nombre de usuario y la dirección IP de la máquina del usuario. Valor predeterminado: Inhabilitada.

Cámara web

Solicitar/no solicitar a los usuarios cada vez que accedan a la cámara web dentro de la aplicación web interna o SaaS configurada con esta política cuando se accede a través de Citrix Enterprise Browser. Valor predeterminado: Preguntar cada vez.

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

Para permitir la cámara web en todo momento sin que se le solicite, realice los siguientes pasos:

1. Crear o editar una política de acceso. Para obtener más detalles, consulte Configurar políticas de acceso.
2. En **Acciones**, seleccione **Permitir con restricciones**.
3. Haga clic en **Cámara web** y luego haga clic en **Editar**.
4. En la página **Configuración de la cámara web** , haga clic en **Permitir siempre el acceso**.
5. Haga clic en **Guardar**y, a continuación, haga clic en **Listo**.

> **Nota**
>
> - Si la restricción de cámara web está habilitada en la política de acceso privado seguro, Citrix Enterprise Browser muestra la configuración **Permitir**.
> - Si la opción **Preguntar cada vez** en la política de acceso privado seguro, la configuración aplicada en Citrix Enterprise Browser varía dependiendo de si se utiliza el servicio de configuración global de aplicaciones (GACS) para administrar Citrix Enterprise Browser.
> - Si se utiliza GACS, la configuración de GACS se aplica en Citrix Enterprise Browser.

- Si no se utiliza GACS, Citrix Enterprise Browser muestra la configuración **Preguntar**.
- Actualmente, Secure Private Access no admite el bloqueo de la cámara web. Si debe bloquear la cámara web, debe hacerlo a través de GACS.

Para obtener más información sobre GACS, consulte Administrar Citrix Enterprise Browser a través del servicio de configuración global de aplicaciones.

Restricción del portapapeles para grupos de seguridad

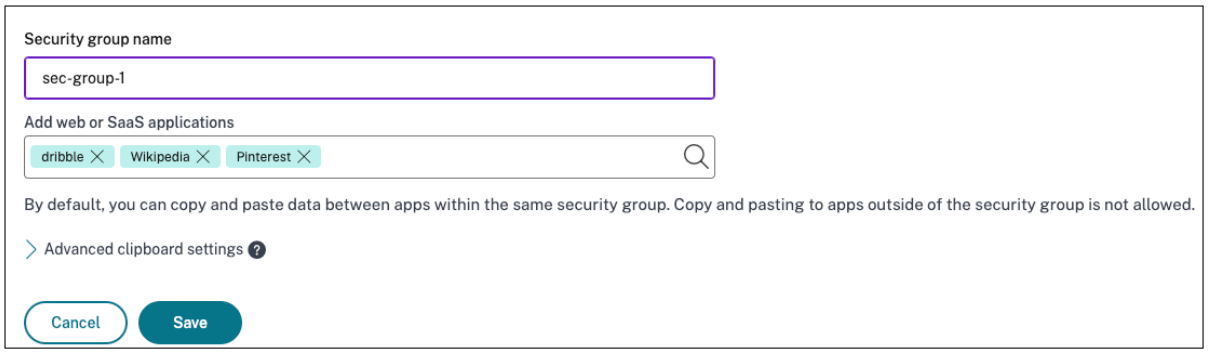
Puede habilitar el acceso al portapapeles para un grupo designado de aplicaciones mediante la restricción **Grupos de seguridad (Aplicaciones > Grupos de seguridad)**. A los grupos de seguridad se les asigna un conjunto de aplicaciones dentro de las cuales se pueden realizar operaciones de copiar y pegar.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

- Cuando la restricción **Grupos de seguridad** está habilitada, no puedes copiar/pegar datos entre aplicaciones en 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/pegar contenido de "Edocs"a "ProdDocs"incluso si la restricción **Copiar** / **Pegar** está habilitada para ambos grupos.
- Para las aplicaciones que no forman parte de un grupo de seguridad, puedes crear una política de acceso con la acción **permitir con restricciones** y seleccionar las restricciones (**Copiar**, **Pegar**o **Portapapeles**). En este caso, la aplicación no es parte de un grupo de seguridad y, por lo tanto, la restricción **Copiar** / **Pegar** se puede aplicar en esa aplicación.

> **Nota**
>
> También puede restringir el acceso al portapapeles para las aplicaciones a las que se accede a través de Citrix Enterprise Browser mediante el servicio de configuración global de aplicaciones (GACS). Si está utilizando GACS para administrar Citrix Enterprise Browser, utilice la opción **Habilitar portapapeles en espacio aislado** para administrar el acceso al portapapeles. Cuando restringe el acceso al portapapeles a través de GACS, se aplica a todas las aplicaciones a las que se accede a través de Citrix Enterprise Browser. Para obtener más información sobre GACS, consulte Administrar Citrix Enterprise Browser a través del servicio de configuración global de aplicaciones.

Para crear un grupo de seguridad, realice los siguientes pasos:

1. En la consola de acceso privado seguro, haga clic en **Aplicaciones** y luego haga clic en **Grupos de seguridad**.
2. Haga clic en **Agregar un nuevo grupo de seguridad**.

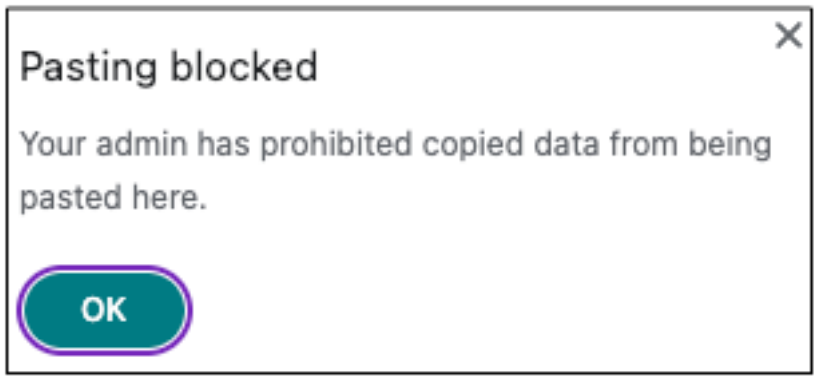


1. Introduzca un nombre para el grupo de seguridad.
2. En **Agregar aplicaciones web o SaaS**, elija las aplicaciones que desea agrupar para habilitar el control de copiar y pegar. Por ejemplo, Wikipedia, Pinterest y Dribble.
3. Haga clic en **Guardar**.

Para obtener detalles sobre la configuración avanzada del portapapeles, consulte Habilitar controles de copiar/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/pegar) de una aplicación a las demás aplicaciones dentro del grupo de seguridad. La operación de copiar y pegar se realiza independientemente de otras restricciones de seguridad que ya estén habilitadas para las aplicaciones.

Sin embargo, los usuarios finales no pueden copiar y pegar 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 la aplicación designada a otra aplicación:



> **Nota**
>
> Puede habilitar copiar/pegar contenido desde aplicaciones locales en máquinas de usuario o controles de aplicaciones no publicadas mediante las opciones en la sección **Configuración avanzada del portapapeles** . Para obtener más detalles, consulte Habilitar controles de copiar/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 en un grupo designado. Puede hacerlo creando políticas de acceso para las aplicaciones y habilitando la restricción **Copiar** / **Pegar** según sus necesidades.

> **Nota**
>
> Asegúrese de que la política de acceso específica que ha creado para el acceso al portapapeles a nivel granular tenga una prioridad mayor que la política que ha creado para los grupos de seguridad.

