Citrix Secure Private Access

Machine translated content

Disclaimer

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

Contents

Citrix Secure Private Access

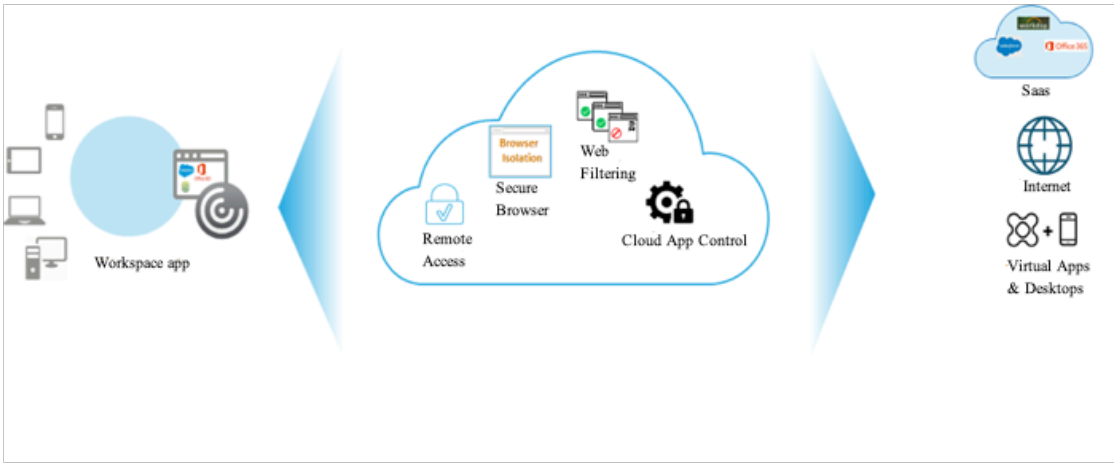
October 21, 2024

El servicio Citrix Secure Private Access permite a los administradores brindar una experiencia cohesiva que integra inicio de sesión único, acceso remoto e inspección de contenido en una única solución para el control de acceso de extremo a extremo. Los administradores de TI pueden controlar el acceso a aplicaciones SaaS aprobadas con una experiencia de inicio de sesión único simplificada. Con el servicio Citrix Secure Private Access, los administradores también pueden proteger la red de la organización y los dispositivos de los usuarios finales contra malware y fugas de datos al filtrar el acceso a sitios web específicos y categorías de sitios web. Los administradores pueden aplicar políticas de seguridad de acceso mejoradas para un acceso seguro a las aplicaciones SaaS. Una vez autenticados, los empleados tienen acceso a todas las aplicaciones comerciales críticas desde cualquier dispositivo, independientemente de si están en las instalaciones de la oficina, en casa o viajando.

Los administradores pueden monitorear las actividades de los usuarios, como los sitios web maliciosos, peligrosos o desconocidos visitados, el ancho de banda consumido y los comportamientos de carga y descarga riesgosos. Al utilizar el análisis de los sitios web y las categorías de sitios web a los que se accede, los administradores pueden tomar medidas correctivas para proteger la red empresarial. Al mismo tiempo, el servicio proporciona a los usuarios finales acceso seguro y sin inconvenientes a todas sus aplicaciones alojadas.

Los administradores también pueden restringir acciones, como impresión restringida, descargas y acceso al portapapeles (copiar y pegar).

El siguiente diagrama es una representación visual del servicio de acceso privado seguro.



Capacidades clave de Citrix Secure Private Access

A continuación se presentan algunas de las tareas clave que puede realizar con el servicio Citrix Secure Private Access:

- **Publicar aplicaciones SaaS con acceso de inicio de sesión único** - Una vez que el usuario está autenticado en Citrix Workspace con una identidad principal, los desafíos de autenticación posteriores a SaaS y aplicaciones web se cumplen automáticamente mediante la función de inicio de sesión único en Citrix Cloud mediante aserciones SAML.

De forma predeterminada, la afirmación SAML utiliza la dirección de correo electrónico asociada con la cuenta de Active Directory del usuario (proveedor de identidad) con la dirección de correo electrónico asociada con la cuenta de aplicación web o SaaS del usuario (proveedor de servicios).

- **Establecer políticas de seguridad mejoradas para aplicaciones SaaS. (Por ejemplo, marca de agua, restricción de copiar y pegar, y evitar descargas).** - Para proteger el contenido, las organizaciones incorporan políticas de seguridad mejoradas dentro de las aplicaciones SaaS. Cada política aplica una restricción en el navegador Citrix Enterprise cuando se usa la aplicación Workspace para escritorio o en el navegador seguro cuando se usa la aplicación Workspace web o móvil.
  - Navegador preferido: deshabilita el uso del navegador local y se basa en el motor del navegador Citrix Enterprise (aplicación Workspace, escritorio) o en el navegador seguro (aplicación Workspace, dispositivo móvil y web).

  - Restringir el acceso al portapapeles: deshabilita las operaciones de cortar/copiar/pegar entre la aplicación y el portapapeles del punto final.
  - Restringir impresión: deshabilita la capacidad de imprimir desde el navegador de la aplicación.
  - Restringir descargas: deshabilita la capacidad del usuario para descargar desde dentro de la aplicación SaaS.
  - Mostrar marca de agua: superpone una marca de agua en la pantalla que muestra el nombre de usuario y la dirección IP del punto final. Si un usuario intenta imprimir o tomar una captura de pantalla, la marca de agua aparece tal como se muestra en la pantalla.

- **Proporcionar acceso contextual** - Aunque una aplicación SaaS autorizada se considera segura, el contenido de la aplicación SaaS en realidad puede ser peligroso y constituir un riesgo de seguridad. Cuando un usuario hace clic en un hipervínculo dentro de una aplicación SaaS, el tráfico se dirige a través de la función de filtrado web, que proporciona una evaluación de riesgos para el hipervínculo. En función de la evaluación de riesgos del hipervínculo y la lista personalizada de categorías de URL, la función de filtrado web permite, rechaza o redirige la solicitud de hipervínculo del usuario de la siguiente manera:

  - Aprobado: el hipervínculo se considera seguro y el navegador Citrix Enterprise que accede dentro de la aplicación Workspace accede al hipervínculo.
  - Denegado: el hipervínculo se considera peligroso y se deniega el acceso.
  - Redirigido: la solicitud de hipervínculo se redirige al servicio de navegador seguro, donde las actividades de navegación en Internet del usuario están aisladas del dispositivo terminal, la red corporativa y la aplicación SaaS.

- **Análisis de seguridad y rendimiento** - Los usuarios acceden invariablemente a aplicaciones SaaS que tienen una seguridad mejorada inherente a ellas. La aplicación Workspace, el servicio Secure Private Access y el servicio Secure Browser proporcionan al servicio de análisis de seguridad información sobre los siguientes comportamientos de usuarios y aplicaciones. Estos análisis afectan la puntuación de riesgo general del usuario:

  - Hora de lanzamiento de la aplicación
  - Hora de finalización de la aplicación
  - Acción de impresión
  - Acceso al portapapeles
  - Acceso URL
  - Carga de datos
  - Descarga de datos

- **Filtrado web:** La función de filtrado web evalúa el riesgo de cada hipervínculo seleccionado dentro de la aplicación SaaS. Acceder a estos sitios y monitorear los cambios en el comportamiento del usuario aumenta el puntaje de riesgo general del usuario porque indica que el

dispositivo terminal está comprometido y comenzó a infectar o cifrar datos o que el usuario y el dispositivo están robando propiedad intelectual.

- **Integración con información de seguridad y gestión de eventos (SIEM)** - Los registros de acceso privado seguro se pueden exportar a través de Kafka a SIEM como Splunk, Sentinel y Elastic. La exportación de registros a SIEM mejora las capacidades de seguridad y mejora la eficacia de la respuesta a incidentes. Para obtener más detalles, consulte Eventos de acceso privado seguro.

Novedades

October 21, 2024

23 de septiembre de 2024

- **Compatibilidad con enrutamiento de aplicaciones basado en contexto y selección de ubicaciones de recursos**

  La configuración de enrutamiento de dominio dinámico en la política de acceso ahora permite a los administradores editar el tipo de enrutamiento interno por URL según el contexto del usuario. Los administradores pueden modificar las ubicaciones de los recursos para que las solicitudes de los usuarios se dirijan al centro de datos óptimo, lo que garantiza que las solicitudes de los usuarios se gestionen de manera eficiente y se optimice el rendimiento. Para obtener más detalles, consulte Enrutamiento de aplicaciones basado en contexto y selección de ubicaciones de recursos.

15 de agosto de 2024

- **Opción para configurar una duración de tiempo para purgar las entradas en la lista de usuarios bloqueados**

  Los administradores ahora pueden establecer una duración específica (de 1 a 99 días) para purgar las entradas en la lista de usuarios bloqueados. Para obtener más detalles, consulte Terminar sesiones de usuarios activos y agregar usuarios a la lista de bloqueo de usuarios.

- **Controles de seguridad adicionales**

  Los siguientes controles de seguridad adicionales ahora están disponibles para restringir el acceso a la aplicación.

  - Micrófono

  - Cámara web
  - Notificaciones
  - Ventanas emergentes
  - Contenido inseguro

  Para obtener más detalles, consulte Opciones de restricción de acceso.

- **Mejoras en la función de filtrado web de sitios web no autorizados**

  La función de sitios web no autorizados (filtrado web) permite a los administradores bloquear el acceso a todo el tráfico no autorizado de forma predeterminada o permitirlo de forma predeterminada a través de Citrix Enterprise Browser. Para obtener más detalles, consulte Sitios web no autorizados.

16 de julio de 2024

- **Controles de seguridad adicionales**

  Los siguientes controles de seguridad adicionales están disponibles para restringir el acceso a la aplicación.

  - Restricción de descarga por tipo de archivo
  - Restricción de carga por tipo de archivo
  - Enmascaramiento de datos personales
  - Administración de la impresora
  - Restricción del portapapeles para grupos de seguridad

  Para obtener más detalles, consulte Opciones de restricción de acceso.

- **Visualización de dominios integrados en la página de descubrimiento de aplicaciones**

  La función de descubrimiento de aplicaciones permite a los administradores crear nuevas aplicaciones o agregar esos dominios a una aplicación existente si un dominio principal o un dominio integrado (HTTP/HTTPS) o la dirección IP de destino (TCP/UDP) no está asociado con una aplicación. La página de descubrimiento de aplicaciones ** muestra tanto el dominio principal como sus dominios integrados subyacentes en una estructura de árbol. Para obtener más detalles, consulte Descubrir dominios o direcciones IP a los que acceden los usuarios finales.

11 de junio de 2024

- **Herramienta de modelado de políticas**

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

- **Compatibilidad con filtros en el gráfico de registros de diagnóstico**

  La opción de filtro en el gráfico **Registros de diagnóstico** ayuda a los administradores a refinar la búsqueda en función de diversos criterios, como el tipo de aplicación, la categoría y la descripción, para facilitar el análisis de registros y la resolución de problemas. Para obtener más detalles, consulte Registros de diagnóstico.

13 de marzo de 2024

- **Soporte para finalizar sesiones de usuarios activos y agregar usuarios a la lista de usuarios deshabilitados**

  Los administradores ahora pueden finalizar inmediatamente todas las sesiones de usuarios finales activos y agregarlos a la lista de usuarios deshabilitados. Agregar un usuario a esta lista de usuarios deshabilitados finaliza todas las sesiones activas de la aplicación Secure Private Access y bloquea el acceso futuro a la aplicación. Para obtener más detalles, consulte Terminar sesiones de usuarios activos y agregar usuarios a la lista de usuarios deshabilitados.

12 de febrero de 2024

- **Disponibilidad general del navegador y análisis antivirus**

  Los análisis del navegador y del antivirus compatibles con el servicio Device Posture ahora están disponibles de forma general. Para obtener más detalles, consulte Escaneos compatibles con la postura del dispositivo.

23 de enero de 2024

- **Disponibilidad general de la verificación del certificado del dispositivo con el servicio Device Posture**

  La verificación del certificado del dispositivo con el servicio Device Posture ahora está disponible de forma general. Para obtener más detalles, consulte Verificación del certificado del dispositivo con el servicio de postura del dispositivo.

20 de diciembre de 2023

- **Disponibilidad general de Secure Private Access en las instalaciones**

  Citrix Secure Private Access para instalaciones locales ya está disponible de forma general. Para obtener más detalles, consulte Novedades.

16 de octubre de 2023

- **Funciones de vista previa de la solución local de acceso privado seguro**

  La solución local Secure Private Access ahora ofrece lo siguiente:

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

  Para obtener más detalles, consulte Acceso privado seguro para instalaciones locales.

- **Funciones de vista previa del servicio de postura del dispositivo**

  El servicio de postura del dispositivo ahora admite las siguientes comprobaciones:

  - El servicio de postura del dispositivo ahora es compatible con las plataformas IGEL.
  - El servicio de postura del dispositivo ahora admite comprobaciones de geolocalización y ubicación de red.

  Para obtener más información, consulte Device Posture.

11 de septiembre de 2023

- **Disponibilidad general de la integración de Device Posture con Microsoft Intune**

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

30 de agosto de 2023

- **Administrar el servicio Citrix Endpoint Analysis Client para la postura del dispositivo**

  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 utiliza con NetScaler y Device Posture. Para obtener más detalles, consulte Administrar el cliente de análisis de puntos finales de Citrix para el servicio de postura del dispositivo.

28 de agosto de 2023

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

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

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 puede habilitar el acceso contextual (Smart Access) a los recursos de Citrix DaaS y Secure Private Access al comparar el certificado del dispositivo final con una autoridad de certificación corporativa para determinar si se puede confiar en el dispositivo final. Para obtener más detalles, consulte Verificación del certificado del dispositivo con el servicio de postura del dispositivo.

  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 de postura del dispositivo y los registros de monitoreo ahora se pueden buscar en DaaS Monitor. Para obtener más detalles, consulte Eventos de postura del dispositivo en Citrix DaaS Monitor.

07 de junio de 2023

- **Herramienta para configurar el acceso privado seguro para instalaciones locales**

  Ahora está disponible una interfaz de usuario simplificada para configurar el acceso privado seguro para la solución local. La herramienta de configuración se puede ejecutar en un controlador de entrega de Citrix Virtual Apps and Desktops para crear una aplicación SaaS o web rápidamente. Además, puede utilizar esta herramienta para establecer restricciones de aplicaciones, enrutamiento de tráfico y configuraciones de NetScaler Gateway. Para obtener más detalles, consulte /es-us/citrix-secure-private-access/service/secure-private-access-for-on-premises-config-tool.html.

29 May 2023

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

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

[SPA-746]

10 de abril de 2023

- **Descubrimiento de aplicaciones**

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

  [ACS-2325]

29 de marzo de 2023

- **Solución de acceso privado seguro para implementaciones locales**

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

  [SPAOP-1]

07 de marzo de 2023

- **Configurar sufijos DNS**

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

  - Habilite el cliente Citrix Secure Access para resolver un nombre de dominio no completamente calificado (nombre de host) en un nombre de dominio completamente calificado (FQDN) agregando el sufijo DNS domain para los servidores back-end.
  - Permitir que los administradores configuren aplicaciones usando direcciones IP (CIDR de IP/rango de IP), de modo que los usuarios finales puedan acceder a las aplicaciones usando el FQDN correspondiente bajo el dominio de sufijo DNS.

  Para obtener más detalles, consulte Sufijos DNS para resolver 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 aplicar ciertos requisitos que los dispositivos finales deben cumplir para obtener acceso a los recursos de Citrix DaaS (aplicaciones y escritorios virtuales) o Citrix Secure Private Access (SaaS, aplicaciones web, TCP y aplicaciones 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, este servicio también se puede integrar con otras soluciones de terceros. Device Posture está integrado con Microsoft Endpoint Manager (MEM) en Windows y macOS. Para obtener más detalles, consulte Integración de Microsoft Endpoint Manager con Device Posture.

  [ACS-1399]

22 de diciembre de 2022

- **Compatibilidad con inicio de sesión único para la URL del espacio de trabajo para usuarios que iniciaron sesión a través de la aplicación Citrix Workspace**

  El cliente Citrix Secure Access ahora admite el inicio de sesión único para la URL del espacio de trabajo cuando ya ha iniciado sesión a través de la aplicación Citrix Workspace. Esta funcionalidad SSO mejora la experiencia del usuario al evitar múltiples autenticaciones. Para obtener más detalles, consulte Compatibilidad de inicio de sesión único para la URL del espacio de trabajo.

  [ACS-1888]

- **Habilitar el acceso a aplicaciones mediante políticas de acceso**

  Para otorgar acceso a las aplicaciones a los usuarios, ahora los administradores deben crear políticas de acceso con una lista de suscripciones de usuarios correspondiente para que las aplicaciones estén disponibles para los usuarios finales. Anteriormente, los administradores tenían que agregar usuarios como suscriptores para habilitar el acceso. Para obtener más detalles, consulte Crear políticas de acceso.

  [ACS-3018]

03 de octubre de 2022

- **Políticas de acceso para otorgar acceso a las aplicaciones**

  La opción de configuración Suscriptores de la aplicación se elimina de la sección Aplicaciones en el asistente de configuración. Para otorgar acceso a las aplicaciones a los usuarios, los administradores deben crear políticas de acceso. En las políticas de acceso, los administradores agregan suscriptores de aplicaciones y configuran controles de seguridad. Para obtener más detalles, consulte Crear políticas de acceso.

  [ACS-3018]

- **Compatibilidad con aplicaciones UDP**

  El servicio de acceso privado seguro ahora admite el acceso a aplicaciones UDP. Para obtener más detalles, consulte Funciones de vista previa.

  [ACS-1430]

09 de septiembre de 2022

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

  Los administradores ahora pueden configurar una política de acceso adaptable con el puntaje de riesgo del usuario proporcionado por Citrix Analytics for Security (CAS). Para obtener más detalles, consulte Acceso adaptativo basado en la puntuación de riesgo del usuario.

  [ACS-877]

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

  Los administradores ahora pueden configurar la política de acceso adaptable según la ubicación desde donde el usuario accede a la aplicación. La ubicación puede ser el país desde donde el usuario accede a la aplicación o la ubicación de la red del usuario. Para obtener más detalles, consulte Acceso adaptativo basado en la ubicación.

  [ACS-99]

- **Generador de políticas de acceso adaptativo mejorado**

  El acceso a las aplicaciones ahora está habilitado solo 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 políticas de acceso para proporcionar acceso a las aplicaciones además de la suscripción a la aplicación. Además, los usuarios o grupos es una condición obligatoria en las políticas de acceso que se deben cumplir para acceder a las aplicaciones. Para obtener más detalles, consulte Crear políticas de acceso.

  [ACS-1850]

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

  Esta función permite a los administradores de clientes controlar (permitir o restringir) quién puede cargar archivos en sus aplicaciones críticas para el negocio. Con esto, sólo los usuarios autorizados podrán cargar archivos en las aplicaciones. Para obtener más detalles, consulte Crear políticas de acceso.

  [ACS-655]

- **Panel de control mejorado**

  El panel de acceso privado seguro ahora proporciona visibilidad detallada de varias métricas de usuario, como uso de aplicaciones, principales usuarios de aplicaciones, principales aplicaciones a las que se accedió, registros de diagnóstico, etc. Para obtener más detalles, consulte Panel de control.

  [ACS-2480]

- **Desuso de la biblioteca**

  Las aplicaciones de acceso privado seguro ahora no están visibles dentro de Citrix Cloud Library. Todas las aplicaciones configuradas de Secure Private Access están dentro de la sección de aplicaciones dentro del mosaico de servicio Secure Private Access. Esto ayuda a los administradores a navegar, editar y configurar las aplicaciones fácilmente.

  [ACS-1546]

- **Registros de auditoría para acceso privado seguro**

  Los eventos relacionados con el servicio Citrix Secure Private Access ahora se capturan en el registro del sistema **Citrix Cloud > .** Para obtener más detalles, 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 y descargar los eventos. Se puede acceder a estos eventos a través de un script de PowerShell. Para obtener más detalles, consulte Registros de diagnóstico para el acceso a aplicaciones SaaS y web empresariales.

  [ACS-805]

- **Guía de solución de problemas**

  Los administradores pueden utilizar la guía de solución de problemas para resolver problemas relacionados con la configuración. Para obtener más detalles, consulte Solucionar problemas relacionados con las aplicaciones.

  [ACS-2719]

15 de julio de 2022

- **Habilitar el acceso a una aplicación solo si se configura una política de acceso**

  El acceso a las aplicaciones ahora está habilitado solo después de que el administrador agrega una política de acceso además de la suscripción a la aplicación. La suscripción a la aplicación por sí sola no permite el acceso a las aplicaciones. Con este cambio, los administradores pueden implementar seguridad adaptativa en función del contexto, como usuarios, ubicación, dispositivo y riesgo. Los administradores deben migrar los controles de seguridad de la aplicación y las políticas de acceso existentes al nuevo marco de políticas de acceso. Para obtener más detalles, consulte Migración de controles de seguridad de aplicaciones y políticas de acceso.

  [ACS-1850]

01 de junio de 2022

- **Servicio de autenticación adaptable**

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

  [CGS-6510]

04 de abril de 2022

- **Cambios de cambio de marca**

  El servicio Citrix Secure Workspace Access ahora se denomina servicio Citrix Secure Private Access.

  [ACS-2322]

- **Flujo de trabajo guiado por el administrador para una fácil incorporación y configuración**

  Secure Private Access ahora tiene una nueva experiencia administrativa optimizada con un proceso paso a paso para configurar el acceso a la red Zero Trust para aplicaciones SaaS, aplicaciones web internas y aplicaciones TCP. Incluye configuración de autenticación adaptativa, aplicaciones que incluyen suscripción de usuarios, políticas de acceso adaptativas y otras dentro de una única consola de administración. Para obtener más detalles, consulte Flujo de trabajo guiado por el administrador para una fácil incorporación y configuración.

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

  [ACS-1102]

- **Panel de acceso privado seguro**

  El panel de acceso privado seguro brinda a los administradores visibilidad completa de sus principales aplicaciones, principales usuarios, estado de los conectores, uso del ancho de banda y todo en un solo lugar para el consumo. Estos datos se obtienen de Citrix Analytics. Para obtener más detalles, consulte el panel de acceso privado seguro .

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

  [ACS-1169]

- **Acceso directo a aplicaciones web empresariales**

  Los clientes ahora pueden habilitar el acceso a la red de confianza cero (ZTNA) para aplicaciones web internas, directamente desde navegadores web nativos como Chrome, Firefox, Safari y Microsoft Edge. Para obtener más detalles, consulte Acceso directo a aplicaciones web empresariales.

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

- **Acceso basado en agente ZTNA a aplicaciones TCP/HTTPS**

  Los clientes de Citrix ahora pueden habilitar Zero Trust Network Access (ZTNA) para todas las aplicaciones cliente-servidor y recursos basados en IP/puerto, además de las aplicaciones web internas. Para obtener más detalles, consulte Compatibilidad con aplicaciones cliente-servidor.

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

  [ACS-970]

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

  La función de acceso adaptativo del servicio Citrix Secure Private Access ofrece un enfoque integral de acceso a la red de confianza cero (ZTNA) que brinda acceso seguro a las aplicaciones. El acceso adaptable permite a los administradores proporcionar un acceso a 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 la postura del dispositivo)
  - Riesgo (puntuación de riesgo del usuario)

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

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

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

- **Registros de auditoría para acceso privado seguro**

  Los eventos relacionados con el servicio Citrix Secure Private Access ahora se capturan en el registro del sistema **Citrix Cloud > .** Para obtener más detalles, 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 y descargar los eventos. Se puede acceder a estos eventos a través de un script de PowerShell. Para obtener más detalles, consulte Registros de diagnóstico para el acceso a aplicaciones SaaS y web empresariales.

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

  [ACS-805]

- **Servicio de autenticación adaptativa**

  Los clientes de Citrix Cloud ahora pueden usar Citrix Workspace para proporcionar autenticación adaptativa a Citrix Virtual Apps y 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 adaptativa es un ADC administrado por Citrix y alojado en Citrix Cloud. Para obtener más detalles, consulte Servicio de autenticación adaptativa.

  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 dentro de Citrix Secure Private Access, ahora puede eliminar la dependencia de una solución VPN tradicional para brindar acceso a todas las aplicaciones privadas para usuarios remotos.

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

  [ACS-870]

11 de octubre de 2021

- **Fusión del mosaico de servicios de Citrix Gateway en un único acceso privado seguro en Citrix Cloud**

  El mosaico de servicio Citrix Gateway ahora está fusionado en un único acceso privado seguro en Citrix Cloud.

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

  [NGSWS-16761]

30 de julio de 2021

- **Controles de seguridad y acceso contextuales para aplicaciones web y SaaS empresariales según la ubicación geográfica del usuario**

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

  [ACS-833]

- **Opción para ocultar una aplicación web o SaaS específica del portal de 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, el servicio Citrix Gateway no devuelve esta aplicación durante la enumeración. Sin embargo, los usuarios aún pueden acceder a la aplicación oculta.

  [ACS-944]

09 de junio de 2021

- **Tabla de rutas para definir las reglas para enrutar el tráfico de la aplicación**

Los administradores ahora pueden usar la tabla de rutas para definir las reglas para enrutar el tráfico de la aplicación directamente a Internet o a través de Citrix Gateway Connector. Los administradores pueden definir el tipo de ruta para las aplicaciones como Externa, Interna, Proxy interno-bypass o Externa a través del conector de puerta de enlace, dependiendo de cómo quieran definir el flujo de tráfico.

[ACS-243]

22 May 2021

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

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

  [ACS-222]

- **Cambio de marca de la interfaz de usuario de Citrix Gateway Connector**

  La interfaz de usuario de Citrix Cloud Gateway Connector cambia de nombre según las pautas de marca de Citrix.

  [NGSWS-17100]

01 May 2021

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

  Los datos del cliente, incluidas las copias de seguridad, se eliminan del almacén de datos del servicio Citrix Secure Private Access después de 90 días de caducidad del derecho al 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 están simplificados para una incorporación más rápida en Citrix Workspace. La federación de dominios ahora se puede realizar en la interfaz de usuario del servicio Citrix Gateway, desde la página de inicio de sesión único.

  [ACS-351]

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

  La herramienta de prueba de conectividad en Citrix Gateway Connector se ha mejorado para gestionar errores de tiempo de espera y generar los registros necesarios.

  [NGSWS-17212]

15 de marzo de 2021

- **Mejoras de la plataforma**

  Se realizaron varias mejoras de la plataforma para aumentar la confiabilidad en la propagación de las configuraciones de administración del cliente a los conectores de Citrix Gateway.

  [ACS-85]

- **Rendimiento mejorado de aplicaciones web**

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

  [NGSWS-16469]

- **Habilitar Citrix Gateway Connector para utilizar conjuntos de cifrado TLS1.2 Grado A o superior**

  Citrix Gateway Connector ahora utiliza TLS1.2 con conjuntos de cifrado de grado A o superior para conectarse al servicio Citrix Cloud y 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 pasa a llamarse Acceso Privado Seguro.

  [NGSWS-14934]

15 de octubre de 2020

- **Opción de seguridad mejorada para ejecutar aplicaciones web empresariales y SaaS dentro del servicio de aislamiento remoto del navegador**

  Los administradores ahora pueden usar la opción de seguridad mejorada, **Seleccione Iniciar aplicación siempre en el servicio de Aislamiento de navegador remoto de Citrix** para iniciar siempre una aplicación en el servicio de Aislamiento de navegador remoto independientemente de otras configuraciones de seguridad mejoradas.

[ACS-123]

08 de octubre de 2020

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

  Los administradores ahora pueden configurar tiempos de espera de sesión para la extensión del navegador Citrix Secure Private Access. Los administradores pueden configurar esta configuración desde la pestaña **Administrar** en la interfaz de usuario del servicio Citrix Gateway.

  [NGSWS-13754]

- **Control RBAC en la configuración de administrador de la extensión del navegador Citrix Secure Private Access**

  El control RBAC ahora se aplica en las configuraciones de administración de la extensión del navegador Citrix Secure Private Access.

  [NGSWS-14427]

24 de septiembre de 2020

- **Habilite el acceso sin VPN a las aplicaciones web empresariales a través de un navegador local**

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

  [ACS-286]

07 de julio de 2020

- **Validar la configuración de Kerberos en Citrix Gateway Connector**

  Ahora puede utilizar el botón **Prueba** en la sección **Inicio de sesión único** para validar la configuración de Kerberos.

  [NGSWS-8581]

19 de junio de 2020

- **Acceso de solo lectura para administradores del servicio Citrix Gateway y del servicio Citrix Secure Private Access**

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

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

  [ACS-205]

08 May 2020

- **Nuevas herramientas de resolución de problemas en Citrix Gateway Connector 13.0**

  - **Rastreo de red:** Ahora puede usar la función **Rastreo** para solucionar problemas de registro de Citrix Gateway Connector. Puede descargar el archivo de seguimiento y compartirlo con los administradores para solucionar problemas. Para obtener más detalles, consulte Solucionar problemas de registro de Citrix Gateway Connector.

    [NGSWS-10799]

  - **Pruebas de conectividad:** Ahora puede usar la función **Prueba de conectividad** para confirmar que no haya errores en la configuración del Conector de puerta de enlace y que el Conector de puerta de enlace pueda conectarse a las URL. Para obtener más detalles, consulte Iniciar sesión y configurar Citrix Gateway Connector.

    [NGSWS-8580]

V2019.04.02

- **Compatibilidad con autenticación Kerberos para el conector de Citrix Gateway con proxy saliente** [NGSWS-6410]

  La autenticación Kerberos ahora es compatible con el tráfico desde Citrix Gateway Connector al proxy saliente. Gateway Connector utiliza las credenciales de proxy configuradas para autenticarse en el proxy saliente.

V2019.04.01

- **El tráfico de aplicaciones web/SaaS ahora se puede enrutar a través de un conector de puerta de enlace alojado en la 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 de esa aplicación para que pase a través de un conector de puerta de enlace local.

