Citrix Secure Private Access

Machine translated content

Disclaimer

Contents

Novedades

February 16, 2024

16 de octubre de 2023

- **Características de vista previa de la solución local de Secure Private Access**

  La solución local de Secure Private Access ahora ofrece lo siguiente:

  - Interfaz de usuario de administración para la primera configuración.
  - Interfaz de usuario de administración para configurar las aplicaciones y las directivas de acceso.
  - Panel de registros.

  Para obtener más información, consulte Secure Private Access para instalaciones locales.

- **Funciones de vista previa del servicio Device Posture**

  El servicio Device Posture ahora admite las siguientes comprobaciones:

  - El servicio Device Posture ahora es compatible con las plataformas IGEL.
  - El servicio Device Posture ahora admite verificaciones de geolocalización y ubicación de red.

  Para obtener más información, consulte Postura del dispositivo.

11 de septiembre de 2023

- **Disponibilidad general de la integración de la postura del dispositivo con Microsoft Intune**

  La integración de la postura del dispositivo con Microsoft Intune ya está disponible de forma general. Para obtener más información, consulte Integración de Microsoft Intune con Device Posture.

30 de agosto de 2023

- **Administrar Citrix Endpoint Analysis Client para el servicio Device Posture**

  El cliente EPA se puede utilizar junto con NetScaler y Device Posture. Se requieren algunos cambios de configuración para administrar el cliente EPA cuando se usa con NetScaler y Device Posture. Para obtener más información, consulte Administrar el servicio Citrix Endpoint Analysis Client for Device Posture.

28 de agosto de 2023

- **Soporte del servicio Device Posture en plataformas iOS**

  El servicio Device Posture ahora es compatible con las plataformas iOS. Para obtener más información, consulte Postura del dispositivo.

  Esta función se encuentra en Tech Preview.

22 de agosto de 2023

- **Comprobación del certificado del dispositivo con el servicio Citrix Device Posture**

  El servicio Citrix Device Posture ahora permite el acceso contextual (Smart Access) a los recursos de Citrix DaaS y Secure Private Access comprobando el certificado del dispositivo final con una entidad de certificación corporativa para comprobar si se puede confiar en el dispositivo final. Para obtener más información, consulte Comprobación del certificado del dispositivo con el servicio Device Posture.

  Esta función se encuentra en Tech Preview.

17 de agosto de 2023

- **Eventos de postura del dispositivo en Citrix DaaS Monitor**

  Los eventos del servicio Device Posture y los registros de supervisión ahora se pueden buscar en DaaS Monitor. Para obtener más información, consulte Eventos de postura del dispositivo en Citrix DaaS Monitor.

07 de junio de 2023

- **Herramienta para configurar Secure Private Access para instalaciones locales**

  Ahora hay disponible una interfaz de usuario simplificada para configurar la solución de Secure Private Access para instalaciones locales. La herramienta de configuración se puede ejecutar en un controlador de entrega de Citrix Virtual Apps and Desktops para crear rápidamente una aplicación web o SaaS. Además, puede utilizar esta herramienta para establecer las restricciones de las aplicaciones, el enrutamiento del tráfico y la configuración de NetScaler Gateway. Para obtener más información, consulte /en-us/citrix-secure-private-access/service/secure-private-access-for-on-premises-config-tool.html .

29 May 2023

- **Disponibilidad general de creación de directivas de acceso con múltiples reglas**

  Puede crear varias reglas de acceso y configurar diferentes condiciones de acceso para diferentes usuarios o grupos de usuarios dentro de una única directiva. Estas reglas se pueden aplicar por separado para las aplicaciones HTTP/HTTPS y TCP/UDP, todo ello dentro de una única directiva. Para obtener más información, consulte Configurar una directiva de acceso con varias reglas.

  [SPA-746]

10 de abril de 2023

- **Detección de aplicaciones**

  La función de detección de aplicaciones ayuda al administrador a ver las aplicaciones privadas internas, como las aplicaciones web y las aplicaciones cliente-servidor (aplicaciones basadas en TCP y UDP) de su organización, y a los usuarios que acceden a esas aplicaciones. Los administradores pueden detectar las aplicaciones especificando el alcance de los dominios (dominios comodín) o las subredes IP. Para obtener más información, consulte Detección de aplicaciones.

  [ACS-2325]

29 de marzo de 2023

- **Solución de Secure Private Access para implementaciones locales**

  Como cliente de Citrix StoreFront y NetScaler Gateway, ahora puede acceder sin problemas a las aplicaciones web y SaaS junto con las aplicaciones virtuales de Citrix y los escritorios virtuales mediante la solución Citrix Secure Private Access para implementaciones locales. Para obtener más información, consulte Secure Private Access para instalaciones locales.

  [SPAOP-1]

07 de marzo de 2023

- **Configurar sufijos DNS**

  La función de sufijo DNS de Citrix Secure Private Access Service se puede utilizar para los siguientes casos de uso:

  - Permita que el cliente Citrix Secure Access resuelva un nombre de dominio no completo (nombre de host) en un nombre de dominio completo (FQDN) agregando el dominio con sufijo DNS para los servidores de fondo.

  - Permita a los administradores configurar las aplicaciones mediante direcciones IP (intervalo IP CIDR/IP), de modo que los usuarios finales puedan acceder a las aplicaciones mediante el FQDN correspondiente en el dominio del sufijo DNS.

Para obtener más información, consulte los sufijos DNS para resolver los FQDN en direcciones IP.

[ACS-2490]

23 de enero de 2023

- **Servicio de postura del dispositivo**

  El servicio Citrix Device Posture es una solución basada en la nube que ayuda a los administradores a cumplir ciertos requisitos que los dispositivos finales deben cumplir para acceder a los recursos de Citrix DaaS (aplicaciones y escritorios virtuales) o Citrix Secure Private Access (SaaS, aplicaciones web, TCP y UDP). Para obtener más información, consulte Device Posture.

  [AAUTH-90]

- **Integración de Microsoft Endpoint Manager con Device Posture**

  Además de los escaneos nativos que ofrece el servicio Device Posture, el servicio Device Posture también se puede integrar con otras soluciones de terceros. Postura del dispositivo está integrado en Microsoft Endpoint Manager (MEM) en Windows y macOS. Para obtener más información, consulte Integración de Microsoft Endpoint Manager con Device Posture.

  [ACS-1399]

22 de diciembre de 2022

- **Single Sign-On para la URL de Workspace para los usuarios que hayan iniciado sesión a través de la aplicación Citrix Workspace**

  El cliente de Citrix Secure Access ahora admite Single Sign-On para la URL de Workspace cuando ya se ha iniciado sesión a través de la aplicación Citrix Workspace. Esta funcionalidad de SSO mejora la experiencia del usuario al evitar múltiples autenticaciones. Para obtener más información, consulta la compatibilidad con inicio de sesión único para la URL de Workspace.

  [ACS-1888]

- **Habilite el acceso a las aplicaciones mediante directivas de acceso**

  Para conceder acceso a las aplicaciones a los usuarios, ahora los administradores deben crear directivas de acceso con una lista de suscripciones de usuarios coincidentes para que las aplicaciones estén disponibles para los usuarios finales. Anteriormente, los administradores tenían

que agregar usuarios como suscriptores para permitir el acceso. Para obtener más información, consulte Crear directivas de acceso.

[ACS-3018]

03 de octubre de 2022

- **Directivas de acceso para conceder el acceso a las aplicaciones**

  La opción de configuración de suscriptores de aplicaciones se elimina de la sección Aplicaciones del asistente de configuración. Para conceder acceso a las aplicaciones a los usuarios, los administradores deben crear directivas de acceso. En las directivas de acceso, los administradores agregan suscriptores a la aplicación y configuran los controles de seguridad. Para obtener más información, consulte Crear directivas de acceso.

  [ACS-3018]

- **Compatibilidad con aplicaciones UDP**

  Secure Private Access Service ahora admite el acceso a las aplicaciones UDP. Para obtener más información, consulte Funciones Tech Preview.

  [ACS-1430]

09 de septiembre de 2022

- **Acceso adaptable basado en la puntuación de riesgo del usuario**

  Los administradores ahora pueden configurar una directiva de acceso adaptable con la puntuación de riesgo de usuario proporcionada por Citrix Analytics for Security (CAS). Para obtener más información, consulte Acceso adaptable basado en la puntuación de riesgo del usuario.

  [ACS-877]

- **Acceso adaptable basado en la ubicación de red del usuario**

  Los administradores ahora pueden configurar la directiva de acceso adaptable en función de la ubicación desde la que el usuario accede a la aplicación. La ubicación puede ser el país desde el que el usuario accede a la aplicación o la ubicación de red del usuario. Para obtener más información, consulte Acceso adaptable según la ubicación.

  [ACS-99]

- **Creador de directivas de acceso adaptable mejorado**

  El acceso a las aplicaciones ahora solo se habilita después de que se cumplan las condiciones configuradas. La suscripción a aplicaciones por sí sola no proporciona a sus clientes acceso a

las aplicaciones. Los administradores deben agregar directivas de acceso para proporcionar acceso a las aplicaciones además de la suscripción a la aplicación. Además, los usuarios o grupos son una condición obligatoria en las directivas de acceso que deben cumplirse para acceder a las aplicaciones. Para obtener más información, consulte Crear directivas de acceso.

[ACS-1850]

- **Restringir la carga de archivos en aplicaciones SaaS/web**

  Esta función permite a los administradores del cliente controlar (permitir o restringir) quién puede subir archivos a sus aplicaciones empresariales de vital importancia. Con esto, solo los usuarios autorizados pueden subir archivos a las aplicaciones. Para obtener más información, consulte Crear directivas de acceso.

  [ACS-655]

- **Panel de mandos mejorado**

  El panel de mandos de Secure Private Access ahora proporciona una visibilidad detallada de varias métricas de usuario, como el uso de la aplicación, los principales usuarios de la aplicación, las principales aplicaciones a las que se accede, los registros de diagnóstico, etc. Para obtener más información, consulte Panel de mandos.

  [ACS-2480]

- **Retirada de la biblioteca**

  Las aplicaciones de Secure Private Access ahora no están visibles en la biblioteca de Citrix Cloud. Todas las aplicaciones configuradas de Secure Private Access se encuentran dentro de la sección de aplicaciones dentro del mosaico de Secure Private Access Service. Esto ayuda a los administradores a navegar, modificar y configurar las aplicaciones con facilidad.

  [ACS-1546]

- **Registros de auditoría para Secure Private Access**

  Los eventos relacionados con el servicio Citrix Secure Private Access ahora se capturan en **Citrix Cloud > Registro del sistema.** Para obtener más información, consulte Registros de auditoría.

  [ACS-876]

- **Registros de diagnóstico para el acceso a aplicaciones web y SaaS empresariales**

  Los eventos de Citrix Secure Private Access ahora están integrados con Citrix Analytics. Citrix Analytics proporciona un punto final público que permite a los administradores acceder a los eventos y descargarlos. Se puede acceder a estos eventos mediante un script de PowerShell. Para obtener más información, consulte Registros de diagnóstico para el acceso a aplicaciones web y SaaS empresariales.

  [ACS-805]

- **Guía para solucionar problemas**

  Los administradores pueden usar la guía de solución de problemas para resolver problemas relacionados con la configuración. Para obtener más información, consulta Solucionar problemas relacionados con las aplicaciones.

  [ACS-2719]

15 de julio de 2022

- **Habilitar el acceso a una aplicación solo si se ha configurado una directiva de acceso**

  El acceso a las aplicaciones ahora se habilita solo después de que el administrador agregue una directiva de acceso además de la suscripción a la aplicación. La suscripción a aplicaciones por sí sola no permite el acceso a las aplicaciones. Con este cambio, los administradores pueden aplicar la seguridad adaptable en función del contexto, como los usuarios, la ubicación, el dispositivo y el riesgo. Los administradores deben migrar los controles de seguridad y las directivas de acceso de las aplicaciones existentes al nuevo marco de directivas de acceso. Para obtener más información, consulte Migración de controles de seguridad de aplicaciones y directivas de acceso.

  [ACS-1850]

01 de junio de 2022

- **Servicio de autenticación adaptable**

  La autenticación adaptable ahora está disponible de forma general (GA). Para obtener información detallada sobre la autenticación adaptable, consulte Servicio de autenticación adaptable.

  [CGS-6510]

04 de abril de 2022

- **Cambios de cambio de marca**

  El servicio Citrix Secure Workspace Access ahora pasa a llamarse servicio Citrix Secure Private Access.

  [ACS-2322]

- **Flujo de trabajo guiado por el administrador para facilitar la incorporación y la configuración**

Secure Private Access ahora tiene una nueva experiencia de administración optimizada con un proceso paso a paso para configurar el acceso de red Zero Trust a aplicaciones SaaS, aplicaciones web internas y aplicaciones TCP. Incluye la configuración de Autenticación adaptable, aplicaciones que incluyen la suscripción de usuarios, directivas de acceso adaptables y otros en una sola consola de administración. Para obtener más información, consulte Flujo de trabajo guiado por el administrador para facilitar la incorporación y la configuración.

Esta función ahora está disponible de forma general (GA).

[ACS-1102]

- **Panel de Secure Private Access**

  El panel de Secure Private Access proporciona a los administradores una visibilidad completa de sus aplicaciones principales, los usuarios principales, el estado de los conectores, el uso del ancho de banda y un solo lugar para el consumo. Estos datos se obtienen de Citrix Analytics. Para obtener más información, consulte el panel de Secure Private Access.

  Esta función ahora está disponible de forma general (GA).

  [ACS-1169]

- **Acceso directo a aplicaciones web empresariales**

  Los clientes ahora pueden habilitar el acceso de red Zero Trust (ZTNA) a las aplicaciones web internas, directamente desde exploradores web nativos como Chrome, Firefox, Safari y Microsoft Edge. Para obtener más información, consulte Acceso directo a aplicaciones web empresariales.

  Esta función ahora está disponible de forma general (GA).

- **Acceso basado en agentes de ZTNA a aplicaciones TCP/HTTPS**

  Los clientes de Citrix ahora pueden habilitar el acceso a la red Zero Trust (ZTNA) para todas las aplicaciones cliente-servidor y los recursos basados en IP/puertos, además de las aplicaciones web internas. Para obtener más información, consulte Compatibilidad con aplicaciones cliente-servidor.

  Esta función ahora está disponible de forma general (GA).

  [ACS-970]

- **Controles de acceso y seguridad adaptables para aplicaciones web, TCP y SaaS empresariales**

  La función de acceso adaptable al servicio Citrix Secure Private Access ofrece un enfoque integral de Zero Trust Network Access (ZTNA) que ofrece acceso seguro a las aplicaciones. El acceso adaptable permite a los administradores proporcionar un acceso de nivel granular a las aplicaciones a las que los usuarios pueden acceder en función del contexto. El término “contexto” aquí se refiere a:

  - Usuarios y grupos (usuarios y grupos de usuarios)
  - Dispositivos (dispositivos de escritorio o móviles)
  - Ubicación (ubicación geográfica o ubicación de red)
  - Postura del dispositivo (comprobación de postura del dispositivo)
  - Riesgo (puntuación de riesgo del usuario)

  Para obtener más información, consulte Controles de acceso y seguridad adaptables para aplicaciones web, TCP y SaaS empresariales.

  Esta función ahora está disponible de forma general (GA).

  [ACS-878, ACS-879, ACS-882]

- **Registros de auditoría para Secure Private Access**

  Los eventos relacionados con el servicio Citrix Secure Private Access ahora se capturan en **Citrix Cloud > Registro del sistema.** Para obtener más información, consulte Registros de auditoría.

  Esta función ahora está disponible de forma general (GA).

  [ACS-876]

- **Registros de diagnóstico para el acceso a aplicaciones web y SaaS empresariales**

  Los eventos de Citrix Secure Private Access ahora están integrados con Citrix Analytics. Citrix Analytics proporciona un punto final público que permite a los administradores acceder a los eventos y descargarlos. Se puede acceder a estos eventos mediante un script de PowerShell. Para obtener más información, consulte Registros de diagnóstico para el acceso a aplicaciones web y SaaS empresariales.

  Esta función ahora está disponible de forma general (GA).

  [ACS-805]

- **Servicio de autenticación adaptable**

  Los clientes de Citrix Cloud ahora pueden usar Citrix Workspace para proporcionar autenticación adaptable a Citrix Virtual Apps and Desktops. La autenticación adaptable es un servicio de Citrix Cloud que permite la autenticación avanzada para clientes y usuarios que inician sesión en Citrix Workspace. El servicio de autenticación adaptable es un ADC administrado por Citrix y alojado en Citrix Cloud. Para obtener más información, consulte Servicio de autenticación adaptable.

  Esta función se encuentra en Tech Preview.

  [CGS-6510]

16 de febrero de 2022

- **Compatibilidad con aplicaciones cliente-servidor** Con la compatibilidad con aplicaciones cliente-servidor en Citrix Secure Private Access, ahora puede eliminar la dependencia de una solución VPN tradicional para proporcionar acceso a todas las aplicaciones privadas a los usuarios remotos.

  Para obtener más información, consulte Compatibilidad con aplicaciones cliente-servidor: Vista previa

  [ACS-870]

11 de octubre de 2021

- **Fusión del mosaico de Citrix Gateway Service en una única instancia de Secure Private Access en Citrix Cloud**

  El mosaico de Citrix Gateway Service ahora se ha fusionado en un único Secure Private Access en Citrix Cloud.

  - Todos los clientes de Secure Private Access, incluidos Citrix Workspace Essentials y Citrix Workspace Standard, ahora pueden usar un solo mosaico de Secure Private Access para configurar aplicaciones web SaaS y empresariales, controles de seguridad mejorados, directivas contextuales, además de directivas de filtrado web.
  - Todos los clientes de Citrix DaaS pueden seguir habilitando Citrix Gateway Service como proxy HDX desde Configuración de Workspace. Sin embargo, se elimina el acceso directo para habilitar Citrix Gateway Service desde el mosaico del servicio de puerta de enlace. Puede habilitar Citrix Gateway Service desde **Configuración del espacio de trabajo > Acceso > Conectividad externa**. Para obtener más información, consulte Conectividad externa. Al mismo tiempo, no hay cambios en la funcionalidad.

  [NGSWS-16761]

30 de julio de 2021

- **Controles de seguridad y acceso contextual para las aplicaciones web empresariales y SaaS en función de la ubicación geográfica del usuario**

  El servicio Citrix Secure Private Access ahora admite el acceso contextual a las aplicaciones web y SaaS empresariales según la ubicación geográfica del usuario.

  [ACS-833]

- **Opción para ocultar una aplicación web o SaaS específica del portal Citrix Workspace**

  Los administradores ahora pueden ocultar una aplicación web o SaaS específica del portal Citrix Workspace. Cuando una aplicación está oculta en el portal de Citrix Workspace, Citrix Gateway Service no devuelve esta aplicación durante la enumeración. Sin embargo, los usuarios pueden seguir accediendo a la aplicación oculta.

  [ACS-944]

09 de junio de 2021

- **Tabla de redirección para definir las reglas para redirigir el tráfico de la aplicación**

  Los administradores ahora pueden usar la tabla de redirección para definir las reglas para redirigir el tráfico de la aplicación directamente a Internet o a través del conector de Citrix Gateway. Los administradores pueden definir el tipo de ruta para las aplicaciones como Externa, Interna, Proxy de derivación interna o Externa a través del conector de Gateway, en función de cómo deseen definir el flujo de tráfico.

  [ACS-243]

22 de mayo de 2021

- **Acceso contextual a aplicaciones web empresariales y SaaS**

  La función de acceso contextual del servicio Citrix Secure Private Access ofrece un enfoque integral de acceso de confianza cero que ofrece acceso seguro a las aplicaciones. El acceso contextual permite a los administradores proporcionar acceso de nivel granular a las aplicaciones a las que los usuarios pueden acceder en función del contexto. El término “contexto”se refiere a los usuarios, grupos de usuarios y a la plataforma (dispositivo móvil o equipo de escritorio) desde la que el usuario accede a la aplicación.

  [ACS-222]

- **Cambio de marca de la interfaz de usuario de un conector de Citrix Gateway**

  La interfaz de usuario de Citrix Cloud Gateway Connector se renombró de acuerdo con las directrices de marca de Citrix.

  [NGSWS-17100]

01 de mayo de 2021

- **Eliminación de datos de clientes del almacén de datos del servicio Citrix Secure Private Access**

Los datos de los clientes, incluidas las copias de seguridad, se eliminan del almacén de datos del servicio Citrix Secure Private Access después de 90 días de que caduquen los derechos de servicio.

[ACS-388]

- **Pasos simplificados para federar un dominio de Azure AD a Citrix Workspace**

  Los pasos para federar un dominio de Azure AD a la aplicación Citrix Workspace ahora se han simplificado para una incorporación más rápida en Citrix Workspace. La federación de dominios ahora se puede realizar en la interfaz de usuario de Citrix Gateway Service, desde la página Single Sign-On.

  [ACS-351]

- **Mejora de la herramienta de prueba de conectividad**

  La herramienta de prueba de conectividad del conector de Citrix Gateway se ha mejorado para controlar los errores de tiempo de espera y generar los registros necesarios.

  [NGSWS-17212]

15 de marzo de 2021

- **Mejoras de plataforma**

  Se han realizado varias mejoras de la plataforma para aumentar la fiabilidad de la propagación de las configuraciones de administración del cliente a conectores de Citrix Gateway.

  [ACS-85]

- **Rendimiento mejorado de las aplicaciones web**

  Se ha mejorado el rendimiento de las aplicaciones web cuando se accede a las aplicaciones web desde el explorador del sistema mediante una VPN sin cliente.

  [NGSWS-16469]

- **Habilitación del conector de Citrix Gateway para utilizar conjuntos de cifrado TLS1.2 de grado A o superior**

  El conector de Citrix Gateway ahora utiliza TLS1.2 con conjuntos de cifrado de grado A o superior para conectarse a Citrix Cloud Service y a otros servidores back-end.

  [NGSWS-16068]

11 de noviembre de 2020

- **Cambio de nombre del servicio Citrix Access Control**

El servicio de control de acceso ahora se llama Secure Private Access.

[NGSWS-14934]

15 de octubre de 2020

- **Opción de seguridad mejorada para lanzar aplicaciones web empresariales y de SaaS dentro del servicio Remote Browser Isolation**

  Los administradores ahora pueden usar la opción de seguridad mejorada, **seleccione Iniciar la aplicación siempre en el servicio Citrix Remote Browser Isolation para lanzar siempre una aplicación en el servicio** Remote Browser Isolation, independientemente de otras configuraciones de seguridad mejoradas.

  [ACS-123]

08 de octubre de 2020

- **Configurar tiempos de espera de sesión para la extensión del explorador Citrix Secure Private Access**

  Los administradores ahora pueden configurar los tiempos de espera de sesión para la extensión del explorador Citrix Secure Private Access. Los administradores pueden configurar esta opción en la ficha **Administrar** de la interfaz de usuario de Citrix Gateway Service.

  [NGSWS-13754]

- **Control RBAC en la configuración de administración de la extensión del explorador Citrix Secure Private Access**

  El control RBAC ahora se aplica en la configuración de administración de la extensión del explorador Citrix Secure Private Access.

  [NGSWS-14427]

24 de septiembre de 2020

- **Habilitar el acceso sin VPN a aplicaciones web empresariales a través de un explorador local**

  Ahora puede usar la extensión de explorador **Citrix Secure Private Access** para permitir el acceso sin VPN a las aplicaciones web empresariales a través de un explorador local. La extensión para exploradores **Citrix Secure Private Access** es compatible con los exploradores Google Chrome y Microsoft Edge.

  [ACS-286]

07 de julio de 2020

- **Validar la configuración de Kerberos en el conector de Citrix Gateway**

  Ahora puede utilizar el botón **Probar** de la sección **Single Sign-On** para validar la configuración de Kerberos.

  [NGSWS-8581]

19 de junio de 2020

- **Acceso de solo lectura para los administradores de Citrix Gateway Service y Citrix Secure Private Access Service**

  Los equipos de administradores de seguridad que utilizan Citrix Gateway Service ahora pueden proporcionar controles granulares, como el acceso de solo lectura a los administradores de Citrix Gateway Service y Citrix Secure Private Access Service.

  - Los administradores con acceso de solo lectura a Citrix Gateway Service tienen acceso para ver únicamente los detalles de la aplicación.
  - Los administradores con acceso de solo lectura a Citrix Secure Private Access Service solo pueden ver la configuración de acceso al contenido.

  [ACS-205]

08 de mayo de 2020

- **Nuevas herramientas de solución de problemas del conector de Citrix Gateway 13.0**

  - **Seguimiento de red:** Ahora puede utilizar la función **Trace** para solucionar problemas de registro del conector de Citrix Gateway. Puede descargar los archivos de seguimiento y compartirlos con los administradores para solucionar problemas. Para obtener más información, consulte Solucionar problemas de registro del conector de Citrix Gateway.

    [NGSWS-10799]

  - **Pruebas de conectividad:** ahora puede utilizar la función **Prueba de conectividad** para confirmar que no hay errores en la configuración del conector de Gateway y que el conector de Gateway puede conectarse a las direcciones URL. Para obtener más información, consulte Iniciar sesión y configurar el conector de Citrix Gateway.

    [NGSWS-8580]

V2019.04.02

- **Soporte de autenticación Kerberos para Citrix Gateway Connector a proxy saliente** [NGSWS-6410]

  Ahora se admite la autenticación Kerberos para el tráfico desde el conector de Citrix Gateway al proxy saliente. El conector de Gateway utiliza las credenciales de proxy configuradas para autenticarse en el proxy saliente.

V2019.04.01

- **El tráfico de aplicaciones web/SaaS ahora se puede redirigir a través de un conector de Gateway alojado en red corporativa, evitando así la autenticación de dos factores.** Si un cliente ha publicado una aplicación SaaS alojada fuera de la red corporativa, ahora se agrega soporte para autenticar el tráfico para que esa aplicación pase por un conector de Gateway.

  Por ejemplo, considera que un cliente tiene una aplicación SaaS protegida por Okta (como Workday). Es posible que el cliente quiera que, aunque el tráfico de datos de Workday real no se redirija a través de Citrix Gateway Service, el tráfico de autenticación al servidor Okta se redirija a través de Citrix Gateway Service a través de un conector de Gateway. Esto ayuda al cliente a evitar una autenticación de segundo factor desde el servidor Okta, ya que el usuario se conecta al servidor Okta desde la red corporativa.

  [NGSWS-6445]

- **Desactivación de filtros de listas de sitios web y categorización de sitios web**. El filtrado de listas de sitios web y la categorización de sitios web se pueden desactivar si el administrador decide no aplicar estas funcionalidades a un cliente específico.

  [NGSWS-6532]

- **Enrutamiento geográfico automático para redireccionamientos del servicio Remote Browser Isolation.** El enrutamiento geográfico automático ahora está habilitado para los redireccionamientos del servicio de aislamiento remoto del navegador.

  [NGSWS-6926]

V2019.03.01

- **El botón "Detectar"se agrega en la página "Agregar un conector de Gateway".** El botón **Detectar** se utiliza para actualizar la lista de conectores, lo que permite que el conector recién agregado se refleje en la sección Conectividad de la aplicación web.

  [CGOP-6358]

- **Se agrega una nueva categoría "Malicioso y peligroso"en las categorías "Filtrado web de Access Control".** Se agrega una nueva categoría denominada **Malicioso y peligroso** en las categorías **Filtrado web de Access Control** bajo el grupo **Malware y Spam**.

  [CGOP-6205]

Funciones retiradas

February 16, 2024

Este artículo le proporciona un aviso anticipado de las funciones del servicio Secure Private Access que se están eliminando gradualmente, para que pueda tomar decisiones comerciales oportunas. Citrix supervisa el uso que hacen los clientes de las funciones que se retirarán y los comentarios que tengan cuando estas se retiran definitivamente. Estos anuncios están sujetos a cambios en las versiones posteriores y es posible que no contengan todas las funciones o funciones retiradas. Para obtener más información sobre la asistencia durante el ciclo de vida de los productos, consulte la Directiva

En la siguiente tabla se enumeran las funciones del servicio Secure Private Access que están en desuso o que se planea dejar de usar.

Elemento	Retirada anunciada en	Fecha en desuso	Alternativa
Método de acceso VPN sin cliente para el acceso a aplicaciones web	Enero de 2023	17 de octubre de 2023	Utilice Citrix Enterprise Browser o Direct Access según su caso de uso. Para obtener más información, consulte Acerca de la retirada del acceso a VPN sin cliente para el acceso a aplicaciones web.

Elemento	Retirada anunciada en	Fecha en desuso	Alternativa
Filtrado web basado en categorías	Diciembre de 2022	31 de diciembre de 2022	Se conservará la función de permitir, denegar o redireccionar mediante RBI por sitio web de Secure Private Access para proporcionar acceso selectivo a sitios web no relacionados con el trabajo desde Citrix Enterprise Browser.
Restricción del control de seguridad	Abril de 2022	15 junio 2022	NA
Connector de Citrix Gateway	Mayo de 2022	30 septiembre 2022	Dispositivo conector. Para migrar Gateway Connector Appliance a Connector Appliance, consulte Migrar Gateway Connector Appliance

Acerca de la retirada del acceso a VPN sin cliente para el acceso a aplicaciones web

- ¿Qué es el método de acceso Clientless VPN (Clientless VPN)?

  Citrix Secure Private Access utiliza el método de acceso basado en CVPN cuando se accede a una aplicación web interna, configurada sin restricciones de seguridad mejoradas, a través de Workspace for Web (aplicación Citrix Workspace para HTML5).

  > **Nota:**
  >
  > El método de acceso VPN sin cliente solo se usa cuando se accede a una aplicación interna a través de Workspace for Web (aplicación Citrix Workspace para HTML5). Solo se bloquean las aplicaciones sin restricciones de seguridad mejoradas configuradas.

- ¿Por qué estamos desaprobando esta función?

  El método de VPN sin cliente utiliza reescrituras de URL del lado del cliente, lo que tiene ciertas limitaciones tecnológicas en toda la industria. En varios casos, puede provocar errores de

acceso a las aplicaciones cuando se reescriben ciertos enlaces de las aplicaciones web. Esto lleva a una mala experiencia para el usuario final. Para brindar la mejor experiencia de acceso a las aplicaciones a nuestros clientes, estamos desaprobando esta función y recomendamos cambiar a una de las alternativas que se mencionan a continuación.

- ¿Cómo afectará a los usuarios finales que accedan a las aplicaciones configuradas de Secure Private Access?

  Si se accede a una aplicación web configurada sin restricciones de seguridad mejoradas a través de Workspace para Web, se bloqueará el acceso a esa aplicación.
  No afectará al acceso de los usuarios finales a las aplicaciones a través de Workspace Application, Direct Access, Remote Browser Isolation Service (RBI) o Secure Access Agent.

- ¿Cuáles son las alternativas y qué deben hacer los administradores?

  Navegador empresarial Citrix: utilice la aplicación Citrix Workspace para acceder a estas aplicaciones a través del explorador web empresarial Citrix. Este método proporciona la mejor experiencia para el usuario final con una configuración de seguridad mejorada (como la restricción de descargas, las restricciones de impresión, las marcas de agua, la restricción del acceso al portapapeles) y la administración del explorador web. Secure Private Access para Citrix Workspace.
  Acceso directo: si quieres un método sin cliente para acceder a las aplicaciones web, utiliza el método de acceso directo mediante el cual se puede acceder a las aplicaciones directamente desde cualquier explorador web nativo, como Chrome. Este método se puede utilizar para casos de uso en los que la aplicación Citrix Workspace no se puede instalar en el dispositivo final o para dispositivos no administrados. Para obtener más información, consulte Acceso directo a aplicaciones web empresariales.

- ¿Afecta a las aplicaciones existentes a las que se accede mediante la aplicación Citrix Workspace o el agente Secure Access?

  No, solo bloqueamos el acceso a las aplicaciones web a las que se accede a través de Workspace for Web. Esta obsolescencia no afectará a ninguna aplicación a la que se acceda mediante la aplicación Citrix Workspace o los clientes de Secure Access que estén instalados en los dispositivos finales. Si se accede a una aplicación web, que está configurada con restricciones de seguridad mejoradas, a través de Workspace for Web o la variante HTML5 de la aplicación Citrix Workspace, se bloqueará el acceso a esas aplicaciones.

- ¿Tiene más preguntas?

  Contacto con Citrix Support.

Introducción a Citrix Secure Private Access

December 27, 2023

En este documento se explica cómo empezar a incorporar y configurar la entrega de aplicaciones SaaS por primera vez. Este documento está destinado a los administradores de aplicaciones.

Requisitos del sistema

Compatibilidad con sistemas operativos: la aplicación Citrix Workspace es compatible con Windows 7, 8, 10 y Mac 10.11 y versiones posteriores.

Compatibilidad con exploradores: acceda a los espacios de trabajo con las versiones más recientes de Edge, Chrome, Firefox o Safari.

Compatibilidad con Citrix Workspace: acceda a espacios de trabajo con Citrix Workspace para cualquiera de las plataformas de escritorio (Windows, Mac).

Funcionamiento

Citrix Secure Private Access ayuda a los administradores de TI y seguridad a gobernar el acceso autorizado de los usuarios finales a las aplicaciones web alojadas en empresas y SaaS sancionadas. Las identidades y atributos de usuario se utilizan para determinar los privilegios de acceso y las directivas de control de acceso determinan los privilegios necesarios para realizar operaciones. Una vez que un usuario se autentica, el control de acceso autoriza el nivel de acceso adecuado y las acciones permitidas asociadas con las credenciales de ese usuario.

Citrix Secure Private Access combina elementos de varios servicios de Citrix Cloud para ofrecer una experiencia integrada para los usuarios finales y los administradores.

Funcionalidad	Servicio/componente que proporciona la funcionalidad
Interfaz de usuario coherente para acceder a las aplicaciones	Aplicación Workspace Experience/Workspace
SSO a aplicaciones SaaS y web	Citrix Gateway Service Standard
Filtrado y categorización web	Servicio de filtrado web
Directivas de seguridad mejoradas para SaaS	Control de aplicaciones de nube
Navegación segura	Remote Browser Isolation Service

Funcionalidad	Servicio/componente que proporciona la funcionalidad
Visibilidad del acceso al sitio web y comportamientos de riesgo	Citrix Analytics

Comience con el servicio Citrix Secure Private Access

1. Inscríbase en Citrix Cloud.
2. Solicitud de derecho al servicio Secure Private Access.
3. Después de la autorización, el servicio Secure Private Access se proporciona en **Mis servicios**.
4. Acceda a la interfaz de usuario del servicio Secure Private Access.

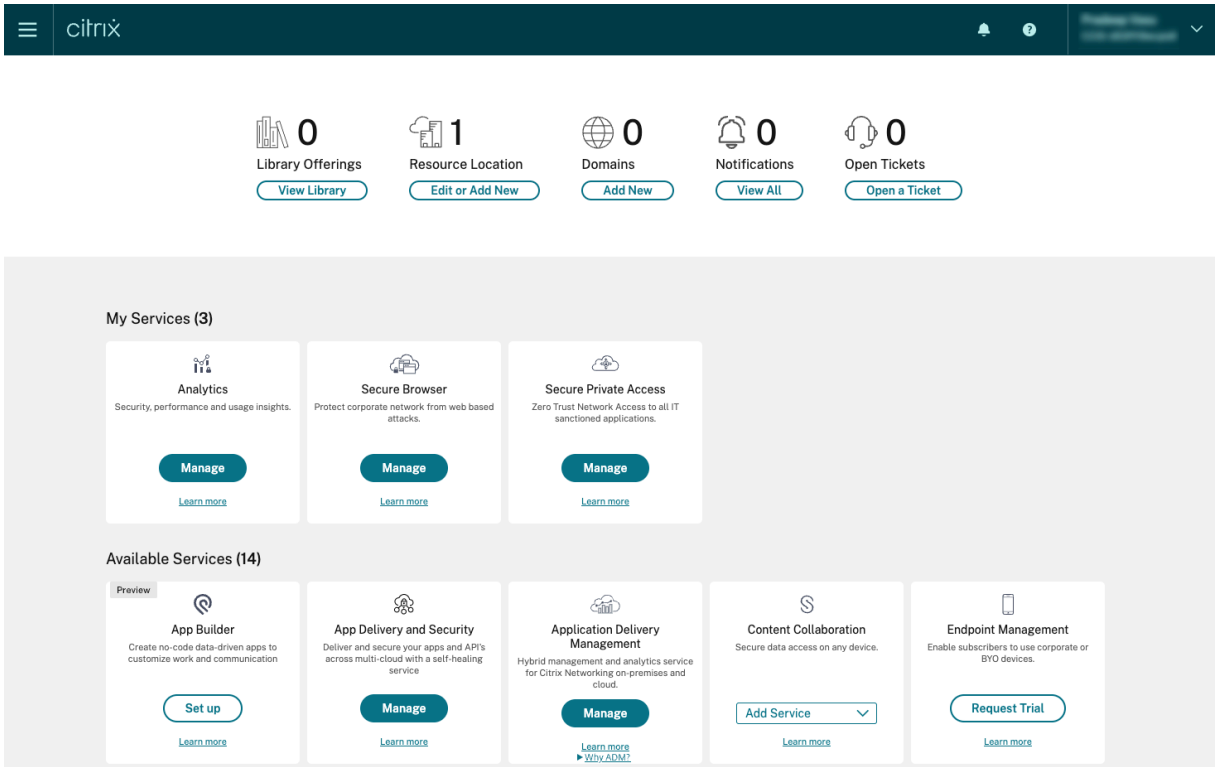
Paso 1: **Registrarse en Citrix Cloud**

Para empezar a usar el servicio Secure Private Access, primero debe crear una cuenta de Citrix Cloud o unirse a una existente creada por otra persona de la empresa. Para obtener instrucciones y procesos detallados sobre cómo proceder, consulte Registrarse en Citrix Cloud .

Paso 2: **Solicitud del derecho al servicio Secure Private Access**

Para solicitar el derecho al servicio Secure Private Access, en la pantalla de **Citrix Cloud**, en la sección **Servicios disponibles**, haga clic en la ficha **Solicitar prueba** presente en el mosaico del servicio Secure Private Access.

Para obtener más información sobre la licencia, consulte https://www.citrix.com/buy/licensing/product.html.



Paso 3: **Autorización posterior, el servicio Secure Private Access se aprovisiona en Mis servicios**

Después de recibir el derecho al servicio Secure Private Access, el mosaico del servicio Secure Private Access se mueve a la sección **Mis servicios**.

Paso 4: **acceder a la interfaz de usuario del servicio Secure Private Access**

Haga clic en la ficha **Administrar** del mosaico para acceder a la interfaz de usuario del servicio Secure Private Access.

Nota:

- Para que los usuarios finales puedan usar el espacio de trabajo y acceder a las aplicaciones, deben descargar y usar la aplicación Citrix Workspace o usar la URL del espacio de trabajo. Debe tener algunas aplicaciones SaaS publicadas en su espacio de trabajo para probar la solución Citrix Secure Private Access. La aplicación Workspace se puede descargar desde https://www.citrix.com/downloads. En la lista **Buscar descargas**, seleccione la **aplicación Citrix Workspace**.
- Si tiene configurado un firewall de salida, asegúrese de que se permita el acceso a los siguientes dominios.

  > – *.cloud.com
  > – *.nssvc.net
  > – *.netscalergateway.net

Dispone de más información en Configurar el proxy y el firewall de Cloud Connector y Requisitos de conectividad con Internet.

- Solo puede agregar una cuenta de Workspace.

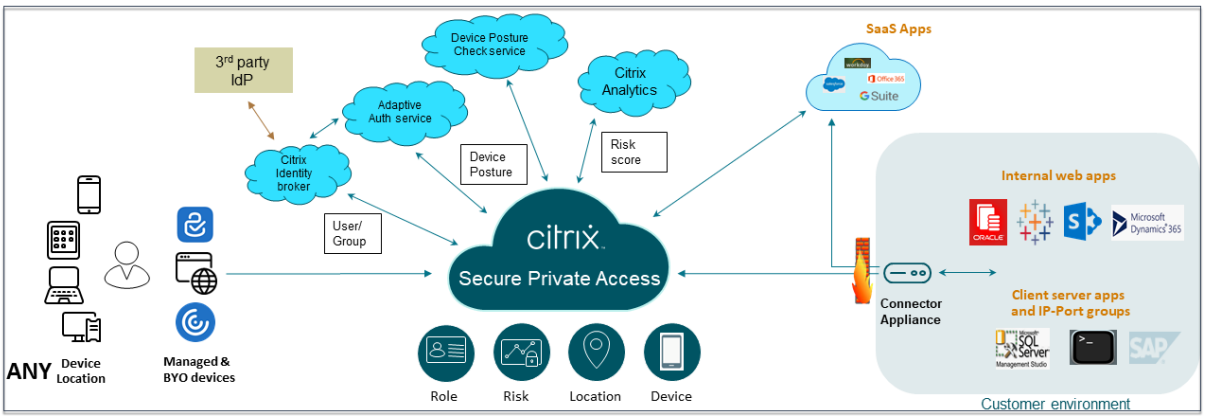
Descripción general de la solución del servicio Secure Private Access

February 16, 2024

Resumen de la solución

Las soluciones VPN tradicionales requieren que los dispositivos de los usuarios finales se administren, proporcionen acceso a nivel de red y apliquen directivas de control de acceso estáticas. Citrix Secure Private Access ofrece al departamento de TI un conjunto de controles de seguridad para protegerse contra las amenazas de los dispositivos BYO, lo que brinda a los usuarios la opción de acceder a sus aplicaciones autorizadas por TI desde cualquier dispositivo, ya sea administrado o BYO.

Citrix Secure Private Access ofrece autenticación adaptativa, soporte de inicio de sesión único y controles de seguridad mejorados para las aplicaciones. Secure Private Access también brinda la capacidad de escanear el dispositivo del usuario final antes de establecer una sesión mediante el servicio Device Posture. En función de los resultados de la autenticación adaptativa o la postura del dispositivo, los administradores pueden definir los métodos de autenticación de las aplicaciones.



Seguridad adaptativa

La autenticación adaptativa determina el flujo de autenticación correcto para la solicitud actual. La autenticación adaptativa puede identificar la posición del dispositivo, la ubicación geográfica, el segmento de red y la organización del usuario o la pertenencia al departamento. Según la información

obtenida, un administrador puede definir cómo quiere autenticar a los usuarios en sus aplicaciones autorizadas por TI. Esto permite a las organizaciones implementar el mismo marco de directivas de autenticación en todos los recursos, incluidas las aplicaciones SaaS públicas, las aplicaciones web privadas, las aplicaciones cliente-servidor privadas y los escritorios como servicio (DaaS). Para obtener más información, consulte Adaptive Security.

Acceso a la aplicación

Secure Private Access puede crear una conexión a las aplicaciones web locales sin depender de una VPN. Esta conexión sin VPN utiliza un Connector Appliance implementado localmente. El Connector Appliance crea un canal de control de salida para la suscripción a Citrix Cloud de la organización. Desde allí, Secure Private Access puede canalizar las conexiones a las aplicaciones web internas sin necesidad de una VPN. Para obtener más información, consulte Acceso a la aplicación.

Single Sign-On

Con la autenticación adaptativa, las organizaciones pueden proporcionar directivas de autenticación sólidas para ayudar a reducir el riesgo de que las cuentas de usuario se vean comprometidas. Las capacidades de inicio de sesión único de Secure Private Access utilizan las mismas directivas de autenticación adaptativa para todas las aplicaciones SaaS, web privada y cliente-servidor. Para obtener más información, consulte Inicio de sesión único.

Seguridad del navegador

Secure Private Access permite a los usuarios finales navegar por Internet de forma segura con un explorador web empresarial seguro y administrado centralmente. Cuando un usuario final lanza una aplicación web privada o SaaS, se toman varias decisiones de forma dinámica para decidir cuál es la mejor manera de ofrecer el mejor servicio a esta aplicación. Para obtener más información, consulte Seguridad del navegador.

Postura del dispositivo

El servicio de postura del dispositivo permite al administrador definir directivas para comprobar la postura de los dispositivos de punto final que intentan acceder a los recursos corporativos de forma remota. Según el estado de cumplimiento de un punto final, el servicio de postura del dispositivo puede denegar el acceso o proporcionar acceso restringido o total a las aplicaciones y escritorios corporativos.

Cuando un usuario final inicia una conexión con Citrix Workspace, el cliente Device Posture recopila información sobre los parámetros del punto final y la comparte con el servicio Device Posture para determinar si la postura del punto final cumple con los requisitos de la directiva.

La integración del servicio Device Posture con Citrix Secure Private Access permite el acceso seguro a aplicaciones SaaS, web, TCP y UDP desde cualquier lugar, con la resiliencia y la escalabilidad de Citrix Cloud. Para obtener más información, consulte Postura del dispositivo.

Soporte para aplicaciones TCP y UDP

En ocasiones, los usuarios remotos necesitan acceder a aplicaciones cliente-servidor privadas que tienen su interfaz en el punto final y su servidor en un centro de datos. Las organizaciones pueden aplicar legítimamente directivas de seguridad estrictas en torno a estas aplicaciones internas y privadas, lo que dificulta que los usuarios remotos accedan a estas aplicaciones sin comprometer los protocolos de seguridad.

El servicio Secure Private Access aborda las vulnerabilidades de seguridad de TCP y UDP al permitir que ZTNA brinde un acceso seguro a estas aplicaciones. Los usuarios ahora pueden acceder a todas las aplicaciones privadas, incluidas las aplicaciones TCP, UDP y HTTPS, mediante un explorador nativo o una aplicación cliente nativa a través del cliente Citrix Secure Access que se ejecuta en sus máquinas.

Los usuarios deben instalar el cliente Citrix Secure Access en sus dispositivos cliente.

- Para Windows, la versión del cliente (22.3.1.5 y versiones 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 (22.02.3 y posteriores) se puede descargar de la App Store.

Para obtener más información, consulte Compatibilidad con aplicaciones cliente-servidor.

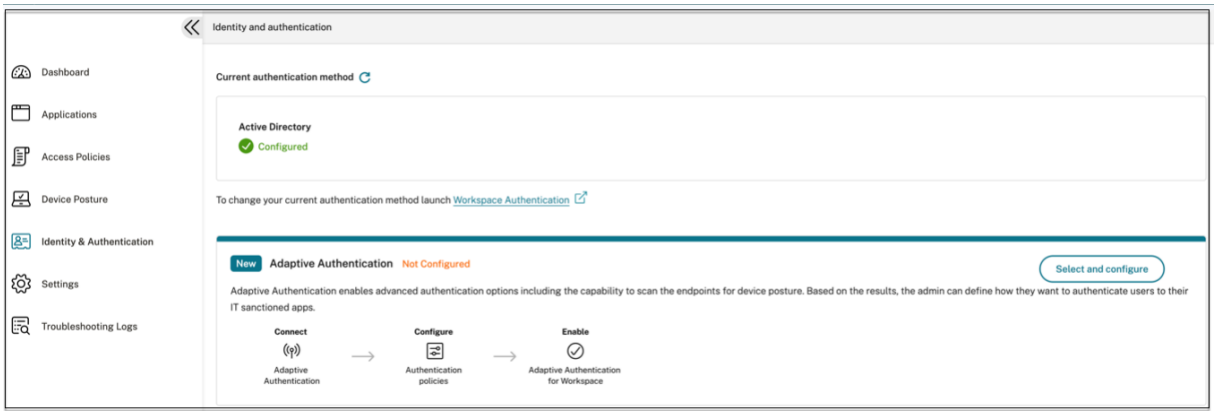
Configurar Citrix Secure Private Access

Habilite el acceso de red de confianza cero a las aplicaciones SaaS, las aplicaciones web internas y las aplicaciones TCP y UDP mediante la consola de administración de Secure Private Access. Esta consola incluye la configuración de la autenticación adaptativa, las aplicaciones que incluyen la suscripción de usuarios y las directivas de acceso adaptativo.

Configurar la identidad y la autenticación

Seleccione el método de autenticación para que los suscriptores inicien sesión en Citrix Workspace. La autenticación adaptable es un servicio de Citrix Cloud que permite la autenticación avanzada para

clientes y usuarios que inician sesión en Citrix Workspace.



Para obtener más información, consulte Configurar la identidad y la autenticación.

Enumerar y publicar aplicaciones

Después de seleccionar el método de autenticación, configure las aplicaciones web, SaaS o TCP y UDP mediante la consola de administración. Para obtener más información, consulte Agregar y administrar aplicaciones.

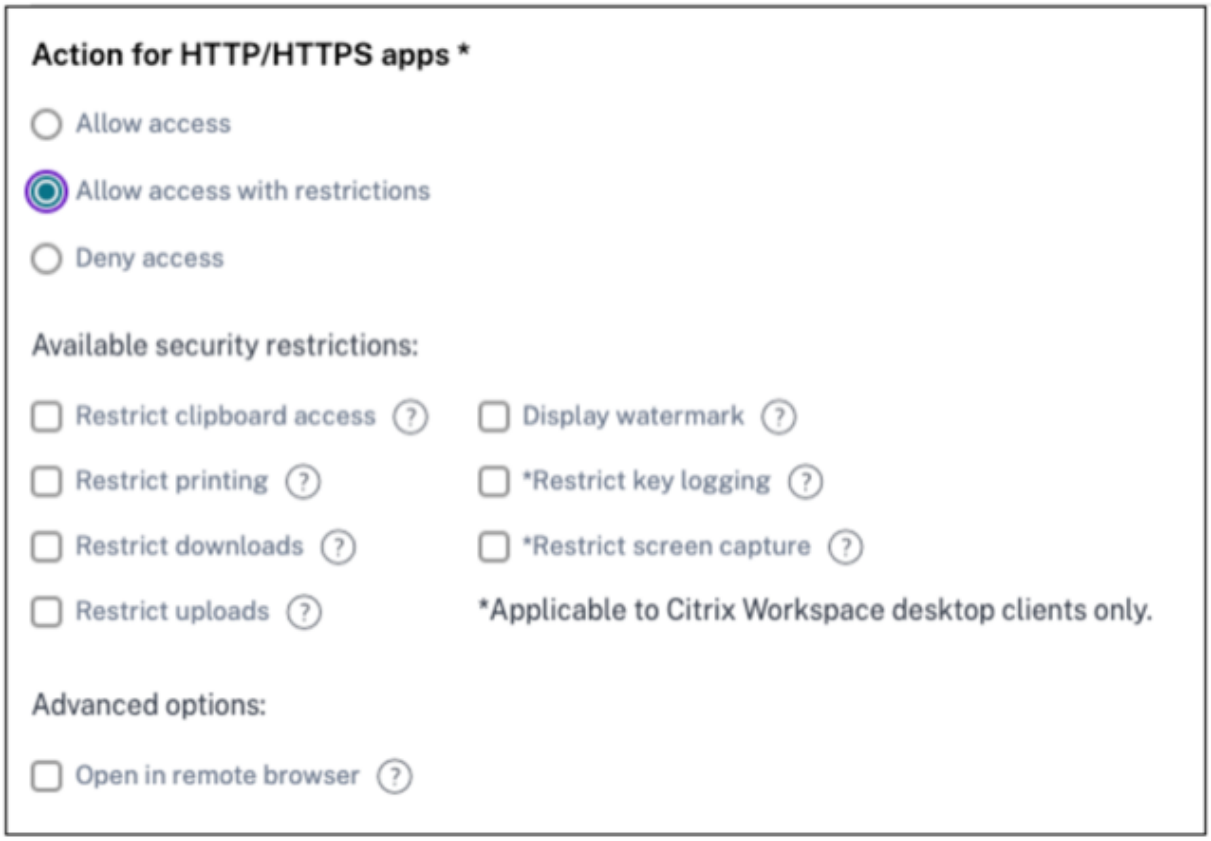
Habilite controles de seguridad mejorados

Para proteger el contenido, las organizaciones incorporan directivas de seguridad mejoradas en las aplicaciones SaaS. Cada directiva impone una restricción en Citrix Enterprise Browser cuando se usa la aplicación Workspace para escritorio o en Secure Browser cuando se usa la aplicación Workspace web o móvil.

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

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

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



Para obtener más información, consulte Configurar una directiva de acceso.

Habilite Citrix Enterprise Browser para el lanzamiento de aplicaciones

Secure Private Access permite a los usuarios finales lanzar sus aplicaciones mediante Citrix Enterprise Browser (CEB). CEB es un explorador basado en cromo integrado con la aplicación Citrix Workspace que permite una experiencia de acceso segura y sin problemas para acceder a aplicaciones web y SaaS desde Citrix Enterprise Browser.

CEB se puede configurar como navegador preferido o como su navegador de trabajo para todas las aplicaciones web o aplicaciones SaaS alojadas internamente con directivas de seguridad. CEB permite a los usuarios abrir todos los dominios de aplicaciones SaaS/web configurados dentro de un entorno seguro y controlado.

Habilitar Citrix Enterprise Browser Los administradores pueden usar el servicio de configuración global de aplicaciones (GACS) para configurar Citrix Enterprise Browser como el explorador predeterminado para lanzar aplicaciones web y SaaS desde la aplicación Citrix Workspace.

Configuración mediante API:

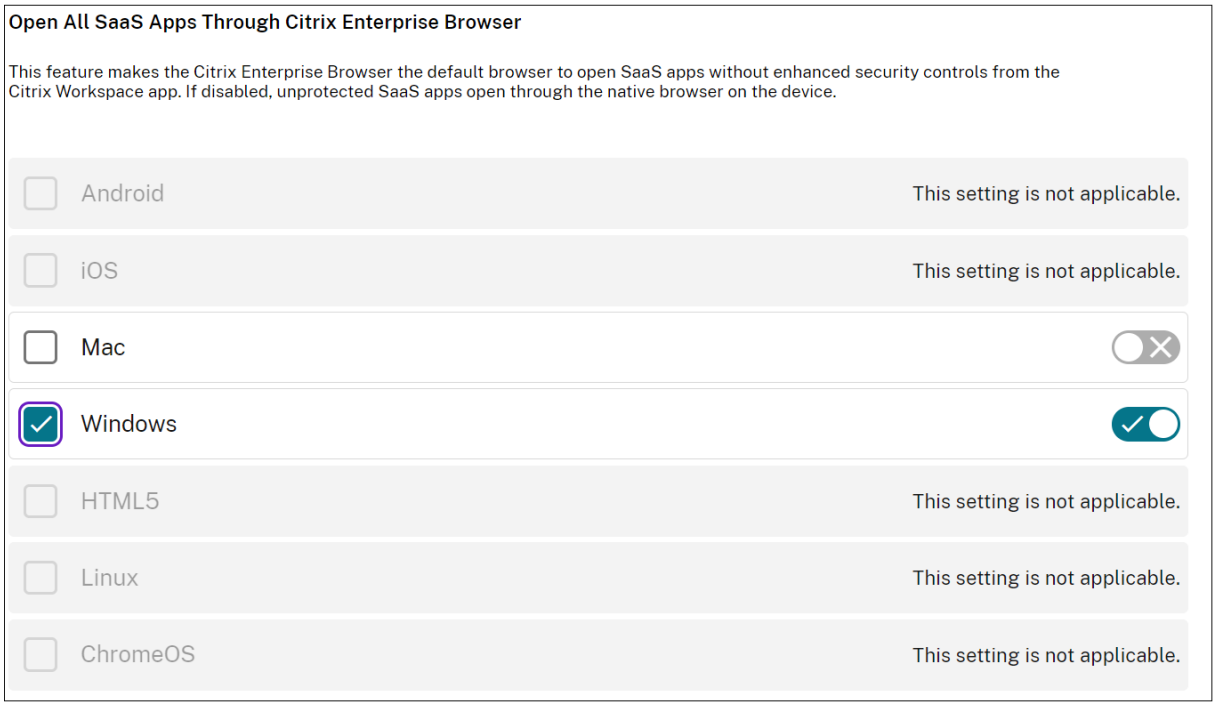
Para configurarlo, este es un archivo JSON de ejemplo para habilitar Citrix Enterprise Browser para todas las aplicaciones de forma predeterminada:

```
"settings": [
                    {

                       "name": "open all apps in ceb",
                       "value": "true"
                     }

                    ]
<!--NeedCopy-->
```

El valor predeterminado es true.

Configuración mediante GUI:

Seleccione los dispositivos para los que CEB debe convertirse en el navegador predeterminado para el lanzamiento de la aplicación.

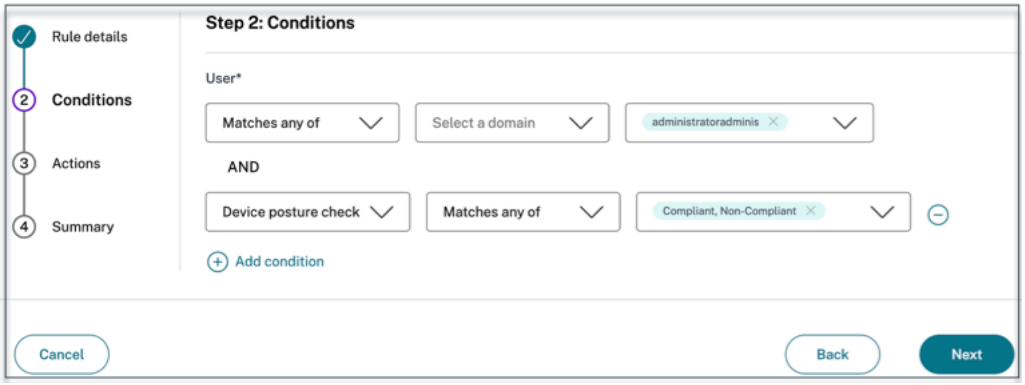


Para obtener más información, consulte Administrar Citrix Enterprise Browser a través de GACS.

Configurar etiquetas para el acceso contextual mediante Device Posture

Tras la verificación de la postura del dispositivo, el dispositivo puede iniciar sesión y se clasifica como compatible o no compatible. Esta clasificación está disponible como etiquetas para el servicio Secure Private Access y se utiliza para proporcionar acceso contextual en función de la posición del dispositivo.

1. Inicie sesión en Citrix Cloud.
2. En el mosaico Acceso privado seguro, haga clic en **Administrar** .
3. Haga clic en **Directivas de acceso** en el menú de navegación de la izquierda y, a continuación, en **Crear directiva**.
4. Introduzca el nombre de la directiva y la descripción de la misma.
5. En **Aplicaciones**, seleccione la aplicación o el conjunto de aplicaciones en las que se debe aplicar esta directiva.
6. Haga clic en **Crear regla** para crear reglas para la directiva.
7. Introduzca el nombre de la regla y una breve descripción de la regla y, a continuación, haga clic en **Siguiente**.
8. Selecciona las condiciones de los usuarios. La condición de usuario es una condición obligatoria que debe cumplirse para conceder acceso a las aplicaciones a los usuarios.
9. Haga clic en **+** para agregar la condición de postura del dispositivo.
10. Seleccione **Verificación de postura del dispositivo** y la expresión lógica en el menú desplegable.
11. Introduzca uno de los siguientes valores en las etiquetas personalizadas:



   - **Compatible**: para dispositivos compatibles
   - **No compatible**: para dispositivos que no cumplen con las normas

12. Haga clic en **Siguiente**.

13. Seleccione las acciones que se deben aplicar en función de la evaluación de la condición y, a continuación, haga clic en **Siguiente**.

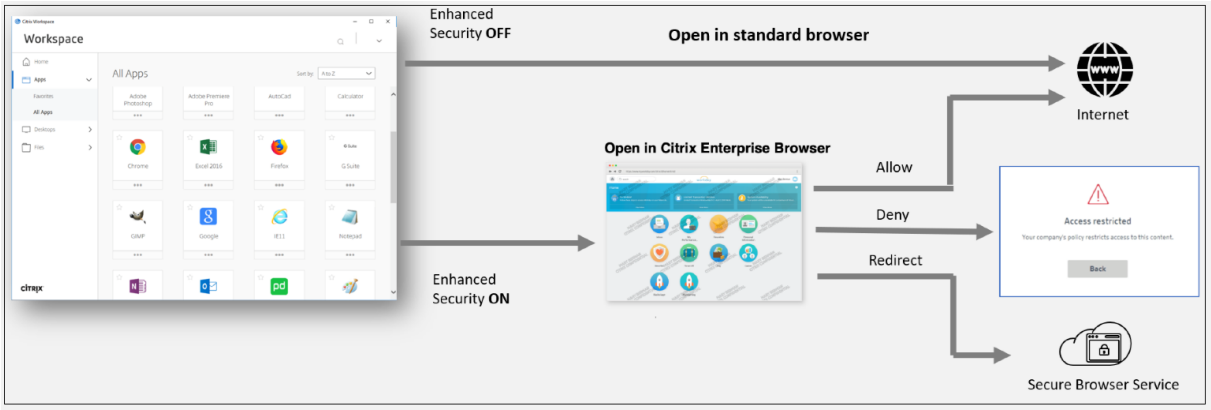
    La página de resumen muestra los detalles de la directiva.

14. Compruebe los detalles y haga clic en **Finalizar** .

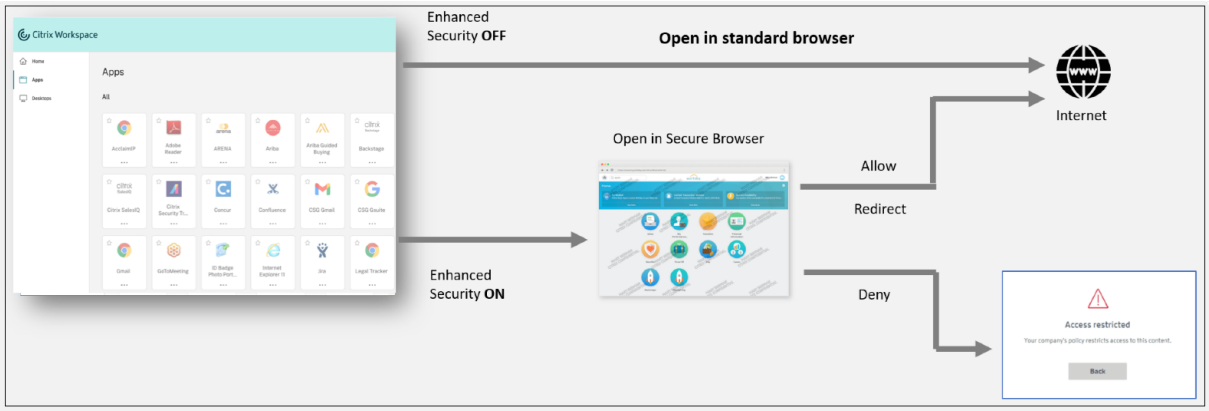
> **Nota:**
>
> Cualquier aplicación de Secure Private Access que no esté etiquetada como compatible o no conforme en la directiva de acceso se trata como la aplicación predeterminada y se puede acceder a ella en todos los terminales, independientemente de la postura del dispositivo.

Experiencia del usuario final

El administrador de Citrix tiene la facultad de ampliar el control de seguridad con la ayuda de Citrix Secure Private Access. La aplicación Citrix Workspace es un punto de entrada para acceder a todos los recursos de forma segura. Los usuarios finales pueden acceder a aplicaciones virtuales, escritorios, aplicaciones SaaS y archivos a través de la aplicación Citrix Workspace. Con Citrix Secure Private Access, los administradores pueden controlar la forma en que el usuario final accede a una aplicación SaaS a través de la interfaz de usuario web de Citrix Workspace Experience o del cliente nativo de la aplicación Citrix Workspace.



Cuando el usuario inicia la aplicación Workspace en el endpoint, ve sus aplicaciones, escritorios, archivos y aplicaciones SaaS. Si un usuario hace clic en la aplicación SaaS cuando la seguridad mejorada está inhabilitada, la aplicación se abre en un navegador estándar que se instala localmente. Si el administrador ha habilitado la seguridad mejorada, las aplicaciones SaaS se abren en el CEB dentro de la aplicación Workspace. La accesibilidad a los hipervínculos dentro de las aplicaciones SaaS y las aplicaciones web se controla en función de las directivas de sitios web no autorizados. Para obtener más información sobre los sitios web no autorizados, consulte Sitios web noautorizados.



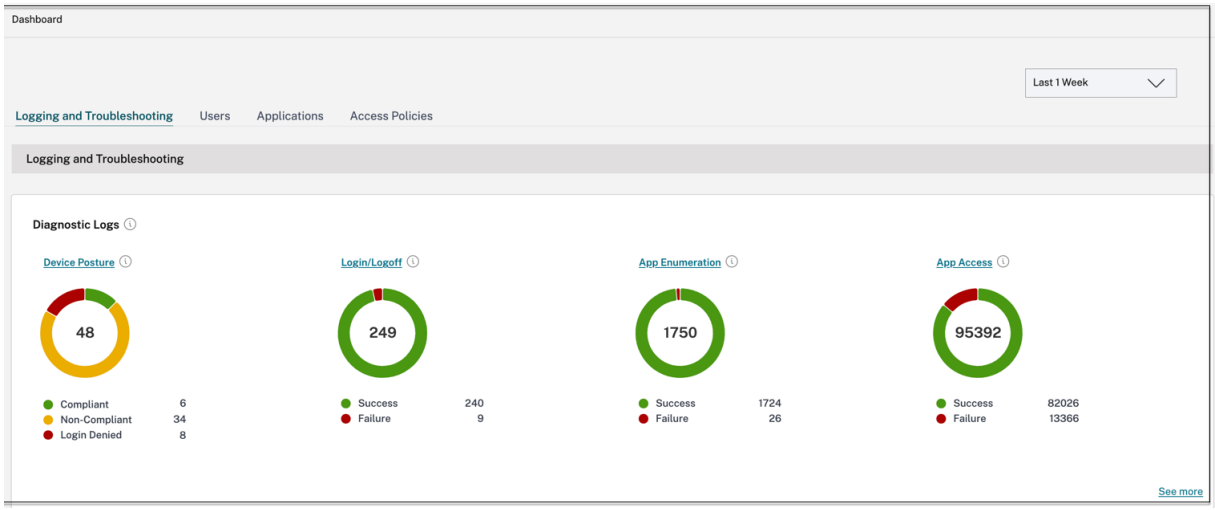
Del mismo modo, con el portal web de Workspace, cuando la seguridad mejorada está inhabilitada, las aplicaciones SaaS se abren en un navegador estándar que se instala de forma nativa. Cuando se habilita la seguridad mejorada, las aplicaciones SaaS se abren en el navegador remoto seguro. Los usuarios pueden acceder a los sitios web dentro de las aplicaciones SaaS en función de las directivas de sitios web no autorizados. Para obtener más información sobre los sitios web no autorizados, consulte Sitios web noautorizados.

Panel de análisis

El panel del servicio Secure Private Access muestra los datos de diagnóstico y uso de las aplicaciones SaaS, Web, TCP y UDP. El panel de control proporciona a los administradores una visibilidad completa de sus aplicaciones, usuarios, estado de los conectores y uso del ancho de banda en un solo lugar para su consumo. Estos datos se obtienen de Citrix Analytics. Las métricas se clasifican en líneas generales en las siguientes categorías.

- Registro y solución de problemas
- Usuarios
- Aplicaciones
- Directivas de acceso

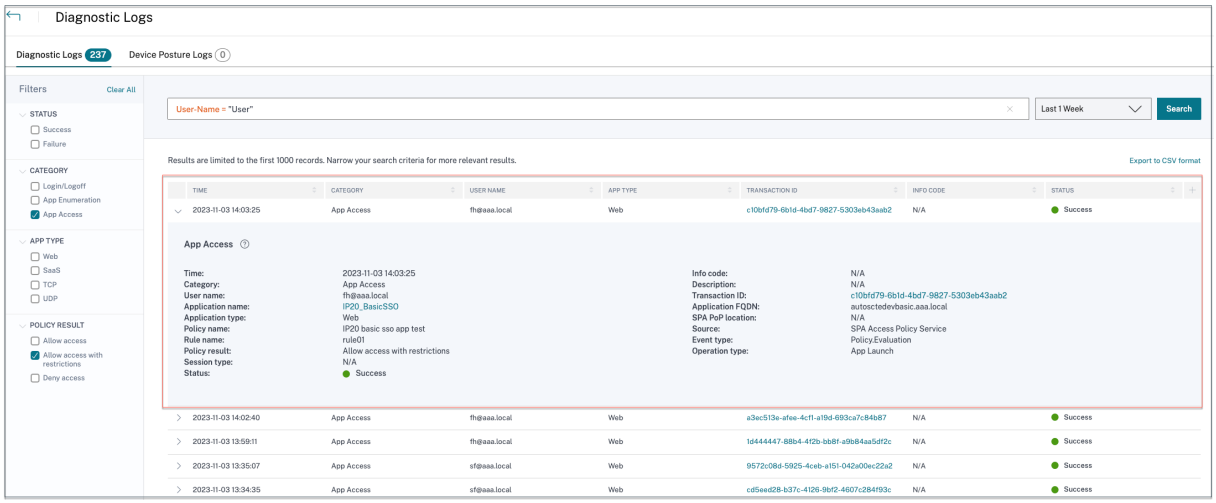
Para obtener más información, consulte Panel de mandos.



Solucionar problemas con las aplicaciones

El gráfico de registros de diagnóstico del panel de control de Secure Private Access proporciona visibilidad de los registros relacionados con la autenticación, el inicio de aplicaciones, la enumeración de aplicaciones y los registros de estado de los dispositivos.

- **Código de información**: algunos eventos de registro, como los errores, tienen un código de información asociado. Al hacer clic en el código de información, los usuarios se redirigen a los pasos de resolución o a más información sobre ese evento.
- **ID de transacción**: los registros de diagnóstico también muestran un ID de transacción que correlaciona todos los registros de Secure Private Access de una solicitud de acceso. Una solicitud de acceso a una aplicación puede generar varios registros, empezando por la autenticación, luego por la enumeración de aplicaciones dentro de la aplicación del espacio de trabajo y, por último, por el acceso a la aplicación en sí. Todos estos eventos generan sus propios registros. El ID de transacción se utiliza para correlacionar todos estos registros. Puede filtrar los registros de diagnóstico mediante el ID de transacción para encontrar todos los registros relacionados con una solicitud de acceso a una aplicación concreta.
  Para obtener más información, consulte Solucionar problemas de Secure Private Access.



Ejemplos de casos de uso

- Acceda a las aplicaciones internas (Web/TCP/UDP) mediante un enfoque de confianza cero sin abrir el tráfico entrante en el firewall
- Adopte un enfoque de confianza cero descubriendo las aplicaciones a las que acceden los usuarios
- Restringir el acceso a las aplicaciones SaaS a Citrix Enterprise Browser
- Restrinja el acceso a las aplicaciones SaaS a las direcciones IP públicas de propiedad de la empresa
- Seguridad mejorada para las aplicaciones SaaS administradas por Azure
- Seguridad mejorada para Office 365
- Seguridad mejorada para las aplicaciones de Okta

Artículos de referencia

- Introducción a Secure Private Access
- Resumen técnico
- Arquitectura de referencia
- Citrix Enterprise Browser
- Administre Citrix Enterprise Browser a través de GACS
- Flujo de trabajo guiado por el administrador para una incorporación y una configuración fáciles

Vídeos de referencia

- Acceso de red de confianza cero (ZTNA) a las aplicaciones
- Acceso privado a aplicaciones web con Citrix Secure Private Access

- Acceso público a aplicaciones SaaS con Citrix Secure Private Access
- Acceso privado a aplicaciones cliente-servidor con Citrix Secure Private Access
- Protección del keylogger con Citrix Secure Private Access
- Protección para compartir pantalla con Citrix Secure Private Access
- Experiencia de usuario final con Citrix Secure Private Access
- Experiencia de inicio de sesión de ZTNA frente a VPN con Citrix Secure Private Access
- Análisis de puertos ZTNA frente a VPN con Citrix Secure Private Access

Novedades de los productos relacionados

- Citrix Enterprise Browser: Acerca de esta versión
- Citrix Workspace: novedades
- Citrix DaaS: novedades
- Cliente Citrix Secure Access | Clientes NetScalerGateway

Flujo de trabajo guiado por el administrador para una incorporación y una configuración fáciles

February 16, 2024

En el servicio Secure Private Access se encuentra disponible una nueva experiencia de administración optimizada con un proceso paso a paso para configurar el acceso de red de confianza cero a las aplicaciones SaaS, las aplicaciones web internas y las aplicaciones TCP. Incluye la configuración de Autenticación adaptable, aplicaciones que incluyen la suscripción de usuarios, directivas de acceso adaptables y otros en una sola consola de administración.

Este asistente ayuda a los administradores a lograr una configuración sin errores, ya sea durante la incorporación o el uso recurrente. Además, hay disponible un nuevo panel de control con total visibilidad de las métricas de uso generales y otra información clave.