Ejemplo:

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

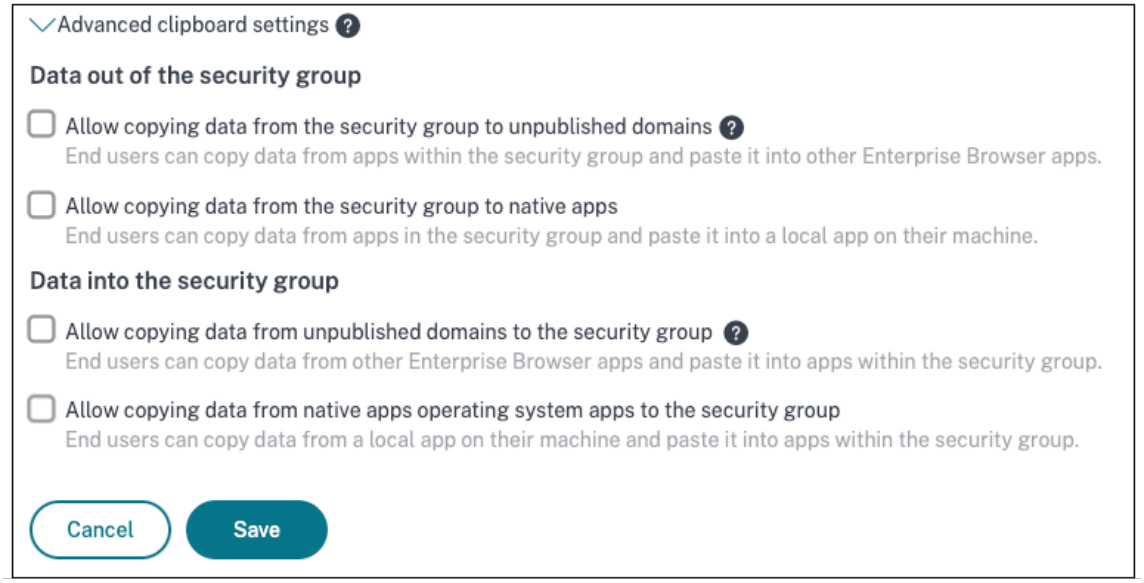
Ahora, desea restringir el pegado de contenido de Wikipedia o Dribble en Pinterest. Para hacerlo, lleve a cabo los siguientes pasos:

1. Crear o editar una política de acceso asignada para la aplicación `Pinterest`. Para obtener detalles sobre cómo crear una política de acceso, consulte Configurar políticas de acceso.
2. En **Acciones**, seleccione **Permitir con restricciones**.
3. Seleccionar **Pegar**.

Aunque Pinterest es parte de un grupo de seguridad que también contiene Wikipedia y Dribble, los usuarios no pueden copiar contenido de Wikipedia o Dribble a Pinterest debido a la política de acceso asociada con Pinterest en la que está habilitada la restricción **Pegar** .

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

1. Crear un grupo de seguridad. Para obtener más detalles, consulte Grupos de seguridad del portapapeles para restricciones de copiar y pegar.
2. Expandir **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** –Habilitar la copia de datos de las aplicaciones en los grupos de seguridad a las aplicaciones que no están publicadas en Secure Private Access.
   - **Permitir la copia de datos del grupo de seguridad a aplicaciones nativas** - Habilite la copia de datos de las aplicaciones en los grupos de seguridad a las aplicaciones locales en sus máquinas.
   - **Permitir la copia de datos de los dominios no publicados al grupo de seguridad** –Habilitar la copia de datos de las aplicaciones no publicadas a través del acceso privado seguro a las aplicaciones en los grupos de seguridad.
   - **Permitir la copia de datos desde aplicaciones nativas del sistema operativo del grupo de seguridad** - Habilitar la copia de datos desde aplicaciones locales en las máquinas a las aplicaciones.

Problemas conocidos

- La tabla de enrutamiento en (**Configuración > Dominio de 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, la función copiar y pegar se deshabilita desde estas aplicaciones, independientemente de las opciones que haya seleccionado en **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 a dominios no publicados**.

En este escenario, si el usuario intenta copiar datos de esta aplicación a otra aplicación en el mismo grupo de seguridad, el control de pegado se deshabilita. Se muestra una notificación al usuario al respecto.

- Para una aplicación SaaS, se puede denegar el acceso a la aplicación si la aplicación está configurada con una política 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 del acceso privado seguro. Además, si la aplicación es parte del grupo de seguridad, la configuración del grupo de seguridad no se respeta y, por lo tanto, no se puede copiar/pegar contenido de la aplicación.

Flujo de usuarios finales

August 26, 2024

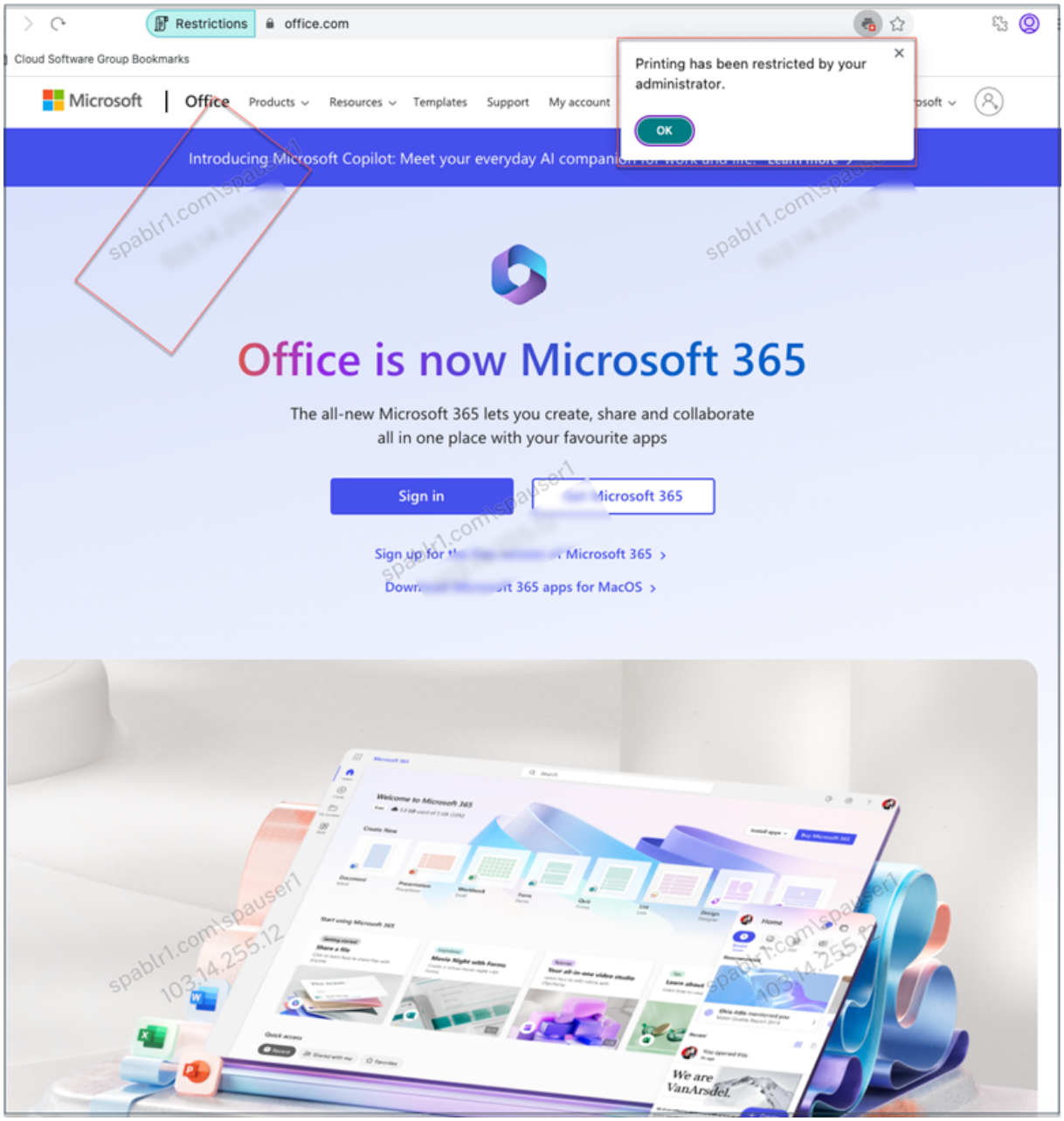
Aplicación SaaS

Supongamos que un administrador ha configurado la aplicación Office 365 con la restricción de marca de agua e impresión para el usuario final. Ahora, cuando el usuario final acceda a la aplicación Office 365, 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 Office 365:

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 Office 365 se ha iniciado y contiene la marca de agua. Además, si el usuario final intenta imprimir algunos datos desde la aplicación Office 365, se le debe mostrar el mensaje de restricción de impresión.