  Por ejemplo, supongamos que un cliente tiene una aplicación SaaS protegida por Okta (como Workday). Es posible que el cliente desee que, aunque el tráfico de datos real de Workday no se enrute a través del servicio Citrix Gateway, el tráfico de autenticación al servidor Okta se enrute a través del servicio Citrix Gateway mediante un conector de puerta de enlace local. Esto ayuda al cliente a evitar una autenticación de segundo factor del servidor Okta cuando el usuario se conecta al servidor Okta desde dentro de la red corporativa.

  [NGSWS-6445]

- **Deshabilitar el filtrado de listas de sitios web y la categorización de sitios web**. El filtrado de listas de sitios web y la categorización de sitios web se pueden deshabilitar si el administrador decide no aplicar estas funcionalidades para un cliente específico.

  [NGSWS-6532]

- **Enrutamiento geográfico automático para redireccionamientos del servicio de aislamiento remoto del navegador.** El enrutamiento geográfico automático ahora está habilitado para las redirecciones del servicio de aislamiento del navegador remoto.

  [NGSWS-6926]

V2019.03.01

- **Se agregó el botón "Detectar"en la página "Agregar un conector de puerta de enlace".** El botón **Detectar** se utiliza para actualizar la lista de conectores, lo que permite que el conector recién agregado se refleje en la sección de conectividad de la aplicación web.

  [CGOP-6358]

- **Se agrega una nueva categoría "Malicioso y peligroso"en las categorías "Filtrado web de control de acceso".** Se agrega una nueva categoría denominada **Malicioso y peligroso** en las categorías **Filtrado web de control de acceso** bajo el grupo **Malware y spam** .

  [CGOP-6205]

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.

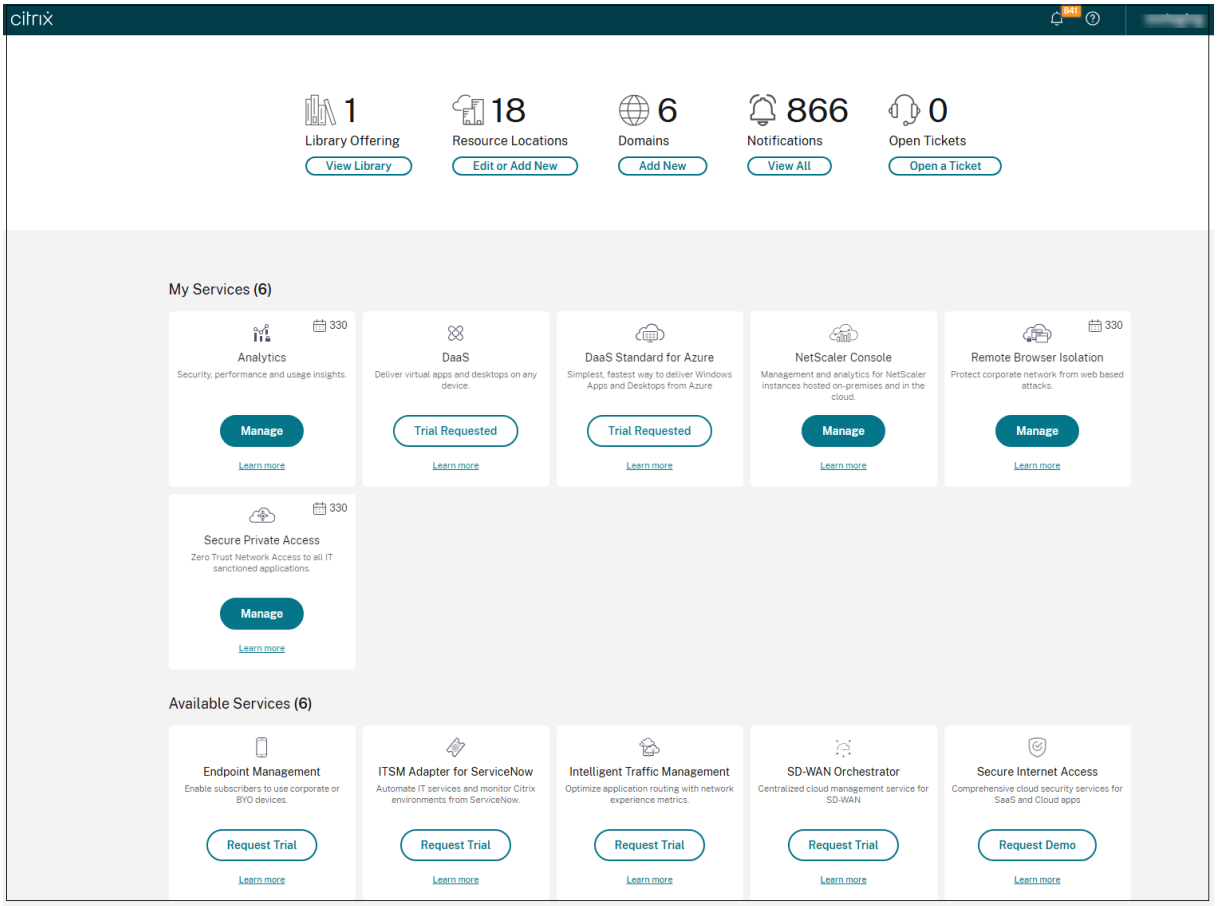
Paso 1: **Registrarse en Citrix Cloud**

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.

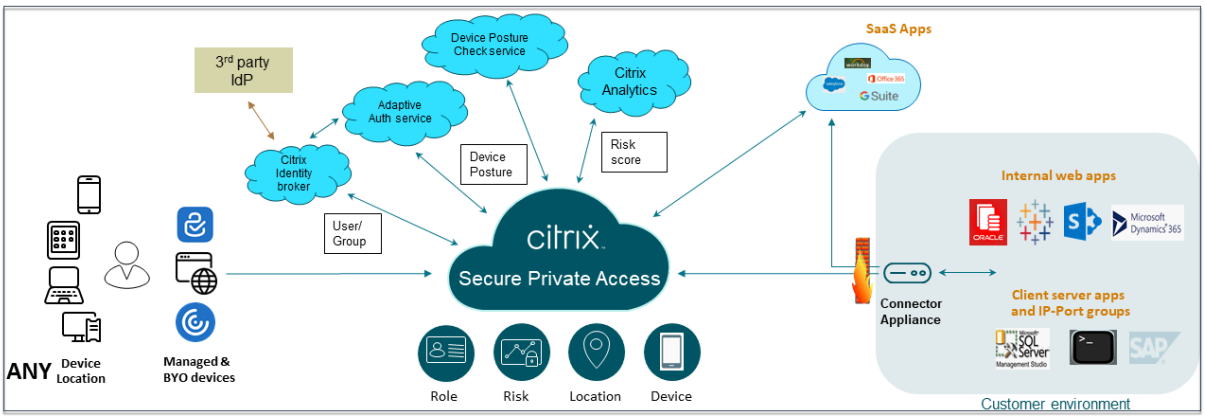
Información general sobre la solución de servicio Secure Private Access

October 21, 2024

Descripción general de la solución

Las soluciones VPN tradicionales requieren que los dispositivos de los usuarios finales sean administrados, brinden acceso a nivel de red y apliquen políticas de control de acceso estáticas. Citrix Secure Private Access brinda a TI un conjunto de controles de seguridad para protegerse contra amenazas de dispositivos BYO, dando a los usuarios la opción de acceder a sus aplicaciones aprobadas 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 proporciona la capacidad de escanear el dispositivo del usuario final antes de establecer una sesión mediante el servicio Device Posture. Según los resultados de la autenticación adaptativa o la postura del dispositivo, los administradores pueden definir los métodos de autenticación para las aplicaciones.



Seguridad adaptativa

La autenticación adaptativa determina el flujo de autenticación correcto para la solicitud actual. La autenticación adaptativa puede identificar la postura del dispositivo, la ubicación geográfica, el segmento de red y la membresía de la organización/departamento del usuario. Con base en la información obtenida, un administrador puede definir cómo desea autenticar a los usuarios en sus aplicaciones autorizadas por TI. Esto permite a las organizaciones implementar el mismo marco de política de autenticación en todos los recursos, incluidas aplicaciones SaaS públicas, aplicaciones web privadas, aplicaciones cliente-servidor privadas y escritorios como servicio (DaaS). Para obtener más detalles, consulte Seguridad adaptativa.

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 dispositivo conector implementado localmente. El dispositivo conector crea un canal de control de salida a la suscripción de Citrix Cloud de la organización. Desde allí, Secure Private Access puede tunelizar conexiones a las aplicaciones web internas sin necesidad de una VPN. Para obtener más detalles, consulte Acceso a aplicaciones.

Single Sign-On

Con la autenticación adaptativa, las organizaciones pueden proporcionar políticas 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 políticas de autenticación adaptativa para todas las aplicaciones SaaS, web privadas y cliente-servidor. Para obtener más detalles, consulte Inicio de sesión único.

Seguridad del navegador

Secure Private Access permite a los usuarios finales navegar de forma segura en Internet con un navegador empresarial seguro y administrado de forma centralizada. Cuando un usuario final lanza una aplicación web privada o SaaS, se toman dinámicamente varias decisiones para decidir cuál es la mejor manera de servir a esta aplicación. Para obtener más detalles, consulte Seguridad del navegador.

Postura del dispositivo

El servicio de postura del dispositivo permite que un administrador defina políticas para verificar la postura de los dispositivos terminales que intentan acceder a los recursos corporativos de forma re-

mota. Según el estado de cumplimiento de un punto final, el servicio de postura del dispositivo puede denegar el acceso o proporcionar acceso restringido o completo 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 comparte esta información con el servicio Device Posture para determinar si la postura del punto final cumple con los requisitos de la política.

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

Soporte para aplicaciones TCP y UDP

A veces, los usuarios remotos necesitan acceso a aplicaciones cliente-servidor privadas que tienen su front-end en el punto final y su back-end en un centro de datos. Las organizaciones pueden aplicar legítimamente políticas de seguridad estrictas en torno a estas aplicaciones internas y privadas, dificultando así el acceso de usuarios remotos a estas aplicaciones sin comprometer los protocolos de seguridad.

El servicio de acceso privado seguro aborda las vulnerabilidades de seguridad de TCP y UDP al permitir que ZTNA brinde acceso seguro a estas aplicaciones. Los usuarios ahora pueden acceder a todas las aplicaciones privadas, incluidas las aplicaciones TCP, UDP y HTTPS, mediante un navegador 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 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 desde la App Store.

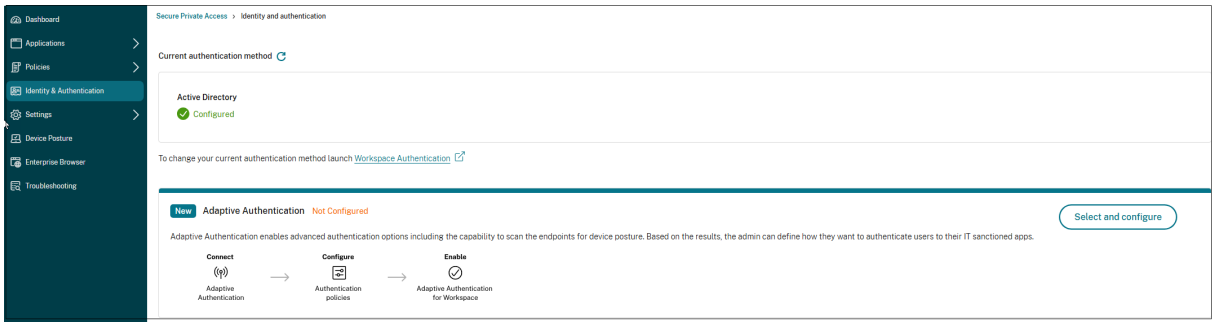
Para obtener más detalles, consulte Compatibilidad con aplicaciones cliente-servidor.

Configurar el acceso privado seguro de Citrix

Habilite el acceso a la red de confianza cero para aplicaciones SaaS, aplicaciones web internas y aplicaciones TCP y UDP mediante la consola de administración de acceso privado seguro. Esta consola incluye la configuración de la autenticación adaptativa, aplicaciones que incluyen suscripción de usuarios y políticas de acceso adaptativas.

Configurar identidad y 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 detalles, consulte Configurar identidad y autenticación.

Enumerar y publicar aplicaciones

Después de haber seleccionado el método de autenticación, configure las aplicaciones Web, SaaS o TCP y UDP mediante la consola de administración. Para obtener más detalles, consulte Agregar y administrar aplicaciones.

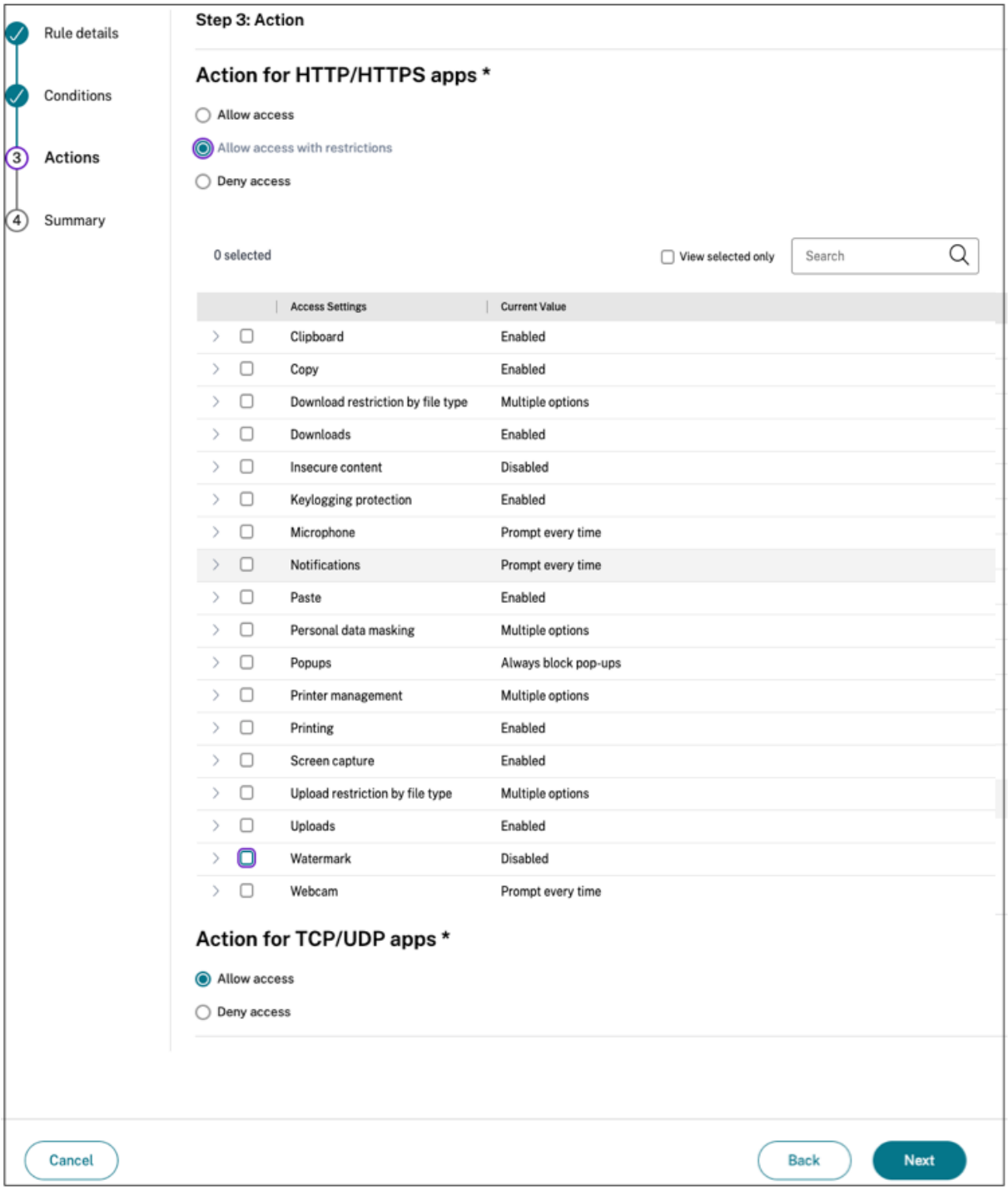
Habilitar controles de seguridad mejorados

Para proteger el contenido, las organizaciones incorporan políticas de seguridad mejoradas dentro de las aplicaciones SaaS. Cada política aplica una restricción en el navegador Citrix Enterprise cuando se usa la aplicación Workspace para escritorio o en el navegador seguro cuando se usa la aplicación Workspace web o móvil.

- **Restringe el acceso al portapapeles**: Deshabilita las operaciones de cortar/copiar/pegar entre la aplicación y el portapapeles del sistema.
- **Restringir impresión**: Deshabilita la capacidad de imprimir desde el navegador Citrix Enterprise.
- **Restringir descargas**: Deshabilita la capacidad del usuario para descargar desde dentro de la aplicación.
- **Restringir cargas**: Deshabilita la capacidad del usuario para cargar dentro de la aplicación.
- **Mostrar marca de agua**: Muestra una marca de agua en la pantalla del usuario mostrando el nombre de usuario y la dirección IP de la máquina del usuario.
- **Restringe el registro de teclas**: Protege contra los registradores de teclas. Cuando un usuario intenta iniciar sesión en la aplicación utilizando el nombre de usuario y la contraseña, todas las claves se cifran en los registradores de teclas. Además, todas las actividades que el usuario

realiza en la aplicación están protegidas contra el registro de teclas. Por ejemplo, si las políticas 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 captura de pantalla**: Deshabilita la capacidad de capturar pantallas usando 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 detalles, consulte Configurar una política de acceso.

Habilitar Citrix Enterprise Browser para el lanzamiento de aplicaciones

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

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

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

Configuración mediante API:

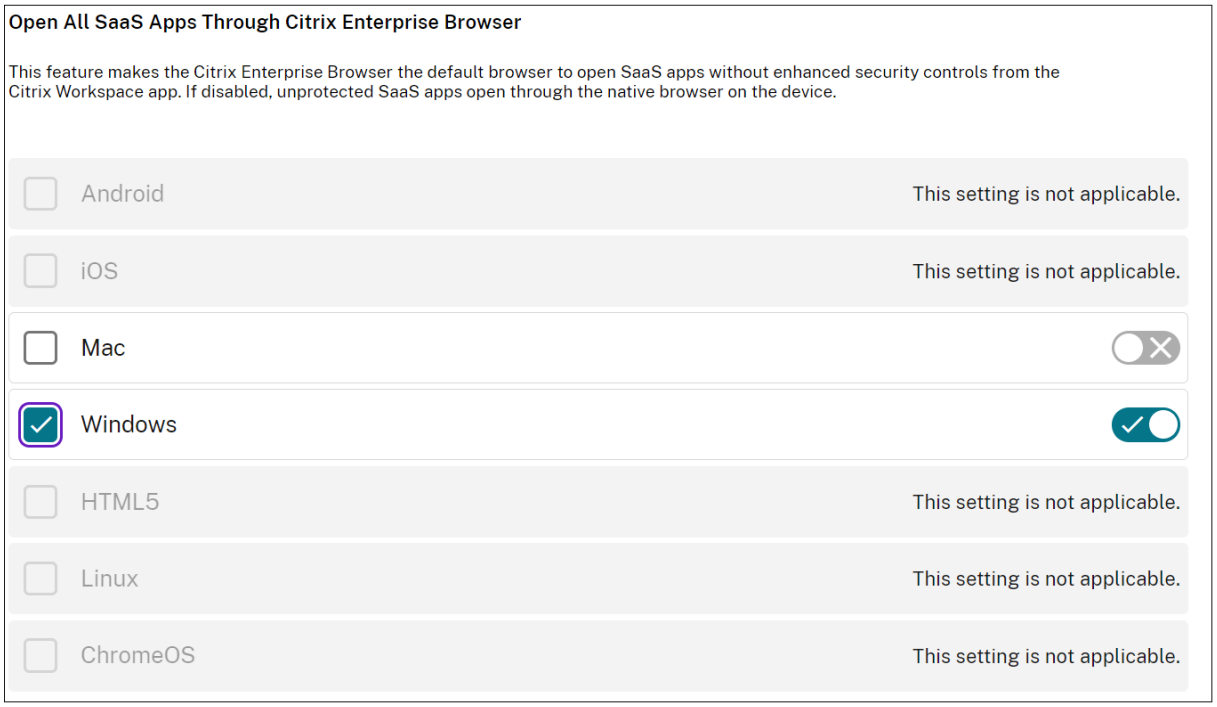
Para configurarlo, aquí hay un archivo JSON de ejemplo para habilitar Citrix Enterprise Browser para todas las aplicaciones, de forma predeterminada:

```
"settings": [
                    {

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

                    ]
```

El valor predeterminado es true.

Configuración a través de GUI:

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



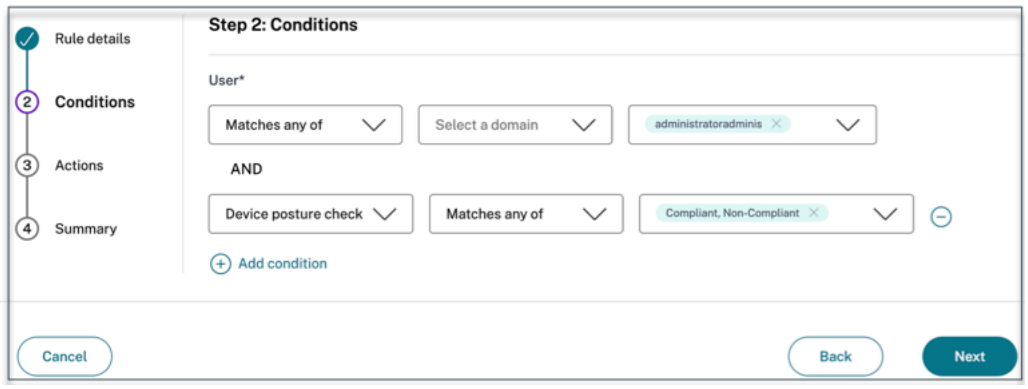
Para obtener más detalles, consulte Administrar Citrix Enterprise Browser a través de GACS.

Configurar etiquetas para acceso contextual mediante la postura del dispositivo

Después de la verificación de la postura del dispositivo, se le permite a este iniciar sesión y se clasifica como compatible o no compatible. Esta clasificación se pone a disposición en forma de etiquetas para el servicio de acceso privado seguro y se utiliza para proporcionar acceso contextual según la postura del dispositivo.

1. Inicie sesión en Citrix Cloud.
2. En el mosaico Acceso privado seguro, haga clic en **Administrar**.
3. Haga clic en **Políticas de acceso** en la navegación izquierda y luego haga clic en **Crear política**.
4. Introduzca el nombre de la política y la descripción de la misma.
5. En **Aplicaciones**, seleccione la aplicación o el conjunto de aplicaciones en las que se debe aplicar esta política.
6. Haga clic en **Crear regla** para crear reglas para la política.
7. Ingrese el nombre de la regla y una breve descripción de la regla y luego haga clic en **Siguiente**.
8. Seleccione las condiciones de los usuarios. La condición de Usuarios 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 del menú desplegable.
11. Introduzca uno de los siguientes valores en las etiquetas personalizadas:



- **Compatible** - Para dispositivos compatibles
- **No compatible** - Para dispositivos no compatibles

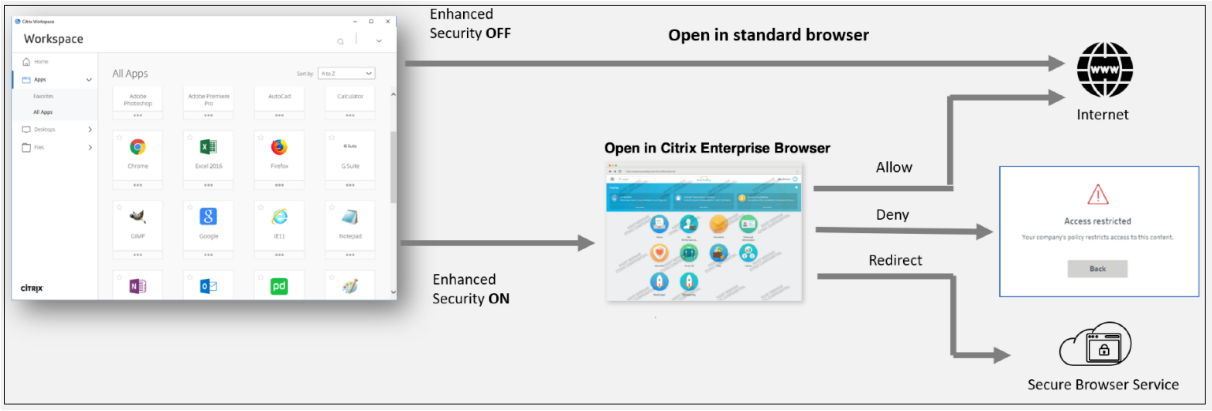
12. Haga clic en **Siguiente**.
13. Seleccione las acciones que se deben aplicar en función de la evaluación de la condición y luego haga clic en **Siguiente**.

    La página Resumen muestra los detalles de la política.
14. Verifique los detalles y haga clic en **Finalizar**.

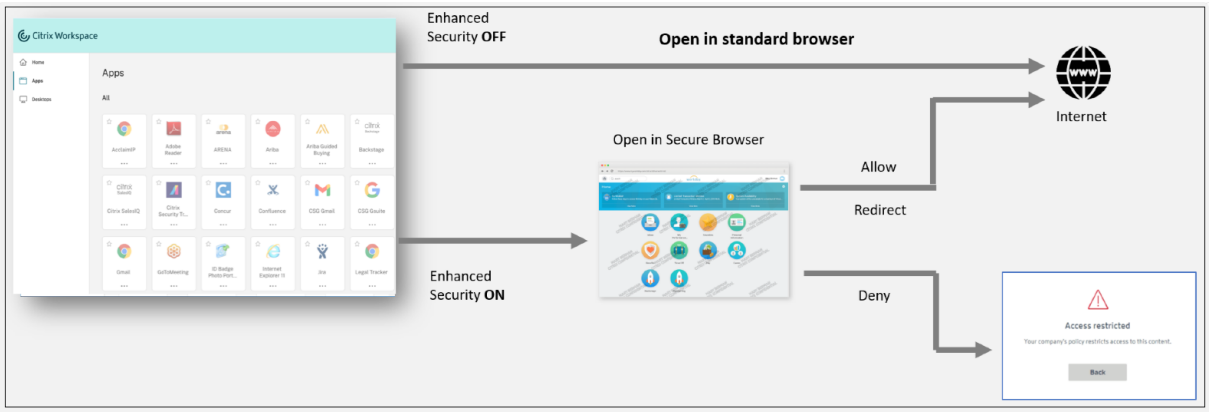
> **Nota**
>
> Cualquier aplicación de acceso privado seguro que no esté etiquetada como compatible o no compatible en la política de acceso se trata como la aplicación predeterminada y es accesible en todos los puntos finales independientemente de la postura del dispositivo.

Experiencia del usuario final

El administrador de Citrix tiene el poder 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 cómo el usuario final accede a una aplicación SaaS a través de la interfaz de usuario web de Citrix Workspace Experience o el cliente de la aplicación nativa de Citrix Workspace.



Cuando el usuario inicia la aplicación Workspace en el punto final, ve sus aplicaciones, escritorios, archivos y aplicaciones SaaS. Si un usuario hace clic en la aplicación SaaS cuando la seguridad mejorada está deshabilitada, la aplicación se abre en un navegador estándar instalado 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 está controlada según las políticas de sitios web no autorizados. Para obtener detalles sobre sitios web no autorizados, consulte Sitios web no autorizados.



De manera similar, con el portal web Workspace, cuando la seguridad mejorada está deshabilitada, las aplicaciones SaaS se abren en un navegador estándar que está instalado de forma nativa. Cuando la seguridad mejorada está habilitada, las aplicaciones SaaS se abren en el navegador remoto seguro. Los usuarios pueden acceder a los sitios web dentro de las aplicaciones SaaS según las políticas de sitios web no autorizados. Para obtener detalles sobre sitios web no autorizados, consulte Sitios web no autorizados.

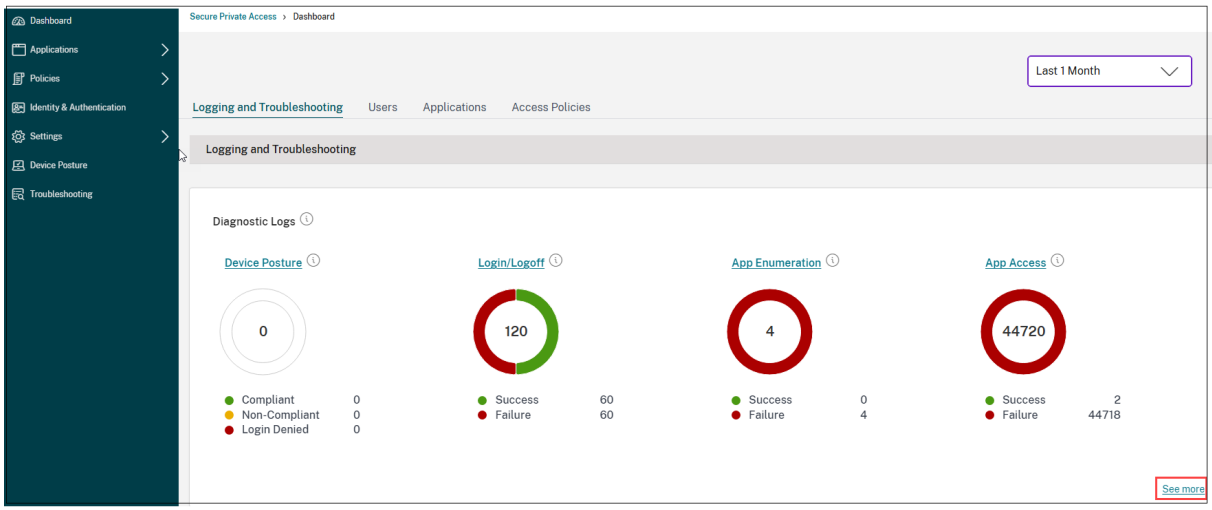
Panel de análisis

El panel del servicio de acceso privado seguro muestra los datos de diagnóstico y uso de las aplicaciones SaaS, web, TCP y UDP. El panel proporciona a los administradores visibilidad completa de sus aplicaciones, usuarios, estado de los conectores y uso del ancho de banda en un solo lugar para el con-

sumo. Estos datos se obtienen de Citrix Analytics. Las métricas se clasifican en términos generales en las siguientes categorías.