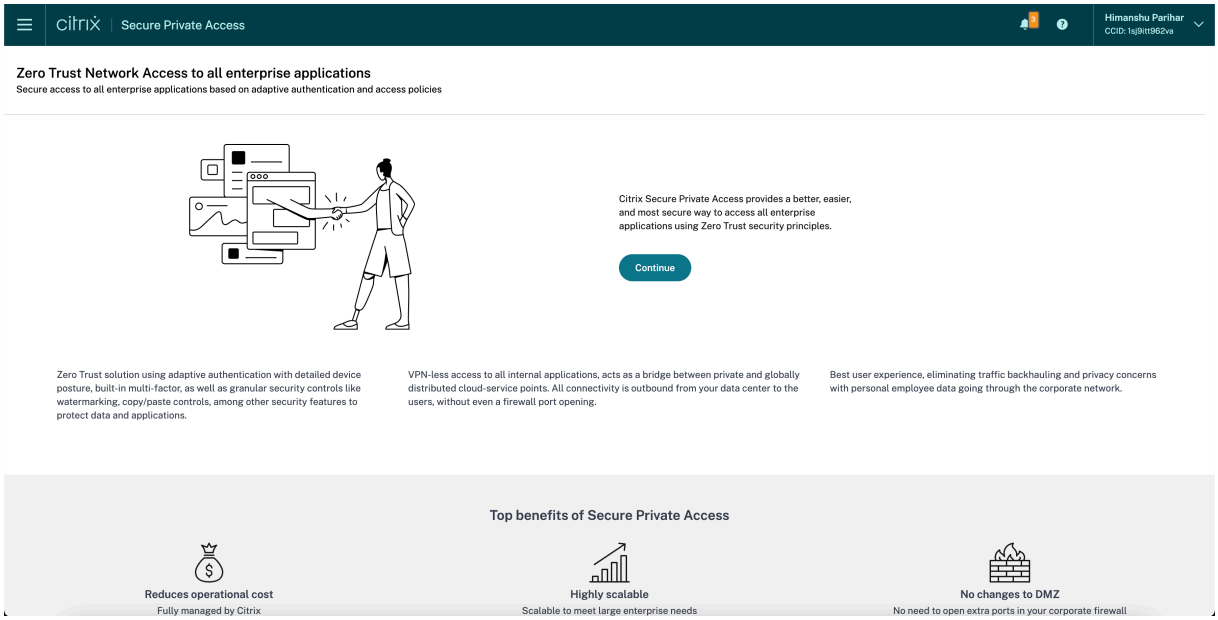
Los pasos de alto nivel incluyen lo siguiente:

1. Elija el método de autenticación para que los suscriptores inicien sesión en Citrix Workspace.
2. Agregue aplicaciones para sus usuarios.
3. Asigna permisos para el acceso a las aplicaciones mediante la creación de las directivas de acceso necesarias.
4. Revise la configuración de la aplicación.

Acceso al asistente de flujo de trabajo guiado por el administrador de Secure Private Access

Realice los siguientes pasos para acceder al asistente.

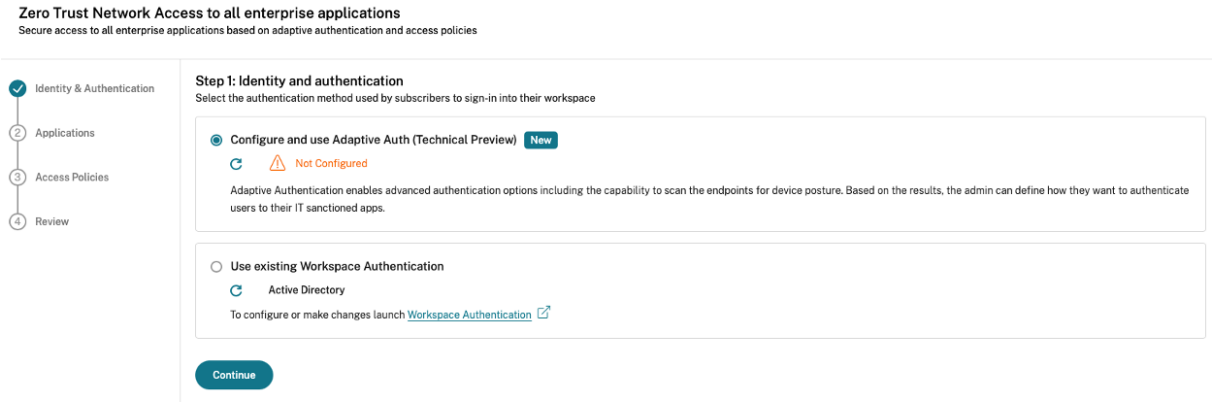
1. En el icono del servicio **Secure Private Access**, haga clic en **Administrar**.
2. En la página Descripción general, haga clic en **Continuar**.



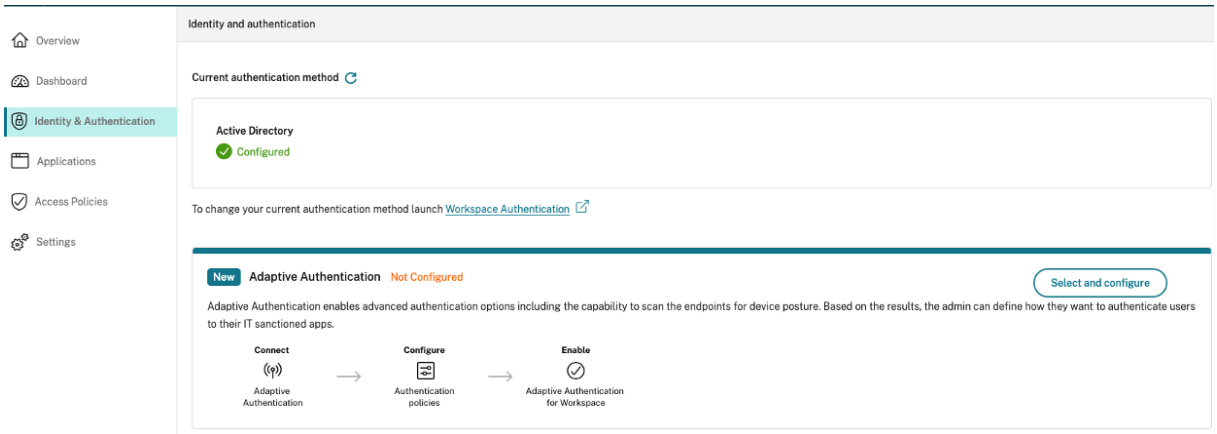
Paso 1: configurar la identidad y la autenticación

Seleccione el método de autenticación para que los suscriptores inicien sesión en Citrix Workspace. La autenticación adaptable es un servicio de Citrix Cloud que permite la autenticación avanzada para clientes y usuarios que inician sesión en Citrix Workspace. El servicio de autenticación adaptable es un Citrix ADC alojado en Citrix, administrado por Citrix y alojado en la nube que proporciona todas las capacidades de autenticación avanzadas, como las siguientes.

- Autenticación de varios factores
- Análisis de postura del dispositivo
- Autentificación condicional
- Acceso adaptable a Citrix Virtual Apps and Desktops
- Para configurar la autenticación adaptable, seleccione **Configurar y usar la autenticación adaptable (vista previa técnica)** y, a continuación, complete la configuración. Para obtener más información sobre la autenticación adaptable, consulte el servicio de autenticación adaptable. Después de configurar la autenticación adaptable, puede hacer clic en **Administrar** para modificar la configuración, si es necesario.



- Si inicialmente seleccionó un método de autenticación diferente y quiere cambiar a Autenticación adaptable, haga clic en **Seleccionar y configurar** y, a continuación, complete la configuración.

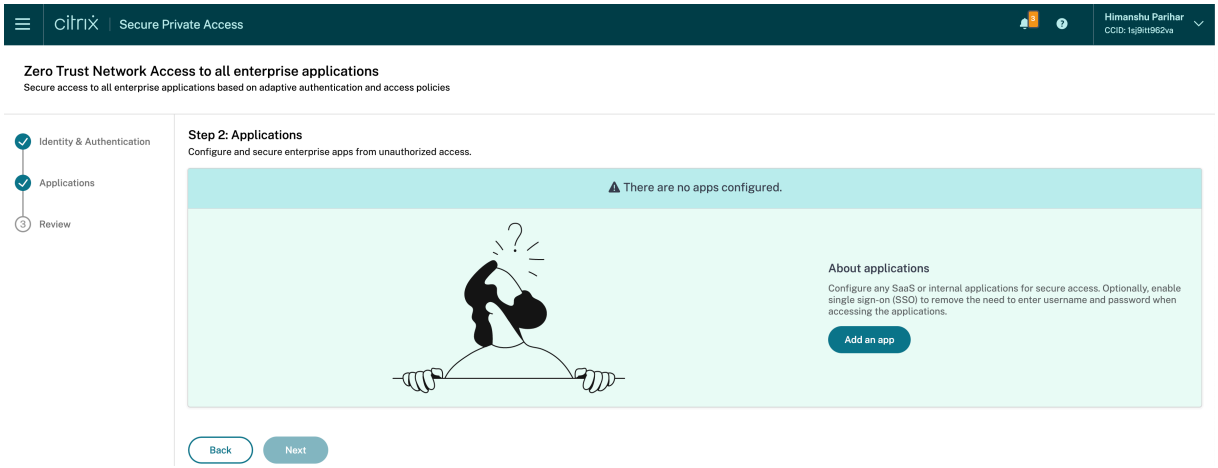


Para cambiar el método de autenticación existente o cambiar el método de autenticación existente, haga clic en **Autenticación de Workspace**

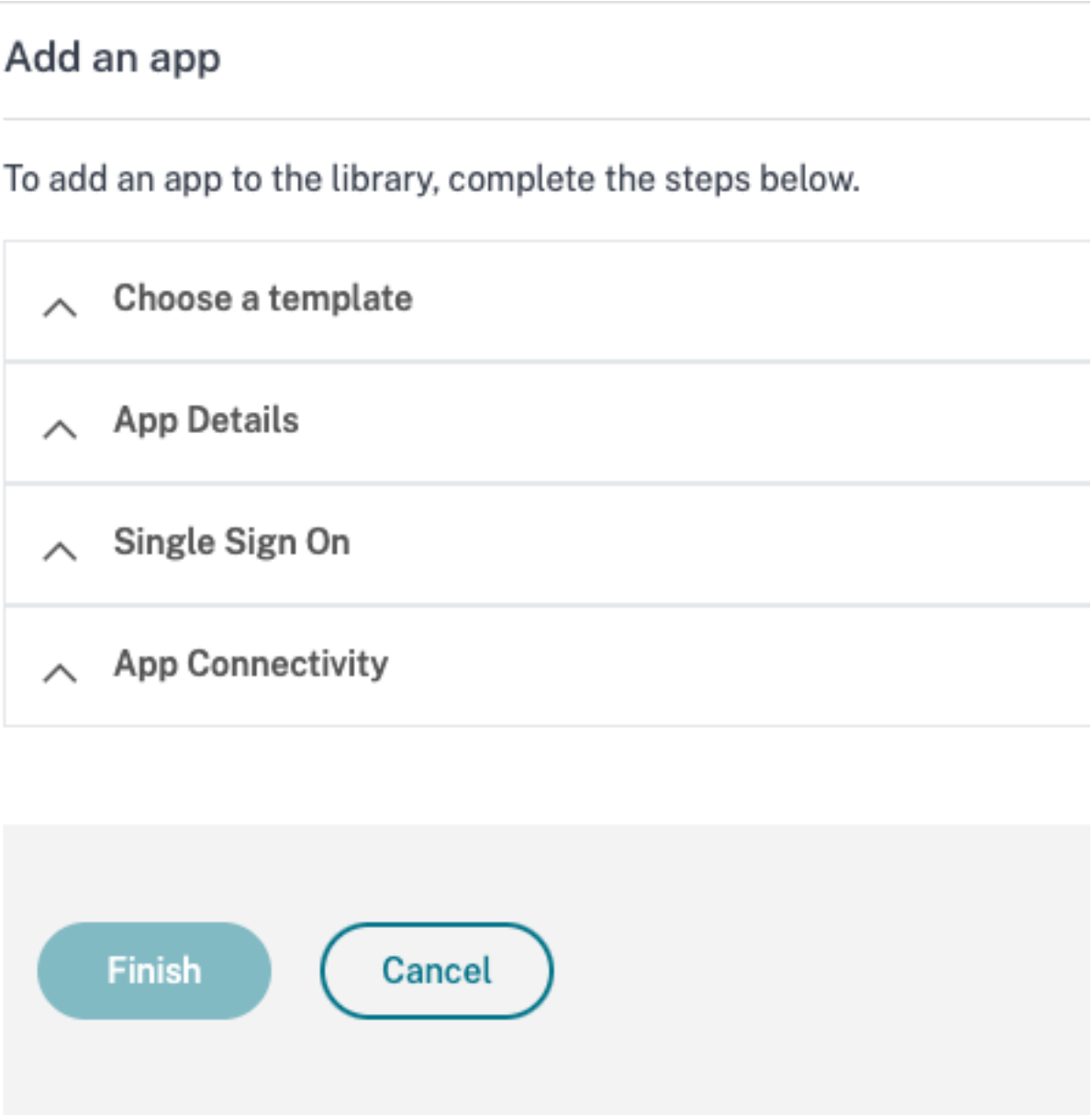
Paso 2: Agregar y administrar aplicaciones

Después de seleccionar el método de autenticación, configure las aplicaciones. Para los usuarios primerizos, la página de inicio de **Aplicaciones** no muestra ninguna aplicación. Para agregar una aplicación, haga clic en **Agregar una aplicación**. Puede agregar aplicaciones SaaS, aplicaciones web y aplicaciones TCP/UDP desde esta página. Para agregar una aplicación, haga clic en **Agregar una aplicación**.

Una vez que haya agregado una aplicación, podrá verla listada aquí.



Complete los pasos que se muestran en la siguiente ilustración para agregar una aplicación.



- **Agregar una aplicación web empresarial**
  - Support for Enterprise web apps
  - Configurar el acceso directo a las aplicaciones web
- **Agregar una aplicación SaaS**
  - Soporte para la aplicación Software as a Service
  - Configuración específica del servidor de aplicaciones SaaS
- **Configurar aplicaciones cliente-servidor**
  - Compatibilidad con aplicaciones cliente-servidor

- **Lanzar una aplicación**
  - Iniciar una aplicación configurada: flujo de trabajo del usuario final
- **Habilitar el acceso de solo lectura a los administradores**
  - Acceso de solo lectura para administradores a aplicaciones SaaS y web

Paso 3: Configurar una directiva de acceso con varias reglas

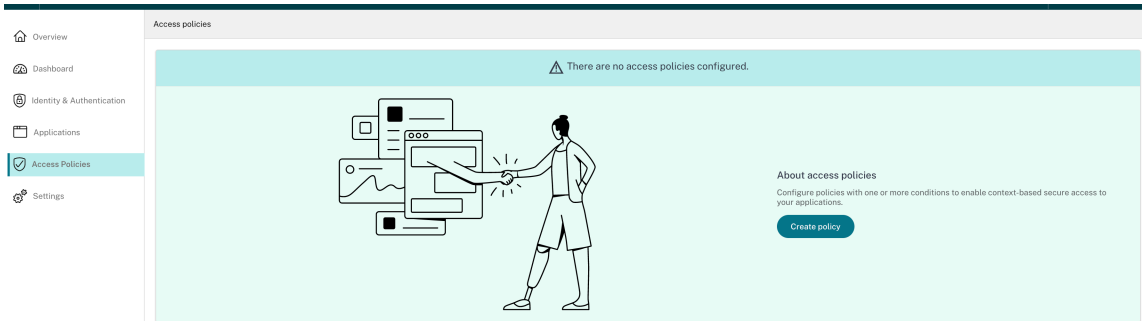
Puede crear varias reglas de acceso y configurar diferentes condiciones de acceso para diferentes usuarios o grupos de usuarios dentro de una única directiva. Estas reglas se pueden aplicar por separado para las aplicaciones HTTP/HTTPS y TCP/UDP, todo ello dentro de una única directiva.

Las directivas de acceso de Secure Private Access permiten habilitar o inhabilitar el acceso a las aplicaciones en función del contexto del usuario o del dispositivo del usuario. Además, puede habilitar el acceso restringido a las aplicaciones al agregar las siguientes restricciones de seguridad:

- Restringir acceso al portapapeles
- Restringir impresión
- Restringir descargas
- Restringir las subidas
- Mostrar marca de agua
- Limitar el registro de claves
- Restringir la captura

Para obtener más información sobre estas restricciones, consulte Opciones de restricciones de acceso disponibles.

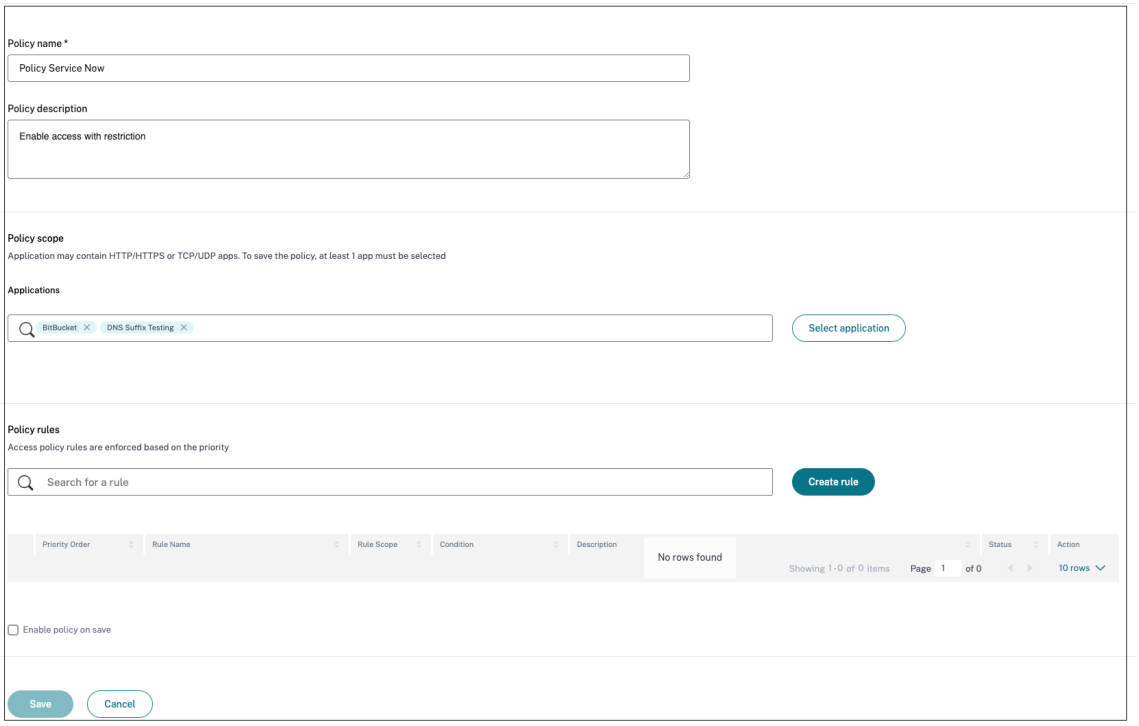
1. En el panel de navegación, haga clic en **Directivas de acceso** y, a continuación, en **Crear directiva**.



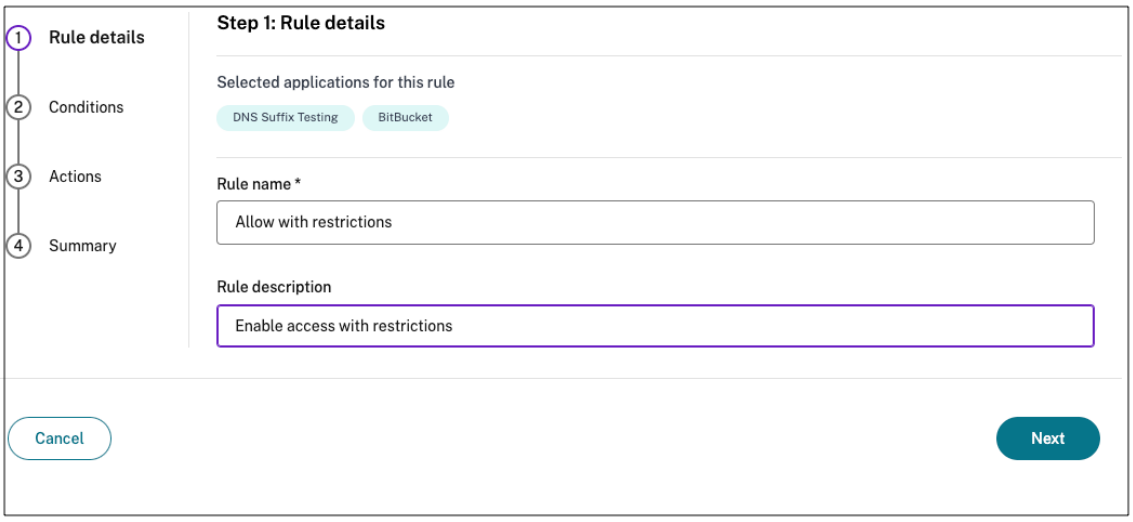
   Para los usuarios primerizos, la página de inicio de **Directivas de acceso** no muestra ninguna directiva. Una vez que haya creado una directiva, podrá verla listada aquí.

2. Introduzca el nombre de la directiva y la descripción de la misma.

3. En **Aplicaciones**, seleccione la aplicación o el conjunto de aplicaciones en las que se debe aplicar esta directiva.
4. Haga clic en **Crear regla** para crear reglas para la directiva.

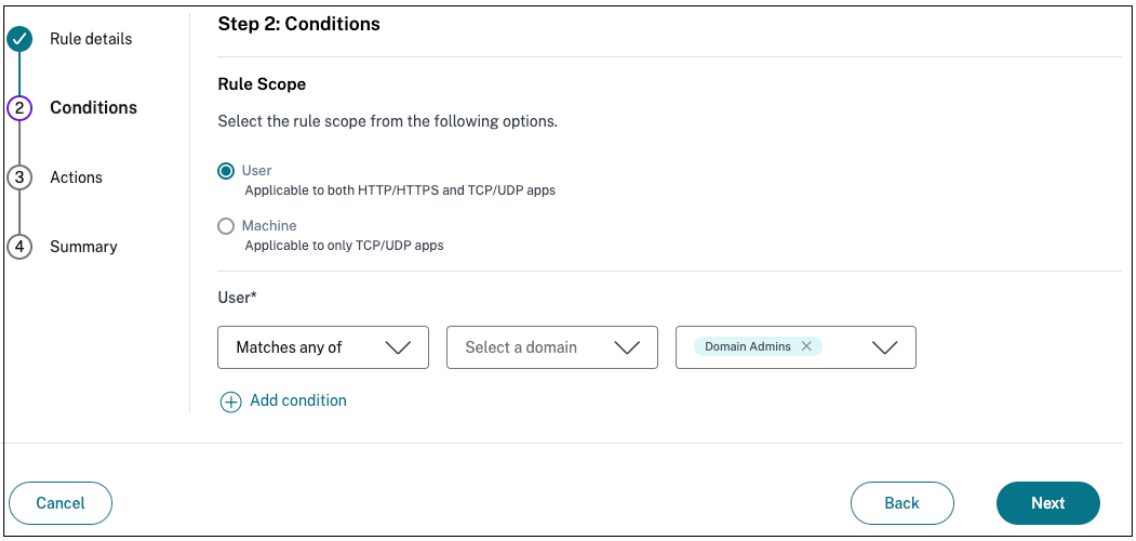


5. Introduzca el nombre de la regla y una breve descripción de la regla y, a continuación, haga clic en **Siguiente**.



6. Selecciona las condiciones de los usuarios. La condición de **usuario** es una condición obligatoria que debe cumplirse para conceder acceso a las aplicaciones a los usuarios. Seleccione una de estas opciones:

- **Coincide con alguno de**: Solo se permite el acceso a los usuarios o grupos que coincidan con alguno de los nombres que figuran en el campo y que pertenezcan al dominio seleccionado.
- **No coincide con ninguno**: Se permite el acceso a todos los usuarios o grupos, excepto los que figuran en el campo y que pertenecen al dominio seleccionado.



7. (Opcional) Haga clic en + para agregar varias condiciones en función del contexto.

   Al agregar condiciones basadas en un contexto, se aplica una operación AND a las condiciones en las que la directiva se evalúa solo si se cumplen los **usuarios** y las condiciones opcionales basadas en el contexto. Puede aplicar las siguientes condiciones según el contexto.

   - Dispositivo de **escritorio** o **móvil**: Seleccione el dispositivo para el que quiere habilitar el acceso a las aplicaciones.
   - **Ubicación geográfica**: Seleccione la condición y la ubicación geográfica desde donde los usuarios acceden a las aplicaciones.
     - **Coincide con cualquiera de:** Solo los usuarios o grupos de usuarios que accedan a las aplicaciones desde cualquiera de las ubicaciones geográficas de la lista tienen habilitado el acceso a las aplicaciones.
     - **No coincide con ninguno:** Se ha habilitado el acceso a todos los usuarios o grupos de usuarios que no sean los de las ubicaciones geográficas enumeradas.
   - **Ubicación de red**: Seleccione la condición y la red mediante la cual los usuarios acceden a las aplicaciones.
     - **Coincide con cualquiera de:** Solo los usuarios o grupos de usuarios que accedan a las aplicaciones desde cualquiera de las ubicaciones de red enumeradas tienen habilitado el acceso a las aplicaciones.
     - **No coincide con ninguno:** Todos los usuarios o grupos de usuarios que no sean los de las ubicaciones de red enumeradas tienen acceso habilitado.

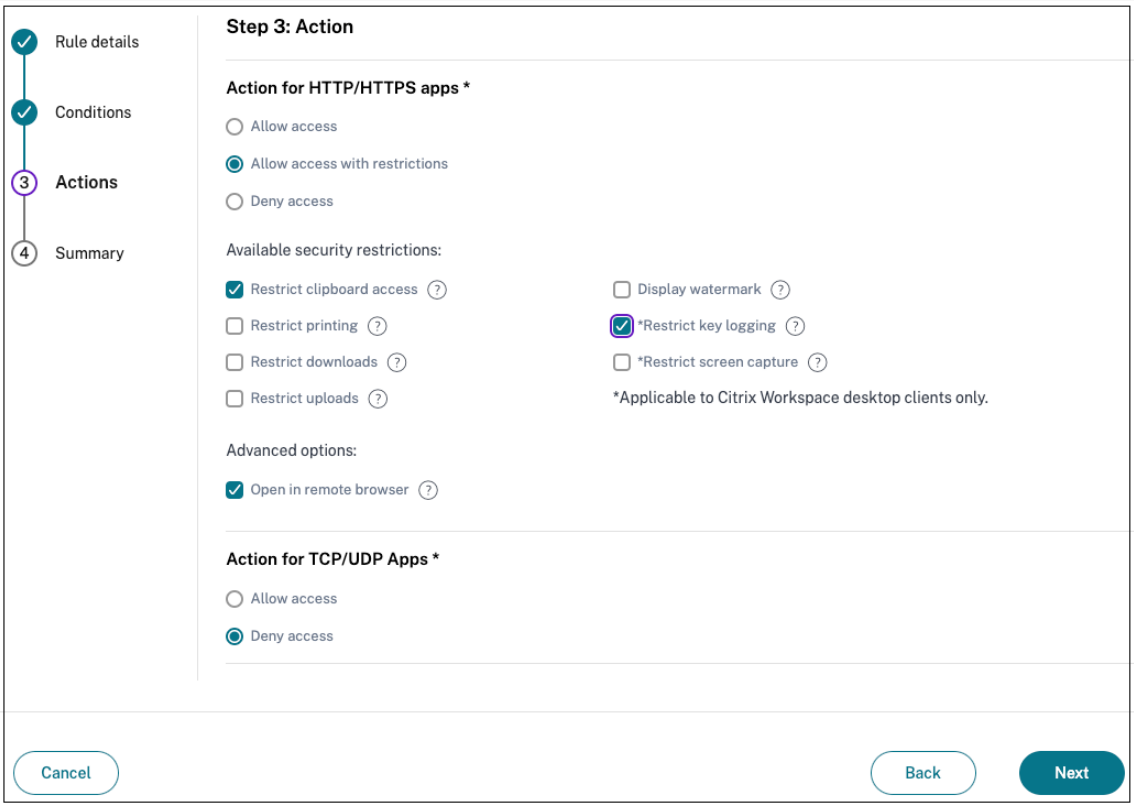
- **Verificación de la postura del dispositivo**: Seleccione las condiciones que debe cumplir el dispositivo del usuario para acceder a la aplicación.
- **Puntuación de riesgo del usuario**: Seleccione las categorías de puntuación de riesgo en función de las cuales los usuarios deben tener acceso a la aplicación.
- **URL**del espacio de trabajo: los administradores pueden especificar filtros en función del nombre de dominio completo correspondiente al espacio de trabajo. Esta opción se encuentra actualmente en versión preliminar.
  - **Coincide con cualquiera de**: Permita el acceso solo cuando la conexión de usuario entrante cumpla con alguna de las URL de Workspace configuradas.
  - **Coincide con todas :**permite el acceso solo cuando la conexión de usuario entrante cumple con todas las URL de Workspace configuradas.

8. Haga clic en **Siguiente**.
9. Seleccione las acciones que se deben aplicar en función de la evaluación de la condición.

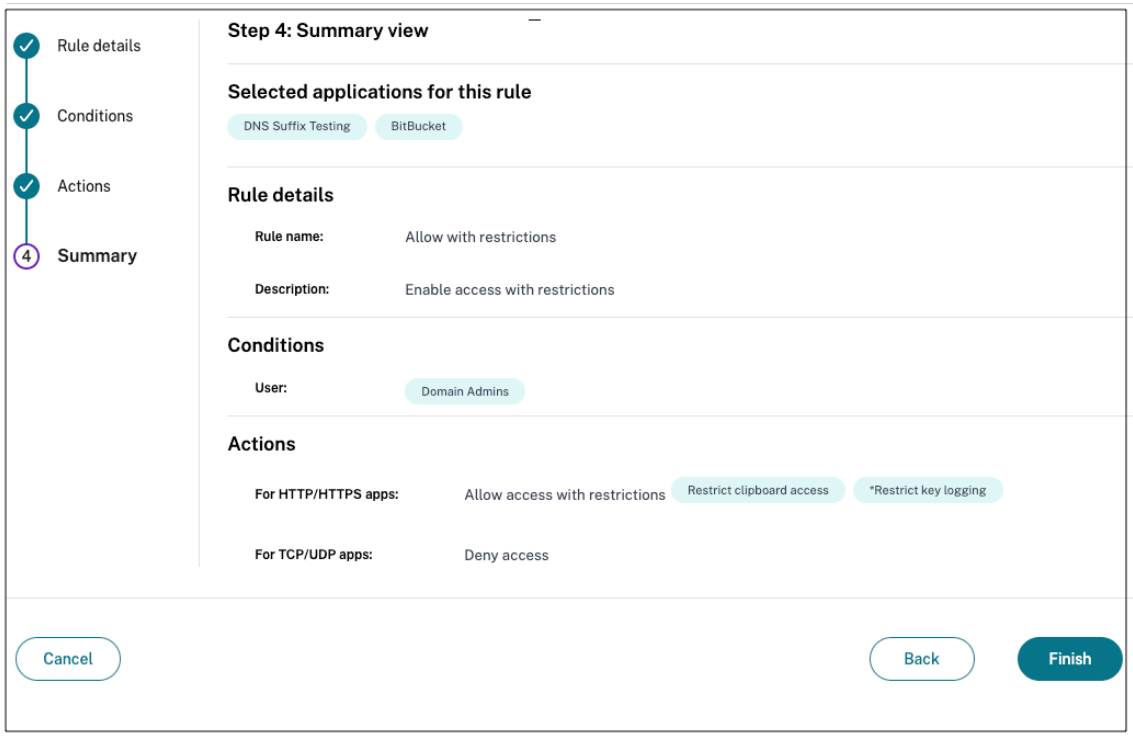
   - Para las aplicaciones HTTP/HTTPS, puede seleccionar lo siguiente:
     - **Permitir el acceso**
     - **Permitir el acceso con restricciones**
     - **Denegar el acceso**

     > **Nota:**
     >
     > Si seleccionas **Permitir el acceso con restricciones**, debes seleccionar las restricciones que quieres aplicar a las aplicaciones. Para obtener más información sobre las restricciones, consulta Opciones de restricciones de acceso disponibles . También puede especificar si quiere que la aplicación se abra en un explorador web remoto o en Citrix Secure Browser.

   - Para el acceso a TCP/UDP, puede seleccionar lo siguiente:
     - **Permitir el acceso**
     - **Denegar el acceso**



10. Haga clic en **Siguiente**. La página de resumen muestra los detalles de la directiva.
11. Puede comprobar los detalles y hacer clic en **Finalizar**.



Puntos a tener en cuenta después de crear una directiva

- La directiva que ha creado aparece en la sección Reglas de directiva y está habilitada de forma predeterminada. Puede inhabilitar las reglas si es necesario. Sin embargo, asegúrese de que haya al menos una regla habilitada para que la directiva esté activa.
- Se asigna un orden de prioridad a la directiva de forma predeterminada. La prioridad con un valor inferior tiene la preferencia más alta. La regla con el número de prioridad más bajo se evalúa primero. Si la regla (n) no coincide con las condiciones definidas, se evalúa la siguiente regla (n+1) y así sucesivamente.

Ejemplo de evaluación de reglas con orden de prioridad:

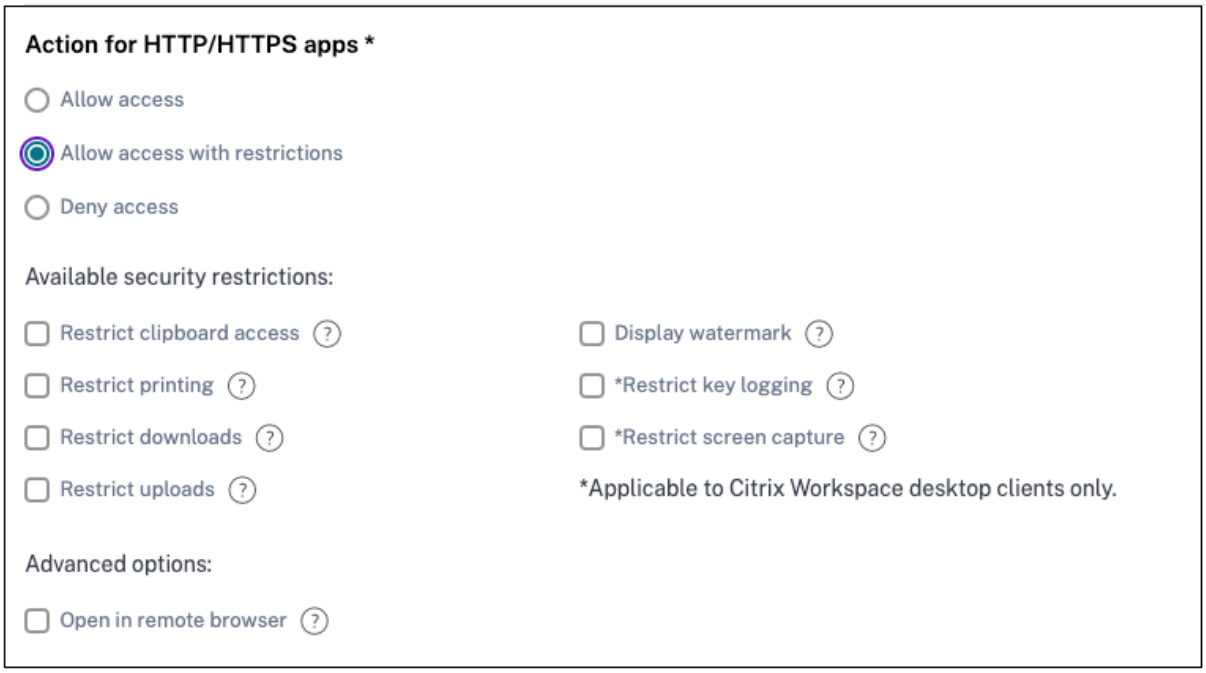
Tenga en cuenta que ha creado dos reglas, la Regla 1 y la Regla 2.
La regla 1 se asigna al usuario A y la regla 2 al usuario B y, a continuación, se evalúan ambas reglas.
Tenga en cuenta que tanto la regla 1 como la regla 2 están asignadas al usuario A. En este caso, la regla 1 tiene la prioridad más alta. Si se cumple la condición de la Regla 1, se aplica la Regla 1 y se omite la Regla 2. De lo contrario, si no se cumple la condición de la Regla 1, la Regla 2 se aplica al usuario A.

> **Nota:**
>
> Si no se evalúa ninguna de las reglas, los usuarios no enumeran la aplicación.

Opciones de restricciones de acceso disponibles

Al seleccionar la acción **Permitir el acceso con restricciones**, debe seleccionar al menos una de las restricciones de seguridad. Estas restricciones de seguridad están predefinidas en el sistema. Los

administradores no pueden modificar ni agregar otras combinaciones. Se pueden habilitar las siguientes restricciones de seguridad para la aplicación.



- **Restringir el acceso al portapapeles:**deshabilita las operaciones de cortar/copiar/pegar entre la aplicación y el portapapeles del sistema.
- **Restringir la impresión:**deshabilita la capacidad de imprimir desde el navegador Citrix Enterprise.
- **Restringir las descargas:**deshabilita la capacidad del usuario para descargar desde la aplicación.
- **Restringir las subidas:**deshabilita la capacidad del usuario de subir contenido dentro de la aplicación.
- **Mostrar marca de agua:**muestra una marca de agua en la pantalla del usuario que muestra el nombre de usuario y la dirección IP de la máquina del usuario.
- **Restringir el registro de claves:**protege contra los registradores de claves. Cuando un usuario intenta iniciar sesión en la aplicación con el nombre de usuario y la contraseña, todas las claves se cifran en los registradores de claves. Además, todas las actividades que el usuario realiza en la aplicación están protegidas contra el registro de claves. Por ejemplo, si las directivas de protección de aplicaciones están habilitadas para Office 365 y el usuario edita un documento de Word de Office 365, todas las pulsaciones de teclas se cifran en los registradores de teclas.
- **Restringir la captura de pantalla:**desactiva la capacidad de capturar las pantallas con cualquiera de los programas o aplicaciones de captura de pantalla. Si un usuario intenta capturar la pantalla, se captura una pantalla en blanco.

- **Abrir en un explorador remoto:**abre la aplicación en el explorador remoto de Citrix.
  - Si selecciona **Abrir en un navegador remoto** y faltan los catálogos del navegador remoto para Secure Private Access, aparece el siguiente mensaje:

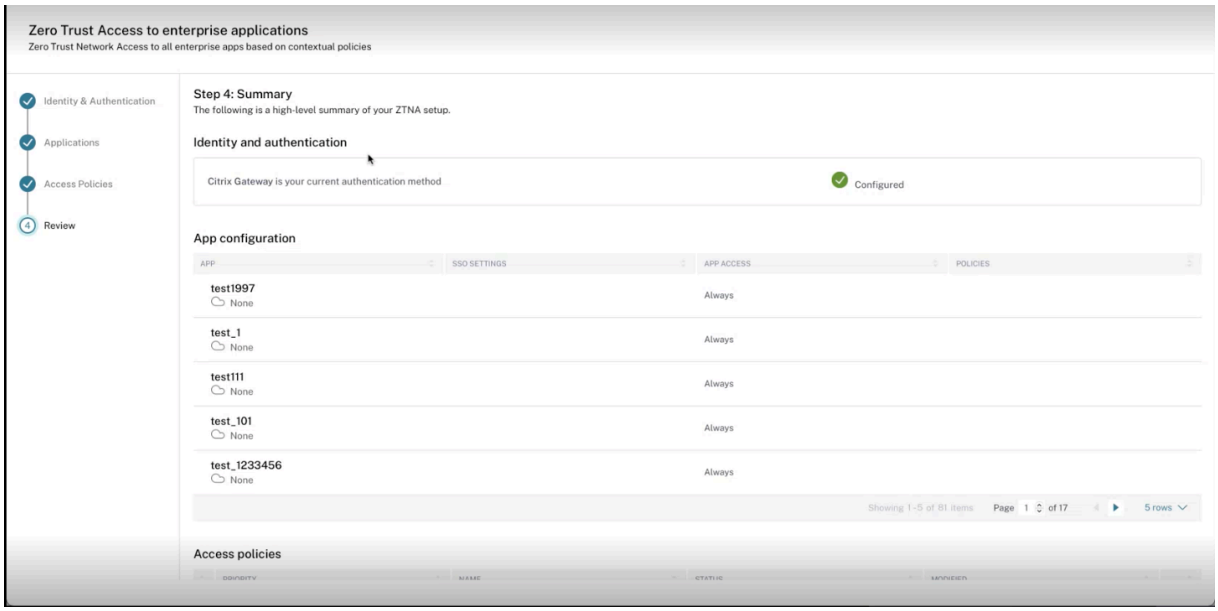
    No hay ningún catálogo publicado de aislamiento remoto disponible para hospedar esta aplicación. Vaya a la consola de Remote Browser Isolation para publicar el catálogo.
  - Además, si intenta iniciar una aplicación web o SaaS, la aplicación no se inicia si faltan los catálogos de RBI y aparece el siguiente mensaje:

    No se ha creado ningún catálogo para gestionar esta solicitud. Contacte con su administrador.

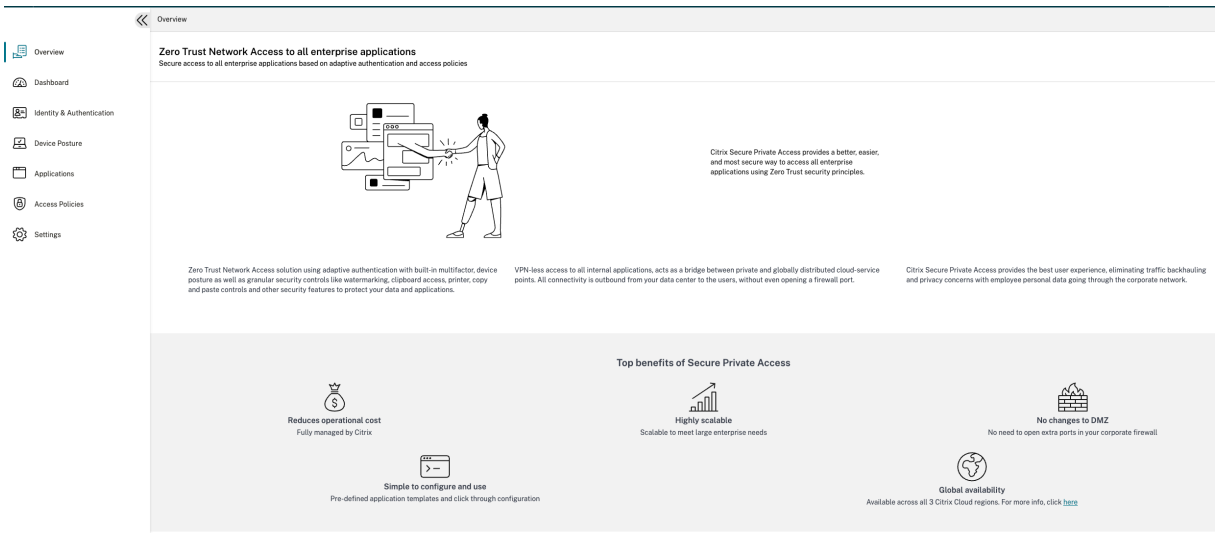
  Para obtener más información sobre Citrix Remote Browser Isolation, consulte Remote Browser Isolation.

Paso 4: Revisar el resumen de cada configuración

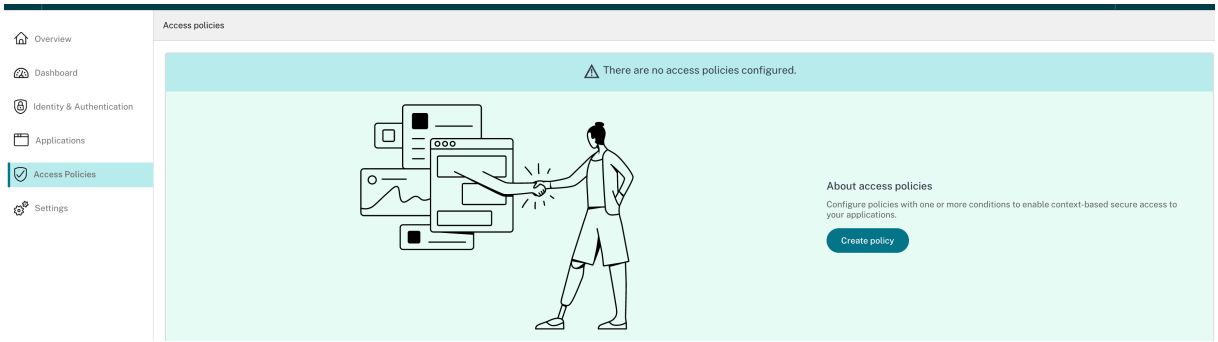
En la página Revisar, puede ver la configuración completa de la aplicación y, a continuación, hacer clic en **Cerrar**.



La siguiente ilustración muestra la página después de completar la configuración de 4 pasos.



> **Importante:**
>
> - Después de completar la configuración con el asistente, puede modificar la configuración de una sección yendo directamente a esa sección. No tiene que seguir la secuencia.
> - Si elimina todas las aplicaciones configuradas o las directivas, debe volver a agregarlas. En este caso, aparece la siguiente pantalla si ha eliminado todas las directivas.



Descripción general del panel

December 27, 2023

El panel del servicio Secure Private Access muestra los datos de diagnóstico y uso de las aplicaciones SaaS, Web, TCP y UDP. El panel de control proporciona a los administradores una visibilidad completa de sus aplicaciones, usuarios, estado de los conectores y uso del ancho de banda en un solo lugar para su consumo. Estos datos se obtienen de Citrix Analytics. Los datos de las distintas entidades se pueden ver durante el tiempo preestablecido o para una línea de tiempo personalizada. Puede desglosar algunas de las entidades para ver más detalles.

Las métricas se clasifican en líneas generales en las siguientes categorías.

- **Registro y solución de problemas**
  - Registros de diagnóstico: registros relacionados con la autenticación, el inicio de aplicaciones, la enumeración de aplicaciones y las comprobaciones del estado del dispositivo.
- **Usuarios**
  - Usuarios activos: Total de usuarios únicos que acceden a las aplicaciones (SaaS, Web y TCP) durante el intervalo de tiempo seleccionado.
  - Cargas: volumen total de datos subidos a través del servicio Secure Private Access durante el intervalo de tiempo seleccionado.
  - Descargas: volumen total de datos descargados a través del servicio Secure Private Access durante el intervalo de tiempo seleccionado.
- **Aplicaciones:**
  - Aplicaciones: número total de aplicaciones (independientemente del intervalo de tiempo) configuradas actualmente.
  - Recuento de inicios de aplicaciones: Total de aplicaciones (sesiones de aplicaciones) iniciadas por cada usuario durante el intervalo de tiempo seleccionado.
  - Dominios configurados: Total de dominios configurados para el intervalo de tiempo seleccionado.
  - Aplicaciones descubiertas: número total de dominios individuales únicos a los que se ha accedido pero que no están asociados a ninguna aplicación
- **Directivas de acceso**
  - Directivas de acceso: Total de directivas de acceso (independientemente del intervalo de tiempo) configuradas actualmente.

Registros de diagnóstico

Utilice el gráfico de **registros de diagnóstico** para ver los registros relacionados con la autenticación, el inicio de la aplicación, la enumeración de aplicaciones y también los registros relacionados con la postura del dispositivo. Puede hacer clic en el enlace **Ver más** para ver los detalles de los registros. Los detalles se presentan en formato tabular. Puede ver los registros de la hora preestablecida o de una línea de tiempo personalizada. Puede agregar columnas al gráfico haciendo clic en el signo +, según la información que quiera ver en el panel. Puede exportar los registros de usuario a formato CSV.

- Puede utilizar los filtros **ESTADO, CATEGORÍA, TIPO DE APLICACIÓN, RESULTADO DE LA DIRECTIVA** para buscar registros relacionados con:

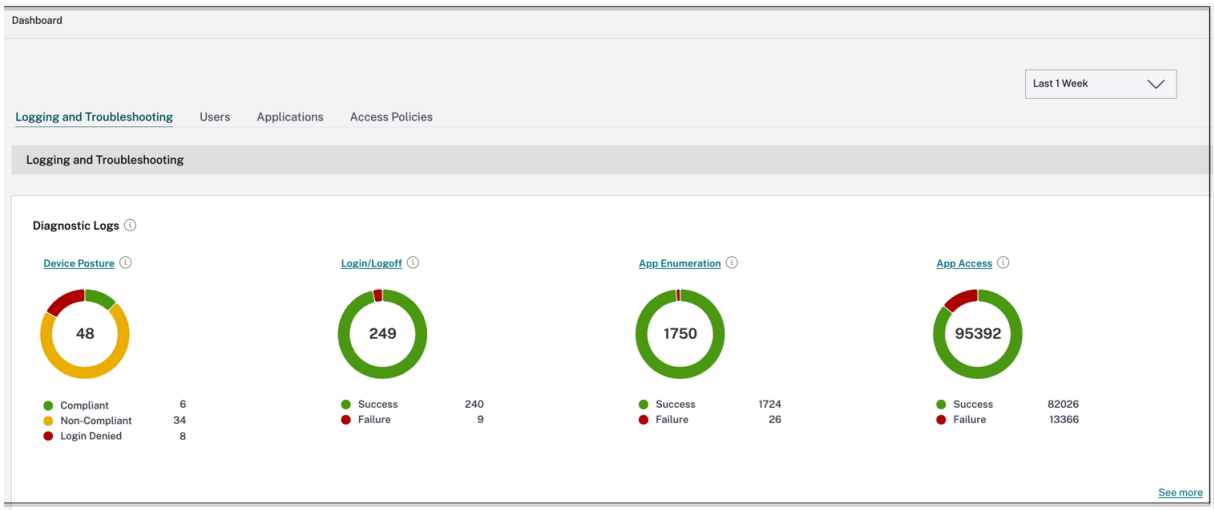
  - autenticación
  - inicio de aplicaciones
  - enumeración de aplicaciones
  - resultados de la evaluación de la directiva de acceso

  También puede utilizar las categorías del campo de búsqueda junto con los operadores de búsqueda de la página **Registros de diagnóstico** para refinar aún más los resultados de la búsqueda. Para obtener más información sobre los operadores de búsqueda, consulte Operadores de búsqueda.

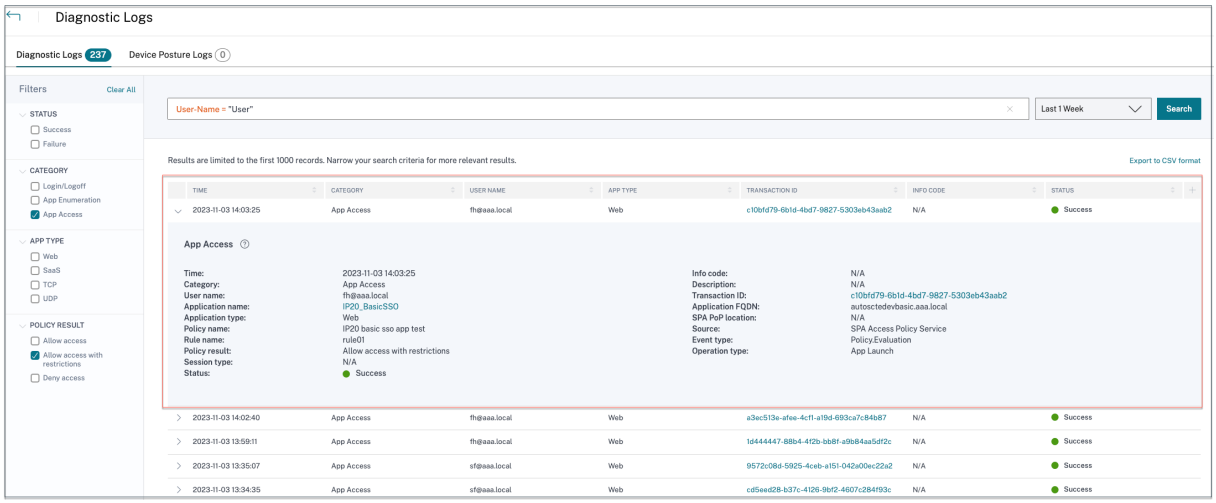
  Por ejemplo, en el campo de búsqueda, puede hacer clic en una categoría `Transaction ID` y un operador igual a (=) y, a continuación, introducir el identificador de la transacción. Por ejemplo, `Transaction-ID =77cdfd46-26b4-142d-9678-002248d60417` para buscar todos los registros relacionados con una solicitud de acceso a una aplicación determinada. Para ver la lista de columnas disponibles que se pueden agregue al panel, haga clic en el signo **+**. Puede agregar o quitar columnas según sea necesario.

- **Registros de postura del dispositivo:** puede refinar la búsqueda en función de los resultados de la directiva (**compatible, no compatible e inicio de sesión denegado**). Para obtener más información sobre la postura del dispositivo, consulte Postura del dispositivo.

> **Nota:**
>
> - Cada evento de error del panel de registros de diagnóstico de Secure Private Access tiene un código de información asociado. Para obtener más información, consulte Código de información.
> - El ID de transacción correlaciona todos los registros de Secure Private Access de una solicitud de acceso. Para obtener más información, consulte ID de transacción.



Puede hacer clic en el icono de expansión (>) para ver los detalles completos de los registros.

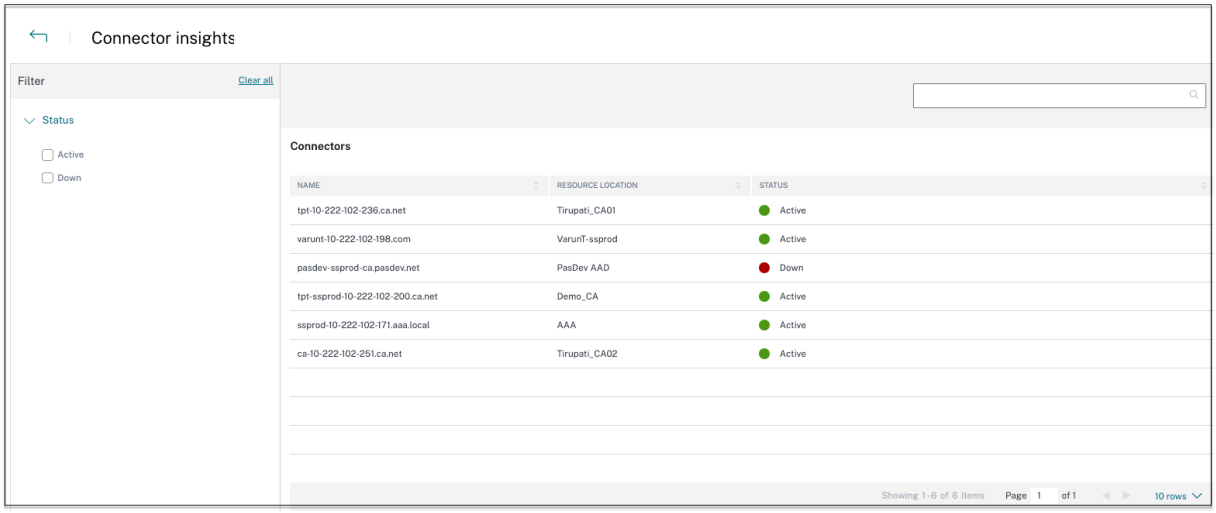


Nota:

- De forma predeterminada, la página **Registros de diagnóstico** muestra los datos de la semana actual y solo los 10000 registros recientes. Utilice la búsqueda por fecha personalizada y los filtros para refinar aún más los resultados de la búsqueda.

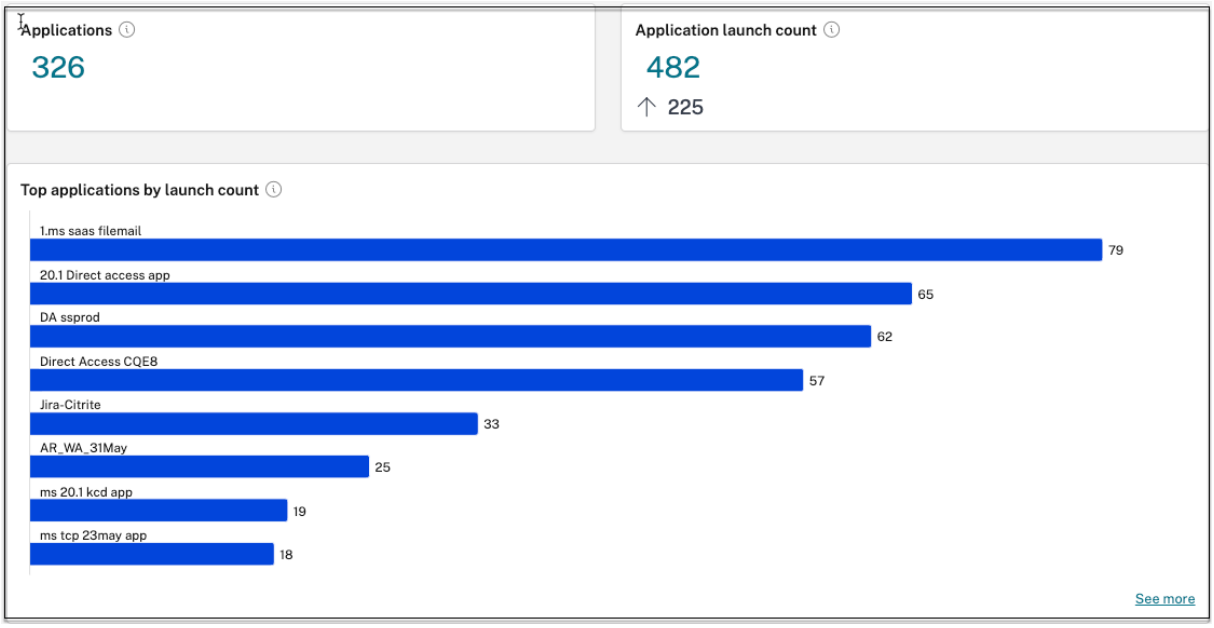
Estado del conector

Utilice la tabla de **estado de los conectores** para ver el estado de los conectores y las ubicaciones de recursos en las que se implementan los conectores. Haga clic en el enlace **Ver más** para ver los detalles. En la página **Información del conector**, puede usar los filtros **Activo o**Inactivo** para filtrar los conectores en función de su estado.



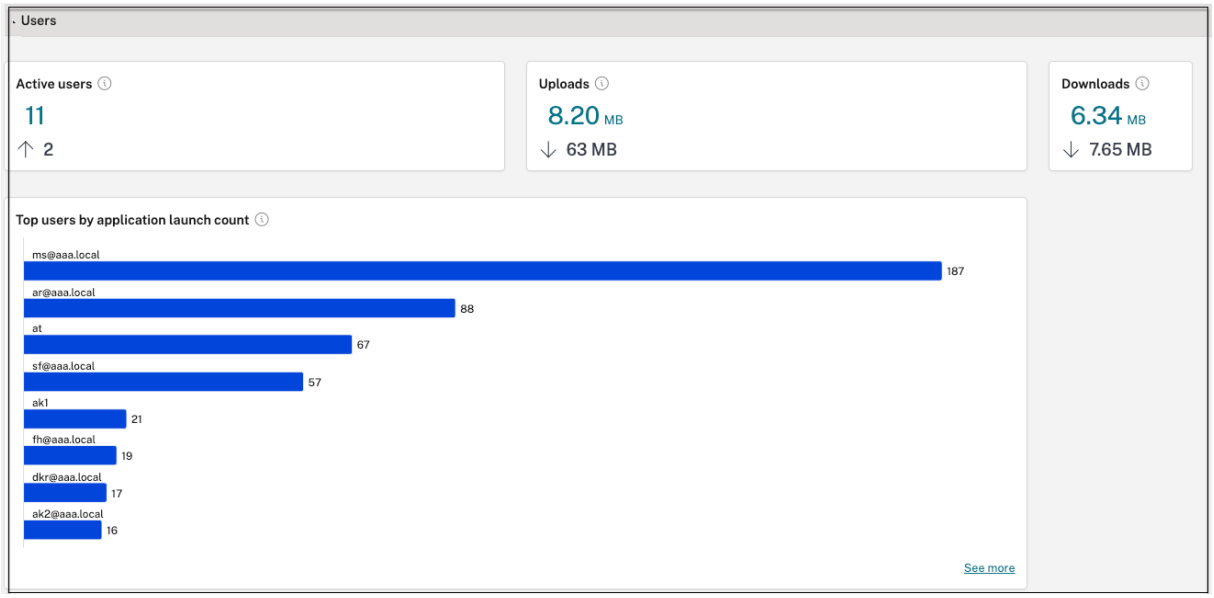
Principales aplicaciones por recuento de lanzamientos

Utilice el gráfico **Recuento de las principales aplicaciones por inicios** para ver la lista de aplicaciones principales en función del número de veces que se lanzó la aplicación, el volumen total de datos cargados en el servidor de aplicaciones y el volumen total de datos descargados del servidor de aplicaciones. Puede aplicar los filtros **Aplicaciones SaaS**, **Aplicaciones web**o **Aplicaciones TCP/UDP** para limitar la búsqueda a aplicaciones específicas. Puede filtrar los datos para un cronograma preestablecido o para un cronograma personalizado.



Número de usuarios principales por número de lanzamientos de aplicaciones

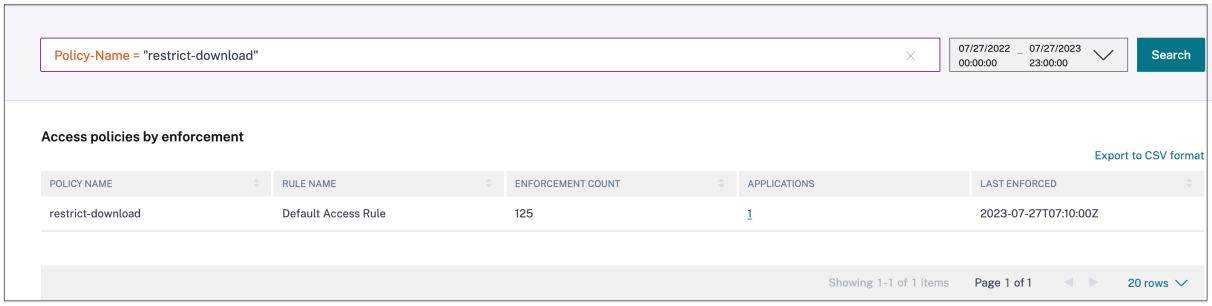
Utilice el gráfico **Recuento de los principales usuarios por inicios de aplicación** para ver los datos por usuario. Por ejemplo, las veces que un usuario ha iniciado la aplicación TCP, el volumen total de datos cargados en el servidor de aplicaciones y el volumen total de datos descargados del servidor de aplicaciones. Puede filtrar los datos para un cronograma preestablecido o para un cronograma personalizado.



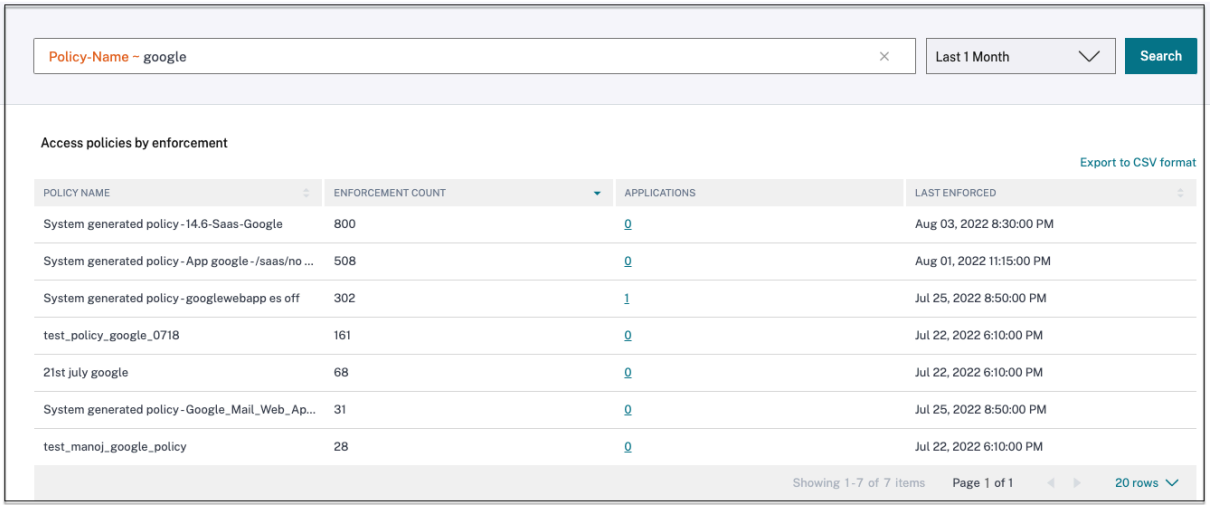
Principales directivas de acceso por aplicación

Utilice el cuadro **Directivas de acceso principales por aplicación** para ver la lista de directivas de acceso que se aplican en las aplicaciones. Haga clic en el enlace **Ver más** para ver la lista de directivas asociadas a las aplicaciones y el número de veces que se aplican las directivas. También puede usar la opción **Buscar** en la página Directivas de acceso para filtrar las directivas en función del nombre de la directiva. También puede buscar directivas específicas mediante los operadores de búsqueda para refinar aún más la búsqueda.

Por ejemplo, puede buscar una directiva denominada “restrict-download”mediante la cadena **Policy-Name**= restrict-download.

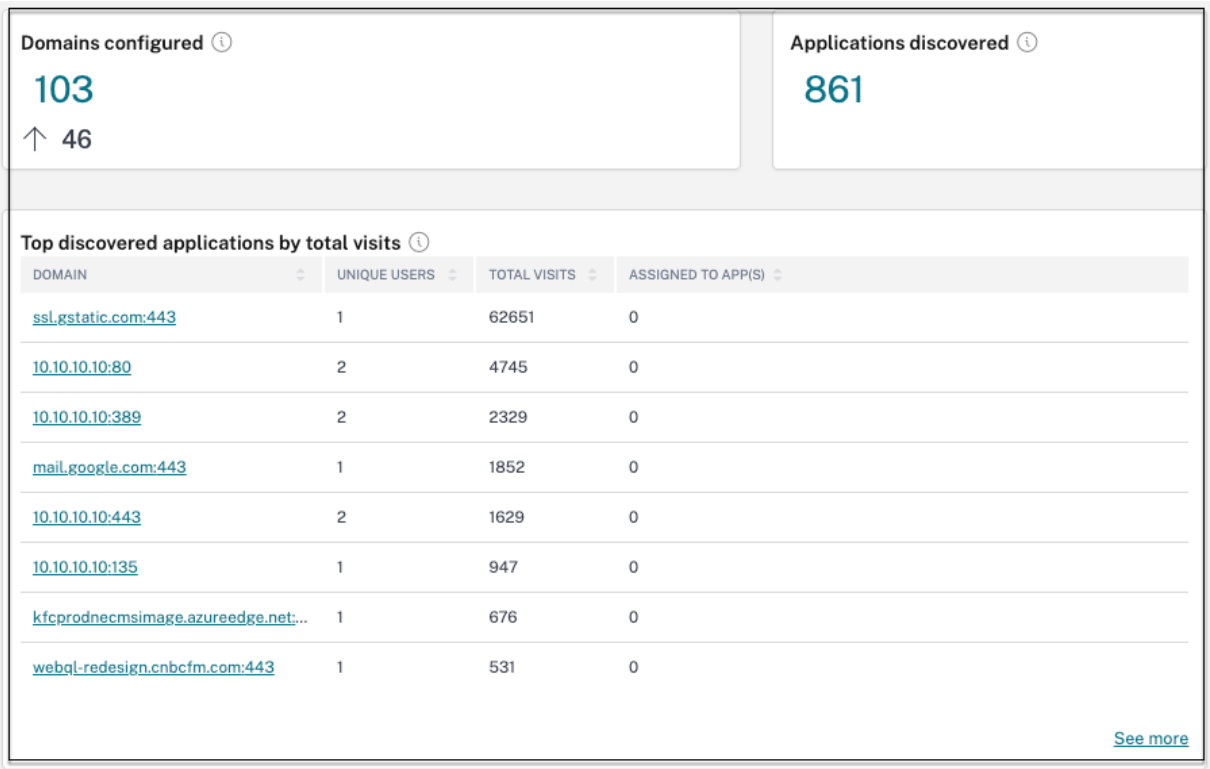


Del mismo modo, para buscar directivas que contengan parcialmente el término “google”, utilice la cadena **Policy-Name ~**google.



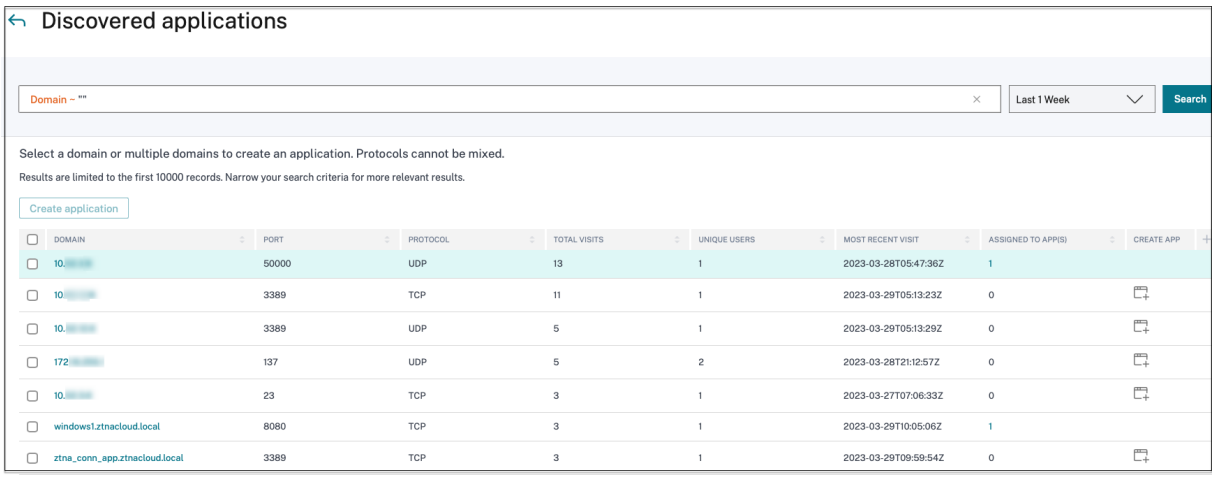
Principales aplicaciones detectadas

Use la **tabla de principales aplicaciones detectadas según el total de visitas** para ver la lista de dominios individuales únicos a los que se ha accedido en algún momento, pero que no están asociados a ninguna aplicación. Estos dominios se enumeran en función del número total de visitas a esos dominios. Los administradores pueden usar este gráfico para ver si muchos usuarios acceden a algún dominio de particular interés. En esos casos, los administradores pueden crear una aplicación con ese dominio para facilitar el acceso.



En el gráfico, la columna **ASIGNADO A LAS APLICACIONES** muestra el número total de aplicaciones que tienen este dominio configurado como parte de sus valores de URL o URL de destino relacionados. Al hacer clic en el número, se muestran las aplicaciones que están asignadas a este dominio.

Puede hacer clic en el enlace **Ver más** para ver más detalles sobre todos los dominios.



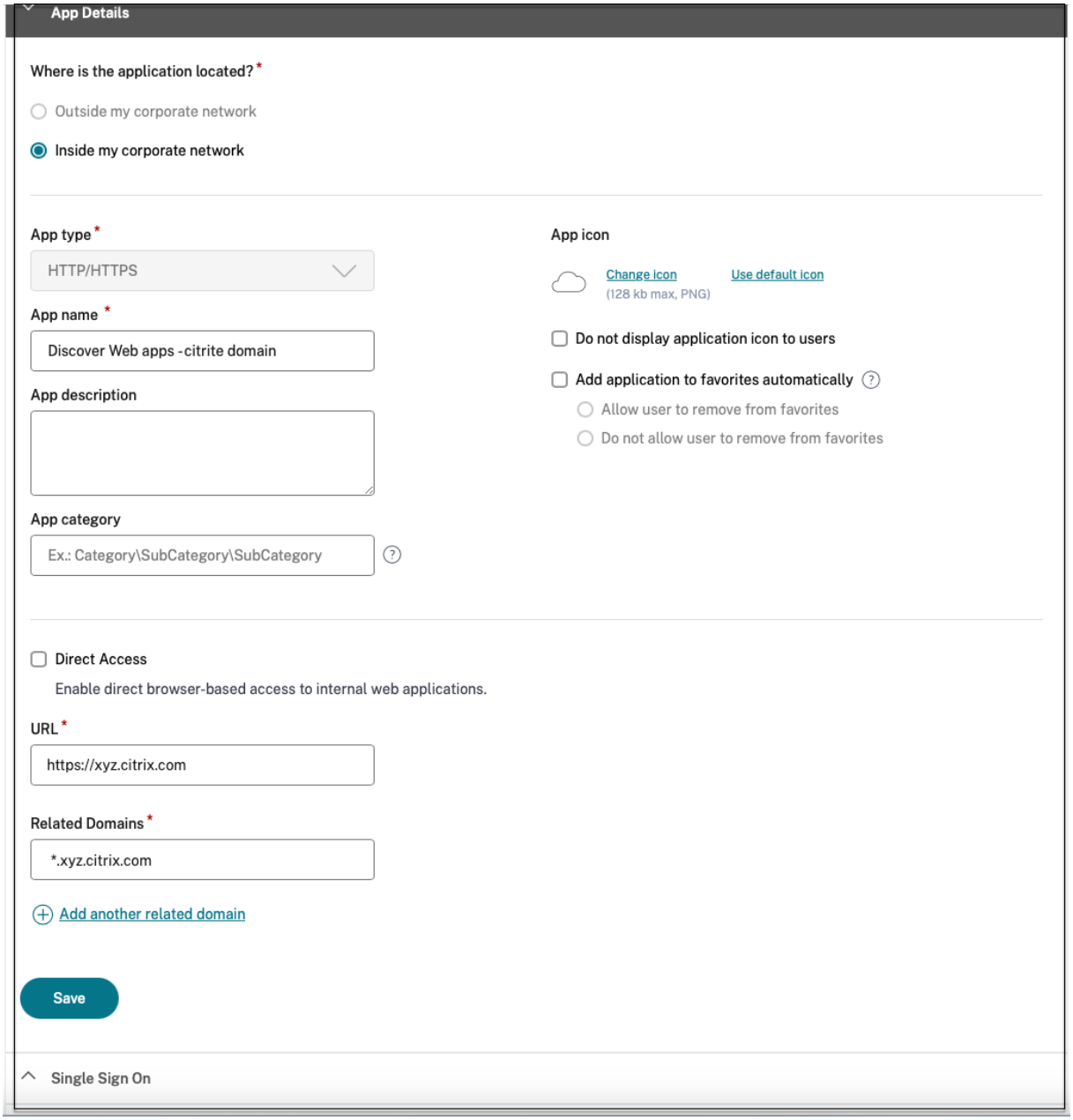
La página **Aplicaciones detectadas** muestra los detalles de los dominios, como el nombre de dominio, el puerto, el protocolo, el total de visitas, los usuarios únicos y la fecha de visita más reciente. Se pueden ordenar todas las columnas del gráfico. Puede usar la barra de búsqueda para buscar por dominio. Puede utilizar los operadores de la barra de búsqueda para buscar dominios específicos, según sus necesidades.