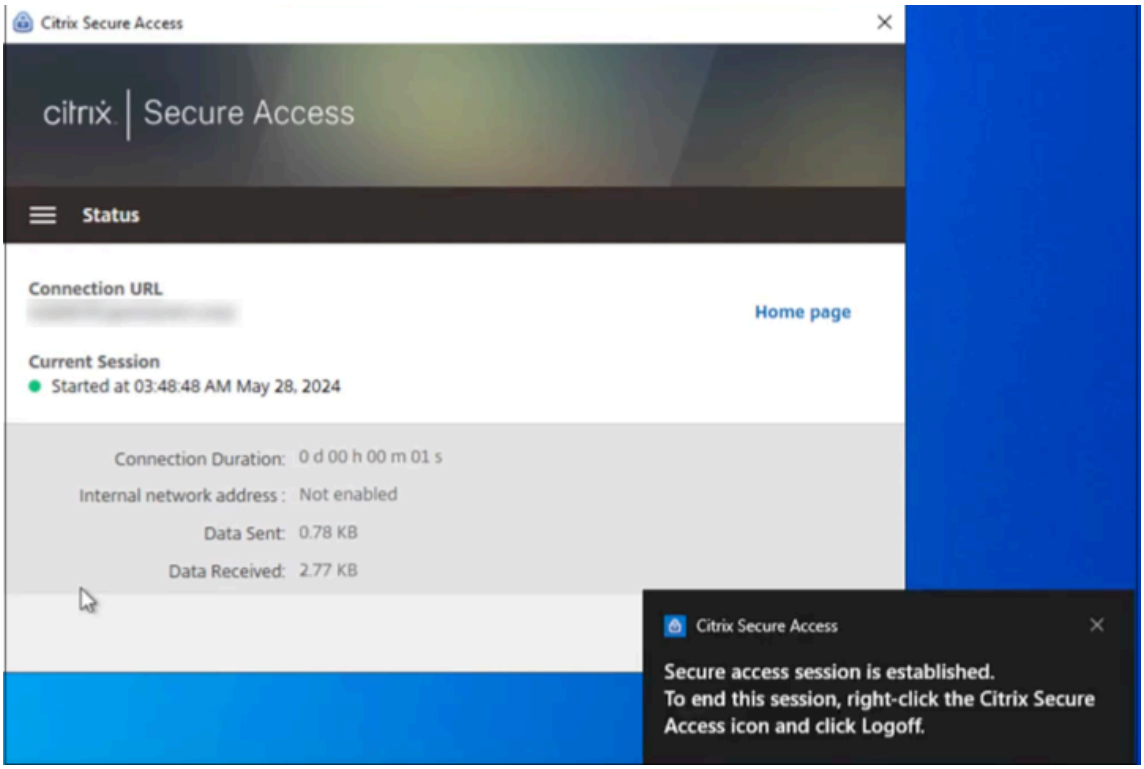
Nota:

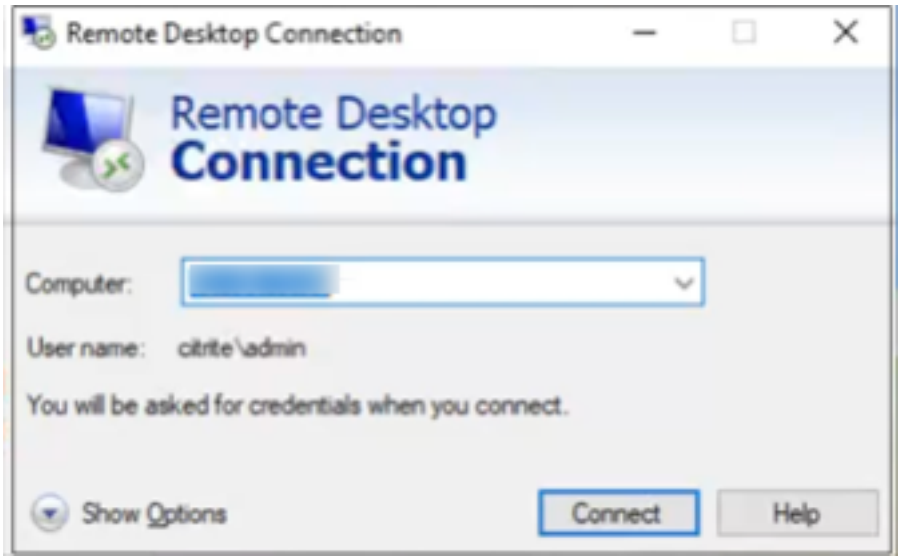
Los administradores deben proporcionar a los usuarios la información de cuenta que necesitan para acceder a los escritorios y aplicaciones virtuales. Para obtener más información, consulte Agregar la URL del almacén a la aplicación Citrix Workspace.

Aplicación TCP/UDP

Si RDP está configurado, los usuarios finales deben realizar los siguientes pasos para acceder a la aplicación TCP/UDP.

1. Inicie sesión en el cliente Citrix Secure Access.
2. Una vez establecida la sesión de acceso seguro, inicie una conexión a escritorio remoto.





a) Presione la tecla **Windows**, escriba **Conexión a Escritorio remoto** y presione **Intro**.
b) Introduzca la dirección IP o el nombre de host del equipo al que intenta conectarse.
c) Haga clic en **Conectar**. Es posible que se le pida que introduzca las credenciales.
d) Introduzca el nombre de usuario y la contraseña del equipo remoto y, a continuación, haga clic en **Aceptar**.

Ahora se ha establecido una conexión de escritorio remoto y el usuario final puede interactuar con el equipo remoto.

Actualización de versión

October 21, 2024

Puede actualizar sus implementaciones de Secure Private Access a una versión más nueva sin tener que configurar primero nuevas máquinas o sitios. 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 complemento Secure Private Access instalado anteriormente.

Secuencia de actualización

La secuencia de actualización es la siguiente:

1. Puede actualizar Secure Private Access a través del controlador de entrega o mediante el mosaico dedicado de Secure Private Access en la interfaz de usuario del instalador, según cómo instaló originalmente Secure Private Access.
    - Si ha instalado Secure Private Access a través de Delivery Controller, no podrá actualizar el componente Secure Private Access solo. En su lugar, debes actualizar todos los componentes. Para obtener más detalles, consulte Actualizar una implementación.
    - Si ha instalado Secure Private Access a través del mosaico dedicado Secure Private Access, puede actualizarlo de forma independiente. Para obtener más detalles, consulte Actualice su instalador de Secure Private Access.

> **Nota**
>
> Le recomendamos que instale Secure Private Access a través del controlador de entrega para entornos POC. Sin embargo, para entornos de producción, le recomendamos que utilice el instalador dedicado para que pueda adaptar nuevas características o funcionalidades.

1. Ejecute los scripts de la base de datos. Para obtener más detalles, consulte Actualizar la base de datos mediante scripts.
2. Reinicie el **Sitio web predeterminado** y **Sitio de administración de Citrix Access Security** En el **Administrador del Servicio de Información de Internet (IIS)** consola para aplicar los cambios.
3. Ejecute nuevamente la configuración de StoreFront. Descargue los scripts de StoreFront desde **Configuración > Configuración**y ejecute los scripts en las máquinas StoreFront correspondientes. Para obtener más detalles, consulte Modificar la configuración de integración.

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

1. (Opcional) Ejecute el script de NetScaler Gateway. Para obtener más detalles, consulte NetScaler Gateway.