- Registro y resolución de problemas
- Usuarios
- Aplicaciones
- Políticas de acceso

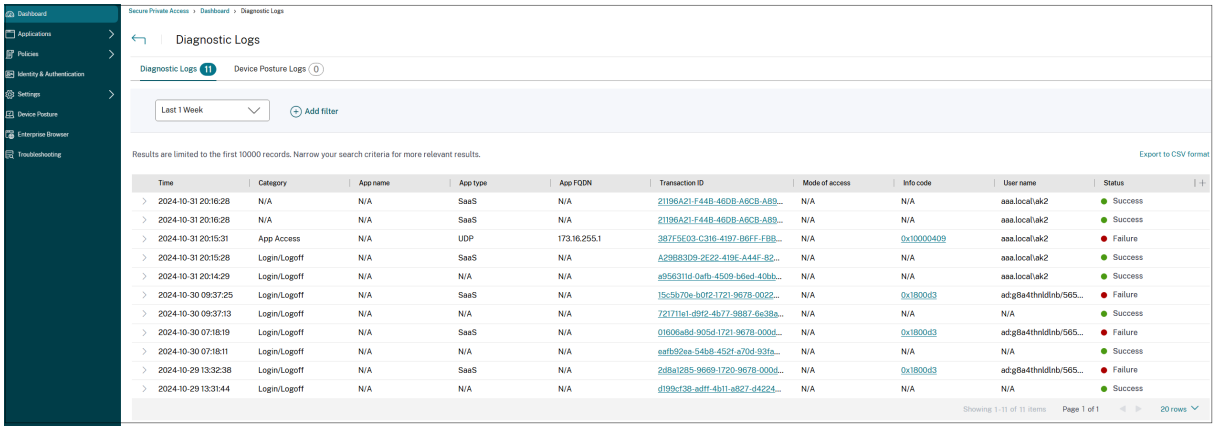
Para obtener más detalles, consulte Panel de control.



Solucionar problemas de aplicaciones

El gráfico de registros de diagnóstico en el panel de acceso privado seguro proporciona visibilidad de los registros relacionados con la autenticación, el inicio de aplicaciones, la enumeración de aplicaciones y los registros de postura del dispositivo.

- **Código de información**: Algunos eventos de registro, como fallas, tienen un código de información asociado. Al hacer clic en el código de información, se redirige a los usuarios 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 acceso privado seguro para una solicitud de acceso. Se pueden generar varios registros a partir de una solicitud de acceso a una aplicación, comenzando por la autenticación, luego la enumeración de aplicaciones dentro de la aplicación del espacio de trabajo y luego 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 utilizando el ID de transacción para encontrar todos los registros relacionados con una solicitud de acceso a una aplicación en particular. Para obtener más detalles, consulte Solucionar problemas de acceso privado seguro.



Ejemplos de casos de uso

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

Artículos de referencia

- Introducción al acceso privado seguro
- 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 fácil incorporación y configuración

Vídeos de referencia

- Acceso a la red de confianza cero (ZTNA) para aplicaciones
- Acceso privado a aplicaciones web con Citrix Secure Private Access
- Acceso a aplicaciones SaaS públicas con Citrix Secure Private Access
- Acceso privado a aplicaciones cliente-servidor con Citrix Secure Private Access

- Protección contra keyloggers con Citrix Secure Private Access
- Protección de pantalla compartida con Citrix Secure Private Access
- Experiencia del usuario final con Citrix Secure Private Access
- Experiencia de inicio de sesión de ZTNA versus VPN con Citrix Secure Private Access
- Escaneos de puertos ZTNA versus VPN con Citrix Secure Private Access

Novedades en productos relacionados

- Citrix Enterprise Browser: Acerca de esta versión
- Citrix Workspace: Novedades
- Citrix DaaS: Novedades
- Cliente de Citrix Secure Access Clientes de NetScaler Gateway

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

October 21, 2024

El servicio de acceso privado seguro ofrece una nueva experiencia administrativa optimizada con un proceso paso a paso para configurar el acceso a la red Zero Trust para aplicaciones SaaS, aplicaciones web internas y aplicaciones TCP. Incluye configuración de autenticación adaptativa, aplicaciones que incluyen suscripción de usuarios, políticas de acceso adaptativas y otras dentro de una única 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, está disponible un nuevo panel con visibilidad completa de las métricas de uso general y otra información clave.

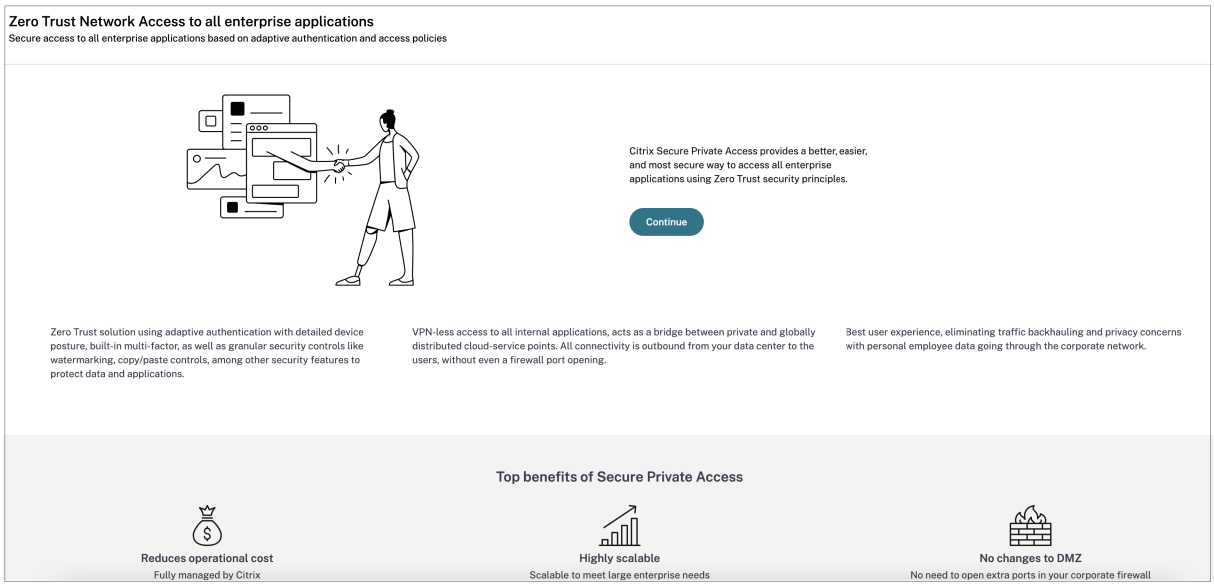
Los pasos de alto nivel incluyen lo siguiente:

1. Elija el método de autenticación para que los suscriptores inicien sesión en Citrix Workspace.
2. Añade aplicaciones para tus usuarios.
3. Asigna permisos para el acceso a la aplicación creando las políticas de acceso necesarias.
4. Revise la configuración de la aplicación.

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

Realice los siguientes pasos para acceder al asistente.

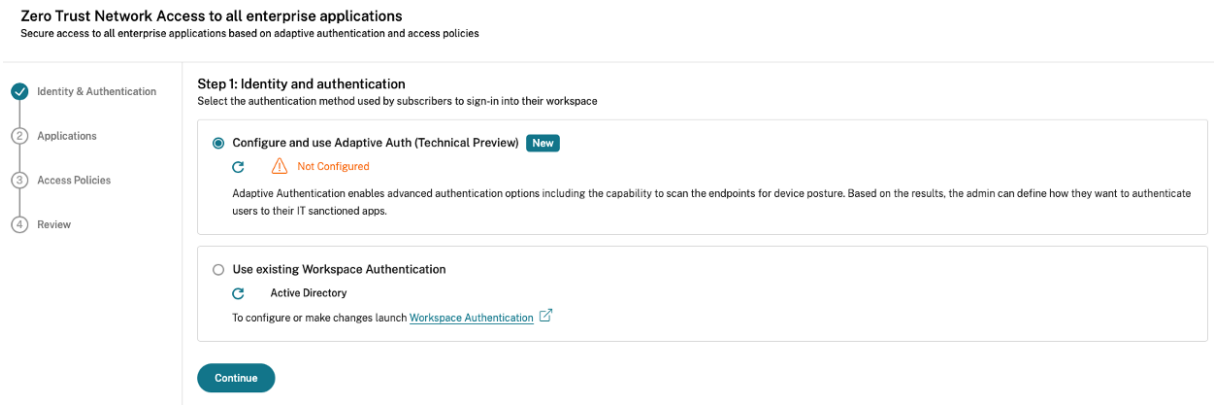
1. En el mosaico de servicio **Acceso privado seguro** , haga clic en **Administrar**.
2. En la página Descripción general, haga clic en **Continuar**.



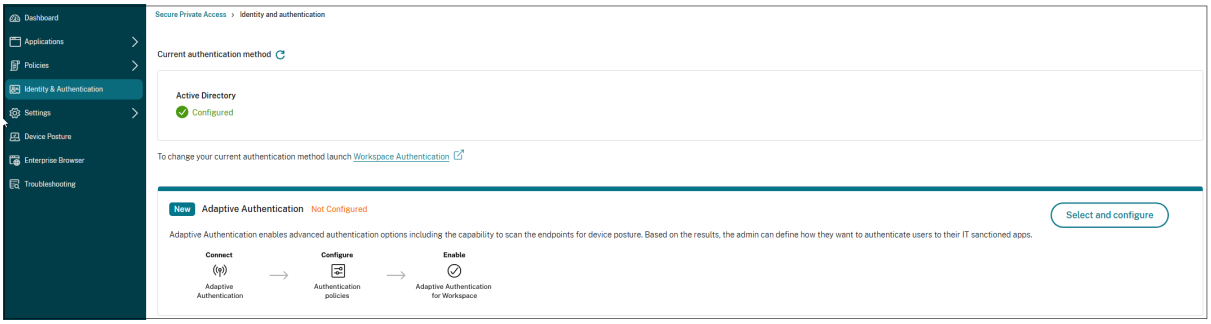
Paso 1: Configurar la identidad y la autenticación

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 adaptativa es un ADC Citrix alojado, administrado por Citrix y alojado en la nube que proporciona todas las capacidades de autenticación avanzadas, como las siguientes.

- Autenticación de varios factores
- Escaneos de postura del dispositivo
- Autenticación condicional
- Acceso adaptativo a Citrix Virtual Apps and Desktops
- Para configurar la autenticación adaptativa, seleccione **Configurar y usar autenticación adaptativa (vista previa técnica)** y luego complete la configuración. Para obtener más detalles sobre la autenticación adaptativa, consulte Servicio de autenticación adaptativa. Después de configurar la autenticación adaptativa, puede hacer clic en **Administrar** para modificar la configuración, si es necesario.



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



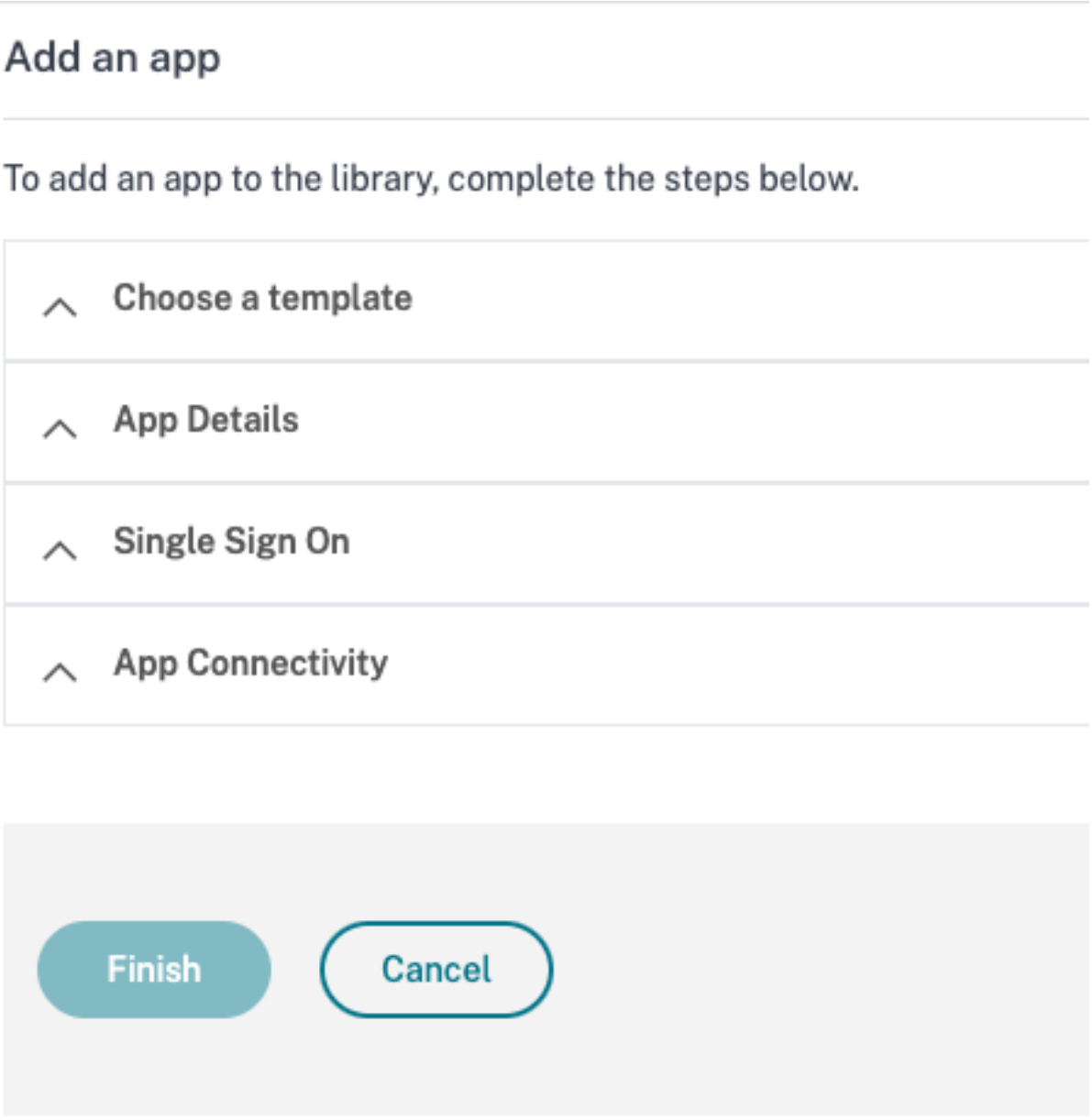
Para cambiar el método de autenticación existente o cambiar el método de autenticación existente, haga clic en **Autenticación del espacio de trabajo**.

Paso 2: Agregar y administrar aplicaciones

Después de haber seleccionado el método de autenticación, configure las aplicaciones. Para los usuarios que lo utilizan por primera vez, la página de inicio **Aplicaciones** no muestra ninguna aplicación. Agregue una aplicación haciendo 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 agregues una aplicación, podrás verla listada aquí.

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



- **Agregar una aplicación web empresarial**
  - Compatibilidad con aplicaciones web empresariales
  - Configurar el acceso directo a las aplicaciones web
- **Agregar una aplicación SaaS**
  - Soporte para aplicaciones de software como servicio
  - Configuración específica del servidor de aplicaciones SaaS
- **Configurar aplicaciones cliente-servidor**
  - Soporte para aplicaciones cliente-servidor

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

Paso 3: Configurar una política de acceso con múltiples reglas

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

Las políticas de acceso dentro de Secure Private Access le permiten habilitar o deshabilitar el acceso a las aplicaciones según el contexto del usuario o del dispositivo del usuario. Además, puedes habilitar el acceso restringido a las aplicaciones agregando las siguientes restricciones de seguridad:

- Restringir acceso al portapapeles
- Restringir la impresión
- Restringir descargas
- Restringir subidas
- Mostrar marca de agua
- Restringir el registro de teclas
- Restringir la captura de pantalla

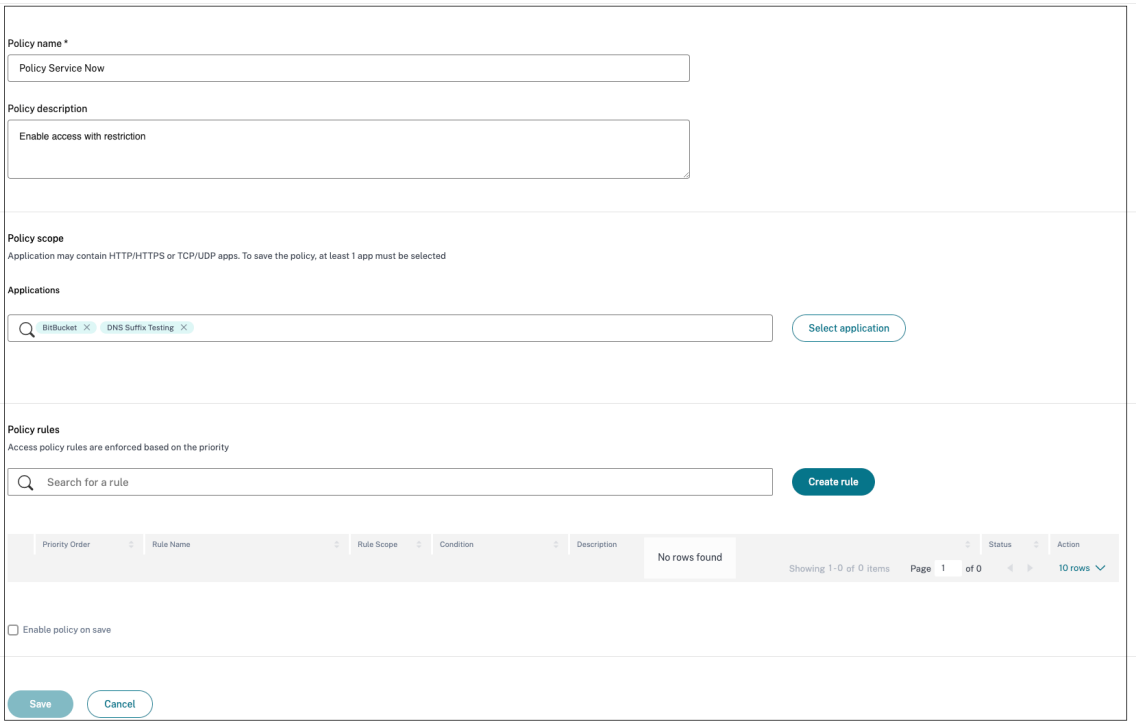
Para obtener más información sobre estas restricciones, consulte Restricciones de acceso disponibles.

1. En el panel de navegación, haga clic en **Políticas de acceso** y luego haga clic en **Crear política**.

   Para los usuarios nuevos, la página de inicio **Políticas de acceso** no muestra ninguna política. Una vez que cree una política, podrá verla listada aquí.

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

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



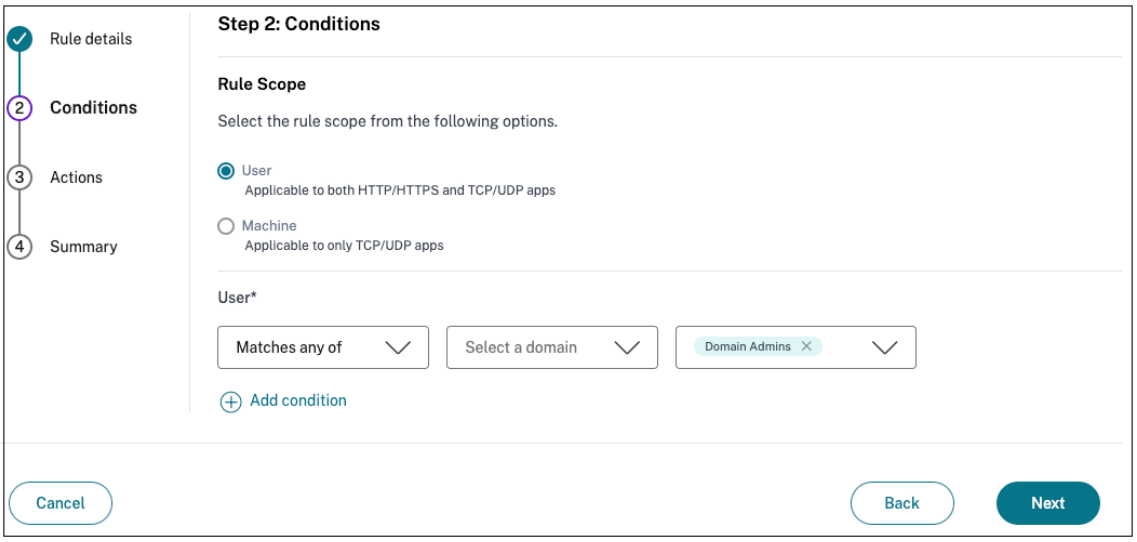
5. Ingrese el nombre de la regla y una breve descripción de la regla y luego haga clic en **Siguiente**.

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

   - **Coincide con cualquiera de** : solo se permite el acceso a los usuarios o grupos que co-

incidan con cualquiera de los nombres enumerados en el campo y que pertenezcan al dominio seleccionado.

- **No coincide con ningún** - Se permite el acceso a todos los usuarios o grupos excepto aquellos enumerados en el campo y que pertenecen al dominio seleccionado.



7. (Opcional) Haga clic en + para agregar múltiples condiciones según el contexto.

   Cuando se agregan condiciones basadas en un contexto, se aplica una operación AND en las condiciones en donde la política se evalúa solo si se cumplen los **Usuarios** y las condiciones contextuales opcionales. Puede aplicar las siguientes condiciones según el contexto.

   - **Escritorio** o **Dispositivo móvil** –Seleccione el dispositivo para el cual desea 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 los siguientes:** Solo los usuarios o grupos de usuarios que acceden a las aplicaciones desde cualquiera de las ubicaciones geográficas enumeradas tienen permitido el acceso a las aplicaciones.
     - **No coincide con ninguno:** Todos los usuarios o grupos de usuarios que no sean los de las ubicaciones geográficas enumeradas tienen acceso habilitado.
   - **Ubicación de red** –Seleccione la condición y la red mediante la cual los usuarios acceden a las aplicaciones.
     - **Coincide con cualquiera de los siguientes:** Solo los usuarios o grupos de usuarios que acceden a las aplicaciones desde cualquiera de las ubicaciones de red enumeradas tienen acceso habilitado 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.

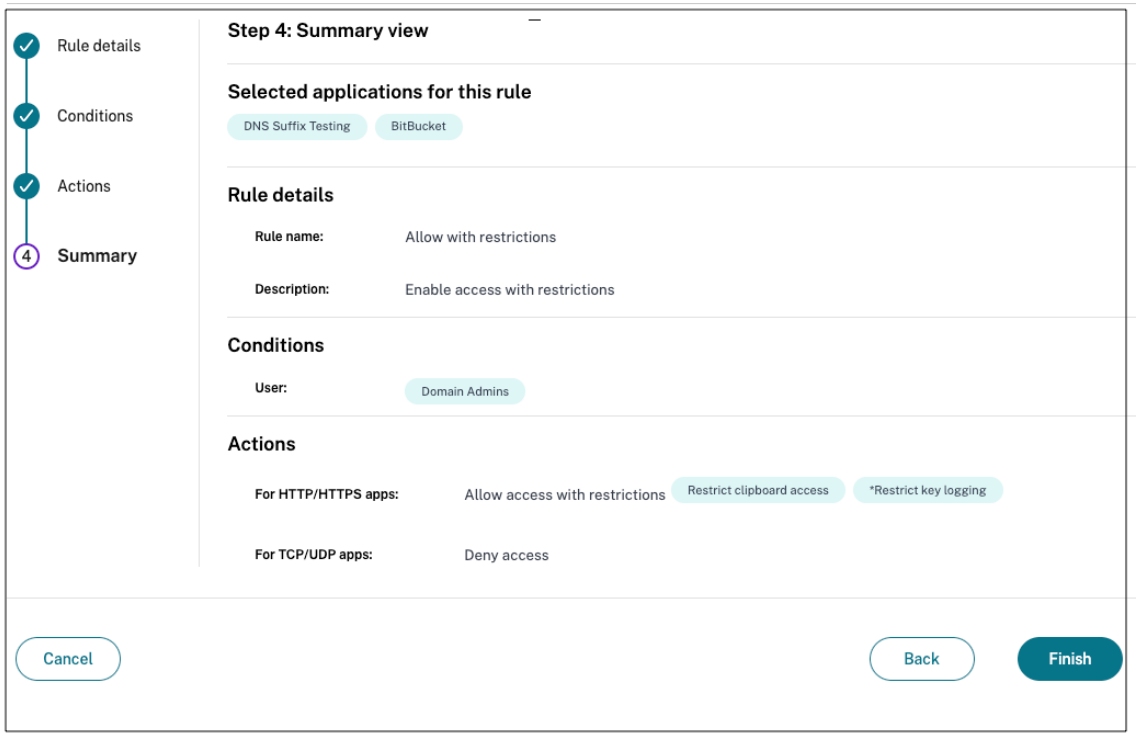
- **Verificación de la postura del dispositivo** –Seleccione las condiciones que debe pasar el dispositivo del usuario para acceder a la aplicación.
- **Puntuación de riesgo del usuario** –Seleccione las categorías de puntuación de riesgo en función de las cuales se debe proporcionar a los usuarios acceso a la aplicación.
- **URL del espacio de trabajo** : los administradores pueden especificar filtros según el nombre de dominio completo correspondiente al espacio de trabajo.
  - **Coincide con cualquiera de** : permite el acceso solo cuando la conexión del usuario entrante coincide con cualquiera de las URL del espacio de trabajo configuradas.
  - **Coincide con todos los** : permite el acceso solo cuando la conexión del usuario entrante cumple con todas las URL del espacio de trabajo configuradas.

8. Haga clic en **Siguiente**.
9. Seleccione las acciones que se deben aplicar en función de la evaluación de la condición.
   - Para aplicaciones HTTP/HTTPS, puede seleccionar lo siguiente:
     - **Permitir acceso**
     - **Permitir acceso con restricciones**
     - **Denegar acceso**

> **Nota**
>
> Si selecciona **Permitir acceso con restricciones**, deberá seleccionar las restricciones que desea aplicar en las aplicaciones. Para obtener detalles sobre las restricciones, consulte Restricciones de acceso disponibles. También puede especificar si desea que la aplicación se abra en un navegador remoto o en Citrix Secure Browser.