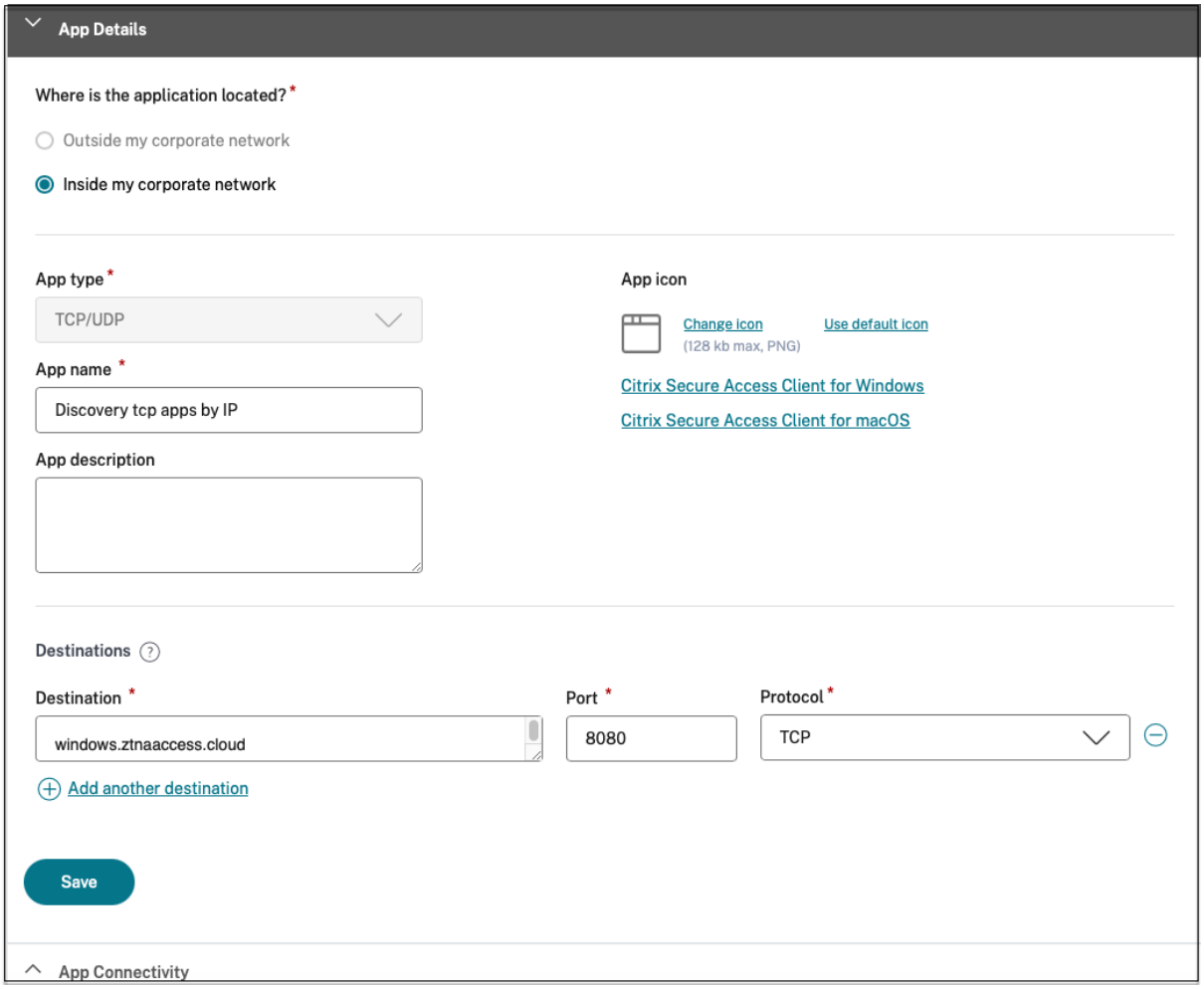
> **Nota:**
>
> - Los protocolos se derivan en función de los puertos estándar utilizados por los clientes.
> - La lista de dominios detectados está limitada a 10 000 registros.

Crear una aplicación a partir del gráfico

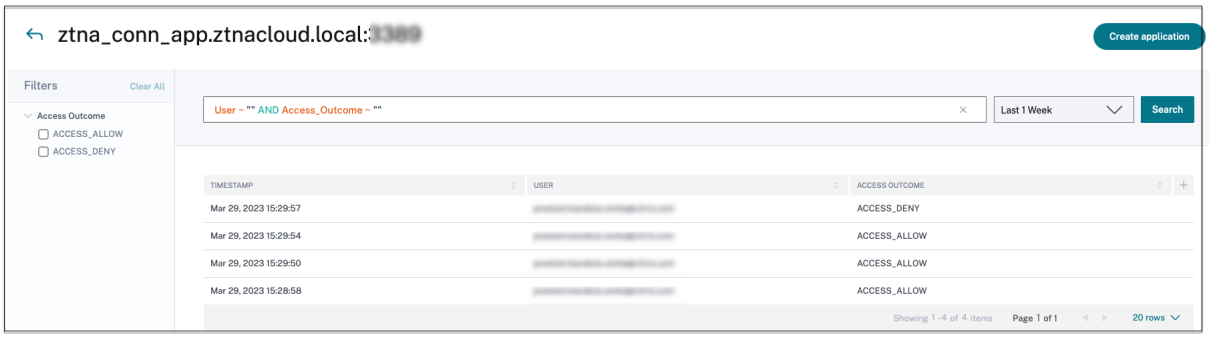
Haga clic en el icono **+** en línea con el dominio correspondiente para crear una aplicación. Aparece el asistente de configuración de la aplicación. El icono de creación de aplicación no aparece en las filas en las que ya se ha creado una aplicación con la misma combinación de dominio, puerto y protocolo y está en estado completo.

- El tipo de aplicación se rellena automáticamente según el protocolo de la aplicación que haya seleccionado. Sin embargo, puede cambiar el tipo si es necesario.
- Los valores de los campos **URL, Dominios relacionados, Destino, Puerto y Protocolo** se rellenan automáticamente. Complete los pasos para agregar una aplicación. Para obtener más información, consulte Flujo de trabajo guiado por el administrador para facilitar la incorporación y su configuración.





También puede hacer clic en el enlace de dominio único para ver más detalles y crear una aplicación para ese dominio. Al hacer clic en un enlace de dominio, se muestran los registros de autenticación de usuario del dominio. Haga clic en el botón **Crear aplicación**. Complete los pasos para agregar una aplicación.



Operadores de búsqueda

Los siguientes son los operadores de búsqueda que puede utilizar para refinar la búsqueda en las tablas Registros de **usuario** y **Políticas de acceso principal por** cumplimiento .

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

Detección de aplicaciones

December 27, 2023

La función de detección de aplicaciones ayuda al administrador a ver las aplicaciones privadas internas, como las aplicaciones web y las aplicaciones cliente-servidor (aplicaciones basadas en TCP y UDP) de su organización, y a los usuarios que acceden a esas aplicaciones. Los administradores pueden detectar las aplicaciones especificando el alcance de los dominios (dominios comodín) o las subredes IP. Para habilitar la función de detección de aplicaciones en Citrix Secure Private Access Service, los administradores deben configurar las subredes o los dominios comodín, o ambos, en los que se deben detectar e informar sobre el acceso de las aplicaciones y los usuarios. Los administradores utilizan el flujo de trabajo de configuración de aplicaciones para definir las subredes amplias y los dominios comodín y completar el mismo flujo de trabajo de directivas de acceso a las aplicaciones que se utiliza para todas las configuraciones de definición de aplicaciones.

Configurar la detección de aplicaciones

La detección de aplicaciones se puede realizar de una de las siguientes maneras:

- Configure el sistema para supervisar e informar sobre los destinos y puertos exactos de las direcciones IP basados en TCP/UDP.

  Especifique la subred junto con el protocolo TCP/UDP y el rango de puertos (introduzca * para incluir el rango completo). Esto permite detectar todas las aplicaciones TCP y UDP desde el agente de acceso seguro.

  Ejemplo: 10.0.0.0/8: TCP: Puerto (*)

- Configure el sistema para supervisar e informar sobre los nombres de host o los dominios totalmente cualificados (FQDN) o ambos de las aplicaciones a las que se accede mediante el protocolo TCP o UDP.

  Especifique el dominio comodín que pertenece a las aplicaciones web que se deben monitorear e informar.

  Ejemplo:`*.citrix.com : TCP : Port (*)`

- Configure el sistema para supervisar e informar sobre los dominios totalmente cualificados (FQDN) a los que se puede acceder desde el navegador empresarial de Citrix.

  Especifique al menos un FQDN para una aplicación web que pertenezca al dominio o subdominio en el que quiere detectar las aplicaciones web internas. Configure el dominio relacionado para incluir el dominio comodín al que pertenece esa aplicación.

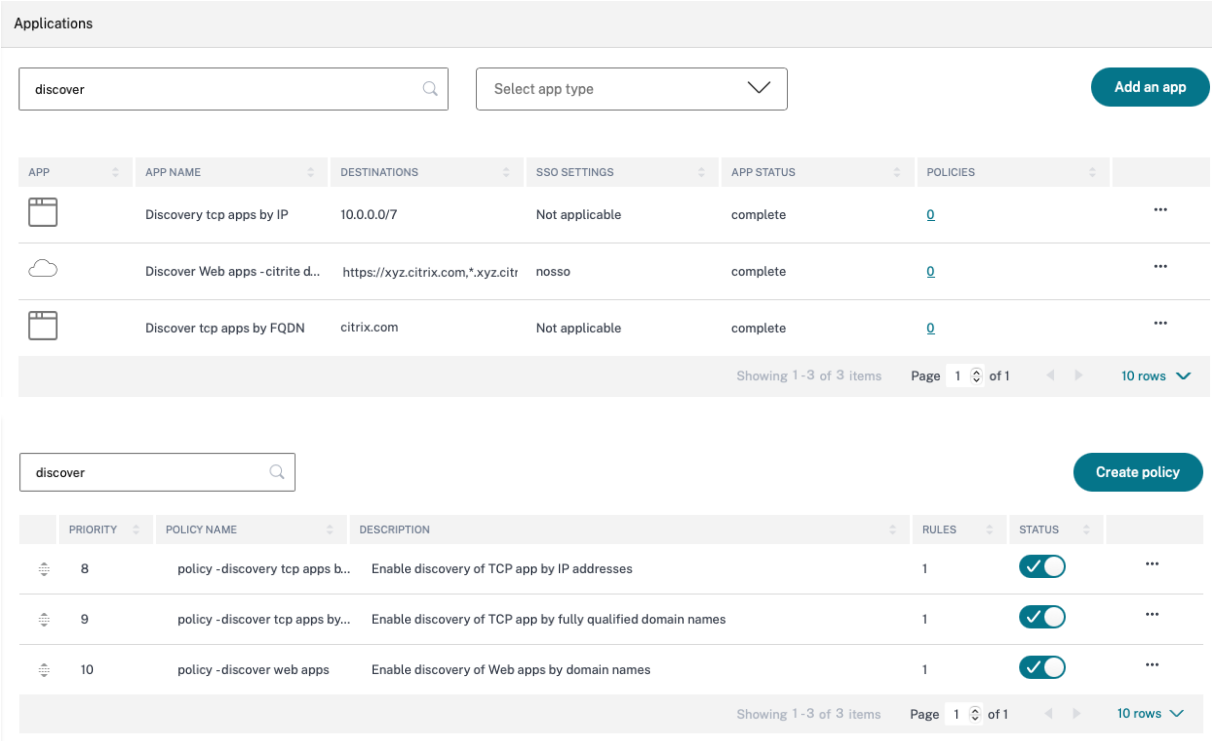
  Ejemplo:

  URL de la aplicación web: `https://test.citrix.com/`

  Dominio relacionado: *.citrix.com

Importante:

- Además de crear las aplicaciones, también debe definir los usuarios a los que se les permite el acceso a las aplicaciones con los dominios y las subredes IP configurados. Esto se hace para evitar el acceso no autorizado o involuntario de otros grupos de usuarios que se encuentran fuera de los grupos de usuarios permitidos.
- Agregue el prefijo **Discover** en el nombre de la aplicación para indicar que se trata de una configuración de aplicación especial para permitir la supervisión y la generación de informes de detecciones. Esta denominación le ayuda a identificar y eliminar los dominios comodín o las subredes IP, o ambos, de modo que pueda reducir la zona de acceso general a la aplicación a solo los FQDN específicos y las combinaciones IP/puerto más adelante, en unas semanas o un mes.



Tras crear las aplicaciones y las directivas de acceso correspondientes, los usuarios pueden seguir accediendo a las aplicaciones desde la aplicación Citrix Workspace y acceder a diferentes dominios. Para acceder a las aplicaciones TCP/UDP, los usuarios deben usar el agente Citrix Secure Access. El acceso a las aplicaciones desde varios métodos de acceso se monitorea en función de la configuración de los dominios y subredes de las aplicaciones y se informa en los paneles.

Configuración y administración de aplicaciones

December 27, 2023

La entrega de aplicaciones mediante el servicio Citrix Secure Private Access le proporciona una solución fácil, segura, sólida y escalable para administrar las aplicaciones. Las aplicaciones que se entregan en la nube tienen las siguientes ventajas:

- Configuración simple: Fácil de operar, actualizar y consumir.
- Single Sign-On: Inicios de sesión sin complicaciones con Single Sign-On.
- Plantilla estándar para diferentes aplicaciones SaaS: configuración basada en plantillas de aplicaciones populares. Estas plantillas rellenan previamente gran parte de la información requerida para configurar las aplicaciones. Solo se debe proporcionar la información específica del cliente.

Support for Enterprise web apps

February 16, 2024

La entrega de aplicaciones web mediante el servicio Secure Private Access permite que las aplicaciones específicas de la empresa se entreguen de forma remota como un servicio basado en la web. Las aplicaciones web más utilizadas incluyen SharePoint, Confluence, OneBug, etc.

Se puede acceder a las aplicaciones web mediante Citrix Workspace mediante el servicio Secure Private Access. El servicio Secure Private Access, junto con Citrix Workspace, proporciona una experiencia de usuario unificada para las aplicaciones web configuradas, las aplicaciones SaaS, las aplicaciones virtuales configuradas o cualquier otro recurso del espacio de trabajo.

El SSO y el acceso remoto a aplicaciones web están disponibles como parte de los siguientes paquetes de servicios:

- Secure Private Access estándar
- Secure Private Access avanzado

Requisitos del sistema

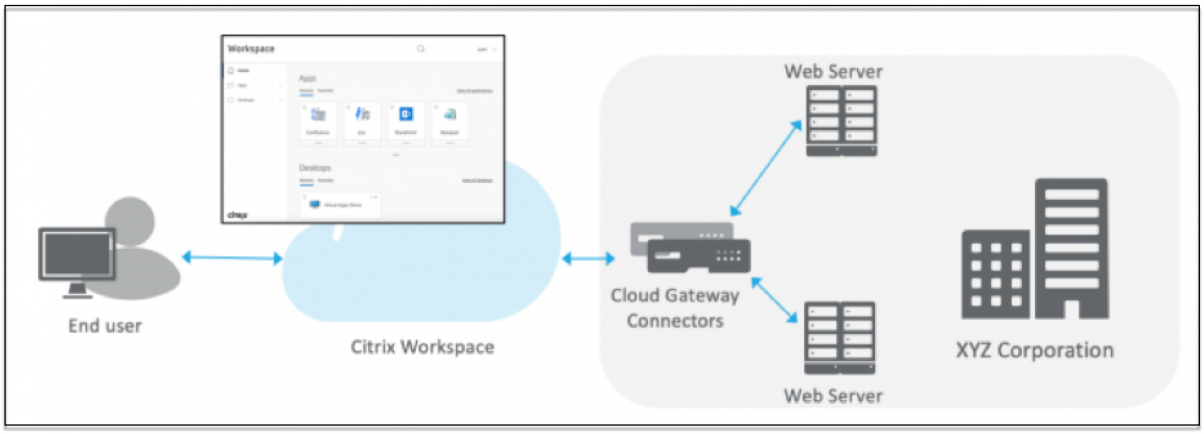
Connector Appliance: Utilice el Connector Appliance con Citrix Secure Private Access Service para permitir el acceso sin VPN a las aplicaciones web empresariales en el centro de datos de los clientes. Para obtener más información, consulte Secure Workspace Access with Connector Appliance.

Funcionamiento

El Citrix Secure Private Access Service se conecta de forma segura al centro de datos local mediante el conector, que se implementa en las instalaciones. Este conector actúa como un puente entre las aplicaciones web empresariales implementadas en las instalaciones y el Citrix Secure Private Access Service. Estos conectores se pueden implementar en un par de alta disponibilidad y solo requieren una conexión saliente.

Una conexión TLS entre el Connector Appliance y Citrix Secure Private Access Service en la nube protege las aplicaciones locales que se enumeran en el servicio en la nube. Se accede a las aplicaciones web y se entregan a través de Workspace mediante una conexión sin VPN.

En la siguiente ilustración se muestra cómo acceder a las aplicaciones web mediante Citrix Workspace.



Configurar una aplicación web

La configuración de una aplicación web implica los siguientes pasos de alto nivel.

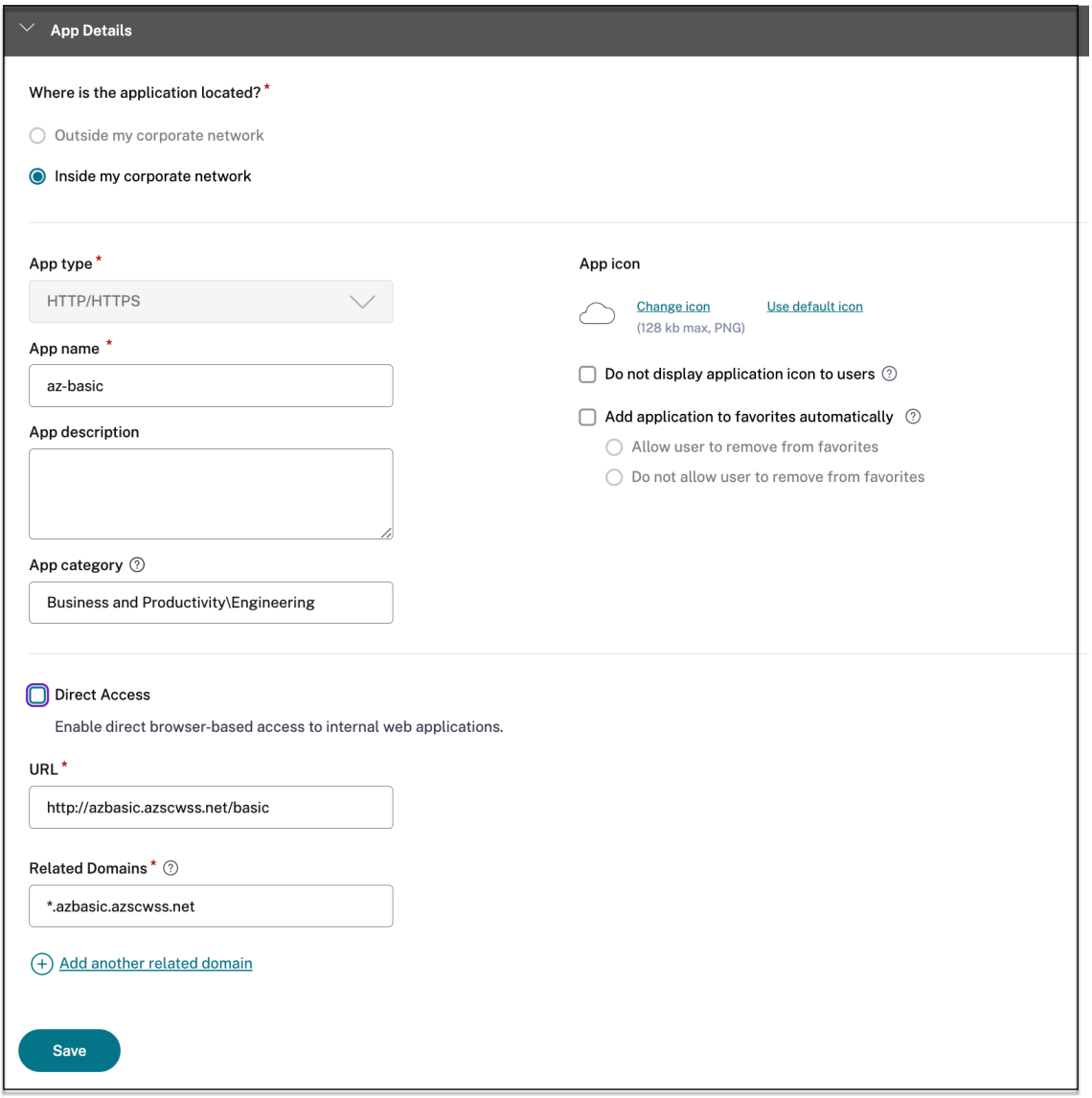
1. Configurar los detalles de la aplicación
2. Configurar el método de inicio de sesión preferido
3. Defina el enrutamiento de aplicaciones

Configurar los detalles de la aplicación

1. En el mosaico **Secure Private Access**, haga clic en **Administrar.**
2. En la página de inicio de Secure Private Access, haga clic en **Continuar** y, a continuación, en **Agregar una aplicación.**

   > **Nota:**
   >
   > El botón **Continuar** solo aparece la primera vez que utilice el asistente. En los usos posteriores, puede navegar directamente a la página **Aplicaciones** y, a continuación, hacer clic en **Agregar una aplicación**.

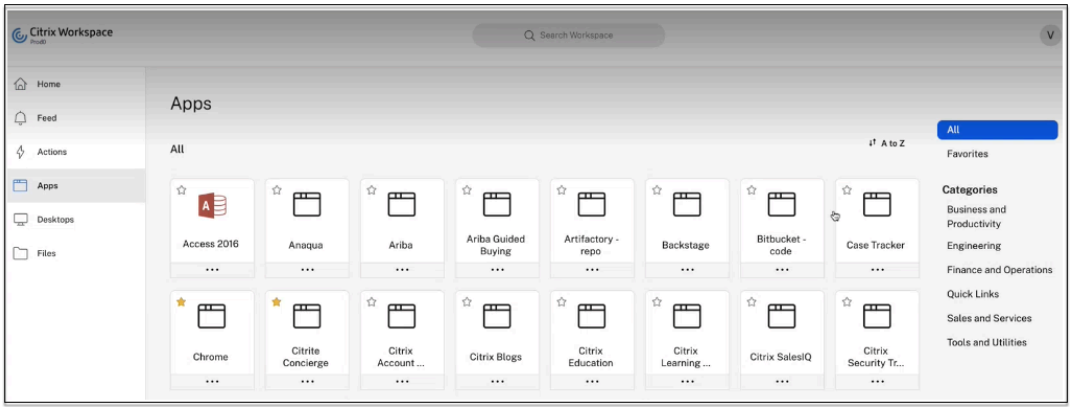
3. Seleccione la aplicación que quiera agregar y haga clic en **Omitir.**
4. En **¿Dónde está la ubicación de la aplicación?**, selecciona la ubicación.
5. Introduzca los siguientes detalles en la sección **Detalles de la aplicación** y haga clic en **Siguiente.**



- **Tipo de aplicación**: Seleccione el tipo de aplicación. Puede seleccionar aplicaciones **HTTP/HTTPS** o **UDP/TCP**.
- **Nombre de la aplicación**: Nombre de la aplicación.
- **Descripción de la aplicación** : una breve descripción de la aplicación. La descripción que introduzcas aquí se mostrará a los usuarios del espacio de trabajo.
- **Categoría de aplicación** : agregue la categoría y el nombre de la subcategoría (si corresponde) con los que debe aparecer la aplicación que va a publicar en la interfaz de usuario de Citrix Workspace. Puede agregar una nueva categoría para cada aplicación o usar las categorías existentes de la interfaz de usuario de Citrix Workspace. Una vez que especifiques una categoría para una aplicación web o SaaS, la aplicación aparecerá en la interfaz de usuario de Workspace en la categoría específica.

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

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



- **Icono de la aplicación**: Haga clic en **Cambiar icono** para cambiar el icono de la aplicación. El tamaño del archivo de iconos debe ser de 128 x 128 píxeles. Si no cambia el icono, se muestra el icono predeterminado.

  Si no desea mostrar el icono de la aplicación, seleccione **No mostrar el icono de la aplicación a los usuarios.**

- Seleccione **Acceso directo** para permitir que los usuarios accedan a la aplicación directamente desde el explorador de un cliente. Para obtener más información, consulte Acceso directo a aplicaciones web empresariales.

- **URL**: URL con su ID de cliente. La URL debe contener su ID de cliente (ID de cliente de Citrix Cloud). Para obtener su ID de cliente, consulte Inscribirse en Citrix Cloud. En caso de que Single Sign-On falle o no quiera utilizar Single Sign-On, se redirigirá al usuario a esta URL.

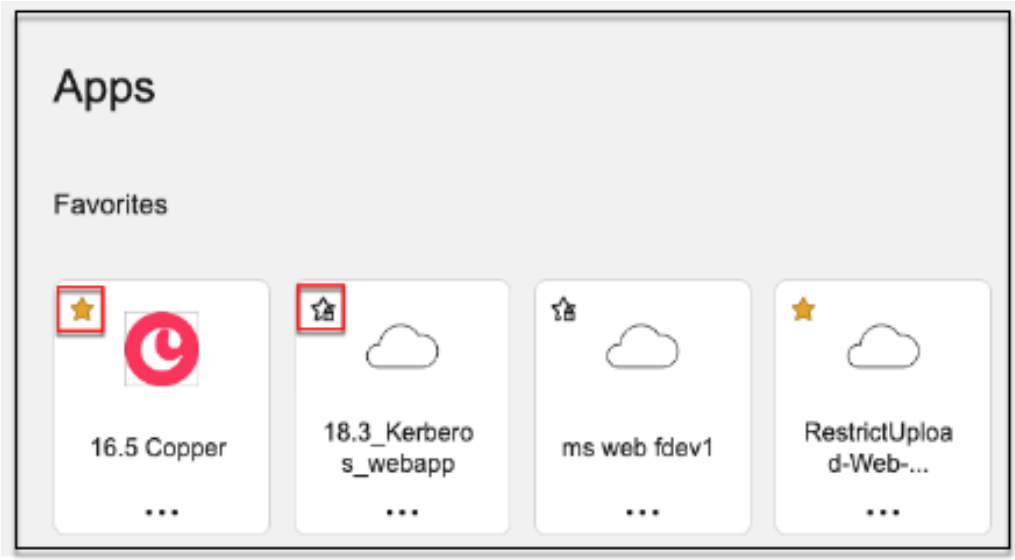
  Nombre de dominio del cliente e **ID de dominio del cliente**: El nombre y el ID de dominio del cliente se utilizan para crear la URL de aplicación y otras URL posteriores en la página

de inicio de sesión único de SAML.

Por ejemplo, si va a agregar una aplicación de Salesforce, su nombre de dominio es `salesforceformyorg` y el ID es 123754, entonces la URL de la aplicación es `https://salesforceformyorg.my.salesforce.com/?so=123754`.

Los campos Nombre de dominio del cliente e ID de cliente son específicos de determinadas aplicaciones.

- **Dominios relacionados** : el dominio relacionado se rellena automáticamente en función de la URL que has proporcionado. El dominio relacionado ayuda al servicio a identificar la URL como parte de la aplicación y a dirigir el tráfico en consecuencia. Puede agregar más de un dominio relacionado.
- Haga clic en **Agregar aplicación a favoritos automáticamente** para agregar esta aplicación como favorita en la aplicación Citrix Workspace.
  - Haga clic en **Permitir al usuario eliminarla de favoritos** para permitir que los suscriptores de la aplicación eliminen la aplicación de la lista de aplicaciones favoritas de la aplicación Citrix Workspace. Al seleccionar esta opción, aparece un icono de estrella amarilla en la esquina superior izquierda de la aplicación en la aplicación Citrix Workspace.
  - Haga clic en **No permitir que el usuario elimine de favoritos** para evitar que los suscriptores eliminen la aplicación de la lista de aplicaciones favoritas de la aplicación Citrix Workspace. Al seleccionar esta opción, aparece un icono de estrella con un candado en la esquina superior izquierda de la aplicación en la aplicación Citrix Workspace.



Si elimina las aplicaciones marcadas como favoritas de la consola del servicio Secure Private Access, estas aplicaciones deben eliminarse manualmente de la lista de fa-

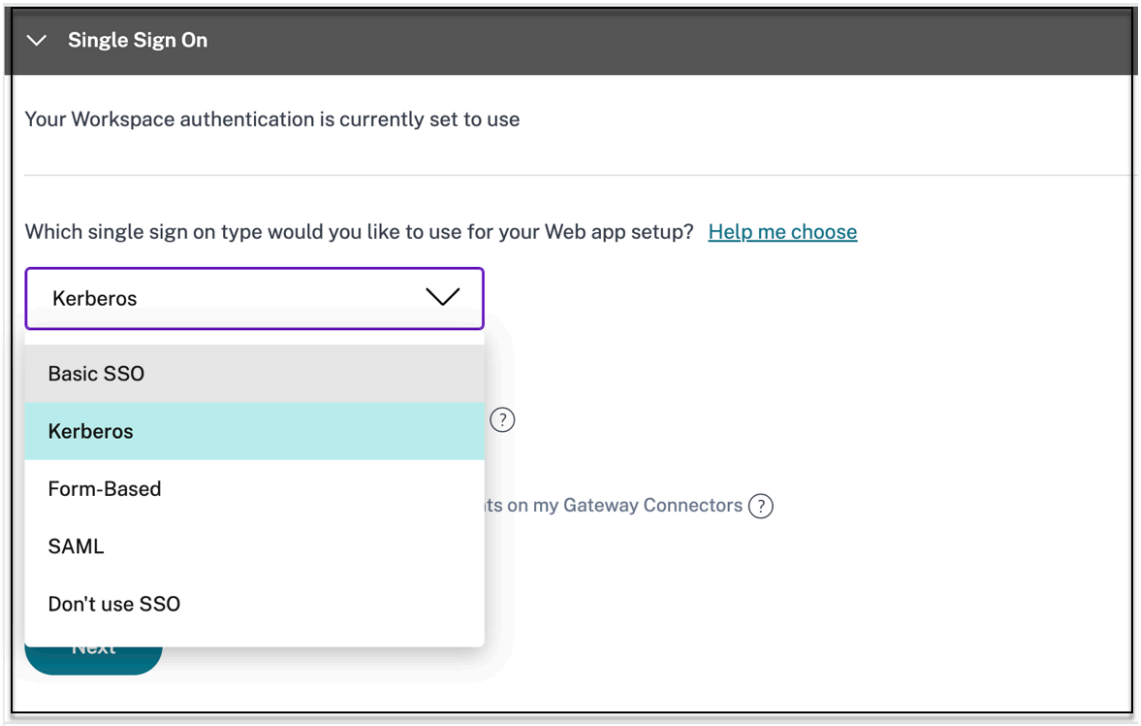
voritos de Citrix Workspace. Las aplicaciones no se eliminan automáticamente de la aplicación Workspace si se eliminan de la consola de servicio de Secure Private Access.

6. Haz clic en **Siguiente.**

> **Importante:**
>
> - Para habilitar el acceso basado en la confianza cero a las aplicaciones, se deniega el acceso a las aplicaciones de forma predeterminada. El acceso a las aplicaciones solo está habilitado si hay una directiva de acceso asociada a la aplicación. Para obtener más información, consulta Acceso denegado a las aplicaciones de forma predeterminada.
> - Si se configuran varias aplicaciones con el mismo FQDN o con alguna variación del FQDN comodín, esto podría provocar un conflicto de configuración. Para obtener más información, consulta Configuración conflictiva que podría ocasionar problemas de acceso a las aplicaciones.

Configurar el método de inicio de sesión preferido

1. En la sección **Single Sign-On**, seleccione el tipo de Single Sign-On que prefiera para usarlo en su aplicación y haga clic en **Guardar**. Están disponibles los siguientes tipos de inicio de sesión único.

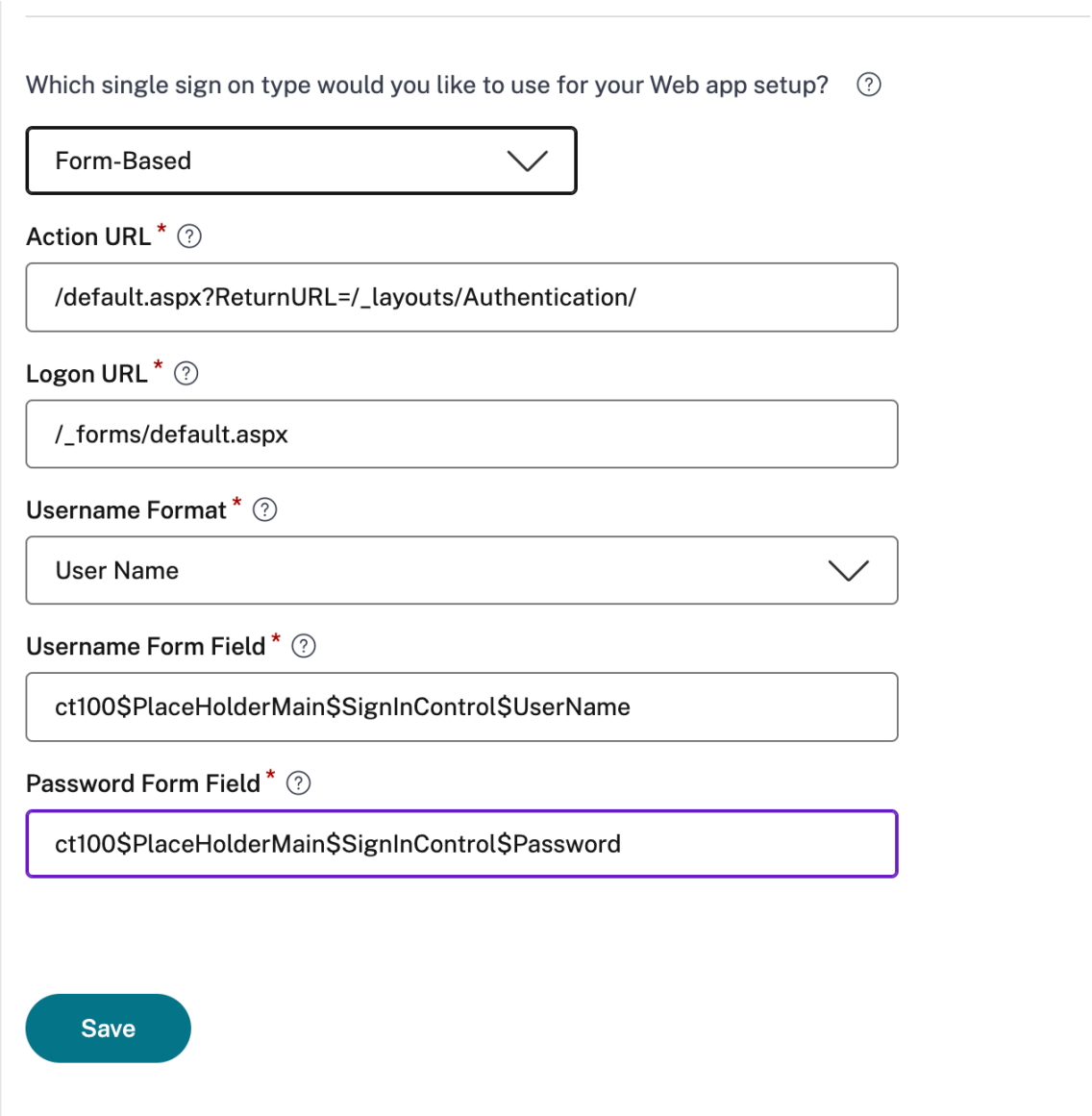


- **Básico**: Si su servidor back-end le presenta un desafío básico 401, elija **SSO básico**. No es

necesario que proporciones ningún detalle de configuración para el tipo de SSO **básico**.

- **Kerberos**: Si su servidor back-end le presenta el desafío negotiate-401, elija **Kerberos**. No es necesario que proporcione ningún detalle de configuración para el tipo de **SSO Kerberos**.
- **Basado en formularios**: Si el servidor back-end le presenta un formulario HTML para la autenticación, elija **Basado en formularios**. Introduzca los detalles de configuración del tipo de SSO **basado en formularios**.
- **SAML**: Elija **SAML** para Single Sign-On basado en SAML en aplicaciones web. Introduzca los detalles de configuración para el tipo de SSO de **SAML** .
- **No usar SSO**: Use la opción **No usar SSO** cuando no necesite autenticar a un usuario en el servidor back-end. Cuando se selecciona la opción **No usar SSO**, se redirige al usuario a la URL configurada en la sección **Detalles de la aplicación**.

Detalles basados en formularios: introduzca los siguientes detalles de configuración basados en formularios en la sección Inicio de sesión único y haga clic en Guardar.



- **URL de acción**: Escriba la dirección URL a la que se envía el formulario completado.
- **URL del formulario de inicio de sesión**: Escriba la URL en la que se presenta el formulario de inicio de sesión.
- **Formato de nombre de usuario**: Seleccione un formato para el nombre de usuario.
- **Campo de formulario de nombre** de usuario: escriba un atributo de nombre de usuario.
- **Campo de formulario de contraseña**: Escriba un atributo de contraseña.

SAML: introduce los siguientes detalles en la sección Iniciar sesión y haga clic en Guardar.

Which single sign on type would you like to use for your Web app setup?

SAML

SAML information

This form generates the XML needed for the application's SAML request.

Sign Assertion *

Assertion

Assertion URL *

https://sharepoint.onelogin/saml_assertion

Relay State

&RelayState = /apex/SSO_Redirect?param1=value1

Audience

Name ID Format *

Email Address

Name ID *

User Name

Launch the app using the specified URL (SP initiated)

- **Afirmación** de firmas: la firma de afirmación o respuesta garantiza la integridad del mensaje cuando la respuesta o afirmación se entrega a la parte que confía (SP). Puede seleccionar **Afirmación, Respuesta, Ambas** o **Ninguna**.
- **URL de aserción**: El proveedor de la aplicación proporciona la URL de aserción. La aserción SAML se envía a esta URL.
- **Estado de retransmisión** : el parámetro Estado de retransmisión se usa para identificar el recurso específico al que acceden los usuarios después de iniciar sesión y dirigirlos al servidor de federación de la parte que confía. Relay State genera una única URL para los usuarios. Los usuarios pueden hacer clic en esta URL para iniciar sesión en la aplicación de destino.
- **Audiencia**: El proveedor de la aplicación proporciona la audiencia. Este valor confirma

que la aserción SAML se ha generado para la aplicación correcta.

- **Formato de ID de nombre**: Seleccione el formato de identificador de nombre admitido.
- **ID de nombre**: Seleccione el ID de nombre admitido.

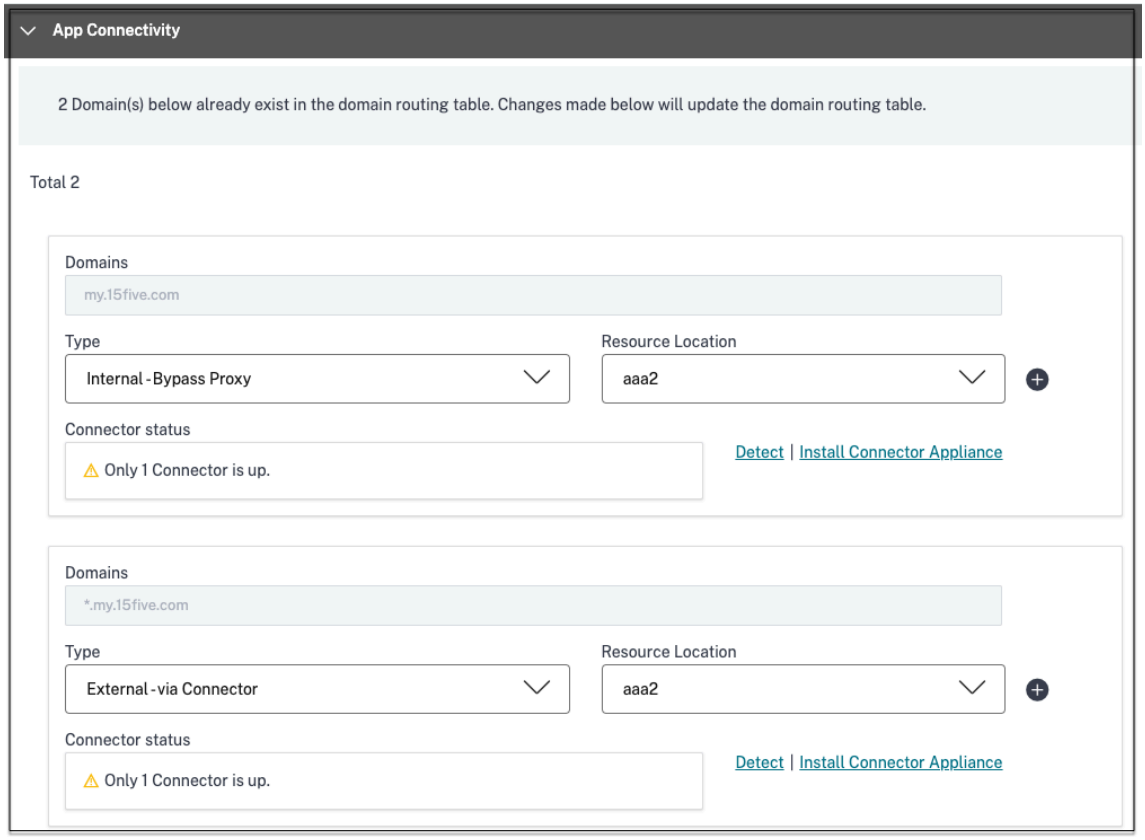
2. En **Atributos avanzados (opcional)**, agregue información adicional sobre el usuario que se envía a la aplicación para tomar decisiones de control de acceso.
3. Descargue el archivo de metadatos haciendo clic en el enlace situado debajo de **Metadatos SAML.** Utilice el archivo de metadatos descargado para configurar el SSO en el servidor de aplicaciones SaaS.

   > **Nota:**
   >
   > - Puede copiar la URL de inicio de sesión único en URL de inicio de **sesión** y utilizarla al configurar Single Sign-On en el servidor de aplicaciones SaaS.
   > - También puede descargar el certificado de la lista de **certificados** y utilizarlo al configurar el inicio de sesión exclusivo en el servidor de aplicaciones SaaS.

4. Haz clic en **Siguiente.**

Defina el enrutamiento de aplicaciones

1. En la sección **Conectividad de aplicaciones**, defina el enrutamiento para los dominios relacionados de las aplicaciones, si los dominios deben enrutarse externa o internamente a través de Citrix Connector Appliance. Para obtener más información, consulte Tablas de redirección para resolver conflictos si los dominios relacionados en las aplicaciones web y SaaS son los mismos.

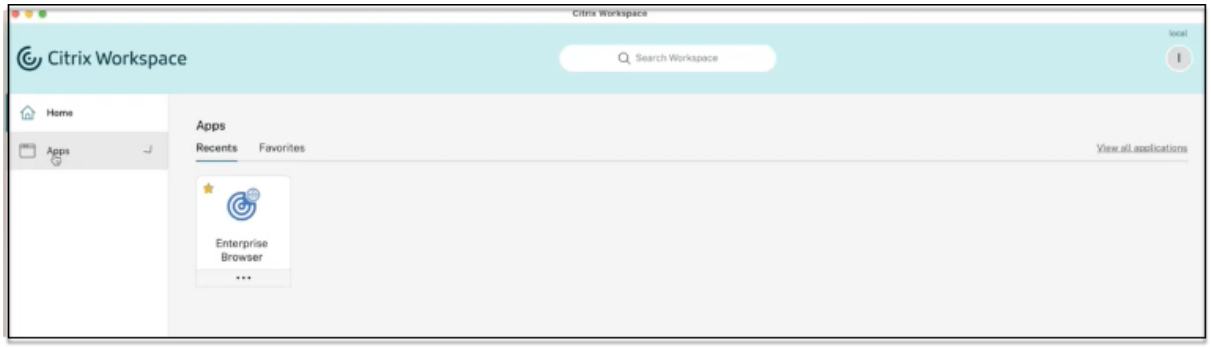


2. Haz clic en **Finalizar.**

   Después de hacer clic en **Finalizar**, la aplicación se agrega a la página Aplicaciones. Puedes editar o eliminar una aplicación desde la página Aplicaciones después de configurarla. Para hacerlo, haga clic en el botón de puntos suspensivos de una aplicación y seleccione las acciones correspondientes.

   - **Modificar aplicación**
   - **Eliminar**

Al publicar una aplicación web o SaaS desde el servicio Secure Private Access y si esa aplicación no está oculta, la aplicación Citrix Enterprise Browser aparece automáticamente en la interfaz de usuario de Citrix Workspace. Además, Citrix Enterprise Browser también se agrega como aplicación favorita de forma predeterminada. Los usuarios finales pueden iniciar el explorador del espacio de trabajo sin una URL y acceder a los sitios web internos mediante los navegadores del espacio de trabajo.



> **Importante:**
>
> - Para conceder acceso a las aplicaciones a los usuarios, los administradores deben crear directivas de acceso. En las directivas de acceso, los administradores agregan suscriptores a la aplicación y configuran los controles de seguridad. Para obtener más información, consulte Crear directivas de acceso.

Dispositivo conector para Secure Private Access

February 16, 2024

El Connector Appliance es un componente de Citrix alojado en el hipervisor. Funciona como un canal de comunicaciones entre Citrix Cloud y las ubicaciones de recursos, lo que permite administrar la nube sin necesidad de una configuración compleja de la red o de la infraestructura. El Connector Appliance permite administrar y centrarse en los recursos que ofrecen más valor a los usuarios.

Todas las conexiones se establecen desde el Connector Appliance hacia la nube mediante el puerto HTTPS estándar (443) y el protocolo TCP. No se aceptan conexiones entrantes. El puerto TCP 443, con los siguientes FQDN, se permite la salida:

- *.nssvc.net
- *.netscalermgmt.net
- *.citrixworkspacesapi.net
- *.citrixnetworkapi.net
- *.citrix.com
- *.servicebus.windows.net
- *.adm.cloud.com

Configuración del acceso privado seguro con Connector Appliance

1. Instale dos o más dispositivos de conexión en la ubicación de recursos.

Para obtener más información sobre la configuración de los Connector Appliances, consulte Connector Appliance para Cloud Services.

2. Para configurar Secure Private Access para conectarse a aplicaciones web locales mediante KCD, configure KCD realizando los siguientes pasos:

   a) Una el Connector Appliance a un dominio de Active Directory.

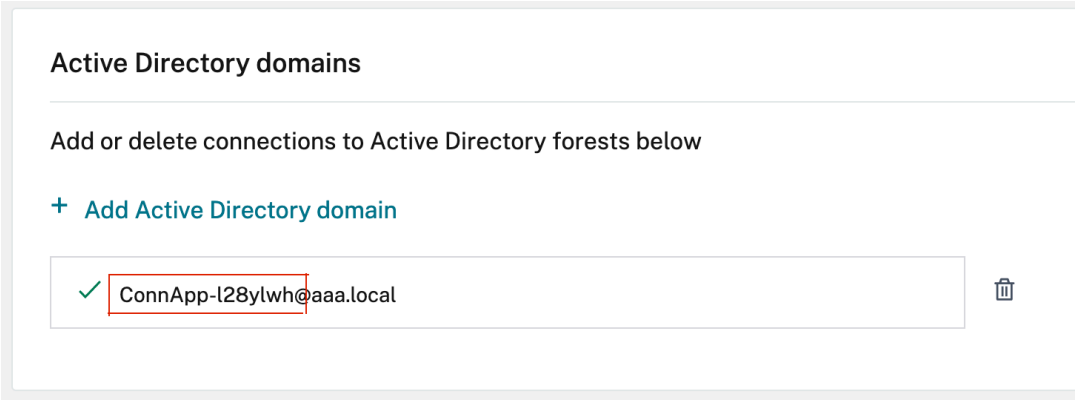
      Unirse a un bosque de Active Directory le permite usar la delegación limitada de Kerberos (KCD) al configurar Secure Private Access, pero no permite las solicitudes de identidad ni la autenticación para usar el Connector Appliance.

      - Conéctese a la página web de administración de Connector Appliances en su explorador web mediante la dirección IP proporcionada en la consola de Connector Appliance.
      - En la sección **Dominios de Active Directory**, haga clic en **+ Agregar dominio de Active Directory**.

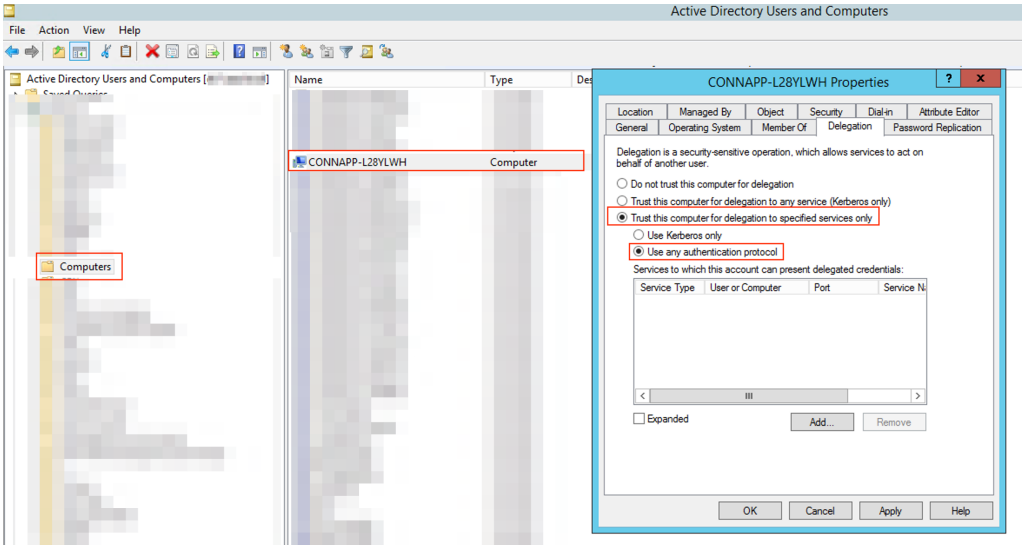
        Si no tiene una sección de **dominios de Active Directory** en la página de administración, contacte con Citrix para solicitar la inscripción en la función Tech Preview.
      - Introduzca el nombre de dominio en el campo **Nombre de dominio**. Haga clic en **Agregar**.
      - Connector Appliance comprueba el dominio. Si la comprobación se realiza correctamente, se abre el cuadro de diálogo **Unirse a Active Directory**.
      - Introduzca el nombre de usuario y la contraseña de un usuario de Active Directory que tenga permiso para unirse a este dominio.
      - Connector Appliance sugiere un nombre de máquina. Si quiere, puede reemplazar el nombre sugerido y proporcionar su propio nombre de máquina (hasta 15 caracteres de longitud). Anote el nombre de la cuenta de la máquina.

        El nombre de esta máquina se crea en el dominio de Active Directory cuando el Connector Appliance se une a él.
      - Haga clic en **Unirse**.

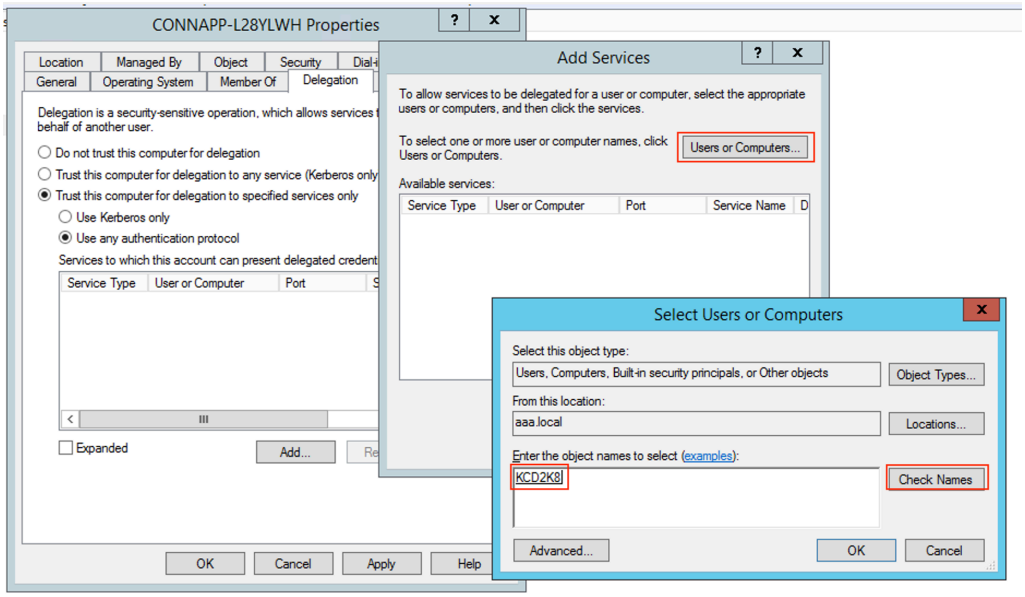
   b) Configure la delegación de restricciones Kerberos para el servidor web sin un equilibrador de carga.



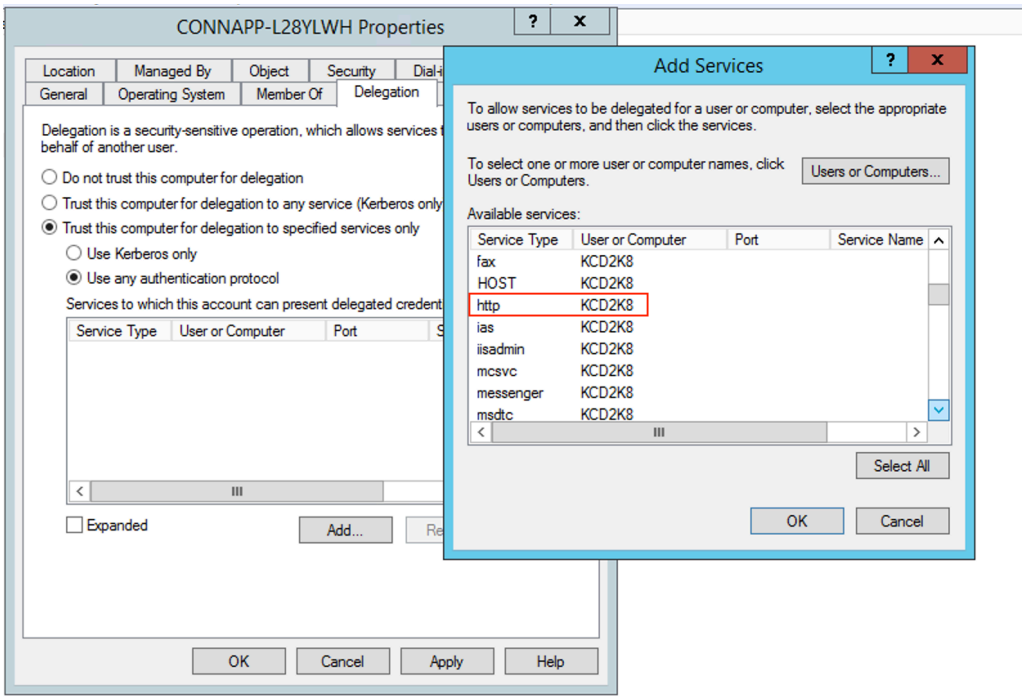
- Identifique el nombre del equipo del dispositivo conector. Puede obtener este nombre desde el lugar donde lo alojó o simplemente desde la interfaz de usuario del conector.
- En la controladora de Active Directory, busque el equipo del dispositivo conector.
- Vaya a las propiedades de la cuenta de equipo del Connector Appliance y vaya a la ficha **Delegación**.
- Elija **Confiar en el equipo para la delegación solo a los servicios especificados.** y, a continuación, selecciona **Usar cualquier protocolo de autenticación.**



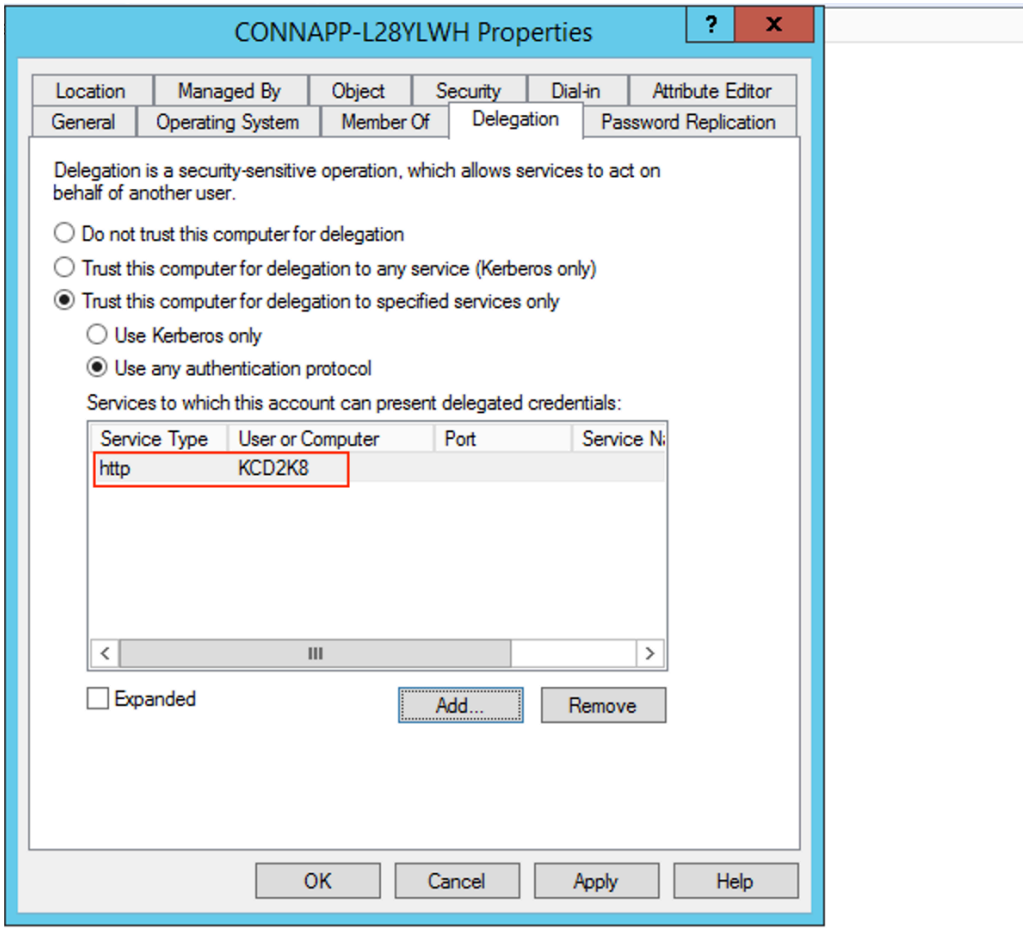
- Haz clic en **Agregar.**
- Haga clic en **Usuarios o equipos.**
- Introduzca el nombre del equipo del servidor web de destino y, a continuación, haga clic en **Comprobar nombres.** En la imagen anterior, **KCD2K8** es el servidor web.



- haga clic en **Aceptar.**
- Seleccione el tipo de servicio **http.**



- Haga clic en **Aceptar**.
- Haga clic en **Aplicar**y, a continuación, en Aceptar .

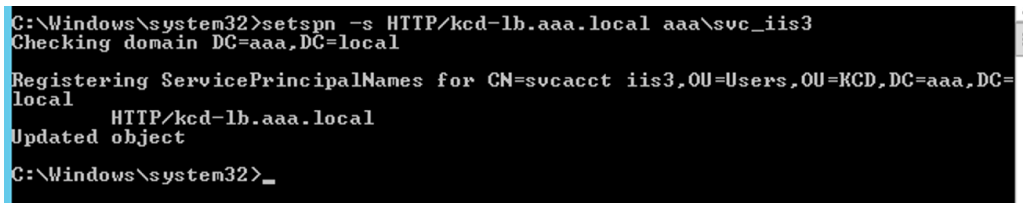


Esto completa el procedimiento para agregar la delegación de un servidor web.

c) Configure la delegación de restricciones Kerberos (KCD) para un servidor web detrás de un equilibrador de carga.

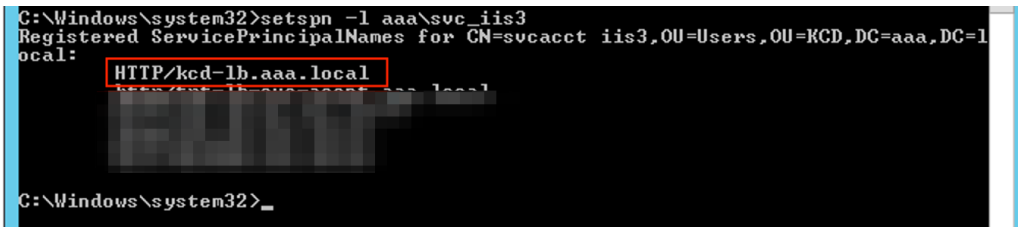
- Agregue el SPN del equilibrador de cargas a la cuenta de servicio mediante este comando `setspn`.

  `setspn -S HTTP/<web_server_fqdn> <service_account>`

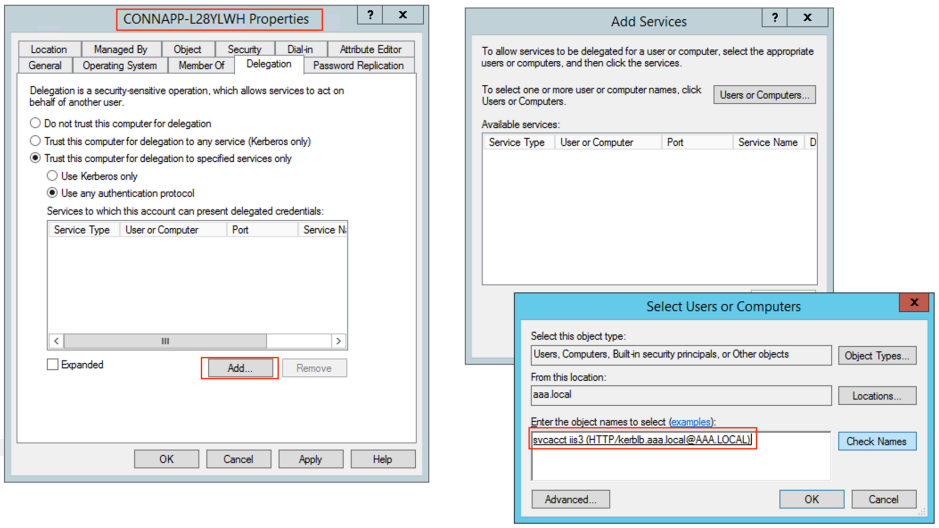


- Confirme los SPN de la cuenta de servicio mediante el siguiente comando.

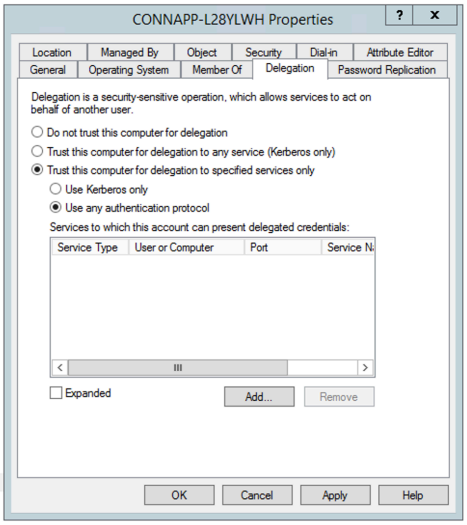
  `setspn -l <service_account>`

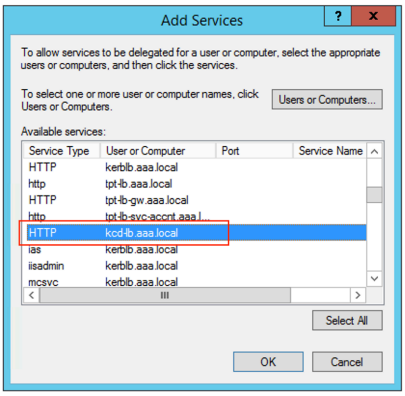


- Cree una delegación para la cuenta de equipo del dispositivo conector.
  - Siga los pasos para *configurar la delegación de restricciones Kerberos para el servidor web* sin un equilibrador de carga para identificar la máquina de CA y navegar hasta la interfaz de usuario de delegación.
  - En Seleccionar **Usuarios y equipos**, seleccione la cuenta de servicio (por ejemplo, aaa\ svc_iis3).

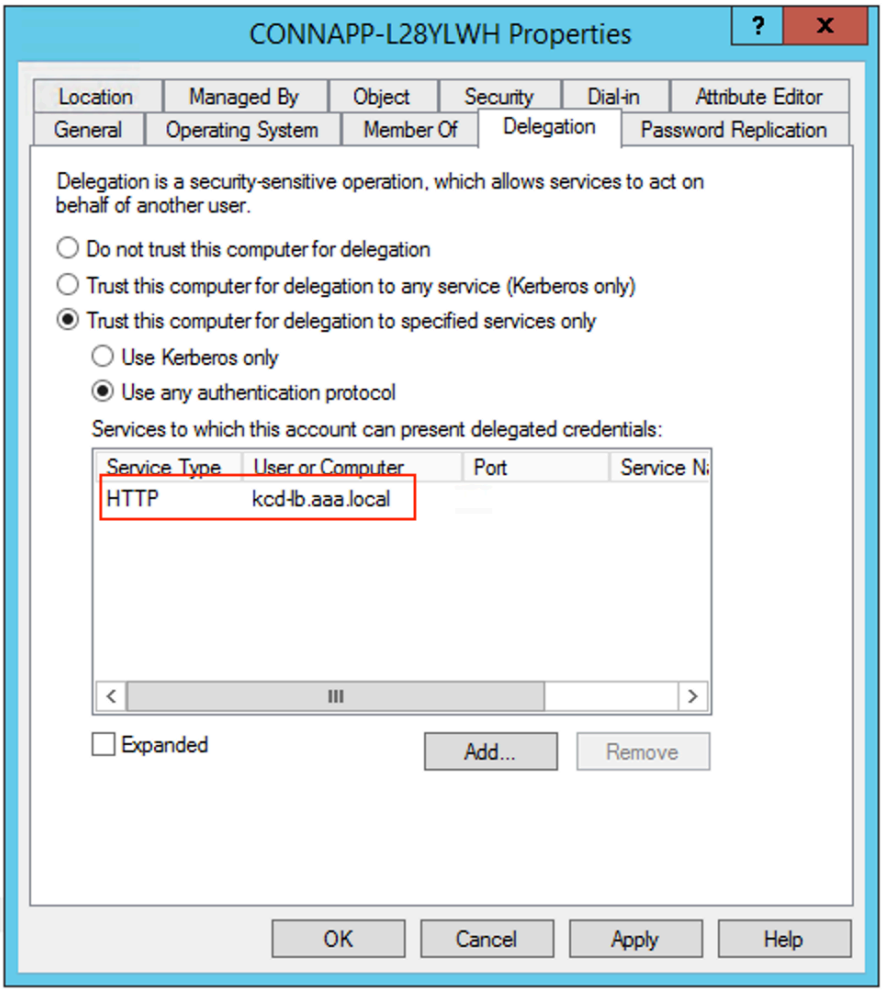


  - En los servicios, seleccione la entrada **ServiceType: HTTP** y User or Computer: web server (por ejemplo, `kcd-lb.aaa.local`)





- Haga clic en **Aceptar**.
- Haga clic en **Aplicar**y**,** a continuación, en Aceptar .

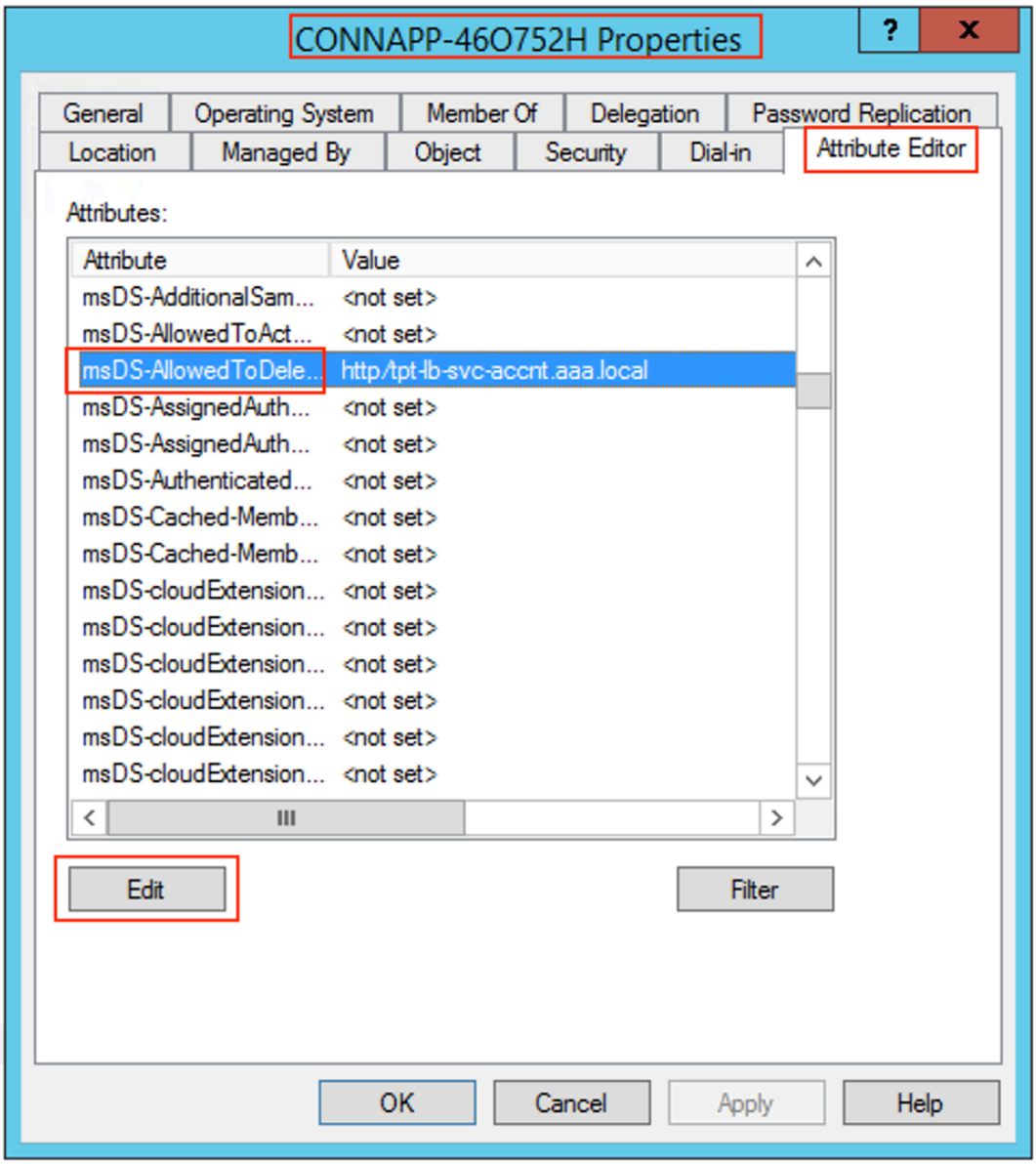


d) Configure la delegación restringida de Kerberos (KCD) para una cuenta de servicio administrada por grupo.