Actualización de componentes

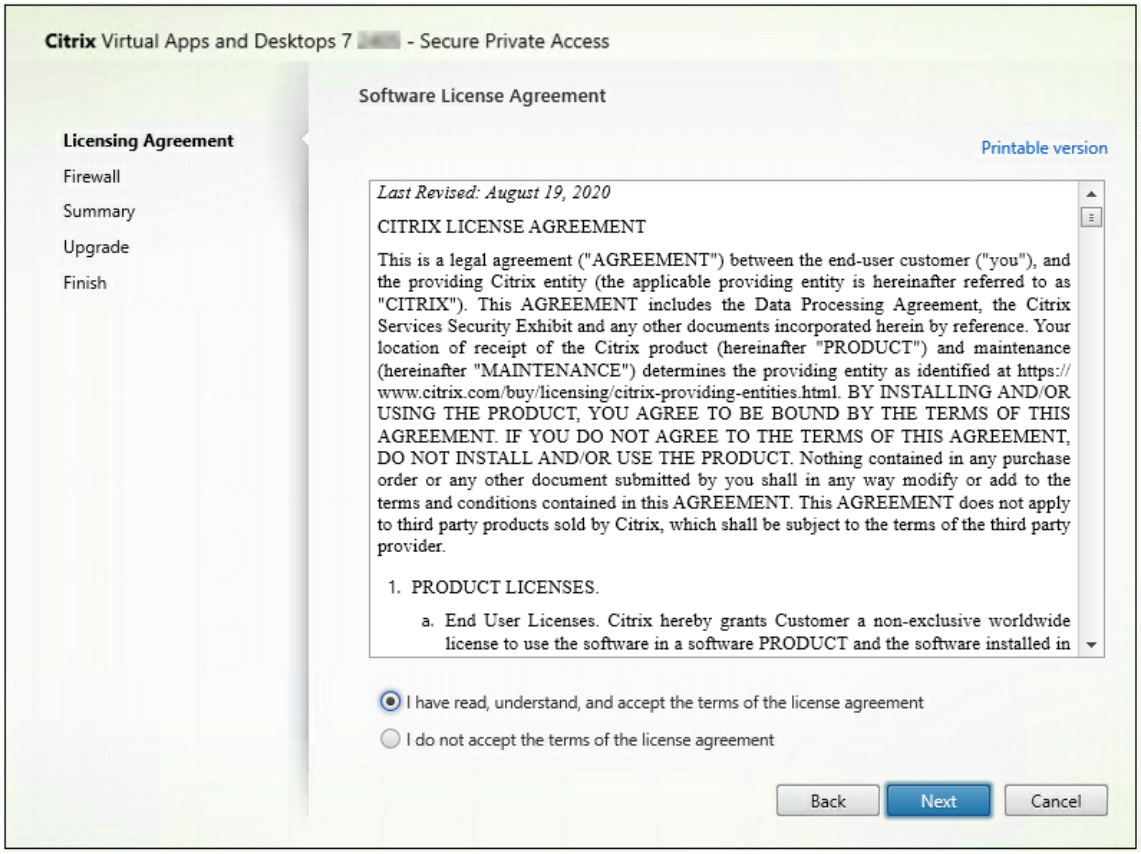
Consulte los siguientes temas para actualizar los componentes involucrados en la implementación local de Secure Private Access.

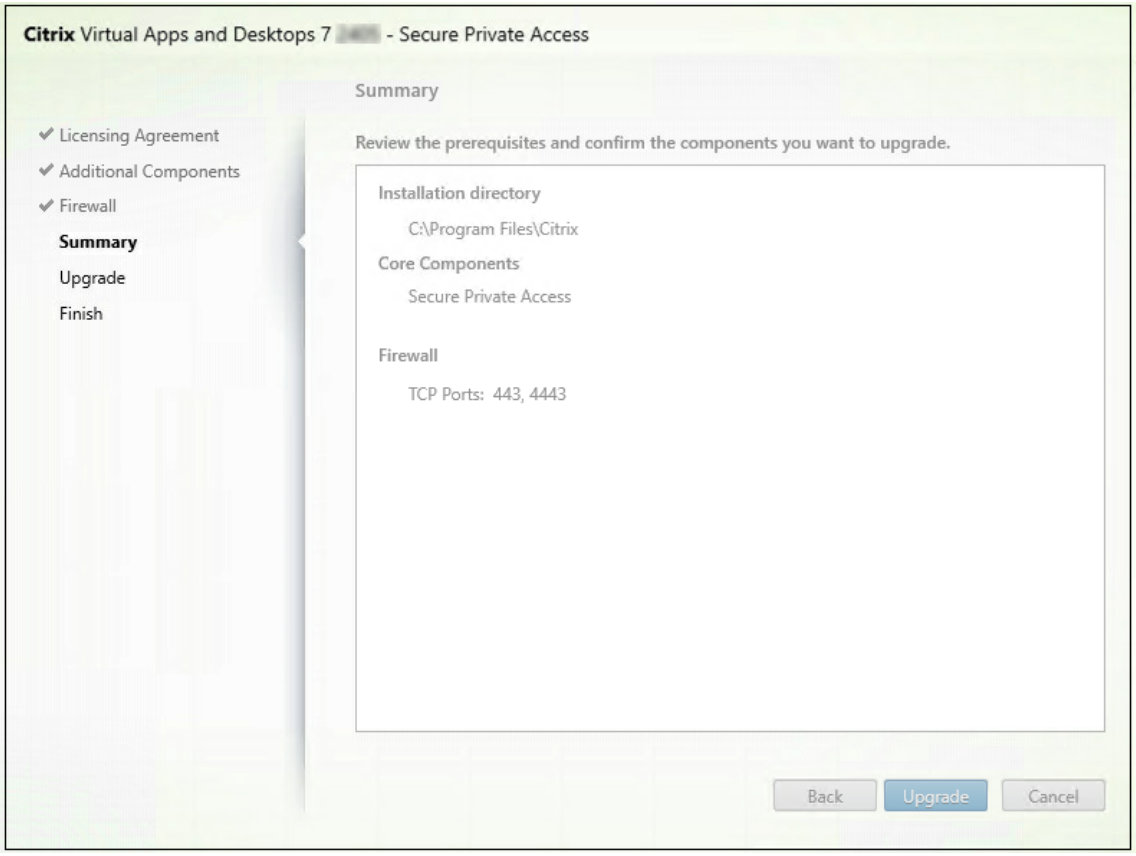
- Cloud Connector
- StoreFront
- NetScaler Gateway
- Servidor de licencias
- Web Studio
- Director

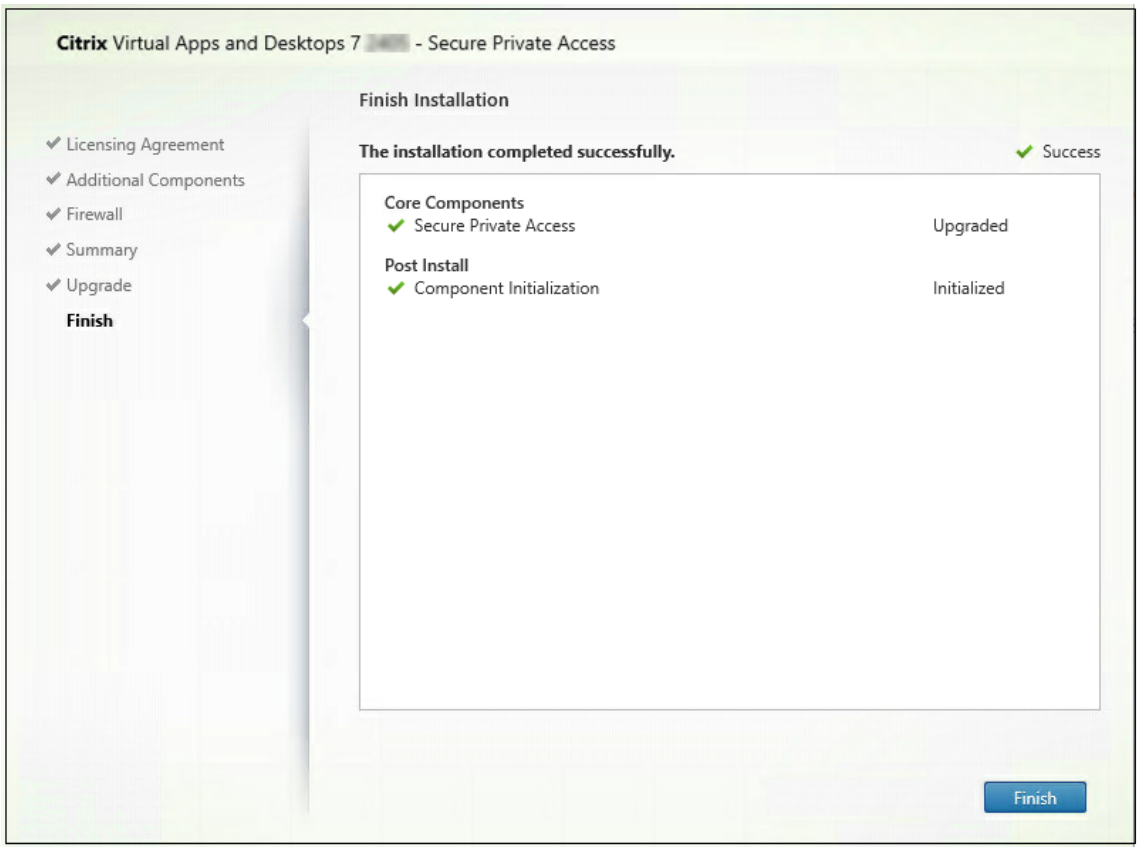
Actualice su instalador de Secure Private Access

October 21, 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 al dominio.
3. Siga las instrucciones en pantalla para completar la instalación.