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

![Crear acción de regla](/en-us/citrix-secure-private-access/media/
   secure-private-access-policy-rule-actions.png)
```

1. Haga clic en **Siguiente**. La página Resumen muestra los detalles de la política.
2. Puede verificar los detalles y hacer clic en **Finalizar**.



Puntos a recordar después de crear una política

- La política que usted creó aparece en la sección Reglas de política y está habilitada de forma predeterminada. Puede desactivar las reglas, si es necesario. Sin embargo, asegúrese de que al menos una regla esté habilitada para que la política esté activa.
- De forma predeterminada, se asigna un orden de prioridad a la política. La prioridad con un valor más bajo tiene la mayor preferencia. 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.

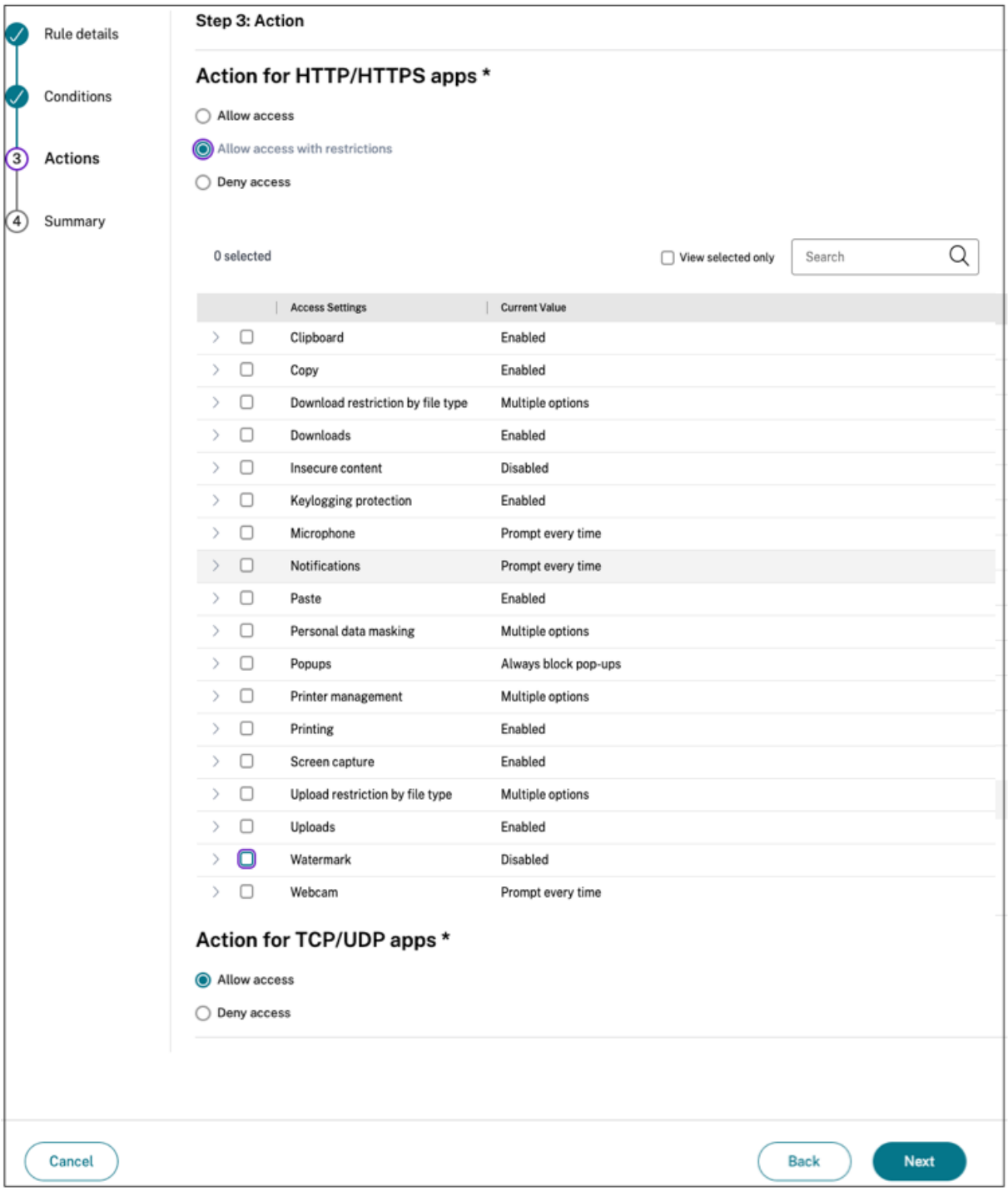
Ejemplo de evaluación de reglas con orden de prioridad:

Considera que has creado dos reglas, Regla 1 y Regla 2. La regla 1 se asigna al usuario A y la regla 2 se asigna al usuario B, luego se evalúan ambas reglas. Considere que ambas reglas, Regla 1 y Regla 2, están asignadas al usuario A. En este caso, la regla 1 tiene mayor prioridad. Si se cumple la condición de la Regla 1, entonces se aplica la Regla 1 y se omite la Regla 2. De lo contrario, si no se cumple la condición de la Regla 1, se aplica la Regla 2 al usuario A.

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

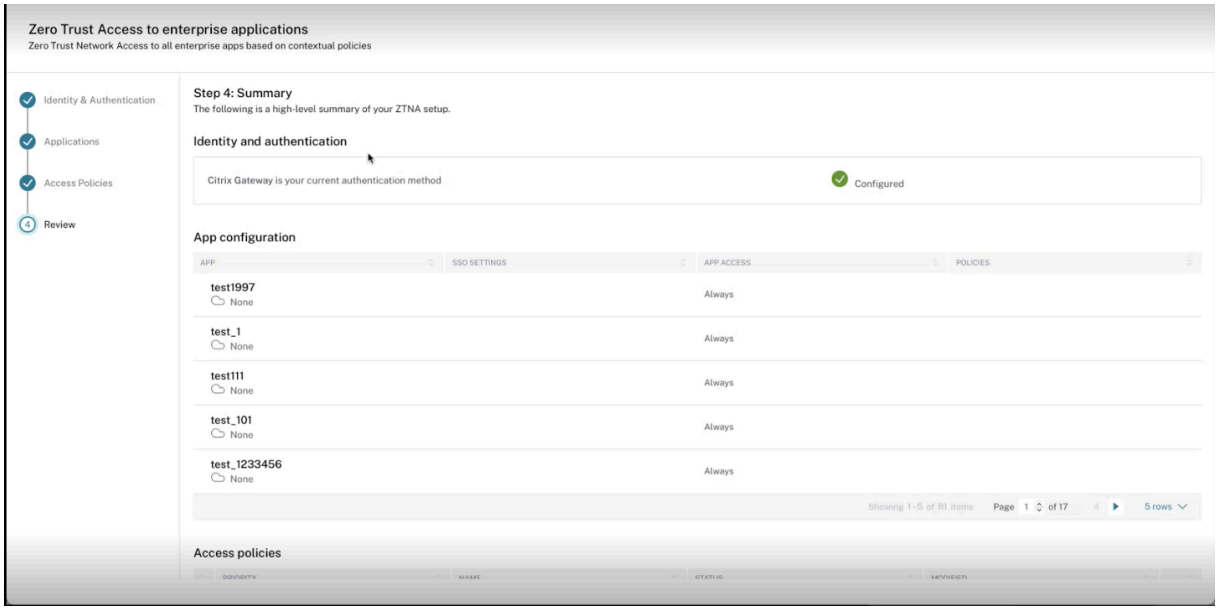
Opciones de restricciones de acceso disponibles

Cuando selecciona la acción **Permitir 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. Para obtener más detalles, consulte Opciones de restricciones de acceso disponibles.

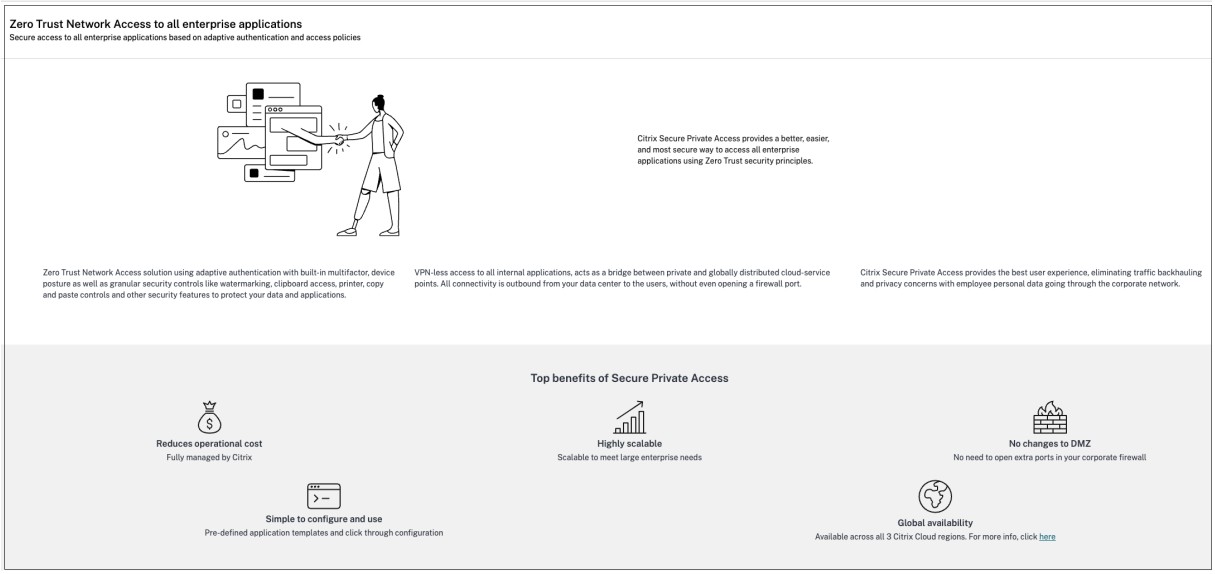


Paso 4: Revisar el resumen de cada configuración

Desde la página de Revisión, puedes ver la configuración completa de la aplicación y luego hacer clic en **Cerrar**.

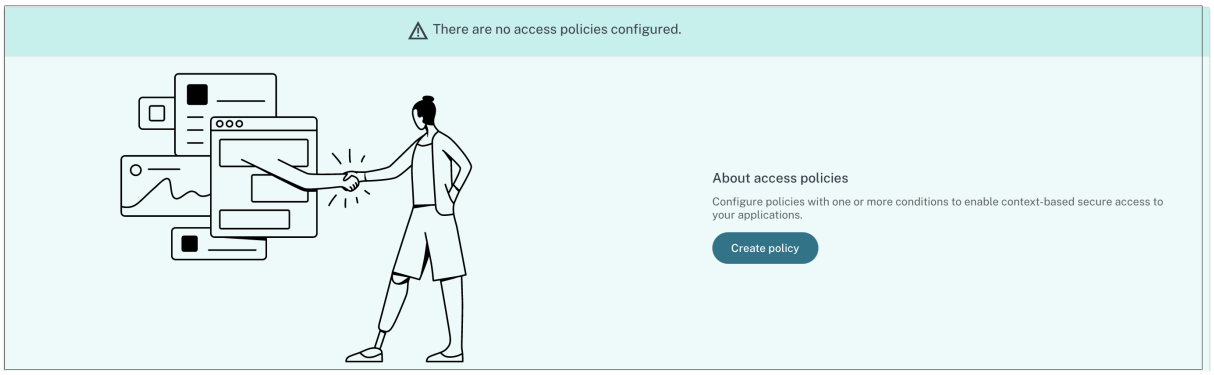


La siguiente figura muestra la página después de haber completado la configuración de 4 pasos.



Importante:

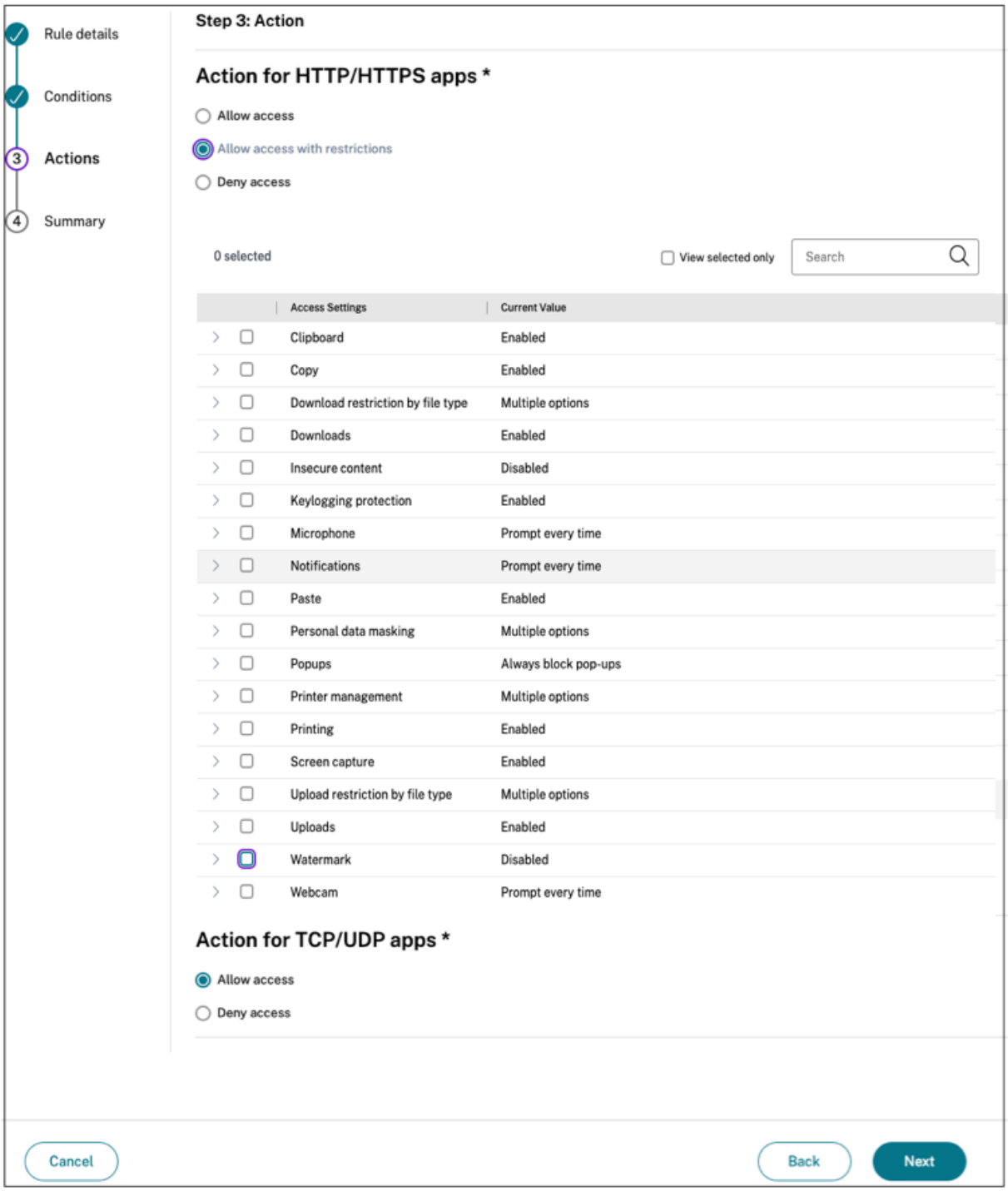
- Una vez que haya completado la configuración mediante el asistente, puede modificar la configuración de una sección yendo directamente a esa sección. No es necesario seguir la secuencia.
- Si elimina todas las aplicaciones configuradas o las políticas, deberá agregarlas nuevamente. En este caso, aparece la siguiente pantalla si ha eliminado todas las políticas.



Opciones de restricción de acceso

October 21, 2024

Cuando selecciona la acción **Permitir acceso con restricciones** al crear una política de acceso, puede seleccionar las restricciones de acceso. Estas restricciones están predefinidas en el sistema. Los administradores no pueden modificar ni agregar otras combinaciones. Para obtener detalles sobre cómo crear una política de acceso y habilitar restricciones de acceso, consulte Configurar una política de acceso.



Portapapeles

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

Copiar

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

> **Nota**
>
> - Si las restricciones **Portapapeles** y **Copiar** están habilitadas en una política, la restricción **Portapapeles** tiene prioridad sobre la restricción **Copiar** .
> - Los usuarios finales deben utilizar Citrix Enterprise Browser versión 2405 o posterior para acceder a las aplicaciones para las que está habilitada esta restricción. De lo contrario, el acceso a la aplicación estará restringido.
> - Para un control granular de la operación de copia dentro de las aplicaciones, los administradores pueden usar la restricción **Grupos de seguridad** . Para obtener más detalles, consulte Restricción del portapapeles para grupos de seguridad.

Restricción de descarga por tipo de archivo

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

> **Nota**
>
> - La restricción de descarga **por tipo de archivo** está disponible además de la restricción de descarga ** .
> - Si las restricciones **Descargas** y **Restricción de descargas por tipo de archivo** están habilitadas en una política, la restricción **Descargas** tiene prioridad sobre la restricción **Restricción de descargas por tipo de archivo** .
> - Los usuarios finales deben utilizar Citrix Enterprise Browser versión 2405 o posterior para acceder a las aplicaciones para las que está habilitada esta restricción. De lo contrario, el acceso a la aplicación estará restringido.

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

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

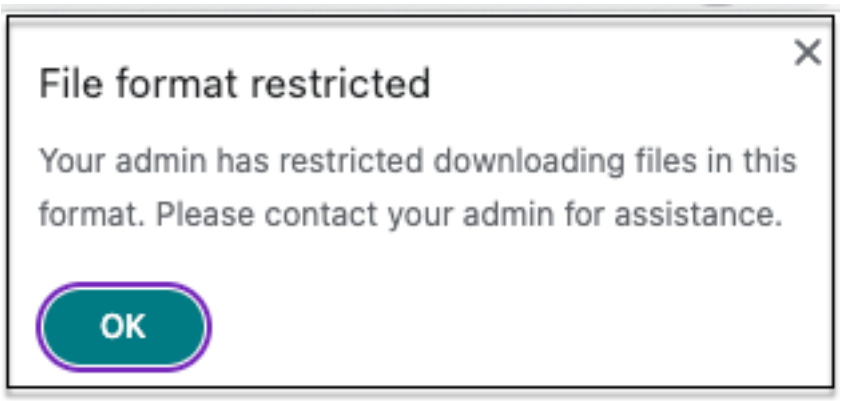
- **Permitir todas las descargas con excepciones** –Seleccionar los tipos que deben bloquearse y permitir todos los demás tipos.
- **Bloquear todas las descargas con excepciones** –Seleccionar solo los tipos que se pueden cargar y bloquear todos los demás tipos.

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

   a) Haga clic en **Agregar tipos MIME personalizados**.
   b) En **Agregar tipos MIME**, ingrese el tipo MIME en el formato `categoría/subcategoría<extension>`. Por ejemplo `imagen/png`.
   c) Haga clic en **Listo**.
   d) Haga clic en **Siguiente** y, a continuación, en **Finalizar**.

   El tipo MIME ahora aparece en la lista de excepciones.

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



Descargas

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

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

Contenido inseguro

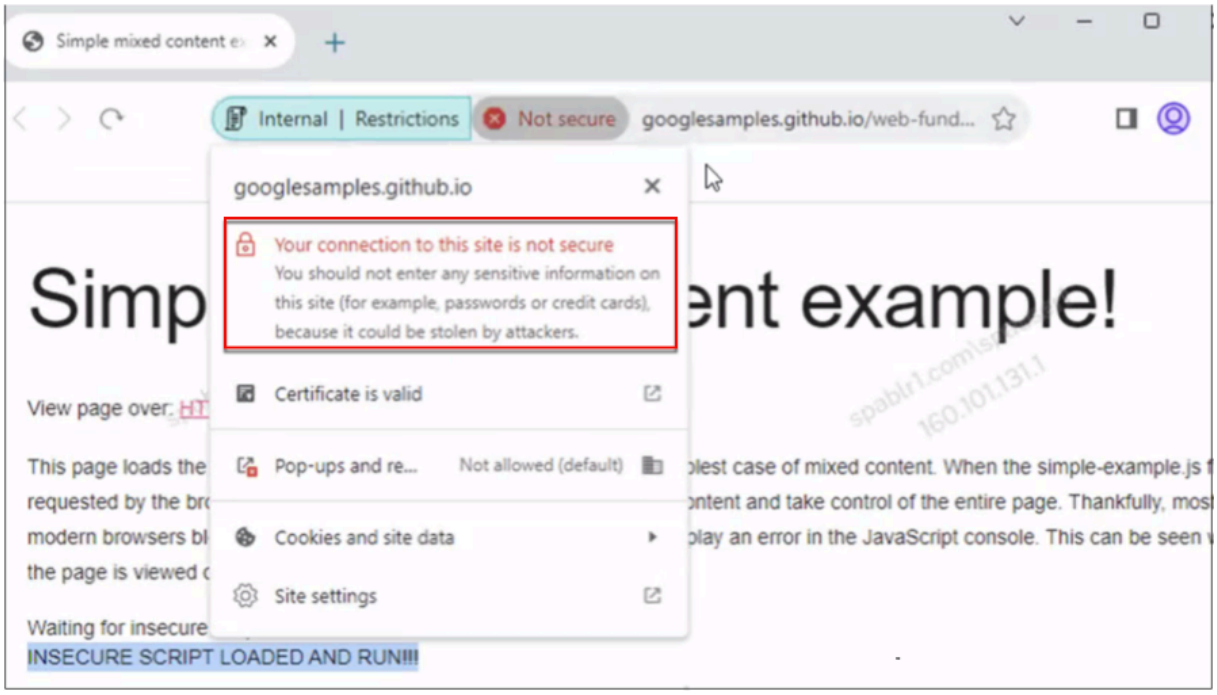
Habilite o deshabilite a los usuarios finales para que no accedan a contenido inseguro dentro del SaaS o la aplicación web interna configurada con esta política cuando accedan a través de Citrix Enterprise Browser. El contenido inseguro es cualquier archivo vinculado desde una página web mediante un enlace HTTP en lugar de un enlace HTTPS. Valor predeterminado: Inhabilitada.

Los usuarios finales deben utilizar Citrix Enterprise Browser versión 126 o posterior para deshabilitar el acceso a contenido inseguro.

Para habilitar el acceso a contenido inseguro, realice los siguientes pasos:

1. Crear o editar una política de acceso. Para obtener más detalles, consulte Crear políticas de acceso.
2. En la página **Paso 3: Acción** , seleccione **Permitir con restricciones**.
3. Seleccione **Contenido inseguro**.
4. Haga clic en **Siguiente** y, a continuación, en **Finalizar**.

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



Protección contra registro de teclas

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

Micrófono

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

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

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

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

> **Nota**
>
> - Si la restricción **Micrófono** está habilitada en la política de Acceso privado seguro, entonces Citrix Enterprise Browser muestra la configuración **Permitir**.
> - Si la opción **Preguntar cada vez** en la política de acceso privado seguro, la configuración aplicada en Citrix Enterprise Browser varía dependiendo de si se utiliza el servicio de configuración global de aplicaciones (GACS) para administrar Citrix Enterprise Browser.
> - Si se utiliza GACS, la configuración de GACS se aplica en Citrix Enterprise Browser.
> - Si no se utiliza GACS, Citrix Enterprise Browser muestra la configuración **Preguntar**.

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

Notificaciones

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

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

Para bloquear notificaciones sin que se le pregunte, realice los siguientes pasos.

1. Crear o editar una política de acceso. Para obtener más detalles, consulte Crear políticas de acceso.
2. En la página **Paso 3: Acción** , seleccione **Permitir con restricciones**.
3. Haga clic en **Notificaciones** y luego haga clic en **Editar**.
4. En la página **Configuración de notificaciones** , haga clic en **Bloquear siempre las notificaciones**.
5. Haga clic en **Guardar**.
6. Haga clic en **Siguiente** y, a continuación, en **Finalizar**.

Pegar

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

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

Enmascaramiento de datos personales

Habilite o deshabilite la redacción o el enmascaramiento de información de identificación personal (PII) en la aplicación web interna o SaaS con esta política cuando se accede a través de Citrix Enterprise Browser. La información de identificación personal puede ser números de tarjetas de crédito, números de seguro social, fechas, etc. También puede definir reglas personalizadas para detectar tipos específicos de información confidencial y enmascararlas en consecuencia. Las restricciones de enmascaramiento de datos personales también brindan una opción para enmascarar total o parcialmente la información.

> **Nota**
>
> Los usuarios finales deben utilizar Citrix Enterprise Browser versión 2405 o posterior para acceder a las aplicaciones para las que está habilitada esta restricción. De lo contrario, el acceso a la aplicación estará restringido.

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

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

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

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

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

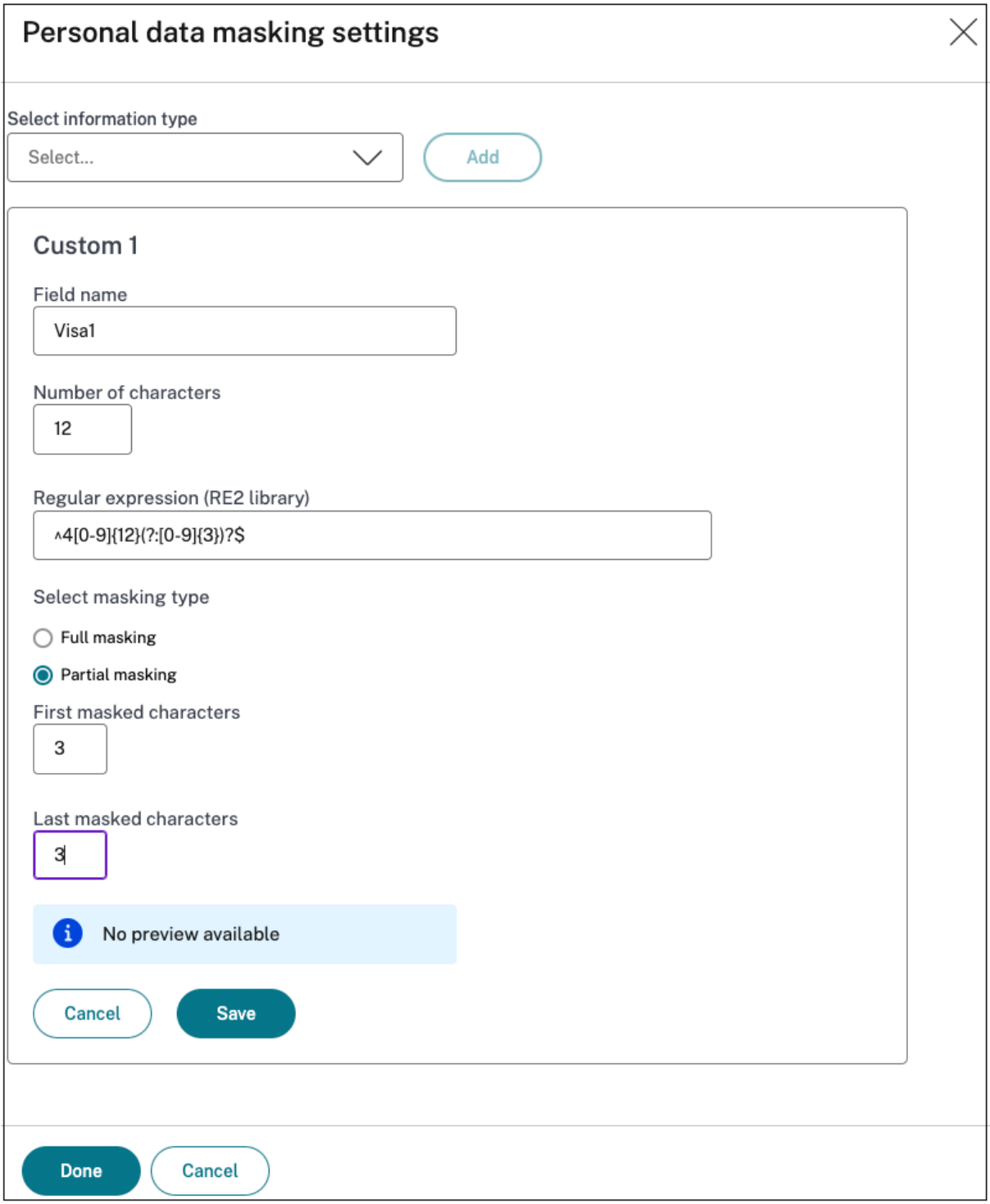
     El campo **Vista previa** muestra el formato de enmascaramiento. Esta vista previa no está disponible para políticas personalizadas.
6. Haga clic en **Guardar** y luego haga clic en **Listo**.
7. Haga clic en **Siguiente** y, a continuación, en **Finalizar**.

Agregar tipo de información personalizada

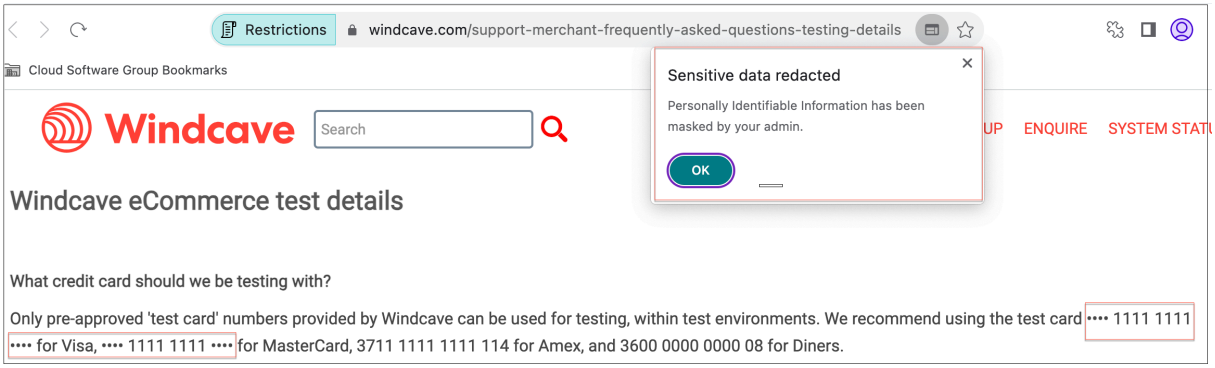
Puede agregar un tipo de información personalizado agregando la expresión regular del tipo de información.

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

7. Haga clic en **Siguiente** y, a continuación, en **Finalizar**.



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



Ventanas emergentes

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

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

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

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

Impresión

Habilite o deshabilite los datos de impresión desde las aplicaciones web internas o SaaS configuradas con esta política cuando se acceda a ellas a través del navegador Citrix Enterprise. Valor predeterminado: habilitado.

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

> **Nota**
>
> Si las restricciones **Impresión** y **Administración de impresoras** están habilitadas en una política, la restricción **Impresión** tiene prioridad sobre la restricción **Administración de impresoras** .

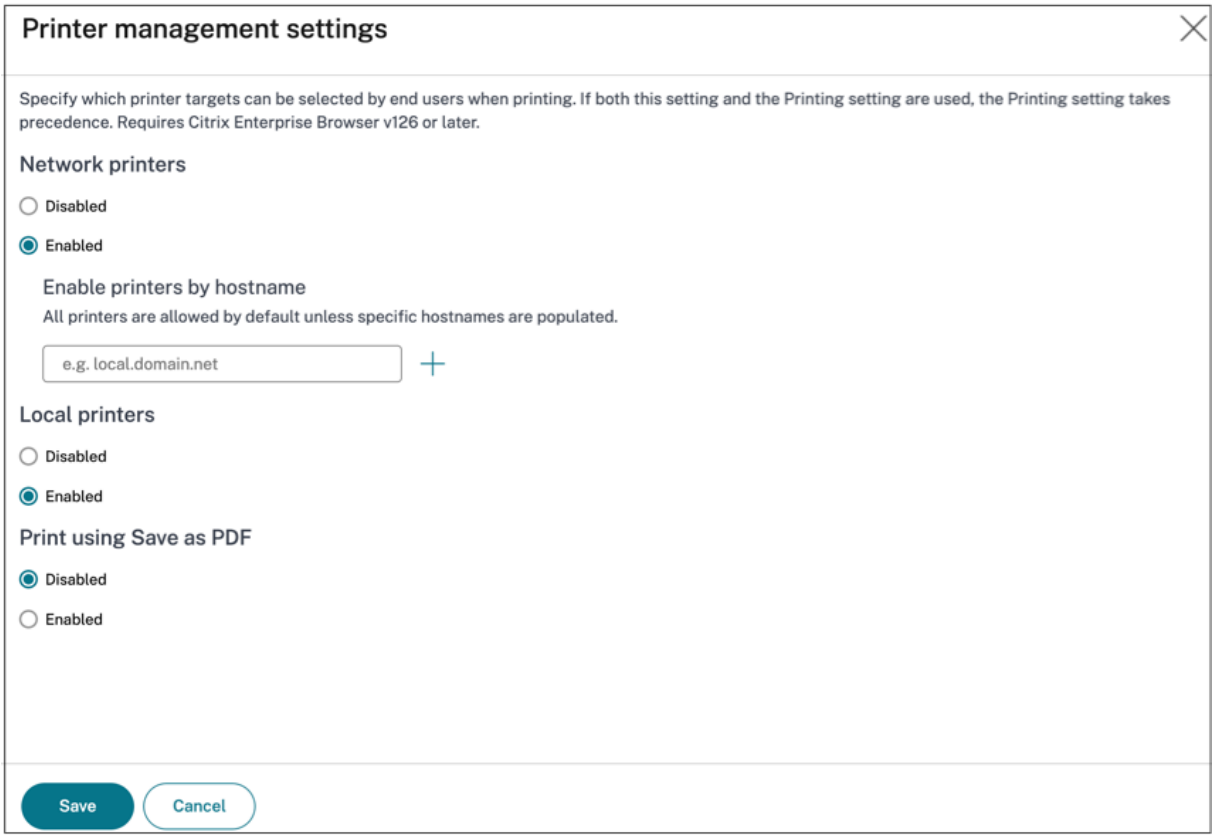
Administración de la impresora

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

> **Nota**
>
> - La restricción **Administración de impresora** está disponible además de la restricción **Impresión** donde la impresión está habilitada o deshabilitada. Si las restricciones **Impresión** y **Administración de impresoras** están habilitadas en una política de acceso, la restricción **Impresión** tiene prioridad sobre la restricción **Administración de impresoras** .
> - Los usuarios finales deben utilizar Citrix Enterprise Browser versión 2405 o posterior para acceder a las aplicaciones para las que está habilitada esta restricción. De lo contrario, el acceso a la aplicación estará restringido.

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

1. Crear o editar una política de acceso. Para obtener más detalles, consulte Crear políticas de acceso.
2. En la página **Paso 3: Acción** , seleccione **Permitir con restricciones**.
3. Haga clic en **Administración de impresoras** y luego haga clic en **Editar**.



1. Seleccione las excepciones según sus necesidades.

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

     - **Inhabilitado:** La impresión desde cualquier impresora de la red está inhabilitada.
     - **Habilitado:** La impresión desde todas las impresoras de la red está habilitada. Si se especifican nombres de host de impresora, se bloquearán todas las demás impresoras de red excepto las especificadas.

     Nota: Las impresoras de red se identifican por sus nombres de host.

   - **Impresoras locales** - Una impresora local es un dispositivo conectado directamente a una computadora individual a través de una conexión por cable. Esta conexión normalmente se facilita a través de USB, puertos paralelos u otras interfaces directas.

     - **Inhabilitado:** La impresión desde todas las impresoras locales está inhabilitada.
     - **Habilitado:** La impresión desde todas las impresoras locales está habilitada.

   - **Imprimir con Guardar como PDF**

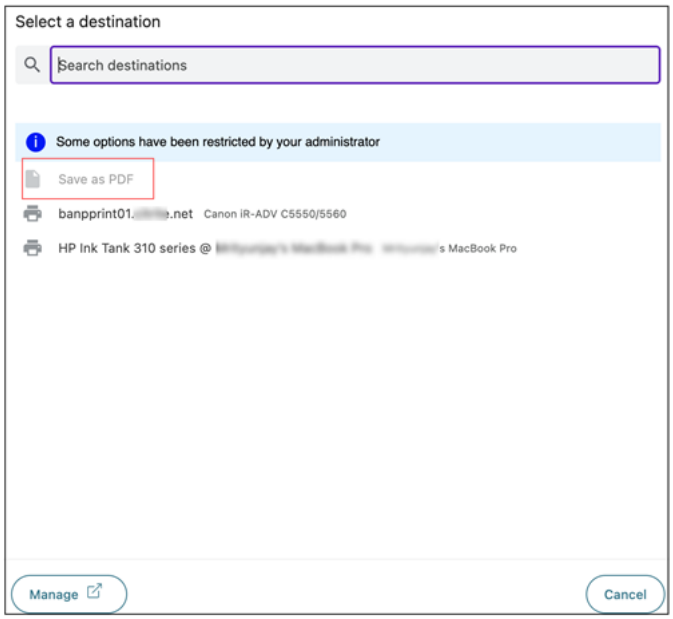
     - **Deshabilitado**: Guardar el contenido de la aplicación en formato PDF está deshabilitado.
     - **Habilitado:** Está habilitado guardar el contenido de la aplicación en formato PDF.

2. Haga clic en **Guardar**.
3. Haga clic en **Siguiente** y, a continuación, en **Finalizar**.

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

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

Si los usuarios finales cambian el nombre de las impresoras de red, no podrán utilizarlas.



Captura de pantalla

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

Restricción de carga por tipo de archivo

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

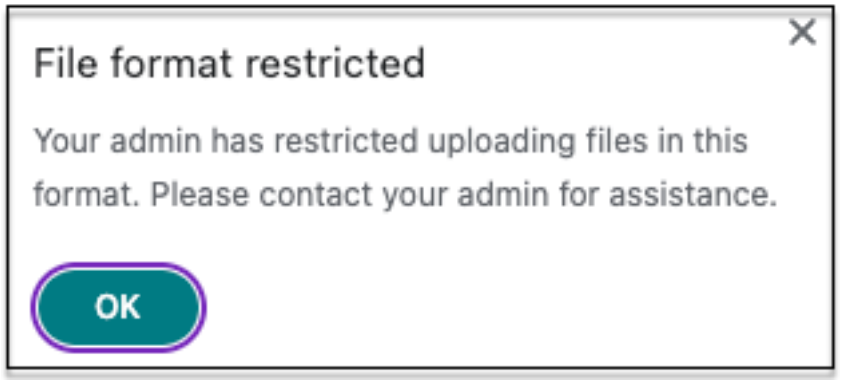
> **Nota**
>
> - La restricción de carga **por tipo de archivo** está disponible además de la restricción de carga ** .
> - Si las restricciones **Cargar** y **Cargar por tipo de archivo** están habilitadas en una política, la restricción **Cargar** tiene prioridad sobre la restricción **Cargar por tipo de archivo** .