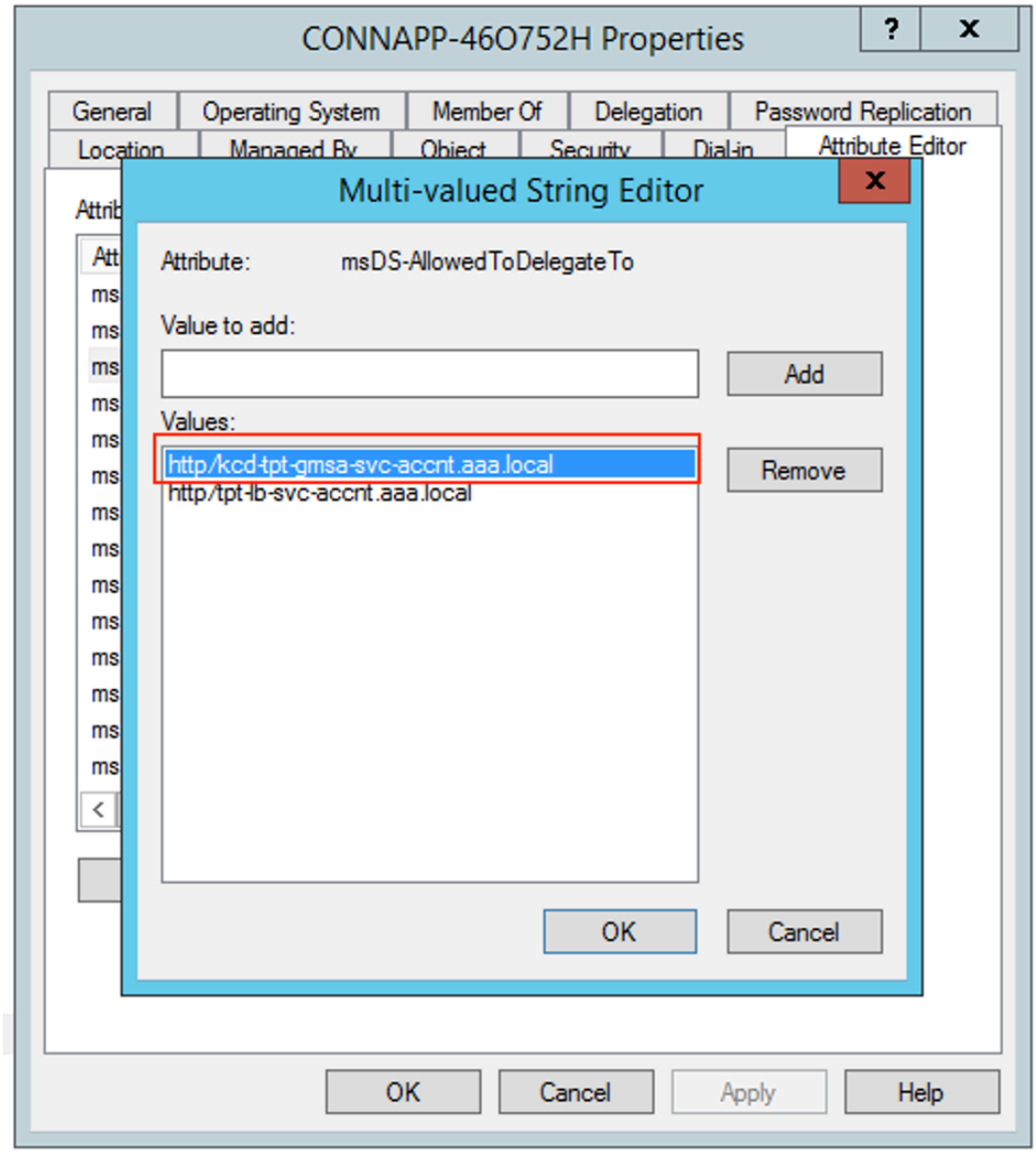
- Agregue SPN a la cuenta de servicio administrado del grupo si aún no lo ha hecho.
  `setspn -S HTTP/<web_server_fqdn> <group_manged_service_account>`
- Confirme el SPN con el siguiente comando.
  `setspn -l <group_manged_service_account>`

Dado que la cuenta de servicio administrado por grupo no se puede mostrar en la búsqueda de `Users and Computers` mientras se agrega la entrada de delegación para la cuenta de equipo, no se puede agregar la delegación de una cuenta de equipo mediante el método habitual. Por lo tanto, puede agregar este SPN como entrada delegada a la cuenta de equipo de la CA mediante el editor de atributos.

- En las propiedades del equipo del Connector Appliance, vaya a la ficha **Editor de atributos** y busque el atributo `msDA-AllowedToDeleteTo`.
- Modifique `msDA-AllowedToDeleteTo attribute` y, a continuación, agregue el SPN.



)



)

e) Migre del NetScaler Gateway Connector al dispositivo Citrix Connector.

- Como los SPN ya están configurados en la cuenta de servicio al configurar el conector de puerta de enlace, no es necesario agregar más SPN para la cuenta de servicio si no se ha configurado una nueva aplicación kerberos. Puede ver la lista de todos los SPN asignados a la cuenta de servicio siguiendo el comando y asignarlos como entradas delegadas para la cuenta de equipo de la CA.

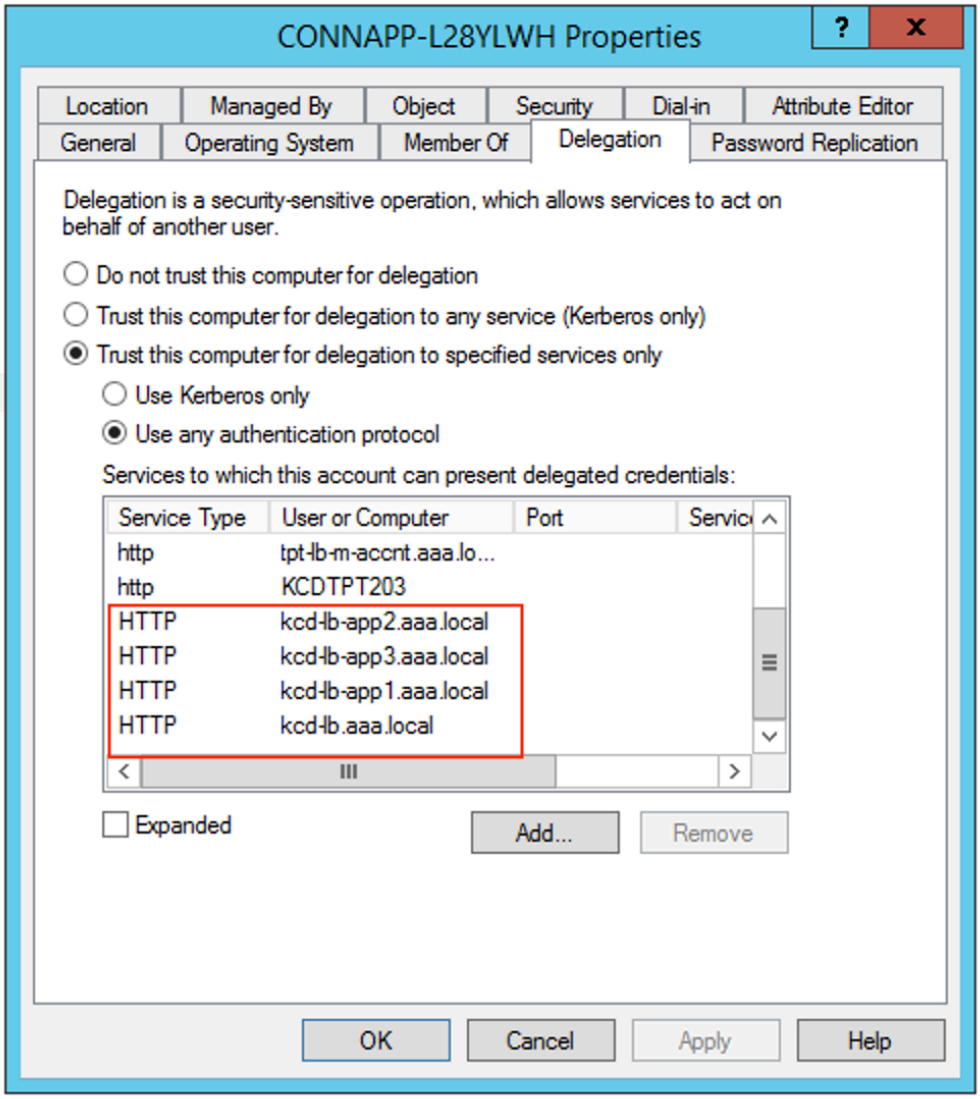
```
setspn -l <service_account>
```



```
C:\Windows\system32>setspn -l aaa\svc_iis3
Registered ServicePrincipalNames for CN=svcacct iis3,OU=Users,OU=KCD,DC=aaa,DC=l
ocal:
        HTTP/kcd-lb-app3.aaa.local
        HTTP/kcd-lb-app2.aaa.local
        HTTP/kcd-lb-app1.aaa.local
        HTTP/kcd-lb.aaa.local
        HTTP/kerblb.aaa.local
        host/kerblb.aaa.local

C:\Windows\system32>_
```

En este ejemplo, los SPN (`kcd-lb.aaa.local`, `kcd-lb-app1.aaa.local`, `kcd-lb-app2.aaa.local`, `kcd-lb-app3.aaa.local`) están configurados para KCD.

- Agregue los SPN necesarios a la cuenta de equipo del dispositivo conector como entrada delegada. Para obtener más información, paso *Crear una delegación para la cuenta de equipo del dispositivo conector*.



En este ejemplo, el SPN requerido se agrega como entradas delegadas para la cuenta de equipo de la CA.

Nota: Estos SPN se agregaron a la cuenta de servicio como entradas delegadas al configurar el conector de puerta de enlace. A medida que se aleja de la delegación de cuentas de servicio, esas entradas se pueden eliminar de la ficha **Delegación** de la cuenta de servicio.

f) Siga la documentación de Citrix Secure Private Access para configurar Citrix Secure Private Access Service. Durante la configuración, Citrix Cloud reconoce la presencia de los Connector Appliances y los utiliza para conectarse a la ubicación de recursos.

- Introducción a Citrix Secure Private Access
- Configuración de Citrix Secure Private Access
- Dispositivo conector para servicios en la nube
- Requisitos de la conectividad a Internet
- Support for Enterprise web apps

Validar la configuración de Kerberos

Si usa Kerberos para el inicio de sesión único, puede comprobar que la configuración del controlador de Active Directory es correcta en la **página de administración de Connector Appliance** . La función **Validación de Kerberos** le permite validar una configuración del modo de solo dominio de Kerberos o una configuración de delegación limitada de Kerberos (KCD).

1. Vaya a la **página de administración de Connector Appliance** .
   a) Desde la consola de Connector Appliance del hipervisor, copie la dirección IP en la barra de direcciones del explorador web.
   b) Introduzca la contraseña que estableció al registrar su Connector Appliance.
2. En el menú Administración de la parte superior derecha, seleccione **Validación de Kerberos**.
3. En el cuadro de diálogo **Validación de Kerberos**, elija el **modo de validación de Kerberos**.
4. Especifique o seleccione el **dominio de Active Directory**.
   - Si piensa validar una configuración del modo de solo dominio de Kerberos, puede especificar cualquier dominio de Active Directory.
   - Si piensa validar una configuración de delegación limitada de Kerberos, debe seleccionar un dominio de una lista de dominios del bosque unido.
5. Especifique el **FQDN del servicio**. Se supone que el nombre de servicio predeterminado es `http`. Si especifica “computer.example.com”, se considera lo mismo que `http/computer.example.com`.
6. Especifique el **nombre de usuario**.

7. Si piensa validar una configuración del modo de solo dominio de Kerberos, especifique la **contraseña** de ese nombre de usuario.
8. Haga clic en **Probar Kerberos**.

Si la configuración de Kerberos es correcta, verá el mensaje `Successfully validated Kerberos setup`. Si la configuración de Kerberos no es correcta, verá un mensaje de error que proporciona información sobre el error de validación.

Migrar conector de puerta de enlace a dispositivo

December 27, 2023

El conector de NetScaler Gateway se ha retirado. Citrix recomienda a sus clientes que utilicen NetScaler Gateway Connectors en su entorno que comiencen a implementar Connector Appliance para todos los casos de uso de Secure Private Access que anteriormente admitía NetScaler Gateway Connector. En este tema se proporcionan pautas para migrar Gateway Connector a Connector Appliance.

Pasos de alto nivel para migrar Gateway Connector Appliance

1. Instale los Connector Appliances, además de los conectores de puerta de enlace, en la misma ubicación de recursos.
2. Cierre los conectores de puerta de enlace y pruebe la conectividad de las aplicaciones web existentes. Compruebe si se puede acceder a la aplicación web alojada en la misma ubicación de recursos.
3. Quite el conector de NetScaler Gateway una vez finalizada la prueba.

Para instalar Connector Appliance

Siga los pasos siguientes para instalar un Connector Appliance.

1. Inicie sesión en Citrix Cloud.
2. En el menú de la parte superior izquierda de la pantalla, selecciona **Ubicaciones de recursos**.
3. Haga clic en el icono más junto a Connector Appliance para la ubicación de recursos en la que desea agregar un Connector Appliance.
4. Seleccione el hipervisor y haga clic en **Descargar imagen**.
5. Descargue e instale Connector Appliance en el hipervisor.

6. Inicie sesión en la interfaz de usuario web (la dirección IP se proporciona en la consola del hipervisor) y configure un proxy si es necesario.
7. Haga clic en el botón **Registrar** y obtenga el código corto.
8. Pegue el código corto en la interfaz de usuario de Citrix Cloud utilizada al descargar Connector Appliance (paso 5).

   El Connector Appliance está registrado.

Para ver los pasos detallados, consulte Connector Appliance for Cloud Services.

Preguntas frecuentes

- ¿Cómo descargo el Connector Appliance?

  Descargue Connector Appliance.
- ¿Cómo instalo el Connector Appliance?

  Instalación del dispositivo conector.
- ¿Cómo registro el Connector Appliance?

  Registro del Connector Appliance.
- ¿Cuáles son los requisitos de conectividad del Connector Appliance?

  Requisitos de conectividad a Internet del dispositivo conector.
- ¿Cuáles son los requisitos del sistema para el Connector Appliance?

  Requisitos del sistema del dispositivo conector.
- ¿Cómo se actualiza el Connector Appliance?

  Actualizaciones del Connector Appliance

Acceso directo a aplicaciones web empresariales

February 16, 2024

Las aplicaciones web empresariales como SharePoint, JIRA, Confluence y otras alojadas por el cliente, ya sea en las instalaciones o en nubes públicas, ahora se puede acceder directamente desde un explorador de cliente. Los usuarios finales ya no necesitan iniciar el acceso a sus aplicaciones web empresariales desde la experiencia de Citrix Workspace. Esta función también permite a los usuarios finales acceder a las aplicaciones web haciendo clic en los enlaces de sus correos electrónicos, herramientas

de colaboración o marcadores del explorador. De este modo, se proporciona una verdadera solución sin espacio para los clientes.

Funcionamiento

- Agregue un registro DNS nuevo o modifique un registro DNS existente para las aplicaciones web empresariales configuradas.
- El administrador de TI agregaría un nuevo registro DNS público o modificaría un registro DNS público existente para el FQDN configurado de la aplicación web empresarial para redirigir al usuario al Citrix Secure Private Access Service.
- Cuando el usuario final inicia el acceso a la aplicación web empresarial configurada, el tráfico de la aplicación se dirige al Citrix Secure Private Access Service, que, a continuación, realizará el acceso mediante proxy a la aplicación.
- Una vez que la solicitud llega al Citrix Secure Private Access Service, comprueba la autenticación del usuario y la autorización de la aplicación, incluidas las comprobaciones de las directivas de acceso contextual.
- Tras una validación satisfactoria, Citrix Secure Private Access Service se comunica con los Connector Appliances de Citrix Cloud, implementados en el entorno del cliente (local o en la nube) para permitir el acceso a la aplicación web empresarial configurada.

Configurar Citrix Secure Private Access para el acceso directo a las aplicaciones web empresariales

Requisitos previos

Antes de empezar, necesita lo siguiente para configurar la aplicación.

- FQDN de aplicación
- Certificado SSL: certificado público para configurar la aplicación
- Ubicación del recurso: Instalar Connector Appliances de Citrix Cloud
- Acceso al registro DNS público para actualizarlo con el nombre canónico (CNAME) proporcionado por Citrix durante la configuración de la aplicación.

Procedimiento para configurar el acceso directo a las aplicaciones web empresariales:

> **Importante:**
>
> Para obtener una configuración completa de principio a fin de una aplicación, consulta Flujo de trabajo guiado por el administrador para una fácil incorporación y configuración.

1. En la página de inicio de Secure Private Access, haga clic en **Continuar.**

> **Nota:**
>
> El botón **Continuar** solo aparece la primera vez que utilice el asistente. En los usos posteriores, puede ir directamente a la página **Aplicaciones** y, a continuación, hacer clic en **Agregar una aplicación**.

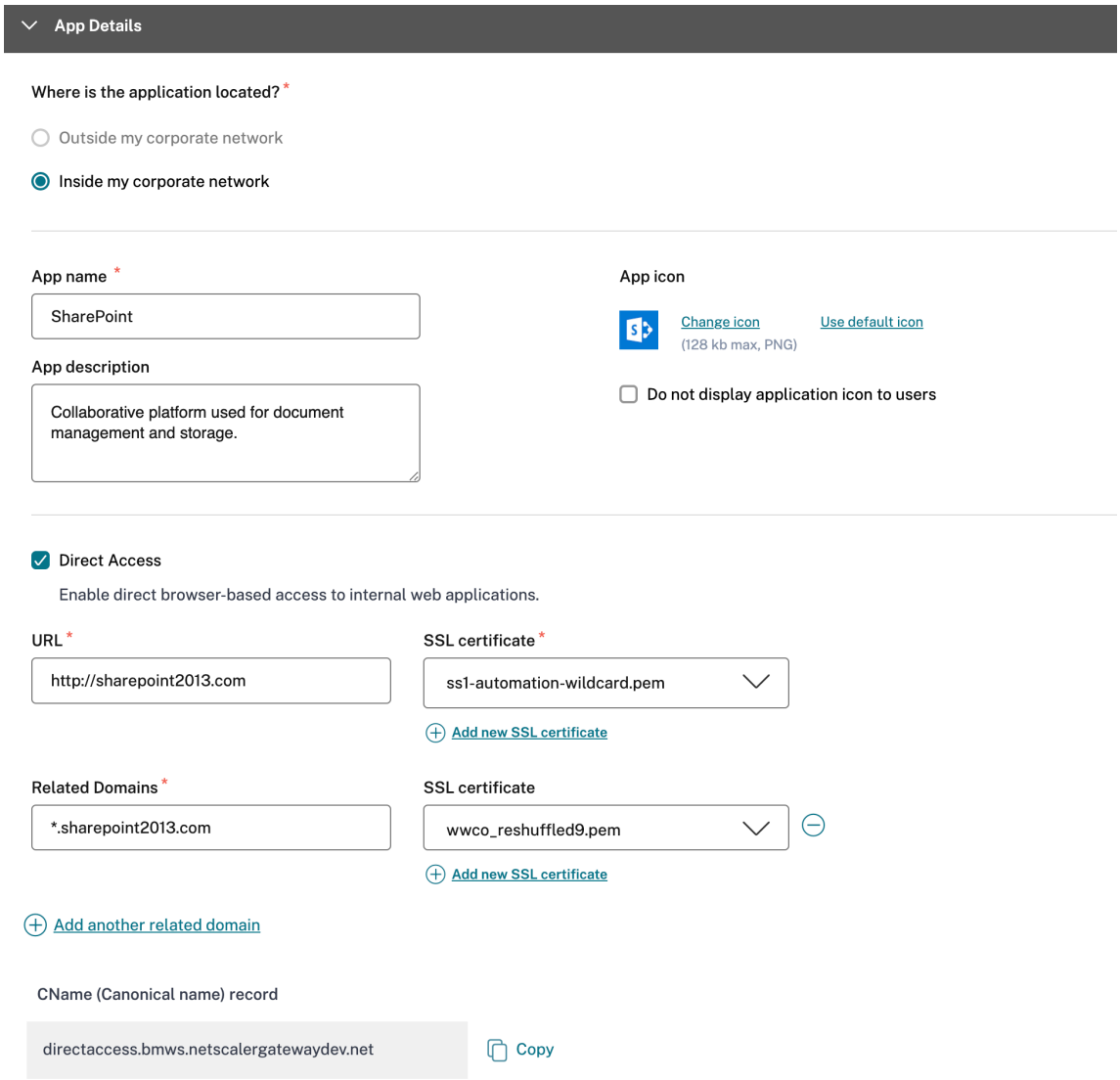
2. Configure la identidad y la autenticación. Para obtener más información, consulte Flujo de trabajo guiado por el administrador para facilitar la incorporación y la configuración.
3. Proceda a agregar una aplicación. Para obtener más información, consulte Agregar y administrar aplicaciones.
4. Seleccione la aplicación que quiera agregar y haga clic en **Omitir.**
5. En **¿Dónde está la ubicación de la aplicación?**, selecciona la ubicación.
6. Introduzca los siguientes detalles en la sección **Detalles de la aplicación** y haga clic en **Siguiente** .
   - **Tipo de aplicación**: Seleccione el tipo de aplicación (HTTP o HTTPS).
   - **Nombre de la aplicación**: Nombre de la aplicación.
   - **Descripción de la aplicación** : una breve descripción de la aplicación. La descripción que introduzcas aquí se mostrará a los usuarios del espacio de trabajo.
   - **Icono de la aplicación**: Haga clic en **Cambiar icono** para cambiar el icono de la aplicación. El tamaño del archivo de iconos debe ser de 128 x 128 píxeles. Si no cambia el icono, se muestra el icono predeterminado.

     Si no desea mostrar el icono de la aplicación, seleccione **No mostrar el icono de la aplicación a los usuarios** .
7. Seleccione **Acceso directo** para permitir que los usuarios accedan a la aplicación directamente desde el explorador de un cliente. Introduzca los siguientes detalles.
   - **URL**: URL de la aplicación back-end. La URL debe estar en formato HTTPS y el administrador debe agregar una entrada de DNS correspondiente.
   - **Certificado SSL**: Seleccione un certificado SSL existente en el menú desplegable o agregue un certificado SSL nuevo haciendo clic en **Agregar certificado SSL nuevo**.

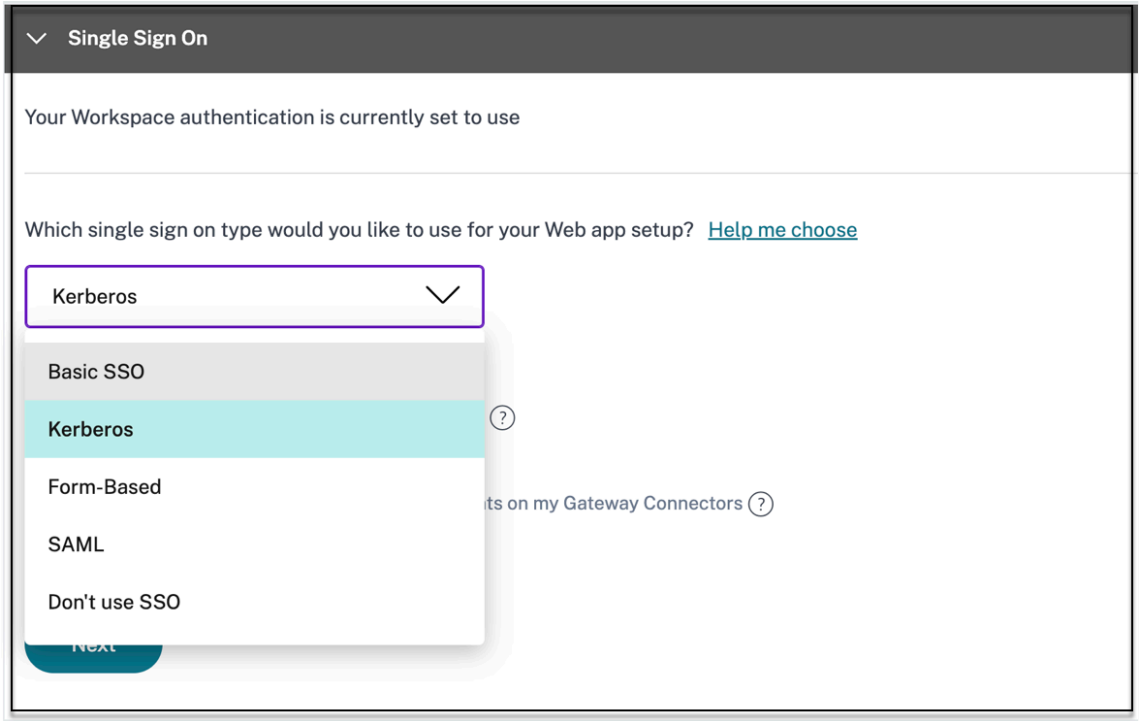
     Puntos a tener en cuenta:

     - Solo se admite un certificado de CA público o de confianza. No se admiten los certificados autofirmados.
     - Debe cargarse una cadena completa de certificados.

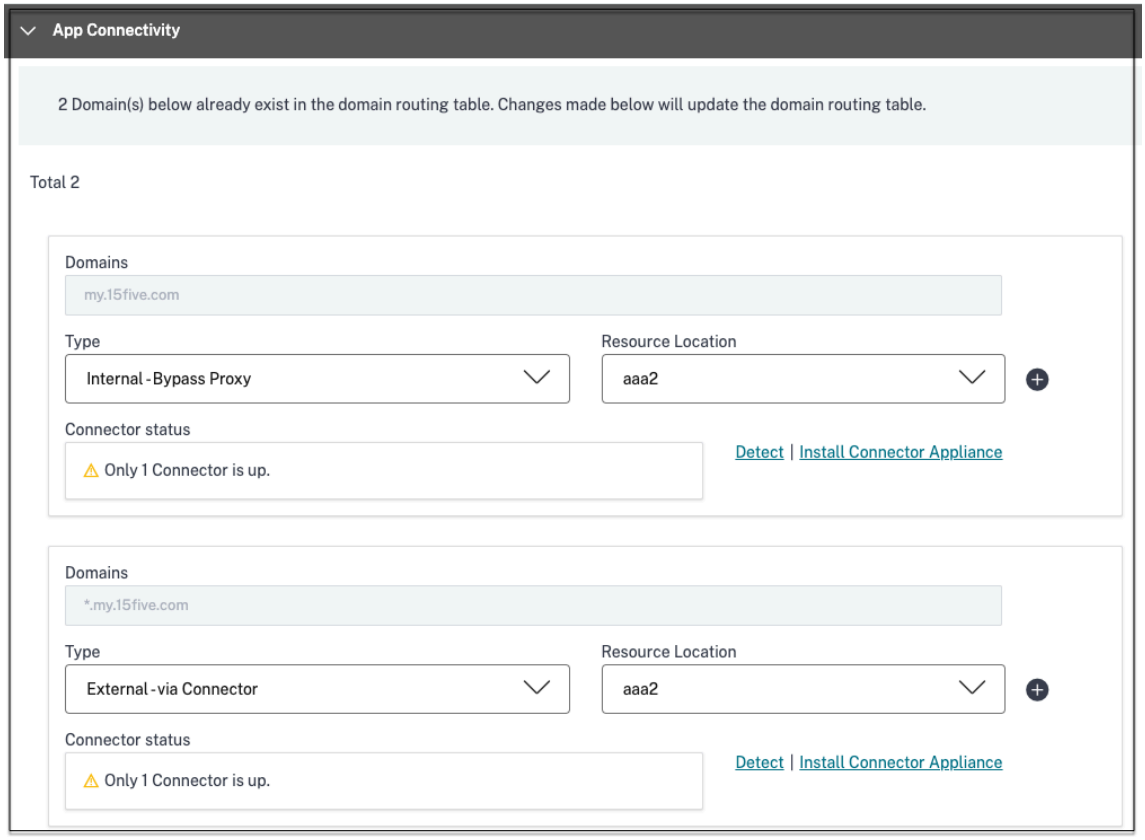
- **Dominios relacionados** : el dominio relacionado se rellena automáticamente en función de la URL que has proporcionado. El dominio relacionado ayuda al servicio a identificar la URL como parte de la aplicación y a dirigir el tráfico en consecuencia. Puede agregar más de un dominio relacionado. Puede vincular un certificado SSL a cada dominio relacionado, esto es opcional.
- **Registro CName**: Generado automáticamente por Secure Private Access. Este es el valor que se debe introducir en el DNS para permitir el acceso directo a la aplicación.



8. Haz clic en **Siguiente.**
9. En la sección Inicio de **sesión único**, seleccione el tipo de inicio de sesión único que prefiera para su aplicación y haga clic en**Siguiente**.



10. En la sección **Conectividad de aplicaciones**, puede seleccionar una ubicación de recursos existente o crear una e implementar un nuevo Connector Appliance. Para elegir una ubicación de recursos existente, haga clic en una de las ubicaciones de recursos de la lista de ubicaciones de recursos, por ejemplo, Mi ubicación de recursos, y haga clic en **Siguiente**. Para obtener más información, consulte Tablas de redirección para resolver conflictos si los dominios relacionados en las aplicaciones web y SaaS son los mismos.



11. Haga clic en **Finalizar**. La aplicación se agrega a la página Aplicaciones. Puede editar o eliminar una desde la página Aplicaciones después de haber configurado la aplicación. Para hacerlo, haga clic en el botón de puntos suspensivos de una aplicación y seleccione las acciones correspondientes.

    - **Modificar aplicación**
    - **Eliminar**

> **Importante:**
>
> - Para habilitar el acceso basado en la confianza cero a las aplicaciones, se deniega el acceso a las aplicaciones de forma predeterminada. El acceso a las aplicaciones solo está habilitado si hay una directiva de acceso asociada a la aplicación. Para obtener más información, consulta Acceso denegado a las aplicaciones de forma predeterminada.
> - Si se configuran varias aplicaciones con el mismo FQDN o con alguna variación del FQDN comodín, esto podría provocar un conflicto de configuración. Para obtener más información, consulta Configuración conflictiva que podría ocasionar problemas de acceso a las aplicaciones.

Compatibilidad con aplicaciones de software como servicio

February 16, 2024

Software as a Service (SaaS) es un modelo de distribución de software para ofrecer software de forma remota como un servicio basado en web. Las aplicaciones SaaS más utilizadas incluyen Salesforce, Workday, Concur, GoToMeeting, etc.

Se puede acceder a las aplicaciones SaaS mediante Citrix Workspace mediante el servicio Secure Private Access. El servicio Secure Private Access, junto con Citrix Workspace, proporciona una experiencia de usuario unificada para las aplicaciones SaaS configuradas, las aplicaciones virtuales configuradas o cualquier otro recurso del espacio de trabajo.

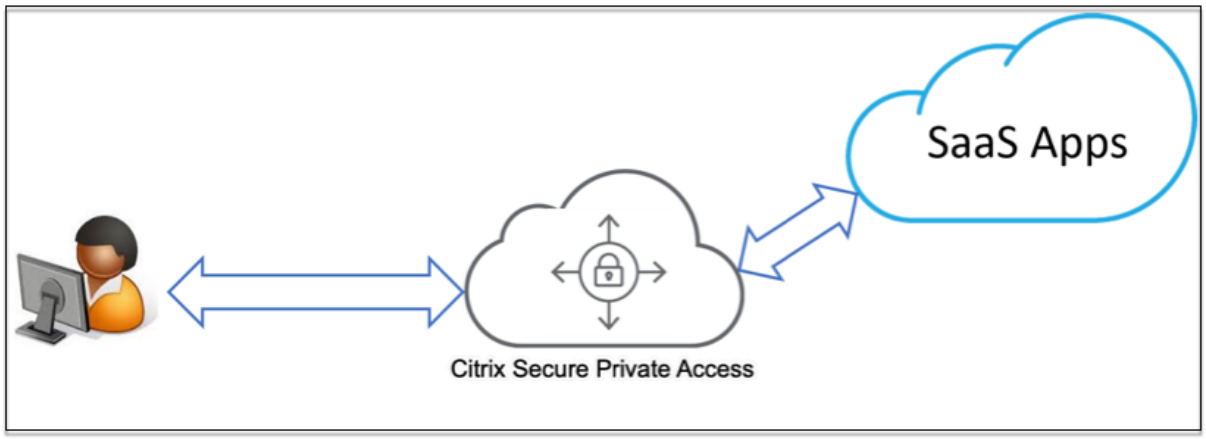
La entrega de aplicaciones SaaS mediante el servicio Secure Private Access le brinda una solución fácil, segura, sólida y escalable para administrar las aplicaciones. Las aplicaciones SaaS suministradas en la nube tienen las siguientes ventajas:

- **Configuración simple** : fácil de operar, actualizar y consumir.
- **Inicio de sesión único:** inicio de sesión sin complicaciones con inicio de sesión único.
- **Plantilla estándar para diferentes aplicaciones**: Configuración basada en plantillas de aplicaciones populares.

Cómo se admiten las aplicaciones SaaS con el servicio Secure Private Access

1. El administrador del cliente configura las aplicaciones SaaS mediante la interfaz de usuario del servicio Secure Private Access.
2. El administrador proporciona la URL del servicio a los usuarios para que accedan a Citrix Workspace.
3. Para iniciar la aplicación, el usuario hace clic en el icono de la aplicación SaaS enumerado.
4. La aplicación SaaS confía en la afirmación de SAML proporcionada por el servicio Secure Private Access y se inicia la aplicación.

> **Nota:**
>
> - Para conceder acceso a las aplicaciones a los usuarios, los administradores deben crear directivas de acceso. En las directivas de acceso, los administradores agregan suscriptores a la aplicación y configuran los controles de seguridad. Para obtener más información, consulte Crear directivas de acceso.
> - Las aplicaciones SaaS configuradas se agregan junto con las aplicaciones virtuales y otros recursos en Citrix Workspace para ofrecer una experiencia de usuario unificada.



Configurar una aplicación SaaS

La configuración de una aplicación SaaS implica los siguientes pasos de alto nivel.

1. Configurar los detalles de la aplicación
2. Configurar el método de inicio de sesión preferido
3. Defina el enrutamiento de aplicaciones

Configurar los detalles de la aplicación

1. En el mosaico **Secure Private Access**, haga clic en **Administrar.**
2. Haga clic en **Continuar** y, a continuación, en **Agregar una aplicación.**

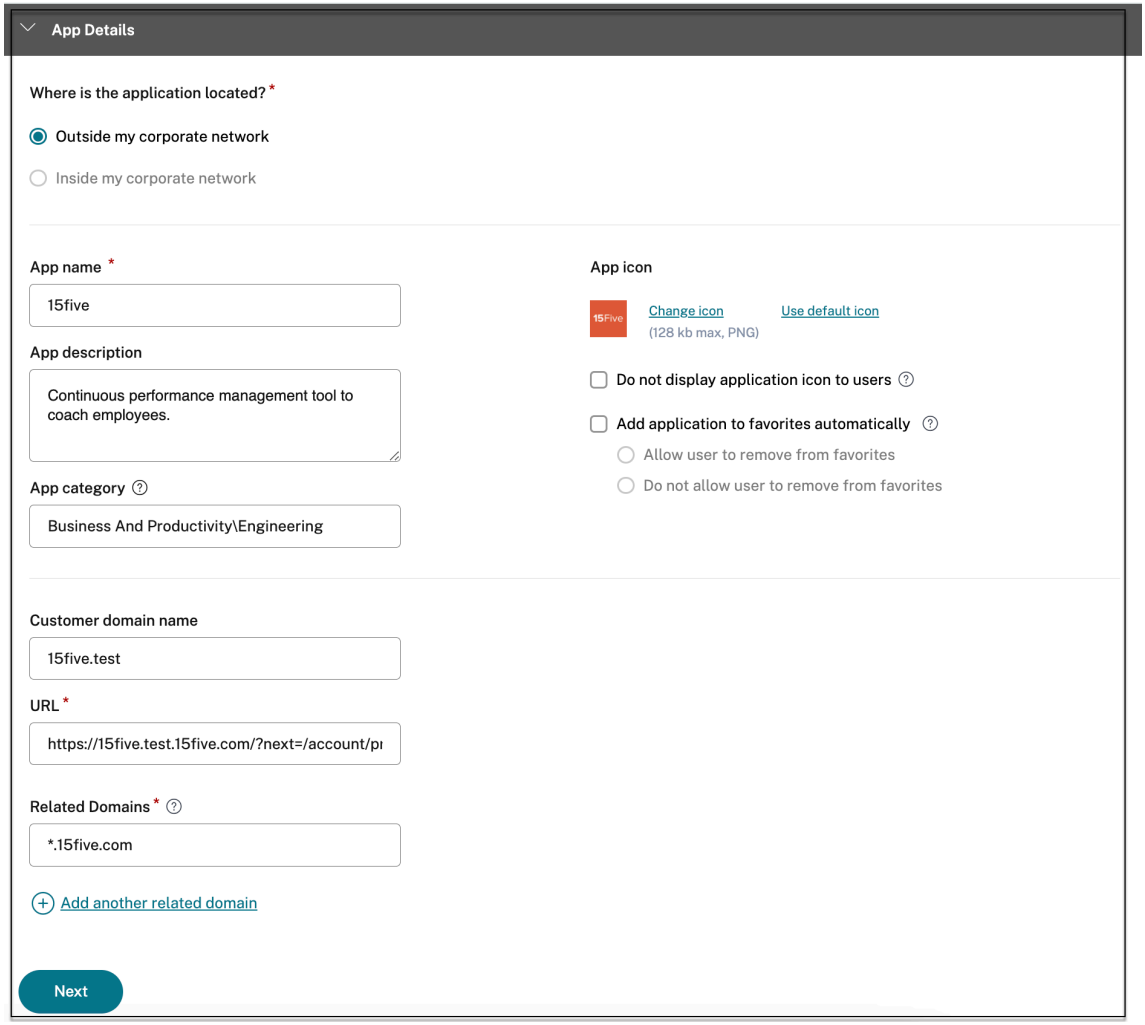
> **Nota:**
>
> - El botón **Continuar** solo aparece la primera vez que utiliza el asistente. En los usos posteriores, puede navegar directamente a la página **Aplicaciones** y, a continuación, hacer clic en **Agregar una aplicación**.
> - Puede agregar una aplicación SaaS manualmente introduciendo los detalles de la aplicación o seleccionando una plantilla de aplicación que esté disponible para una lista de aplicaciones SaaS populares. La plantilla rellena previamente gran parte de la información necesaria para configurar las aplicaciones. Sin embargo, se debe proporcionar la información específica del cliente. Para obtener detalles sobre la plantilla de configuración de aplicaciones SaaS, consulte Configuración específica del servidor de aplicacionesSaaS

3. Configura la aplicación.
   - Para introducir los detalles de la aplicación manualmente, haga clic en **Omitir.**

- Para configurar la aplicación mediante una plantilla, haga clic en **Siguiente.**

La **red Fuera de mi empresa** está habilitada de forma predeterminada para una aplicación SaaS.

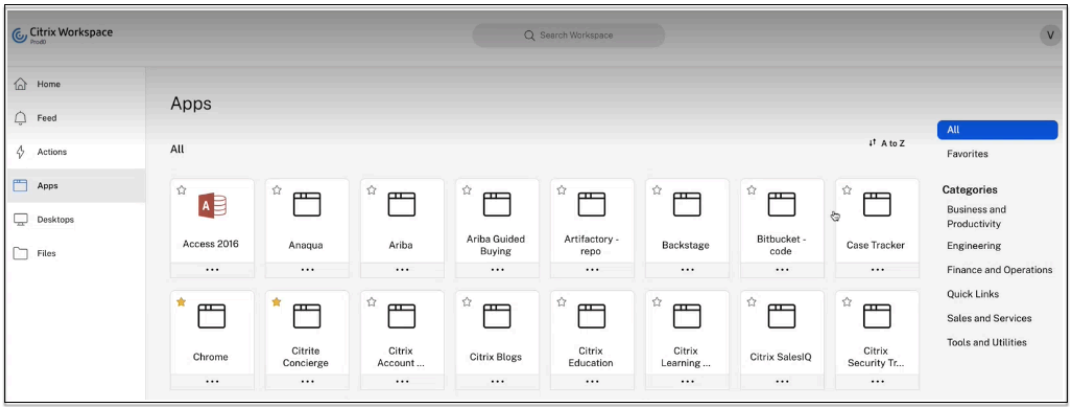
4. Introduzca los siguientes detalles en la sección **Detalles de la aplicación** y haga clic en **Siguiente.**



- **Nombre de la aplicación**: Nombre de la aplicación.
- **Descripción de la aplicación** : una breve descripción de la aplicación. La descripción que introduzcas aquí se mostrará a los usuarios del espacio de trabajo.
- **Categoría de aplicación** : agregue la categoría y el nombre de la subcategoría (si corresponde) con los que debe aparecer la aplicación que va a publicar en la interfaz de usuario de Citrix Workspace. Puede agregar una nueva categoría para cada aplicación o usar las categorías existentes de la interfaz de usuario de Citrix Workspace. Una vez que especifiques una categoría para una aplicación web o SaaS, la aplicación aparecerá en la interfaz de usuario de Workspace en la categoría específica.

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

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



- **Icono de la aplicación**: Haga clic en **Cambiar icono** para cambiar el icono de la aplicación. El tamaño del archivo de iconos debe ser de 128 x 128 píxeles. Si no cambia el icono, se muestra el icono predeterminado.

  Si no desea mostrar el icono de la aplicación, seleccione **No mostrar el icono de la aplicación a los usuarios** .

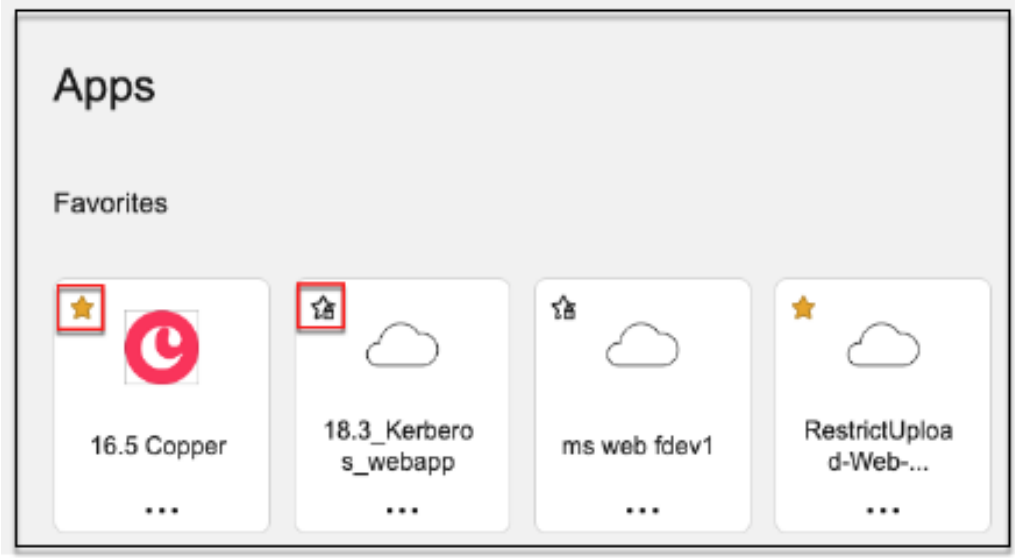
- **URL**: URL con su ID de cliente. La URL debe contener su ID de cliente (ID de cliente de Citrix Cloud). Para obtener su ID de cliente, consulte Inscribirse en Citrix Cloud. En caso de que Single Sign-On falle o no quiera utilizar Single Sign-On, se redirigirá al usuario a esta URL.
- **Nombre de dominio del cliente** e **ID de dominio del cliente**: El nombre y el ID de dominio del cliente se utilizan para crear la URL de aplicación y otras URL posteriores en la página de inicio de sesión único de SAML.

  Por ejemplo, si va a agregar una aplicación de Salesforce, su nombre de dominio es `salesforceformyorg` y el ID es 123754, entonces la URL de la aplicación es

`https://salesforceformyorg.my.salesforce.com/?so=123754.`

Los campos Nombre de dominio del cliente e ID de cliente son específicos de determinadas aplicaciones.

- **Dominios relacionados** : el dominio relacionado se rellena automáticamente en función de la URL que has proporcionado. El dominio relacionado ayuda al servicio a identificar la URL como parte de la aplicación y a dirigir el tráfico en consecuencia. Puede agregar más de un dominio relacionado.
- Haga clic en **Agregar aplicación a favoritos automáticamente** para agregar esta aplicación como favorita en la aplicación Citrix Workspace.
  - Haga clic en **Permitir al usuario eliminarla de favoritos** para permitir que los suscriptores de la aplicación eliminen la aplicación de la lista de aplicaciones favoritas de la aplicación Citrix Workspace. Al seleccionar esta opción, aparece un icono de estrella amarilla en la esquina superior izquierda de la aplicación en la aplicación Citrix Workspace.
  - Haga clic en **No permitir que el usuario elimine de favoritos** para evitar que los suscriptores eliminen la aplicación de la lista de aplicaciones favoritas de la aplicación Citrix Workspace. Al seleccionar esta opción, aparece un icono de estrella con un candado en la esquina superior izquierda de la aplicación en la aplicación Citrix Workspace.



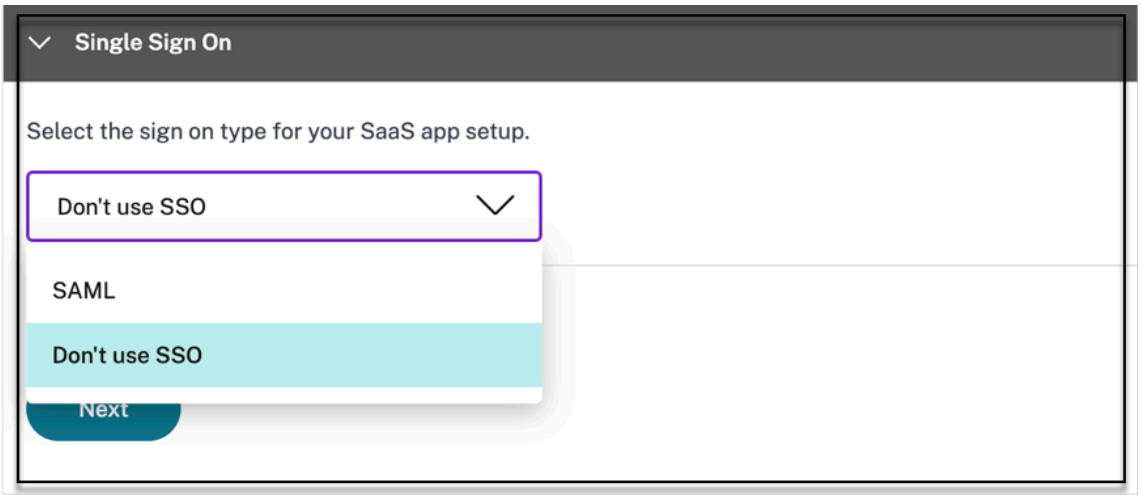
Si elimina las aplicaciones marcadas como favoritas de la consola del servicio Secure Private Access, estas aplicaciones deben eliminarse manualmente de la lista de favoritos de Citrix Workspace. Las aplicaciones no se eliminan automáticamente de la aplicación Workspace si se eliminan de la consola de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

5. Haz clic en **Siguiente.**

> **Importante:**
>
> - Para habilitar el acceso basado en la confianza cero a las aplicaciones, se deniega el acceso a las aplicaciones de forma predeterminada. El acceso a las aplicaciones solo está habilitado si hay una directiva de acceso asociada a la aplicación. Para obtener más información, consulta Acceso denegado a las aplicaciones de forma predeterminada.
> - Si se configuran varias aplicaciones con el mismo FQDN o con alguna variación del FQDN comodín, esto podría provocar un conflicto de configuración. Para obtener más información, consulta Configuración conflictiva que podría ocasionar problemas de acceso a las aplicaciones.

Establecer un método de inicio de sesión preferido

1. En la sección **Single Sign-On**, seleccione el tipo de Single Sign-On que prefiera para usarlo en su aplicación y haga clic en **Guardar**. Están disponibles los siguientes tipos de inicio de sesión único.



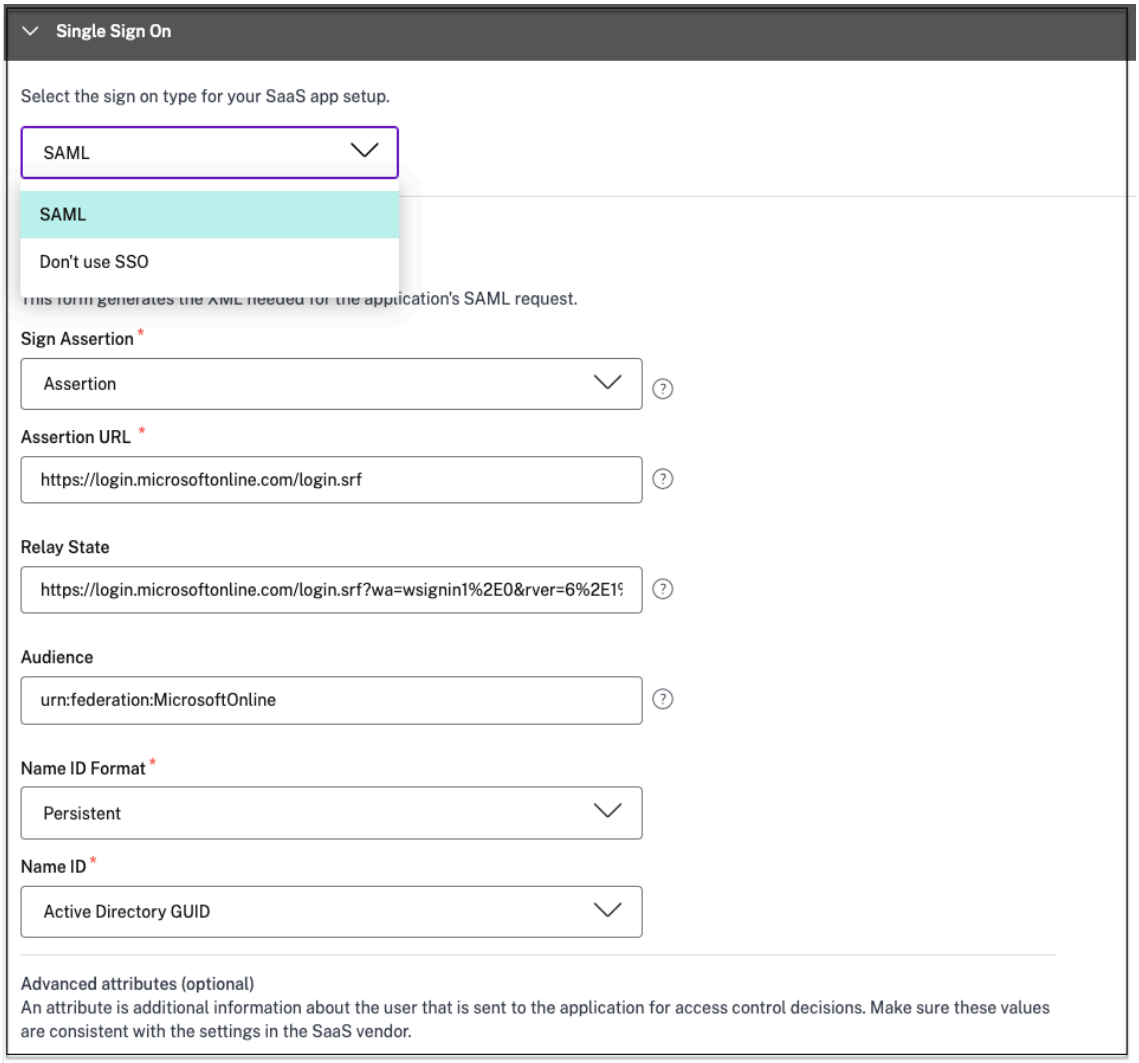
   - **No usar SSO**: Use la opción **No usar SSO** cuando no necesite autenticar a un usuario en el servidor back-end. Cuando se selecciona la opción **No usar SSO**, se redirige al usuario a la URL configurada en la sección **Detalles de la aplicación**.
   - **SAML**: Elija **SAML** para Single Sign-On basado en SAML en aplicaciones web. Introduzca los detalles de configuración para el tipo de SSO de **SAML** .

     Introduzca los siguientes detalles en la sección Iniciar sesión y haga clic en **Guardar**.

     - **Afirmación** de firmas: la firma de afirmación o respuesta garantiza la integridad del mensaje cuando la respuesta o afirmación se entrega a la parte que confía (SP). Puede seleccionar **Afirmación, Respuesta, Ambas** o **Ninguna**.

- **URL de aserción**: El proveedor de la aplicación proporciona la URL de aserción. La aserción SAML se envía a esta URL.
- **Estado de retransmisión** : el parámetro Estado de retransmisión se usa para identificar el recurso específico al que acceden los usuarios después de iniciar sesión y dirigirlos al servidor de federación de la parte que confía. Relay State genera una única URL para los usuarios. Los usuarios pueden hacer clic en esta URL para iniciar sesión en la aplicación de destino.
- **Audiencia**: El proveedor de la aplicación proporciona la audiencia. Este valor confirma que la aserción SAML se ha generado para la aplicación correcta.
- **Formato de ID de nombre**: Seleccione el formato de identificador de nombre admitido.
- **ID de nombre**: Seleccione el ID de nombre admitido.
- Seleccione **Iniciar la aplicación con la URL específica (iniciada por el SP) para anular el flujo iniciado** por el proveedor de identidad y usar solo el flujo iniciado por el proveedor de servicios.

2. En **Atributos avanzados (opcional)**, agregue información adicional sobre el usuario que se envía a la aplicación para tomar decisiones de control de acceso.



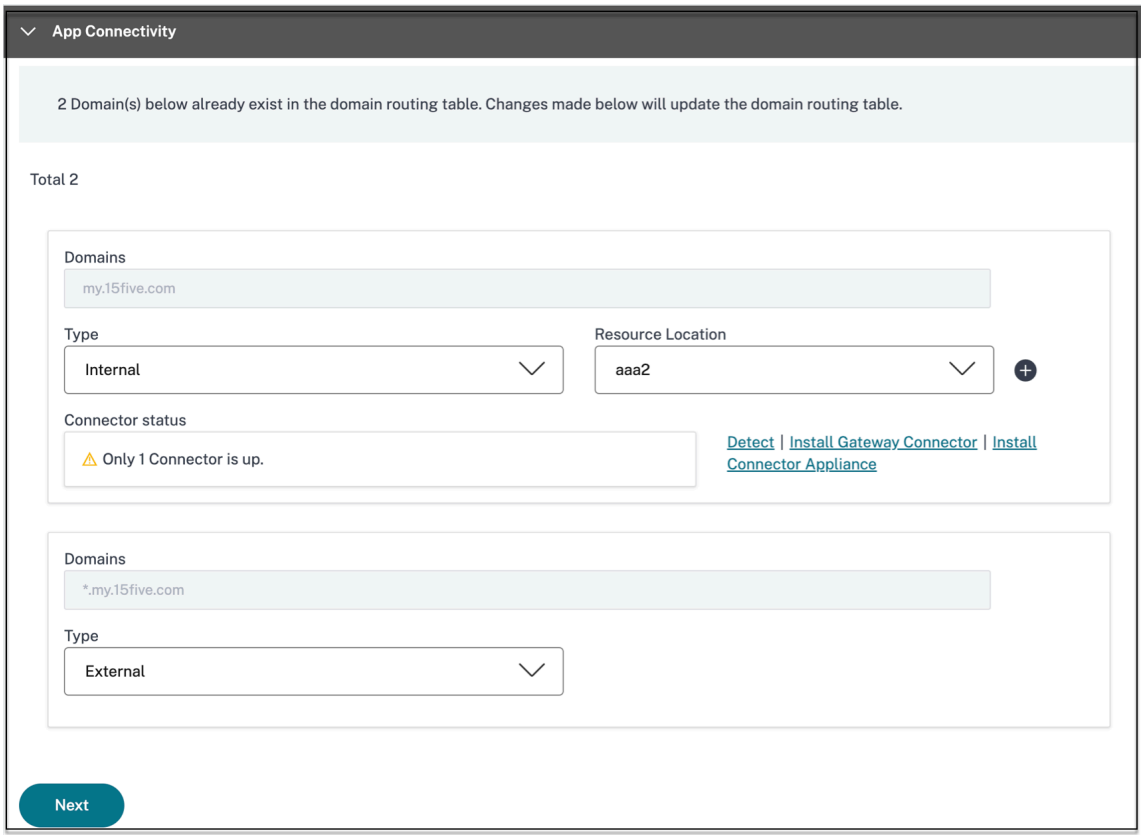
3. Para descargar el archivo de metadatos, haga clic en el enlace situado debajo de **Metadatos SAML**. Utilice el archivo de metadatos descargado para configurar el SSO en el servidor de aplicaciones SaaS.

   > **Nota:**
   >
   > - Puede copiar la URL de inicio de sesión único en URL de inicio de **sesión** y utilizarla al configurar Single Sign-On en el servidor de aplicaciones SaaS.
   > - También puede descargar el certificado de la lista de **certificados** y utilizarlo al configurar el inicio de sesión exclusivo en el servidor de aplicaciones SaaS.

4. Haz clic en **Siguiente.**

Defina el enrutamiento de aplicaciones

1. En la sección **Conectividad de aplicaciones**, defina la redirección de los dominios relacionados de las aplicaciones, si los dominios deben redirigirse de manera externa o interna a través de Connector Appliances de Citrix. Para obtener más información, consulte Tablas de redirección para resolver conflictos si los dominios relacionados en las aplicaciones web y SaaS son los mismos.

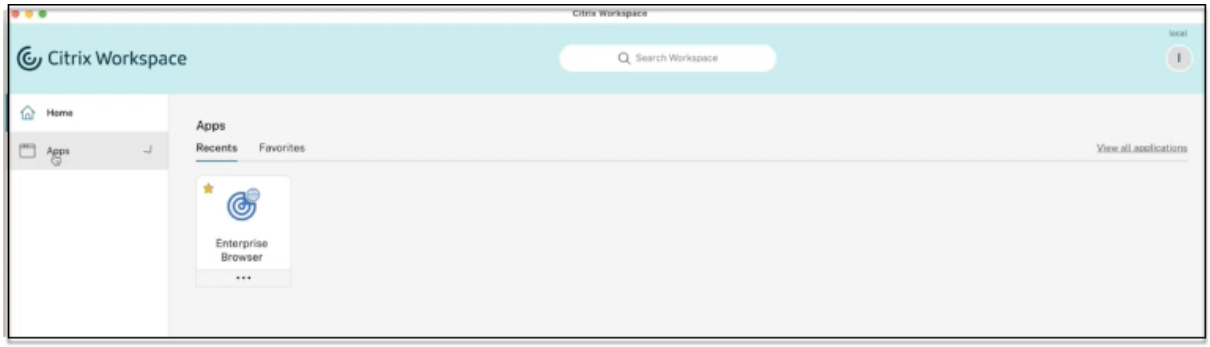


2. Haz clic en **Finalizar.**

   Después de hacer clic en **Finalizar**, la aplicación se agrega a la página Aplicaciones. Puedes editar o eliminar una aplicación desde la página Aplicaciones después de configurarla. Para hacerlo, haga clic en el botón de puntos suspensivos de una aplicación y seleccione las acciones correspondientes.

   - **Modificar aplicación**
   - **Eliminar**

Al publicar una aplicación web o SaaS desde el servicio Secure Private Access y si esa aplicación no está oculta, la aplicación Citrix Enterprise Browser aparece automáticamente en la interfaz de usuario de Citrix Workspace. Además, Citrix Enterprise Browser también se agrega como aplicación favorita de forma predeterminada. Los usuarios finales pueden iniciar el explorador del espacio de trabajo sin una URL y acceder a los sitios web internos mediante los navegadores del espacio de trabajo.



Referencias

Para obtener una configuración completa de principio a fin de una aplicación, consulta Flujo de trabajo guiado por el administrador para una fácil incorporación y configuración.

Compatibilidad con aplicaciones cliente-servidor

February 16, 2024

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

Con el soporte adicional de las aplicaciones cliente-servidor dentro de Citrix Secure Private Access, ahora puede eliminar la dependencia de una solución VPN tradicional para proporcionar acceso a todas las aplicaciones privadas para los usuarios remotos.

Funciones en Tech Preview

Compatibilidad con sufijos DNS para resolver FQDN en direcciones IP.

Funcionamiento

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

- Para Windows, la versión del cliente (22.3.1.5 y versiones 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 (22.02.3 y posteriores) se puede descargar de la App Store.

Configuración administrativa: acceso basado en el cliente de Citrix Secure Access a aplicaciones TCP/UDP

Requisitos previos

Asegúrese de que se cumplan los siguientes requisitos para acceder a las aplicaciones TCP/UDP.

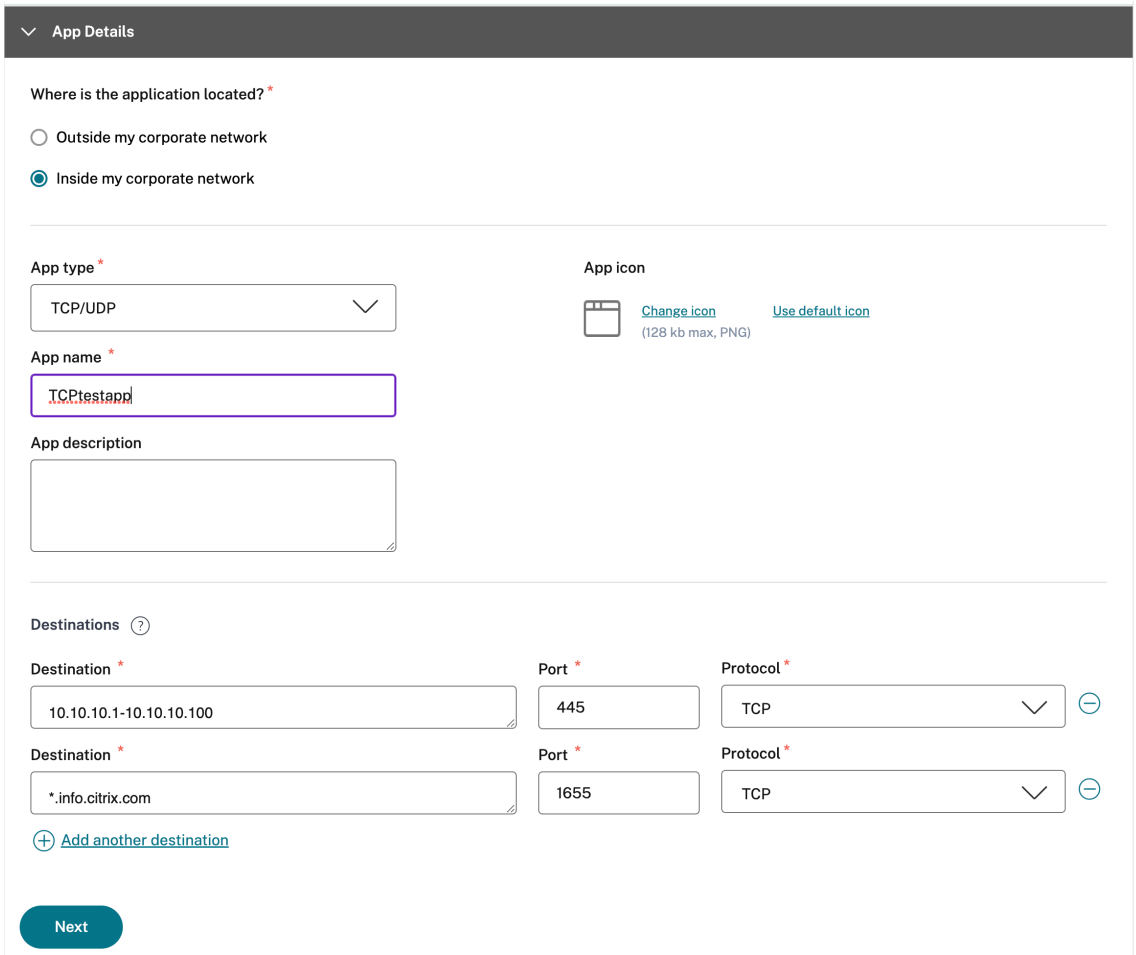
- Acceso a Citrix Secure Private Access en Citrix Cloud.
- Citrix Cloud Connector: instale una configuración de dominio de Citrix Cloud Connector para Active Directory tal como se capturó en la instalación de Cloud Connector.
- Administración de identidades y accesos: complete la configuración. Para obtener más información, consulte Administración de identidades y accesos.
- Connector Appliance: Citrix recomienda instalar dos Connector Appliances en una configuración de alta disponibilidad en la ubicación de recursos. El conector se puede instalar en las instalaciones, en el hipervisor del centro de datos o en la nube pública. Para obtener más información sobre Connector Appliance y su instalación, consulte Connector Appliance for Cloud Services.
- Debe utilizar un Connector Appliance para las aplicaciones TCP/UDP.

> **Importante:**
>
> Para obtener una configuración completa de principio a fin de una aplicación, consulta Flujo de trabajo guiado por el administrador para una fácil incorporación y configuración.

1. En el mosaico de Citrix Secure Private Access, haga clic en **Administrar**.
2. Haz clic en **Continuar** y, a continuación, en **Añadir una aplicación** .

   > **Nota:**
   >
   > El botón **Continuar** solo aparece la primera vez que utilice el asistente. En los usos posteriores, puede ir directamente a la página **Aplicaciones** y, a continuación, hacer clic en **Agregar una** aplicación .

   La aplicación es una agrupación lógica de destinos. Podemos crear una aplicación para varios destinos: cada destino significa diferentes servidores en el back-end. Por ejemplo, una aplicación puede tener un SSH, un RDP, un servidor de base de datos y un servidor web. No es necesario crear una aplicación por destino, pero una aplicación puede tener muchos destinos.
3. En la sección **Elija una plantilla**, haga clic en **Omitir** para configurar la aplicación TCP/UDP manualmente.
4. En la sección **Detalles de la aplicación**, seleccione **Dentro de mi red corporativa**, introduzca los siguientes detalles y haga clic en **Siguiente**.



- **Tipo de aplicación**: Seleccione TCP/UDP.
- **Nombre de la aplicación**: Nombre de la aplicación.
- **Icono de aplicación**: se muestra un icono de aplicación. Este campo es opcional.
- **Descripción de la aplicación**: Descripción de la aplicación que quiere agregar. Este campo es opcional.
- **Destinos**: Direcciones IP o FQDN de las máquinas back-end que residen en la ubicación de recursos. Se pueden especificar uno o más destinos de la siguiente manera.
  - **Dirección IP v4**
  - **Intervalo de direcciones IP** —Ejemplo: 10.68.90.10-10.68.90.99
  - **CIDR** —Ejemplo: 10.106.90.0/24
  - **FQDN de las máquinas o nombre de dominio**: Dominio único o comodín. Ejemplo: ex.destination.domain.com, *.domain.com

> **Importante:**
>
> Los usuarios finales pueden acceder a las aplicaciones mediante el FQDN incluso si el administrador ha configurado las aplicaciones con la dirección IP. Esto es posible porque el cliente Citrix Secure Access puede resolver un FQDN en la dirección IP real.
> La siguiente tabla proporciona ejemplos de varios destinos y cómo acceder a las aplicaciones con estos destinos:

Entrada de destino	Cómo acceder a la aplicación
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.
10.10.10.0/24	Se espera que el usuario final acceda a la aplicación solo a través de las direcciones IP configuradas en el CIDR IP.
10.10.10.101	Se espera que el usuario final acceda a la aplicación solo a través de 10.10.10.101
`*.info.citrix.com`	Se espera que el usuario final acceda a los subdominios de `info.citrix.com` y también `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 se permite un *.
info.citrix.com	Se espera que el usuario final `info.citrix.com` solo acceda a los subdominios y no a ellos. Por ejemplo, `sub1.info.citrix.com` no es accesible.

- **Puerto**: El puerto en el que se ejecuta la aplicación. Los administradores pueden configurar varios puertos o rangos de puertos por destino.

  La siguiente tabla proporciona ejemplos de puertos que se pueden configurar para un destino.

Entrada de puerto	Descripción
*	De forma predeterminada, el campo puerto está establecido en "*" (cualquier puerto). Se admiten los números de puerto del 1 al 65535 para el destino.
1300–2400	Se admiten los números de puerto del 1300 al 2400 para el destino.
38389	Solo se admite el número de puerto 38389 para el destino.
22,345,5678	Los puertos 22, 345, 5678 son compatibles con el destino.
1300–2400, 42000-43000,22,443	El número de puerto varía de 1300 a 2400, 42000 a 43000, y los puertos 22 y 443 son compatibles con el destino.

> **Nota:**
>
> El puerto comodín (*) no puede coexistir con los números o intervalos de puertos.

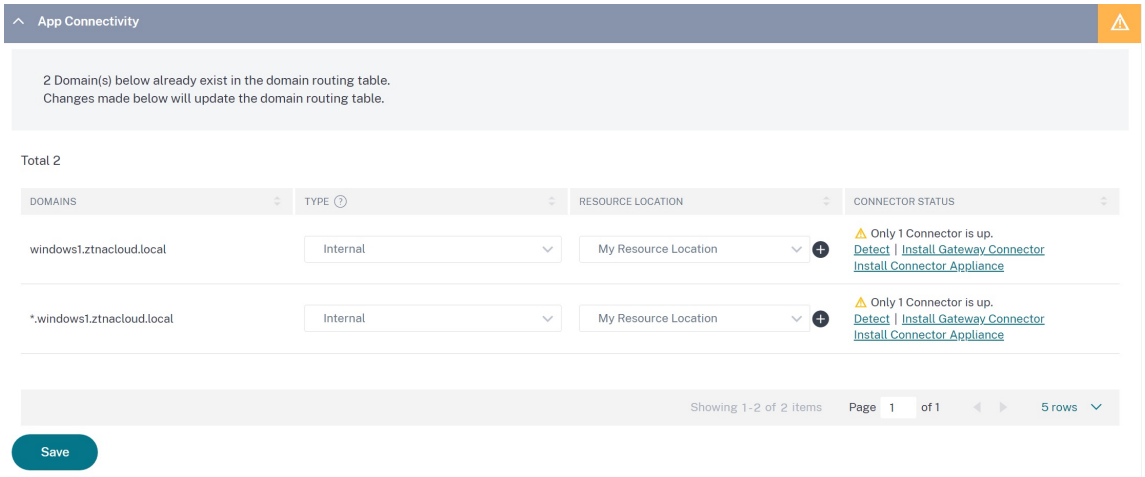
- **Protocolo**: TCP/UDP

5. En la sección **Conectividad de aplicaciones**, hay disponible una versión reducida de la tabla **Dominios de aplicaciones** para tomar las decisiones de redirección. Para cada destino, puede elegir una ubicación de recursos diferente o igual. Los destinos configurados en el paso anterior se rellenan en la columna **DESTINO**. Los destinos que se agregan aquí también se agregan a la tabla principal de **dominios de aplicaciones**. La tabla **Dominios de aplicación** es la fuente de información fiable para tomar la decisión de enrutamiento a fin de dirigir el establecimiento de la conexión y el tráfico a la ubicación de recursos correcta. Para obtener más información sobre la tabla **Dominios de aplicación** y los posibles casos de conflicto de IP, consulte la sección *Dominios de aplicación: resolución de conflictos de direcciones IP*.
6. Para los siguientes campos, seleccione una entrada en el menú desplegable y haga clic en **Siguiente**.

> **Nota:**
>
> Solo se admite el tipo de ruta interna.

- **UBICACIÓN DE RECURSOS**: En el menú desplegable, debe conectarse a una ubicación de recursos con al menos un Connector Appliance instalado.

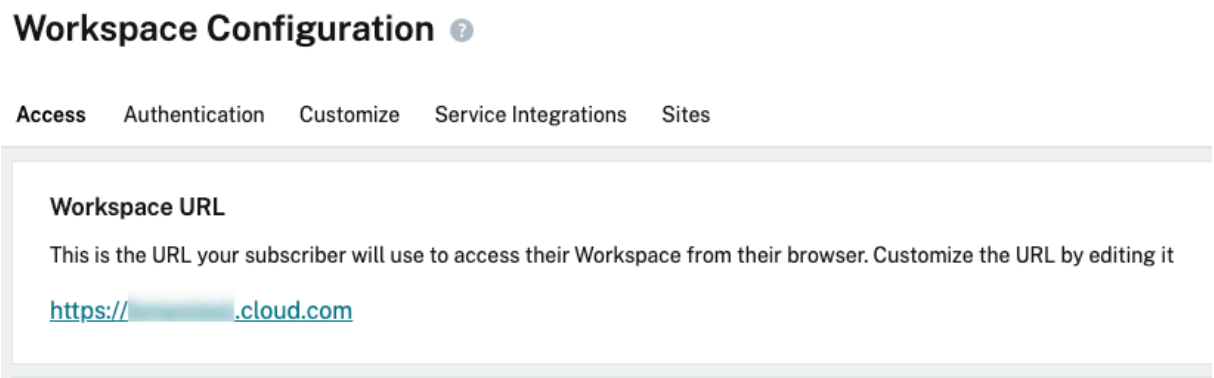
> **Nota:**
>
> La instalación del Connector Appliance se admite desde la sección Conectividad de aplicaciones. También puede instalarlo en la sección Ubicaciones de recursos del portal de Citrix Cloud. Para obtener más información sobre la creación de una ubicación de recursos, consulte Configurar ubicaciones de recursos.