> **Importante:**
>
> Después de actualizar el instalador para lanzar la última versión, debe volver a ejecutar el script de StoreFront para que los nuevos detalles del punto final estén disponibles.

Siguientes pasos

- Configurar acceso privado seguro
- Configurar NetScaler Gateway
- Configurar aplicaciones
- Configurar políticas de acceso para las aplicaciones

Actualice la base de datos mediante scripts

December 27, 2023

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

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

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

Administrar configuraciones

October 21, 2024

Después de haber instalado Secure Private Access, puede modificar la configuración desde la página **Configuración** . Puede administrar el enrutamiento de dominios de aplicaciones, 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 detalles sobre cómo actualizar o modificar la configuración, consulte los siguientes temas:

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

Gestionar sitios web no autorizados

También puedes configurar reglas para sitios web no autorizados. Las aplicaciones (intranet o internet) que no estén configuradas dentro de Secure Private Access se consideran "Sitios web no autorizados". Para obtener más detalles, consulte Sitios web no autorizados.

Herramienta de modelado de políticas

La herramienta de modelado de políticas proporciona visibilidad del resultado del acceso a la aplicación (permitido o permitido con restricciones o denegado). Los administradores pueden verificar los resultados de acceso para usuarios específicos y la condición del usuario. Para obtener más detalles, consulte Herramienta de modelado de políticas.

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.

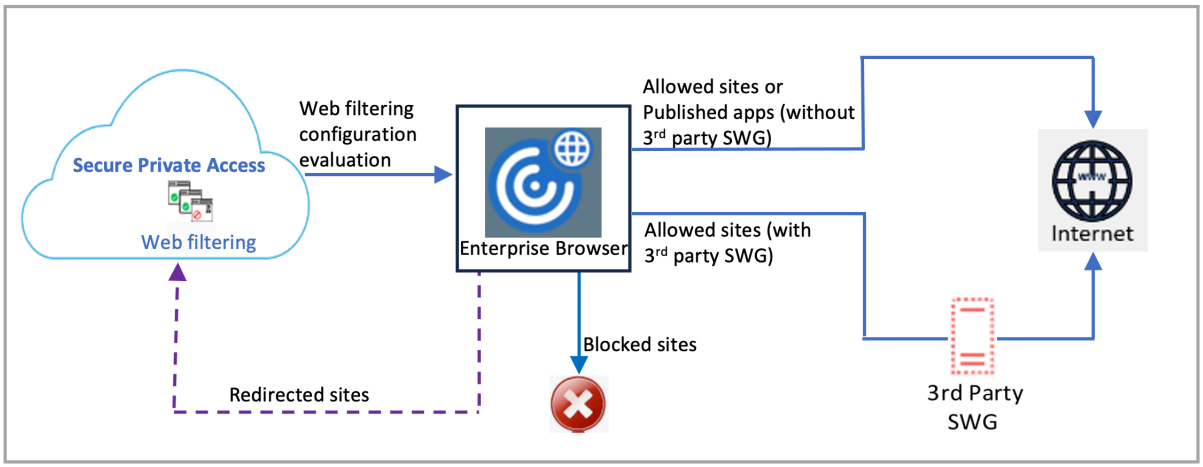
Para todas las demás URL de Internet o aplicaciones SaaS que no tengan una aplicación configurada, los administradores pueden usar la ficha **Parámetros > Sitios web no autorizados** de la consola de administración para permitir o denegar el acceso a través de Citrix Enterprise Browser.

> **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.



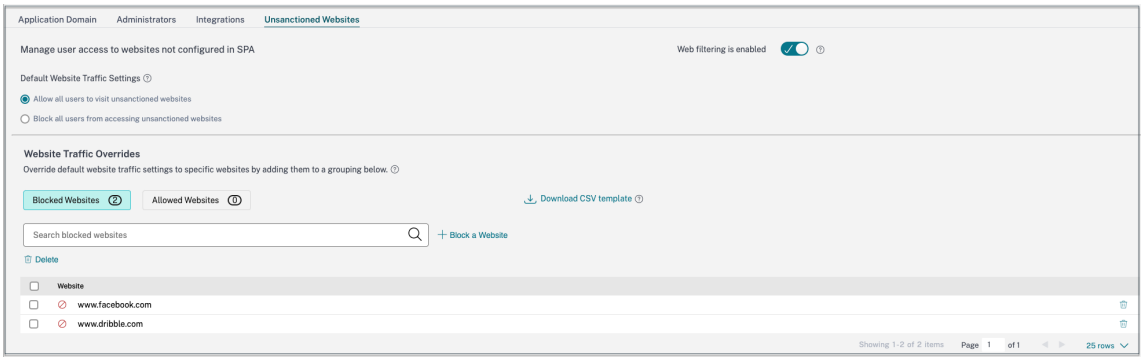
Cuando llega una solicitud, se llevan a cabo las comprobaciones siguientes y se toman las medidas correspondientes:

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.

Administrar la configuración después de la instalación

October 21, 2024

Administrar el enrutamiento de dominios de aplicaciones

Puede ver una lista de dominios de aplicaciones agregados en su configuración de Acceso Privado Seguro. La tabla de dominios de la aplicación enumera todos los dominios relacionados y cómo se enruta el tráfico de la aplicación (externa o internamente).

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

Administrar administradores

Puede ver la lista de administradores y también agregar administradores desde la página **Configuración > Administradores** . Al administrador que instala el Acceso Privado Seguro por primera vez se le concede permiso completo. Luego, este administrador puede agregar otros administradores a la configuración.

También puede agregar grupos de administradores para que el acceso esté habilitado para todos los administradores en ese grupo.