> - Los usuarios finales deben utilizar Citrix Enterprise Browser versión 2405 o posterior para acceder a las aplicaciones para las que está habilitada esta restricción. De lo contrario, el acceso a la aplicación estará restringido.

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

1. Crear o editar una política de acceso. Para obtener más detalles, consulte Crear políticas de acceso.
2. En la página **Paso 3: Acción** , seleccione **Permitir con restricciones**.
3. Haga clic en **Restricción de carga por tipo de archivo** y luego haga clic en **Editar**.
4. En la página **Configuración de restricción de carga por tipo de archivo** , seleccione una de las siguientes opciones:
   - **Permitir todas las cargas con excepciones** –Cargar todos los archivos excepto los tipos seleccionados.
   - **Bloquea todas las cargas con excepciones** –Bloquea la carga de todos los tipos de archivos, excepto los tipos seleccionados.
5. Si el tipo de archivo no existe en la lista, haga lo siguiente:
   a) Haga clic en **Agregar tipos MIME personalizados**.
   b) En **Agregar tipos MIME**, ingrese el tipo MIME en el formato `categoría/subcategoría<extension>`. Por ejemplo `imagen/png`.
   c) Haga clic en **Listo**.
   d) Haga clic en **Siguiente** y, a continuación, en **Finalizar**.

   El tipo MIME ahora aparece en la lista de excepciones.

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



Subidas

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

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

Marca de agua

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

Cámara web

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

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

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

1. Crear o editar una política de acceso. Para obtener más detalles, consulte Crear políticas de acceso.
2. En la página **Paso 3: Acción** , seleccione **Permitir con restricciones**.
3. Haga clic en **Cámara web** y luego haga clic en **Editar**.

4. En la página **Configuración de la cámara web** , haga clic en **Permitir siempre el acceso**.
5. Haga clic en **Guardar**.
6. Haga clic en **Siguiente** y, a continuación, en **Finalizar**.

> **Nota**
>
> - Si la restricción **Cámara web** está habilitada en la política de acceso privado seguro, Citrix Enterprise Browser muestra la configuración **Permitir**.
> - Si la opción **Preguntar cada vez que** está habilitada en la política de acceso privado seguro, la configuración aplicada en Citrix Enterprise Browser varía dependiendo de si se utiliza el servicio de configuración global de aplicaciones (GACS) para administrar Citrix Enterprise Browser.
> - Si se utiliza GACS, la configuración de GACS se aplica en Citrix Enterprise Browser.
> - Si no se utiliza GACS, Citrix Enterprise Browser muestra la configuración **Preguntar**.

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

Restricción del portapapeles para grupos de seguridad

Puede restringir el acceso al portapapeles a cualquier grupo designado de aplicaciones. Estos grupos designados de aplicaciones se crean como grupos de seguridad para que los usuarios finales puedan copiar y pegar contenidos solo dentro de esos grupos de seguridad. Para habilitar el acceso al portapapeles dentro de las aplicaciones de un grupo de seguridad, solo debe tener una política de acceso configurada con la acción **permitir** o **permitir con restricciones** sin seleccionar ninguna configuración de acceso.

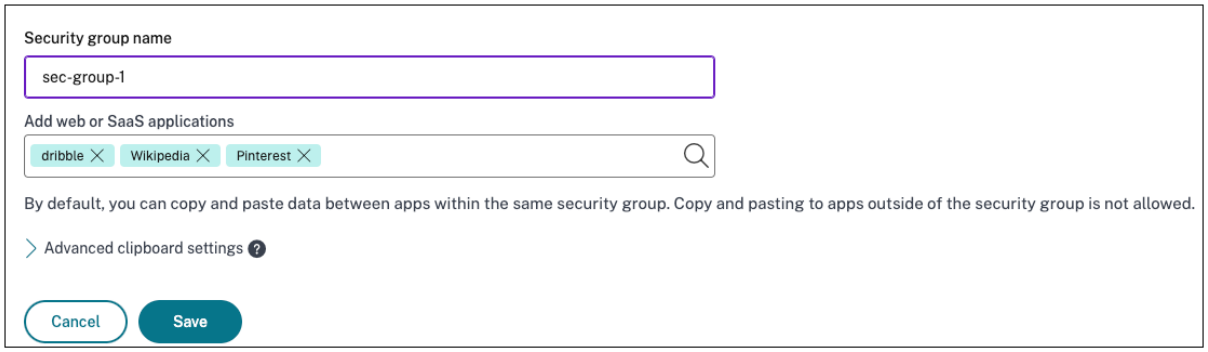
- Cuando la restricción **Grupos de seguridad** está habilitada, no puedes copiar/pegar datos entre aplicaciones en diferentes grupos de seguridad. Por ejemplo, si la aplicación “ProdDocs” pertenece al grupo de seguridad “SG1”y la aplicación “Edocs”pertenece al grupo de seguridad “SG2”, no puede copiar/pegar contenido de “Edocs”a “ProdDocs”incluso si la restricción **Copiar / Pegar** está habilitada para ambos grupos.
- Para las aplicaciones que no forman parte de un grupo de seguridad, puedes crear una política de acceso con la acción **permitir con restricciones** y seleccionar las restricciones (**Copiar**, **Pegar**o **Portapapeles**). En este caso, la aplicación no es parte de un grupo de seguridad y se puede aplicar la restricción **Copiar / Pegar** en esa aplicación.

> **Nota**
>
> También puede restringir el acceso al portapapeles para las aplicaciones a las que se accede a través de Citrix Enterprise Browser mediante el servicio de configuración global de aplicaciones

> (GACS). Si está utilizando GACS para administrar Citrix Enterprise Browser, utilice la opción **Portapapeles en espacio aislado habilitado** para administrar el acceso al portapapeles. Cuando restringe el acceso al portapapeles a través de GACS, se aplica a todas las aplicaciones a las que se accede a través de Citrix Enterprise Browser.

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

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

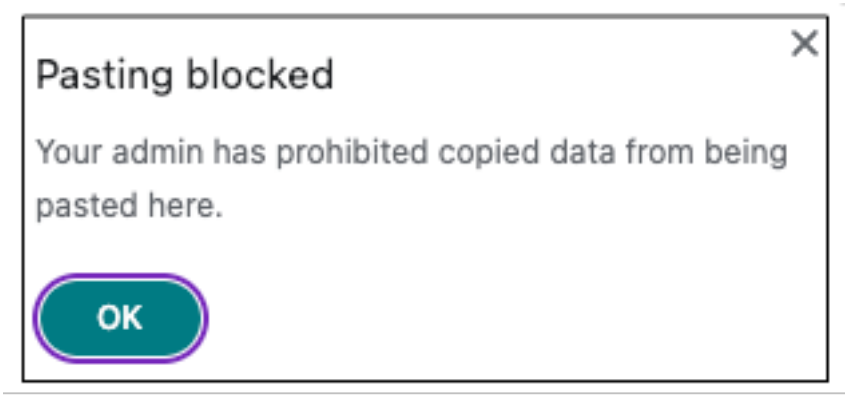


1. Introduzca un nombre para el grupo de seguridad.
2. En **Agregar aplicaciones web o SaaS**, elija las aplicaciones que desea agrupar para habilitar el control de copiar y pegar. Por ejemplo, Wikipedia, Pinterest y Dribble.
3. Haga clic en **Guardar**.

Para obtener más información sobre **Portapapeles avanzado** Configuración, consulte Habilitación de controles de copiar y pegar para aplicaciones nativas y aplicaciones no publicadas.

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

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



> **Nota**
>
> Puede copiar y pegar el contenido entre las aplicaciones de un grupo de seguridad y otras aplicaciones locales en las máquinas o aplicaciones web no publicadas mediante las opciones en **Configuración avanzada del portapapeles**. Para obtener más detalles, consulte Habilitar controles de copiar/pegar para aplicaciones nativas y aplicaciones no publicadas.

Habilitar el acceso al portapapeles a nivel granular

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

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

Ejemplo:

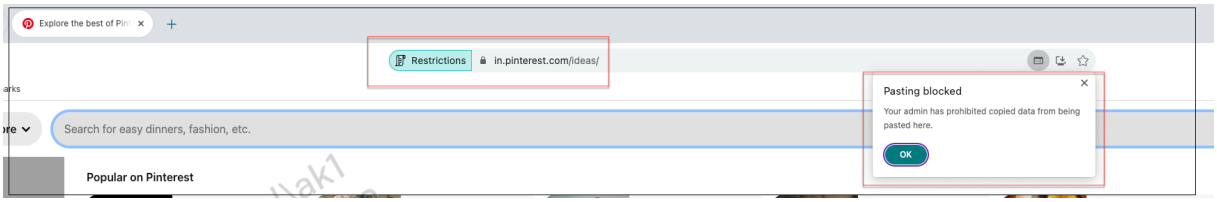
Considere que ha creado un grupo de seguridad con tres aplicaciones, a saber, Wikipedia, Pinterest y Dribble.

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

1. Crear o editar una política de acceso asignada para la aplicación `Pinterest`. Para obtener detalles sobre la creación de una política de acceso, consulte Crear políticas de acceso.
2. En la página **Paso 3: Acción** , seleccione **Permitir con restricciones**.
3. Seleccionar **Pegar**.

Aunque Pinterest es parte de un grupo de seguridad que también contiene Wikipedia y Dribble, los usuarios no pueden copiar contenido de Wikipedia o Dribble a Pinterest debido a la política de acceso

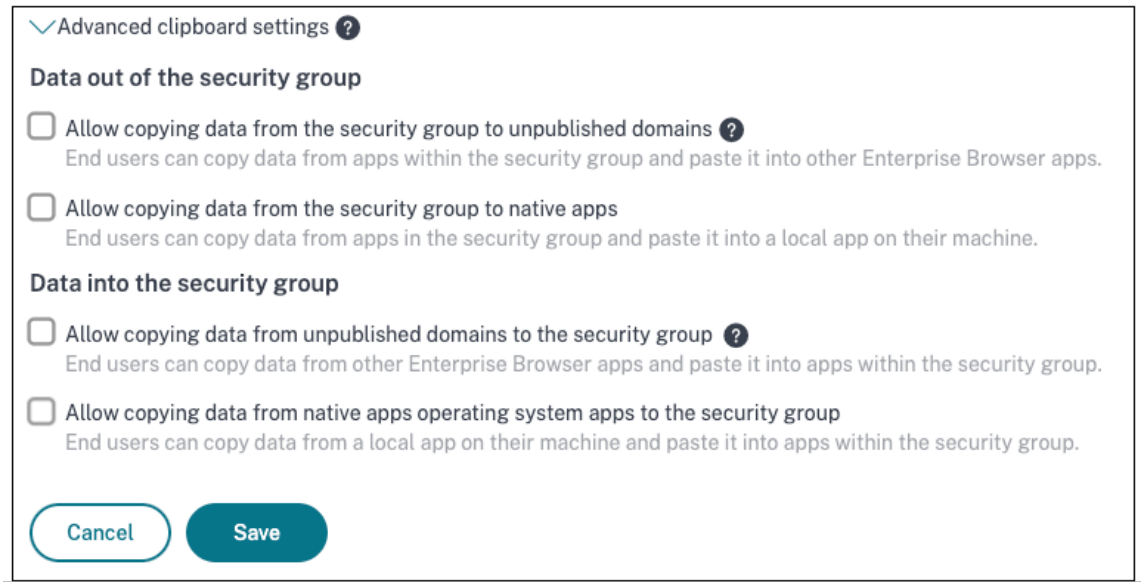
asociada con Pinterest en la que la restricción **Pegar** está deshabilitada.



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

Puede copiar y pegar el contenido entre las aplicaciones de un grupo de seguridad y otras aplicaciones locales en las máquinas o aplicaciones web no publicadas mediante las opciones en **Configuración avanzada del portapapeles**

1. Crear un grupo de seguridad. Para obtener más detalles, consulte Crear grupos de seguridad.
2. Expandir **Configuración avanzada del portapapeles**.



3. Seleccione cualquiera de las siguientes opciones según sus necesidades:

   - **Permitir la copia de datos del grupo de seguridad a dominios no publicados** –Habilitar la copia de datos de las aplicaciones en los grupos de seguridad a las aplicaciones que no están publicadas en Secure Private Access.
   - **Permitir la copia de datos del grupo de seguridad a aplicaciones nativas** - Habilite la copia de datos de las aplicaciones en los grupos de seguridad a las aplicaciones locales en sus máquinas.
   - **Permitir la copia de datos de los dominios no publicados al grupo de seguridad** –Habilitar la copia de datos de las aplicaciones no publicadas a través del acceso privado seguro a las aplicaciones en los grupos de seguridad.

- **Permitir la copia de datos desde aplicaciones nativas del sistema operativo del grupo de seguridad** - Habilitar la copia de datos desde aplicaciones locales en las máquinas a las aplicaciones.

Problemas conocidos

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

  Por ejemplo, supongamos el siguiente escenario:

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

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

- Para una aplicación SaaS, se puede denegar el acceso a la aplicación si la aplicación está configurada con una política de acceso con la acción **Denegar acceso.** Los usuarios finales aún pueden acceder a la aplicación porque el tráfico de la aplicación no se canaliza a través del acceso privado seguro. Además, si la aplicación es parte del grupo de seguridad, las configuraciones del grupo de seguridad no se respetan y, por lo tanto, no se puede copiar/pegar contenido de la aplicación.

Herramienta de modelado de políticas

October 21, 2024

Tener varias aplicaciones y varias políticas de acceso puede dificultar que los administradores comprendan el resultado exacto del acceso a la aplicación por parte del usuario final, es decir, si al usuario final se le permite o se le niega el acceso a una aplicación en función de todas las configuraciones.

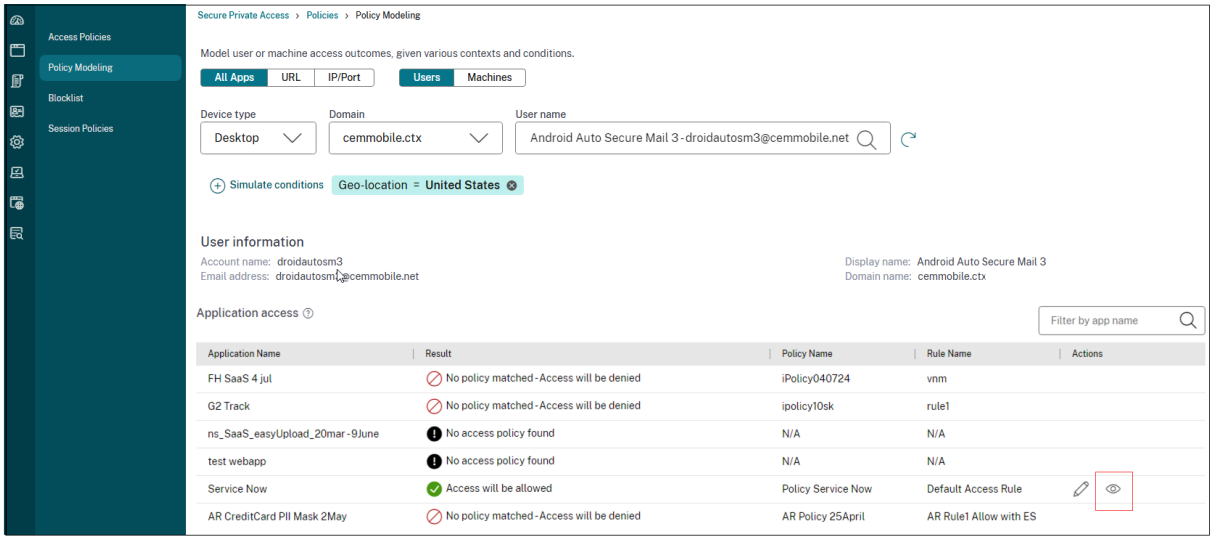
La herramienta de modelado de políticas (A**políticas de acceso > Modelado de políticas**) resuelve este problema al brindarles a los administradores visibilidad completa de los resultados de acceso a

la aplicación esperados (permitido/permitido con restricción/denegado) en función de sus configuraciones existentes. Los administradores pueden verificar los resultados de acceso de cualquier usuario en función de las condiciones del usuario, como el tipo de dispositivo, la postura del dispositivo, la ubicación geográfica, la ubicación de la red, la puntuación de riesgo del usuario y la URL del espacio de trabajo.

Para analizar la configuración de la política de acceso, realice los siguientes pasos.

1. En la consola de acceso privado seguro, haga clic en **Políticas de acceso** y luego haga clic en la pestaña **Modelado de políticas** .
2. Añade los siguientes detalles:
    - **Tipo de dispositivo**: Seleccione el tipo de dispositivo del usuario final. (**Escritorio** está seleccionado de forma predeterminada).
    - **Dominio**: Seleccione el dominio asociado con el usuario.
    - **Usuario**: Seleccione el nombre de usuario para el cual desea analizar las aplicaciones y las políticas asociadas.
3. También puede simular un conjunto de condiciones/restricciones en el usuario final y sus dispositivos. >**Nota:** > >Agregue las condiciones de usuario exactas para obtener resultados precisos.
4. Haga clic en **para simular condiciones**.
5. Seleccione la condición (Postura del dispositivo, Geolocalización, Ubicación de la red, Puntuación de riesgo del usuario y URL del espacio de trabajo) y luego seleccione el valor asociado.
6. Haga clic en el signo **+** para agregar más condiciones.
7. Haga clic en **Aplicar**.

Las aplicaciones, las políticas asociadas y las reglas para el usuario seleccionado se muestran en formato tabular.



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.

Compatibilidad con aplicaciones web empresariales

October 21, 2024

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

Se puede acceder a aplicaciones web mediante Citrix Workspace mediante el servicio Secure Private Access. El servicio de acceso privado seguro junto con Citrix Workspace proporciona una experiencia de usuario unificada para las aplicaciones web configuradas, aplicaciones SaaS, 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:

- Estándar de acceso privado seguro
- Secure Private Access Advanced

Requisitos del sistema

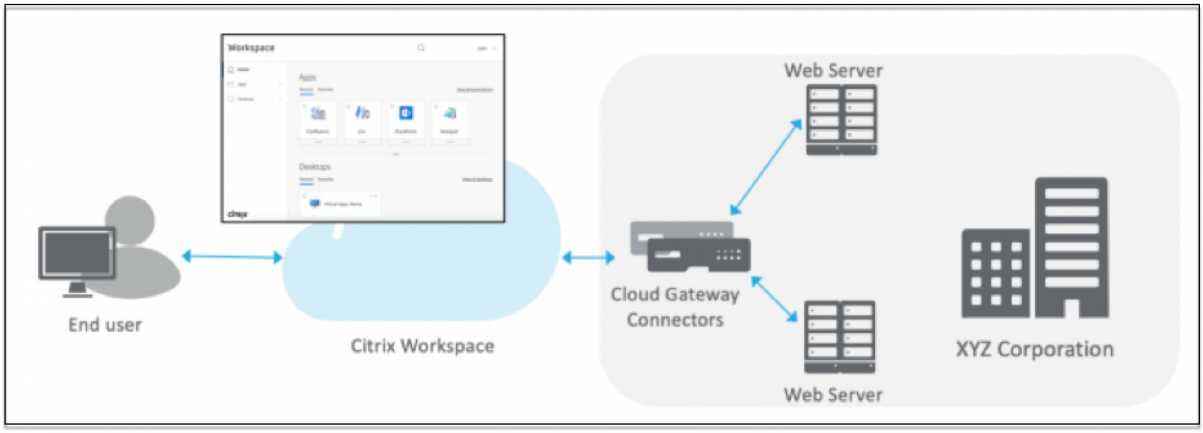
Dispositivo conector : utilice el dispositivo conector con el servicio Citrix Secure Private Access para admitir el acceso sin VPN a las aplicaciones web empresariales en el centro de datos de los clientes. Para obtener más detalles, consulte Acceso seguro al espacio de trabajo con el dispositivo Connector.

Funcionamiento

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

Una conexión TLS entre el dispositivo conector y el servicio Citrix Secure Private Access 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 utilizando una conexión sin VPN.

La siguiente figura ilustra el acceso a 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. Establecer el método de inicio de sesión preferido
3. Definir el enrutamiento de la aplicación

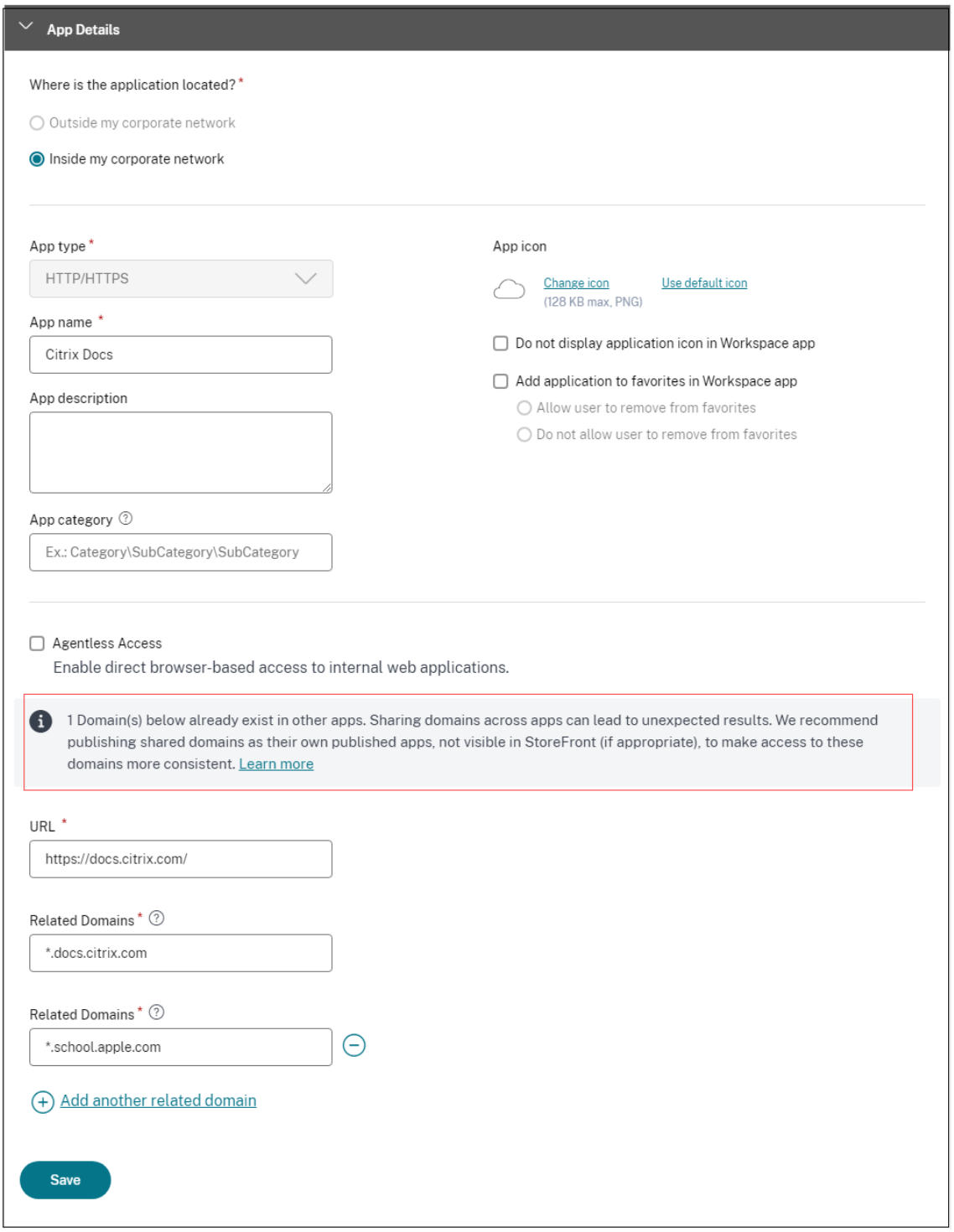
Configurar los detalles de la aplicación

1. En el mosaico **Acceso privado seguro** , haga clic en **Administrar.**
2. En la página de inicio de Acceso privado seguro, haga clic en **Continuar** y luego haga clic en **Agregar una aplicación.**

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

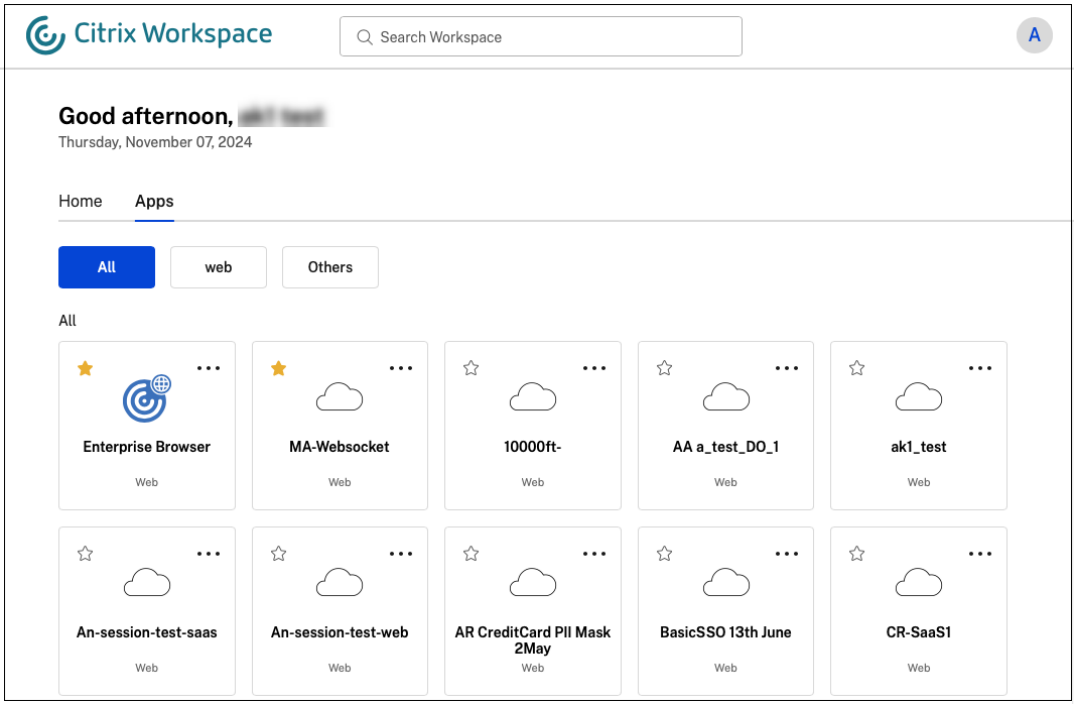
cación.

1. Seleccione la aplicación que desea agregar y haga clic en **Omitir.**
2. En **¿Dónde está la ubicación de la aplicación?**, seleccione la ubicación.
3. Ingresa los siguientes detalles en la sección **Detalles de la aplicación** y haz clic en **Siguiente.**



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

    Por ejemplo, si introduce el parámetro **Negocios y Productividad** categoría incorrectamente como **Negocio y productividad** En **Categoría de aplicación** campo, entonces una nueva categoría llamada **Negocio y productividad** aparece en la interfaz de usuario de Citrix Workspace, además de la **Negocios y productividad** categoría.



- **Ícono de la aplicación** –Haga clic en **Cambiar ícono** para cambiar el ícono de la aplicación. El tamaño del archivo del icono debe ser de 128x128 píxeles. Si no cambia el icono, se mostrará el icono predeterminado.