7. Haga clic en **Finalizar**. La aplicación se agrega a la página **Aplicaciones** . Puede modificar o eliminar una aplicación desde la página **Aplicaciones** después de haberla configurado. Para hacerlo, haga clic en el botón de puntos suspensivos de una aplicación y seleccione las acciones correspondientes.

   - **Modificar aplicación**
   - **Eliminar**

> **Nota:**
>
> - Para conceder acceso a las aplicaciones a los usuarios, los administradores deben crear directivas de acceso. En las directivas de acceso, los administradores agregan suscriptores a la aplicación y configuran los controles de seguridad. Para obtener más información, consulte Crear directivas de acceso.
> - Para configurar los métodos de autenticación requeridos para los usuarios, consulte Configurar la identidad y la autenticación.
> - Para obtener la URL del espacio de trabajo que se compartirá con los usuarios, en el menú Citrix Cloud, haga clic en **Configuración del espacio de trabajo** y seleccione la ficha **Acceso**.



Configuración administrativa: acceso basado en el cliente de Citrix Secure Access a las aplicaciones HTTP/HTTPS

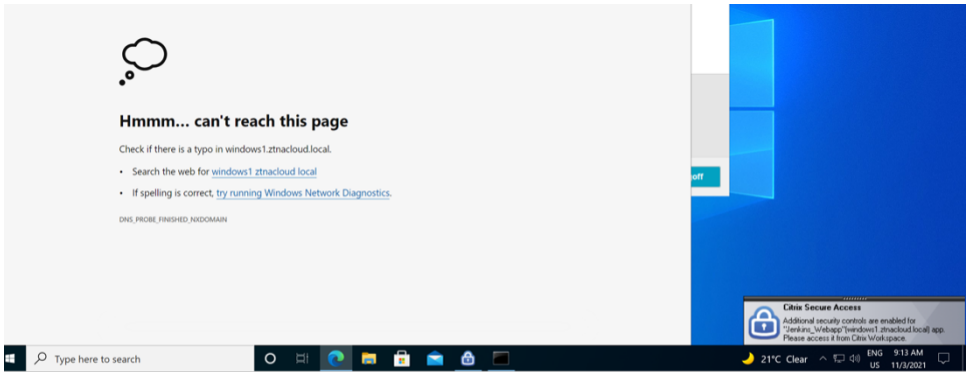
> **Nota:**
>
> Para acceder a las aplicaciones HTTP/HTTPS nuevas o existentes mediante el cliente Citrix Secure Access, debe instalar al menos un Connector Appliance (se recomiendan dos para una alta disponibilidad) en la ubicación de recursos. El Connector Appliance se puede instalar en las instalaciones, en el hipervisor del centro de datos o en la nube pública. Para obtener más información sobre Connector Appliance y su instalación, consulte Connector Appliance for Cloud Services.

Requisitos previos

- Acceso a Citrix Secure Private Access en Citrix Cloud.

Puntos que tener en cuenta

- No se puede acceder a las aplicaciones web internas que cuentan con controles de seguridad mejorados a través del cliente Citrix Secure Access.
- Si intenta acceder a una aplicación HTTP (S) que tiene habilitados los controles de seguridad mejorados, se muestra el siguiente mensaje emergente. **Se habilitan controles de seguridad adicionales para la aplicación <”nombre de la aplicación”(FQDN)>. Acceda a ella desde Citrix Workspace.**



- Si quiere habilitar la experiencia de SSO, acceda a las aplicaciones web mediante la aplicación Citrix Workspace o el portal web.

Los pasos para configurar aplicaciones HTTP (S) siguen siendo los mismos que los de la funcionalidad existente que se explica en Soporte para aplicaciones web empresariales.

Acceso adaptable a aplicaciones TCP/UDP y HTTP(S)

El acceso adaptable proporciona a los administradores la capacidad de controlar el acceso a las aplicaciones críticas para la empresa en función de varios factores contextuales, como la verificación de la postura del dispositivo, la ubicación geográfica del usuario, el rol del usuario y la puntuación de riesgo proporcionada por el servicio Citrix Analytics.

> **Nota:**
>
> - Puede denegar el acceso a las aplicaciones TCP/UDP, los administradores crean directivas basadas en los usuarios, los grupos de usuarios, los dispositivos desde los que los usuarios acceden a las aplicaciones y la ubicación (país) desde donde se accede a una aplicación. El acceso a las aplicaciones está permitido de forma predeterminada.
> - La suscripción de usuario realizada para una aplicación es aplicable a todos los destinos de aplicaciones TCP/UDP configurados para las aplicaciones TCP/UDP.

Para crear una directiva de acceso adaptable

Los administradores pueden usar el asistente de flujo de trabajo guiado por el administrador para configurar Zero Trust Network Access a las aplicaciones SaaS, las aplicaciones web internas y las aplicaciones TCP/UDP en el servicio Secure Private Access.

> **Nota:**
>
> - Para obtener más información sobre la creación de una directiva de acceso adaptable, consulte Crear directivas de acceso.

> - Para obtener una configuración integral de Zero Trust Network Access a las aplicaciones SaaS, las aplicaciones web internas y las aplicaciones TCP/UDP en el servicio Secure Private Access, consulte Flujo de trabajo guiado por el administrador para facilitar la incorporación y la configuración.

Puntos que tener en cuenta

- El acceso a una aplicación web existente para la que esté habilitada la seguridad mejorada se deniega a través del cliente de acceso seguro. Aparece un mensaje de error que sugiere iniciar sesión con la aplicación Citrix Workspace.
- Las configuraciones de directivas para la aplicación web basadas en la puntuación de riesgo del usuario, la comprobación de la postura del dispositivo, etc. a través de la aplicación Citrix Workspace, se aplican al acceder a la aplicación a través del cliente Secure Access.
- La directiva vinculada a una aplicación se aplica a todos los destinos de la aplicación.

Resolución de DNS

El dispositivo conector debe tener una configuración de servidor DNS para la resolución de DNS.

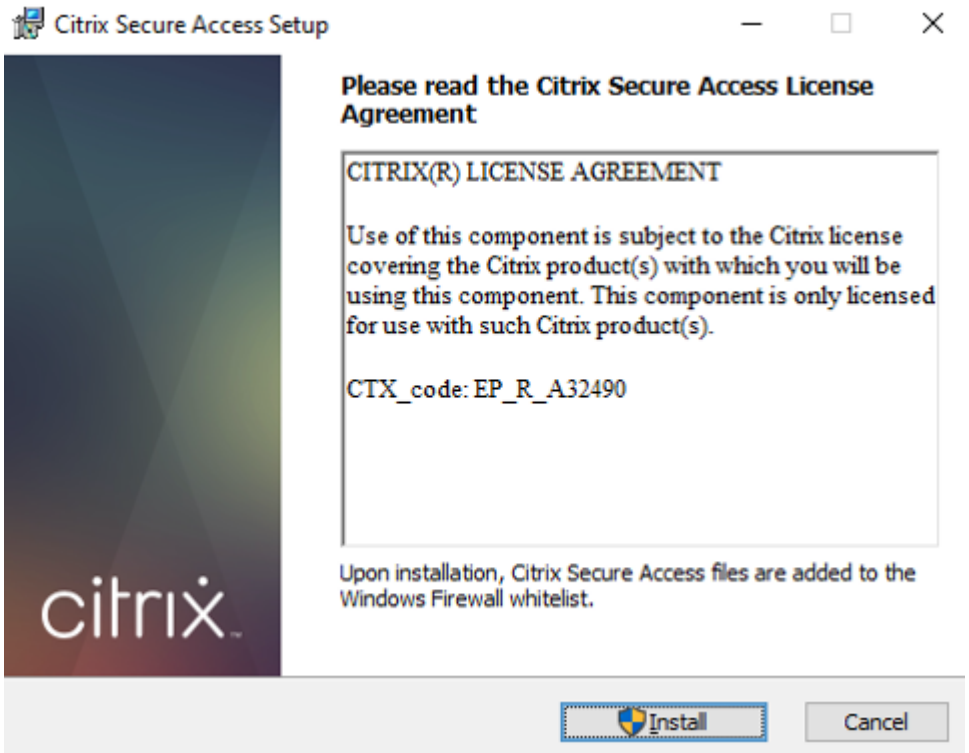
Pasos para instalar el cliente Citrix Secure Access en una máquina Windows

Versiones de SO compatibles:

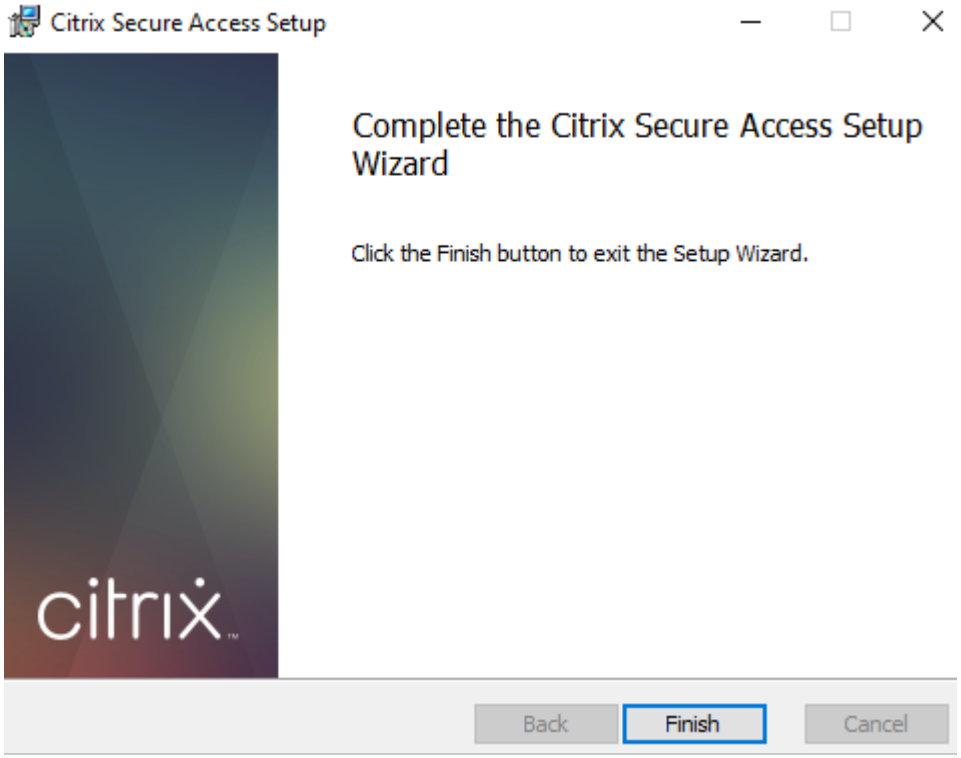
Windows: Windows 11, Windows 10, Windows Server 2016 y Windows Server 2019.

Los siguientes son 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, se actualiza el mismo.



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



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

pasos de instalación de Microsoft Edge Runtime

Ahora se requiere Microsoft Edge Runtime para la interfaz de usuario de autenticación en el cliente de Secure Access.
Se instala de forma predeterminada en las últimas máquinas con Windows 10 y Windows 11. Para máquinas de versiones anteriores, lleve a cabo los siguientes pasos.

1. Vaya al siguiente enlace: https://go.microsoft.com/fwlink/p/?LinkId=2124703.
2. Descargue e instale Microsoft Edge. Si el sistema de usuario no tiene instalado el motor de ejecución de Microsoft Edge, el cliente Citrix Secure Access le pide que lo instale cuando intente conectarse a la URL de Workspace.

> **Nota:**
>
> Puede usar una solución automatizada, como el software SCCM, o una política de grupo para enviar el cliente Citrix Secure Access o Microsoft Edge Runtime a las máquinas cliente.

Pasos para instalar el cliente Citrix Secure Access en una máquina macOS

Requisitos previos:

- Descargue el cliente Citrix Secure Access para macOS de la App Store. Esta aplicación está disponible en 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 de VPN y vuelva a crear el mismo perfil.

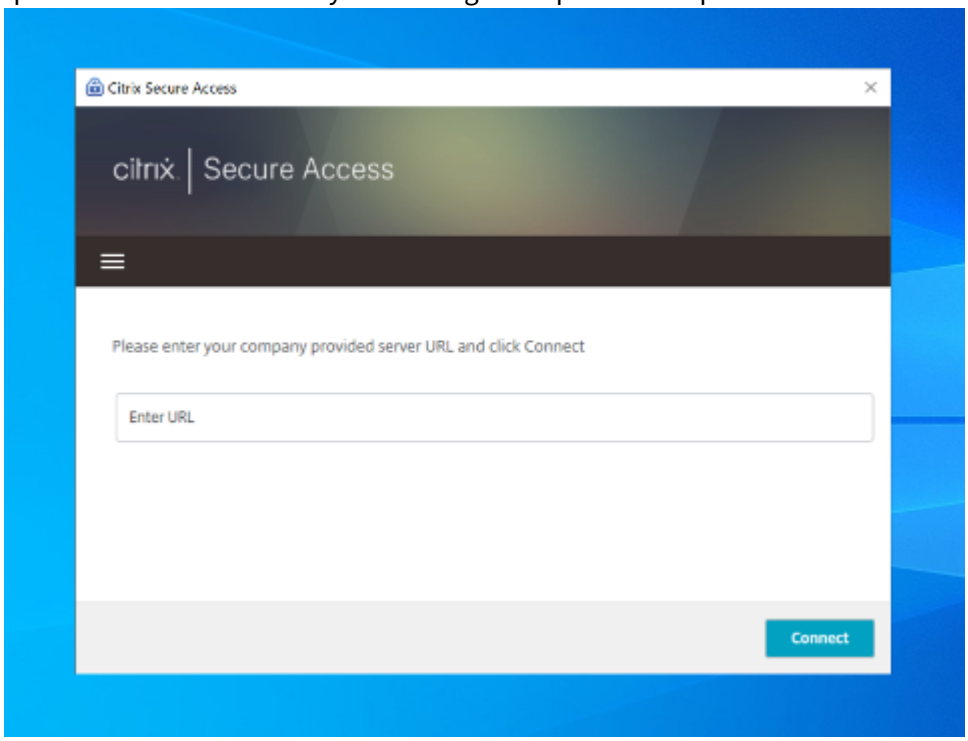
Versiones de SO compatibles:

- Se admiten macOS: 12.x (Monterey), 11.x (Big Sur) y 10.15 (Catalina).
- Dispositivos móviles: iOS y Android no son compatibles.

Iniciar una aplicación configurada: flujo de usuarios finales

1. Inicie el cliente Citrix Secure Access en el dispositivo cliente.
2. Introduzca la URL del espacio de trabajo proporcionada por el administrador del cliente en el campo URL del cliente Citrix Secure Access y haga clic en **Conectar**. Se trata de una actividad

que se realiza una sola vez y la URL se guarda para su uso posterior.



3. Se solicita al usuario que se autentique según el método de autenticación configurado en Citrix Cloud.
   Tras la autenticación correcta, el usuario puede acceder a las aplicaciones privadas configuradas.

Mensajes de notificación al usuario

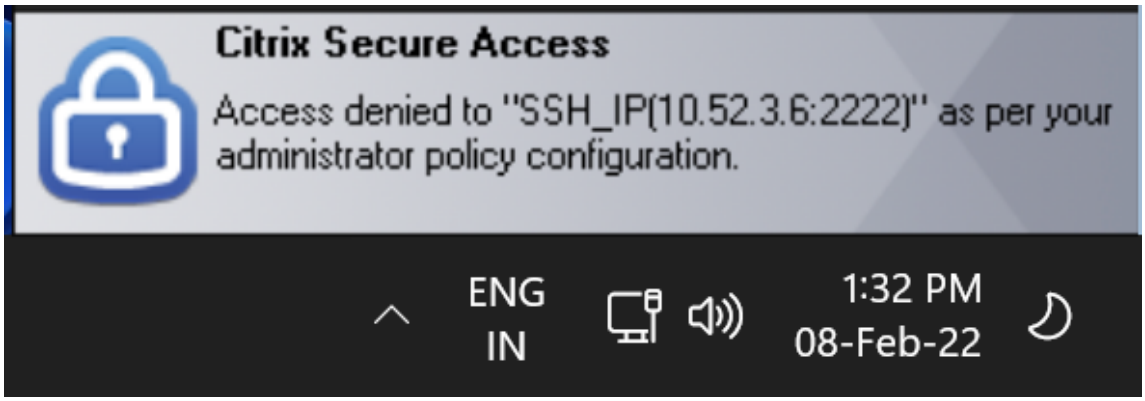
Aparece un mensaje de notificación emergente en los siguientes casos:

- El administrador no autoriza la aplicación para el usuario.

  Causa: la aplicación configurada para la dirección IP o el FQDN de destino a los que se accede no está suscrita para el usuario que ha iniciado sesión.

- La evaluación de la directiva de acceso da lugar a denegación de acceso.

  Causa: se deniega el acceso a la dirección IP o al FQDN de destino porque la directiva enlazada a la aplicación se evalúa como “Denegar acceso”al usuario que ha iniciado sesión.



- El control de seguridad mejorado está habilitado para la aplicación.

  Causa: el control de seguridad mejorado está habilitado para la aplicación para el destino al que se accede. La aplicación se puede iniciar mediante la aplicación Citrix Workspace.

Información adicional

Dominios de aplicación: resolución de conflictos de direcciones IP

Los destinos que se agregan al crear una aplicación se agregan a una tabla de redirección principal. La tabla de enrutamiento es la fuente de información veraz para tomar la decisión de enrutamiento a fin de dirigir el establecimiento de la conexión y el tráfico a la ubicación de recursos correcta.

- La dirección IP de destino debe ser única en todas las ubicaciones de recursos.
- Citrix recomienda evitar la superposición de direcciones IP o dominios en la tabla de enrutamiento. En caso de que encuentre una superposición, debe resolverla.

A continuación se presentan los tipos de casos de conflicto. La **superposición completa** es el único caso de error que restringe la configuración del administrador hasta que se resuelva el conflicto.

Casos de conflicto	Entrada de dominio de aplicación existente	Nueva entrada desde la adición de aplicaciones	Comportamiento
Superposición de subconjunto	10.10.10.0-10.10.10.255 RL1	10.10.10.50-10.10.10.60 RL1	Permitir; Información de advertencia: superposición de subconjuntos del dominio IP con las entradas existentes
Superposición de subconjunto	10.10.10.0-10.10.10.255 RL1	10.10.10.50-10.10.10.60 RL2	Permitir; Información de advertencia: Superposición de subconjuntos del dominio IP con las entradas existentes
Superposición parcial	10.10.10.0-10.10.10.100 RL1	10.10.10.50-10.10.10.200 RL1	Permitir; Información de advertencia: superposición parcial del dominio IP con las entradas existentes
Superposición parcial	10.10.10.0-10.10.10.100 RL1	10.10.10.50-10.10.10.200 RL2	Permitir; Información de advertencia: superposición parcial del dominio IP con las entradas existentes
Superposición completa	10.10.10.0/24 RL1	10.10.10.0-10.10.10.255 RL1	Error; el dominio de IP `<Completely overlapping IP domain's value>` se superpone completamente con las entradas existentes. Cambie la entrada IP de redirección existente o configure un destino diferente

Casos de conflicto	Entrada de dominio de aplicación existente	Nueva entrada desde la adición de aplicaciones	Comportamiento
Superposición completa	10.10.10.0/24 RL1	10.10.10.0-10.10.10.255 RL2	Error; el dominio de IP `<Completely overlapping IP domain's value>` se superpone completamente con las entradas existentes. Cambie la entrada IP de redirección existente o configure un destino diferente
Coincidencia exacta	20.20.20.0/29 RL1	20.20.20.0/29	Permitir; los dominios existen en la tabla de enrutamiento de dominios. Los cambios realizados actualizan la tabla de redirección de dominios

Nota:

- Si los destinos agregados resultan en una superposición completa, se muestra un error al configurar la aplicación en la sección **Detalles de la aplicación**. El administrador debe resolver este error modificando los destinos en la sección **Conectividad de aplicaciones**.

  Si no hay errores en la sección **Detalles de la aplicación**, el administrador puede proceder a guardar los detalles de la aplicación. Sin embargo, en la sección **Conectividad de aplicaciones**, si los destinos tienen un subconjunto y una superposición parcial entre sí o con entradas existentes en la tabla de redirección principal, se muestra un mensaje de advertencia. En este caso, el administrador puede optar por resolver el error o continuar con la configuración.

- Citrix recomienda mantener una tabla de **dominio de aplicación** limpia. Es más fácil configurar nuevas entradas de redirección si los dominios de las direcciones IP se dividen en fragmentos apropiados sin superposiciones.

Registros de configuración de scripts de inicio y cierre de sesión

El cliente de Citrix Secure Access accede a la configuración del script de inicio y cierre de sesión desde los siguientes registros cuando el cliente de Citrix Secure Access se conecta al servicio en la nube de Citrix Secure Private Access.

Registro: HKEY_LOCAL_MACHINE>SOFTWARE>Citrix>Secure Access Client

- Ruta del script de inicio de sesión: SecureAccessLogInScript type REG_SZ
- Ruta del script de cierre de sesión: SecureAccessLogOutScript type REG_SZ

Referencias a las notas

- Notas de la versión de Citrix Secure Access para Windows
- Notas de la versión de Citrix Secure Access para macOS
- Notas de la versión de Citrix Secure Private Access

Direcciones CIDR reservadas para los servidores TCP y UDP

December 27, 2023

Los administradores pueden configurar direcciones IP CIDR reservadas para los servidores TCP/UDP. Estas direcciones IP se comparten en la respuesta de DNS en lugar de la dirección IP real durante la resolución de DNS.

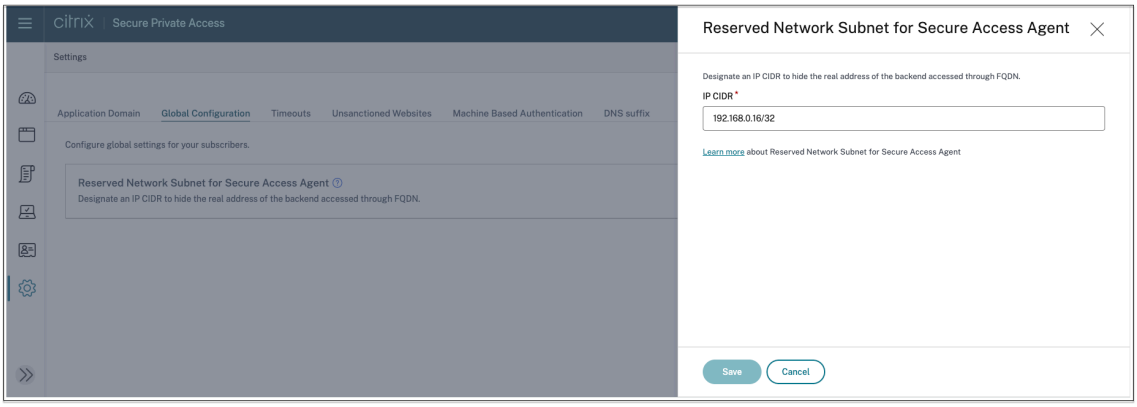
Los siguientes son los rangos de direcciones IP CIDR reservados permitidos:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

> **Nota:**
>
> Asegúrese de que las direcciones IP reservadas no entren en conflicto con lo siguiente:
>
> - Dirección IP configurada para aplicaciones TCP/UDP en la ubicación de recursos del cliente.
> - Subred de red de las máquinas cliente.

Configurar direcciones IP CIDR reservadas

1. Haga clic en **Configuración**y, a continuación, en **Configuración global**.



2. En **Subred de red reservada para Secure Access Agent**, haga clic en **Administrar**.
3. En **IP CIDR**, introduzca el rango de direcciones IP privadas.
4. Haga clic en **Guardar**.

Sufijos DNS para convertir los FQDN en direcciones IP

December 27, 2023

El sufijo DNS es una configuración global que se aplica a todos los usuarios finales. La función de sufijo DNS de Citrix Secure Private Access Service se puede utilizar para los siguientes casos de uso:

- Permita que el cliente Citrix Secure Access resuelva un nombre de dominio no completo (nombre de host) en un nombre de dominio completo (FQDN) agregando el dominio con sufijo DNS para los servidores de fondo.
- Permita a los administradores configurar las aplicaciones mediante direcciones IP (intervalo IP CIDR/IP), de modo que los usuarios finales puedan acceder a las aplicaciones mediante el FQDN correspondiente en el dominio del sufijo DNS.

Por ejemplo, al resolver un nombre de dominio no completo “workday”, si el sufijo DNS “citrix.net”está configurado, el sistema operativo agrega el sufijo “citrix.net”y lo resuelve como “workday.citrix.net”.

Si se configuran varios sufijos DNS, los sufijos DNS se resuelven en una secuencia. Por ejemplo, supongamos que se agregan los siguientes sufijos:

- `".citrix.net"`
- `".citrix.com"`
- `".xenserver.com"`

Cuando un usuario final escribe “workday”, el sistema operativo intenta resolver los FQDN en la siguiente secuencia. Si tiene éxito con un sufijo, se omiten los sufijos restantes.

1. workday.citrix.net
2. workday.citrix.com
3. workday.xenserver.com

> **Importante:**
>
> - La configuración del sufijo DNS solo puede permitir al cliente resolver un nombre de dominio no totalmente cualificado mediante el sufijo del dominio configurado mediante la función de sufijo DNS. Para que un usuario final pueda acceder a un FQDN en el dominio de sufijo DNS, el administrador debe configurar una aplicación con una dirección IP, un FQDN o un dominio comodín. Para obtener más información, consulte el punto 4 del Ejemplo de caso de uso.
> - Si se configuran dos aplicaciones diferentes, una con FQDN y otra con dirección IP (ambas correspondientes al mismo servidor de fondo), la directiva de la aplicación con la dirección IP tiene mayor prioridad. Para obtener más información, consulte el punto 5 del Ejemplo de caso de uso.

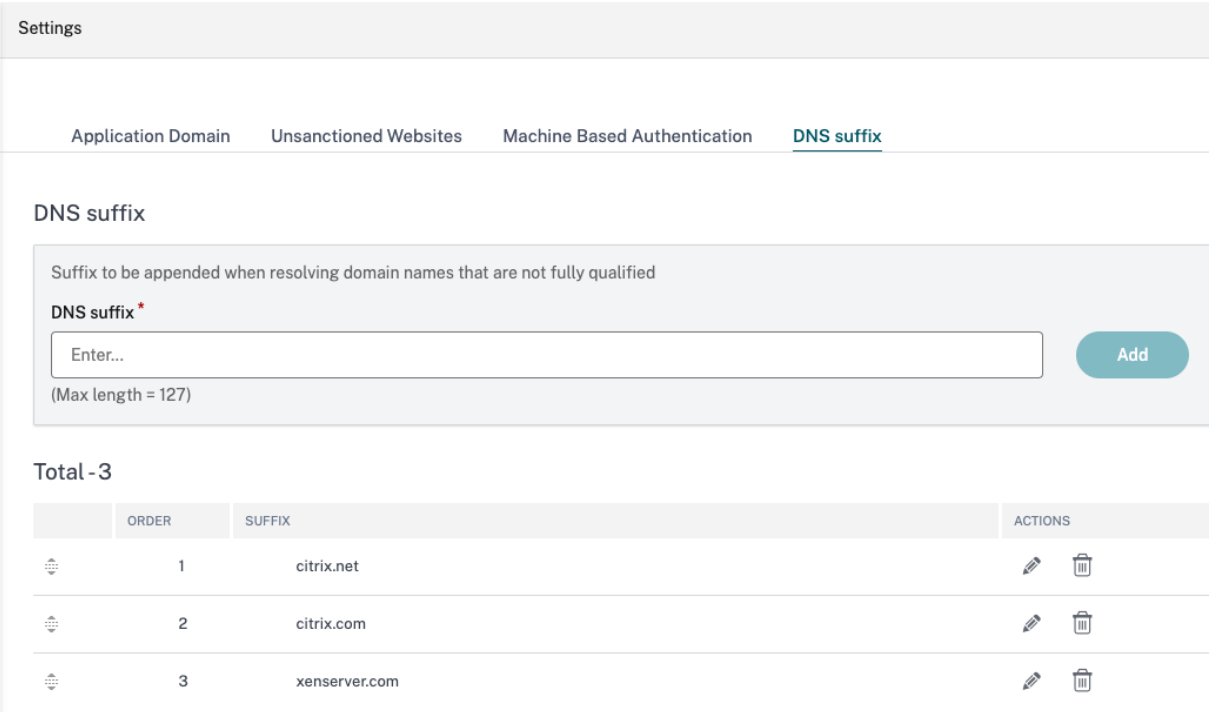
Requisitos previos

> - Los clientes deben tener derecho a la edición Secure Private Access Advanced para utilizar la función de sufijos DNS.
> - Póngase en contacto con el equipo de administración de productos de Citrix para habilitar los marcadores de funciones del sufijo DNS.

Cómo agregar sufijos DNS

1. En el mosaico de Secure Private Access, haga clic en **Administrar**.
2. En la página de inicio de Secure Private Access, haga clic en **Parámetros** y, a continuación, en **Sufijo DNS**.
3. En el campo **Sufijo DNS**, introduzca el sufijo que se debe agregar al resolver un nombre que no esté completamente cualificado.
4. Haga clic en **Agregar**.

Los sufijos se enumeran según el orden en que se agregan. Los administradores pueden eliminar o modificar los sufijos.



Ejemplo de caso de uso

Se deben tener en cuenta las siguientes cuestiones:

- Un administrador ha asignado la dirección IP 192.0.2.1 a una máquina de la red del cliente.
- Los FQDN de la máquina (con direcciones IP 192.0.2.1) se encuentran en el dominio “citrix.net” (por ejemplo, workday.citrix.net).

	Configuración de sufijo DNS y de aplicaciones	Experiencia del usuario final
1	El administrador configura el sufijo DNS como “citrix.net”y crea una aplicación con la dirección IP 192.0.2.1 con una directiva de acceso configurada como “allow”para el usuario1.	Cuando el usuario1 intenta conectarse a “workday”, el FQDN lleva el sufijo “citrix.net” (workday.citrix.net) y la dirección IP se resuelve como 192.0.2.1. Dado que 192.0.2.1 está permitida para el usuario1 con una aplicación configurada, se concede el acceso. **Nota:** El usuario final puede acceder a la aplicación Workday con 192.0.2.1 o workday.citrix.net o “workday”. Sin la configuración del sufijo DNS, se deniega el acceso a través de “workday”y “workday.citrix.net”.

	Configuración de sufijo DNS y de aplicaciones	Experiencia del usuario final
2	El administrador configura el sufijo DNS como “citrix.net”, crea una aplicación con FQDN (workday.citrix.net) y establece la directiva de acceso como “allow”para el usuario1.	Cuando el usuario1 intenta conectarse a “workday”, “citrix.net” lleva el sufijo “workday” (workday.citrix.net). El usuario final puede acceder a Workday porque una aplicación está configurada con “workday.citrix.net”y la directiva de acceso está configurada en “allow”para el usuario1. **Nota:** El usuario final puede acceder a la aplicación Workday con workday.citrix.net o “workday”. Se deniega el acceso a 192.0.2.1 porque no hay ninguna aplicación configurada con esta dirección IP.

	Configuración de sufijo DNS y de aplicaciones	Experiencia del usuario final
3	El administrador configura el sufijo DNS como “citrix.net”, crea una aplicación con el dominio comodín “*.citrix.net”y establece la directiva de acceso como “allow”para el usuario1.	Cuando el usuario1 intenta conectarse a “workday”, “citrix.net” lleva el sufijo “workday” (workday.citrix.net). El usuario final puede acceder a Workday porque una aplicación está configurada con “*.citrix.net”y la directiva de acceso está configurada en “allow”para el usuario1. **Nota:** El usuario final puede acceder a Workday con workday.citrix.net o “workday”. Se deniega el acceso a 192.0.2.1 porque no hay ninguna aplicación configurada con esta dirección IP.

	Configuración de sufijo DNS y de aplicaciones	Experiencia del usuario final
4	El administrador configura el sufijo DNS como “citrix.net”. No hay ninguna aplicación configurada para el usuario1 con FQDN (workday.citrix.net) o 192.0.2.1.	Cuando el usuario1 intenta conectarse a “workday”, el cliente agrega el sufijo “citrix.net”a “workday”y resuelve “workday.citrix.net”en 192.0.2.1. Sin embargo, el usuario1 no puede conectarse al servidor privado (work-day.citrix.net/192.0.2.1) porque no hay ninguna aplicación configurada con 192.0.2.1 o workday.citrix.net o *. citrix.net para el usuario1.

	Configuración de sufijo DNS y de aplicaciones	Experiencia del usuario final
5	El administrador configura el sufijo DNS como “citrix.net”. Agrega una aplicación con la dirección IP 192.0.2.1 y establece la directiva de acceso en “deny”para el usuario1. A continuación, agrega otra aplicación con FQDN (workday.citrix.net) que se resuelve en 192.0.2.1 y establece la directiva de acceso en “allow”para el usuario1.	Cuando el usuario1 intenta conectarse a “workday”, el sufijo “citrix.net”es Workday (workday.citrix.net) y la dirección IP se resuelve como 192.0.2.1. Sin embargo, se deniega el acceso a Workday, ya que la directiva de la aplicación configurada con la IP 192.0.2.1 tiene prioridad sobre la aplicación configurada con FQDN.

Inicio de sesión único en el cliente Citrix Secure Access a través de la aplicación Citrix Workspace

December 27, 2023

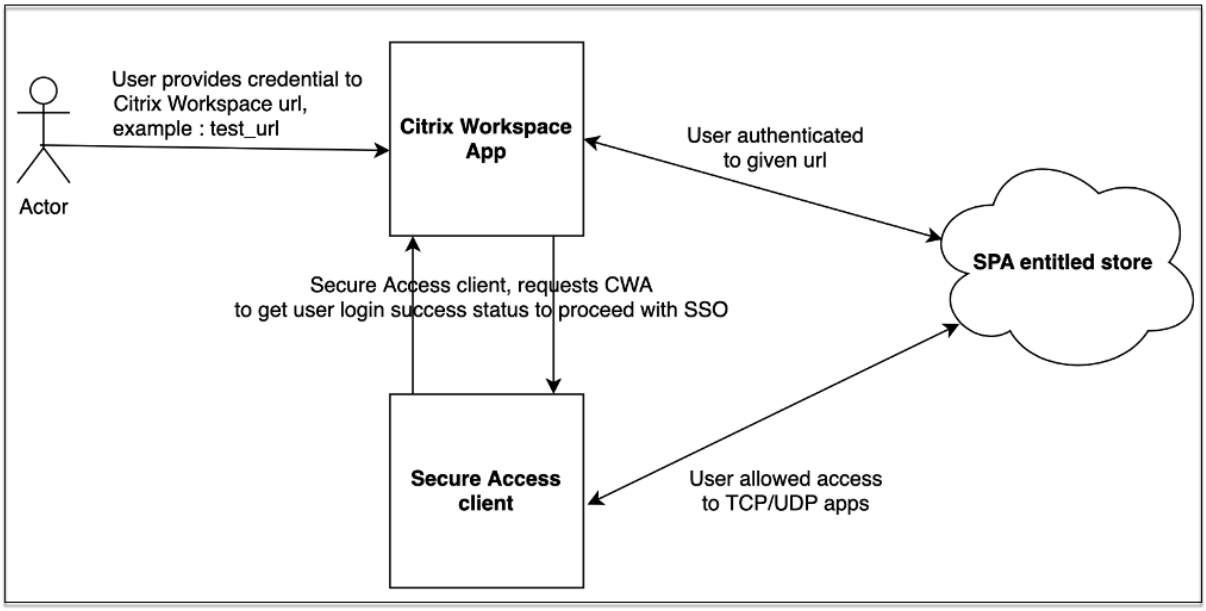
El cliente de Citrix Secure Access ahora admite Single Sign-On para la URL de Workspace cuando ya se ha iniciado sesión a través de la aplicación Citrix Workspace. Esta funcionalidad de SSO mejora la experiencia del usuario al evitar múltiples autenticaciones.

Requisitos previos

- Tanto la aplicación Citrix Workspace como el cliente Secure Access deben estar instalados en el dispositivo.
- Los usuarios deben haber iniciado sesión primero en la aplicación Citrix Workspace para que se produzca el SSO automático en el cliente Citrix Secure Access.

> **Nota:**
>
> La función de inicio de sesión único solo es compatible con el almacén principal que está configurado en la aplicación Citrix Workspace. Si el usuario inicia sesión en cualquier otro almacén que no sea el principal, no se produce el inicio de sesión único. El usuario debe iniciar sesión manualmente en el cliente Citrix Secure Access.

En la siguiente ilustración se muestra el flujo de SSO entre la aplicación Citrix Workspace y el cliente de Citrix Secure Access.



Requisitos de funciones para Windows

- Versión de la aplicación Citrix Workspace: **Citrix Workspace 22.10.5.14 (2210.5) o una versión posterior**
- Versión de Citrix Secure Access: **22.10.1.9 o una versión posterior**
- Registro de Windows de Citrix Secure Access: **EnableCWASSO**

La función SSO está inhabilitada de forma predeterminada. Para habilitar esta función, agregue este Registro en la máquina del usuario final.

- Nombre del Registro: EnableCWASSO
- Ruta del Registro: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
- Tipo de Registro: REG_DWORD
- Valor del Registro: 1

> **Importante:**
>
> A veces, es posible que las máquinas de los usuarios finales tengan que reiniciarse para establecer correctamente el inicio de sesión único con la aplicación Citrix Workspace.

Tiempos de espera para las sesiones de usuario

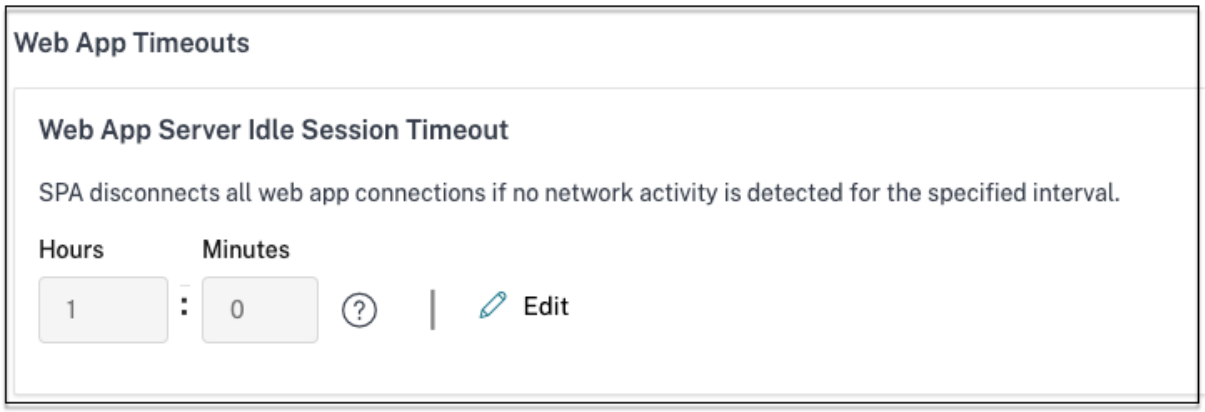
December 27, 2023

Puede configurar un período de espera para que las aplicaciones web y el cliente Citrix Secure Access finalicen las sesiones de los usuarios si no hay actividad en la red durante el período de tiempo especificado.
Para el cliente Citrix Secure Access, también puede configurar el cliente Citrix Secure Access para que finalice una sesión si no hay actividad del usuario durante ese período de tiempo especificado. Además, puede configurar una desconexión forzada en el cliente Citrix Secure Access, independientemente de la actividad del usuario y de la red, una vez que caduque el período de tiempo configurado.

Tiempo de espera para los servidores de aplicaciones web

1. Vaya a **Configuración > Tiempos de espera.**
2. En Tiempo de espera de **sesión inactiva del servidor de aplicaciones web, seleccione el tiempo**, en horas y minutos, durante el que la sesión de la aplicación web puede estar inactiva. El servicio Secure Private Access finaliza la sesión una vez transcurrido este tiempo si la sesión permanece inactiva.

   La duración mínima es de 1 hora y la máxima puede ser de 168 horas. El valor predeterminado es de 2 horas.

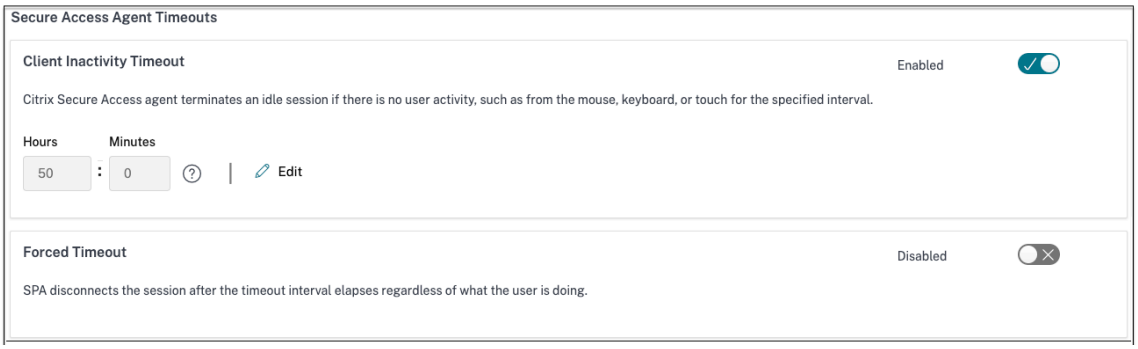


Tiempos de espera para el cliente Citrix Secure Access

Puede configurar los siguientes tiempos de espera para el cliente Citrix Secure Access:

- Inactividad del cliente
- Tiempo de espera forzado

1. Vaya a **Configuración > Tiempos de espera.**



2. En Tiempo de **espera del agente de Secure Access**, seleccione la duración, en horas y minutos, del tiempo de espera que desee aplicar.

   - Tiempo de espera de**inactividad del cliente**: el tiempo después del cual el cliente Citrix Secure Access finaliza una sesión, si no hay actividad del usuario (ratón o teclado) durante el período configurado. Esta opción está desactivada de forma predeterminada. Debe habilitar la opción mediante el botón para aplicar el período de tiempo de espera configurado. Sin embargo, si inhabilita el botón después de guardar la configuración, el cliente no inicia un tiempo de espera.

     La duración mínima es de 5 minutos y la máxima puede ser de 168 horas. El valor predeterminado es 8 horas.

   - **Tiempo de espera forzado**: tiempo transcurrido el cual el cliente Citrix Secure Access finaliza una sesión, independientemente de la actividad del usuario o de la red. Esta opción está desactivada de forma predeterminada. Debe habilitar la opción mediante el botón para aplicar el período de tiempo de espera configurado. Sin embargo, si inhabilita el botón después de guardar la configuración, el cliente no inicia un tiempo de espera.

     Aparece un mensaje de notificación 15 minutos antes de la finalización de la sesión.

     La duración mínima es de 1 hora y la máxima puede ser de 168 horas. El valor predeterminado es 168 horas.

> **Nota:**

> Si habilita más de una de estas configuraciones, el primer intervalo de tiempo de espera que caduque cierra la conexión del usuario.

Migración de controles de seguridad de aplicaciones y directivas de acceso al nuevo marco de directivas de acceso

December 27, 2023

Citrix ha realizado cambios para permitir el acceso a las aplicaciones en el producto. Anteriormente, las aplicaciones debían suscribirse a los usuarios o grupos de usuarios en la sección **Aplicaciones > Suscriptores de aplicaciones** del asistente para permitir el acceso. En adelante, se requiere al menos una directiva de acceso para permitir el acceso a las aplicaciones. Al crear las directivas, la condición de **usuarios o grupos** es una condición obligatoria que debe cumplirse para permitir el acceso a las aplicaciones a los usuarios. Para obtener más información, consulte Crear directivas de acceso.

Además, la sección **Seguridad mejorada** de la configuración de la aplicación está en desuso. Ahora puede aplicar controles de seguridad granulares, como la restricción del portapapeles, la restricción de descarga y las restricciones de impresión, además de opciones avanzadas, como abrir una aplicación en el navegador remoto desde Directivas de acceso. Con este cambio, los clientes pueden aplicar la seguridad adaptativa en función del contexto, como los usuarios, la ubicación, el dispositivo y el riesgo.

Para migrar los controles de seguridad y las directivas de acceso de sus aplicaciones al nuevo marco de directivas de acceso y evitar cualquier tiempo de inactividad en el acceso a las aplicaciones, Citrix ha realizado los cambios necesarios. Como resultado, es posible que observe algunos cambios en su lista de directivas, como los siguientes:

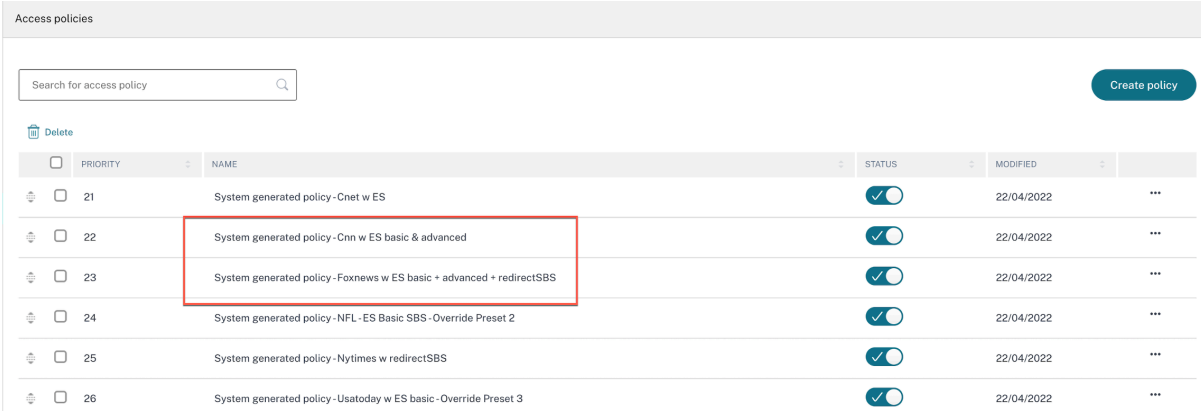
- Creación de directivas
- Una sola directiva dividida en varias directivas
- Nombres de directivas con el prefijo `<System generated policy - App name>`

> **Nota:**
>
> Si las aplicaciones no tienen usuarios o grupos agregados, no se crean nuevas directivas.

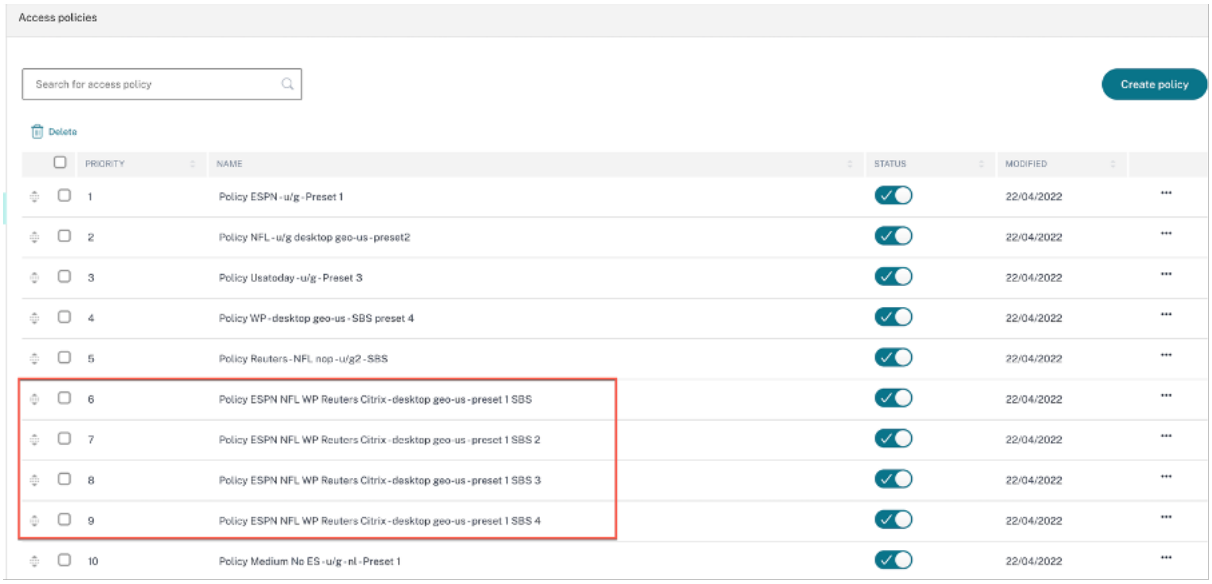
En la siguiente tabla se resumen los cambios.

Si hubiera configurado un…	Entonces…
Aplicación sin condiciones de seguridad mejoradas	Se crea una nueva directiva con usuarios y grupos como condición obligatoria. Los usuarios o grupos se derivan de las directivas de acceso. La acción se establece en **Permitir acceso**.
Aplicación con condiciones de seguridad mejoradas	Se crea una nueva directiva con usuarios y grupos como condición obligatoria. Los usuarios o grupos se derivan de las directivas de acceso. La acción se establece en **Permitir con restricción.** Según la condición de seguridad de nivel de aplicación configurada anteriormente. Las restricciones de seguridad correspondientes se seleccionan al crear la directiva. Las directivas migradas llevan el prefijo `<System generated policy - App name>`.
Directiva de acceso con ajustes preestablecidos	Si la directiva ya tenía una condición de grupo de usuarios seleccionada, entonces se crea una nueva directiva tal cual y las condiciones de seguridad correspondientes se seleccionan en la directiva de acceso en función de los ajustes preestablecidos.
Directiva de acceso sin condición de usuario o grupo	Como los usuarios o grupos son una condición obligatoria para acceder a las aplicaciones, una sola directiva que se configuró para varias aplicaciones ahora se divide en varias directivas, ya que cada aplicación puede tener un conjunto diferente de usuarios o grupos. Los usuarios o grupos se derivan de las directivas de acceso. Para cada directiva, los usuarios o grupos se establecen como condición obligatoria.

En la siguiente figura se muestran ejemplos de nombres de directivas con el prefijo `<System generated policy - App name>`.



La siguiente figura muestra un ejemplo de una sola directiva dividida en varias directivas.



Configuración de aplicaciones mediante una plantilla

December 27, 2023

La configuración de las aplicaciones SaaS con inicio de sesión único en el servicio Secure Private Access se simplifica mediante el aprovisionamiento de una lista de plantillas para las aplicaciones SaaS populares. La aplicación SaaS que se va a configurar se puede seleccionar de la lista.

La plantilla rellena previamente gran parte de la información necesaria para configurar las aplicaciones. Sin embargo, se debe proporcionar la información específica del cliente.

> **Nota:**
>
> La siguiente sección contiene los pasos que se deben realizar en el servicio Secure Private Access para configurar y publicar una aplicación mediante una plantilla. Los pasos de configuración que se deben realizar en el servidor de aplicaciones se presentan en la sección siguiente.

Configurar y publicar aplicaciones mediante una plantilla

En el mosaico **Secure Private Access**, haga clic en **Administrar.**

1. Haga clic en **Continuar** y, a continuación, en **Agregar una aplicación.**

   > **Nota:**
   >
   > El botón **Continuar** solo aparece la primera vez que utilice el asistente. En los usos posteriores, puede navegar directamente a la página **Aplicaciones** y, a continuación, hacer clic en **Agregar una aplicación**.

2. Seleccione la aplicación que quiera configurar en la lista **Elegir una plantilla** y haga clic en **Siguiente.**

3. Introduce los siguientes detalles en la sección **Detalles de la aplicación** y haga clic en **Guardar.**

   Nombre de la aplicación: Nombre de la aplicación.

   Descripción de la aplicación: Una breve descripción de la aplicación. La descripción que introduzca aquí se mostrará a los usuarios del espacio de trabajo.

   Icono de la aplicación: Haga clic en **Cambiar icono** para cambiar el icono de la aplicación. El tamaño del archivo de iconos debe ser de 128 x 128 píxeles. Si no cambia el icono, se muestra el icono predeterminado.

   Si no desea mostrar el icono de la aplicación, seleccione **No mostrar el icono de la aplicación a los usuarios.**

   URL: URL con su ID de cliente. Se redirige al usuario a esta URL si:
   - El inicio de sesión único falla, o
   - Se selecciona la opción **No usar SSO**.

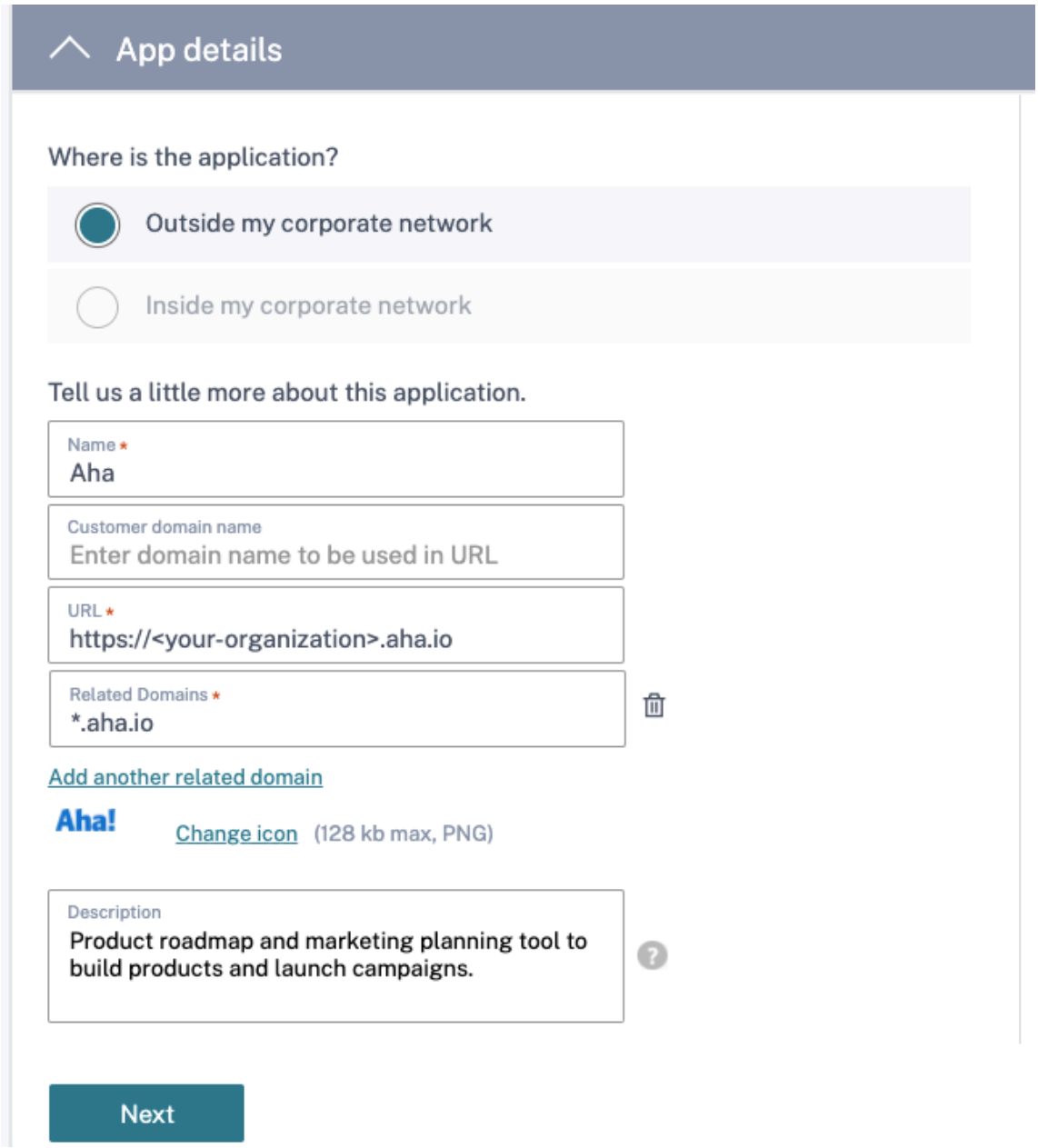
   Nombre de dominio del cliente e **ID de dominio del cliente**: El nombre y el ID de dominio del cliente se utilizan para crear una URL de aplicación y otras URL posteriores en la página de inicio de sesión único de SAML.

   Por ejemplo, si va a agregar una aplicación Salesforce, su nombre de dominio es `salesforceformyorg` y el ID es 123754, la URL de la aplicación es `https://salesforceformyorg.my.salesforce.com/?so=123754`.

Los campos Nombre de dominio del cliente e ID de cliente son específicos de determinadas aplicaciones.

Dominios relacionados: El dominio relacionado se rellena automáticamente en función de la URL que ha proporcionado. El dominio relacionado ayuda al servicio a identificar la URL como parte de la aplicación y a dirigir el tráfico en consecuencia. Puede agregar más de un dominio relacionado.

Icono: Haga clic en el **icono Cambiar** para cambiar el icono de la aplicación. El tamaño del archivo de iconos debe ser de 128 x 128 píxeles. Si no cambia el icono, se muestra el icono predeterminado.



4. Introduzca los siguientes detalles de configuración de SAML en la sección Inicio de **sesión único** y haga clic en **Guardar.**

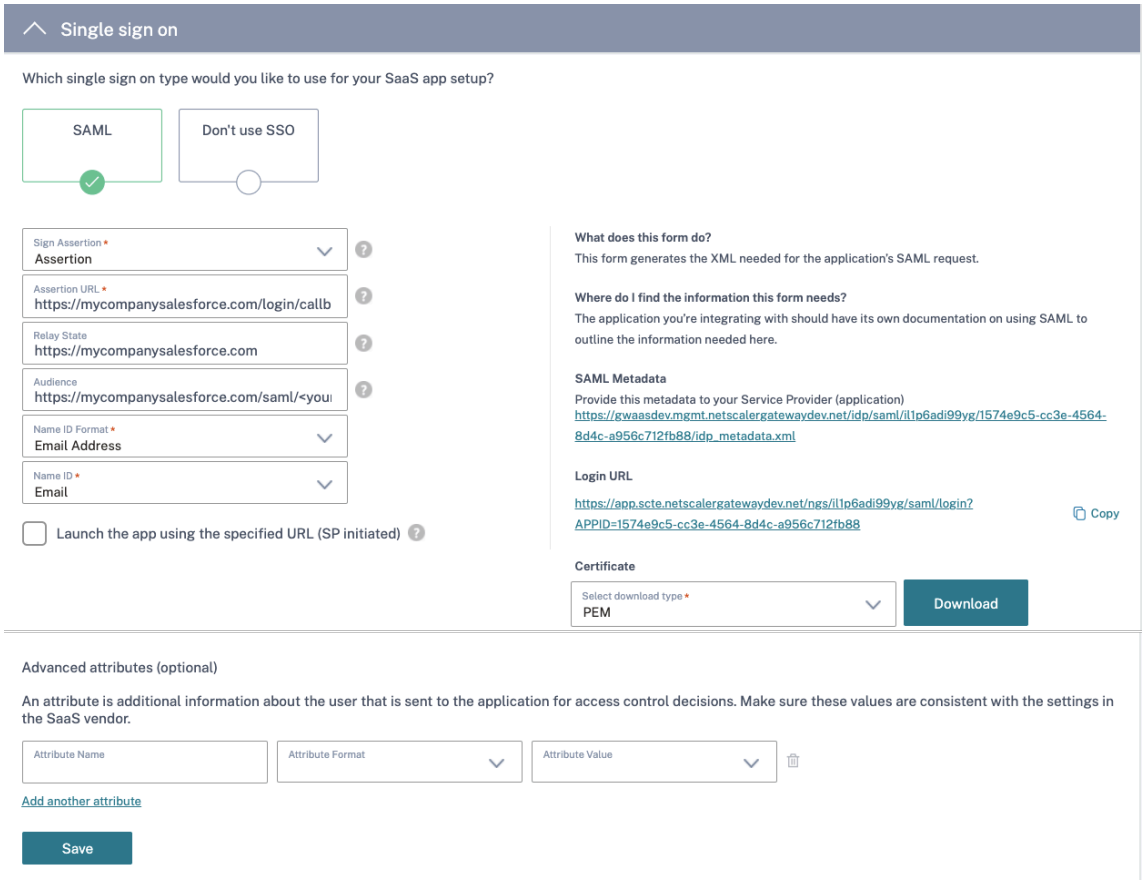
   URL de aserción: URL de aserción SAML de la aplicación SaaS proporcionada por el proveedor de la aplicación. La aserción SAML se envía a esta URL.

   Estado de retransmisión: El parámetro Estado de retransmisión se utiliza para identificar el recurso específico al que acceden los usuarios después de iniciar sesión y dirigirse al servidor de federación de la parte que confía. Relay State genera una única URL para los usuarios. Los usuarios pueden hacer clic en esta URL para iniciar sesión en la aplicación de destino.

   Audiencia: Proveedor de servicios al que va dirigida la afirmación.

   Formato de ID de nombre: Tipo de formato de usuario admitido.

   ID de nombre: nombre del tipo de formato de usuario.



   Nota:

   Cuando se selecciona la opción **No usar SSO**, se redirige al usuario a la URL configurada en la sección **Detalles de la aplicación**.

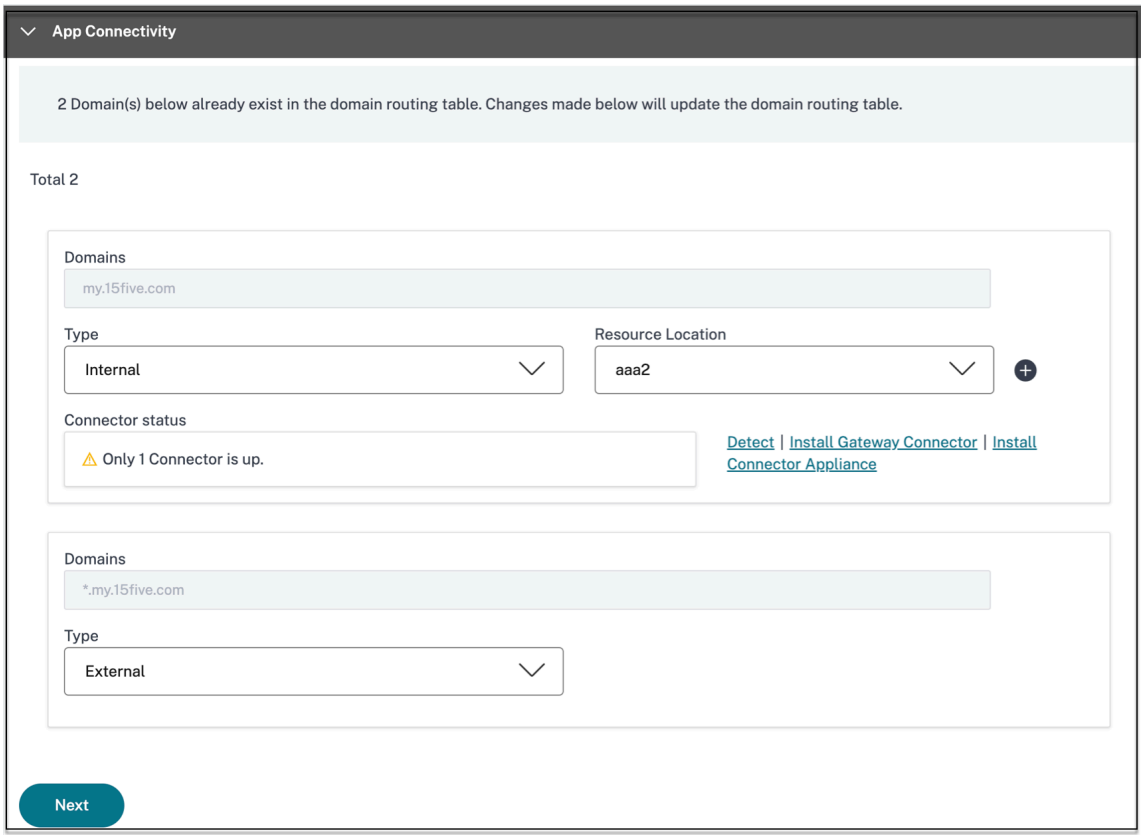
5. Descargue el archivo de metadatos haciendo clic en el enlace situado debajo de **Metadatos SAML.** Utilice el archivo de metadatos descargado para configurar el SSO en el servidor de apli-

caciones SaaS.

Nota:

- Puede copiar la URL de inicio de sesión único en URL de inicio de **sesión** y utilizarla al configurar Single Sign-On en el servidor de aplicaciones SaaS.
- También puede descargar el certificado de la lista de **certificados** y utilizarlo al configurar el inicio de sesión exclusivo en el servidor de aplicaciones SaaS.

6. Haz clic en **Siguiente.**
7. En la sección **Conectividad de aplicaciones**, defina la redirección de los dominios relacionados de las aplicaciones, si los dominios deben redirigirse de manera externa o interna a través de un Connector Appliance de Citrix. Para obtener más información, consulte Tablas de redirección para resolver conflictos si los dominios relacionados en las aplicaciones web y SaaS son los mismos.



8. Haz clic en **Finalizar.**

   Después de hacer clic en **Finalizar**, la aplicación se agrega a la página Aplicaciones. Puede modificar o eliminar una aplicación desde la página Aplicaciones después de haberla configurado. Para hacerlo, haga clic en el botón de puntos suspensivos de una aplicación y seleccione las acciones correspondientes.

- **Modificar aplicación**
- **Suprimir**

> **Nota:**
>
> Para conceder acceso a las aplicaciones a los usuarios, los administradores deben crear directivas de acceso. En las directivas de acceso, los administradores agregan suscriptores a la aplicación y configuran los controles de seguridad. Para obtener más información, consulte Crear directivas de acceso.

Configuración específica del servidor de aplicaciones SaaS

December 27, 2023

A continuación se presentan los enlaces a los documentos que contienen instrucciones sobre la configuración específica del servidor de aplicaciones mediante una plantilla. Actualmente, Citrix admite las siguientes aplicaciones SaaS, aunque sigue alimentando la lista.

- 15Five: Herramienta de gestión continua del rendimiento para entrenar a los empleados.
- 10000 ft: Herramienta de gestión de proyectos para planificar el crecimiento.
- 4me: Herramienta de gestión de servicios para la colaboración entre equipos internos, externos y subcontratados.
- Abacus: Software de informes de gastos en tiempo real.
- Absorb: Herramienta de gestión del aprendizaje.
- Accompa: Herramienta de gestión de requisitos para crear productos.
- Adobe Captivate Prime: Sistema de gestión del aprendizaje para ofrecer experiencias de aprendizaje personalizadas en todos los dispositivos.
- Aha: Hoja de ruta de productos y herramienta de planificación de marketing para crear productos y lanzar campañas.
- AlertOps: Herramienta de respuesta a incidencias de colaboración para gestionar incidentes de TI.
- Allocadia: Herramienta de gestión del rendimiento de marketing para gestionar el proceso de planificación de marketing de una organización. ‘
- Anaplan: Herramienta de planificación para ayudar a las organizaciones a tomar decisiones conectando datos, personas y planes.
- &frankly: Una herramienta de interacción para impulsar el cambio en el lugar de trabajo.

- Anodot: Una plataforma de IA que supervisa datos de series temporales, detecta anomalías y pronostica el rendimiento del negocio en tiempo real.
- App Follow: Herramienta de gestión de productos para acelerar el crecimiento global de las aplicaciones y aumentar la fidelidad de los clientes.
- Assembla: Herramienta de control de versiones y gestión del código fuente para el desarrollo de software.
- Automox: Herramienta de gestión de parches para realizar un seguimiento, controlar y gestionar el proceso de aplicación de parches.
- Azendoo: Herramienta de colaboración para que los equipos conversen y colaboren.
- BambooHR: Herramienta de gestión de recursos humanos para gestionar los datos de los empleados.
- Bananatag: Herramienta para rastrear y programar correos electrónicos, rastrear archivos y crear plantillas de correo electrónico
- Base CRM: Herramienta de gestión de ventas para administrar correos electrónicos, llamadas telefónicas y notas.
- Beekeeper: Herramienta para integrar múltiples sistemas operativos y canales de comunicación en un Secure Hub al que se puede acceder desde dispositivos móviles y de escritorio.
- BitaBIZ: Herramienta de comunicación y planificación de ausencias y vacaciones para la gestión de licencias y ausencias.
- BlazeMeter: Paquete de software de pruebas.
- Blissbook: Herramienta de gestión de directivas para crear manuales de empleados.
- BlueJeans: Solución de videoconferencia.
- Bold360: Herramienta de chat en vivo para la participación del cliente.
- Bonusly: Herramienta de reconocimiento de empleados y gestión de recompensas para reconocer las contribuciones del equipo.
- Box: Herramienta de gestión de contenido y uso compartido de archivos para administrar, compartir y acceder a su contenido.
- Branch: Una plataforma de enlaces móviles que impulsa los enlaces profundos y los dispositivos móviles.
- Brandfolder: Herramienta de gestión de activos digitales para almacenar y compartir activos digitales.
- Breezy HR: Software de contratación y sistema de seguimiento de solicitantes.

- Buddy Punch - Herramienta de gestión del tiempo para supervisar la asistencia de los empleados.
- Bugsnag: Herramienta de monitorización para gestionar la estabilidad de las aplicaciones y notificar errores y datos de diagnóstico.
- Buildkite: Herramienta de infraestructura para el desarrollo de software de integración continua.
- Bullseye Locations: Herramienta localizadora de tiendas para localizar una tienda o distribuidor en un dispositivo.
- CA Flowdock: Herramienta de colaboración para que los equipos se comuniquen y colaboren.
- CakeHR: Herramienta de gestión de recursos humanos para la gestión de asistencia y rendimiento.
- Cardboard: Herramienta colaborativa de planificación de productos para realizar un seguimiento de la información desorganizada.
- Citrix Cedexis: Herramienta de administración del tráfico para sitios web de gran tamaño para aprovechar el abastecimiento de centros de datos, proveedores de nube y redes de entrega de contenido de varios proveedores.
- CipherCloud: Plataforma que proporciona protección de datos de extremo a extremo y protección contra amenazas avanzada, así como capacidades completas de cumplimiento normativo para una empresa que adopta aplicaciones basadas en la nube.
- Celoxis: Herramienta de gestión de proyectos para crear planes de proyecto, automatizar el trabajo y colaborar.
- CircleHD: Herramienta de formación, aprendizaje y colaboración para compartir vídeos y diapositivas dentro de la organización.
- Circonus: herramienta de análisis y supervisión de datos para entregar alertas, gráficos, cuadros de mando e inteligencia de aprendizaje automático.
- Cisco Umbrella: Plataforma de seguridad en la nube para proporcionar la primera línea de defensa contra las amenazas en Internet.
- Citrix RightSignature: Una solución para que los documentos se firmen electrónicamente.
- ClearSlide: Herramienta de participación de ventas que permite a los usuarios compartir contenido y material de ventas para la interacción con el cliente.
- Cloudability: Plataforma de gestión de costes en la nube para mejorar la visibilidad, la optimización y la gobernanza en los entornos de nube.
- CloudAMQP: Herramienta de cola de mensajes para pasar mensajes entre procesos y otros sistemas.

- CloudCheckr: Herramienta de gestión de costes, seguridad, generación de informes y análisis para ayudar a los usuarios a optimizar sus implementaciones de AWS y Azure.
- CloudMonix: Herramienta para supervisión y automatización de recursos en la nube y en las instalaciones.
- CloudPassage: Herramienta de visibilidad y supervisión continua para reducir el riesgo cibernético y mantener el cumplimiento normativo.
- CloudRanger: Herramienta para optimizar sus copias de seguridad, recuperación ante desastres y control de servidores para la nube de AWS.
- Clubhouse: Herramienta de gestión de proyectos para el desarrollo de software.
- Coggle: Aplicación web de mapas mentales para crear documentos estructurados jerárquicamente, como un árbol ramificado.
- Comm100: Software de atención al cliente y herramienta de comunicación para profesionales de atención al cliente.
- Confluence: Herramienta de colaboración de contenido para ayudar a los equipos a colaborar y compartir conocimientos.
- ConceptShare: Herramienta de corrección para entregar contenido de forma más rápida, rápida y económica.
- Concur: Herramienta de gestión de viajes y gastos para gestionar los gastos sobre la marcha.
- ConnectWise Control: Herramienta de gestión empresarial para proporcionar soporte y acceso remotos.
- Contactzilla: Herramienta de gestión de contactos para acceder a información de contacto actualizada.
- ContractSafe: Herramienta de gestión de contratos para rastrear, almacenar y gestionar contratos.
- Contentful: Software de contenido para crear, administrar y distribuir contenido a cualquier plataforma.
- Convo: Herramienta de colaboración y comunicación del equipo para conversaciones internas.
- Copper: Herramienta CRM.
- Cronitor: Herramienta de monitorización para trabajos cron.
- Crowdin: Solución que proporciona una localización continua y sin problemas para los desarrolladores.
- Dashlane: Herramienta de administración de contraseñas que también administra billeteras digitales.