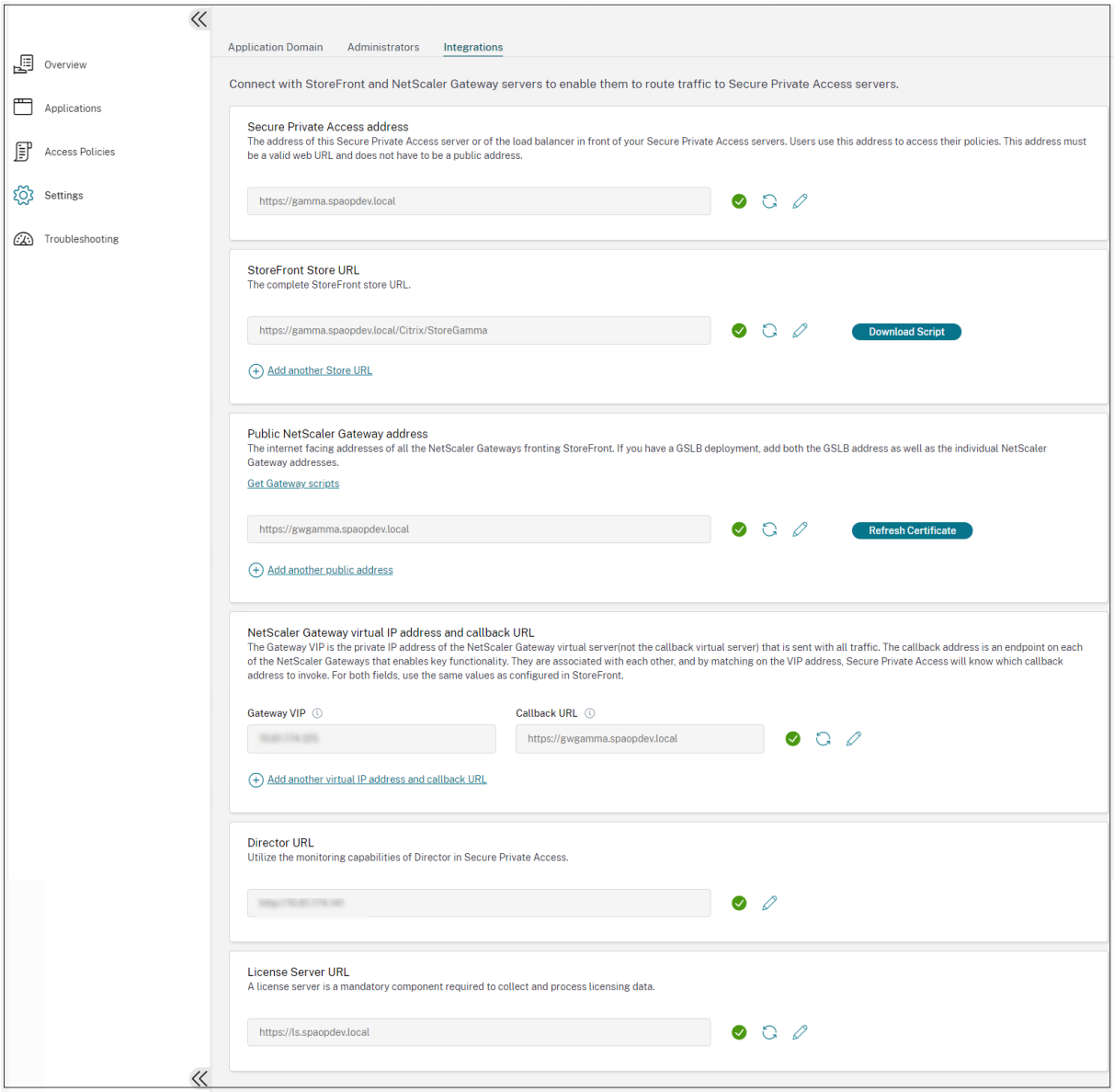
1. En la página **Administradores** , haga clic en **Agregar**.
2. En **Dominio**, seleccione el dominio al que debe agregarse este administrador.
3. En **Usuarios o grupo de usuarios**, seleccione el usuario o el grupo al que pertenece este usuario.
4. En **Tipo de administrador**, seleccione el tipo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

Modificar la configuración de integración

Una vez que haya configurado el acceso privado seguro, puede modificar o actualizar las entradas de StoreFront y NetScaler Gateway desde la pestaña **Integraciones** .

1. Haga clic en **Configuración > Integraciones**.
2. Haga clic en el icono de edición según la configuración que desee modificar y actualizar la entrada.
3. Haga clic en el icono de actualización para asegurarse de que la configuración sea válida.

> **Nota**
>
> - Si se cambia la dirección de acceso privado seguro, descargue el script de StoreFront y ejecútelo en el host de StoreFront.
> - Si Secure Private Access está instalado en una máquina diferente a StoreFront, descargue el script de StoreFront y ejecútelo en StoreFront.