```
If you do not want to display the app icon, select **Do not
   display application icon to users.**
```

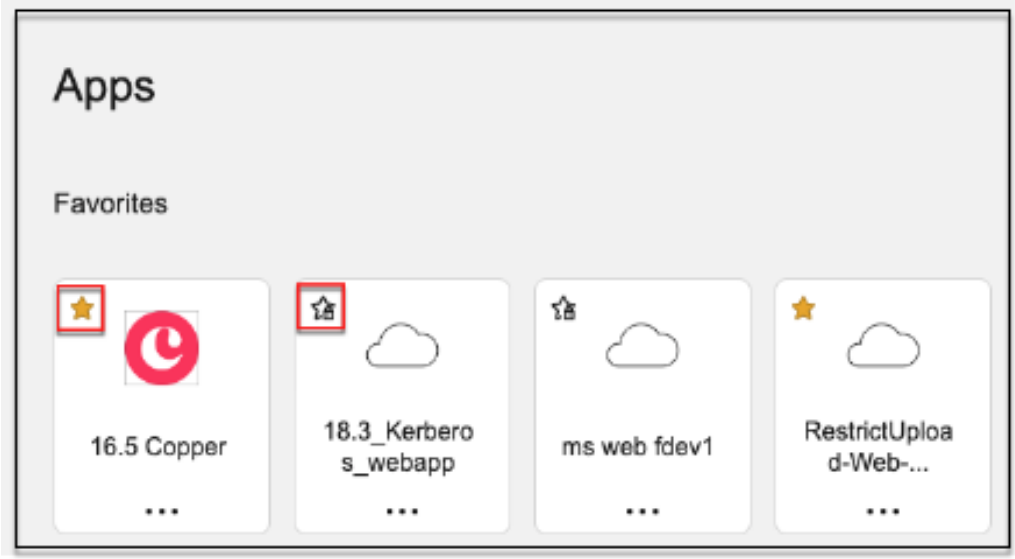
- Seleccione **Acceso directo** para permitir que los usuarios accedan a la aplicación directamente desde un navegador del cliente. Para obtener más detalles, consulte Acceso directo a aplicaciones web empresariales.
- **URL** –URL con su ID de cliente. La URL debe contener su ID de cliente (ID de cliente de Citrix Cloud). Para obtener su ID de cliente, consulte Registrarse en Citrix Cloud. En caso de que el SSO falle o no desee utilizarlo, el usuario será redirigido a esta URL.

```
**Customer domain name** and **Customer domain ID** -
   Customer domain name and ID are used to create the app URL
    and other subsequent URLs in the SAML SSO page.

For example, if you're adding a Salesforce app, your domain
   name is `salesforceformyorg` and ID is 123754, then the
   app URL is `https://salesforceformyorg.my.salesforce.com/?
   so=123754.`

Customer domain name and Customer ID fields are specific to
   certain apps.
```

- **Dominios relacionados** –El dominio relacionado se completa automáticamente según la

URL que usted proporcionó. El dominio relacionado ayuda al servicio a identificar la URL como parte de la aplicación y 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 que el usuario elimine de favoritos** para permitir que los suscriptores de la aplicación eliminen la aplicación de la lista de aplicaciones favoritas en la aplicación Citrix Workspace. Cuando selecciona esta opción, aparece un ícono de estrella amarilla en la esquina superior izquierda de la aplicación en la aplicación Citrix Workspace.
  - 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 en la aplicación Citrix Workspace. Cuando selecciona esta opción, aparece un ícono de estrella con un candado en la esquina superior izquierda de la aplicación Citrix Workspace.



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

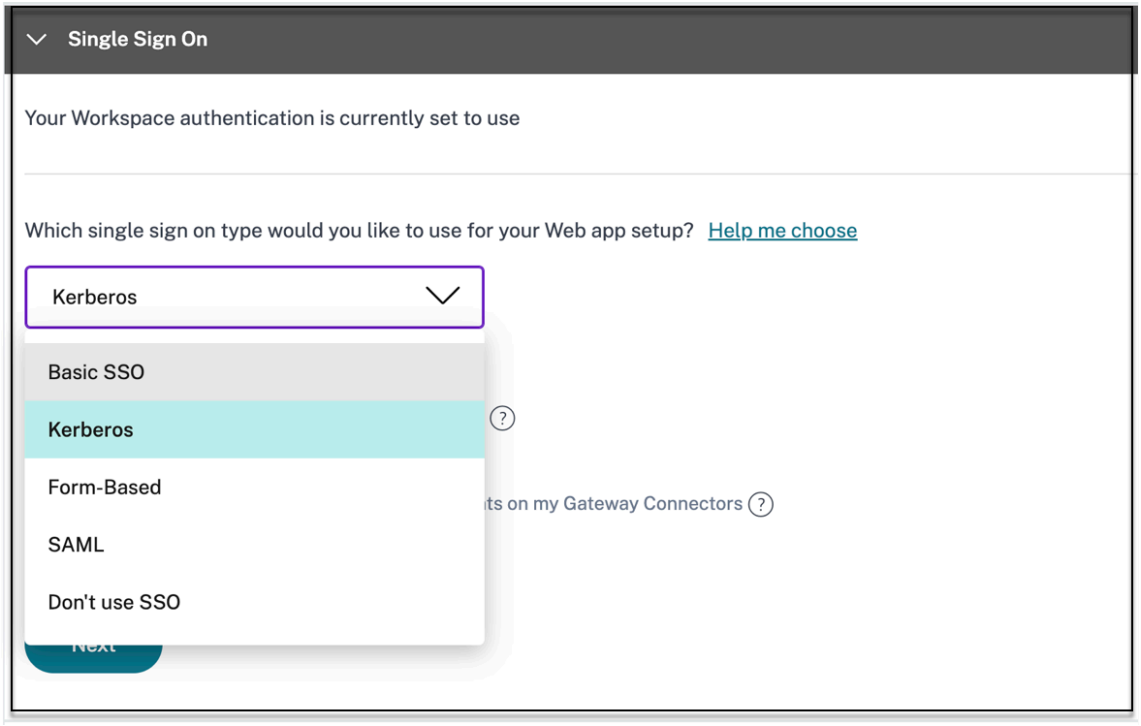
4. Haga clic en **Siguiente.**

> **Importante:**
>
> - Para permitir el acceso basado en confianza cero a las aplicaciones, se les niega el acceso de forma predeterminada. El acceso a las aplicaciones solo está habilitado si hay una política

> de acceso asociada a la aplicación. Para obtener más detalles, consulte Acceso denegado a las aplicaciones, de forma predeterminada.
> - Si se configuran varias aplicaciones con el mismo FQDN o alguna variación del FQDN comodín, esto podría generar una configuración conflictiva. Para obtener más detalles, consulte Configuración conflictiva que podría generar problemas de acceso a la aplicación.

Establecer el método de inicio de sesión preferido

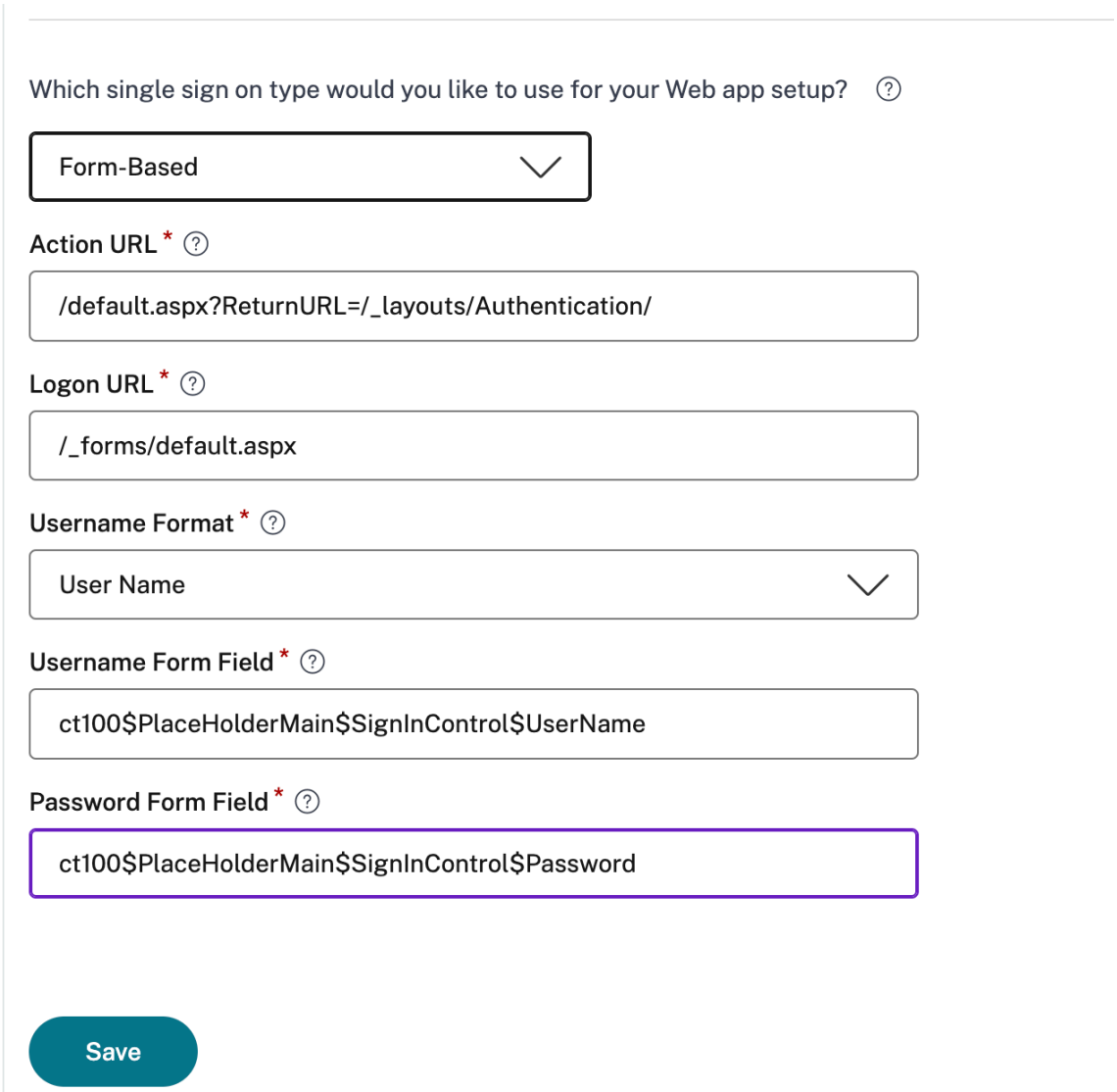
1. En la sección **Inicio de sesión único** , seleccione el tipo de inicio de sesión único que prefiera utilizar para su aplicación y haga clic en **Guardar.** Están disponibles los siguientes tipos de inicio de sesión único.



- **Básico** –Si su servidor back-end le presenta un desafío básico 401, elija **SSO básico**. No es necesario proporcionar 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 proporcionar ningún detalle de configuración para el tipo SSO **Kerberos** .
- **Basado en formulario** –Si su servidor back-end le presenta un formulario HTML para la autenticación, elija **Basado en formulario**. Ingrese los detalles de configuración para el tipo de SSO basado en formulario ** .
- **SAML** - Elija **SAML** para SSO basado en SAML en aplicaciones web. Ingrese los detalles de configuración para el tipo de SSO **SAML** .
- **No usar SSO** –Utilice 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** , el usuario es redirigido

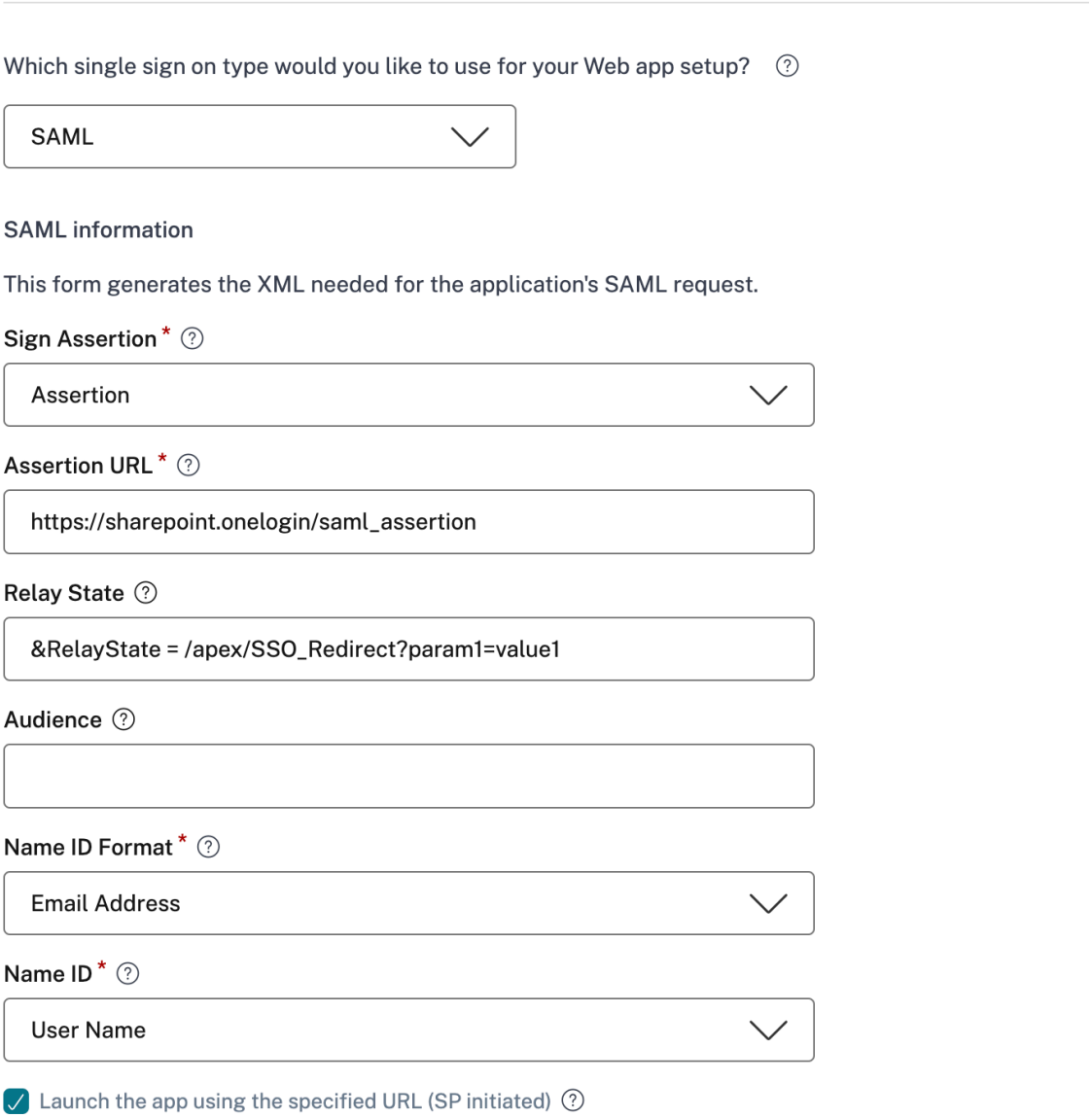
a la URL configurada en la sección **Detalles de la aplicación** .

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



- **URL de acción** - Escriba la URL a la que se envía el formulario completo.
- **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: Ingrese los siguientes detalles en la sección Iniciar sesión y haga clic en Guardar.



- **Firmar afirmación** - Firmar una afirmación o respuesta garantiza la integridad del mensaje cuando la respuesta o afirmación se entrega a la parte confiada (SP). Puede seleccionar **Afirmación, Respuesta, Ambas,** o **Ninguna**.
- **URL de afirmación** : la URL de afirmación la proporciona el proveedor de la aplicación. La aserción SAML se envía a esta URL.
- **Estado del relé** –El parámetro Estado del relé se utiliza para identificar el recurso específico al que acceden los usuarios después de iniciar sesión y ser dirigidos al servidor de federación de la parte confiada. 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** –La audiencia la proporciona el proveedor de la aplicación. Este valor confirma que la afirmación SAML se genera 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)** agrega información adicional sobre el usuario que se envía a la aplicación para decisiones de control de acceso.
3. Descargue el archivo de metadatos haciendo clic en el enlace debajo de **Metadatos SAML.** Utilice el archivo de metadatos descargado para configurar SSO en el servidor de aplicaciones SaaS.

> **Nota**
>
> - Puede copiar la URL de inicio de sesión de SSO en **URL de inicio de sesión** y usar esta URL al configurar SSO en el servidor de aplicaciones SaaS.
> - También puede descargar el certificado de la lista **Certificado** y usar el certificado al configurar SSO en el servidor de aplicaciones SaaS.

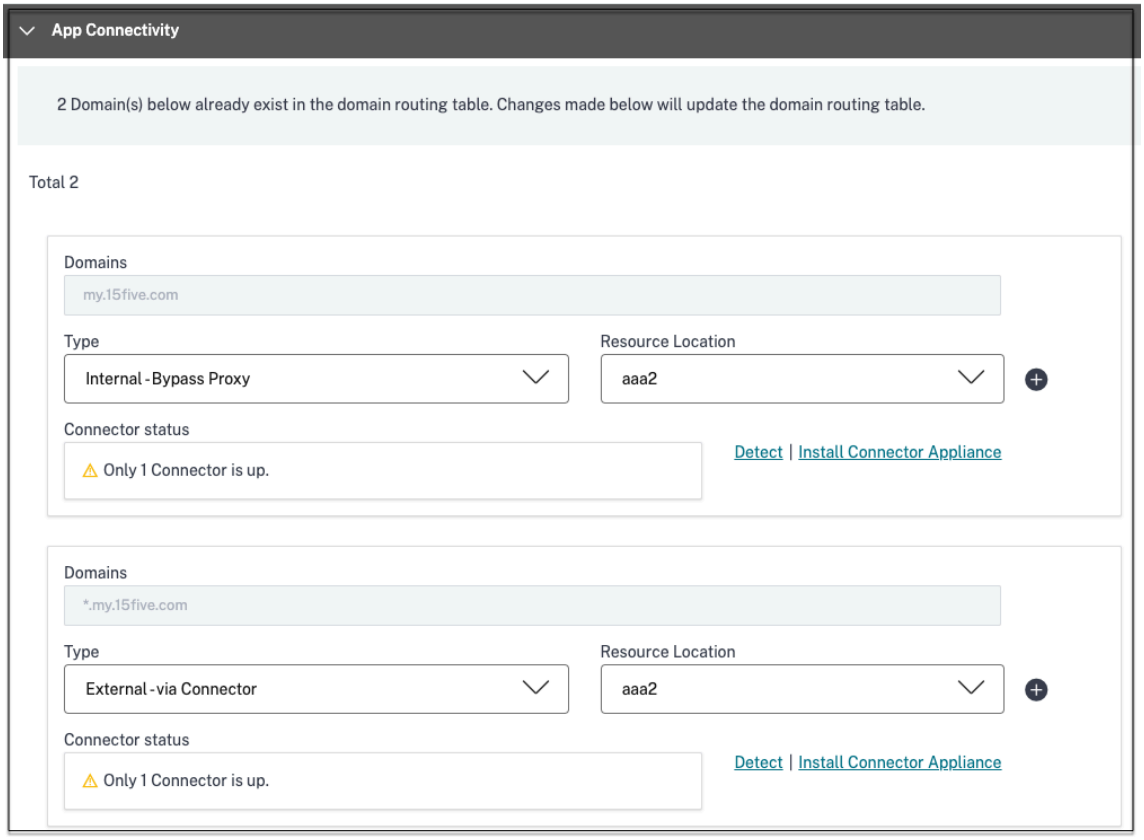
1. Haga clic en **Siguiente.**

Definir el enrutamiento de la aplicación

1. En la sección **Conectividad de aplicaciones** , se define el enrutamiento para los dominios relacionados de las aplicaciones, si los dominios se deben enrutar externa o internamente a través de Citrix Connector Appliance.

   - **Interno: omitir proxy** : el tráfico del dominio se enruta a través de Citrix Cloud Connector, sin pasar por el proxy web del cliente configurado en el dispositivo Connector.
   - **Interno a través del conector** : las aplicaciones pueden ser externas, pero el tráfico debe fluir a través del dispositivo conector hacia la red externa.
   - **Externo** –El tráfico fluye directamente a Internet.

   Para obtener más detalles, consulte Tablas de ruta para resolver conflictos si los dominios relacionados en las aplicaciones web y SaaS son los mismos.

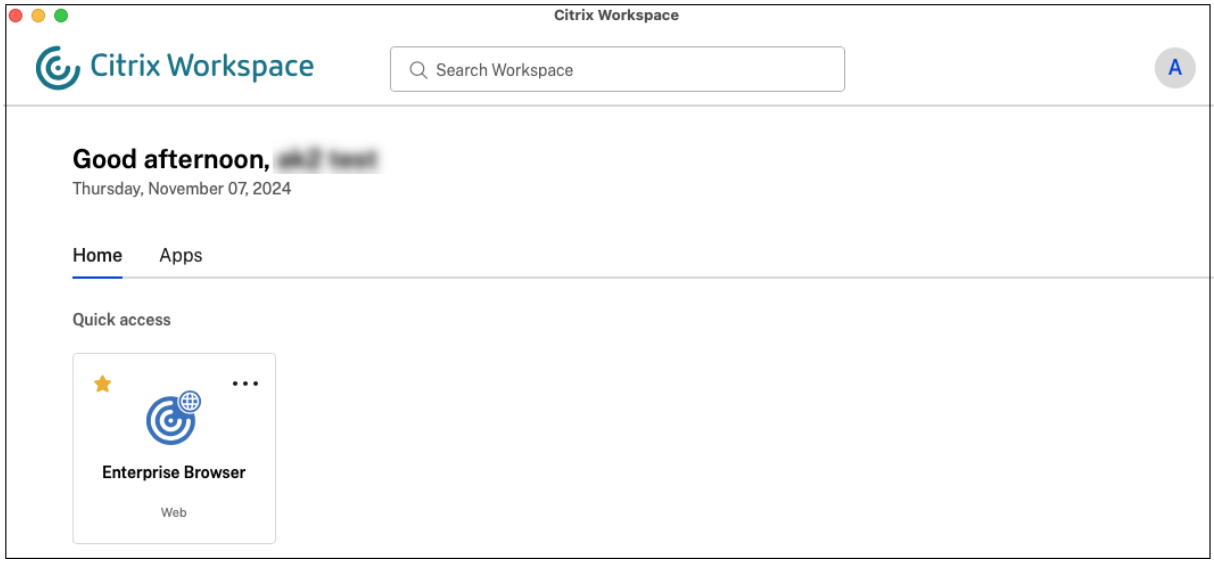


2. Haga clic en **Finalizar.**

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

   - **Editar aplicación**
   - **Eliminar**

Cuando publica 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 navegador del espacio de trabajo sin una URL y acceder a sitios web internos mediante los navegadores del espacio de trabajo.



Importante:

- Para otorgar acceso a las aplicaciones a los usuarios, los administradores deben crear políticas de acceso. En las políticas de acceso, los administradores agregan suscriptores de aplicaciones y configuran controles de seguridad. Para obtener más detalles, consulte Crear políticas de acceso.

Acceso directo a aplicaciones web empresariales

October 21, 2024

Ahora se puede acceder directamente desde el navegador del cliente a aplicaciones web empresariales como SharePoint, JIRA, Confluence y otras alojadas por el cliente en sus instalaciones o en nubes públicas. 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 enlaces desde sus correos electrónicos, herramientas de colaboración o marcadores del navegador. De esta manera, se proporciona a los clientes una verdadera solución de huella cero.

Funcionamiento

- Agregue un nuevo registro DNS 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 de la aplicación web empresarial configurada para redirigir al usuario al servicio Citrix Secure Private Access.
- Cuando el usuario final inicia el acceso a la aplicación web empresarial configurada, el tráfico de la aplicación se dirige al servicio Citrix Secure Private Access, que luego actuará como proxy del acceso a la aplicación.
- Una vez que la solicitud llega al servicio Citrix Secure Private Access, este verifica la autenticación del usuario y la autorización de la aplicación, incluidas las verificaciones de las políticas de acceso contextual.
- Tras una validación exitosa, el servicio Citrix Secure Private Access se comunica con los dispositivos Citrix Cloud Connector, implementados en el entorno del cliente (ya sea localmente o en la nube) para permitir el acceso a la aplicación web empresarial configurada.

Configurar Citrix Secure Private Access para acceder directamente a las aplicaciones web empresariales

Requisitos previos

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

- FQDN de la aplicación
- Certificado SSL: certificado público para la aplicación que se va a configurar
- Ubicación de recursos: instalación de dispositivos Citrix Cloud Connector
- 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 una configuración completa de extremo a extremo de una aplicación, consulte 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** aparece solo la primera vez que utiliza el asistente. En los usos posteriores, puedes navegar directamente a la página **Aplicaciones** y, luego, hacer clic en **Agregar una aplicación**.

1. Configurar identidad y autenticación. Para obtener más detalles, consulte Flujo de trabajo guiado por el administrador para una fácil incorporación y configuración.

2. Proceda a agregar una aplicación. Para obtener más detalles, consulte Agregar y administrar aplicaciones.
3. Seleccione la aplicación que desea agregar y haga clic en **Omitir.**
4. En **¿Dónde está la ubicación de la aplicación?**, seleccione la ubicación.
5. Ingrese 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 ingresa aquí se muestra a sus usuarios en el espacio de trabajo.
    - **Ícono de la aplicación** –Haga clic en **Cambiar ícono** para cambiar el ícono de la aplicación. El tamaño del archivo del icono debe ser de 128x128 píxeles. Si no cambia el icono, se mostrará el icono predeterminado.

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

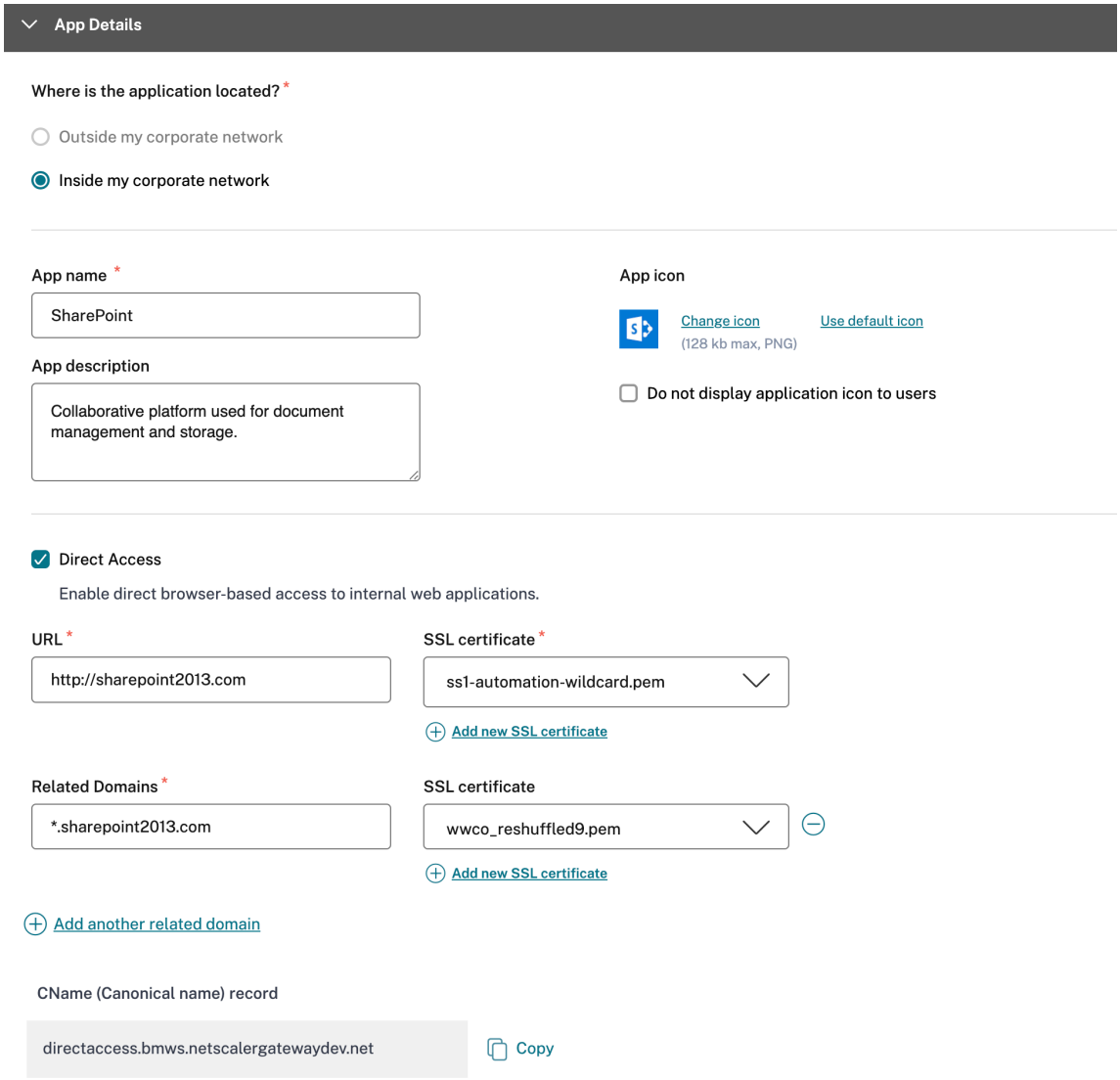
6. Seleccione **Acceso directo** para permitir que los usuarios accedan a la aplicación directamente desde un navegador del cliente. Introduzca los siguientes detalles.

    - **URL** –URL para la aplicación back-end. La URL debe estar en formato HTTPS y el administrador debe agregar una entrada DNS correspondiente.
    - **Certificado SSL** –Seleccione un certificado SSL existente en el menú desplegable o agregue un nuevo certificado SSL haciendo clic en **Agregar nuevo certificado SSL**.

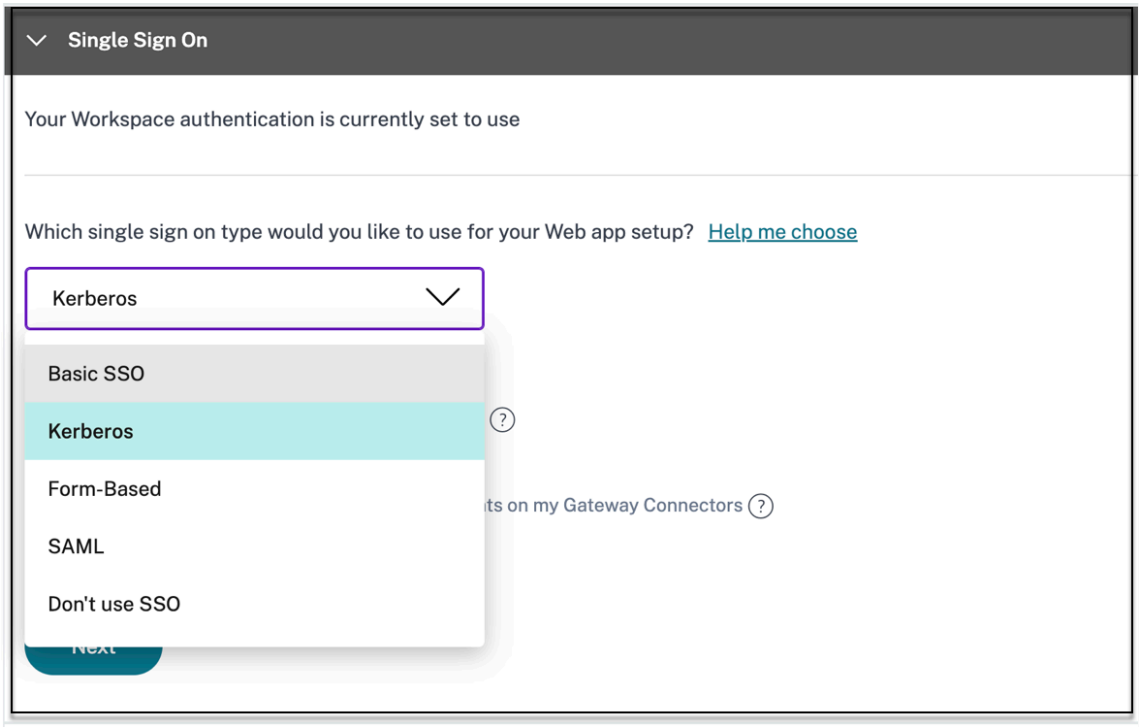
      Puntos que tener en cuenta:

        - Solo se admite un certificado CA público o de confianza. No se admiten certificados autofirmados.
        - Se debe cargar una cadena completa de certificados.

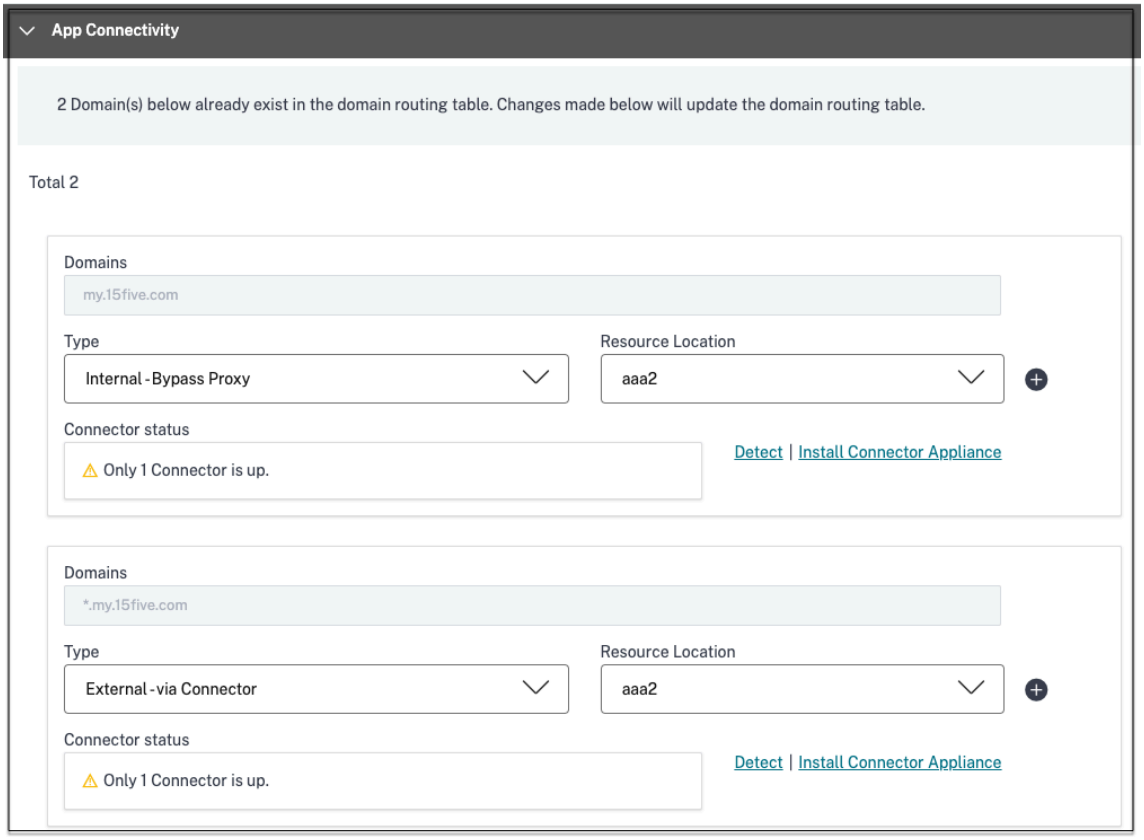
    - **Dominios relacionados** –El dominio relacionado se completa automáticamente según la URL que usted proporcionó. El dominio relacionado ayuda al servicio a identificar la URL como parte de la aplicación y dirigir el tráfico en consecuencia. Puede agregar más de un dominio relacionado. Puede vincular 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 ingresar en el DNS para habilitar el acceso directo a la aplicación.



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



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



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

    - **Editar aplicación**
    - **Eliminar**

> **Importante:**
>
> - Para permitir el acceso basado en confianza cero a las aplicaciones, se les niega el acceso de forma predeterminada. El acceso a las aplicaciones solo está habilitado si hay una política de acceso asociada a la aplicación. Para obtener detalles sobre la creación de políticas de acceso, consulte Crear políticas de acceso.
> - Si se configuran varias aplicaciones con el mismo FQDN o alguna variación del FQDN comodín, esto podría generar una configuración conflictiva. Para evitar configuraciones conflictivas, consulte Mejores prácticas para configuraciones de aplicaciones web y SaaS.

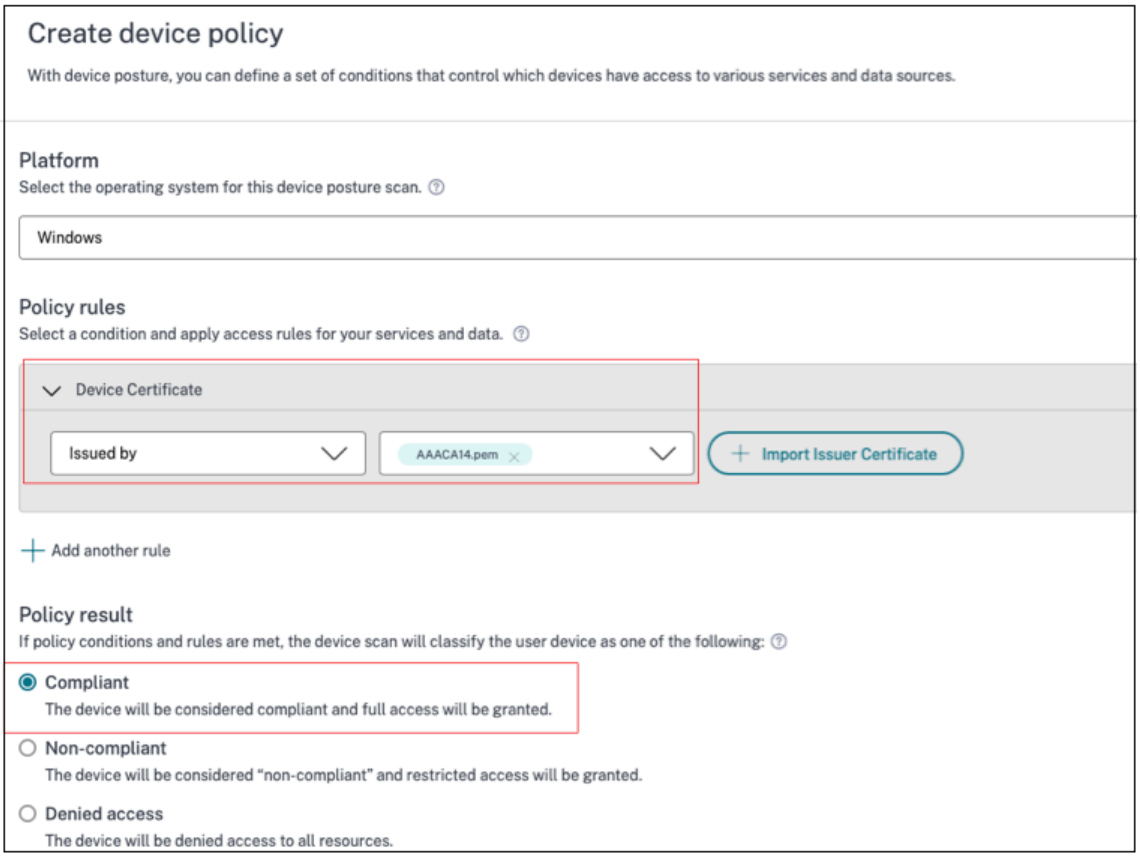
Servicio de postura del dispositivo con aplicaciones de acceso directo

Citrix Secure Private Access con aplicaciones de acceso directo, cuando se combina con el servicio Device Posture, puede garantizar que solo los dispositivos compatibles accedan a aplicaciones confidenciales a través del acceso directo. Los administradores pueden bloquear el acceso a dispositivos no compatibles o no administrados según los resultados del análisis del servicio de postura del dispositivo.

Pasos para habilitar el acceso directo solo para dispositivos compatibles

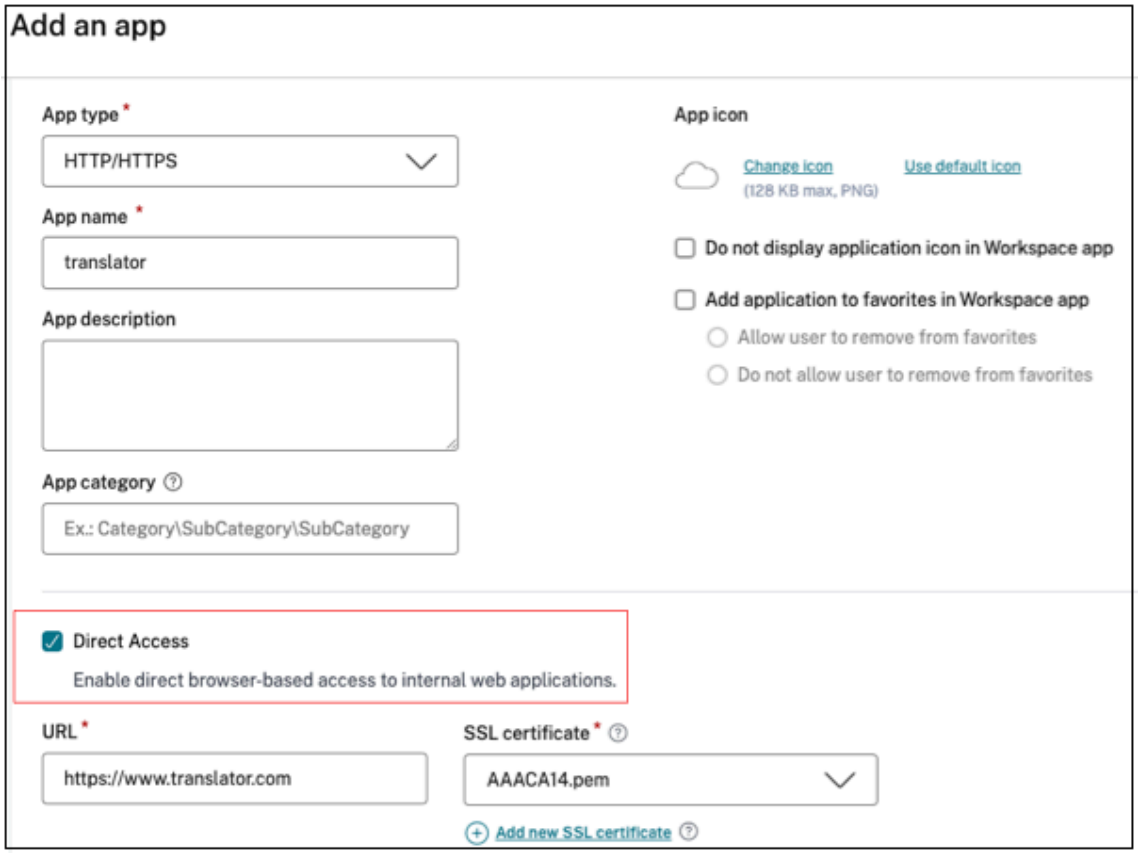
Para habilitar el acceso directo únicamente a dispositivos compatibles, el administrador debe realizar los siguientes pasos:

1. Desde la consola de administración del servicio Postura del dispositivo, cree una política de postura del dispositivo para verificar las condiciones del escaneo de postura del dispositivo, como el certificado del dispositivo, el antivirus, el navegador y luego seleccione **Cumple** como la acción del resultado de la política. Para obtener más detalles, consulte Configurar la postura del dispositivo.



2. Desde la consola de administración de Secure Private Access, realice lo siguiente:

- Cree una aplicación para la que desee habilitar el acceso directo. Para obtener más detalles, consulte Acceso directo a aplicaciones web empresariales.



- Configurar el acceso privado seguro con la postura del dispositivo. En el ámbito de la regla ****, seleccione **Verificación de postura del dispositivo > Coincide con cualquiera de** e ingrese la etiqueta **Cumple**. Esta etiqueta se envía desde el servicio de postura del dispositivo.

> **Nota**
>
> La etiqueta debe ingresarse exactamente como se capturó anteriormente, utilizando mayúsculas iniciales (Compliant). De lo contrario, las políticas de postura del dispositivo no funcionan como se espera. Para obtener más detalles, consulte Configuración de Citrix Secure Private Access con Device Posture.