- Declaree: Herramienta de gestión de viajes y gastos para viajes de negocios.
- Dell Boomi: Una herramienta de integración para conectar datos y aplicaciones en la nube y locales.
- Deskpro: Herramienta de asistencia técnica para facilitar la gestión de tickets, la autoayuda del cliente y los comentarios de los clientes.
- Deputy: Herramienta de gestión de la fuerza laboral para programar y rastrear el tiempo, las tareas y la comunicación de los empleados.
- DigiCert: Herramienta de gestión de certificados y solución de problemas para certificados SSL para sitios web.
- Dmarcian: Herramienta de supervisión de correo electrónico para filtrar spam, malware y phishing.
- DocuSign: Una herramienta de firma en línea para diferentes documentos, como seguros, médicos y bienes raíces.
- DOME9 ARC: Herramienta de seguridad y cumplimiento para gestionar entornos de nube pública.
- Dropbox: Herramienta de almacenamiento en la nube para compartir y almacenar archivos de forma segura.
- Duo: Herramienta de seguridad para proporcionar un acceso seguro a sus aplicaciones.
- Dynatrace: Servicios de laboratorio médico.
- Easy Projects: Herramienta de gestión de proyectos.
- EdApp: Herramienta de gestión del aprendizaje para el aprendizaje del espacio de trabajo.
- EduBrite: Herramienta de gestión del aprendizaje para crear, entregar y realizar un seguimiento de programas de formación.
- Ekarda: Herramienta de diseño de tarjetas electrónicas.
- Envoy: Herramienta de gestión de visitantes para gestionar personas y paquetes.
- Evernote: Aplicación para tomar notas, organizar, listas de tareas y archivar.
- Expensify: Herramienta de gestión de gastos para la gestión de informes de gastos, seguimiento de recibos y viajes de negocios.
- ezeep: Herramienta de gestión de infraestructura de impresión para imprimir desde cualquier dispositivo, desde cualquier ubicación a cualquier impresora en la nube.
- EZOfficeInventory: Herramienta de gestión de inventario para realizar un seguimiento de todos sus activos y equipos.

- EZRentOut: Herramienta de alquiler de equipos para realizar un seguimiento de la calidad y disponibilidad de los equipos.
- Fastly: Plataforma en la nube perimetral para atender y proteger las aplicaciones más cerca de los usuarios.
- Favro: Herramienta de planificación y colaboración para el flujo organizacional.
- Federated Directory: Herramienta de directorio de contactos entre empresas para buscar en las libretas de direcciones corporativas de diferentes empresas.
- Feeder
- Feedly: Herramienta de agregación de noticias para compilar feeds de noticias de diferentes fuentes.
- FileCloud: Solución de software que proporciona una plataforma de alojamiento y uso compartido de archivos sólida y segura para las organizaciones.
- Fivetran: Herramienta para ayudar a los analistas a replicar datos en un almacén en la nube.
- Flatter Files: Archivador plano digital para dibujos y documentos para proporcionar una forma segura y sencilla de proporcionar acceso al contenido.
- Float: Herramienta de planificación de recursos para la programación de proyectos y la gestión de la utilización de los equipos.
- Flock: Herramienta de colaboración.
- Formstack: Un generador de formularios en línea y una herramienta de recopilación de datos.
- FOSSA: Herramientas automatizadas de análisis de licencias de código abierto y gestión de vulnerabilidades integradas de forma nativa en CI/CD.
- Freshdesk: Herramienta de atención al cliente para ayudar a satisfacer las necesidades de los clientes.
- Freshservice: Herramienta de asistencia técnica de TI para simplificar las operaciones de TI.
- FrontApp: Herramienta de colaboración para gestionar todas las conversaciones en un solo lugar.
- Frontify: Plataforma para facilitar y agilizar las operaciones diarias de branding, marketing y desarrollo.
- Fulcrum: Plataforma de recopilación de datos móviles que le permite crear formularios móviles y recopilar datos fácilmente.
- Fusebill: Software de gestión de facturación y facturación recurrente.
- G-Suite: Conjunto de aplicaciones inteligentes para conectar a las personas de su empresa.
- GetGuru: Software de gestión de conocimientos.

- GitBook: Herramienta para crear y mantener su documentación.
- GitHub: Un servicio de alojamiento basado en web para el control de versiones que utiliza Git para repositorios alojados detrás de un firewall corporativo.
- GitLab: Una plataforma DevOps completa, entregada como una única aplicación.
- GlassFrog: Software para la práctica de Holacracy.
- GoodData: Una plataforma de análisis y BI integrada que proporciona análisis rápidos, fiables y fáciles de usar
- GoToMeeting: Software de reuniones en línea con funciones de videoconferencia HD.
- HackerRank: Proporciona desafíos de programación competitivos para consumidores y empresas.
- HappyFox: Software de mesa de ayuda en línea y sistema de tickets de soporte basado en web.
- Helpjuice: Solución de gestión del conocimiento para crear y mantener bases de conocimiento.
- Help Scout: Software de atención al cliente y herramienta de Knowledge Base para profesionales de atención al cliente.
- Hello sign: Interfaz de firma electrónica para permitir la firma desde cualquier lugar, en cualquier momento y en cualquier dispositivo.
- HelpDocs: Software de bases de conocimientos para guiar a los usuarios cuando están atascados.
- Honeybadger: Herramienta de supervisión del estado de las aplicaciones.
- Harness: Herramienta para la entrega e integración continuas para aplicaciones Java, .NET en AWS, GCP, Azure y Bare Metal.
- HelpDocs: Herramienta para crear una Knowledge Base autorizada para guiar a sus usuarios cuando están atascados.
- Helpmonks: Una plataforma de correo electrónico colaborativa para la colaboración en equipo.
- Hoshinplan: Herramienta para visualizar sus planes estratégicos y rastrear estados en un lienzo.
- Hosted Graphite: Herramienta para supervisar el rendimiento de su sitio web, aplicación, servidor y contenedor.
- Humanity: Software de programación de empleados en línea para gestionar turnos, horarios, nóminas y cronometraje.
- Igloo: Proveedor de soluciones de intranet y lugar de trabajo digital para resolver los desafíos de TI en toda su organización.
- iLobby: Solución de gestión de registro de visitantes basada en la nube.

- Illumio: Sistema de seguridad para evitar la propagación de brechas dentro del centro de datos y los entornos de nube.
- Image Relay: Software de gestión de activos digitales y gestión de marca para organizar y compartir archivos digitales de forma segura.
- Informatica: Herramienta para la integración de aplicaciones SaaS y plataforma para desarrollar e implementar servicios de integración personalizados.
- Intelligent contract: Software de gestión de contratos.
- iMeet Central: Software de gestión de proyectos para especialistas en marketing, agencias creativas y empresas.
- InteractGo: Herramienta para medir datos históricos y en tiempo real sobre el rendimiento del sistema.
- iQualify One: Herramienta de aprendizaje y gestión para ofrecer experiencias de aprendizaje auténticas.
- InsideView: Soluciones de datos e inteligencia para solucionar problemas de ventas, marketing y otros problemas de negocios.
- Insightly: Una gestión de relaciones con los clientes (CRM) basada en la nube y herramientas de gestión de proyectos para pequeñas y medianas empresas.
- ITGlue : Una plataforma de documentación de TI basada en la nube para ayudar a los MSP a estandarizar la documentación, crear bases de conocimientos, gestionar contraseñas y realizar un seguimiento de los dispositivos.
- Jitbit: Software de mesa de ayuda y sistema de tickets para administrar y rastrear los correos electrónicos de solicitudes de soporte entrantes y sus tickets asociados.

JupiterOne: Plataforma de software para crear y gestionar todo su proceso de seguridad.

- Kanbanize: Un software Kanban de cartera en línea para una gestión eficiente.
- Klipfolio: Una plataforma de tablero en línea para crear paneles empresariales potentes en tiempo real para su equipo o sus clientes.
- Jira: Herramienta para planificar, dar seguimiento y gestionar sus incidencias y proyectos.
- Kanban Tool: Software de gestión visual para mejorar el rendimiento de su equipo y aumentar la productividad.
- Keeper Security: Gestor de contraseñas y software de seguridad para proteger sus contraseñas e información privada.
- Kentik: Herramienta para aplicar big data para monitorización de red y rendimiento, protección contra ataques DDoS y análisis de flujos de red ad hoc en tiempo real.

- Kissflow: Herramienta de flujo de trabajo y software de gestión de flujos de trabajo de procesos empresariales para automatizar su proceso de flujo de trabajo.
- KnowBe4: Herramienta para proporcionar formación en concienciación sobre seguridad y phishing simulado.
- KnowledgeOwl: Base de conocimientos y herramienta de creación.
- Kudos: Sistemas de procesos minoristas, de trabajo, de proyectos y de cumplimiento.
- LaunchDarkly: Plataforma de gestión de funciones que permite a los equipos de desarrollo y operaciones controlar el ciclo de vida de las funciones.
- Lifesize: Solución de videoconferencia.
- Litmos: Sistema de gestión del aprendizaje para formación de empleados, formación de clientes, formación de cumplimiento y formación de socios.
- LiquidPlanner: Software de gestión de proyectos online para su negocio.
- LeanKit: Software de gestión del trabajo y procesos empresariales basado en Lean para ayudar a las empresas a visualizar el trabajo, optimizar los procesos y entregar más rápido.
- LiveChat: Software de chat en vivo y mesa de ayuda para empresas.
- LogDNA: Herramienta para recopilar, supervisar, analizar y analizar registros de todas las fuentes en una herramienta de registro centralizada.
- Mango: Software de colaboración en equipo para consolidar y optimizar las aplicaciones aisladas en una única plataforma.
- Manuscript: Una herramienta de escritura que le ayuda a planificar, modificar y compartir su trabajo.
- Marketo: Software de automatización para ayudar a los equipos de marketing a dominar el arte y la ciencia del marketing digital.
- Matomo: Una plataforma de análisis web que evalúa todo el recorrido del usuario de todos los que visitan el sitio web.
- Meisterplan: Software que ayuda a las organizaciones a crear carteras de proyectos.
- Mingle: Una herramienta ágil de colaboración y gestión de proyectos para proporcionar un lugar de trabajo combinado para todo el equipo.
- MojoHelpDesk: Software de mesa de ayuda y sistema de tickets.
- Monday: Software de gestión de equipos para planificar, realizar un seguimiento y colaborar en todo su trabajo en una sola herramienta.
- Mixpanel: Sistema para rastrear las interacciones de los usuarios con la web y los dispositivos móviles.

- MuleSoft: Software de integración para conectar aplicaciones SaaS y empresariales en la nube y en las instalaciones.
- MyWebTimesheets: Sistema de seguimiento del tiempo en línea para realizar un seguimiento del tiempo dedicado a varios proyectos/trabajos/actividades.
- New Edge: Servicio de red de aplicaciones seguro para TI híbrida.
- NextTravel: Herramienta de software de gestión de viajes corporativos.
- N2F: Herramienta de gestión de informes de gastos para gestionar sus gastos de negocio y viajes.
- New Relic: Plataforma de inteligencia digital para medir y supervisar el rendimiento de las aplicaciones y la infraestructura.
- Nmbrs: Software de nómina y recursos humanos en la nube para empresas.
- Nuclino: Software de colaboración para colaborar y compartir información en tiempo real.
- Office 365: El servicio de suscripción basado en la nube de Microsoft.
- OfficeSpace: Plataforma basada en la nube que ayuda a las organizaciones a asignar espacio de trabajo.
- OneDesk: Software de gestión de proyectos y mesa de ayuda para conectar con sus clientes y apoyarlos.
- OpsGenie: Una plataforma de gestión de incidentes para que los equipos de operaciones de TI y DevOps agilicen las alertas y los procesos de resolución de incidentes.
- Orginio: Una herramienta de creación de organigramas en línea para visualizar la estructura organizativa.
- Oomnitza: Solución de plataforma de gestión de activos de TI para rastrear y gestionar activos.
- OpenEye: Aplicación móvil para ver vídeos en directo y grabados en la grabadora Apex.
- Oracle ERP Cloud: Conjunto de aplicaciones de software basadas en la nube para gestionar funciones empresariales.
- Pacific Timesheet: Herramienta de hojas de horas basada en web para nómina, horas de proyecto y gastos.
- PagerDuty: Sistema de gestión de operaciones digitales.
- PandaDoc: Una aplicación móvil para que los usuarios de iPhone accedan a sus documentos, análisis y panel de control directamente desde sus teléfonos móviles.
- Panopta: Herramienta de monitorización de infraestructuras.
- Panorama9: Plataforma de gestión de TI basada en la nube para la supervisión de redes empresariales.

- Papyrs: Editor para diseñar sus propias páginas de intranet.
- ParkMyCloud: Herramienta SaaS de uso único para conectarse a AWS, Azure Services o GCP.
- Peakon: Herramienta para medir y mejorar el compromiso de los empleados.
- People HR: Sistema de software de recursos humanos para todas las funciones clave de RR. HH.
- Pingboard: Herramienta para crear organigramas para organizar equipos y planificar la fuerza laboral.
- Pigeonhole Live: Plataforma interactiva de preguntas y respuestas.
- Pipedrive: CRM de ventas y software de gestión de procesos.
- PlanMyLeave: Sistema de gestión de licencias para gestionar y hacer un seguimiento de las licencias de los empleados.
- PlayVox: Herramienta de supervisión de calidad del servicio al cliente.
- Podbean: Proveedor de servicios de podcast.
- Podio: Una herramienta basada en web para organizar la comunicación del equipo, los procesos empresariales, los datos y el contenido en los espacios de trabajo de gestión de proyectos.
- POPin: Plataforma de resolución de multitudes y aplicación móvil que pone en práctica la participación del equipo para la resolución de problemas
- Postman: Entorno de desarrollo de API.
- Prescreen: Herramienta de seguimiento de candidatos para publicar vacantes de empleo en línea y sin conexión.
- ProductBoard: Herramienta de gestión de productos.
- ProdPad: Software de gestión de productos para desarrollar estrategias de productos.
- Proto.io: Plataforma de creación de prototipos de aplicaciones para crear prototipos totalmente interactivos y de alta fidelidad.
- Proxyclick: Solución de gestión de visitantes basada en la nube para gestionar visitantes, crear su imagen de marca y garantizar la seguridad.
- Pulumi: Plataforma de desarrollo nativa en la nube para contenedores, sin servidor, infraestructura y Kubernetes.
- PurelyHR: Herramienta de gestión de licencias para acceder a los datos de licencias de los empleados.
- Promapp: Herramienta de gestión de procesos empresariales (BPM).
- Prescreen: Sistema de seguimiento de candidatos basado en la nube para publicar vacantes de empleo en línea y fuera de línea.

- QAComplete: Herramienta de gestión de pruebas de software.
- Qualaroo: Herramienta de comentarios para obtener información de los clientes.
- Quality Built, LLC: Herramienta para el sector financiero, de seguros y de la construcción para proporcionar servicios de seguros de calidad de terceros fiables e innovadores.
- Qubole: Plataforma de autoservicio para análisis de big data creada en Amazon.
- Questetra BPM Suite: Plataforma de procesos empresariales basada en web para flujos de trabajo rutinarios.
- QuestionPro: Software de encuestas en línea para crear encuestas y cuestionarios.
- Quandora: Solución de gestión del conocimiento basada en preguntas y respuestas.
- Quip: Paquete de software de productividad colaborativa para dispositivos móviles y web.
- Rackspace: Servicios de computación en la nube administrados.
- ReadCube: Herramienta para la gestión de referencias web, de escritorio y móviles.
- RealtimeBoard: Herramienta de colaboración de pizarra para que las organizaciones colaboren más allá de formatos, herramientas, ubicaciones y zonas horarias.
- Receptive: Herramienta para recopilar comentarios de clientes, equipos y del mercado en un solo lugar.
- Remedyforce: Sistema de asistencia y gestión de servicios de TI.
- Retrace: Herramienta de gestión del rendimiento de las aplicaciones que proporciona seguimiento de errores, agregación de datos y alertas automáticas.
- Robin: Herramientas de experiencia en el lugar de trabajo para programar salas de reuniones de conferencias y reservas de escritorios.
- Rollbar: Herramientas de depuración y alerta de errores en tiempo real para desarrolladores.
- Really Simple Systems: Software CRM basado en la nube para que las pequeñas empresas administren sus ventas y marketing.
- Reamaze: Software de atención al cliente para apoyar, atraer y convertir a los clientes mediante chat, redes sociales, SMS, preguntas frecuentes y correo electrónico en una única plataforma.
- Resource Guru: Software de gestión de recursos para programar personas, equipos y otros recursos.
- Retrace: Gestión del rendimiento de las aplicaciones para integrar perfiles de código, seguimiento de errores, registros de aplicaciones y métricas.
- Roadmunk: Software de hoja de ruta de productos y herramienta de hoja de ruta para crear hojas de ruta de productos.

- Runscope: Herramienta para crear, administrar y realizar pruebas y monitores de API funcionales.
- Salesforce: Herramienta de CRM para gestionar la información de contacto de los clientes, integrar las redes sociales y facilitar la colaboración con los clientes en tiempo real.
- SalesLoft: Plataforma de compromiso de ventas para ventas eficientes y que aumentan los ingresos
- Salsify: Plataforma de gestión de la experiencia del producto (PXM).
- Samanage: Herramienta para la gestión de servicios de TI.
- Samepage: Software de colaboración para gestionar proyectos online.
- Screencast-O-Matic: Herramienta para hacer screencast y modificar vídeo.
- ScreenSteps: Herramientas para crear documentos visuales centrados en capturas de pantalla.
- SendSafely: Plataforma de cifrado para el intercambio seguro de archivos y correos electrónicos.
- Sentry: Software de seguimiento de errores de código abierto.
- ServiceDesk Plus: Herramienta para service desk de TI.
- ServiceNow: Plataforma en la nube para crear flujos de trabajo digitales.
- SharePoint: Plataforma colaborativa utilizada para la administración y el almacenamiento de documentos.
- Shufflrr: Herramienta de gestión de presentaciones para crear, actualizar, compartir y difundir presentaciones.
- Sigma Computing: Una herramienta de análisis para explorar, analizar y visualizar datos.
- Signavio: Una herramienta de modelado de procesos empresariales.
- Skeddly: Herramienta para automatizar los recursos de AWS.
- Skills Base: Herramienta de gestión del talento para realizar un seguimiento y documentar el rendimiento y las habilidades de los empleados.
- Skyprep : Sistema de gestión del aprendizaje (LMS) para formar a clientes y empleados.
- Slack: Herramienta de colaboración para comunicar y compartir información.
- Slemma: Herramienta de análisis de datos para crear informes de datos a partir de varios conjuntos de datos.
- Sli.do: Herramienta de interacción para reuniones, eventos y conferencias.
- SmartDraw: Herramienta de diagramas que se utiliza para crear diagramas de flujo, organigramas, mapas mentales, gráficos de proyectos y otros elementos visuales empresariales.

- SmarterU: Sistema de gestión del aprendizaje (LMS) para formar a clientes y empleados.
- Smartsheet: Herramienta de colaboración para asignar tareas, realizar un seguimiento del proceso del proyecto, administrar calendarios y compartir documentos.
- SparkPost: Servicio de entrega de correo electrónico.
- Split: Aplicación de división de facturas.
- Spoke: Herramienta de asistencia técnica para archivar tíquets de servicio.
- Spotinst: Una plataforma de optimización SaaS que ayuda a las empresas a adquirir y gestionar la capacidad de la infraestructura en la nube.
- SproutVideo: Plataforma para alojar vídeos empresariales.
- Stackify: Herramienta de solución de problemas que proporciona soporte con un conjunto de herramientas que incluyen Prefix y Retrace.
- StatusCast: Página alojada para mantener informados a sus empleados y clientes sobre el tiempo de inactividad y el mantenimiento del sitio web.
- StatusDashboard: Plataforma de comunicaciones para alojar paneles de estado y transmitir notificaciones de incidentes a los clientes.
- Status Hero: Herramienta para realizar un seguimiento de las actualizaciones de estado y los objetivos diarios de su equipo.
- StatusHub: Plataforma para alojar la página de estado del servicio.
- Statuspage: Herramienta para comunicar el estado y las incidencias.
- SugarCRM: Herramienta de CRM para automatización de Salesforce, campañas de marketing, atención al cliente, colaboración, CRM móvil, CRM social e informes.
- Sumo Logic: Software de análisis de datos que se centra en casos de uso de seguridad, operaciones y BI.
- Supermood: Plataforma de recursos humanos para recopilar los comentarios de los empleados en tiempo real.
- Syncplicity: Herramienta para compartir y sincronizar archivos.
- Tableau: Herramienta para crear visualizaciones de datos interactivas.
- TalentLMS: Sistema de gestión del aprendizaje (LMS) para facilitar seminarios, cursos y otros programas de formación en línea.
- Tallie: Herramienta para capturar y cargar recibos, generar informes de gastos y personalizar detalles de gastos.
- Targetprocess: Software de gestión de proyectos ágil para Scrum, Kanban, SAFe, etc.

- Teamphoria: Software para proporcionar métricas de compromiso de los empleados en tiempo real, revisiones y reconocimiento de los empleados.
- TeamViewer: Aplicación de software patentada para control remoto, uso compartido de escritorios, reuniones en línea, conferencias web y transferencia de archivos entre equipos.
- Tenable.io: Herramienta que proporciona datos para identificar, investigar y priorizar la solución de vulnerabilidades y configuraciones erróneas en su entorno de TI.
- Testable: Herramienta para crear experimentos y encuestas conductuales.
- TestingBot: Herramienta para proporcionar varias versiones de explorador para pruebas en vivo y automatizadas.
- TestFairy: Plataforma de pruebas móviles, para proporcionar a las empresas grabaciones de vídeo, registros e informes de fallos de sesiones móviles.
- TextExpander: Herramienta de comunicación para insertar fragmentos de texto de un repositorio de correos electrónicos y otro contenido, a medida que escribe.
- TextMagic: Servicio de mensajería para conectar con los clientes.
- ThousandEyes: Herramienta para supervisar la infraestructura de red, solucionar problemas de entrega de aplicaciones y mapear el rendimiento de Internet.
- Thycotic Secret Server: Herramienta de software de gestión de cuentas para gestionar contraseñas.
- TimeLive: Herramienta para proporcionar hojas de horas y realizar un seguimiento del tiempo.
- Tinfoil Security: Software de solución de seguridad para detectar vulnerabilidades.
- Trisotech: Herramienta que permite a los clientes descubrir, modelar y analizar su empresa digital.
- Trumba: Herramienta para publicar calendarios de eventos online, interactivos.
- TwentyThree: Plataforma de marketing de vídeo para integrar y agregar vídeos a la pila de marketing.
- Twilio: Una plataforma de desarrollo para comunicaciones.
- Ubersmith: Software de gestión empresarial para soluciones de facturación basada en el uso, presupuestos, gestión de pedidos, gestión de infraestructura y tickets de mesa de ayuda.
- UniFi: Software de comunicación y colaboración con funciones de voz, colaboración web y videoconferencia.
- UPTRENDS: Solución de monitorización de sitios web para realizar un seguimiento del tiempo de actividad y el rendimiento

- UserEcho: Herramienta de foro de la comunidad que ayuda a las empresas a gestionar los comentarios de
- UserVoice: Software de gestión de comentarios sobre productos que permite a las empresas tomar decisiones sobre productos basadas en datos.
- VALIMAIL: Software de autenticación de correo electrónico para autenticar correos electrónicos legítimos y bloquear ataques de phishing.
- Veracode: El analizador de código fuente y el escáner de código protegen a las empresas de las amenazas cibernéticas y las puertas traseras de las aplicaciones.
- Velpic: Sistema de gestión del aprendizaje (LMS) diseñado para agilizar la formación en el lugar de trabajo.
- VictorOps: Software de gestión de incidentes para proporcionar observabilidad, colaboración y alertas en tiempo real de DevOps.
- VIDIZMO: Software empresarial de transmisión de vídeo en directo y bajo demanda.
- Visual Paradigm: Plataforma online de modelado visual y diagramación para la colaboración en equipo.
- Vtiger: Herramienta CRM que permite a los equipos de ventas, soporte y marketing organizarse y colaborar.
- WaveMaker: Software para crear y ejecutar aplicaciones personalizadas.
- Weekdone: Herramienta para crear el panel de mandos de los gerentes y el servicio de gestión de equipos para empresas.
- Wepow: Herramienta para conectar a reclutadores, candidatos a puestos de trabajo y empleadores a través de una solución de entrevistas por video y móvil.
- When I Work: Herramienta para la programación de los empleados y el seguimiento del tiempo.
- WhosOnLocation: Herramienta para rastrear el flujo de personas a través de sitios y zonas.
- Workable: Sistema de seguimiento de solicitantes.
- Workday: Herramienta de gestión financiera, recursos humanos y planificación.
- Workpath: Herramienta para gestionar los objetivos y el rendimiento de la organización.
- Workplace: Herramienta de colaboración de Facebook para ayudar a los empleados a comunicarse a través de una interfaz familiar.
- Workstars: Plataforma para programas de reconocimiento de empleados sociales y de pares.
- Workteam: Herramienta para realizar un seguimiento del tiempo y la asistencia de los empleados.
- Wrike: Software de colaboración y gestión de proyectos sociales.

- XaitPorter: Software de coautoría de documentos para licitaciones y propuestas y otros documentos comerciales.
- Ximble: Herramienta para la programación de empleados y el seguimiento del tiempo.
- XMatters: Plataforma de colaboración con un software de alertas que se integra con otras herramientas creando un proceso fluido y una comunicación eficaz.
- Yodeck: Herramienta para gestionar pantallas de forma remota, a través de la web o del móvil.
- Zendesk: Software para solicitar atención al cliente y registrar tickets de soporte.
- Ziflow: Herramienta para equipos de producción creativa.
- Zillable: Plataforma de colaboración con capacidades de comunicación.
- Zing tree: Un kit de herramientas para crear árboles de decisión interactivos y solucionadores de problemas.
- ZIVVER: Herramienta que permite la transferencia segura de correo electrónico y archivos desde su programa de correo electrónico familiar.
- Zoho: Suite de aplicaciones empresariales.
- Zoom: Software de comunicación y colaboración con funciones de voz, colaboración web y videoconferencia.
- Zuora: Un software basado en suscripciones que permite a una empresa lanzar, gestionar y transformarse en un negocio de suscripción.

Iniciar una aplicación configurada: flujo de trabajo del usuario final

December 27, 2023

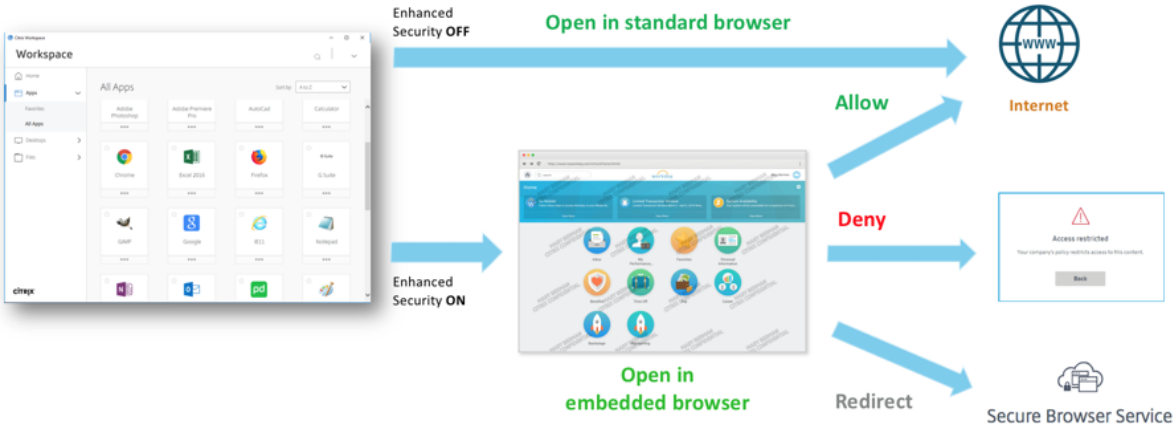
Como usuario final, debe hacer lo siguiente:

1. Descargue la aplicación Citrix Workspace desde https://www.citrix.com/downloads. En la lista **Buscar descargas**, seleccione la **aplicación Citrix Workspace**.
2. Inicie sesión y busque sus aplicaciones SaaS. Haga clic en la aplicación para iniciarla.

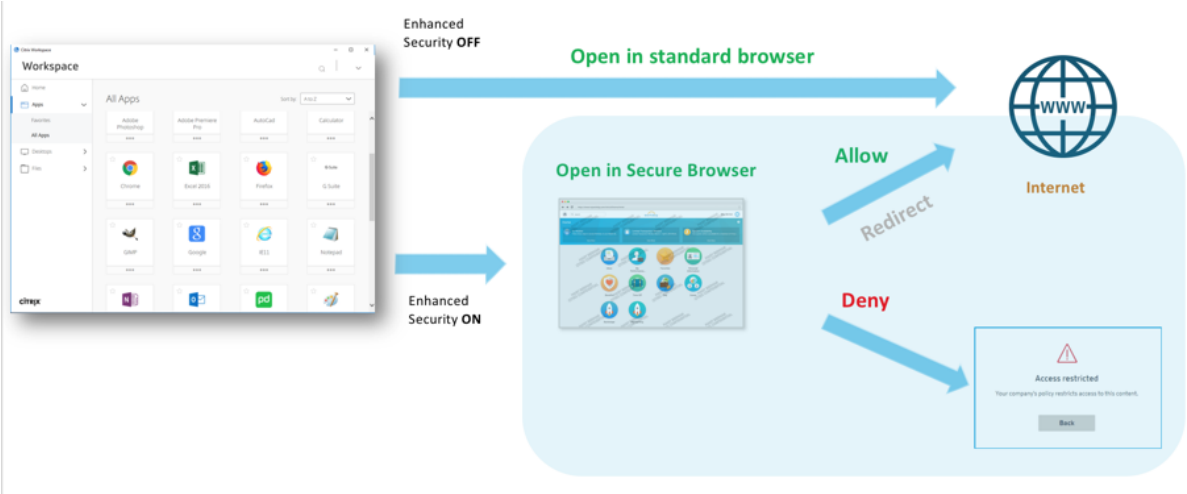
Ahora puede usar la aplicación SaaS desde la aplicación Citrix Workspace o desde el portal web de Citrix Workspace.

Dependiendo de la configuración definida por el administrador, las aplicaciones SaaS se abren con el motor del explorador web dentro de la aplicación Workspace o se le redirige a un explorador web seguro.

En el siguiente diagrama se muestra un flujo de trabajo completo para la aplicación Citrix Workspace.



En el siguiente diagrama se muestra un flujo de trabajo general para el portal web de Citrix Workspace.



Acceso de solo lectura para administradores a aplicaciones SaaS y web

December 27, 2023

Por lo general, las organizaciones comprenden varios administradores y los administradores deben tener distintos niveles de privilegios de acceso. Los equipos de administradores de seguridad que utilizan el servicio Secure Private Access pueden proporcionar controles granulares, como el acceso de solo lectura para los administradores. A los administradores que no agreguen o modifiquen una aplicación se les puede proporcionar acceso de solo lectura para ver los detalles de la aplicación. Los

administradores del servicio Secure Private Access con acceso de solo lectura no pueden realizar las siguientes tareas.

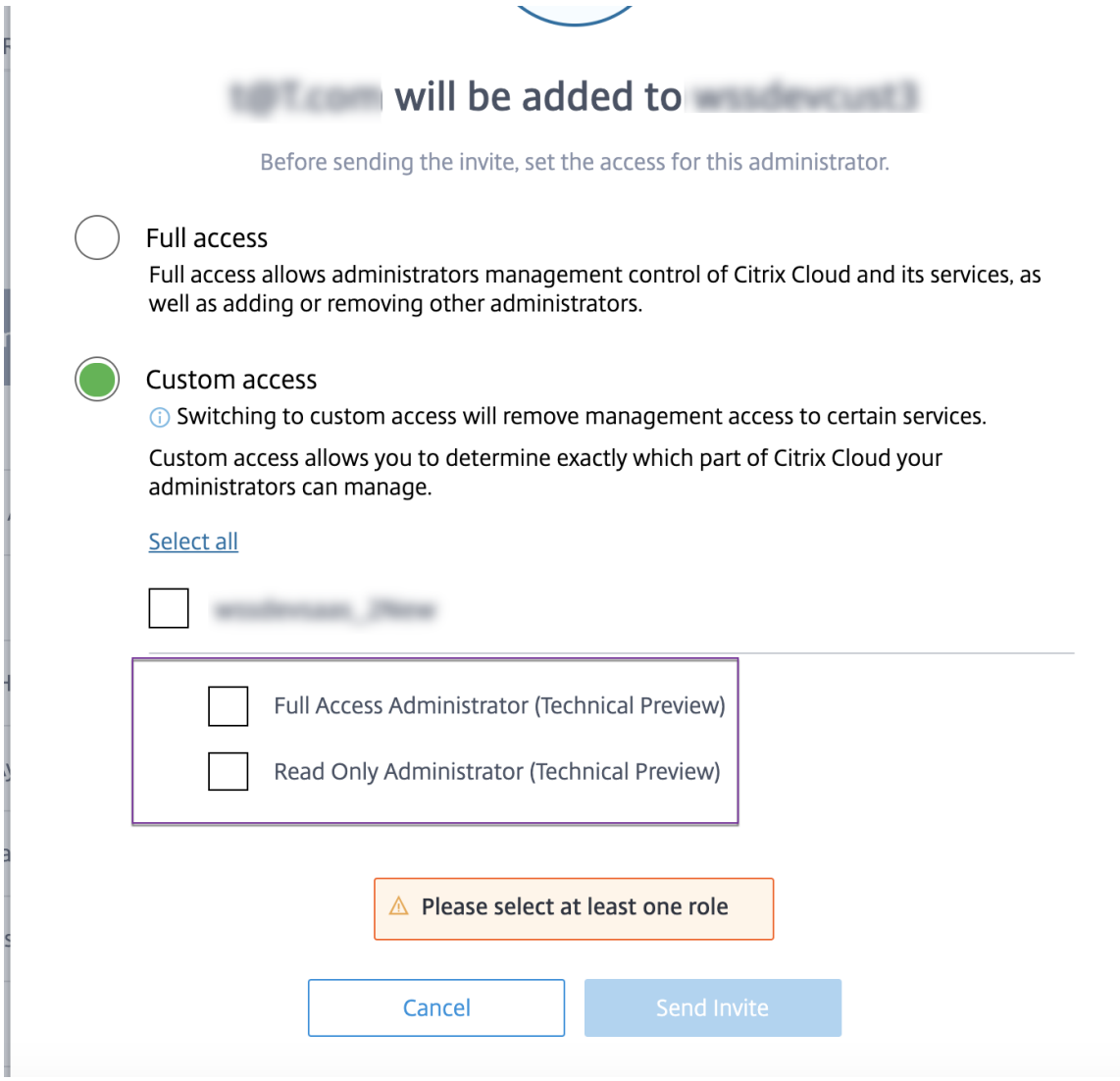
- Agregue aplicaciones web o SaaS empresariales.
- Agregue nuevos dispositivos de conector en ubicaciones de recursos nuevas o existentes.

Cómo proporcionar acceso de solo lectura a los administradores

Después de iniciar sesión en Citrix Cloud, seleccione **Administración de acceso e identidad** en el menú.
En la página Administración de acceso e identidad, haga clic en **Administradores**. La consola muestra todos los administradores actuales de la cuenta.

Agregar un administrador con acceso de solo lectura

1. En **Agregar administradores**, seleccione el proveedor de identidades desde el que desea seleccionar el administrador. A veces, es posible que Citrix Cloud le pida que inicie sesión primero en el proveedor de identidad (por ejemplo, Azure Active Directory).
2. Si se selecciona **Identidad de Citrix**, introduzca la dirección de correo electrónico del usuario y, a continuación, haga clic en **Invitar**.
3. Si Azure Active Directory está seleccionado, escriba el nombre del usuario que quiere agregar y, a continuación, haga clic en Invitar.
4. Seleccione **Acceso personalizado**. Aparecen las siguientes opciones:
   - **Seleccione Administrador de acceso completo (Vista previa técnica)**: Proporciona acceso completo.
   - **Administrador de solo lectura (Vista previa técnica)**: Proporciona acceso de solo lectura.
5. Seleccione **Administrador de solo lectura (Vista previa técnica)**.



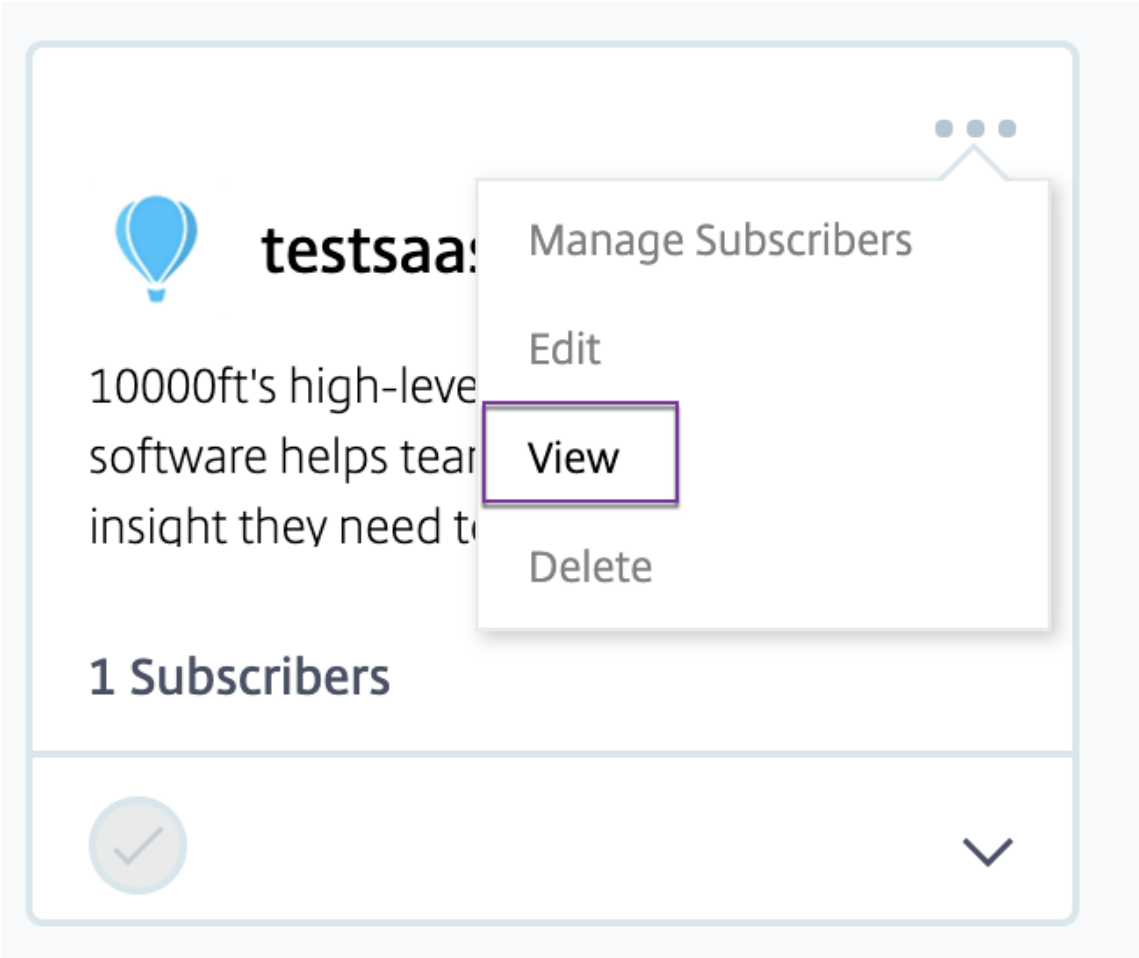
6. Haga clic en **Enviar invitación**.

> **Importante:**
>
> - Cuando proporciona acceso de **administrador de solo lectura** a los administradores del servicio NetScaler Gateway, también debe habilitar la **biblioteca** de la lista de **administración general** para esos administradores. Solo entonces, la opción **Ver** para las aplicaciones está habilitada para los administradores.
> - El botón **Agregar una aplicación web/SaaS** está inhabilitado para los usuarios con acceso de **administrador de solo lectura**.

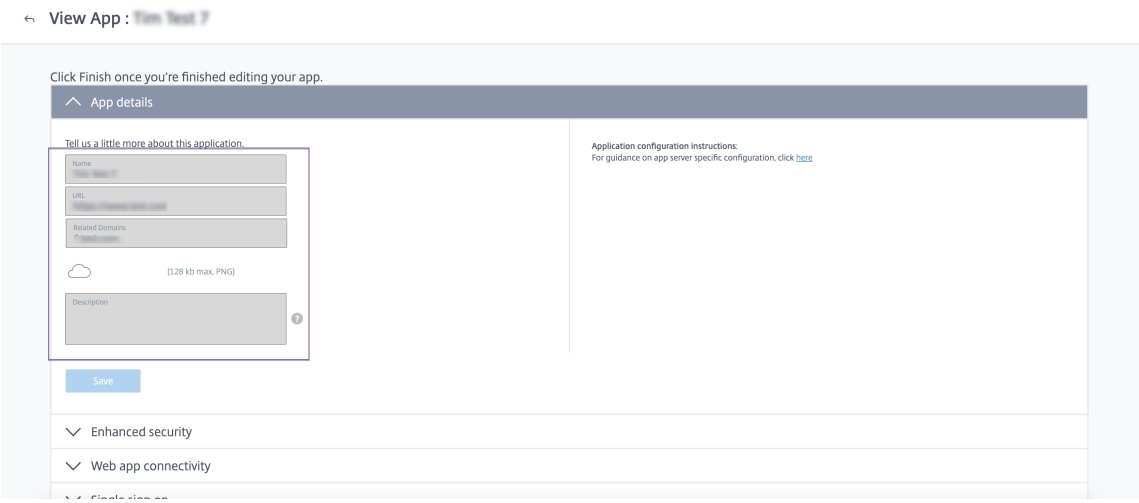
Para ver los detalles de la aplicación cuando los administradores tienen acceso de solo lectura

1. Después de iniciar sesión en Citrix Cloud, seleccione **Biblioteca** en el menú.

2. Seleccione la aplicación en la que desea ver los detalles y haga clic en los **puntos suspensivos**. Solo está habilitada la opción **Ver**. Todas las demás opciones están inhabilitadas.



3. Haga clic en **Ver**.



Acceso denegado a las aplicaciones, de forma predeterminada

February 16, 2024

Para habilitar el acceso basado en la confianza cero a las aplicaciones, se deniega el acceso a las aplicaciones de forma predeterminada. El acceso a las aplicaciones solo está habilitado si hay una directiva de acceso asociada a la aplicación.

- **Acceso a las aplicaciones publicadas:**
  - Cuando un usuario final accede a un FQDN asociado a una aplicación publicada, el acceso solo se permite si se configura explícitamente una directiva de acceso con la acción **Permitir**acceso.

    > **Nota:**
    >
    > Si hay varias aplicaciones que coinciden con el FQDN de la aplicación, las directivas de las aplicaciones coincidentes se evalúan en función de la prioridad de la directiva.

  - Si una directiva de acceso no coincide con la aplicación publicada o si una aplicación no está asociada a una directiva de acceso, se deniega el acceso a la aplicación de forma predeterminada.

    Para obtener más información sobre las directivas de acceso, consulte Directivas de acceso.

- **Acceso a aplicaciones internas o no publicadas.** El acceso a las aplicaciones internas o no publicadas se habilita en función del tipo de enrutamiento definido al configurar la aplicación.
  - Si el tipo de enrutamiento se define como **Externo**, el tráfico fluye directamente a Internet. El acceso está habilitado para dichas aplicaciones.
  - Si el tipo de enrutamiento se define como **interno** o **externo a través del conector**, se deniega el acceso a dichas aplicaciones.
  - Si el tipo de enrutamiento no está definido para un FQDN no publicado, la aplicación se considera externa. El acceso a dichas aplicaciones se basa en las reglas configuradas para las aplicaciones no autorizadas, si están habilitadas. Para obtener más información, consulte Configurar reglas para sitios web no autorizados.

  El tipo de enrutamiento se define en la interfaz de usuario de Secure Private Access. Haga clic en **Configuración > Dominio de la aplicación**. Para obtener más información, consulte Tablas de rutas.

Configuración conflictiva que podría ocasionar problemas de acceso a la aplicación

Si hay varias aplicaciones configuradas con el mismo FQDN o con alguna variación del FQDN comodín, es posible que se produzcan los siguientes problemas.

- Los sitios web dejan de cargarse o pueden mostrar una página en blanco.
- La página "Acceso bloqueado"puede aparecer al acceder a una URL.
- Es posible que la página de inicio de sesión no se cargue.

Recomendaciones

Para abordar los problemas anteriores, recomendamos lo siguiente:

1. Configure todos los FQDN comunes y sus dominios relacionados en una sola aplicación.

   Por ejemplo, si tiene algunas aplicaciones que usan Azure AD como IdP y necesita configurar `login.microsoftonline.com` y otros dominios relacionados (`*.msauth.net`), cree una única aplicación común con `login.microsoftonline.com` como FQDN, y `*.login.microsoftonline.com` y `*.msauth.net` como los dominios relacionados.

   Si la aplicación común va a estar oculta en la aplicación Citrix Workspace, seleccione la opción **No mostrar el icono de la aplicación a los usuarios al** configurar la aplicación. Para obtener más información, consulte Configurar una aplicación web.

2. Cree una directiva de acceso para la aplicación común y permita el acceso a todos los usuarios. Para obtener más información, consulte Configurar una directiva de acceso.

3. Verifique los registros de diagnóstico para confirmar si el FQDN coincide con la aplicación y si la directiva se aplica según lo previsto.

Registros de diagnóstico

December 27, 2023

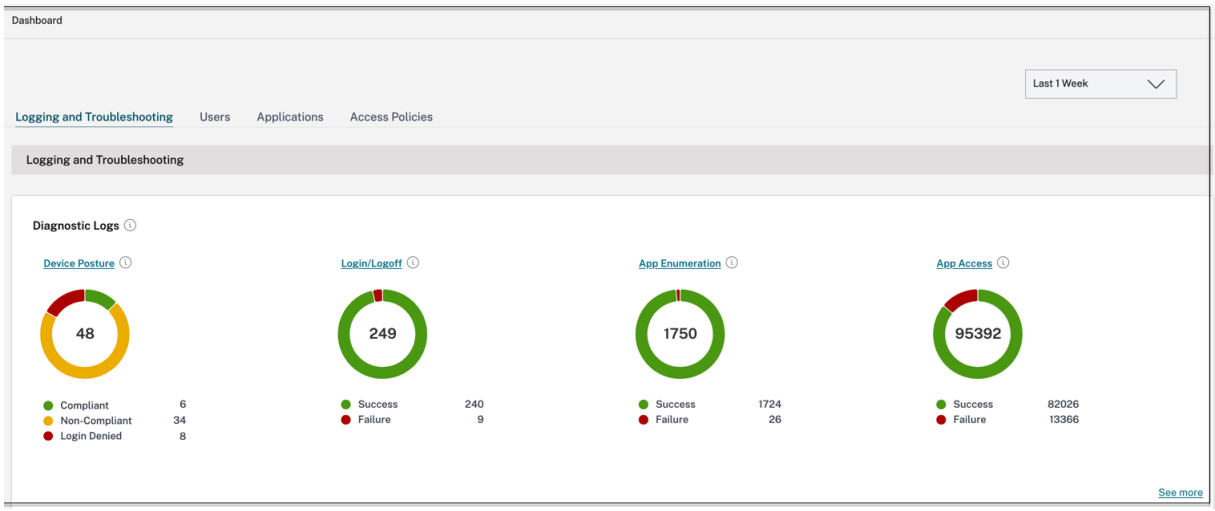
El panel del servicio Secure Private Access muestra los datos de diagnóstico y uso de las aplicaciones SaaS, Web, TCP y UDP. Utilice el gráfico de **registros de diagnóstico** para ver los registros relacionados con la autenticación, el inicio de la aplicación, la enumeración de aplicaciones y también los registros relacionados con la postura del dispositivo. Puede hacer clic en el enlace **Ver más** para ver los detalles de los registros. Los detalles se presentan en formato tabular. Puede ver los registros de la hora preestablecida o de una línea de tiempo personalizada. Puede agregar columnas al gráfico haciendo clic en el signo +, según la información que quiera ver en el panel. Puede exportar los registros de usuario a formato CSV.

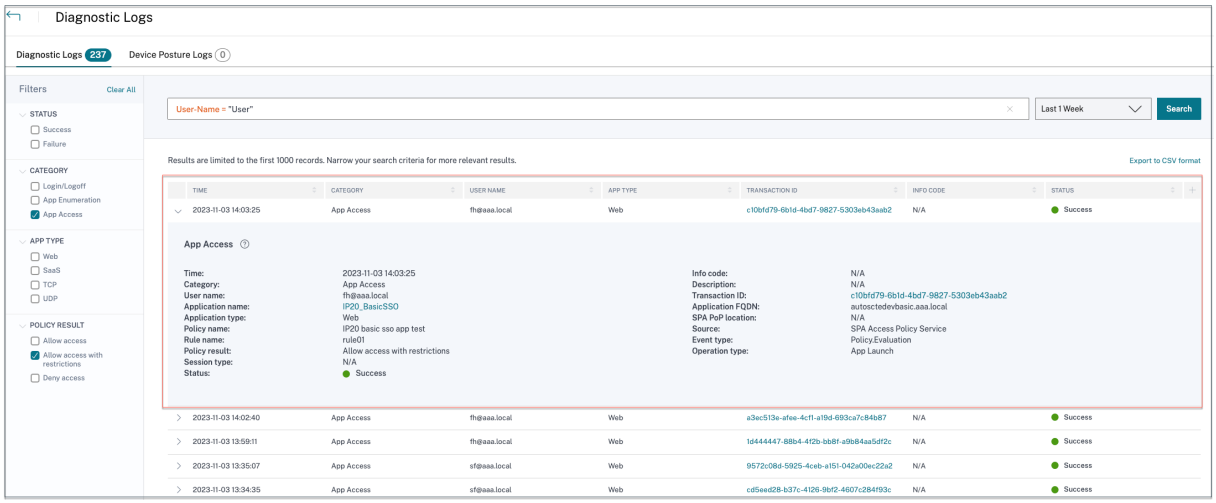
- Puede utilizar los filtros (**ESTADO, CATEGORÍA, TIPO DE APLICACIÓN**) para buscar registros relacionados con la autenticación, el inicio de la aplicación y la enumeración de aplicaciones. También puede utilizar las categorías del campo de búsqueda junto con los operadores de búsqueda de la página de **registros de diagnóstico** para refinar aún más los resultados de la búsqueda. Para obtener más información sobre los operadores de búsqueda, consulte Operadores de búsqueda.

  Por ejemplo, en el campo de búsqueda, puede hacer clic en una categoría `Transaction ID` y un operador igual a (=) y, a continuación, introducir el identificador de la transacción. Por ejemplo, `Transaction-ID =77cdfd46-26b4-142d-9678-002248d60417` para buscar todos los registros relacionados con una solicitud de acceso a una aplicación determinada. Para ver la lista de columnas disponibles que se pueden agregue al panel, haga clic en el signo **+**. Puede agregar o quitar columnas según sea necesario.

- **Registros de postura del dispositivo:** puede refinar la búsqueda en función de los resultados de la directiva (**compatible, no compatible e inicio de sesión denegado**). Para obtener más información sobre la postura del dispositivo, consulte Postura del dispositivo.

> **Nota:**
>
> - Cada evento de error del panel de registros de diagnóstico de Secure Private Access tiene un código de información asociado. Para obtener más información, consulte Código de información.
> - El ID de transacción correlaciona todos los registros de Secure Private Access de una solicitud de acceso. Para obtener más información, consulte ID de transacción.





Nota:

- De forma predeterminada, la página **Registros de diagnóstico** muestra los datos de la semana actual y solo los 10000 registros recientes. Utilice la búsqueda por fecha personalizada y los filtros para refinar aún más los resultados de la búsqueda.

Registros de auditoría

February 16, 2024

Los eventos relacionados con el servicio Secure Private Access ahora se capturan en **Citrix Cloud > System Log**. Todos los eventos que un administrador realiza en el servicio Citrix Secure Private Access se envían a Citrix Cloud y se capturan en los registros del sistema. Los eventos de administración pueden ser, entre otros, los siguientes:

- Configuración de una aplicación web o SaaS
- Suscribirse a una aplicación
- Eliminar una aplicación
- Configuración de una política de acceso adaptable

La siguiente ilustración muestra los eventos relacionados con Secure Private Access en el **registro del sistema**. Para obtener detalles como la exportación de eventos, la recuperación de eventos para un período de tiempo específico, el reenvío de eventos de registro y la retención de datos, consulte Registro del sistema.

Controles de acceso y seguridad adaptables para aplicaciones web, TCP y SaaS empresariales

December 27, 2023

En las situaciones actuales en constante cambio, la seguridad de las aplicaciones es vital para cualquier empresa. Tomar decisiones de seguridad basadas en el contexto y, a continuación, permitir el acceso a las aplicaciones reduce los riesgos asociados a la vez que permite el acceso a los usuarios.

La función de acceso adaptable al servicio Citrix Secure Private Access ofrece un enfoque integral de acceso de confianza cero que ofrece acceso seguro a las aplicaciones. El acceso adaptable permite a los administradores proporcionar un acceso de nivel granular a las aplicaciones a las que los usuarios pueden acceder en función del contexto. El término "contexto"aquí se refiere a:

- Usuarios y grupos (usuarios y grupos de usuarios)
- Dispositivos (dispositivos de escritorio o móviles)
- Ubicación (ubicación geográfica o ubicación de red)
- Postura del dispositivo (comprobación de postura del dispositivo)
- Riesgo (puntuación de riesgo del usuario)

La función de acceso adaptable aplica directivas adaptables a las aplicaciones a las que se accede. Estas directivas determinan los riesgos en función del contexto y toman decisiones de acceso dinámicas para conceder o denegar el acceso a las aplicaciones web empresarial, SaaS, TCP y UDP.

Funcionamiento

Para conceder o denegar el acceso a las aplicaciones, los administradores crean directivas basadas en los usuarios, los grupos de usuarios, los dispositivos desde los que los usuarios acceden a las aplicaciones, la ubicación (país o ubicación de la red) desde la que el usuario accede a la aplicación y la puntuación de riesgo del usuario.

Las directivas de acceso adaptable tienen prioridad sobre las directivas de seguridad específicas de la aplicación que se configuran al agregar el SaaS o una aplicación web en el servicio Secure Private Access. Los controles de seguridad por aplicación se sobrescriben con las directivas de acceso adaptable.

Las directivas de acceso adaptable se evalúan en tres casos:

- Durante una enumeración de aplicaciones web, TCP o SaaS desde el servicio Secure Private Access: si se deniega el acceso a la aplicación a este usuario, el usuario no puede ver esta aplicación en el espacio de trabajo.

- Al iniciar la aplicación: después de enumerar la aplicación y cambiar la directiva de adaptación para denegar el acceso, los usuarios no pueden iniciar la aplicación aunque la aplicación se haya enumerado anteriormente.
- Cuando la aplicación se abre en un Citrix Enterprise Browser o en un servicio de aislamiento remoto de navegadores, Citrix Enterprise Browser aplica algunos controles de seguridad. El cliente aplica estos controles. Cuando se inicia Citrix Enterprise Browser, el servidor evalúa las directivas adaptables del usuario y las devuelve al cliente. A continuación, el cliente aplica las directivas de forma local en Citrix Enterprise Browser.

Cree una directiva de acceso adaptable con varias reglas

Puede crear varias reglas de acceso y configurar diferentes condiciones de acceso para diferentes usuarios o grupos de usuarios dentro de una única directiva. Estas reglas se pueden aplicar por separado para las aplicaciones HTTP/HTTPS y TCP/UDP, todo ello dentro de una única directiva.

Las directivas de acceso de Secure Private Access permiten habilitar o inhabilitar el acceso a las aplicaciones en función del contexto del usuario o del dispositivo del usuario. Además, puede habilitar el acceso restringido a las aplicaciones al agregar las siguientes restricciones de seguridad:

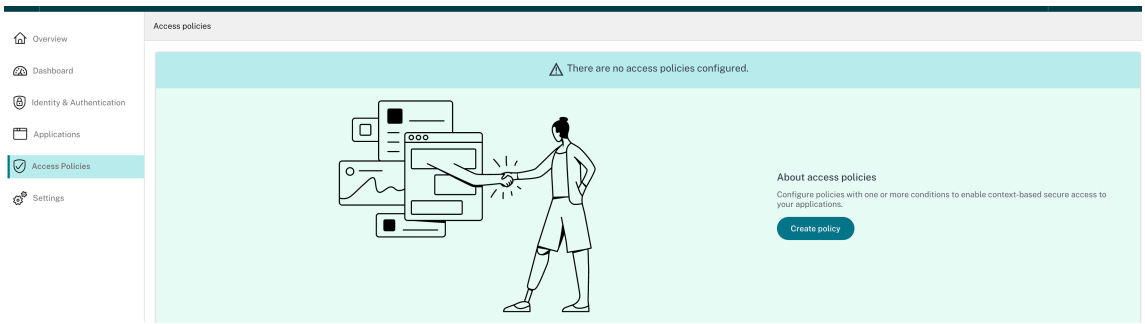
- Restringir acceso al portapapeles
- Restringir impresión
- Restringir descargas
- Restringir las subidas
- Mostrar marca de agua
- Limitar el registro de claves
- Restringir la captura

Para obtener más información sobre estas restricciones, consulte Opciones de restricciones de acceso disponibles.

Asegúrese de haber completado las siguientes tareas antes de configurar una directiva de acceso.

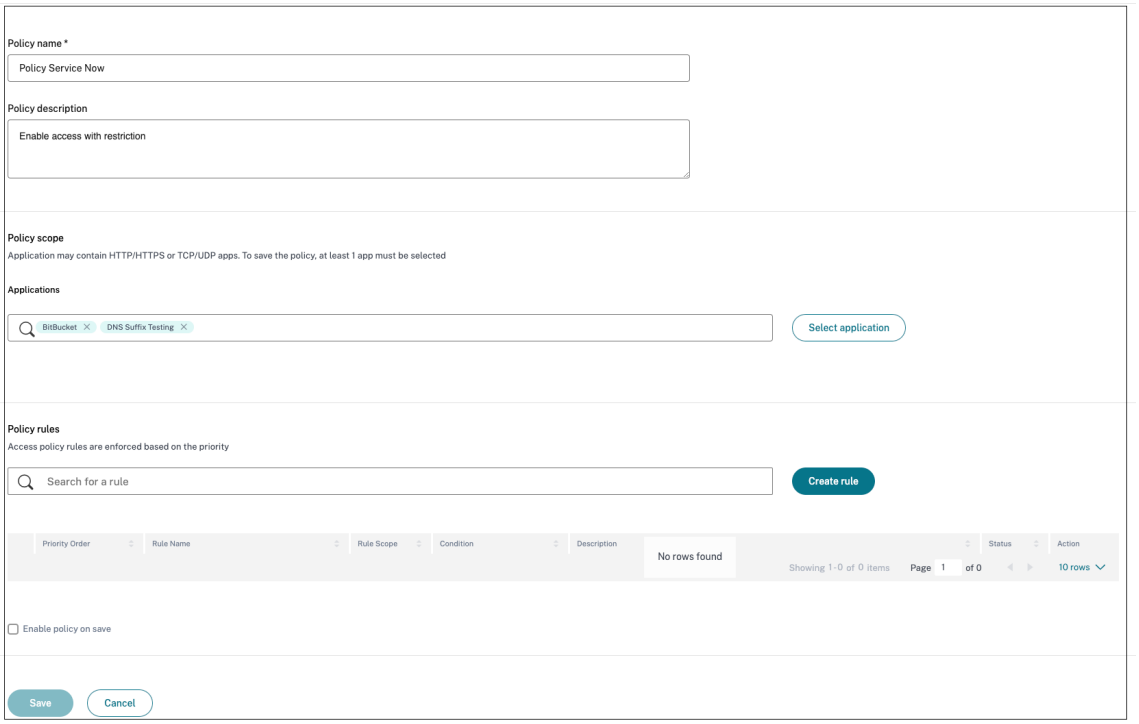
- Configurar la identidad y la autenticación
- Aplicaciones configuradas

1. En el panel de navegación, haga clic en **Directivas de acceso** y, a continuación, en **Crear directiva**.

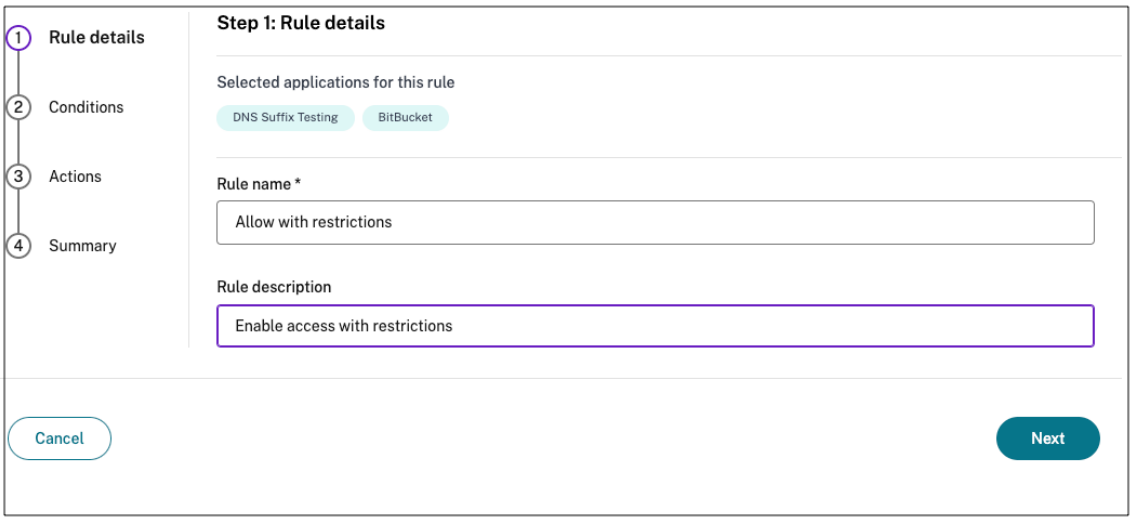


Para los usuarios primerizos, la página de inicio de **Directivas de acceso** no muestra ninguna directiva. Una vez que haya creado una directiva, podrá verla listada aquí.

2. Introduzca el nombre de la directiva y la descripción de la misma.
3. En **Aplicaciones**, seleccione la aplicación o el conjunto de aplicaciones en las que se debe aplicar esta directiva.
4. Haga clic en **Crear regla** para crear reglas para la directiva.

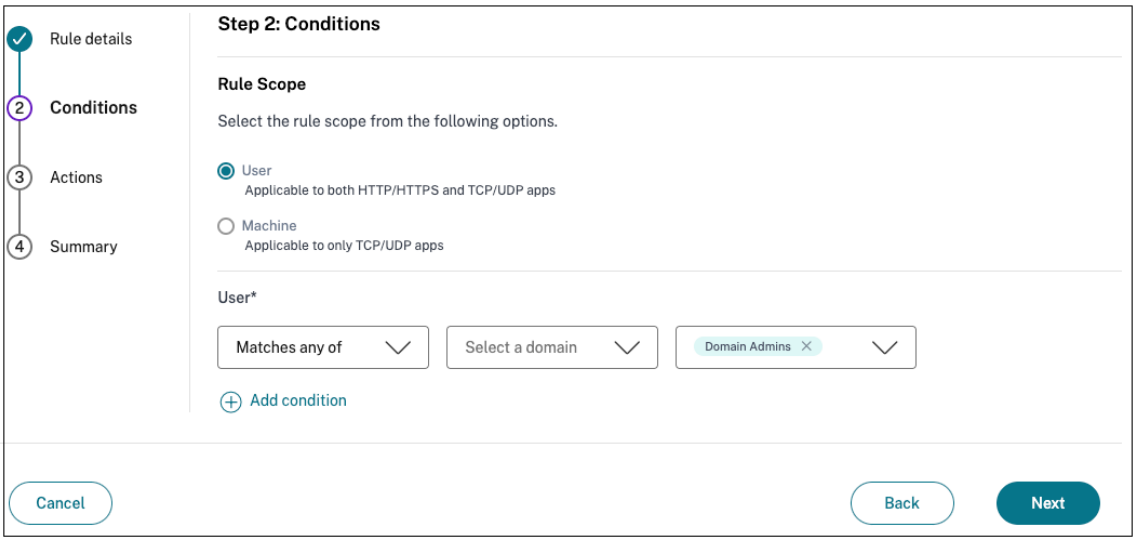


5. Introduzca el nombre de la regla y una breve descripción de la regla y, a continuación, haga clic en **Siguiente**.



6. Selecciona las condiciones de los usuarios. La condición de **usuario** es una condición obligatoria que debe cumplirse para conceder acceso a las aplicaciones a los usuarios. Seleccione una de estas opciones:

   - **Coincide con alguno de**: Solo se permite el acceso a los usuarios o grupos que coincidan con alguno de los nombres que figuran en el campo y que pertenezcan al dominio seleccionado.
   - **No coincide con ninguno**: Se permite el acceso a todos los usuarios o grupos, excepto los que figuran en el campo y que pertenecen al dominio seleccionado.



7. (Opcional) Haga clic en + para agregar varias condiciones en función del contexto.

   Al agregar condiciones en función de un contexto, se aplica una operación AND a las condiciones en las que la directiva se evalúa solo si se cumplen las condiciones de **Users*** y las condiciones opcionales basadas en el contexto. Puede aplicar las siguientes condiciones según el contexto.

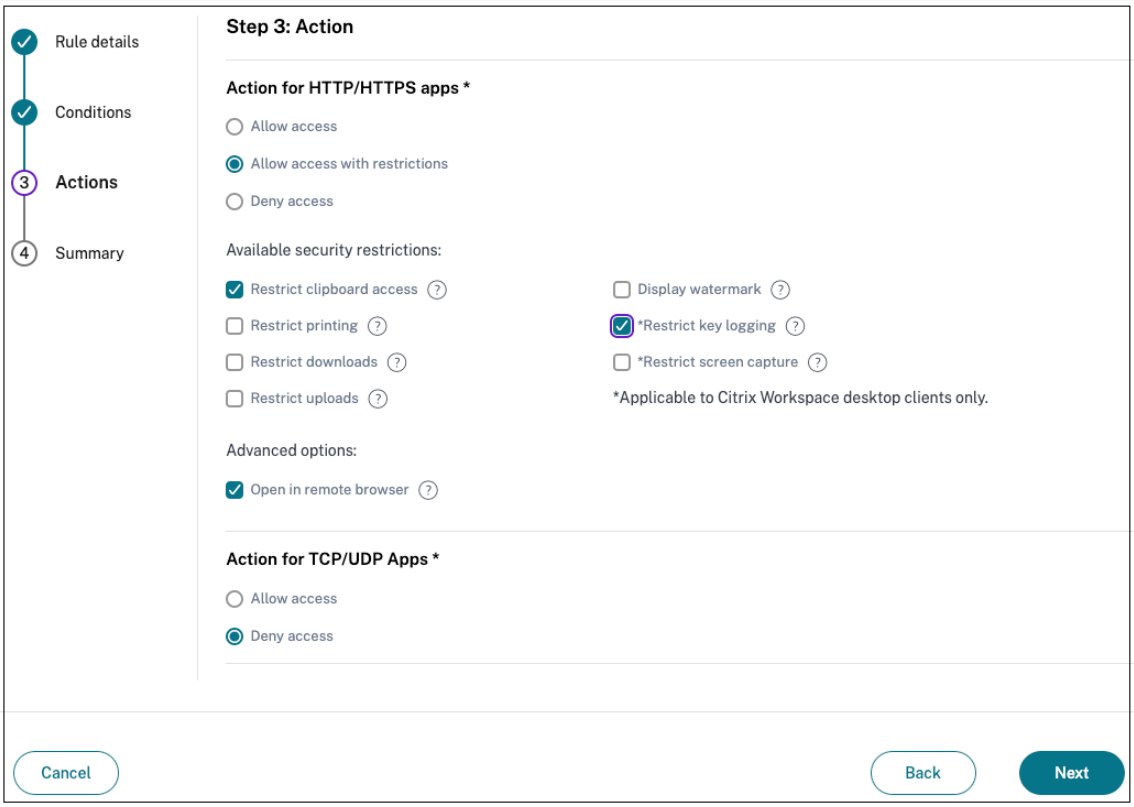
- Dispositivo de **escritorio** o **móvil**: Seleccione el dispositivo para el que quiere habilitar el acceso a las aplicaciones.
- **Ubicación geográfica**: Seleccione la condición y la ubicación geográfica desde donde los usuarios acceden a las aplicaciones.
- **Ubicación de red**: Seleccione la condición y la red mediante la cual los usuarios acceden a las aplicaciones.
- **Verificación de la postura del dispositivo**: Seleccione las condiciones que debe cumplir el dispositivo del usuario para acceder a la aplicación.
- **Puntuación de riesgo del usuario**: Seleccione las categorías de puntuación de riesgo en función de las cuales los usuarios deben tener acceso a la aplicación.

8. Haga clic en **Siguiente**.
9. Seleccione las acciones que se deben aplicar en función de la evaluación de la condición.

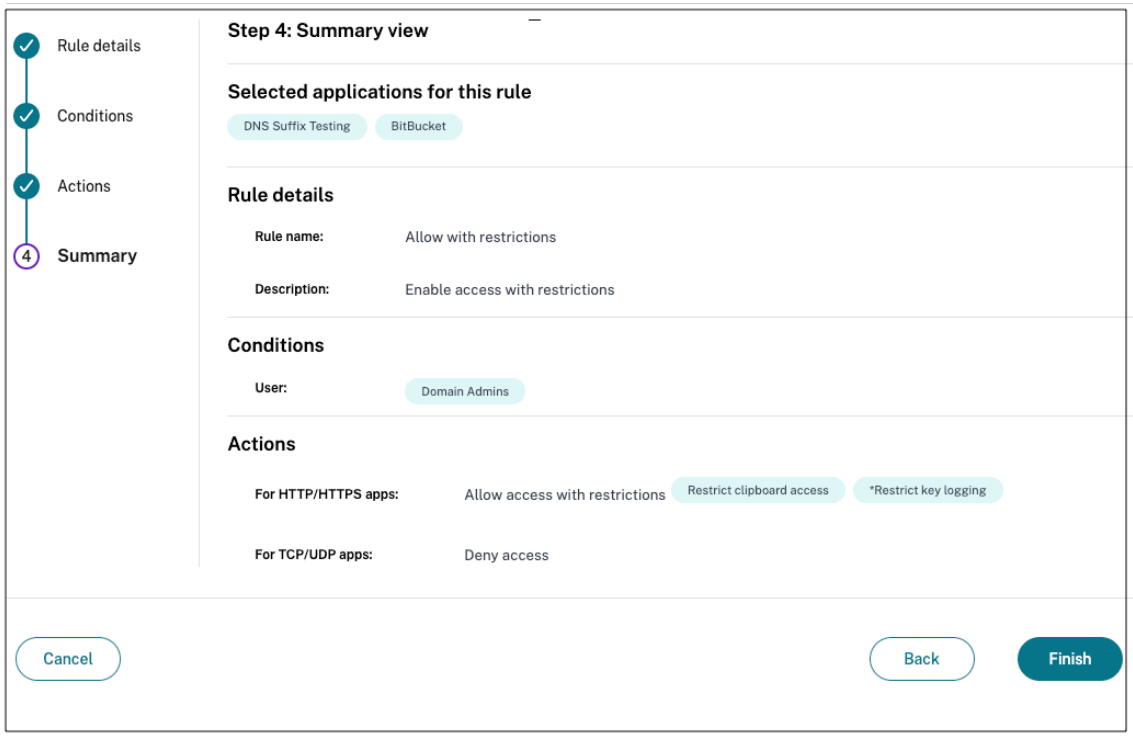
   - Para las aplicaciones HTTP/HTTPS, puede seleccionar lo siguiente:
     - **Permitir el acceso**
     - **Permitir el acceso con restricciones**
     - **Denegar el acceso**

     > **Nota:**
     >
     > Si seleccionas **Permitir el acceso con restricciones**, debes seleccionar las restricciones que quieres aplicar a las aplicaciones. Para obtener más información sobre las restricciones, consulte Opciones de restricciones de acceso disponibles. También puede especificar si quiere que la aplicación se abra en un explorador web remoto o en Citrix Secure Browser.

   - Para el acceso a TCP/UDP, puede seleccionar lo siguiente:
     - **Permitir el acceso**
     - **Denegar el acceso**



10. Haga clic en **Siguiente**. La página de resumen muestra los detalles de la directiva.
11. Puede comprobar los detalles y hacer clic en **Finalizar**.



Puntos a tener en cuenta después de crear una directiva

- La directiva que ha creado aparece en la sección Reglas de directiva y está habilitada de forma predeterminada. Puede inhabilitar las reglas si es necesario. Sin embargo, asegúrese de que haya al menos una regla habilitada para que la directiva esté activa.
- Se asigna un orden de prioridad a la directiva de forma predeterminada. La prioridad con un valor inferior tiene la preferencia más alta. La regla con el número de prioridad más bajo se evalúa primero. Si la regla (n) no coincide con las condiciones definidas, se evalúa la siguiente regla (n+1) y así sucesivamente.