Administrar aplicaciones y directivas

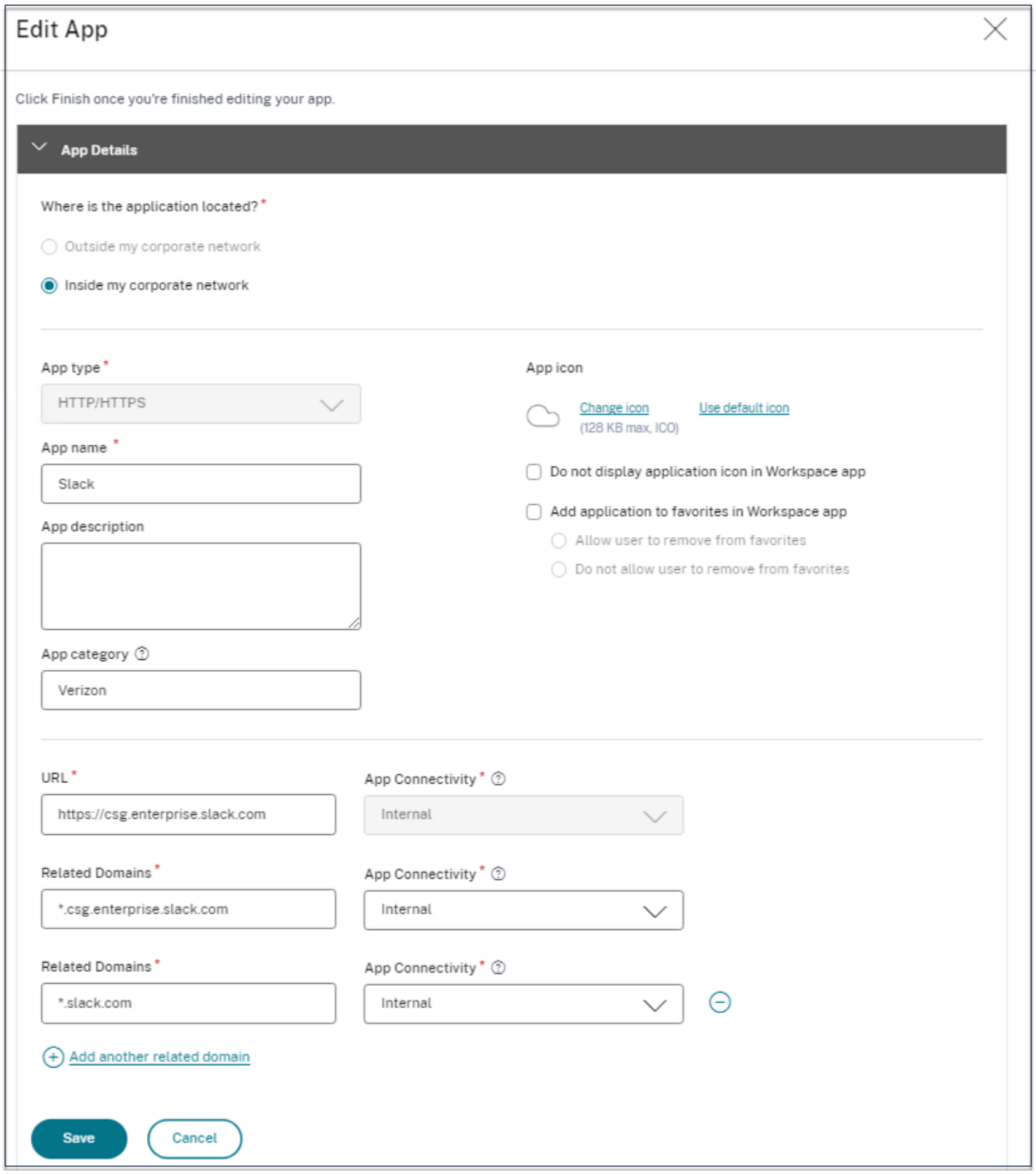
June 19, 2024

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

Modificar una aplicación

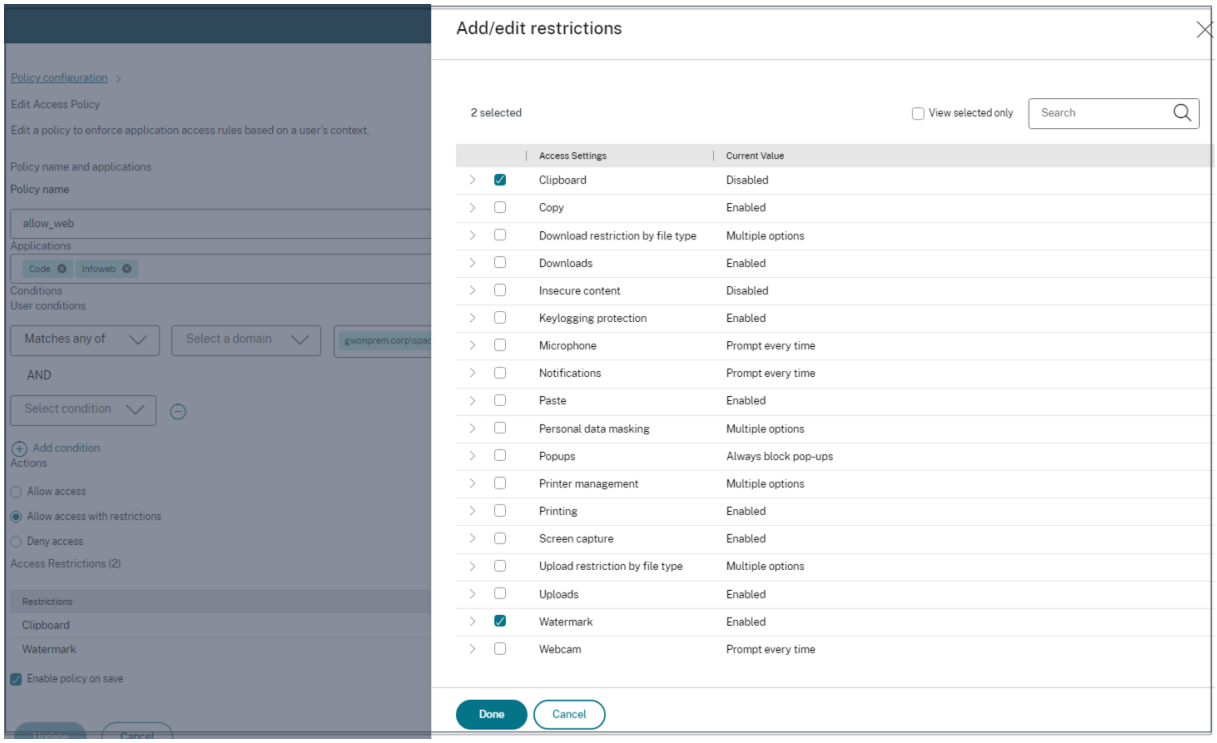
1. En la consola de administración de Secure Private Access, haga clic en **Aplicaciones**.

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 **Guardar**.



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**.



Desinstalar Secure Private Access

October 21, 2024

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

1. Seleccione **Citrix Virtual Apps and Desktops 7 2408 –Acceso privado seguro**.
2. Haga clic en **Desinstalar**.
3. Siga las instrucciones en pantalla y complete la desinstalación.

> **Nota**
>
> Si se completa la configuración posterior a la instalación de Secure Private Access, antes de

> desinstalar Secure Private Access, descargue el archivo StoreFrontScripts.zip desde la consola de administración para eliminar el complemento Secure Private Access de la configuración de la tienda StoreFront.

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

1. Inicie sesión en la consola de administración de Secure Private Access.
2. Haga clic en **Configuración** y luego haga clic en la pestaña **Integraciones** .
3. Haga clic en **Descargar script** en la sección URL de la tienda StoreFront.

Eliminar el complemento Secure Private Access de la configuración de la tienda StoreFront

Después de desinstalar Secure Private Access, debe eliminar el complemento Secure Private Access de la configuración de la tienda 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 privilegios de administrador.
5. Ejecute este comando:

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

Supervisión y solución de problemas

June 19, 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

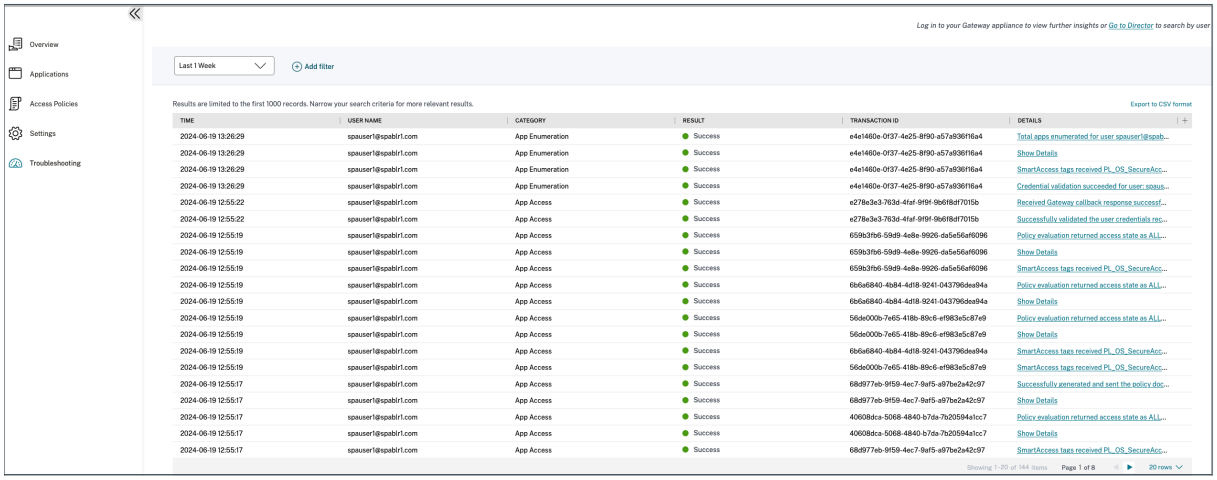
- Configurar Director con Secure Private Access
- Ver una sesión de Secure Private Access en Director
- Lista de códigos de sesión de Secure Private Access en Director.
- Director.

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. Puede usar la opción **Agregar filtro** para refinar la búsqueda en función de diversos criterios, como la categoría de la aplicación, el nombre de usuario y el ID de la transacción. 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.

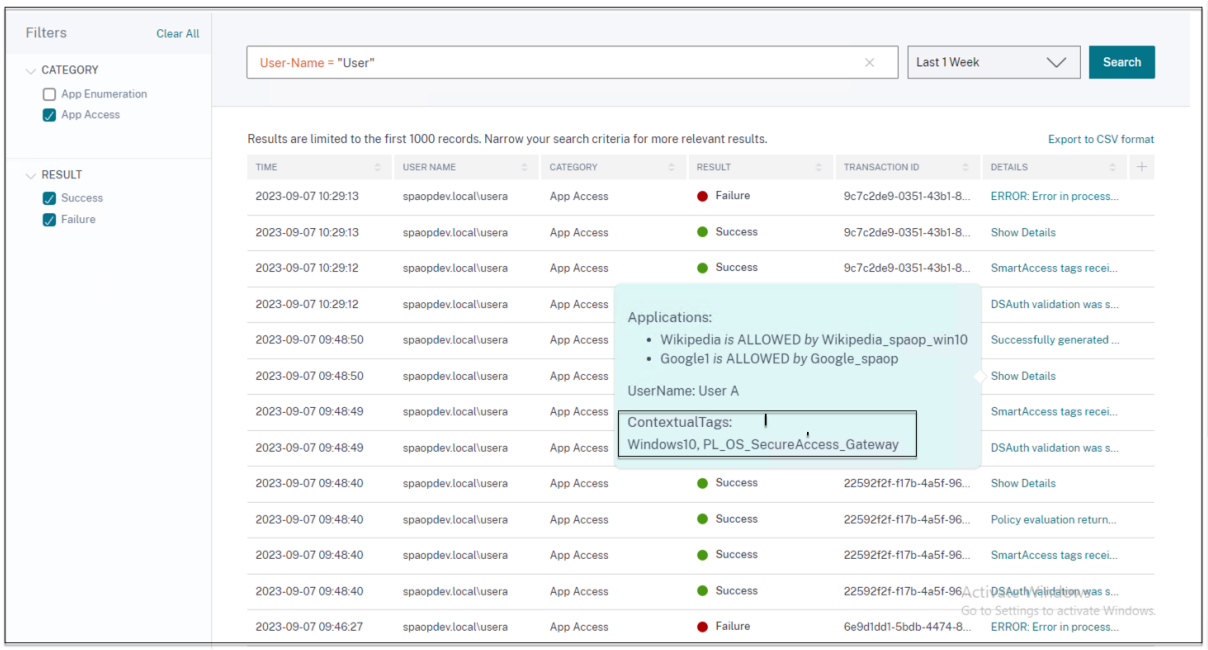
Por ejemplo, puede buscar un evento del tipo "Enumeración"utilizando la cadena **Event-Type > = (igual a algún valor) > Enumeration** en el campo de búsqueda.