```
1 ![Postura del dispositivo para acceso directo3](/en-us/citrix-secure-
    private-access/media/spa-direct-access-device-posture-3.png)
```

Una vez realizada esta configuración, en función de los resultados del escaneo de postura del dispositivo, el dispositivo se etiqueta como compatible, no compatible o con inicio de sesión denegado y se habilita el acceso a la aplicación en consecuencia.

Ejemplo:

Considere que ha creado una política de postura del dispositivo para verificar la presencia de un certificado de dispositivo en un dispositivo terminal y determinar su estado de inicio de sesión. Una vez que se establecen las políticas de postura del dispositivo y se habilita la postura del dispositivo, se producen las siguientes acciones cuando un usuario final inicia sesión en Citrix Workspace.

1. El escaneo de postura del dispositivo verifica el dispositivo terminal para detectar la presencia de un certificado de dispositivo.
    - Si el certificado del dispositivo está presente en el dispositivo, el dispositivo se etiqueta como compatible con **.
    - Si el certificado del dispositivo no está presente en el dispositivo, el dispositivo se etiqueta como **no compatible**.
2. Luego, esta información se pasa al servicio Citrix Secure Private Access como etiquetas.
3. La política de acceso se evalúa en función de la clasificación del dispositivo.
    - Si el dispositivo es compatible, se permite el acceso directo a las aplicaciones.
    - Si el dispositivo no es compatible, se deshabilita el acceso directo a las aplicaciones.

Experiencia del usuario final

La experiencia del usuario final se basa en la clasificación del dispositivo como compatible o no compatible.

- **Dispositivo compatible:**

  El usuario puede iniciar la aplicación de acceso directo desde Citrix Workspace o desde el navegador utilizando la URL de la aplicación.
- **Dispositivo no conforme:**
    - La aplicación no está enumerada en Citrix Workspace.
    - El usuario no puede iniciar la aplicación desde el navegador utilizando la URL de la aplicación.
    - Se muestra al usuario una página de acceso bloqueado.

Soporte para aplicaciones de software como servicio

October 21, 2024

El software como servicio (SaaS) es un modelo de distribución de software para entregar software de forma remota como un servicio basado en la 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 de acceso privado seguro 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.

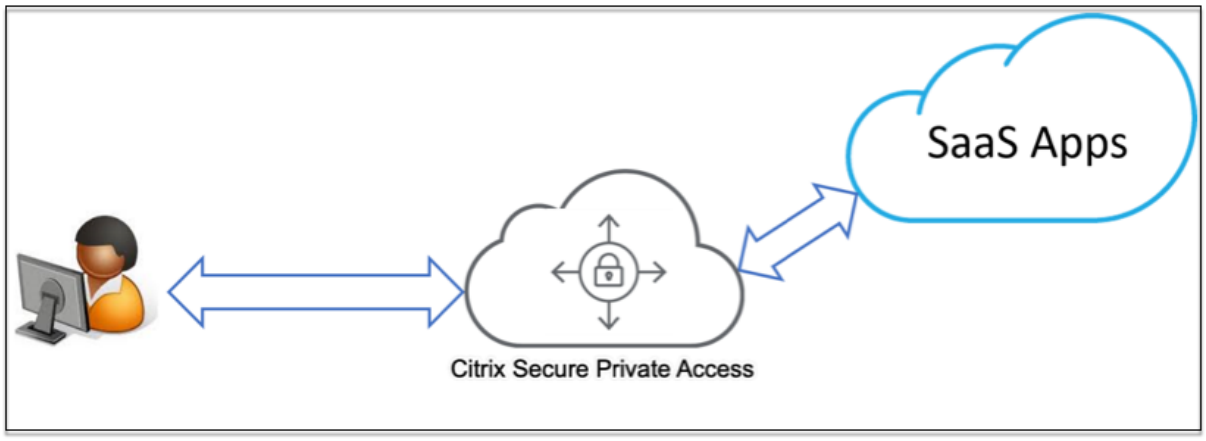
La entrega de aplicaciones SaaS mediante el servicio de acceso privado seguro le proporciona una solución fácil, segura, sólida y escalable para administrar las aplicaciones. Las aplicaciones SaaS entregadas en la nube tienen los siguientes beneficios:

- **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 respaldan 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 de acceso privado seguro.
2. El administrador proporciona la URL del servicio a los usuarios para acceder a Citrix Workspace.
3. Para iniciar la aplicación, el usuario hace clic en el ícono de la aplicación SaaS enumerado.
4. La aplicación SaaS confía en la afirmación SAML proporcionada por el servicio de acceso privado seguro y se inicia la aplicación.

> **Nota**
>
> - Para otorgar acceso a las aplicaciones a los usuarios, los administradores deben crear políticas de acceso. En las políticas de acceso, los administradores agregan suscriptores de aplicaciones y configuran controles de seguridad. Para obtener más detalles, consulte Crear políticas de acceso.
> - Las aplicaciones SaaS configuradas se agregan junto con aplicaciones virtuales y otros recursos en Citrix Workspace para 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. Establecer el método de inicio de sesión preferido
3. Definir el enrutamiento de la aplicación

Configurar los detalles de la aplicación

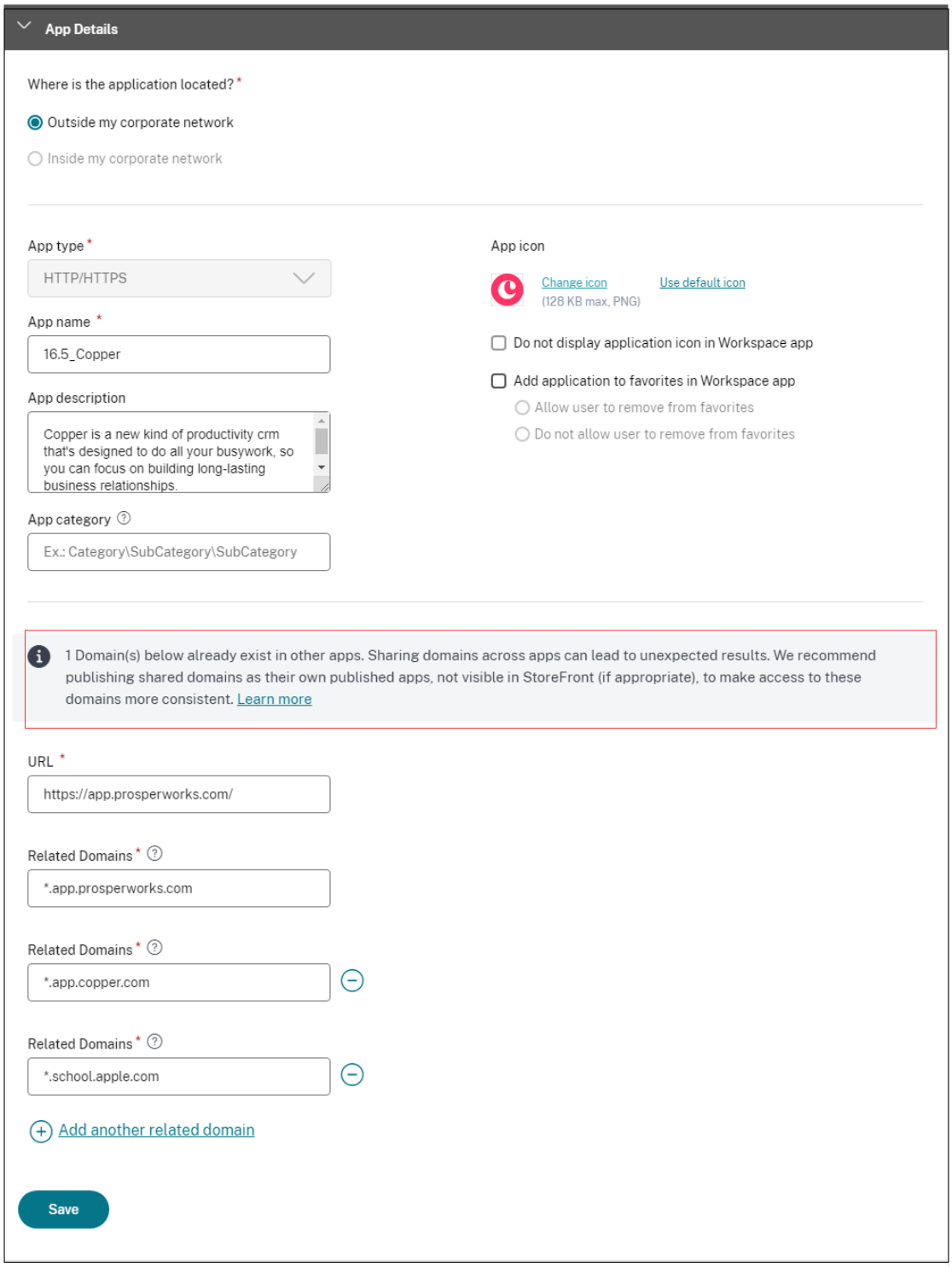
1. En el mosaico **Acceso privado seguro** , haga clic en **Administrar.**
2. Haga clic en **Continuar** y luego haga clic en **Agregar una aplicación.**

> **Nota**
>
> - El botón **Continuar** aparece solo la primera vez que utiliza el asistente. En los usos posteriores, puede navegar directamente a la página **Aplicaciones** y luego hacer clic en **Agregar una aplicación.**
> - Puede agregar una aplicación SaaS manualmente ingresando 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, todavía se debe proporcionar la información específica del cliente. Para conocer los detalles de la plantilla de configuración de la aplicación SaaS, consulte Configuración específica del servidor de aplicaciones SaaS.

1. Configurar la aplicación.
   - Para ingresar los detalles de la aplicación manualmente, haga clic en **Omitir.**
   - Para configurar la aplicación usando una plantilla, haga clic en **Siguiente.**

El **Fuera de mi red corporativa** está habilitado de forma predeterminada para una aplicación SaaS.

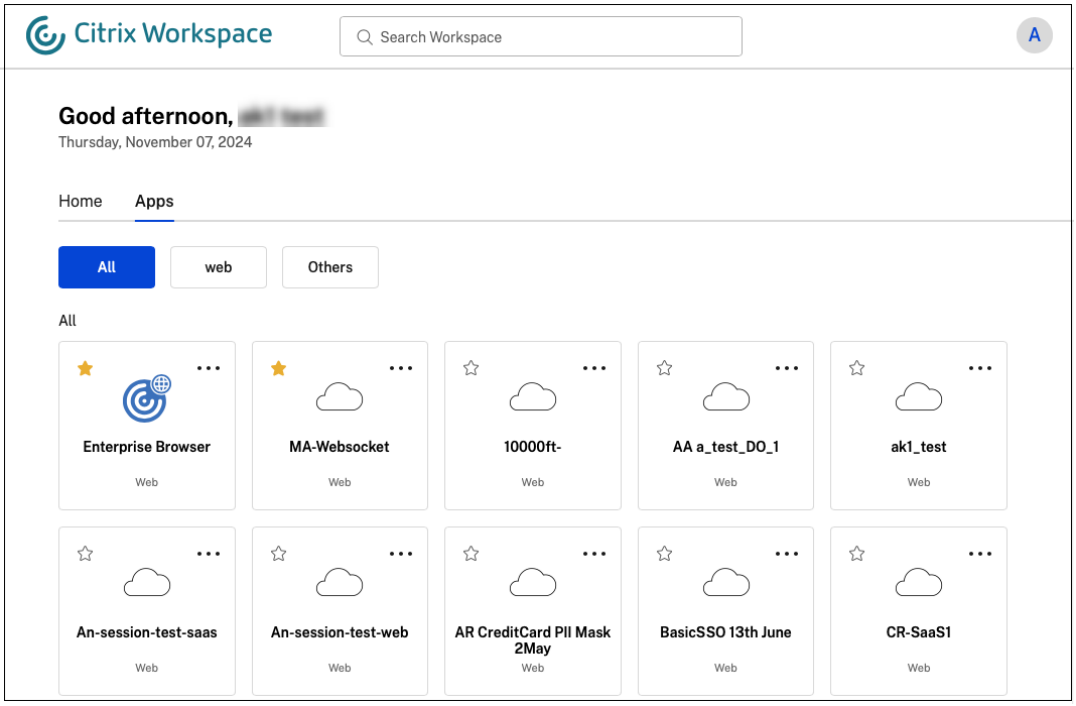
2. Ingresa los siguientes detalles en la sección **Detalles de la aplicación** y haz clic en **Siguiente.**



- **Nombre de la aplicación** –Nombre de la aplicación.

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

    Por ejemplo, si introduce el parámetro **Negocios y Productividad** categoría incorrectamente como **Negocio y productividad** En **Categoría de aplicación** campo, entonces una nueva categoría llamada **Negocio y productividad** aparece en la interfaz de usuario de Citrix Workspace, además de la **Negocios y productividad** categoría.



- **Ícono de la aplicación** –Haga clic en **Cambiar ícono** para cambiar el ícono de la aplicación. El tamaño del archivo del icono debe ser de 128x128 píxeles. Si no cambia el icono, se mostrará el icono predeterminado.

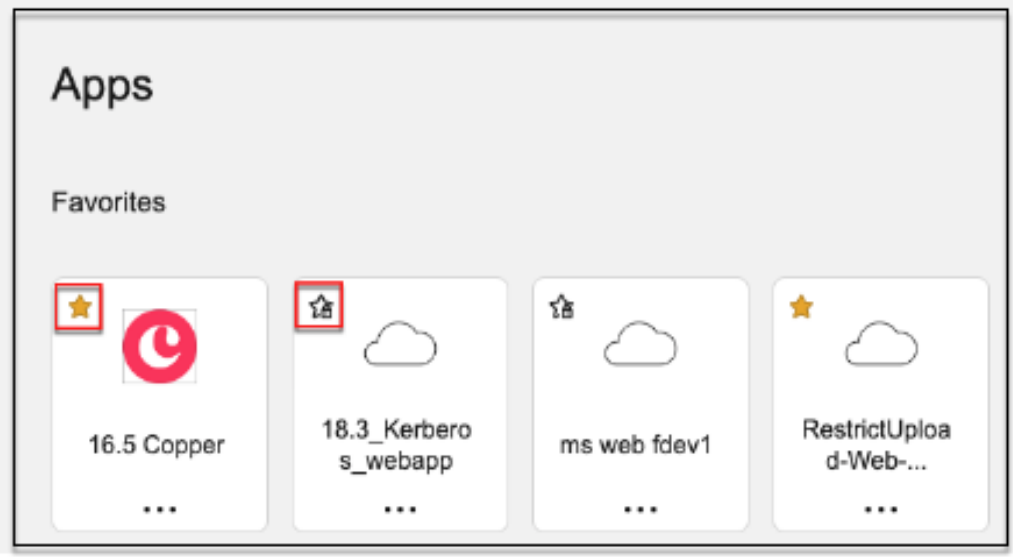
```
If you do not want to display the app icon, select **Do not display application icon to users**.
```

- **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 Registrarse en Citrix Cloud. En caso de que el SSO falle o no desee utilizarlo, el usuario será redirigido a esta URL.
- **Nombre de dominio del cliente** y **ID de dominio del cliente** : el nombre de dominio y la ID del cliente se utilizan para crear la URL de la aplicación y otras URL posteriores en la página SSO SAML.