Ejemplo de evaluación de reglas con orden de prioridad:

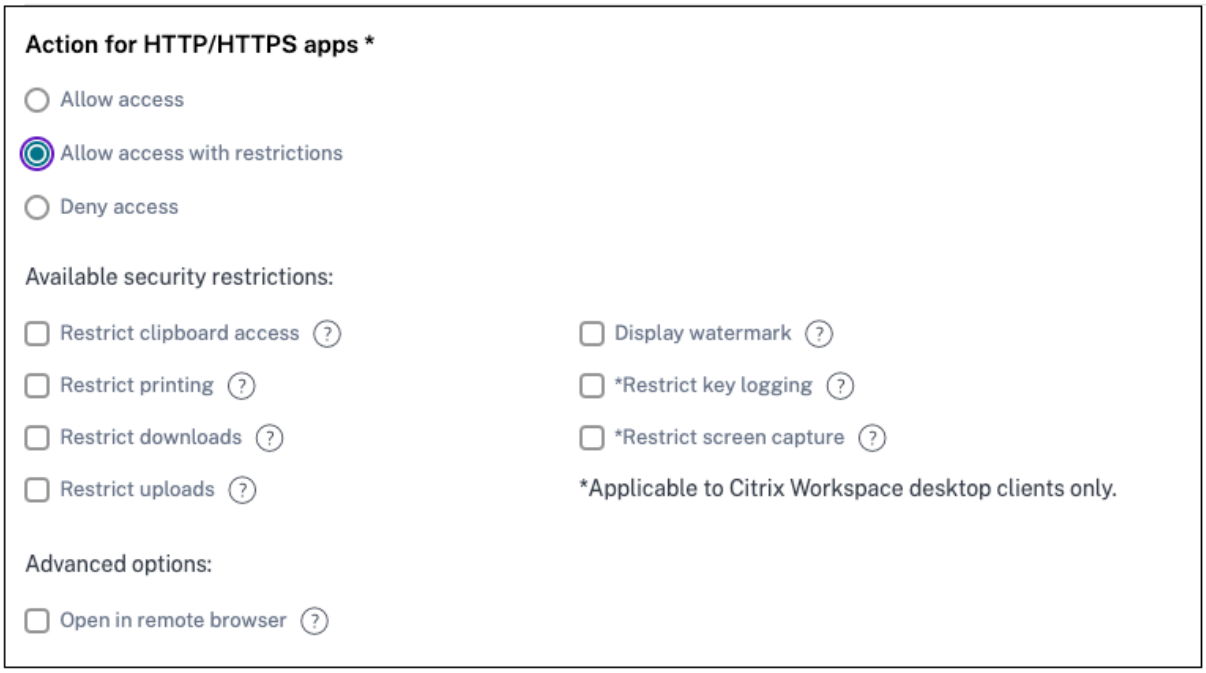
Suponga que ha creado dos reglas, la Regla 1 y la Regla 2.
La regla 1 se asigna al usuario A y la regla 2 al usuario B y, a continuación, se evalúan ambas reglas. Supongamos que tanto la regla 1 como la regla 2 están asignadas al usuario A. En este caso, la regla 1 tiene la prioridad más alta. Si se cumple la condición de la Regla 1, se aplica la Regla 1 y se omite la Regla 2. De lo contrario, si no se cumple la condición de la Regla 1, la Regla 2 se aplica al usuario A.

> **Nota:**
>
> Si no se evalúa ninguna de las reglas, los usuarios no enumeran la aplicación.

Opciones de restricciones de acceso disponibles

Al seleccionar la acción **Permitir el acceso con restricciones**, debe seleccionar al menos una de las restricciones de seguridad. Estas restricciones de seguridad están predefinidas en el sistema. Los

administradores no pueden modificar ni agregar otras combinaciones. Se pueden habilitar las siguientes restricciones de seguridad para la aplicación.

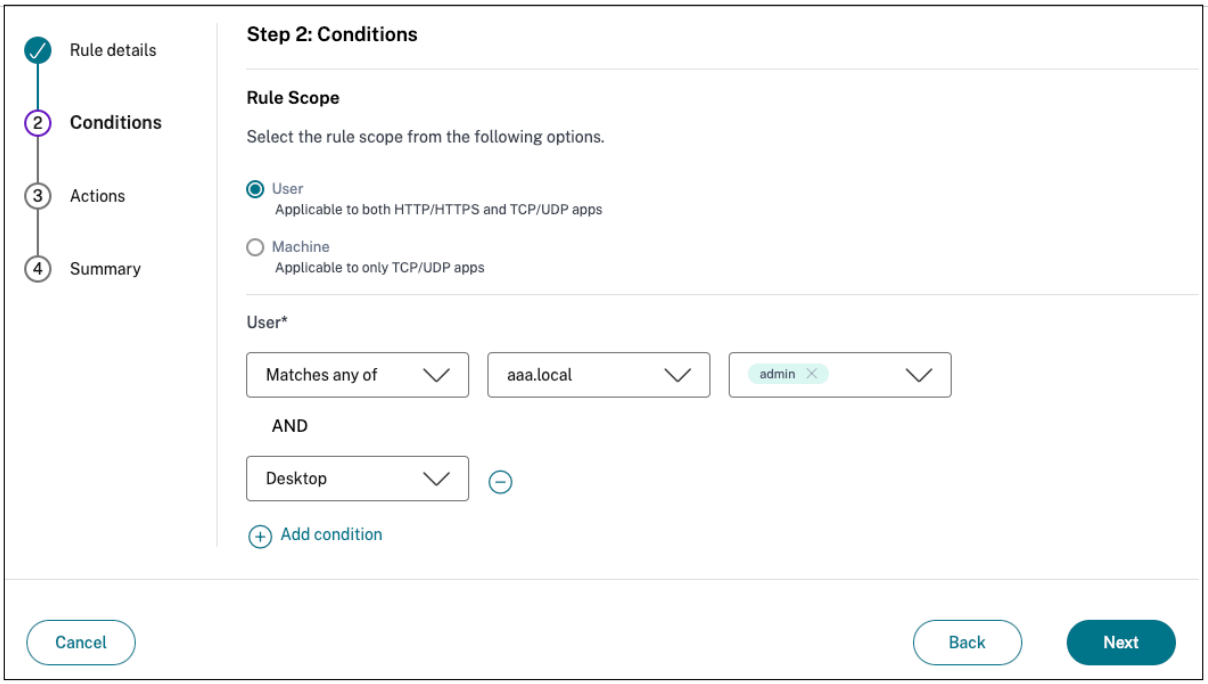


- **Restringir el acceso al portapapeles:**deshabilita las operaciones de cortar/copiar/pegar entre la aplicación y el portapapeles del sistema.
- **Restringir la impresión:**deshabilita la capacidad de imprimir desde el navegador Citrix Enterprise.
- **Restringir las descargas:**deshabilita la capacidad del usuario para descargar desde la aplicación.
- **Restringir las subidas:**deshabilita la capacidad del usuario de subir contenido dentro de la aplicación.
- **Mostrar marca de agua:**muestra una marca de agua en la pantalla del usuario que muestra el nombre de usuario y la dirección IP de la máquina del usuario.
- **Restringir el registro de claves:**protege contra los registradores de claves. Cuando un usuario intenta iniciar sesión en la aplicación con el nombre de usuario y la contraseña, todas las claves se cifran en los registradores de claves. Además, todas las actividades que el usuario realiza en la aplicación están protegidas contra el registro de claves. Por ejemplo, si las directivas de protección de aplicaciones están habilitadas para Office 365 y el usuario edita un documento de Word de Office 365, todas las pulsaciones de teclas se cifran en los registradores de teclas.
- **Restringir la captura de pantalla:**desactiva la capacidad de capturar las pantallas con cualquiera de los programas o aplicaciones de captura de pantalla. Si un usuario intenta capturar la pantalla, se captura una pantalla en blanco.

Acceso adaptable basado en dispositivos

Para configurar una directiva de acceso adaptable en función de la plataforma (dispositivo móvil o equipo de escritorio) desde la que el usuario accede a la aplicación, utilice el procedimiento Crear una directiva de acceso adaptable con múltiples reglas con los siguientes cambios.

- En la página **Paso 2: Condiciones**, haga clic en **Agregar condición.**
- Selecciona Dispositivo **de escritorio** o **móvil**.
- Complete la configuración de la directiva.



Acceso adaptable según la ubicación

Un administrador puede configurar la directiva de acceso adaptable en función de la ubicación desde la que el usuario accede a la aplicación. La ubicación puede ser el país desde el que el usuario accede a la aplicación o la ubicación de red del usuario. La ubicación de la red se define mediante un rango de direcciones IP o direcciones de subred.

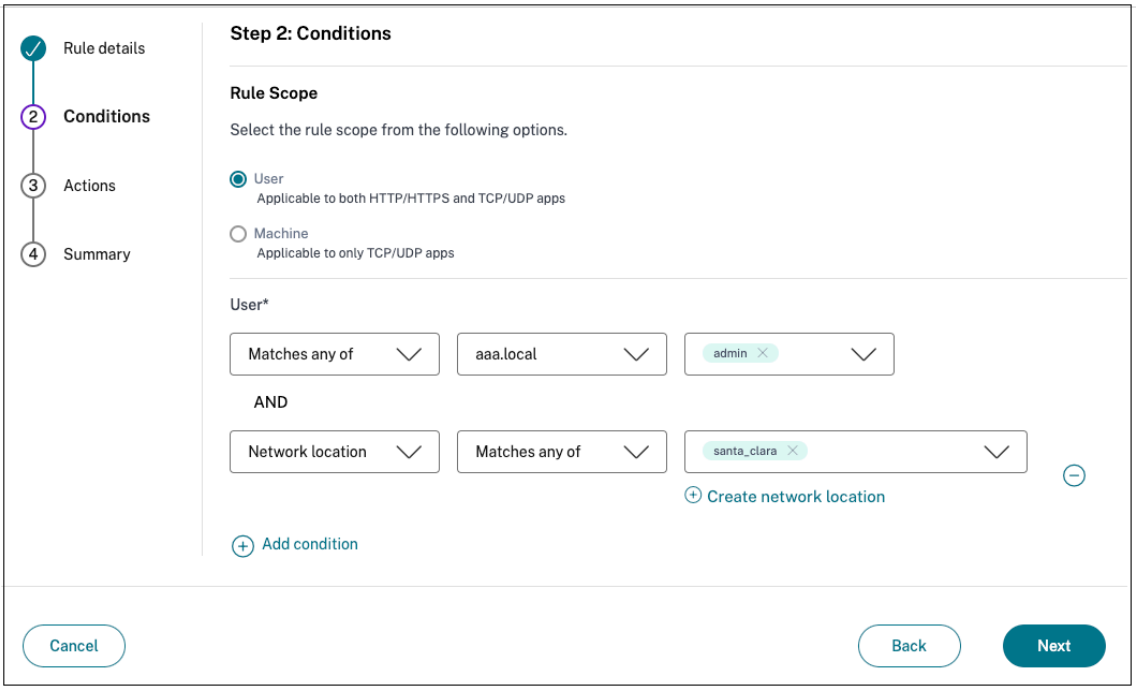
Para configurar una directiva de acceso adaptable en función de la ubicación, utilice el procedimiento [Crear una directiva de acceso adaptable con múltiples reglas] con los siguientes cambios.

- En la página **Paso 2: Condiciones**, haga clic en **Agregar condición.**
- Selecciona **Geolocalización o Ubicación** de **red.**
- Si ha configurado varias ubicaciones geográficas o ubicaciones de red, seleccione una de las siguientes según sus necesidades.

- **Coincide con cualquiera de**: Las ubicaciones geográficas o ubicaciones de red coinciden con cualquiera de las ubicaciones geográficas o ubicaciones de red configuradas en la base de datos.
- **No coincide con ninguna**: Las ubicaciones geográficas o las ubicaciones de red no coinciden con las ubicaciones geográficas o las ubicaciones de red configuradas en la base de datos.

Nota:

- Si selecciona **Geolocalización**, la dirección IP de origen del usuario se evalúa con la dirección IP de la base de datos del país. Si la dirección IP del usuario se asigna al país de la directiva, se aplica la directiva. Si el país no coincide, se omite esta directiva adaptable y se evalúa la siguiente directiva adaptable.
- Para **Ubicación de red**, puede seleccionar una ubicación de red existente o crear una ubicación de red. Para crear una nueva ubicación de red, haga clic en **Crear ubicación de red**.
- Asegúrese de haber habilitado Adaptive Access desde **Citrix Cloud > Citrix Workspace > Access > Adaptive Access**. De lo contrario, no podrá agregar las etiquetas de ubicación. Para obtener más información, consulte Habilitar el acceso adaptable.
- También puede crear una ubicación de red desde la consola de Citrix Cloud. Para obtener más información, consulte Configuración de ubicación de red de Citrix Cloud.



- Complete la configuración de la directiva.

Acceso adaptable en función de la postura del dispositivo

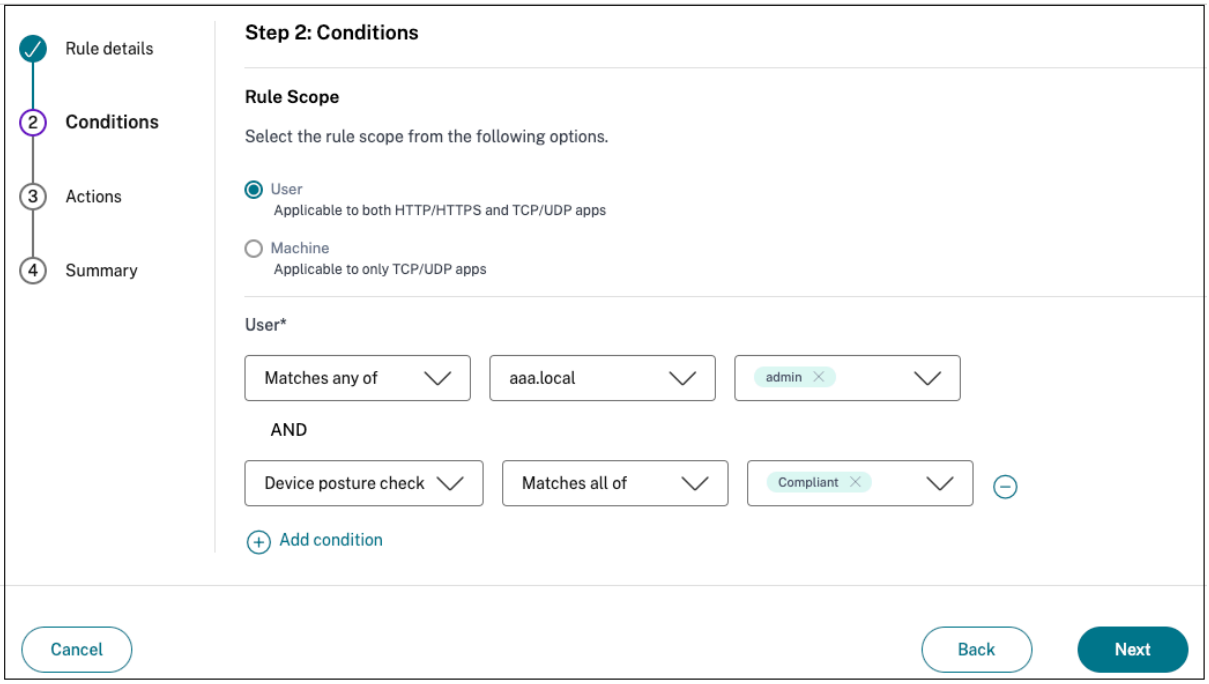
Puede configurar el servicio Secure Private Access para aplicar el control de acceso mediante etiquetas de postura del dispositivo. Una vez que se permite que un dispositivo inicie sesión después de la verificación de la postura del dispositivo, el dispositivo se puede clasificar como compatible o no compatible. Esta información está disponible como etiquetas para los servicios Citrix DaaS y Citrix Secure Private Access y se utiliza para proporcionar un acceso contextual en función de la postura del dispositivo.

Para obtener información completa sobre el servicio Device Posture, consulte Device Posture.

Para configurar una directiva de acceso adaptable en función de la postura del dispositivo, utilice el procedimiento Crear una directiva de acceso adaptable con múltiples reglas con los siguientes cambios.

- En la página **Paso 2: Condiciones**, haga clic en **Agregar condición.**
- Seleccione **Verificación de postura del dispositivo** y la expresión lógica en el menú desplegable.
- Introduzca uno de los siguientes valores en las etiquetas personalizadas:
  - **Compatible**: para dispositivos compatibles
  - **No compatible**: para dispositivos que no cumplen con las normas

> **Nota:**
>
> La sintaxis de las etiquetas de clasificación de dispositivos debe introducirse de la misma manera que se capturó anteriormente, es decir, en mayúsculas iniciales (compatible y no compatible). De lo contrario, las directivas de postura del dispositivo no funcionan según lo previsto.



Acceso adaptable basado en la puntuación de riesgo del usuario

> **Importante:**
>
> Esta función solo está disponible para los clientes si tienen derecho a Security Analytics.

La puntuación de riesgo del usuario es un sistema de puntuación para determinar los riesgos asociados con las actividades de los usuarios en su empresa. Los indicadores de riesgo se asignan a las actividades de los usuarios que parecen sospechosas o que pueden representar una amenaza a la seguridad de su organización. Los indicadores de riesgo se activan cuando el comportamiento del usuario se desvía de lo normal. Cada indicador de riesgo puede tener uno o más factores de riesgo asociados. Estos factores de riesgo ayudan a determinar el tipo de anomalías en los eventos de usuario. Los indicadores de riesgo y sus factores de riesgo asociados determinan la puntuación de riesgo de un usuario. La puntuación de riesgo se calcula periódicamente y hay un retraso entre la acción y la actualización de la puntuación de riesgo. Para obtener más información, consulte Indicadores de riesgo de usuarios de Citrix.

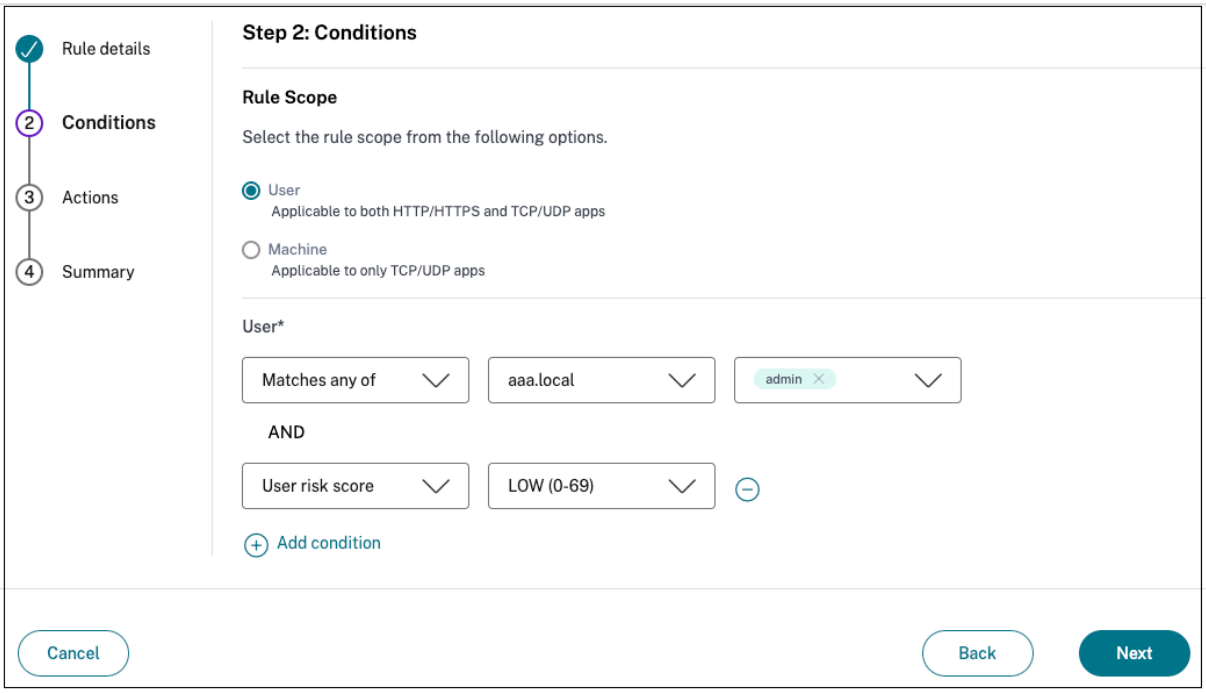
Para configurar una directiva de acceso adaptable con puntuación de riesgo, utilice el procedimiento Crear una directiva de acceso adaptable con múltiples reglas con los siguientes cambios.

- En la página **Paso 2: Condiciones**, haga clic en **Agregar condición.**
- Seleccione **Puntuación de riesgo del usuario** y, a continuación, seleccione la condición de riesgo.
  - Etiquetas preestablecidas obtenidas del servicio CAS

  * **BAJO** 1—69
  * **MEDIANO** 70—89
  * **ALTO** 90-100

> **Nota:**
>
> Una puntuación de riesgo de 0 no se considera que tenga un nivel de riesgo “Bajo. “

- Tipos de umbrales
  * **Mayor o igual que**
  * **Menor o igual que**
- Un rango numérico
  * **Rango**



Tablas de enrutamiento para resolver conflictos derivados de los mismos dominios relacionados

December 27, 2023

La función de dominios de aplicaciones de Citrix Secure Private Access Service permite a los clientes tomar decisiones de enrutamiento que permiten enrutar dominios de aplicaciones relacionados de forma externa o interna a través de Connector Appliances.

Tenga en cuenta que el cliente ha configurado los mismos dominios relacionados tanto en una aplicación SaaS como en una aplicación web interna.
Por ejemplo, si Okta es el proveedor de identidades SAML tanto para Salesforce (aplicación SaaS) como para Jira (aplicación web interna), el administrador podría configurar `*.okta.com` como dominio relacionado en la configuración de ambas aplicaciones. Esto genera un conflicto y el usuario final experimenta un comportamiento incoherente. En este caso, el administrador puede definir reglas para enrutar estas aplicaciones de forma externa o interna a través de los Connector Appliances, según los requisitos.

La función Dominios de aplicación también permite a los administradores configurar los Connector Appliances para evitar los servidores proxy web del cliente y acceder a los servidores web internos. Estas directivas de omisión se configuraban previamente de forma manual mediante la ejecución de los comandos NSCLI en el Connector Appliance.

Cómo funciona la tabla de redirección

Los administradores pueden definir el tipo de ruta de las aplicaciones como externa, interna o externa mediante Connector Appliance, según cómo quieran definir el flujo de tráfico.

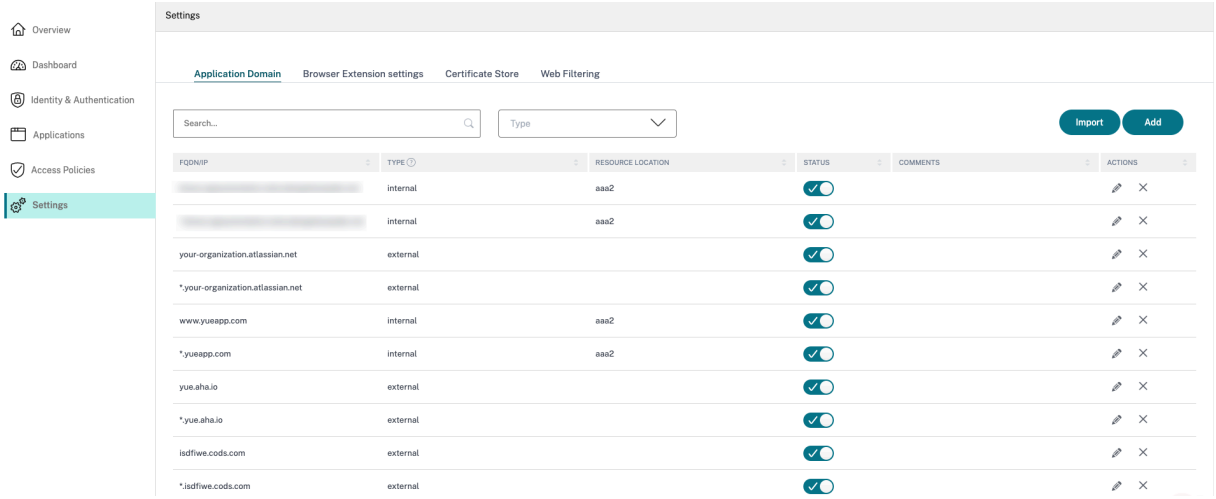
- **Externo**: El tráfico fluye directamente a Internet.
- **Interno**: El tráfico fluye a través del Connector Appliance.
  - En el caso de una aplicación web, el tráfico fluye dentro del centro de datos.
  - En el caso de una aplicación SaaS, el tráfico se redirige fuera de la red a través del Connector Appliance.
- **Interno - Omitir proxy**: El tráfico del dominio se redirige a través de los Connector Appliances de Citrix Cloud, sin pasar por el proxy web del cliente configurado en el Connector Appliance.
- **Externo mediante conector** : Las aplicaciones son externas, pero el tráfico debe fluir a través del Connector Appliance hacia la red externa.

> **Nota:**
>
> - Las entradas de ruta no afectan a las directivas de seguridad que están configuradas en las aplicaciones.
> - Si los administradores no tienen intención de utilizar una entrada de la tabla de redirección o si las aplicaciones correspondientes no funcionan según lo previsto, los administradores pueden simplemente inhabilitar la entrada en lugar de eliminarla.
> - Todos los dispositivos Connector de un cliente en particular, independientemente del tipo de aplicación, obtienen la configuración de SSO. Anteriormente, la configuración de SSO de una aplicación concreta estaba vinculada a una ubicación de recursos.

Tabla de redirección principal

Se puede acceder a la tabla de rutas principal desde el mosaico **Acceso privado seguro**.

1. Inicie sesión en la cuenta de Citrix Cloud.
2. En el mosaico Acceso privado seguro, haga clic en **Administrar** .
3. En el panel de navegación, haga clic en **Configuración.** Aparecerá la página **Dominios de aplicaciones**.



La tabla de redirección principal muestra las columnas siguientes.

- **FQDN/IP:** FQDN o la dirección IP para la que se quiere configurar el tipo de redirección de tráfico.
- **Tipo**: Tipo de aplicación. **Interno**, **Externo** o **Externo mediante conector**, tal como se seleccionó al agregar la aplicación.

  > **Importante:**
  >
  > Si hay conflictos, se muestra un icono de alerta para la fila correspondiente de la tabla. Para resolver el conflicto, los administradores deben hacer clic en el icono triangular y cambiar el tipo de aplicación en la tabla principal.

- **Ubicación del recurso:** Ubicación de recursos para redirección de tipo **Internal**. Si no se asigna una ubicación de recursos, aparece un icono triangular en la columna **Ubicación de recursos** de la aplicación correspondiente. Al pasar el ratón sobre el icono, se muestra el siguiente mensaje.

  Falta la ubicación de recursos. Asegúrese de que una ubicación de recursos esté asociada a este FQDN.

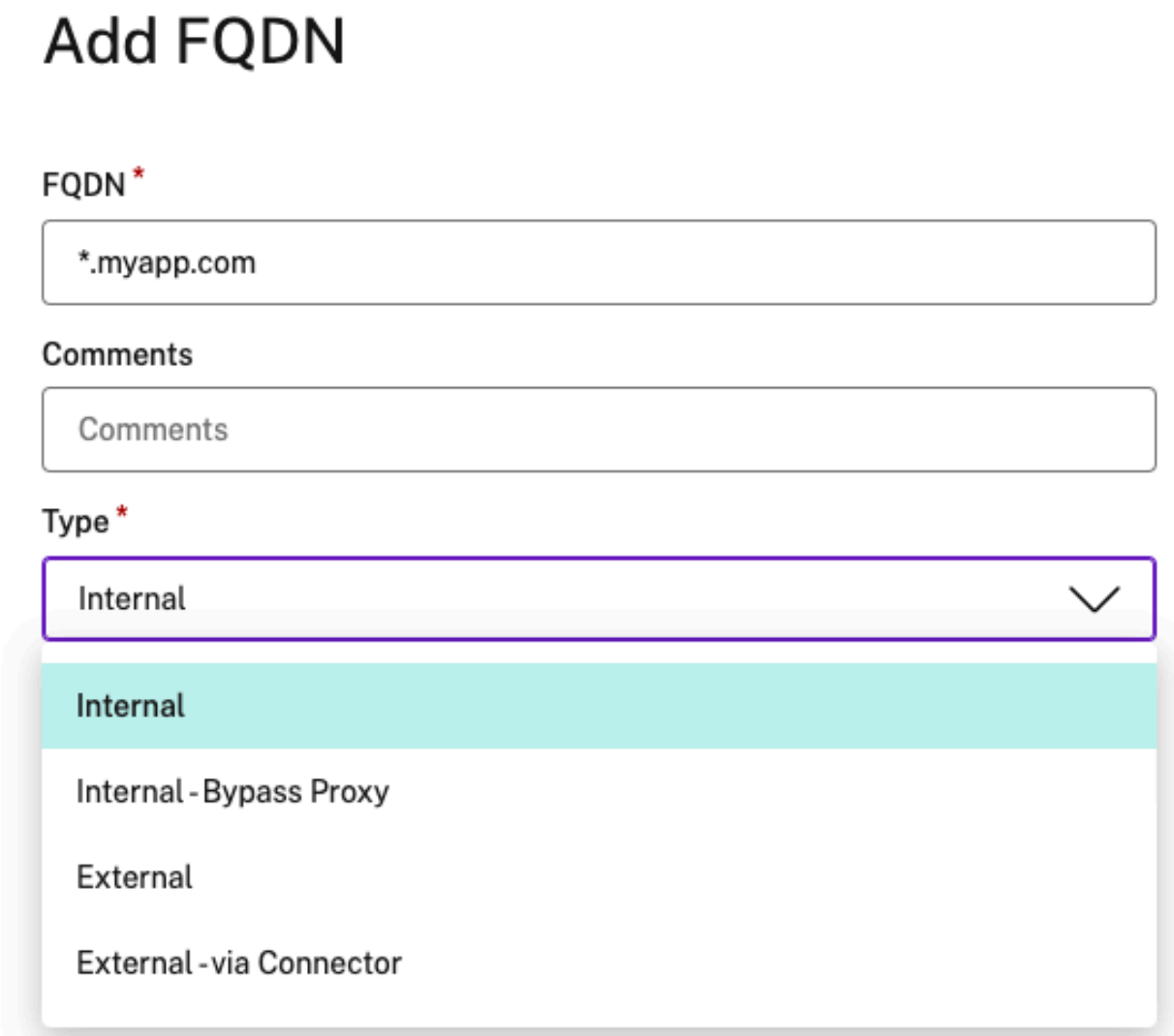
- **Estado:** El conmutador de la columna **Estado** se puede utilizar para inhabilitar la ruta de una entrada de ruta sin eliminar la aplicación. Cuando se apaga el conmutador, la entrada de ruta no surte efecto. Además, si existen FQDN de concordancia exacta, los administradores pueden seleccionar la ruta que quiere habilitar o inhabilitar.

- **Comentarios:** muestra los comentarios, si los hay.
- **Acciones:** El icono de edición se utiliza para agregar una ubicación de recursos o cambiar el tipo de entrada de ruta. El icono de borrar se utiliza para borrar la ruta.

Agregar un FQDN a la tabla Dominios de aplicación

Los administradores pueden agregar un FQDN a la tabla Dominios de aplicación y elegir el tipo de redirección adecuado para él.

1. Haga clic en **Agregar** en la página Dominio de aplicaciones.
2. Introduzca el nombre de FQDN y seleccione el tipo de ruta adecuado para el FQDN.



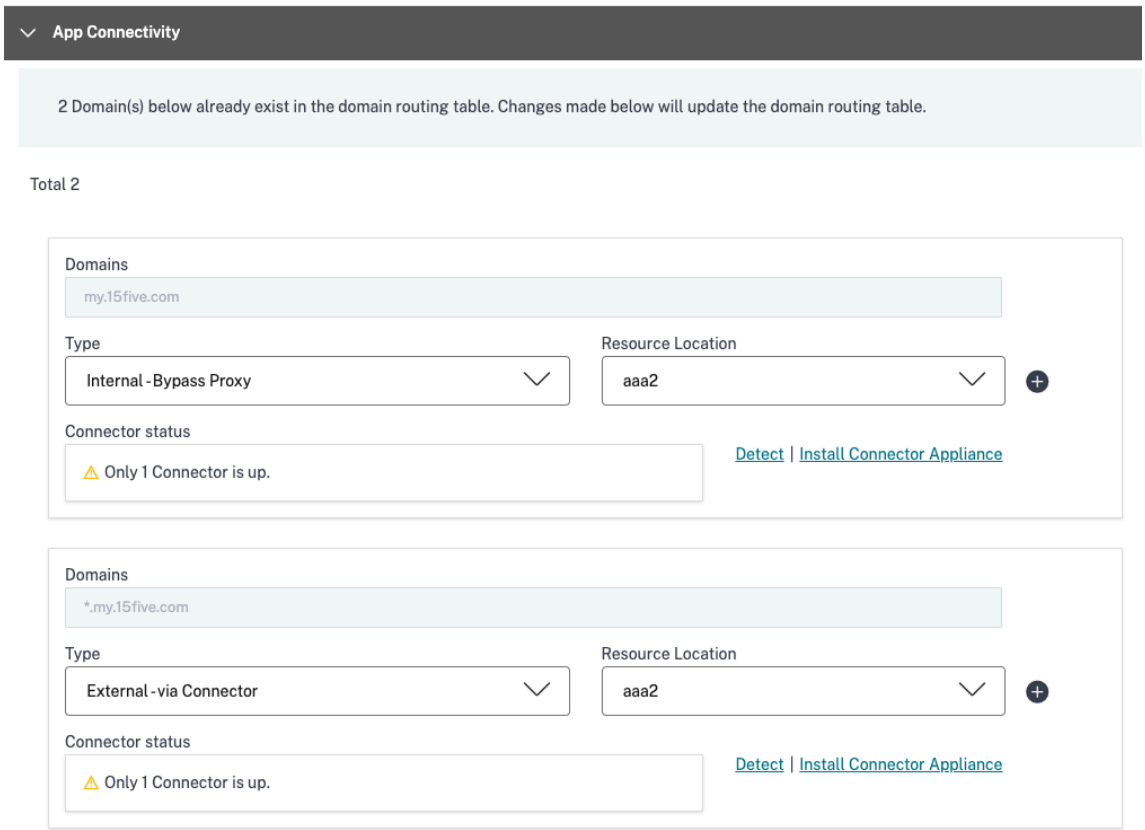
Mesa de ruta mini

Hay disponible una versión mini de la tabla Dominios de aplicación para tomar las decisiones de redirección durante la configuración de la aplicación. La tabla de minirrutas disponible en la sección **Conectividad de aplicaciones** de la interfaz de usuario de Citrix Secure Private Access Service.

Para agregar rutas a la tabla de redirección mini

Los pasos para agregar una aplicación al Citrix Secure Private Access Service siguen siendo los mismos que se describen en los temas Compatibilidad con aplicaciones de software como servicio y Compatibilidad con aplicaciones web empresariales, excepto en los dos cambios siguientes:

1. Siga estos pasos:
   - Elige una plantilla.
   - Introduce los detalles de la aplicación
   - Elija detalles de seguridad mejorados, según corresponda.
   - Seleccione el método de inicio de sesión único, según proceda.
2. Haga clic en **Conectividad de aplicaciones** - Hay disponible una versión mini de la tabla Application Domains para tomar las decisiones de redirección durante la configuración de la aplicación.



- **Dominios:** La columna Dominios muestra una o varias filas de una aplicación concreta. La primera fila muestra la URL de la aplicación real que el administrador ha introducido al agregar los detalles de la aplicación. Las demás filas son dominios relacionados que se introducen al agregar los detalles de la aplicación. Si la URL de la aplicación y los dominios relacionados son los mismos, se muestran en una fila.

Una fila muestra la URL de aserción SAML, si se ha seleccionado SSO SAML.

- **Tipo:** selecciona una de las siguientes opciones.
  - **Externo**: El tráfico fluye directamente a Internet.
  - **Interno**: El tráfico fluye a través del Connector Appliance y la aplicación se trata como una aplicación web.
    * En el caso de una aplicación web, el tráfico fluye dentro del centro de datos.
    * En el caso de una aplicación SaaS, el tráfico se redirige fuera de la red a través del Connector Appliance.
  - **Interno - Omitir proxy**: El tráfico del dominio se redirige a través de los Connector Appliances de Citrix Cloud, sin pasar por el proxy web del cliente configurado en el Connector Appliance.
  - **Externo mediante conector**: Las aplicaciones son externas, pero el tráfico debe fluir a través del Connector Appliance hacia la red externa.
- **Ubicación del recurso:** se rellena automáticamente al seleccionar el tipo Interno para una aplicación. Cámbielo si se quiere una ubicación de recursos diferente.
- **Estado del Connector Appliance:** Se rellena automáticamente, junto con la ubicación del recurso, al seleccionar el tipo Interno para una aplicación.

Sitios web no autorizados

December 27, 2023

> **Importante:**
>
> La función **de filtrado de sitios web** pasa a llamarse **Sitios web no autorizados**.

La función de sitios web no autorizados evalúa el riesgo de cada hipervínculo seleccionado en la aplicación SaaS. El acceso a estos sitios y la supervisión de los cambios en el comportamiento del usuario aumenta la puntuación general de riesgo del usuario, ya que indica que el dispositivo de punto final está comprometido y ha comenzado a infectar o cifrar datos o que el usuario y el dispositivo están robando propiedad intelectual.

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, si se debe redirigir a una sesión de navegador segura o si se puede permitir el acceso a la URL.

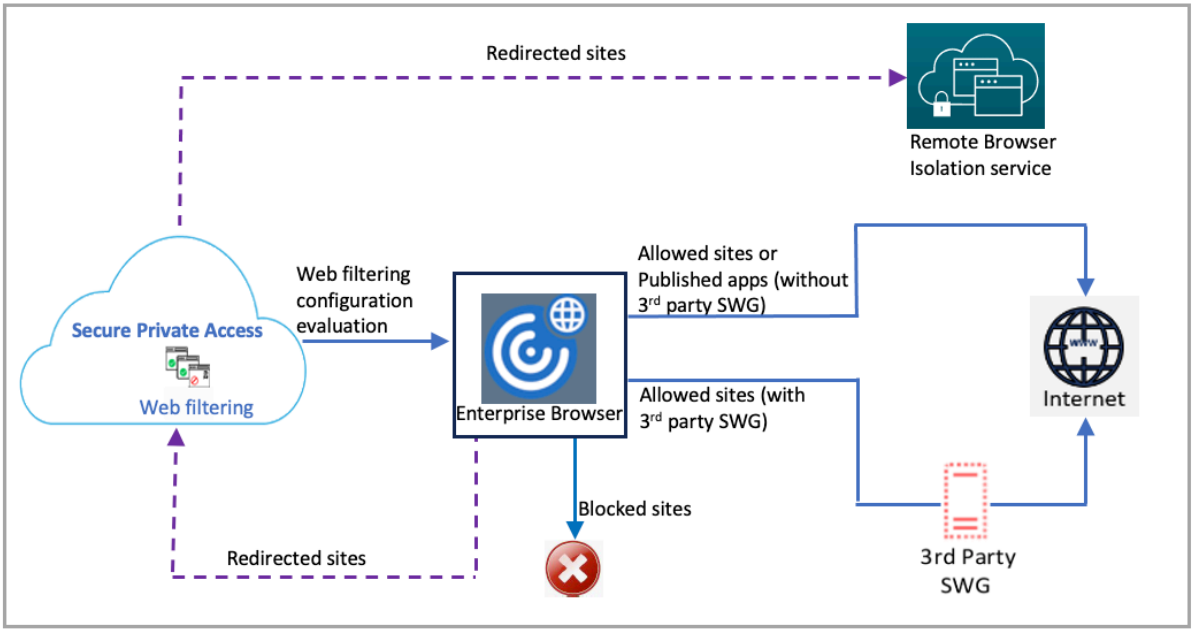
Configurar reglas para sitios web no autorizados

December 27, 2023

> **Importante:**
>
> - El filtrado web basado en categorías dejará de estar en desuso el 31 de diciembre de 2022. Para obtener más información, consulte Desventajas de funciones.
> - La función **Filtrado de sitios web** pasa a llamarse **Sitios web no autorizados**.

Los sitios web no autorizados son las aplicaciones que no están configuradas en la configuración de Secure Private Access, pero a las que se puede acceder desde Citrix Enterprise Browser. Puede configurar reglas para estos sitios web no autorizados. Por ejemplo, un enlace dentro de una aplicación SaaS puede apuntar a un sitio web malicioso. Con estas reglas, un administrador puede tomar una URL específica de un sitio web o una categoría de sitio web y permitir el acceso, bloquear el acceso o redirigir la solicitud a una instancia de explorador web alojada y segura, lo que ayuda a prevenir los ataques por explorador web. Puedes usar caracteres comodín, como *.example.com/*, para controlar el acceso a todos los dominios de ese sitio web y a todas las páginas de ese dominio.

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



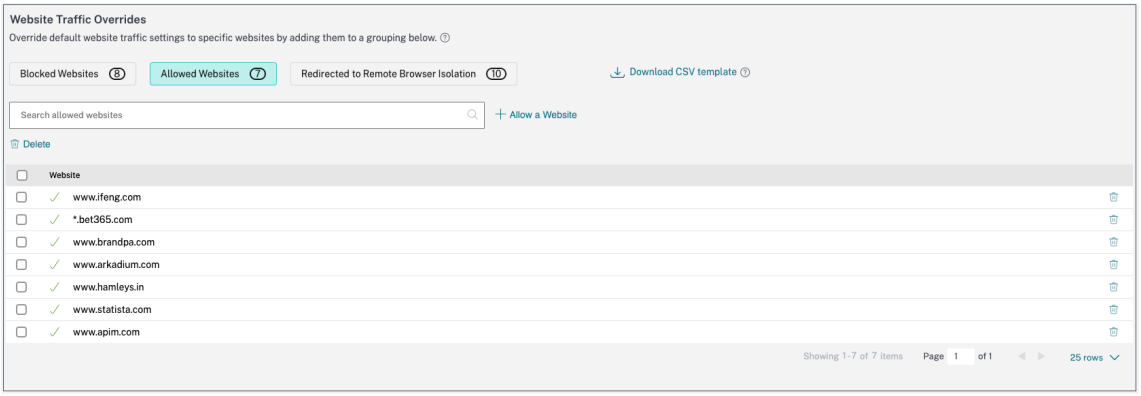
Cuando llega una solicitud, se llevan a cabo las comprobaciones siguientes y se toman las medidas correspondientes:

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. Redirigir
      iii. Permitir
   b) Si no corresponde, se consultan las categorías de sitios web.
3. Si no corresponde, se aplica la acción predeterminada (PERMITIR). La acción predeterminada no se puede cambiar.

Para configurar reglas para sitios web no activos

1. En la página de inicio de Secure Private Access, haga clic en **Configuración** en el panel de navegación.
2. Haga clic en **Sitios web no autorizados** y, a continuación, en **Modificar.**

3. Habilite **Filtrar lista de sitios web**. Haga clic en **Agregar** en la sección correspondiente para bloquear o permitir sitios web, o bien, redirigir al usuario a un explorador web seguro. Por ejemplo, para bloquear sitios web, en la sección de sitios web bloqueados, haga clic en **Agregar**.



   - Indique un sitio web al que los usuarios no puedan acceder y haga clic en **Agregar**.
   - Para permitir el acceso a sitios web, en la sección de sitios web permitidos, haga clic en **Agregar**. Indique un sitio web al que los usuarios puedan acceder y haga clic en **Agregar**.
   - Para redirigir a los usuarios a un explorador web seguro, en la sección para redirigir a sitios web, haga clic en **Agregar**. Indique un sitio web al que los usuarios solo puedan acceder a través de un explorador web alojado en Citrix y haga clic en **Agregar**.

4. Haga clic en **Guardar** para que los cambios surtan efecto.

> **Nota:**
>
> - La función de filtrado de listas de sitios web redirige todo el tráfico de Citrix Enterprise Browser a través de Secure Private Access Service, evitando los firewalls y el filtrado de contenido existentes. Si quiere que los firewalls o el filtrado de contenido existentes, o ambos, se apliquen al tráfico de Citrix Enterprise Browser, debe inhabilitar la opción **Filtrar listas de sitios web**. La opción **Filtrar lista de sitios web** está habilitada de forma predeterminada.
> - Un cliente (organización) de Secure Browser Standard Service de pago obtiene 5000 horas de uso al año de forma predeterminada. Durante más horas, deberán comprar los paquetes de complementos para Secure Browser. Puede realizar un seguimiento del uso del servicio Remote Browser Isolation. Para obtener más información, consulte Supervisar el uso. Para obtener más información sobre el servicio Remote Browser Isolation, consulte el servicio Secure Browser Standard.

Integración de ADFS con Secure Private Access

December 27, 2023

Las reglas de reclamos son necesarias para controlar el flujo de reclamos a través del proceso de reclamos. Las reglas de reclamación también se pueden utilizar para personalizar el flujo de reclamaciones durante el proceso de ejecución de la regla de reclamación. Para obtener más información sobre las reclamaciones, consulte la documentación de Microsoft.

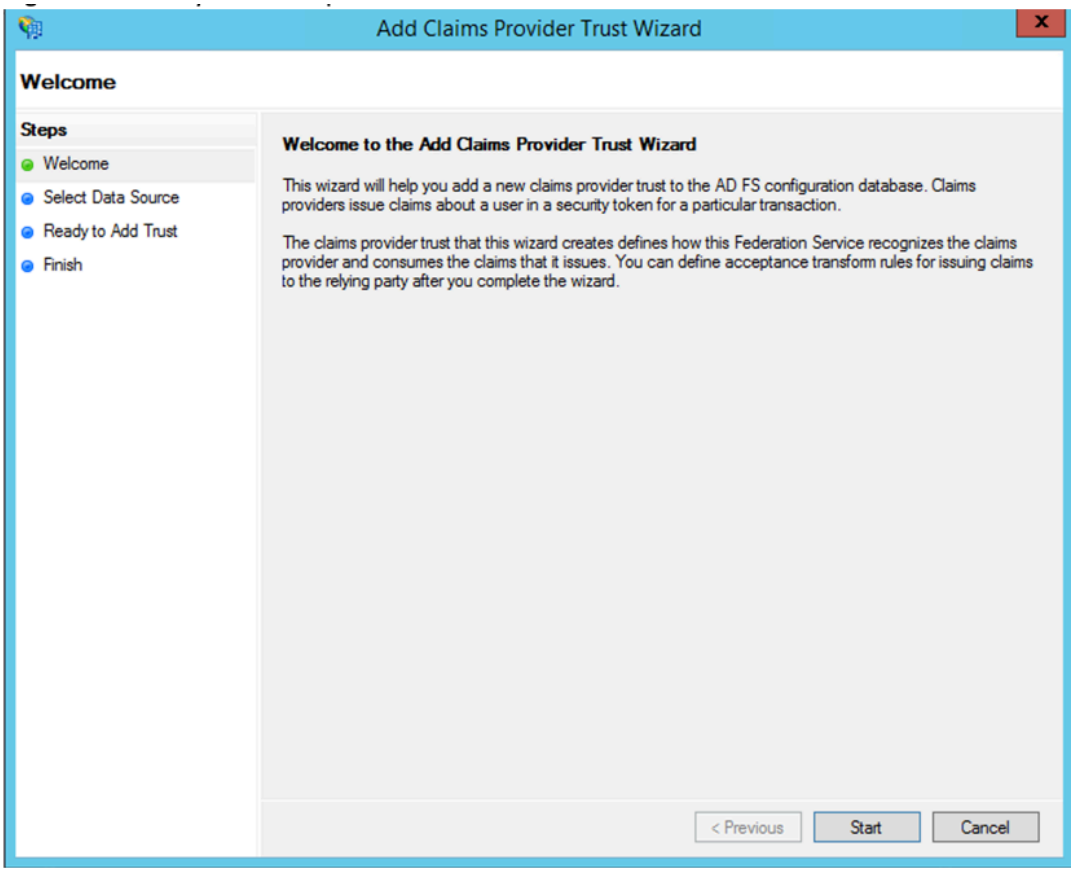
Para configurar ADFS para que acepte reclamos de Citrix Secure Private Access, debe realizar los siguientes pasos:

1. Agregue la confianza del proveedor de reclamos en ADFS.
2. Complete la configuración de la aplicación en Citrix Secure Private Access.

Agregue la confianza del proveedor de reclamos en ADFS

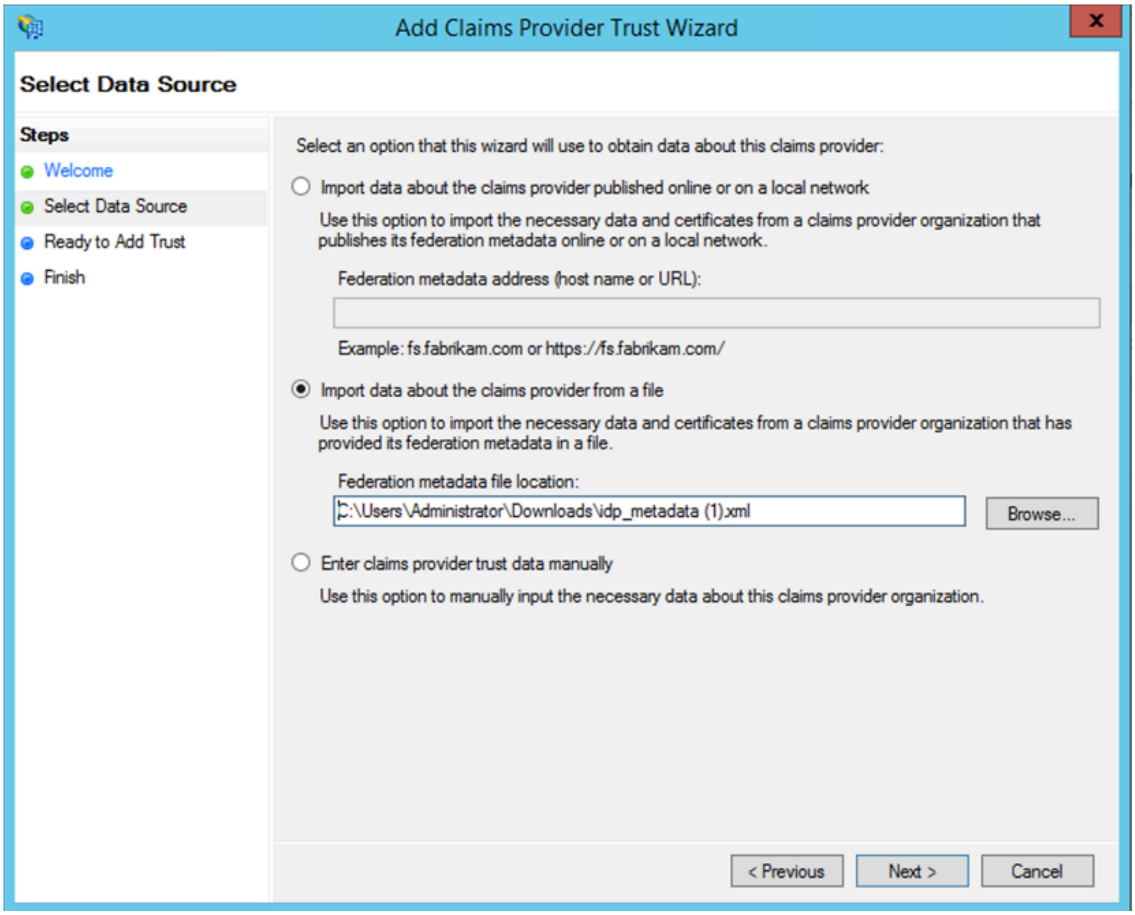
1. Abra la consola de administración de ADFS. Vaya a **ADFS > Relación de confianza > Confianza del proveedor de reclamos**.

    a) Haga clic con el botón derecho y seleccione **Agregar confianza del proveedor**



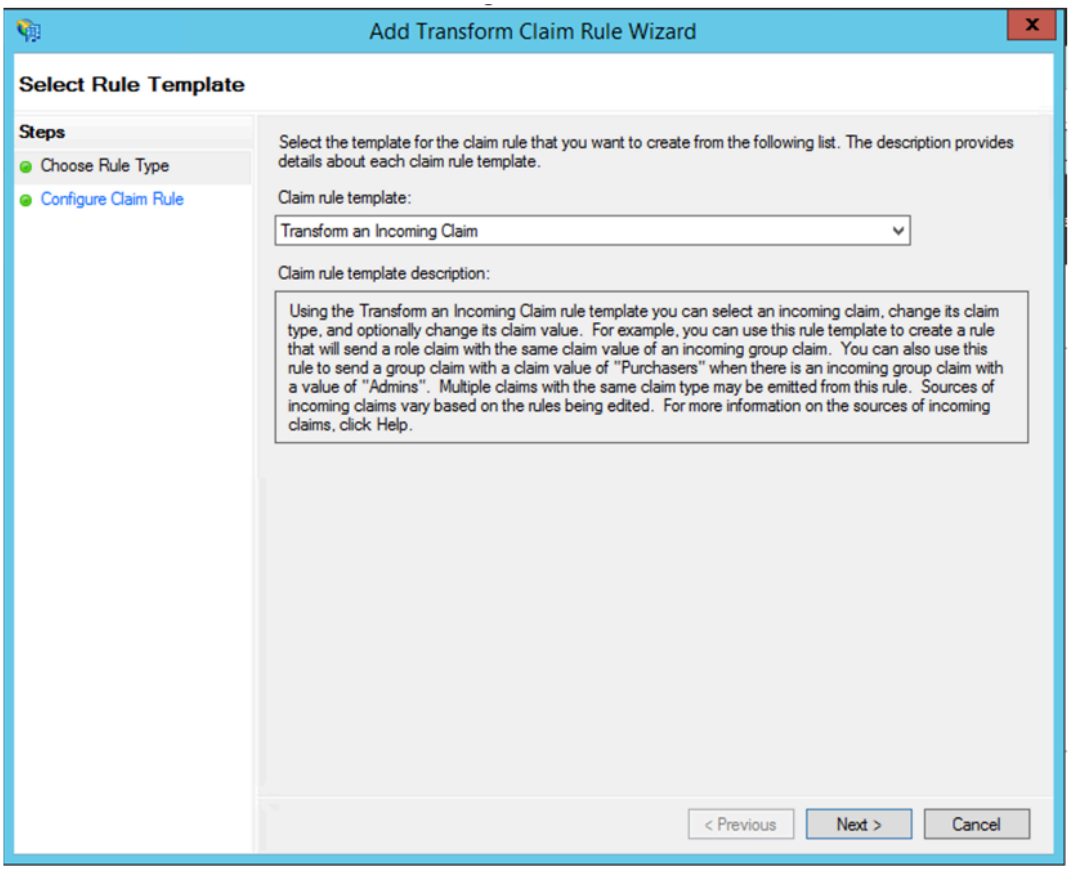
b) Agregue una aplicación en Secure Private Access que se utilice para federarse a ADFS. Para obtener más información, consulte Configuración de aplicaciones en Citrix Secure Private Access.

> **Nota:**
>
> Primero agregue la aplicación y, desde la sección de configuración de SSO de la aplicación, puede descargar el archivo de metadatos SAML y, a continuación, importar el archivo de metadatos en ADFS.

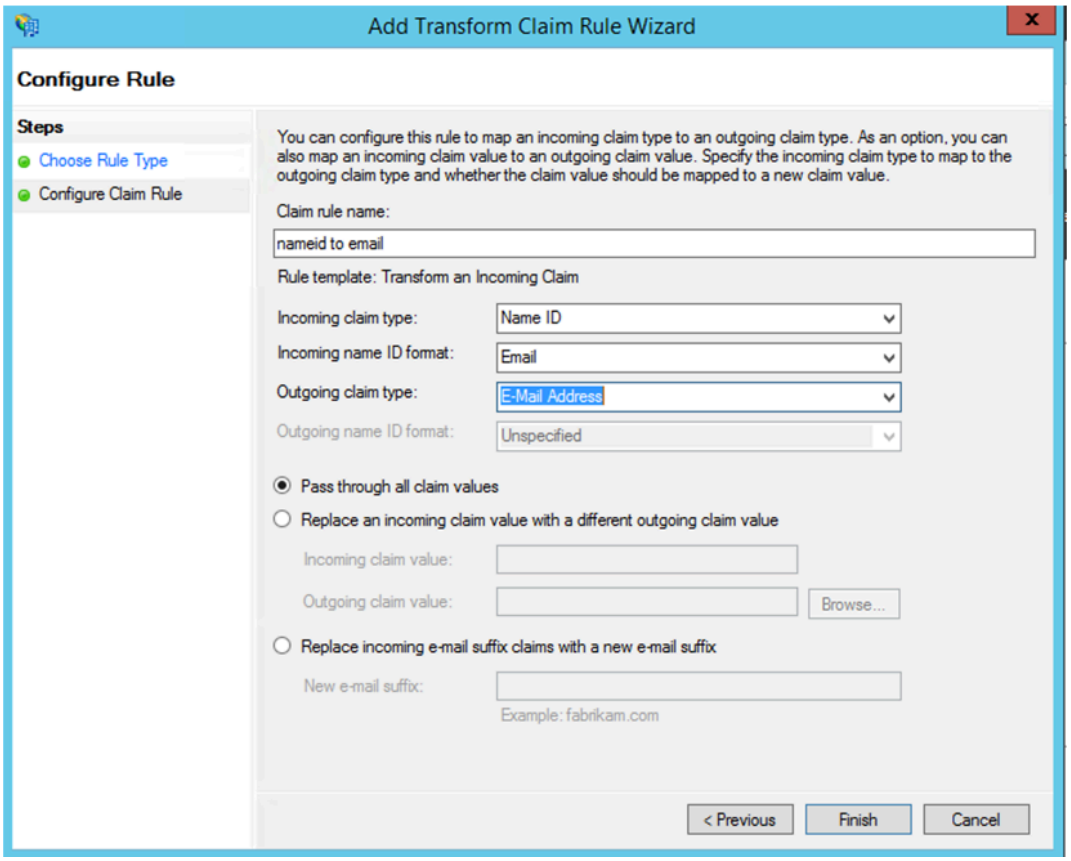


a) Complete los pasos para terminar de agregar la confianza del proveedor de reclamos. Después de agregar la confianza del proveedor de reclamos, aparecerá una ventana para modificar la regla de reclamación.

b) Agrega una regla de reclamo con **Transformar un reclamo entrante**.



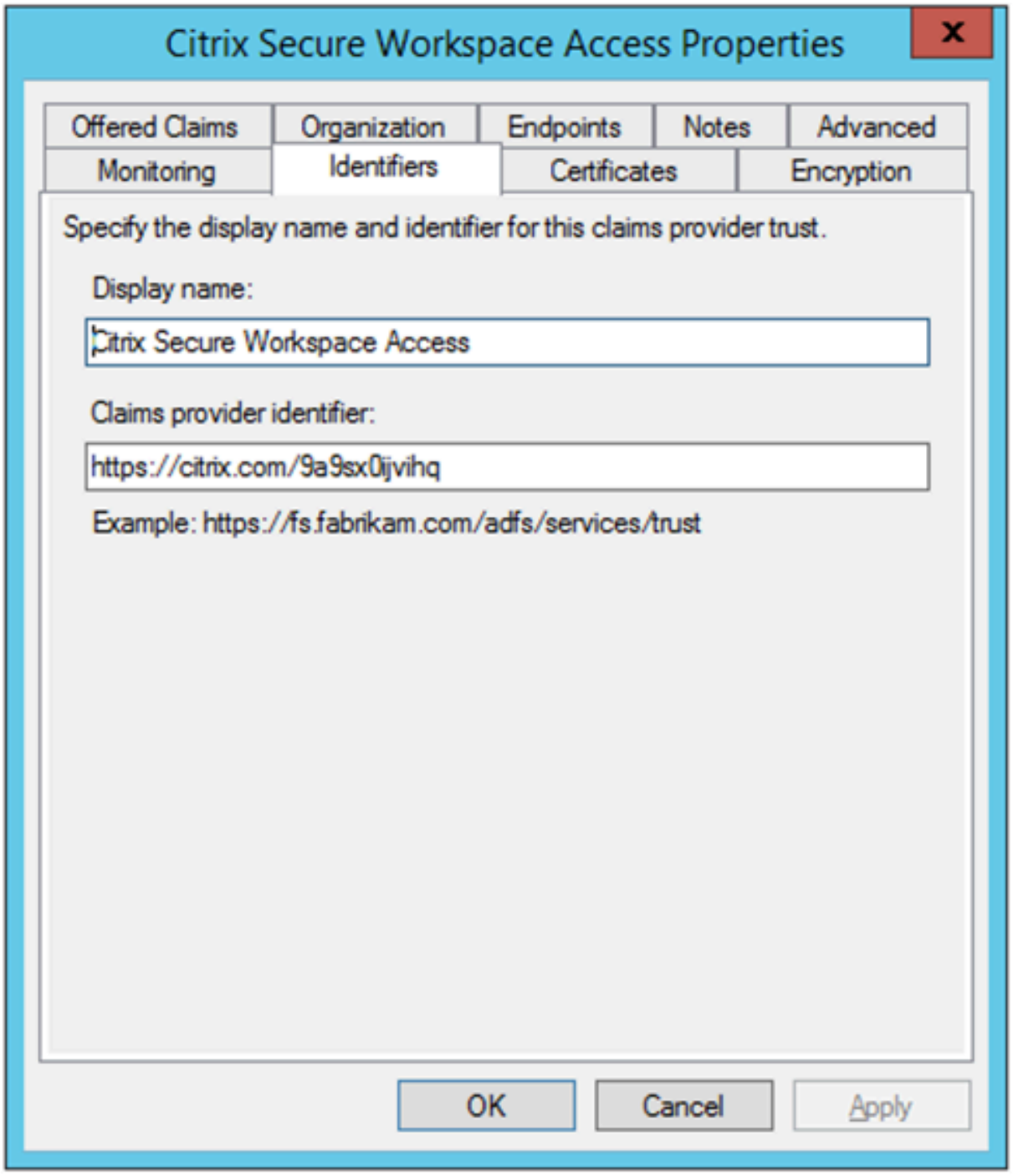
c) Complete los parámetros tal y como se muestra en la siguiente ilustración. Si su ADFS acepta otros reclamos, utilícelos y configure el SSO en Secure Private Access también en consecuencia.



Ahora ha configurado la confianza del proveedor de notificaciones que confirma que ADFS ahora confía en Citrix Secure Private Access para SAML.

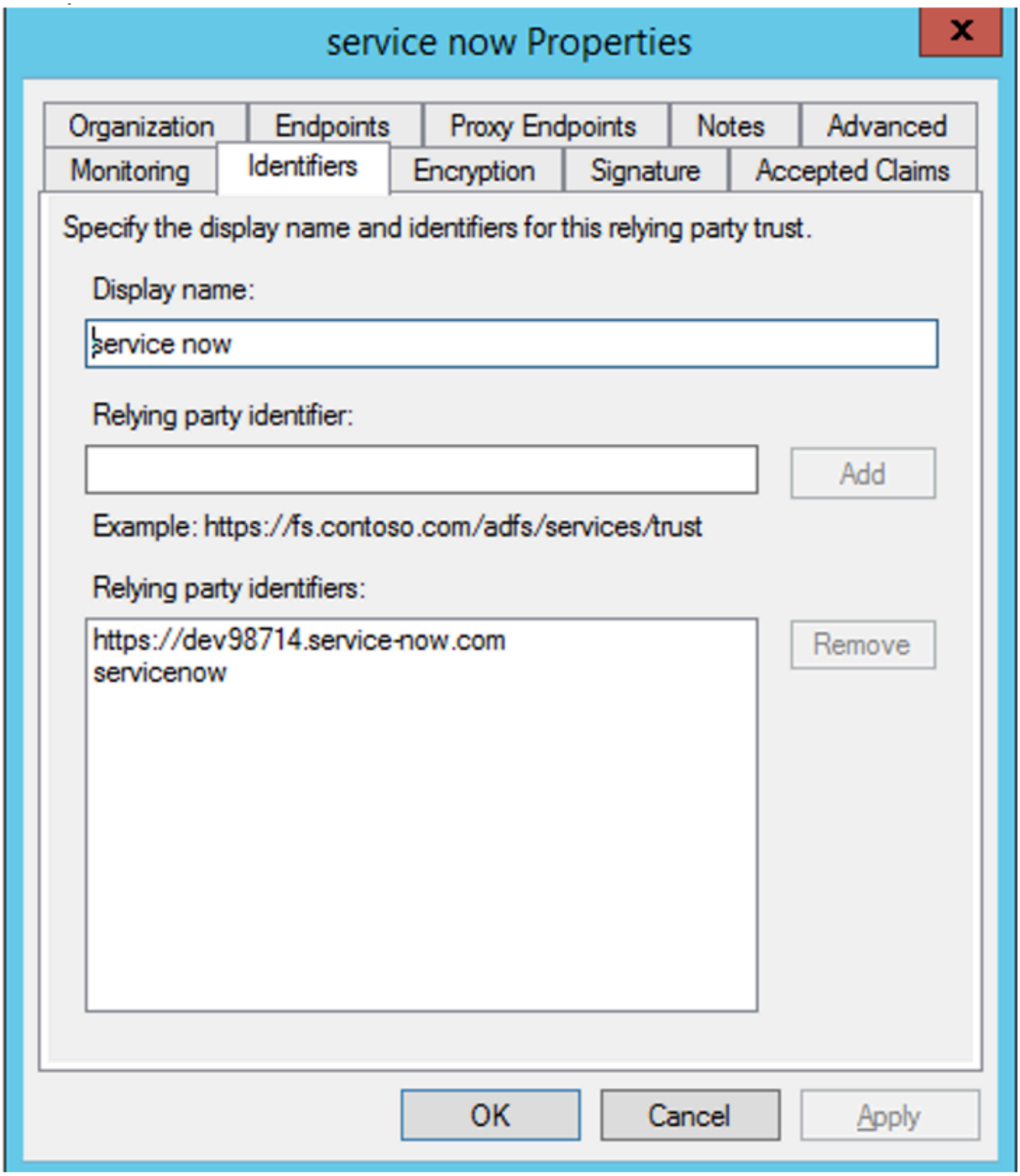
ID de confianza del proveedor de reclamaciones

Anote el identificador de confianza del proveedor de reclamos que agregó. Necesita este ID para configurar la aplicación en Citrix Secure Private Access.



Identificador de parte transmisora

Si su aplicación SaaS ya está autenticada mediante ADFS, entonces ya debe haber agregado la confianza de la parte de retransmisión para esa aplicación. Necesita este ID para configurar la aplicación en Citrix Secure Private Access.



Habilitar el estado de retransmisión en el flujo iniciado por

RelayState es un parámetro del protocolo SAML que se utiliza para identificar el recurso específico al que acceden los usuarios después de iniciar sesión y dirigirse al servidor de federación de la parte de confianza. Si RelayState no está habilitado en ADFS, los usuarios ven un error después de autenticarse en los proveedores de recursos que lo requieren.

Para ADFS 2.0, debe instalar la actualización KB2681584 (paquete acumulativo de actualizaciones 2) o KB2790338 (paquete acumulativo de actualizaciones 3) para proporcionar compatibilidad con RelayState. ADFS 3.0 tiene compatibilidad con RelayState incorporada. En ambos casos, RelayState aún debe estar habilitado.

Para habilitar el parámetro RelayState en los servidores ADFS

1. Abre el archivo.
   - Para ADFS 2.0, introduzca el siguiente archivo en el Bloc de notas: %systemroot%\inetpub\adfs\ls\web.
   - Para ADFS 3.0, introduzca el siguiente archivo en el Bloc de notas: %systemroot%\ADFS\Microsoft.Ident
2. En la sección Microsoft.identityServer.web, agregue una línea para useRelyStateForIdpInitiatedSignOn de la siguiente manera y guarde el cambio:
   ```
   <microsoft.identityServer.web> ... <useRelayStateForIdpInitiatedSignOn
    enabled="true"/> ...</microsoft.identityServer.web>
   ```
   - Para ADFS 2.0, ejecute `IISReset` para reiniciar IIS.
3. Para ambas plataformas, reinicie los Servicios de federación de Active Directory (`adfssrv`) `service`.
   Nota: Si tiene Windows 2016 o Windows 10, utilice el siguiente comando de PowerShell para habilitarlo.
   ```
   Set-AdfsProperties -EnableRelayStateForIdpInitiatedSignOn $true
   ```

Enlace a los comandos - https://docs.microsoft.com/en-us/powershell/module/adfs/set-adfsproperties?view=win10-ps

Configuración de aplicaciones en Citrix Secure Private Access

Puede configurar el flujo iniciado por el IdP o el flujo iniciado por el SP. Los pasos para configurar el flujo iniciado por el proveedor de identidad o el SP en Citrix Secure Private Access son los mismos, excepto que para el flujo iniciado por el SP, debe seleccionar la casilla de verificación **Iniciar la aplicación con la URL especificada (iniciado por el SP)** en la interfaz de usuario.

Flujo iniciado por IdP

1. Al configurar el flujo iniciado por el IdP, configure lo siguiente.
   - **URL de la aplicación**: Utilice el siguiente formato para la URL de la aplicación.
     ```
     https://<adfs fqdn>/adfs/ls/idpinitiatedsignon.aspx?LoginToRP
     =<rp id>&RedirectToIdentityProvider=<idp id>
     ```


- **FQDN de ADFS**: FQDN de la configuración de ADFS.
- **ID de RP**: ID de RP es el ID que puede obtener de la confianza de la parte de retransmisión. Es lo mismo que el identificador de parte de retransmisión. Si se trata de una URL, se produce la codificación de URL.
- ID de**IDP: el ID** de IdP es el mismo que el ID de confianza del proveedor de reclamos. Si se trata de una URL, se produce la codificación de URL.

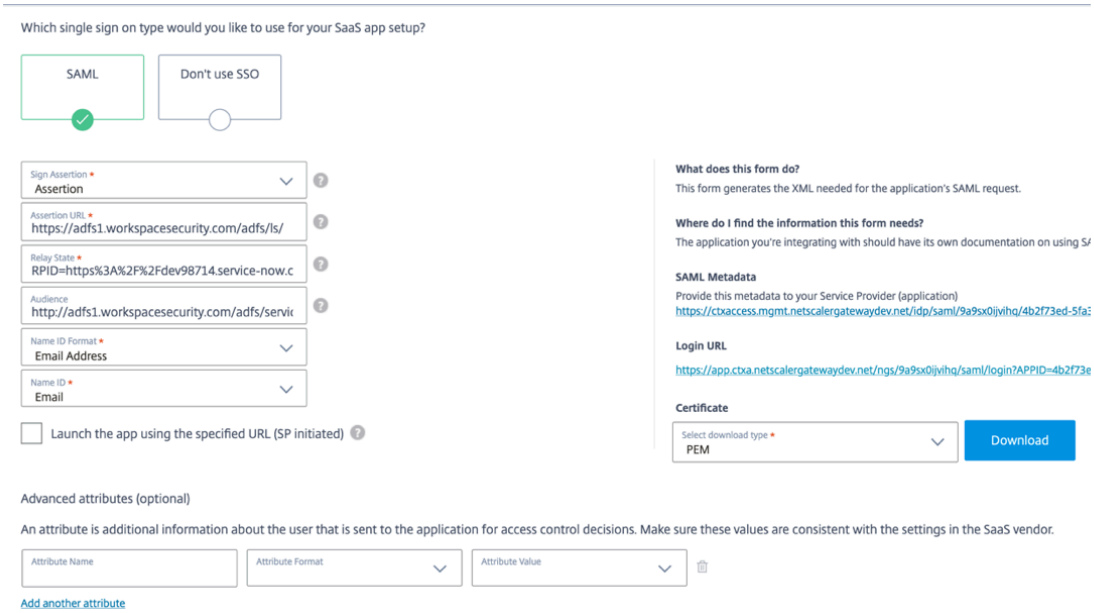
  Ejemplo: https://adfs1.workspacesecurity.com/adfs/ls/idpinitiatedsignon.aspx?LoginToRP=https%3A%2F%2Fdev98714.service-now.com&RedirectToIdentityProvider=https%3A%2F%2Fcitrix.com%2F9a9sx0ijvihq

2. Configuración de SSO SAML.

   A continuación se muestran los valores predeterminados del servidor ADFS. Si se cambia alguno de los valores, obtenga los valores correctos de los metadatos del servidor ADFS. Los metadatos de federación del servidor ADFS se pueden descargar desde su extremo de metadatos de federación, cuyo extremo se puede conocer en **ADFS > Servicio > Dispositivos de punto final.**

   - **URL de afirmación** —`https://<adfs fqdn>/adfs/ls/`
   - **Estado de retransmisión**: El estado de retransmisión es importante para el flujo iniciado por IdP. Siga este enlace para construirlo correctamente - `https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/jj127245(v=ws.10)`

     Ejemplo: RPID=https%3A%2F%2Fdev98714.service-now.com&RelayState=https%3A%2F%2Fdev9871
     now.com%2F
   - **Público** —`http://<adfsfqdn>/adfs/services/trust`
   - Para ver los demás valores de configuración de SSO SAML, consulte la siguiente imagen. Para obtener más información, consulte https://docs.citrix.com/en-us/citrix-secure-private-access/service/support-saas-apps.html



3. Guarda y suscribe la aplicación al usuario.

Flujo iniciado por SP

Para el flujo iniciado por el SP, configure los valores tal como se capturaron en la sección **Flujo iniciado por IDP**. Además, active la casilla de verificación **Iniciar la aplicación con la URL especificada (iniciada por el SP)**.