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. Si la autenticación de nFactor está configurada, los nombres de las acciones de EPA nFactor que están validados para los usuarios actuales también se capturan como parte de las etiquetas contextuales.



Solución de problemas básicos

June 19, 2024

En este tema se enumeran algunos de los errores que puede encontrar durante 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

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

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

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

  Este mensaje de error puede aparecer en cualquiera de los 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.

    Resolución: debe eliminar manualmente la base de datos.
  - Elija configurar la base de datos manualmente (seleccionando Configuración manual en la página Configuración de bases de datos) mediante el script y 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

  Resolución:

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

Fallos de StoreFront

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

  Actualice las entradas de StoreFront desde la ficha **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.

  Resolución:

  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>`

  Resolución:

  1. Es posible que haya una restricción en la directiva de ejecución de PowerShell. Ejecute el comando de script de PowerShell `Get-ExecutionPolicy` para obtener más información.
  2. Si está restringido, debe omitirlo y ejecutar manualmente un script de configuración de StoreFront.
  3. Haga clic en **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.

  Resolución:

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

  1. Haga clic en **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 compatible con Windows x64 con privilegios de administrador y después ejecute ConfigureStoreFront.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>

Resolución:

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

Resolución:

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
 }
```


Solucionar problemas de sesiones mediante Director

October 21, 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. Las siguientes tablas 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 acceso privado seguro en Director

> **Nota**
>
> - Los códigos que contienen "0"en el segundo dígito representan un flujo de ejecución normal. Por ejemplo, 1000 representa una enumeración de aplicaciones exitosa.
> - Los códigos que contienen "1"en el segundo dígito representan una falla o excepción. Por ejemplo, 2101 representa una falla de sesión. En caso de falla o excepción, se recomienda resolver dichos problemas examinando los registros. Si eso no resuelve el problema, comuníquese con el soporte técnico.

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 al menos una de ellas falló en su evaluación.
1103	fallo	No se enumeraron aplicaciones y al menos una de ellas falló en su evaluación.
1000	Success	La enumeración fue exitosa. Se enumeró al menos una aplicación.

Código	Estado	Descripción
1001	Success	No se enumeraron aplicaciones porque todas fueron rechazadas por las políticas.
1002	Success	No se enumeraron aplicaciones porque no coincidieron ninguna política.
1003	Success	No se enumeraron aplicaciones porque algunas fueron rechazadas y para otras no coincidieron con ninguna política.
1004	Success	No se enumeraron aplicaciones porque no hay políticas para evaluar.

Códigos relacionados con la sesión

Código	Estado	Descripción
2101	Fallo	Error de sesión.
2102	activo/inactivo/falla	La sesión está activa o finalizada o falló al menos un inicio de aplicación en la sesión.
2000	Active	La sesión está activa.
2001	Inactivo	La sesión ha finalizado/está inactiva.

Códigos de mensajes de enumeración de aplicaciones

Código	Estado	Descripción
3101	Fallo	Enumeración de aplicaciones: se produjo un error interno (actualmente sin uso).

Código	Estado	Descripción
3102	Fallo	La aplicación no se enumeró porque hubo una excepción durante la evaluación de la política.
3103	Fallo	El estado de enumeración de la aplicación es nulo: se produjo un error interno durante la evaluación de la política.
3104	Permitir/denegar/fallar	Error al recuperar los detalles de la política para la aplicación.
3000	Allow	Se permite la enumeración de aplicaciones.
3001	Denegar	La enumeración de aplicaciones está denegada por política.
3002	Denegar	La aplicación no se enumeró porque no coincidió ninguna política.
3003	Desconocido	Se desconoce el estado de enumeración de la aplicación.
3004	Lanzamiento de la aplicación desde CEB	Intento de inicio de aplicación desde Citrix Enterprise Browser.

Códigos de mensajes de inicio de la aplicación

Código	Estado	Descripción
4101	Fallo	Error al iniciar la aplicación: se produjo un error interno durante el inicio de la aplicación
4102	Fallo	Error de inicio de la aplicación (interno)
4103	Permitir/denegar/fallar	Error al recuperar los detalles de la política para la aplicación

Código	Estado	Descripción
4000	Allow	Se permite el lanzamiento de la aplicación.
4001	Denegar	Se denegó el lanzamiento de la aplicación debido a una política.
4002	Denegar	Se denegó el inicio de la aplicación porque no coincidía ninguna política.

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

ID de suceso	Resumen	Descripción	Origen
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
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 del uso compartido de registros en soluciones SIEM

Integración con Scout

August 26, 2024

Citrix Scout está integrado con Secure Private Access para permitir a los administradores recopilar registros y métricas para la solución de problemas. Para obtener información sobre qué información se recopila, consulte Qué se recopila.

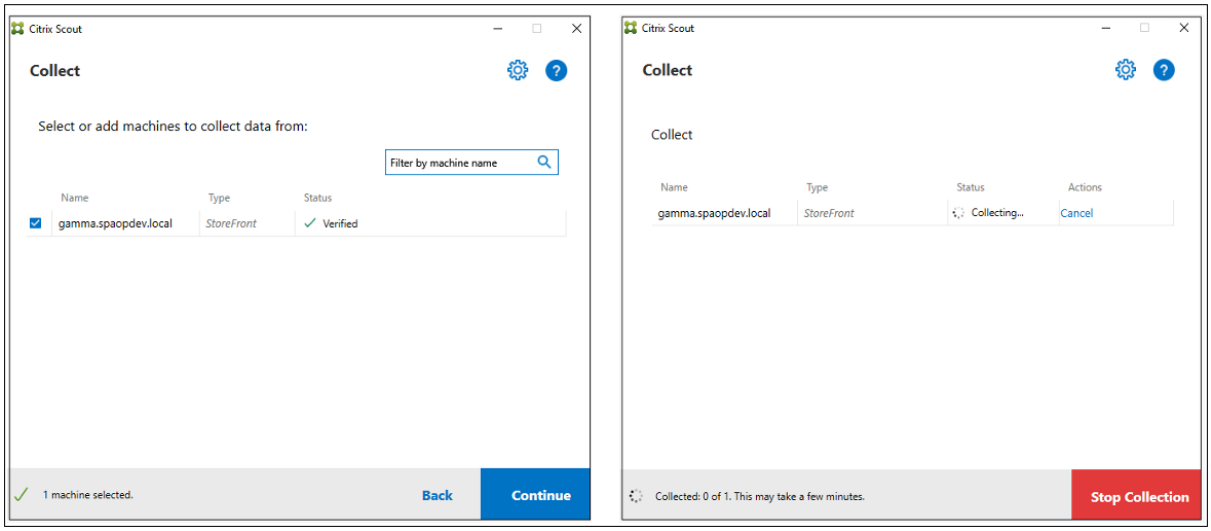
Para empezar a recopilar los registros de Secure Private Access, siga estos pasos:

1. Seleccione una máquina de Secure Private Access para iniciar la recopilación.
2. Haga clic en **Continuar**.

Puede hacer clic en **Detener la recopilación** en cualquier momento para detener la recopilación.

Citrix Scout también obtiene los siguientes registros. Estos registros se almacenan en un paquete en la máquina local y se pueden cargar en Citrix Cloud.

- C:\Program Files\Citrix\Citrix Access Security\Admin\AdminService\logs\spa-admin
- C:\Program Files\Citrix\Citrix Access Security\Runtime\RuntimeService\logs\spa-runtime



Configuración de retención de registros

June 19, 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:

```
1   "TroubleshootingLogs": {
2
3     "CleanupPeriodInHours": 12,
4     "CleanupDataOlderThanDays": 7,
5     "CleanupOldestDataIfEntriesCountAbove": 0
6    }
```

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

June 19, 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

December 27, 2023

Citrix Secure Private Access para entornos locales