Solucionar problemas de Secure Private Access

February 16, 2024

Usa este tema para solucionar algunos de los problemas de configuración, autenticación y SSO de la aplicación o relacionados con el acceso a la aplicación. Copia el código de información de la columna "Código de información"de los registros de diagnóstico de Secure Private Access y, a continuación, busca ese código en esta página para encontrar los pasos de solución de problemas correspondientes. Las siguientes son algunas preguntas frecuentes que le ayudarán a utilizar mejor este tema.

¿Preguntas frecuentes?

¿Qué son los registros de diagnóstico de Secure Private Access?

¿Dónde puedo encontrar los registros de Secure Private Access?

¿Qué detalles puedo encontrar en los registros de diagnóstico de Secure Private Access?

¿Qué eventos se capturan en los registros de diagnóstico de Secure Private Access?

¿Cómo utilizo el tema de solución de problemas de Secure Private Access para resolver un error que he detectado?

¿Qué es un código de información? ¿Dónde puedo encontrarlos?

¿Qué es un identificador de transacción? ¿Cómo lo uso?

¿Cuáles son todas las ubicaciones PoP de Secure Private Access?

¿Qué hago si no puedo resolver mi error mediante el código de información y la tabla de búsqueda de errores?

Tabla de búsqueda de códigos de información

La siguiente tabla de búsqueda de errores proporciona una visión general completa de los diversos errores que los usuarios pueden encontrar cuando utilizan el servicio Secure Private Access.

Código de información	Descripción	La resolución
0x180006, 0x1800B7	No se pudo iniciar la aplicación porque se superó la longitud del FQDN de la aplicación	No se pudo iniciar la aplicación porque se superó la longitud del FQDN de la aplicación
0x180022	No se pudo iniciar la aplicación porque el servicio de autenticación está inactivo	Falló el inicio de la aplicación porque el servicio de autenticación está inactivo
0x180001, 0x18001A, 0x18001B, 0x18008A, 0x1800A9, 0x1800AA, 0x1800AB, 0x1800AC, 0x1800AD, 0x1800AE, 0x1800AF, 0x1800B0, 0x1800B1, 0x1800B2, 0x1800B3, 0x180048	Errores de inicio de sesión único, error de establecimiento de conexión entre Citrix Cloud y los conectores locales, error de SSO de SAML, FQDN de aplicación no válido	Se ha denegado el acceso a la aplicación
0x1800EF	Problema de conexión a Connector Appliance	Problema de conexión a Connector Appliance
0x18009D	Error en la búsqueda/conexión de DNS	Secure Browser Service: errores de búsqueda/conexión de DNS

Código de información	Descripción	La resolución
0x1800A0, 0x1800A2, 0x1800A3, 0x1800A5, 0x1800A6, 0x1800A7	Falló el inicio de la aplicación web porque no se pudo conectar a la aplicación web de fondo	Falló el inicio de la aplicación web porque no se pudo conectar a la aplicación web de fondo
0x1800BC, 0x1800BF	El usuario no tiene derecho a acceder a la aplicación web/SaaS	El usuario no tiene derecho a acceder a la aplicación web/SaaS
0x1800BD	El usuario no tiene derecho a acceder a la aplicación web/SaaS para DirectAccess	El usuario no tiene derecho a acceder a la aplicación web/SaaS para DirectAccess
0x1800D0	No se pudo iniciar la sesión del agente Citrix Secure Access al obtener la configuración de la aplicación	No se pudo iniciar la sesión del agente Citrix Secure Access al obtener la configuración de la aplicación
0x1800CD, 0x1800CE, 0x1800D6, 0x1800EA	El inicio de sesión del agente Citrix Secure Access falló al obtener la configuración de la aplicación, el inicio de la aplicación Citrix Secure Access Agent no se pudo iniciar durante la evaluación de la directiva, el inicio de la aplicación Citrix Secure Access Agent no se pudo iniciar	Solicitudes de clientes mal formadas
0x1800DE	No se pudo iniciar la aplicación Citrix Secure Access Agent durante la evaluación de la directiva	No se pudo iniciar la aplicación Citrix Secure Access Agent durante la evaluación de la directiva
0x180055, 0x1800DF, 0x1800E3	Aplicaciones restringidas por una directiva contextual, acceso denegado debido a la configuración de la directiva	Una o más aplicaciones que no aparecen en el panel del usuario
0x1800EB	No se pudo iniciar la aplicación Citrix Secure Access Agent porque no se admite IPv6	No se pudo iniciar la aplicación Citrix Secure Access Agent porque no se admite IPv6

Código de información	Descripción	La resolución
0x1800EC, 0x1800ED	No se pudo iniciar la aplicación Citrix Secure Access Agent debido a una dirección IP no válida	No se pudo iniciar la aplicación Citrix Secure Access Agent debido a una dirección IP no válida
0x10000001, 0x10000002, 0x10000003, 0x10000004	Error de inicio de sesión del cliente Citrix Secure Access debido a un problema de red	Problema de accesibilidad de la conectividad de red con el cliente Citrix Secure Access
0x10000006	Error de inicio de sesión en el cliente Citrix Secure Access debido a un proxy en el medio	El servidor proxy interfiere en la conectividad del cliente con el servicio
0x10000007	Error de inicio de sesión del cliente Citrix Secure Access debido a una entidad de certificación que no es de confianza	Se ha observado un problema con el certificado de servidor no confiable
0x10000008	Error de inicio de sesión del cliente Citrix Secure Access debido a un certificado no válido	Se ha observado un problema de certificado de servidor no válido
0x1000000A	Error de inicio de sesión en el cliente Citrix Secure Access debido a un problema de configuración	No se pudo iniciar sesión porque la configuración está vacía para el usuario
0x1000000B	Error de inicio de sesión del cliente Citrix Secure Access debido a un error de conexión	Conexión finalizada por la red o el usuario final
0x10000010	Error de inicio de sesión en el cliente Citrix Secure Access debido a una sesión caducada	No se pudo descargar la configuración porque la sesión ha caducado
0x10000013	Error de inicio de sesión en el cliente Citrix Secure Access debido a la enorme lista de configuraciones	El cliente Citrix Secure Access no pudo iniciar sesión
0x11000003	Error de inicio de sesión en el cliente Citrix Secure Access debido a un error en la creación del canal de control	No se pudo establecer el canal de control porque la sesión ha caducado

Código de información	Descripción	La resolución
0x11000004	Error de inicio de sesión del cliente Citrix Secure Access debido a un error en la creación del canal de control	Fallo al establecer el canal de control
0x11000005	Error de inicio de sesión del cliente Citrix Secure Access debido a un error en la creación del canal de control	Fallo al establecer el canal de control
0x11000006	Error de inicio de sesión del cliente Citrix Secure Access debido a un error en la creación del canal de control	No se pudo establecer el canal de control debido a un problema de red
0x12000001	Error al cerrar sesión en el cliente Citrix Secure Access porque la sesión ya ha caducado	No se puede cerrar sesión porque la sesión ha terminado
0x12000002	Error al cerrar sesión en el cliente Citrix Secure Access porque la sesión ya ha agotado el tiempo de espera	La sesión se ha terminado forzosamente
0x13000001	No se pudo acceder a la aplicación porque la sesión expiró	No se pudo iniciar la aplicación porque la sesión ha caducado
0x13000002	El acceso a la aplicación falló porque la licencia no es adecuada	Falló el lanzamiento de la aplicación debido a un problema de licencia
0x13000003, 0x13000008, 0x001800DF	El acceso a la aplicación falló porque el acceso está prohibido, se deniega el inicio de la aplicación TCP/UDP según la directiva	No se pudo iniciar la aplicación porque el servicio deniega el acceso
0x13000004, 0x13000005	No se pudo acceder a la aplicación porque el servidor no está disponible	No se pudo iniciar la aplicación porque el cliente no puede acceder al servicio

Código de información	Descripción	La resolución
0x13000007	No se pudo acceder a la aplicación porque la directiva de acceso está inhabilitada o el usuario no está suscrito	Falló el lanzamiento de la aplicación porque falló la evaluación de la directiva y la validación de la configuración
0x13000009	No se pudo acceder a la aplicación porque falta la entrada de enrutamiento	No se pudo iniciar la aplicación debido a problemas en la tabla de dominios de la aplicación
0x1300000B	El cliente cerró la conexión	El cliente cerró la conexión con el servicio Secure Private Access
0x1300000C	Falló la resolución de FQDN a través de ZTNA	El servidor DNS no puede resolver el FQDN
0x001800D3	Error al descargar la configuración de las aplicaciones al iniciar sesión	No se pudo obtener la lista de destinos de aplicaciones configurada
0x001800D9, 0x001800DA	El inicio de la aplicación TCP/UDP ha fallado durante el análisis de la respuesta de evaluación de la directiva, el inicio de la aplicación TCP/UDP ha fallado y el resultado no es válido durante la evaluación de la directiva	Problema de configuración de la aplicación
0x001800DB	No se pudo iniciar la aplicación TCP/UDP debido a que la configuración de ubicación de recursos no es válida	Problema con la ubicación del recurso

Código de información	Descripción	La resolución
0x13000006, 0x001800DC, 0x001800DD	El lanzamiento de la aplicación TCP ha fallado debido a una directiva de seguridad mejorada configurada para la aplicación que no es compatible, el lanzamiento de la aplicación TCP ha fallado debido a una redirección del servicio de explorador web seguro no compatible configurada para la aplicación TCP	La directiva de seguridad mejorada está vinculada a la aplicación HTTP
0x001800DE	No se pudo iniciar la aplicación TCP/UDP porque no se encontró ninguna configuración de aplicación para el destino	No se puede localizar la aplicación
0x001800EA	No se pudo iniciar la aplicación TCP debido a que el FQDN de destino es demasiado largo	La longitud del nombre de host supera los 256 caracteres
0x001800ED	El inicio de la aplicación TCP falló debido a una IP de destino no válida	Dirección IP no válida
0x001800EF	El inicio de la aplicación TCP falló durante el establecimiento de la conexión al servidor TCP privado	No se puede establecer una conexión de extremo a extremo
0x001800F5	Falló el inicio de la aplicación UDP debido a la dirección IPV6	IPv6 recibido en la solicitud de la aplicación
0x001800F9	El tráfico UDP no se pudo entregar porque se perdió la conexión del cliente	No se pudo entregar el tráfico UDP
0x001800FF	Fallo en la entrega del tráfico de datos UDP	Fallo en la entrega del tráfico de datos UDP
0x10000401	Fallo en el marcado del servidor Citrix Rendezvous	No se pudo iniciar la aplicación debido a problemas de conectividad de red

Código de información	Descripción	La resolución
0x10000402, 0x1000040C	No se puede registrar el Connector Appliance, error de inicialización de la conexión de red UDP	El dispositivo Connector no se pudo registrar en el servicio Secure Private Access
0x10000403, 0x10000404, 0x10000407, 0x1000040A, 0x1000040B, 0x1000040F, 0x10000410	Error de conexión, error de transmisión del paquete de control, error al leer el servicio de puerta de enlace, error de análisis de paquetes de control, error al escribir el servicio de puerta de enlace	Problema de conectividad con el Connector Appliance
0x10000405, 0x10000408, 0x10000409, 0x1000040D, 0x1000040E, 0x10000412	Back-end inalcanzable, error en la transmisión de paquetes UDP, error en la recepción de paquetes UDP, error al escribir el back-end, el backend cerró la conexión	Problemas de conectividad con Connector Appliance y los servidores TCP/UDP privados de fondo
0x10000406	Error en la resolución de DNS	El dispositivo Connector no puede resolver el DNS para los FQDN
0x10000411	El servicio Gateway cerró la conexión	Conexión al servidor privado finalizada
0x10000413	Error al determinar el motivo de la interrupción de la conexión	No se pudieron conectar ni enviar datos a la IP o FQDN del servicio privado
0x100508	El contexto del usuario no coincide con las condiciones de la regla de acceso	No hay condiciones de directiva coincidentes
0x100509	Directiva de acceso no asociada a la aplicación	No hay directiva de acceso asociada a la aplicación
0x10050C	Resultados de la evaluación de directivas de múltiples aplicaciones a las que el usuario podría tener derecho	Información de enumeración de aplicaciones

Código de información	Descripción	La resolución
0x00180101	Error al iniciar la aplicación TCP/UDP porque falta una entrada de enrutamiento en la tabla de dominios de la aplicación	Error al iniciar la aplicación TCP/UDP porque falta una entrada de enrutamiento en la tabla de dominios de la aplicación
0x00180102	Error al iniciar la aplicación TCP/UDP porque los conectores no están en buen estado	Error al iniciar la aplicación TCP/UDP porque los conectores no están en buen estado
0x00180103	Error en la solicitud UDP/DNS porque no se puede acceder al conector	Error en la solicitud UDP/DNS porque no se puede acceder al conector
0x20580001	No se pudo cargar la página porque la cookie NGS ha caducado	No se pudo cargar la página porque la cookie NGS ha caducado
0x20580002	No se pudo recuperar la directiva de acceso debido a un error en la red	No se pudo recuperar la directiva de acceso debido a un error en la red
0x20580003	Falló la búsqueda de la directiva de acceso al analizar el token web JSON	Falló la búsqueda de la directiva de acceso al analizar el token web JSON
0x20580004	Fallo de red al obtener los detalles de la directiva de acceso	Fallo de red al obtener los detalles de la directiva de acceso
0x20580005	Falló la búsqueda de directivas al obtener el certificado público	Falló la búsqueda de directivas al obtener el certificado público
0x20580007	Falló la búsqueda de directivas al validar la firma de JWT	Falló la búsqueda de directivas al validar la firma de JWT
0x20580008	Falló la búsqueda de directivas al validar el certificado público	Falló la búsqueda de directivas al validar el certificado público
0x2058000A	No se pudo determinar el entorno del almacén para formar una URL de directiva	No se pudo determinar el entorno del almacén para formar una URL de directiva

Código de información	Descripción	La resolución
0x2058000B	No se pudo obtener la respuesta a la solicitud de recuperación de la directiva de acceso	No se pudo obtener la respuesta a la solicitud de recuperación de la directiva de acceso
0x2058000C	Falló la búsqueda de la directiva de acceso debido a un token de autenticación DS secundario caducado	Falló la búsqueda de la directiva de acceso debido a un token de autenticación DS secundario caducado
0x10200002	El dispositivo Connector no está registrado	El dispositivo Connector no está registrado
0x10200003	No se puede conectar al dispositivo conector	No se puede conectar al dispositivo conector
0x10000301	Falló la conexión al servicio SPA de Citrix	Falló la conexión al servicio Citrix Secure Private Access
0x10000303, 0x10000304	No se puede acceder al servidor proxy	No se puede acceder al servidor proxy
0x10000305	Fallo en la autenticación del servidor proxy	Fallo en la autenticación del servidor proxy
0x10000306	No se puede acceder a los servidores proxy configurados	No se puede acceder a los servidores proxy configurados
0x10000307	Se recibió una respuesta de error del servidor back-end	Se recibió una respuesta de error del servidor back-end
0x10000005	No se puede enviar la solicitud a la URL de destino	No se puede enviar la solicitud a la URL de destino
0x10000107	No se pudo procesar el SSO	No se pudo procesar el SSO
0x10000108, 0x1000010B	No se pudo procesar el SSO, no se pudo determinar la configuración del SSO	No se pudo procesar el SSO, no se pudo determinar la configuración del SSO
0x10000101, 0x10000102, 0x10000103, 0x10000104	Falló el SSO de FormFill, configuración incorrecta de la aplicación de formulario	Falló el SSO de FormFill, configuración incorrecta de la aplicación de formulario

Código de información	Descripción	La resolución
0x1000010A	Falló el SSO de FormFill, configuración incorrecta de la aplicación de formulario	Falló el SSO de FormFill, configuración incorrecta de la aplicación de formulario
0x10000202	Falló el SSO de Kerberos	Falló el SSO de Kerberos
0x10000203	No se pudo procesar el inicio de sesión único para el tipo de autenticación	No se pudo procesar el inicio de sesión único para el tipo de autenticación
0x10000204	El SSO de Kerberos falló pero se recurrió a NTLM	El SSO de Kerberos falló pero se recurrió a NTLM

Pasos de resolución

Las siguientes secciones proporcionan los pasos de resolución para la mayoría de los códigos de información. Para los códigos en los que no se hayan capturado los pasos de resolución, póngase en contacto con el soporte de Citrix.

Una o más aplicaciones que no aparecen en el panel del usuario

Código de información: 0x180055, 0x1800DF, 0x1800E3

Debido a la configuración de la directiva contextual, es posible que algunos usuarios o dispositivos no vean las aplicaciones. Parámetros como los factores de confianza (postura del dispositivo o puntuación de riesgo) pueden afectar a la accesibilidad de las aplicaciones.

1. Copie el ID de transacción de la columna `reasons` correspondiente al código de error `0x18005C` en el archivo CSV de registros de diagnóstico.
2. Modifique el filtro de la columna `prod` en el archivo CSV para mostrar eventos del componente llamado `SWA.PSE` o `SWA.PSE.EVENTS`. Este filtro solo muestra los registros relacionados con la evaluación de directivas.
3. Busque la carga útil de la directiva evaluada en la columna `reason`. Esta carga útil muestra la directiva evaluada para el contexto del usuario para todas las aplicaciones a las que está suscrito el usuario.
4. Si la evaluación de la directiva indica que se ha denegado la aplicación para el usuario, las posibles razones pueden ser:

    - Condiciones coincidentes incorrectas en la directiva: compruebe la configuración de directivas de aplicaciones en Citrix Cloud

- Reglas de coincidencia incorrectas en la directiva: compruebe la configuración de directivas de aplicaciones en Citrix Cloud
- Regla predeterminada de coincidencia incorrecta en la directiva: este es un caso de caída. Ajuste las condiciones en consecuencia.

El usuario no tiene derecho a acceder a la aplicación web/SaaS

Código de información: 0x1800BC, 0x1800BF

Es posible que el usuario haya hecho clic en el enlace de la aplicación para la que no esté suscrito.

Asegúrese de que el usuario tenga una suscripción a las aplicaciones.

1. Vaya a la aplicación en el portal de administración.
2. Modifique la aplicación y vaya a la ficha **Suscripción**.
3. Asegúrese de que el usuario objetivo tenga una entrada en la lista de suscripciones.

Rendimiento lento de la aplicación del back-end

Código de información:0x18000F

Hay casos en los que la red del cliente es inestable debido a que los conectores de una ubicación de recursos pueden estar inactivos o es posible que el propio servidor de fondo no responda.

1. Asegúrese de que el dispositivo conector esté ubicado geográficamente cerca del servidor de fondo para descartar las latencias de la red.
2. Compruebe que el firewall del servidor del back-end no bloquee el Connector Appliance.
3. Compruebe si el cliente se está conectando al POP en la nube más cercano.

   Por ejemplo, `nslookup nssvc.dnsdiag.net` en el cliente, el nombre canónico de la respuesta indica el servidor geoespecífico, como `aws-us-w.g.nssvc.net`.

No se pudo iniciar la aplicación porque se superó la longitud del FQDN de la aplicación

Código de información: 0x180006, 0x1800B7

Los FQDN de aplicaciones no deben superar los 512 caracteres. Compruebe el FQDN de la aplicación en la página de configuración de la aplicación. Asegúrese de que la longitud no supere los 512 bytes.

1. Vaya a la ficha **Aplicaciones** de la consola de administración.
2. Busque la aplicación cuyo FQDN supere los 512 caracteres.
3. Modifique la aplicación y corrija la longitud del FQDN de la aplicación.

Se ha superado la longitud de detalles

Código de información: 0x18000E

Compruebe las directivas si están bloqueando el acceso a la aplicación.

1. Ve a **Políticas de acceso** .
2. Busca las directivas en las que la aplicación tiene derechos.
3. Revise las reglas y condiciones de la directiva para el usuario final.

Se ha denegado el acceso a la aplicación

Código de información: 0x180001, 0x18001A, 0x18001B, 0x18008A, 0x1800A9, 0x1800AB, 0x1800AC, 0x1800AD, 0x1800AE, 0x1800AF, 0x1800B0, 0x1800B1, 0x1800B2, 0x1800B3, 0x180048

Esto está relacionado con las políticas contextuales, en las que las políticas deniegan la aplicación a un usuario determinado.

Compruebe las directivas si están bloqueando el acceso a la aplicación

1. Ve a **Políticas de acceso** .
2. Busca las directivas en las que la aplicación tiene derechos.
3. Revise las reglas y condiciones de la directiva para el usuario final.

Aplicaciones no enumeradas

Es posible que las aplicaciones no aparezcan en la lista enumerada debido a la denegación de directivas o a que la integración de Secure Private Access no esté habilitada.

- Si el acceso debe estar habilitado para algunas de las aplicaciones pero no ves ninguna aplicación, prueba a habilitar la integración de Secure Private Access.
  - Inicie sesión en Citrix Cloud.
  - Seleccione **Configuración del espacio** de trabajo en el menú desplegable y, a continuación, haga clic en **Integraciones de servicios**.
  - Haga clic en el botón de puntos suspensivos de Secure Private Access y, a continuación, en **Habilitar.**
- Si la integración de Secure Private Access ya está habilitada, inhabilítela y vuelva a habilitarla para comprobar si tiene alguna aplicación.

Problema de conexión a Connector Appliance

Código de información: 0x1800EF

El enrutamiento de aplicaciones falla debido a la falta de disponibilidad de las conexiones TCP con los conectores locales.

Revisar los eventos del componente del controlador

1. Busque el `transaction ID` para el código de error `0x1800EF` en el archivo CSV de registros de diagnóstico.
2. Filtra todos los eventos que coincidan con el ID de transacción en el archivo csv.
3. Además, filtre la columna `prod` del archivo CSV que coincida con `SWA.GOCTRL`.

   Si ve eventos con el mensaje de `connectType` `multiconnect::success`?, entonces:

   - Esto indica que la solicitud de establecimiento de túnel se transmitió correctamente al controlador.
   - Compruebe si `Resource Location` en el mensaje del registro es correcto. Si no es correcta, corrija la ubicación del recurso en la sección de configuración de aplicaciones del portal de administración de Citrix.
   - Compruebe si `VDA Ip and Port` en el mensaje del registro es correcto. La IP y el puerto del VDA indican la IP y el puerto de la aplicación de fondo. Si no es correcto, corrija el FQDN o la dirección IP de la aplicación en la sección de configuración de aplicaciones del portal de administración de Citrix.
   - Revise los eventos de Connector si no encuentra ningún problema mencionado anteriormente.

   Si ve eventos con el mensaje de `connectType` `connect::failure` o `multiconnect::success`, entonces:

   - Compruebe si la solución recomendada para este mensaje de registro indica - `Check if connector is still connected to same pop`. Esto indica que es posible que el conector de la ubicación de recursos se haya caído. Proceda a revisar los eventos de Connector.
   - Póngase en contacto con el servicio de atención al cliente de Citrix si no aparecen los mensajes mencionados anteriormente

   Si ve eventos con el mensaje `connectType` de `IntraAll::failure`, contacte con el servicio de atención al cliente de Citrix.

Revisión de eventos del componente conector

1. Busque el `transaction ID` para el código de error `0x1800EF` en el archivo CSV de registros de diagnóstico.
2. Filtra todos los eventos que coincidan con el ID de transacción en el archivo csv.
3. Además, filtre la columna `prod` del archivo CSV que coincida con `SWA.ConnectorAppliance.WebApps`.
4. Si ve eventos con `status` como `failure`, entonces:
   - Revise el mensaje `reason` de cada uno de estos eventos de error.
   - `UnableToRegister` indica que el conector no se pudo registrar correctamente en Citrix Cloud. Póngase en contacto con Citrix Support.
   - `IsProxyRequiredCheckError` o `ProxyDialFailed` o `ProxyConnectionFailed` o `ProxyAuthenticationFailure` o `ProxiesUnReachable` indican que el conector no pudo resolver la URL del back-end mediante la configuración del proxy. Compruebe que la configuración del proxy sea correcta.
   - Para obtener más información sobre la depuración, consulte Eventos SSO de Connector

Errores de registro único

Para el inicio de sesión único, se extraen y aplican diferentes atributos de SSO de la configuración de la aplicación durante el inicio de la aplicación. Si ese usuario en particular no tiene los atributos o si los atributos son incorrectos, es posible que se produzca un error en el inicio de sesión único. Asegúrese de que la configuración sea correcta.

1. Vaya a **Directivas de acceso.**
2. Busca las directivas en las que la aplicación tiene derechos.
3. Revise las reglas y condiciones de la directiva para el usuario final.

Los métodos de SSO, como Form SSO, Kerberos y NTLM, los ejecuta el conector local. Revise los siguientes registros de diagnóstico del conector.

Revisar los eventos de SSO del componente conector

1. Filtre `component name` en el archivo CSV que coincida `SWA.ConnectorAppliance.WebApps`.
2. ¿Vaya los eventos con el estado “error”?
   - Revise el mensaje de cada uno de estos eventos de error.
   - `IsProxyRequiredCheckError` o `ProxyDialFailed` o `ProxyConnectionFailed` o `ProxyAuthenticationFailure` o `ProxiesUnReachable` indican que el conector no pudo resolver la URL del back-end mediante la configuración del proxy. Compruebe que la configuración del proxy sea correcta.

- `FailedToReadRequest` o `RequestReceivedForNonSecureBrowse` o `UnableToRetrieveUserCredentials` o `CCSPolicyIsNotLoaded` o `FailedToLoadBaseC` o `ProcessConnectionFailure` o `WebAppUnSupportedAuthType` indica un fallo en la tunelización. Póngase en contacto con Citrix Support.
- `UnableToConnectTargetServer` indica que no se puede acceder al servidor del back-end desde el conector. Compruebe de nuevo la configuración del back-end.
- `IncorrectFormAppConfiguration` o `NoLoginFormFound` o `FailedToConstructForLog` o `FailedToLoginViaFormBasedAuth` indica un error de autenticación basada en formularios. Consulte la sección Configuración de SSO del formulario en Configuración de aplicaciones en el portal de administración de Citrix.
- `NTLMAuthNotFound` indica un error de autenticación basada en NTLM. Consulte la sección Configuración de SSO NTLM en la configuración de la aplicación en el portal de administración de Citrix.
- Para obtener más información sobre la depuración, consulte Eventos de Connector.

Falló el inicio de la aplicación porque el servicio de autenticación está inactivo

Código de información: 0x180022

Secure Private Access permite a los administradores configurar un servicio de autenticación de terceros, como el Active Directory tradicional, AAD, Okta o SAML. Las interrupciones en estos servicios de autenticación pueden causar este problema.

Compruebe si los servidores de terceros están activos y se puede acceder a ellos.

Fallo de SSO de SAML

Código de información: 0x18008A, 0x1800A9, 0x1800AA, 0x1800AB, 0x1800AC, 0x1800AD, 0x1800AE, 0x1800AF, 0x1800B0, 0x1800B1, 0x1800B2, 0x1800B3

Los usuarios se enfrentan a un error de autenticación durante el inicio de la aplicación cuando se inicia el IdP o pueden ver enlaces inaccesibles cuando se inicia el SP. Compruebe la configuración de la aplicación SAML en el lado del servicio Secure Private Access y también en la configuración del proveedor de servicios.

Configuración de Secure Private Access:

1. Vaya a la ficha **Aplicaciones**.
2. Busca la aplicación SAML problemática.
3. Modifique la aplicación y vaya a la ficha **Single Sign-On**.
4. Compruebe los campos siguientes.
    - URL de aserción

- Estado de retransmisión
- Audiencia
- Formato de identificador de nombre, identificador de nombre y otros atributos

Configuración del proveedor de servicios:

1. Inicie sesión en el proveedor de servicios.
2. Vaya a **Configuración de SAML.**
3. Compruebe el certificado del IdP, el público y la URL de inicio de sesión del IdP

Si la configuración parece correcta, póngase en contacto con el soporte de Citrix.

FQDN de aplicación no válido

Código de información: 0x180048

Es posible que el administrador del cliente haya proporcionado un FQDN no válido o un FQDN en el que la resolución de DNS falla en el servidor del back-end.

En este caso, el usuario final ve un error en la página web. Compruebe la configuración de la aplicación.

Validación de aplicaciones SaaS Compruebe si se puede acceder a la aplicación desde la red.

Validación de aplicaciones web

1. Vaya a la ficha **Aplicaciones**.
2. Modifique la aplicación problemática.
3. Vaya a la página **Detalles de la aplicación**.
4. Comprueba la URL. La URL debe estar accesible en la intranet o en Internet.

Secure Browser Service: error en la búsqueda/conexión de DNS

Código de información: 0x18009D

Experiencia de navegación interrumpida a través del servicio de aislamiento remoto del navegador. Compruebe el servidor del back-end al que el usuario final intenta conectarse.

1. Vaya al servidor del back-end y compruebe si está en funcionamiento y si puede recibir las solicitudes.
2. Compruebe la configuración del proxy si detiene la conexión con el servidor del back-end.

> **Nota:**
>
> El servicio Citrix Remote Browser Isolation se conocía anteriormente como Secure Browser Service.

CWA Web: errores de búsqueda/conexión de DNS para aplicaciones web

Código de información: 0x1800A0, 0x1800A2, 0x1800A3, 0x1800A5, 0x1800A6, 0x1800A7

Experiencia de navegación interrumpida de las aplicaciones web que se ejecutan dentro de una red corporativa.

1. Filtre los registros de diagnóstico de los FQDN que no se pueden resolver.
2. Compruebe la accesibilidad del servidor del back-end desde el interior de la red corporativa.
3. Compruebe la configuración del proxy para ver si el conector está bloqueado y no puede llegar al servidor del back-end.

Acceso directo: mal configurada como aplicación web

Dado que el tráfico de aplicaciones web siempre se redirige a través del conector, al configurar el acceso directo en ellas se produce un error de acceso a la aplicación.

Compruebe si hay conflictos de configuración entre la tabla de dominios de redirección y la configuración de la aplicación.

1. Vaya a la aplicación en el portal de administración.
2. Modifique la aplicación y comprueba si el acceso directo está habilitado.
3. Compruebe el FQDN de la aplicación dentro de la tabla de dominios de enrutamiento si está marcado como interno.

El usuario no tiene derecho a acceder a la aplicación web/SaaS para DirectAccess

Código de información: 0x1800BD

La configuración de la aplicación inhabilita el acceso directo para el tráfico que se origina en los clientes basados en explorador web.

Asegúrese de que el usuario tenga una suscripción a las aplicaciones.

1. Vaya a la aplicación en el portal de administración.
2. Modifique la aplicación y compruebe la configuración de acceso sin agente.

Directivas de seguridad mejoradas: configuración incorrecta de Secure Browser Service

Código de información: 0x1800C3

Se ha visto un comportamiento incorrecto de lo que pretendían las reglas de la directiva. Consulte las directivas de acceso contextual.

1. Vaya a la ficha **Directivas**.
2. Consulte las directivas asociadas a la aplicación.
3. Consulte las reglas de esas directivas.

Directivas de seguridad mejoradas: configuración errónea de directivas

Se ha visto un comportamiento incorrecto de lo que pretendían las reglas de la directiva. Compruebe la configuración de seguridad mejorada.

1. Vaya a la aplicación.
2. Haga clic en la ficha **Directivas de acceso**.
3. Comprueba la configuración en la sección **Restricciones de seguridad disponibles:**

No se pudo iniciar la sesión del agente Citrix Secure Access al obtener la configuración de la aplicación

Código de información: 0x1800D0

La aplicación Citrix Secure Access no puede establecer correctamente un túnel completo a Citrix Cloud.

1. Revise la configuración del dominio de redirección para las aplicaciones TCP/UDP.
2. Asegúrese de que el número máximo de entradas esté dentro del límite de 16 000.

Aplicaciones TCP/UDP: solicitudes de clientes mal formadas

Código de información: 0x1800CD, 0x1800CE, 0x1800D6, 0x1800EA

El túnel VPN no está establecido o es posible que algunos FQDN no estén tunelizados.

1. Asegúrese de que los proxies del medio no fabriquen ni reconstruyan las solicitudes.
2. Presuntos ataques de intermediario.

Aplicaciones TCP/UDP: configuración incorrecta de redireccionamiento de Secure Browser

Código de información: 0x1800DD

Los redireccionamientos del servicio de aislamiento remoto del navegador solo se pueden aplicar a aplicaciones web y no a aplicaciones TCP/UDP. Revise la configuración de la aplicación en la GUI del servicio Secure Private Access.

> **Nota:**
>
> El servicio Citrix Remote Browser Isolation se conocía anteriormente como Secure Browser Service.

No se pudo iniciar la aplicación del agente Citrix Secure Access durante la evaluación de la directiva

Código de información: 0x1800DE

Asegúrese de que todos los FQDN internos que el cliente Citrix Secure Access va a tunelizar tengan la entrada correspondiente en la tabla de dominios de enrutamiento.

No se pudo iniciar la aplicación Citrix Secure Access Agent porque no se admite IPv6

Código de información: 0x1800EB

Revise las entradas del dominio de redirección. Asegúrese de que no haya entradas IPV6 en la tabla.

No se pudo iniciar la aplicación Citrix Secure Access Agent debido a una dirección IP no válida

Código de información:0x1800EC, 0x1800ED

Revise las entradas del dominio de redirección. Asegúrese de que las direcciones IP sean válidas y apunten al backend correcto.

Problema de accesibilidad de la conectividad de red con el cliente Citrix Secure Access

Código de información: 0x10000001, 0x10000002, 0x10000003, 0x10000004

1. Compruebe si se puede acceder a la red del equipo cliente. Si se puede acceder a la red, póngase en contacto con el soporte de Citrix con los registros de depuración del cliente.
2. Compruebe si el proxy o el firewall están bloqueando la red.

Para recopilar los registros de depuración de los clientes, consulte Cómo recopilar los registros de los clientes.

El servidor proxy interfiere en la conectividad del cliente con el servicio

Código de información: 0x10000006

1. Compruebe si se puede acceder a la red del equipo cliente.
2. Compruebe si el proxy está configurado correctamente en el cliente.
3. Si no hay problemas con ambos, póngase en contacto con el soporte de Citrix con los registros de depuración del cliente.

Para recopilar los registros de depuración de los clientes, consulte Cómo recopilar los registros de los clientes.

Se ha observado un problema con el certificado de servidor no confiable

Código de información: 0x10000007

Póngase en contacto con el soporte de Citrix para comprobar si una CA válida ha generado correctamente el certificado del servidor.

Se ha observado un problema de certificado de servidor no válido

Código de información: 0x10000008

Póngase en contacto con el soporte de Citrix para comprobar si el certificado del servidor está autofirmado, caducado o proviene de una fuente que no es de confianza.

No se pudo iniciar sesión porque la configuración está vacía para el usuario

Código de información: 0x1000000A

1. Asegúrese de que esté configurada al menos una aplicación TCP/UDP/HTTP. Para obtener más información, consulte Agregar y administrar aplicaciones.
2. Asegúrese de que la tabla Dominio de la aplicación (**Secure Private Access > Configuración > Dominio de la aplicación**) no esté vacía o que todas las entradas no estén inhabilitadas. Los destinos configurados en la aplicación TCP/UDP/HTTP se agregan automáticamente a esta tabla.

Se recomienda no eliminar ni inhabilitar los destinos o la URL de una aplicación TCP/UDP/HTTP activa.

Conexión finalizada por la red o el usuario final

Código de información: 0x1000000B

Compruebe si la red está interrumpida o si el usuario final canceló la conexión durante la conexión a la sesión de ZTNA.

No se pudo descargar la configuración porque la sesión ha caducado

Código de información: 0x10000010

Es posible que la sesión de VPN haya caducado durante la solicitud de descarga de la configuración de sesión de ZTNA. Intente volver a iniciar sesión en el cliente Citrix Secure Access.

El cliente Citrix Secure Access no pudo iniciar sesión

Código de información: 0x10000013

El cliente Citrix Secure Access no pudo iniciar sesión porque el tamaño de la configuración supera el límite máximo de configuración.

1. Revise la configuración del dominio de enrutamiento para las aplicaciones TCP/UDP en **Secure Private Access > Configuración**Dominio de la aplicación
2. Asegúrese de que la cantidad de entradas no sea enorme. Si la lista de entradas es enorme, desactive o elimine los destinos no utilizados.

   Si se espera que la lista de destinos supere los 1000 segundos, intente aumentar el tamaño máximo de descarga de la configuración actualizando la clave de registro ConfigSize. Para obtener más información, consulte las claves de registro del cliente VPN de Citrix Gateway.

No se pudo establecer el canal de control porque la sesión ha caducado

Código de información: 0x11000003

El canal de control para el establecimiento de la solicitud de DNS ha fallado porque la sesión ha caducado.

Es posible que la sesión de ZTNA haya caducado durante la configuración del canal de control.

Intente volver a iniciar sesión en el cliente Citrix Secure Access.

Fallo al establecer el canal de control

Código de información: 0x11000004

Se ha producido un error en el canal de control para el establecimiento de solicitudes de DNS.

- **Mantenga la ubicación de los recursos en buen estado:**

1. Inicie sesión en Citrix Cloud.
2. Haga clic en **Ubicación de recursos** en el menú de tres líneas.
3. Ejecute una comprobación del estado de los dispositivos conectores en la ubicación de recursos correspondiente.
4. Si esto no soluciona el problema, intente reiniciar la máquina virtual del conector.

- **Mantenga el dispositivo con conector HA:**

1. Inicie sesión en Citrix Cloud.
2. Haga clic en **Ubicación de recursos** en el menú de tres líneas.
3. Asegúrese de que la ubicación de recursos esperada tenga al menos dos dispositivos Connector.

Asegúrese de lo siguiente:

- La LAN de ubicación de recursos funciona correctamente.
- No hay ningún firewall o proxy en el medio que bloquee el acceso de Connector Appliance al servicio o a los servidores back-end.
- La red de clientes está en buen estado.
- Los servidores privados de fondo están en funcionamiento.
- Los servidores DNS están en funcionamiento.
- Los FQDN se pueden resolver.

Si cumple con las recomendaciones anteriores, haga lo siguiente.

1. Obtenga el ID de transacción del registro de diagnóstico de este error.
2. Filtre todos los eventos que coincidan con el ID de la transacción en el panel de Secure Private Access.
3. Compruebe si se ha producido algún error en los registros de diagnóstico del cliente o del dispositivo o servicio Connector que coincida con el ID de la transacción. A continuación, tome las medidas apropiadas en consecuencia.
4. Compruebe si la ubicación del recurso se ha elegido correctamente para el destino en la tabla de dominios de la aplicación (**Secure Private Access > Configuración > Dominio de la aplicación**).
5. Compruebe si la aplicación está configurada con el puerto, los rangos de IP y los dominios correctos. Para obtener más información, consulte Agregar y administrar aplicaciones.

Si aún no puede resolver el problema, póngase en contacto con el soporte de Citrix con el código de error correspondiente al ID de transacción y a los registros del cliente.

Para recopilar los registros de depuración de los clientes, consulte Cómo recopilar los registros de los clientes.

Fallo al establecer el canal de control

Código de información: 0x11000005

No se pudo establecer el canal de control (para la solicitud de DNS).

1. Compruebe los derechos de licencia del servicio Secure Private Access.
2. Si no tiene derecho, póngase en contacto con el soporte de Citrix para comprobar la licencia.

Para obtener información detallada, consulte https://www.citrix.com/buy/licensing/product.html.

No se pudo establecer el canal de control debido a un problema de red

Código de información: 0x11000006

No se pudo establecer el canal de control (para la solicitud de DNS) debido a un problema de red.

1. Compruebe si se puede acceder al servicio Secure Private Access.
2. Si no se puede acceder a él, póngase en contacto con el soporte de Citrix con el código de error y los registros del cliente.

Para recopilar los registros de depuración de los clientes, consulte Cómo recopilar los registros de los clientes.

No se pudo establecer el canal de control debido a la insuficiencia de IIP

Código de información: 0x11000007

No se pudo establecer el canal de control (para la solicitud de DNS) debido a la insuficiencia de IIP.

Póngase en contacto con el soporte de Citrix con el código de error y los registros del cliente.

Para recopilar los registros de depuración de los clientes, consulte Cómo recopilar los registros de los clientes.

No se puede cerrar sesión porque la sesión ha terminado

Es posible que este problema se haya producido porque el equipo cliente (teclado o ratón) estuvo inactivo durante un período de tiempo de espera superior al configurado.

Código de información: 0x12000001

Intente volver a iniciar sesión en el cliente Citrix Secure Access.

La sesión se ha terminado forzosamente

La sesión se termina forzosamente cuando se alcanza el tiempo de espera forzado configurado.

Código de información: 0x12000002

Intente volver a iniciar sesión en el cliente Citrix Secure Access.

No se pudo iniciar la aplicación porque la sesión ha caducado

Código de información: 0x13000001

1. La sesión de ZTNA ha caducado durante el lanzamiento de la aplicación.
2. Intente volver a iniciar sesión en el cliente Citrix Secure Access.

Falló el lanzamiento de la aplicación debido a un problema de licencia

Código de información: 0x13000002

1. Compruebe si la licencia del servicio Secure Private Access es la que le corresponde.
2. Si no tiene derecho, póngase en contacto con el soporte de Citrix para comprobar la licencia.

Para obtener información detallada, consulte https://www.citrix.com/buy/licensing/product.html.

No se pudo iniciar la aplicación porque el servicio deniega el acceso

Código de información: 0x13000003, 0x13000008, 0x001800DF

El inicio de la aplicación se deniega según la configuración de la directiva para el usuario y la aplicación.

Asegúrese de lo siguiente.

- No se utilizan los mismos destinos en varias aplicaciones (HTTP, HTTPS, TCP, UDP)
- No hay destinos superpuestos en varias aplicaciones.

- Las directivas de acceso están vinculadas a las aplicaciones.

Compruebe también las condiciones y acciones de las directivas configuradas para la aplicación denegada. A continuación, revise las condiciones y acciones de la directiva.

Para obtener más información, consulte Directivas de acceso.

No se pudo iniciar la aplicación porque el cliente no puede acceder al servicio

Código de información: 0x13000004, 0x13000005

1. Compruebe si se puede acceder al Servicio de Secure Private Access.
2. Vuelva a iniciar la aplicación.
3. Si no se puede acceder a la aplicación durante mucho tiempo, póngase en contacto con el soporte de Citrix con el código de error y los registros del cliente.

Para recopilar los registros de depuración de los clientes, consulte Cómo recopilar los registros de los clientes.

Falló el lanzamiento de la aplicación porque falló la evaluación de la directiva y la validación de la configuración

Código de información: 0x13000007

No se pudo iniciar la aplicación porque el servicio Secure Private Access no pudo evaluar la directiva y validar la configuración.

No se pudo localizar la aplicación como destino al que se accedió.

No sepudo iniciar la aplicación porque el servicio deniega el acceso.

No se pudo iniciar la aplicación debido a problemas en la tabla de dominios de la aplicación

Código de información: 0x13000009

Error al iniciar la aplicación porque la tabla de dominios de la aplicación no tiene una entrada para el destino al que se ha accedido.

Compruebe que la entrada de ruta esté configurada correctamente para la aplicación en **Secure Private Access > Configuración > Dominio de la aplicación**.

El cliente cerró la conexión con el servicio Secure Private Access

Código de información: 0x1300000B

1. Compruebe si el usuario final cerró la conexión manualmente.
2. De lo contrario, póngase en contacto con el soporte de Citrix con el código de error y los registros del cliente.

Para recopilar los registros de depuración de los clientes, consulte Cómo recopilar los registros de los clientes.

El servidor DNS no puede resolver el FQDN

Código de información: 0x1300000C

Este problema se produce cuando el Connector Appliance no resuelve el DNS de los FQDN.

1. Compruebe la entrada DNS del FQDN de la aplicación correspondiente en el servidor DNS.
2. Asegúrese de que haya configurado un servidor DNS adecuado en los dispositivos Connector. Para obtener más información, consulte Configuración de los ajustes de red en la página de administración Connector Appliance.

No se puede localizar la aplicación

Código de información: 0x001800DE

Es posible que no pueda localizar la aplicación para el destino al que ha accedido el usuario. Esto puede ocurrir si la asignación de ubicación entre el destino y el recurso no aparece en la tabla del dominio de la aplicación.

- Asegúrese de que la aplicación TCP/UDP o HTTP esté configurada para el destino al que se accede.
- Asegúrese de que el usuario tenga una suscripción a la aplicación para el destino al que se ha accedido.

1. Vaya a la aplicación en el portal de administración.
2. Modifique la aplicación y vaya a la ficha **Suscripción**.
3. Asegúrese de que el usuario objetivo tenga una entrada en la lista de suscripciones.
4. Asegúrese de que la tabla del **dominio de la aplicación** tenga el destino y la ubicación de recursos adecuada.

No se pudo obtener la lista de destinos de aplicaciones configurada

Código de información: 0x001800D3

- Asegúrese de que esté configurada al menos una aplicación TCP/UDP/HTTP. Para obtener más información, consulte Agregar y administrar aplicaciones.
- Asegúrese de que la página de la tabla del dominio de la aplicación (**Secure Private Access > Configuración > Dominio de la aplicación**) no esté vacía o que no estén inhabilitadas todas las entradas. Los destinos configurados en la aplicación TCP/UDP/HTTP se agregan automáticamente a esta tabla. Se recomienda no eliminar ni inhabilitar los destinos o direcciones URL de la aplicación TCP/UDP/HTTP activa en la tabla de dominios de aplicación.

Problema de configuración de la aplicación

La configuración de la aplicación contiene un carácter especial o algún problema de configuración de directivas.

Código de información: 0x001800D9, 0x001800DA

Asegúrese de lo siguiente:

- La configuración de la aplicación no contiene caracteres no admitidos.
- La dirección IP de destino o el intervalo de direcciones IP o el CIDR IP son válidos.
- El destino de la aplicación se habilita en la tabla Dominio de la aplicación (**Secure Private Access > Configuración > Dominio de la aplicación**).
- Las directivas están configuradas y enlazadas a la aplicación correspondiente.
- La configuración de las directivas de acceso es correcta.

Problema con la ubicación del recurso

Código de información: 0x001800DB

- Asegúrese de que esté configurada una ubicación de recursos.
  1. En el menú desplegable de Citrix Cloud, seleccione **Ubicación de recursos**.
  2. Asegúrese de que la ubicación de recursos esperada esté configurada y que la ubicación del recurso esté activa.
- Asegúrese de seleccionar la ubicación de recursos correcta para el destino en la tabla del dominio de la aplicación (**Secure Private Access > Configuración > Dominio de la aplicación**).

Los destinos configurados en la aplicación TCP/UDP/HTTP se agregan automáticamente a esta tabla. Se recomienda no eliminar ni inhabilitar los destinos o las direcciones URL de la aplicación TCP/UDP/HTTP activa en la tabla de dominios de aplicación.

La directiva de seguridad mejorada está vinculada a la aplicación HTTP

Código de información: 0x001800DC, 0x001800DD, 0x13000006

Se accede a la aplicación HTTP que tiene una directiva de seguridad mejorada vinculada a través del cliente Citrix Secure Access.

- Asegúrese de que no se utilice el mismo destino para las aplicaciones TCP/UDP y HTTP.
- Si la directiva de seguridad mejorada está habilitada para la aplicación HTTP/HTTPS, se recomienda acceder a la aplicación solo a través de la aplicación Citrix Workspace o el servicio Citrix Remote Browser Isolation.
- Inhabilite el control de seguridad mejorado para que las aplicaciones HTTP/HTTPS accedan a la aplicación a través del cliente Citrix Secure Access.
  - Vaya al portal de administración de Secure Private Access.
  - Haga clic en la ficha **Aplicaciones** y busque el nombre de la directiva de la aplicación HTTP/HTTPS de destino a la que se ha accedido.
  - Haga clic en la ficha **Directivas de acceso** y busque el nombre de la directiva identificado anteriormente.
  - Seleccione la directiva y haga clic en **Modificar**.
  - Cambie la acción de **Permitir el acceso con restricciones** a **Permitir el acceso.**

Para obtener más información sobre la configuración, consulte Agregar y administrar aplicaciones.

> **Nota:**
>
> El servicio Citrix Remote Browser Isolation se conocía anteriormente como Secure Browser Service.

La longitud del nombre de host supera los 256 caracteres

Código de información: 0x001800EA

El nombre de host recibido en la solicitud de inicio de la aplicación supera los 256 caracteres.

Se recomienda que los caracteres del nombre FQDN no superen los 256 caracteres.

Dirección IP no válida

Código de información: 0x001800ED

La dirección IP recibida en la solicitud de lanzamiento de la aplicación no es válida.

Se recomienda acceder solo a una dirección IP privada válida de los clientes.

No se puede establecer una conexión de extremo a extremo

Código de información: 0x001800EF

No se puede establecer una conexión de extremo a extremo entre el cliente y el servidor configurado en la ubicación de recursos.

- Asegúrese de que la ubicación del recurso esté activa.
  - En el menú desplegable de Citrix Cloud, seleccione **Ubicación de recursos**.
  - Realice una comprobación del estado de los dispositivos Connector en la ubicación de recursos correspondiente.
  - Si esto no soluciona el problema, reinicie la máquina virtual del conector.
- Mantener un Connector Appliance de alta disponibilidad
  - En el menú desplegable de Citrix Cloud, seleccione **Ubicación de recursos**.
  - Asegúrese de que la ubicación del recurso tenga al menos dos dispositivos Connector.
- Asegúrese de lo siguiente:
  - La LAN de ubicación de recursos funciona correctamente.
  - No hay firewalls ni proxies en el centro que bloqueen a Connector Appliance en los servidores de servicio o back-end.
  - La red de clientes está en buen estado.
  - Los servidores privados de fondo están en buen estado.
  - Los servidores DNS están en buen estado.
  - Los FQDN se pueden resolver.

Si no hay ningún problema con estas opciones, haga lo siguiente:

1. Obtenga el ID de transacción de los registros de diagnóstico de este error.
2. Filtre todos los eventos que coincidan con el ID de la transacción en el panel del servicio Secure Private Access.
3. Compruebe los registros de diagnóstico correspondientes al ID de la transacción en el panel del servicio Secure Private Access y, a continuación, tome las medidas adecuadas en consecuencia.
4. Compruebe que se haya seleccionado una ubicación de recursos correcta como destino en la tabla del dominio de la aplicación (**Secure Private Access > Configuración > Dominio de la aplicación**).
5. Compruebe si la aplicación está configurada (**Secure Private Access > Aplicaciones**) con la dirección IP, el puerto y el FQDN correctos.

Si ninguno de estos pasos resuelve el problema, póngase en contacto con el soporte de Citrix con el código de error correspondiente al ID de la transacción y recopile los registros de los clientes.

Para recopilar los registros de depuración de los clientes, consulte Cómo recopilar los registros de los clientes.

IPv6 recibido en la solicitud de la aplicación

Código de información: 0x001800F5

Se recibe un IPv6 en la solicitud de aplicación que no es compatible. Actualmente, solo se admite IPv4.

Modifique la aplicación para solucionar el problema de la dirección IP de la aplicación.

1. Vaya al portal de administración de Secure Private Access.
2. Haga clic en la ficha **Aplicaciones**.
3. Busque la aplicación y haga clic en **Modificar**.

Para obtener más información, consulte Agregar y administrar aplicaciones.

No se pudo entregar el tráfico UDP

Código de información: 0x001800F9

El tráfico UDP no se pudo entregar porque se perdió la conexión del cliente

1. Compruebe si la sesión del cliente está activa.
2. Cierre sesión y, a continuación, vuelva a iniciar sesión.

Fallo en la entrega del tráfico de datos UDP

Código de información: 0x001800FF

- Busque el identificador de transacción para ver el código de error y filtre todos los eventos que coincidan con el ID de la transacción en el panel del servicio Secure Private Access.
- Compruebe si se ha producido algún error en el otro componente que coincida con el ID de la transacción. Si se encuentra un problema en otros componentes, tome las medidas apropiadas en consecuencia.
- Si esto no resuelve el problema, póngase en contacto con el servicio de asistencia de Citrix con el código de error y el ID de transacción correspondiente.

No se pudo iniciar la aplicación debido a problemas de conectividad de red

Código de información: 0x10000401

Error al iniciar la aplicación debido a problemas de conectividad de red entre Connector Appliance y el servicio Secure Private Access

1. Compruebe la conectividad pública a Internet del Connector Appliance.
2. Compruebe si alguna regla de proxy o firewall bloquea la conexión.
3. Si algún proxy está causando el problema, omita el proxy e intente iniciar la aplicación de nuevo.
4. Compruebe el estado del dispositivo Connector (**Citrix Cloud > Ubicación de recursos**).

Para obtener más información sobre la configuración de red, consulte Configuración de red del Connector Appliance.

Connector Appliance no pudo registrarse en el servicio Secure Private Access

Código de información: 0x10000402, 0x1000040C

1. Vaya a la página de administración de Connector Appliances y consulte el resumen del conector.
2. Si el estado del conector no es correcto, vaya a la ubicación de recursos en el portal de administración.
3. Realice una comprobación del estado de los dispositivos Connector en la ubicación de recursos correspondiente.
4. Si se produce un error en la comprobación de estado, reinicie la máquina virtual del conector.
5. Compruebe el resumen del conector y vuelva a ejecutar la comprobación de estado.

Para obtener más información sobre la configuración de red, consulte Configuración de red del Connector Appliance.

Problema de conectividad con el Connector Appliance

Código de información: 0x10000403, 0x10000404, 0x10000407, 0x1000040A, 0x1000040B, 0x1000040F, 0x10000410

- Busca el código de error en el ID de la transacción.
- Filtre todos los eventos que coincidan con el ID de la transacción en el panel de Secure Private Access.
- Compruebe si se ha producido algún error en el otro componente que coincida con el ID de la transacción, si lo encuentra, realice la solución alternativa correspondiente para hacer coincidir ese código de error.
- Si no se encuentra ningún error en otros componentes, haga lo siguiente:
  - Vaya a la página de administración de Connector Appliances.

  - Descargue el informe de diagnóstico. Para obtener más información, consulte Generar un informe de diagnóstico.
  - Capture el rastreo del paquete. Para obtener más información, consulte Verificar la conexión de red.

- Póngase en contacto con el soporte de Citrix para obtener este informe de diagnóstico y el rastreo de paquetes, junto con el código de error y el ID de transacción.

Problemas de conectividad con Connector Appliance y los servidores TCP/UDP privados de fondo

Código de información: 0x10000405, 0x10000408, 0x10000409, 0x1000040D, 0x1000040E, 0x10000412

El Connector Appliance tiene un problema de conectividad con los servidores TCP/UDP privados del fondo.

- Compruebe si el servidor de fondo al que el usuario final intenta conectarse está en funcionamiento y puede recibir las solicitudes.
- Compruebe la accesibilidad de los servidores back-end desde el interior de la red corporativa.
- Compruebe la configuración del proxy para ver si el conector está bloqueado y no puede llegar al servidor del back-end.
- Si solicita una aplicación basada en FQDN, compruebe la entrada DNS de la aplicación correspondiente en el servidor DNS.

Connector Appliance no resuelve el DNS de los FQDN

Código de información: 0x10000406

- Compruebe la entrada DNS del FQDN de la aplicación correspondiente en el servidor DNS.
- Asegúrese de que haya configurado un servidor DNS adecuado en los dispositivos Connector. Para obtener más información, consulte Configuración de los ajustes de red en la página de administración Connector Appliance.

Conexión al servidor privado finalizada

Código de información: 0x10000411

El cliente o el servicio Secure Private Access finalizan la conexión al servidor privado.

1. Compruebe si el usuario final ha cerrado la aplicación.

2. Compruebe otros registros de diagnóstico que coincidan con el ID de transacción de este registro y tome las medidas apropiadas en consecuencia.
3. Vuelva a iniciar la aplicación.
4. Si esto no resuelve el problema, póngase en contacto con el soporte de Citrix con el código de error y el ID de la transacción.

No se pudieron conectar ni enviar datos a la IP o FQDN del servicio privado

Código de información: 0x10000413

- Conexión al servidor privado finalizada
- [Problemas de conectividad con Connector Appliance y servidores TCP/UDP privados de back-end] (/en-us/citrix-secure-private-access/service/secure-private-access-troubleshooting). html#connectivity-issues-with-connector-appliance-and-backend-private-tcpudp-servers). Revise las entradas del dominio de redirección. Asegúrese de que las direcciones IP sean válidas y apunten al back-end correcto.

No hay condiciones de directiva coincidentes

Código de información: 0x100508

El contexto de usuario no coincide con las condiciones de la regla de acceso definidas en las directivas asignadas a la aplicación.

Actualice la configuración de la directiva para que coincida con el contexto del usuario.

No hay directiva de acceso asociada a la aplicación

Código de información: 0x100509

1. En la GUI del servicio Citrix Secure Private Access, haga clic en **Directivas de acceso en el panel** de navegación de la izquierda.
2. Asegúrese de que haya una directiva de acceso asociada a la aplicación correspondiente.
3. Si no hay una directiva de acceso asociada a la aplicación, cree una directiva de acceso para la aplicación. Para obtener más información, consulte Crear directivas de acceso.
4. Si esto no resuelve el problema, póngase en contacto con el soporte de Citrix.

No se encontró ninguna configuración de aplicación para el FQDN o la dirección IP

Código de información: 0x10050A

No se encontró ninguna aplicación coincidente para el FQDN entrante o la solicitud de dirección IP. Por lo tanto, la aplicación se clasifica como una aplicación inédita. Si esto no es lo esperado, haga lo siguiente.

1. Diríjase al portal de administración del servicio Secure Private Access.
2. Haga clic en **Aplicaciones** en el menú de navegación de la izquierda.
3. Busca la aplicación y haga clic en **Modificar**.
4. Agregue un FQDN o la dirección IP a la aplicación. Puede agregar el dominio exacto, la dirección IP o un dominio comodín.

   Nota: Agregar un FQDN o una dirección IP en **Secure Private Access > Configuración > Dominio de la aplicación** no resuelve este problema. Debe agregarse como parte de la configuración de la aplicación.

Información de enumeración de aplicaciones

Código de información: 0x10050C

Este código captura los resultados de la evaluación de directivas de varias aplicaciones a las que el usuario podría tener derecho. Es posible que se deniegue el acceso a la aplicación por los siguientes motivos:

- El contexto del usuario no coincide con las condiciones de la regla de acceso definidas en las directivas asignadas a la aplicación. Para obtener más información, consulte No hay condiciones de directiva coincidentes.
- No hay ninguna directiva de acceso asociada a la aplicación: para obtener más información, consulte No hay ninguna directiva de acceso asociada a la aplicación.
- Se configura una política asociada a la aplicación para denegar el acceso. En este caso, no es necesario realizar ninguna acción según lo previsto.
- Error interno inesperado al aplicar la directiva de acceso. Para obtener más información, póngase en contacto con el soporte de Citrix.

Error al iniciar la aplicación TCP/UDP porque falta una entrada de enrutamiento en la tabla de dominios de la aplicación

Código de información: 0x00180101

Este problema puede producirse si la configuración de la aplicación está presente pero falta la entrada de enrutamiento o se eliminó anteriormente.

Agregue una entrada de enrutamiento (**Secure Private Access > Configuración > Dominio de la aplicación**) para el destino al que se accede.

Error al iniciar la aplicación TCP/UDP porque los conectores no están en buen estado

Código de información: 0x00180102

Este problema puede producirse si ninguno de los conectores está activo o responde a la nueva conexión.

Realice una comprobación del estado de los dispositivos Connector en la ubicación de recursos correspondiente.

Error en la solicitud UDP/DNS porque no se puede acceder al conector

Código de información: 0x00180103

Este problema puede producirse si el tráfico UDP/DNS no puede llegar al conector.

Realice una comprobación del estado de los dispositivos Connector en la ubicación de recursos correspondiente.

No se pudo cargar la página porque la cookie NGS ha caducado

Código de información: 0x20580001

1. Reinicia el navegador e intenta abrir de nuevo la aplicación.
2. Si esto no resuelve el problema, póngase en contacto con el soporte de Citrix.

No se pudo recuperar la directiva de acceso debido a un error en la red

Código de información: 0x20580002

1. Compruebe la URL y la conexión de red.
2. Reinicia el navegador e intenta abrir de nuevo la aplicación.
3. Si esto no resuelve el problema, póngase en contacto con el soporte de Citrix.

Falló la búsqueda de la directiva de acceso al analizar el token web JSON

Código de información:0x20580003

1. Reinicia el navegador e intenta abrir de nuevo la aplicación.
2. Si esto no resuelve el problema, póngase en contacto con el soporte de Citrix.

Fallo de red al obtener los detalles de la directiva de acceso

Código de información:0x20580004

1. Compruebe si la directiva de acceso está habilitada.
2. Reinicia el navegador e intenta abrir de nuevo la aplicación.
3. Si esto no resuelve el problema, póngase en contacto con el soporte de Citrix.

No se pudo obtener la directiva al obtener el certificado público

Código de información: 0x20580005

1. Reinicia el navegador e intenta abrir de nuevo la aplicación.
2. Si esto no resuelve el problema, póngase en contacto con el soporte de Citrix.

No se pudo obtener la directiva al validar la firma del token web JSON

Código de información: 0x20580007

1. Comprueba si la hora de la red y la hora del dispositivo del usuario están sincronizadas.
2. Reinicia el navegador e intenta abrir de nuevo la aplicación.
3. Si esto no resuelve el problema, póngase en contacto con el soporte de Citrix.

Falló la búsqueda de directivas al validar el certificado público

Código de información: 0x20580008

1. Reinicia el navegador e intenta abrir de nuevo la aplicación.
2. Si esto no resuelve el problema, póngase en contacto con el soporte de Citrix.

No se pudo determinar el entorno del almacén para formar una URL de directiva

Código de información: 0x2058000A

1. Reinicia el navegador e intenta abrir de nuevo la aplicación.
2. Si esto no resuelve el problema, póngase en contacto con el soporte de Citrix.

No se pudo obtener una respuesta para la solicitud de recuperación de la directiva de acceso

Código de información: 0x2058000B

1. Reinicia el navegador e intenta abrir de nuevo la aplicación.
2. Si esto no resuelve el problema, póngase en contacto con el soporte de Citrix.

Falló la búsqueda de la directiva de acceso debido a un token de autenticación DS secundario caducado

Código de información: 0x2058000C

1. Reinicia el navegador e intenta abrir de nuevo la aplicación.
2. Si esto no resuelve el problema, póngase en contacto con el soporte de Citrix.

Connector Appliance no está registrado

Código de información: 0x10200002

Compruebe el registro del Connector Appliance.

Para obtener más información, consulte Registrar el dispositivo Connector en Citrix Cloud.

No se puede conectar al Connector Appliance

Código de información: 0x10200003

El Connector Appliance no puede comunicarse entre Citrix Cloud y las ubicaciones de recursos.

Compruebe el registro del conector.

Para obtener más información, consulte Registrar el dispositivo Connector en Citrix Cloud.

Falló la conexión al servicio Citrix Secure Private Access

Código de información: 0x10000301

Compruebe la configuración de red de Connector Appliance. Para obtener más información, consulte Configuración de red de su Connector Appliance.

No se puede acceder al servidor proxy

Código de información: 0x10000303, 0x10000304

Compruebe la configuración del servidor proxy y asegúrese de que Connector Appliance pueda acceder a él. Para obtener más información, consulte Registrar el dispositivo Connector en Citrix Cloud.

Fallo en la autenticación del servidor proxy

Código de información: 0x10000305

Compruebe las credenciales del servidor proxy y asegúrese de que están configuradas correctamente en Connector Appliance. Para obtener más información, consulte Después de registrar su Connector Appliance.

No se puede acceder a los servidores proxy configurados

Código de información: 0x10000306

Compruebe la configuración de red de Connector Appliance, la configuración del firewall o la configuración del servidor proxy. Para obtener más información, consulte los siguientes temas:

- Parámetros de red de Connector Appliance
- Registrar el Connector Appliance en Citrix Cloud
- Comunicación de Connector Appliance

Se recibió una respuesta de error del servidor back-end

Código de información: 0x10000307

Compruebe el código de estado HTTP del servidor web de fondo, si no es un código esperado.

No se puede enviar la solicitud a la URL de destino

Código de información: 0x10000005

Compruebe la URL de destino o compruebe la configuración de red de Connector Appliance. Para obtener más información, consulte Configuración de red de su Connector Appliance.

No se pudo procesar el SSO

Código de información: 0x10000107

No se pudieron recuperar los datos de configuración de la aplicación de Citrix Cloud.

Compruebe la configuración de red de Connector Appliance y asegúrese de que el servidor NTP esté configurado y de que no haya problemas con la franja horaria. Para obtener más información, consulte Configuración de red de su Connector Appliance.

Falló la conexión al servicio Citrix Secure Private Access

Código de información: 0x10000108, 0x1000010B

Compruebe la configuración de red de Connector Appliance. Para obtener más información, consulte Configuración de red de su Connector Appliance.

No se pudo procesar el SSO, no se pudo determinar la configuración del SSO

Código de información: 0x1000010A

Compruebe la configuración del SSO y asegúrese de que Connector Appliance pueda acceder al servidor.

Falló el SSO de FormFill, configuración incorrecta de la aplicación de formulario

Código de información: 0x10000101, 0x10000102, 0x10000103, 0x10000104

Comprueba la configuración de la aplicación del formulario SSO y asegúrate de que los campos de nombre de usuario, contraseña, acción y URL de inicio de sesión estén correctamente configurados en los ajustes de la aplicación.

Falló el SSO de Kerberos

Código de información: 0x10000202

Compruebe la configuración del SSO de Kerberos en el servidor back-end y en el controlador de dominio. Compruebe también la configuración de autenticación NTLM alternativa.

Para ver la configuración de SSO de Kerberos, consulte Validaciónde la configuración de Kerberos.

No se pudo procesar el inicio de sesión único para el tipo de autenticación

Código de información: 0x10000203

Compruebe la configuración de SSO en el servicio Secure Private Access y en el servidor back-end. Para el servicio Secure Private Access, consulte Establecer el método de inicio de sesión preferido.

El SSO de Kerberos falló pero se recurrió a NTLM

Código de información: 0x10000204

No se pudo recuperar el vale de Kerberos del controlador de dominio. Como autenticación secundaria, Connector Appliance ha probado la autenticación NTLM alternativa.

Para habilitar la autenticación Kerberos correcta, compruebe la configuración del SSO de Kerberos en el servidor back-end y el controlador de dominio.

Para obtener más información, consulte Validación de la configuración de Kerberos.

Cómo recopilar registros de clientes

- **Cliente Windows:**
  1. Abre la aplicación y asegúrate de que el registro esté activado.
  2. Ahora conéctese al servicio Secure Private Access y duplique el problema al que se enfrenta.
  3. En la aplicación, vaya a **Registro** y haga clic en **Recopilar archivos de registro**. Esto genera el archivo de registro.
  4. Guarde el archivo de registro en el escritorio del equipo cliente.
- **Cliente Mac:**
  1. Abra la aplicación y ve a **Registros > Detallados**.
  2. Borre los registros y proceda a reproducir el problema.
  3. Vuelva a **Registros > Exportar registros**. Esto crea un archivo zip que contiene archivos de registro.

Respuestas a las preguntas frecuentes

¿Qué son los registros de diagnóstico de Secure Private Access?

Los registros de diagnóstico de Secure Private Access capturan todos los eventos que se producen cuando un usuario accede a cualquier aplicación (Web/SaaS/TCP/UDP). Estos registros capturan la

postura del dispositivo, la autenticación de la aplicación, la enumeración de aplicaciones y los registros de acceso a las aplicaciones.

¿Dónde puedo encontrar los registros de Secure Private Access?

1. Inicie sesión en Citrix Cloud.
2. En el icono del servicio Secure Private Access, haga clic en **Administrar** .
3. Haga clic en el **panel** de navegación de la izquierda de la interfaz de usuario de administración.
4. En el gráfico **de registros de diagnóstico**, haga clic en el enlace **Ver más**.

¿Qué detalles puedo encontrar en los registros de diagnóstico de Secure Private Access?

El panel de registros de usuarios de Secure Private Access proporciona los siguientes detalles de forma predeterminada.

- **Marca horaria**: Hora del evento en UTC.
- **Nombre de usuario**: Nombre de usuario del usuario final que accede a la aplicación.
- **Nombre de la aplicación**: Nombre de la aplicación o aplicaciones a las que se accedió.
- **Información de la directiva**: Muestra el nombre de la directiva o directivas de acceso que se activaron durante el evento.
- **Estado**: Muestra el estado del evento, el éxito o el error.
- **Código de información**: Consulte más información sobre el código de información.
- **Descripción**: Muestra el motivo del error o más detalles sobre el evento.
- **FQDN de la aplicación**: FQDN de la aplicación a la que se accedió
- **Tipo de evento**: Muestra el tipo de evento asociado a la operación realizada.
- **Tipo de operación**: Muestra la operación para la que se generó el registro.
- **Categoría**: Hay tres categorías disponibles según el tipo de evento. Es decir, la autenticación de aplicaciones, la enumeración de aplicaciones o el acceso a aplicaciones. Estas opciones también están disponibles como opciones de filtro. Puede utilizar estas opciones para filtrar los

registros según el tipo de problema al que se enfrente.

- **ID de transacción**: Aprenda a usar un identificador de transacción
  Puede obtener los siguientes detalles haciendo clic en el botón + situado en el extremo derecho del panel de control:
- **Ubicación PoP de SPA**: Muestra el nombre/ID de la ubicación PoP del servicio de Secure Private Access que se utilizó durante el acceso a la aplicación. Consulte las ubicaciones de PoP de Secure Private Access

¿Qué eventos se capturan en los registros de diagnóstico de Secure Private Access?

Los registros de diagnóstico de Secure Private Access capturan los siguientes eventos:

- **Postura del dispositivo:** Estado del dispositivo del usuario final. Estos registros capturan información sobre los resultados de la postura del dispositivo. Si el dispositivo se consideró compatible, no compatible o denegado el acceso según la directiva de postura del dispositivo.
- Inicio**o cierre de sesión: eventos relacionados**con el estado de inicio o cierre de sesión del usuario final en el cliente Citrix Secure Access y la autenticación en el espacio de trabajo (proveedores internos o externos).
- **Enumeración de aplicaciones**: en el servicio Secure Private Access, las políticas de acceso configuradas por los administradores deciden qué usuario puede acceder a qué aplicación. Las aplicaciones denegadas no son visibles (no se enumeran) para los usuarios finales de la aplicación Citrix Workspace. Estos eventos ayudan a saber a qué aplicaciones se les permitió o denegó el acceso a un usuario en función de las políticas de acceso configuradas en el servicio Secure Private Access.
- **Acceso a la aplicación**: eventos de acceso a aplicaciones o puntos finales del usuario final, estado de permisión/denegación, estado de inicio de sesión único y estado de conectividad según las directivas de acceso configuradas para el intervalo de tiempo seleccionado.

¿Cómo utilizo el tema de solución de problemas de Secure Private Access para resolver un error que he detectado?

1. Obtenga el código de información del error que intenta resolver.
2. Busca el código de información en la tabla de búsqueda de errores.
3. Siga los pasos de resolución proporcionados para ese código de información.

¿Qué es un código de información? ¿Dónde puedo encontrarlos?

Algunos eventos de registro, como los errores, tienen un código de información asociado. Busque este código de información en la tabla de búsqueda de errores para encontrar los pasos de resolución o más información sobre ese evento.

¿Qué es un identificador de transacción? ¿Cómo lo uso?

El ID de transacción correlaciona todos los registros de Secure Private Access de una solicitud de acceso. Una solicitud de acceso a una aplicación puede generar varios registros, empezando por la autenticación, luego por la enumeración de aplicaciones dentro de la aplicación del espacio de trabajo y, por último, por el acceso a la aplicación en sí. Todos estos eventos generan sus propios registros. El ID de transacción se utiliza para correlacionar todos estos registros. Puede filtrar los registros de diagnóstico mediante el ID de transacción para encontrar todos los registros relacionados con una solicitud de acceso a una aplicación concreta.

¿Cuáles son todas las ubicaciones PoP de Secure Private Access?

La siguiente es la lista de ubicaciones de PoP de Secure Private Access.

Nombre de PoP	Zona	Region
az-us-e	Azure eastus	Virginia
az-us-w	Azure westus	California
az-us-sc	Azure southcentralus	Texas
az-aus-e	Azure australiaeast	Nueva Gales del Sur
az-eu-n	Azure northeurope	Irlanda
az-eu-w	Azure westeurope	Países Bajos
az-jp-e	Azure japaneast	Tokio, Saitama
az-bz-s	Azure brazilsouth	Estado de Sao Paulo
az-asia-se	Azure southeastasia	Singapur
az-uae-n	Azure uaenorth	Dubái
az-in-s	Azure southindia	Chenái
az-asia-hk	Azure eastasia	Hong Kong

¿Qué hago si no puedo resolver mi error mediante el código de información y la tabla de búsqueda de errores?

Póngase en contacto con Citrix Support.

Referencias

- **Agregar una aplicación web**
  - Support for Enterprise web apps
  - Configurar el acceso directo a las aplicaciones web
- **Agregar una aplicación SaaS**
  - Soporte para la aplicación Software as a Service
  - Configuración específica del servidor de aplicaciones SaaS
- **Configurar aplicaciones cliente-servidor**
  - Compatibilidad con aplicaciones cliente-servidor
- **Crear directivas de acceso**
  - Crear directivas de acceso
- **Tablas de rutas**
  - Tablas de rutas