```
For example, if you're adding a Salesforce app, your domain name is `salesforceformyorg` and ID is 123754, then the app URL is `https://salesforceformyorg.my.salesforce.com/?so=123754.`

Customer domain name and Customer ID fields are specific to certain apps.
```

- **Dominios relacionados** –El dominio relacionado se completa automáticamente según la URL que usted proporcionó. El dominio relacionado ayuda al servicio a identificar la URL como parte de la aplicación y 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 que el usuario elimine de favoritos** para permitir que los suscriptores de la aplicación eliminen la aplicación de la lista de aplicaciones favoritas en la aplicación Citrix Workspace. Cuando selecciona esta opción, aparece un ícono de estrella amarilla en la esquina superior izquierda de la aplicación en la aplicación Citrix Workspace.
  - 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 en la aplicación Citrix Workspace. Cuando selecciona esta opción, aparece un ícono de estrella con un candado en la esquina superior izquierda de la aplicación Citrix Workspace.



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

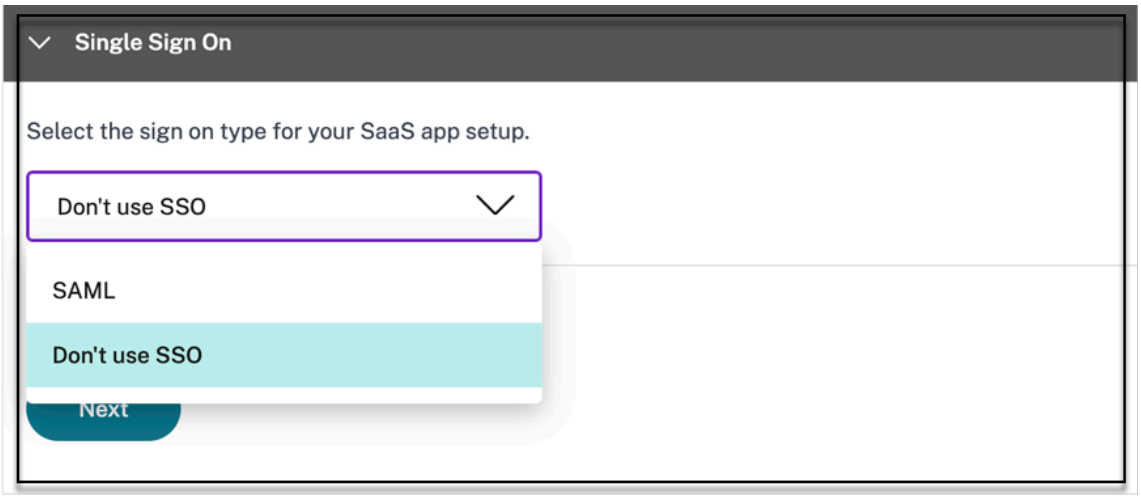
3. Haga clic en **Siguiente.**

> **Importante:**
>
> - Para permitir el acceso basado en confianza cero a las aplicaciones, se les niega el acceso de forma predeterminada. El acceso a las aplicaciones solo está habilitado si hay una política de acceso asociada a la aplicación. Para obtener más detalles, consulte Acceso denegado a las aplicaciones, de forma predeterminada.
> - Si se configuran varias aplicaciones con el mismo FQDN o alguna variación del FQDN comodín, esto podría generar una configuración conflictiva. Para obtener más detalles, con-

> sulte Configuración conflictiva que podría generar problemas de acceso a la aplicación.

Establecer un método de inicio de sesión preferido

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



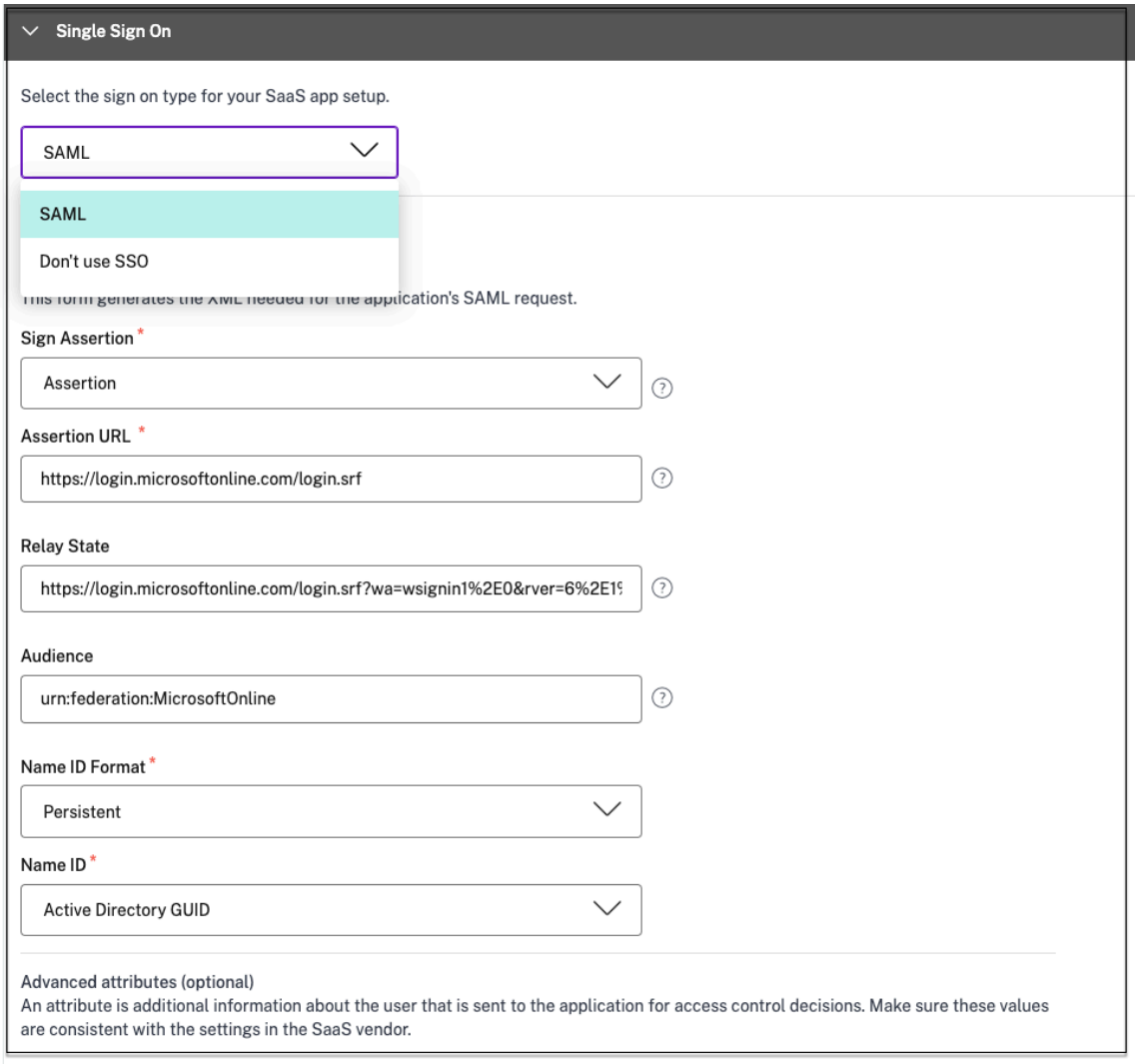
   - **No usar SSO** –Utilice la opción **No usar SSO** cuando no necesite autenticar a un usuario en el servidor back-end. Cuando se selecciona la opción **No usar SSO** , el usuario es redirigido a la URL configurada en la sección **Detalles de la aplicación** .
   - **SAML** - Elija **SAML** para SSO basado en SAML en aplicaciones web. Ingrese los detalles de configuración para el tipo de SSO **SAML** .

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

     - **Firmar afirmación** - Firmar una afirmación o respuesta garantiza la integridad del mensaje cuando la respuesta o afirmación se entrega a la parte confiada (SP). Puede seleccionar **Afirmación, Respuesta, Ambas,** o **Ninguna**.
     - **URL de afirmación** : la URL de afirmación la proporciona el proveedor de la aplicación. La aserción SAML se envía a esta URL.
     - **Estado del relé** –El parámetro Estado del relé se utiliza para identificar el recurso específico al que acceden los usuarios después de iniciar sesión y ser dirigidos al servidor de federación de la parte confiada. 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** –La audiencia la proporciona el proveedor de la aplicación. Este valor confirma que la afirmación SAML se genera 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 usando la URL específica (iniciada por el proveedor de servicios)** 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 las decisiones de control de acceso.



3. Descargue el archivo de metadatos haciendo clic en el enlace debajo de **Metadatos SAML**. Utilice el archivo de metadatos descargado para configurar SSO en el servidor de aplicaciones SaaS.

> **Nota**
>
> - Puede copiar la URL de inicio de sesión de SSO en **URL de inicio de sesión** y usar esta URL

> al configurar SSO en el servidor de aplicaciones SaaS.
> - También puede descargar el certificado de la lista **Certificado** y usar el certificado al configurar SSO en el servidor de aplicaciones SaaS.

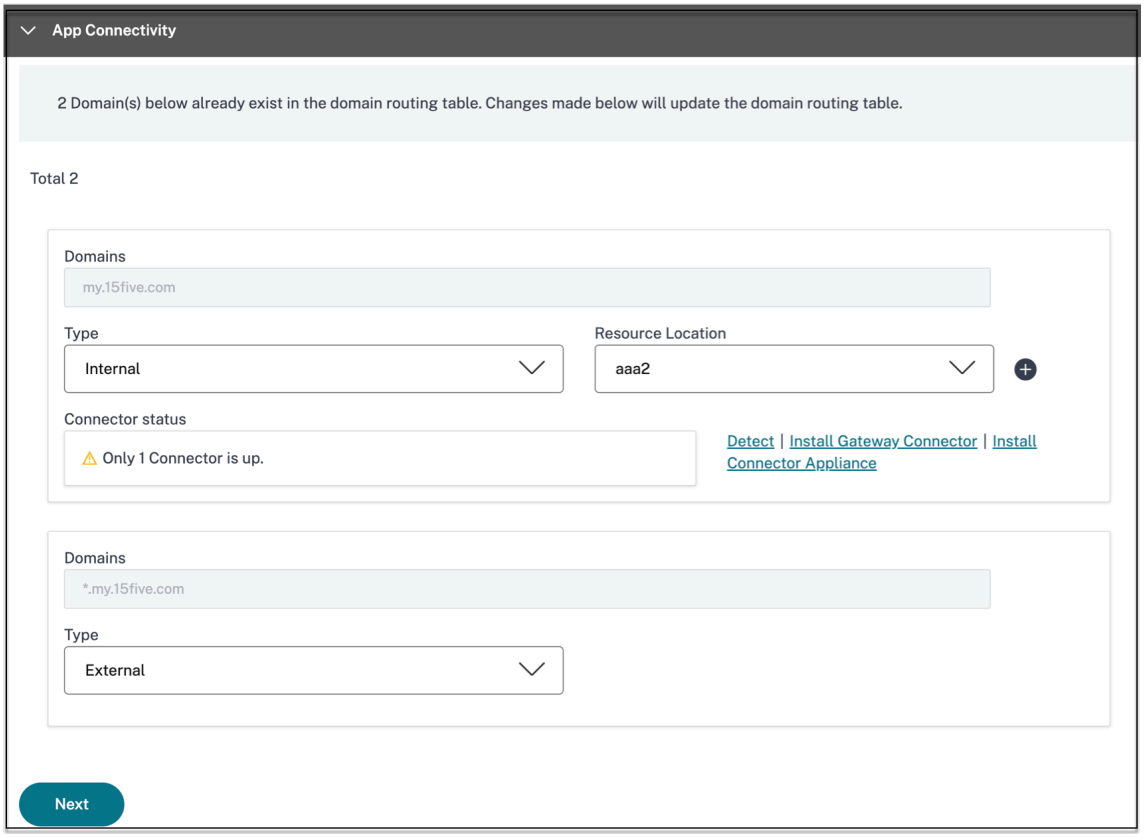
1. Haga clic en **Siguiente.**

Definir el enrutamiento de la aplicación

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 dispositivos Citrix Connector.

   - **Interno –Omitir proxy** : el tráfico del dominio se enruta a través de Citrix Cloud Connector, sin pasar por el proxy web del cliente configurado en el dispositivo Connector.
   - **Interno a través del conector** : las aplicaciones pueden ser externas, pero el tráfico debe fluir a través del dispositivo conector hacia la red externa.

   Para obtener más detalles, consulte Tablas de ruta para resolver conflictos si los dominios relacionados en las aplicaciones web y SaaS son los mismos.

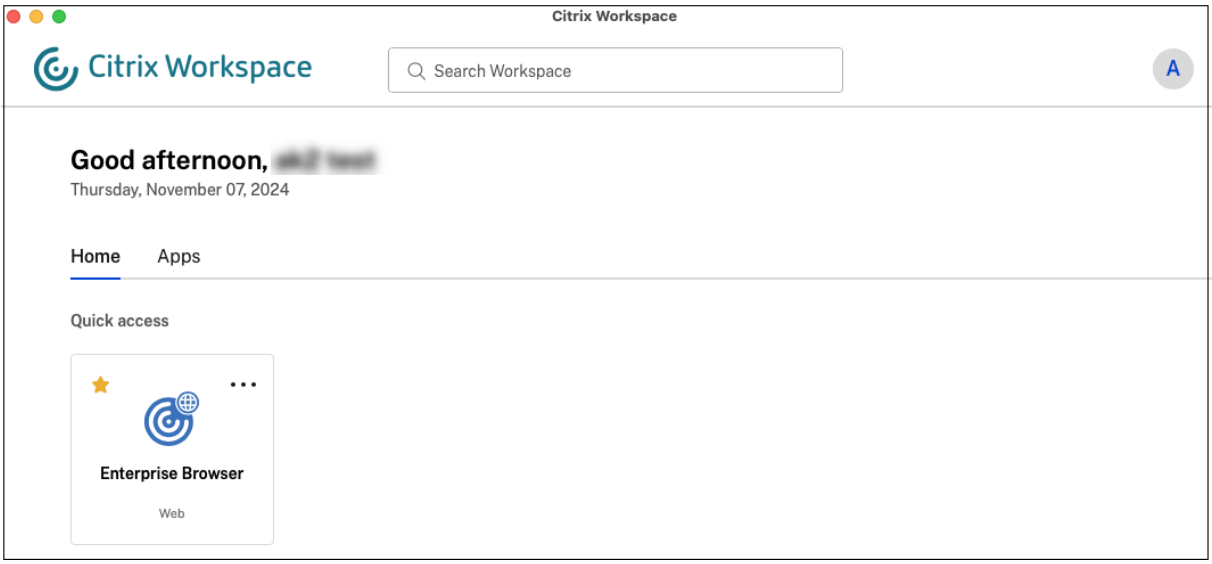


2. Haga clic en **Finalizar.**

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

- **Editar aplicación**
- **Eliminar**

Cuando publica 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 navegador del espacio de trabajo sin una URL y acceder a sitios web internos mediante los navegadores del espacio de trabajo.



Referencias

Para una configuración completa de extremo a extremo de una aplicación, consulte Flujo de trabajo guiado por el administrador para una fácil incorporación y configuración.

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**.

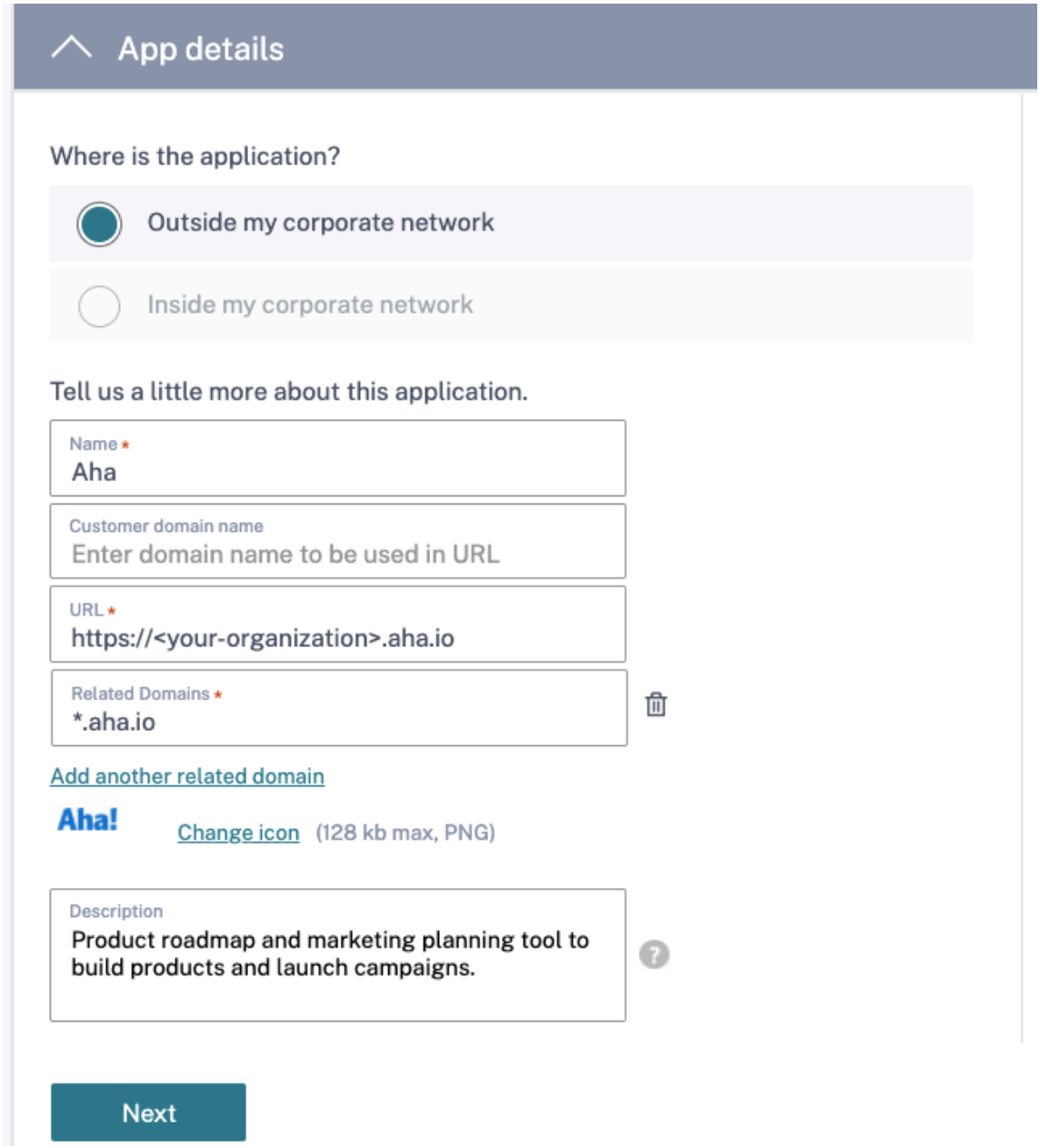
   Nombre de dominio del cliente e **ID de dominio del cliente**: El nombre y el ID de dominio del cliente se utilizan para crear una URL de aplicación y otras URL posteriores en la página de inicio de sesión único de SAML.

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.**

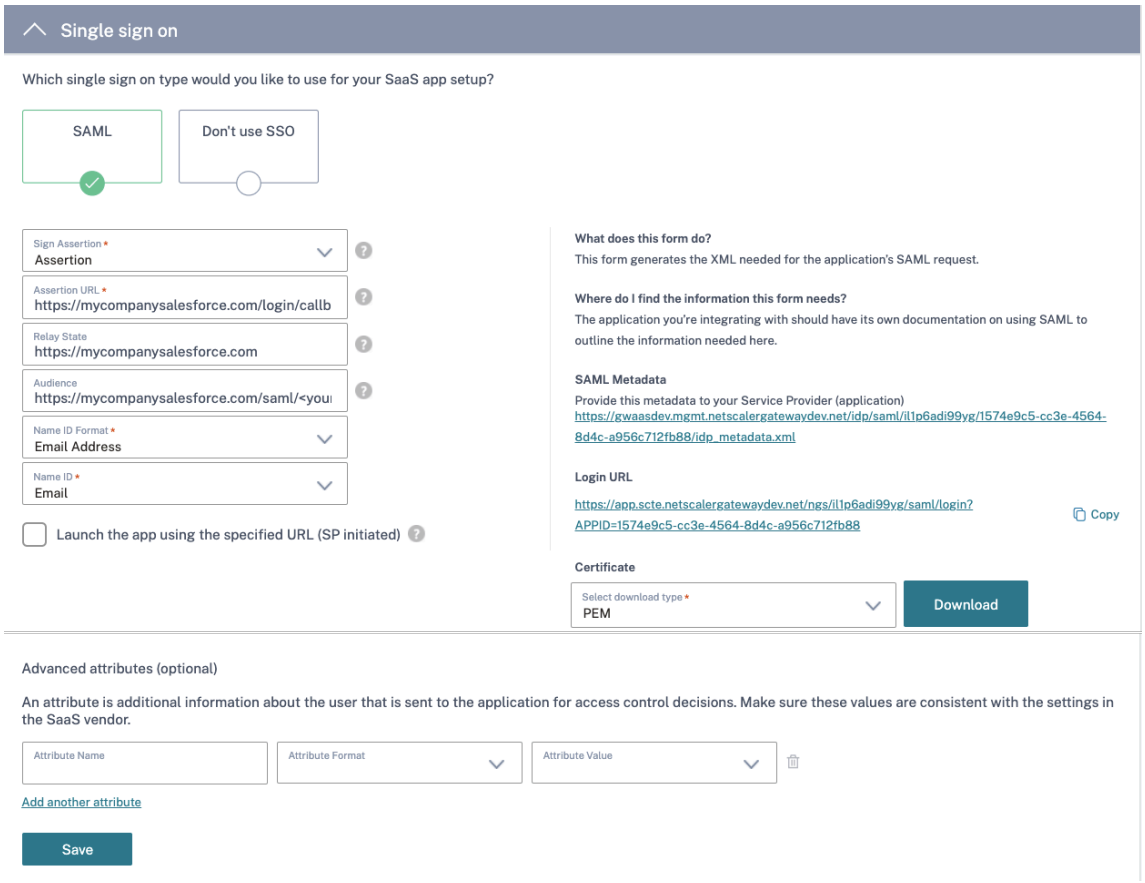
   URL de aserción: URL de aserción SAML de la aplicación SaaS proporcionada por el proveedor de la aplicación. La aserción SAML se envía a esta URL.

   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**.

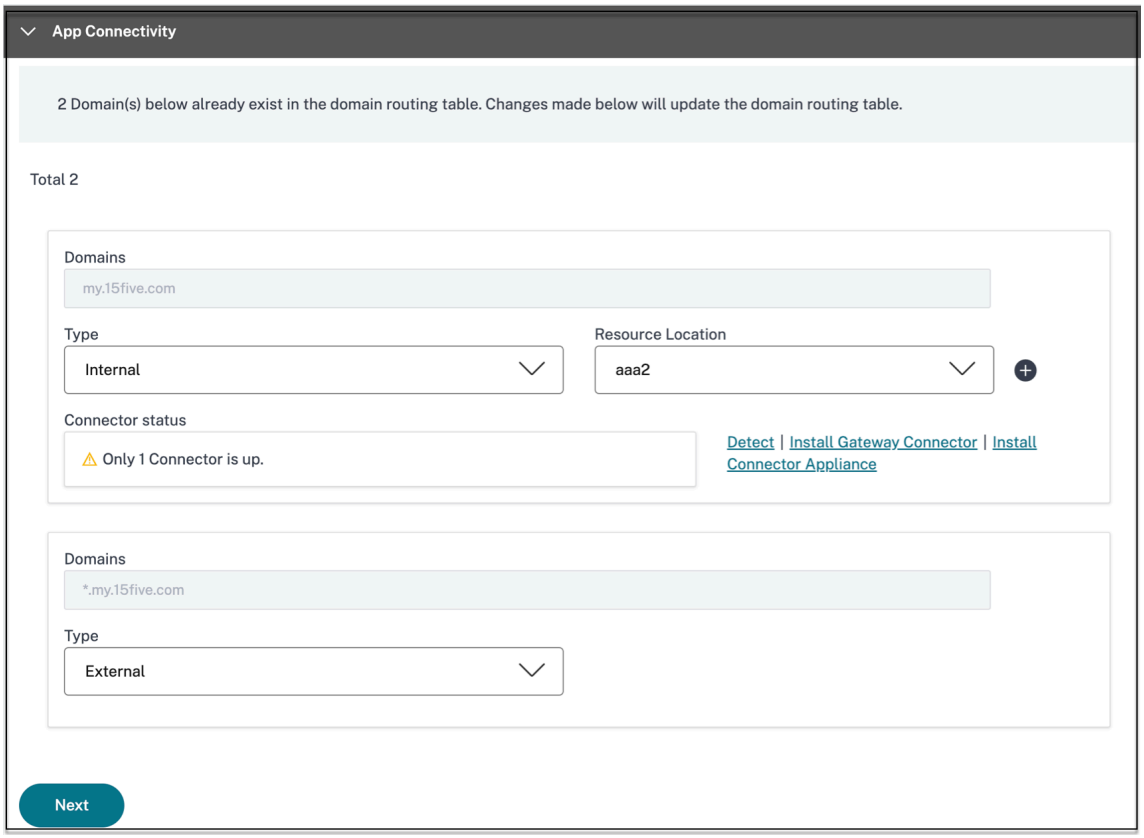
5. Descargue el archivo de metadatos haciendo clic en el enlace situado debajo de **Metadatos SAML.** Utilice el archivo de metadatos descargado para configurar el SSO en el servidor de aplicaciones SaaS.

   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.

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.

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.

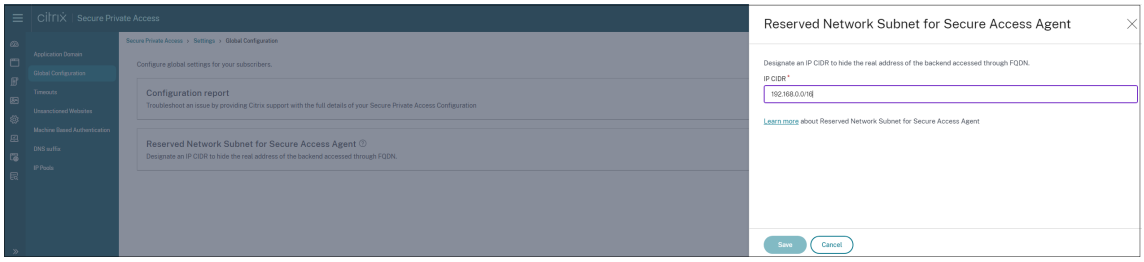
Los siguientes son los rangos de direcciones IP CIDR reservados permitidos:

- 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.

		Configuración de sufijo DNS y de aplicaciones	Experiencia del usuario final
			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”.
	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.

Dispositivo conector para Secure Private Access

June 21, 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 Secure Private Access 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.

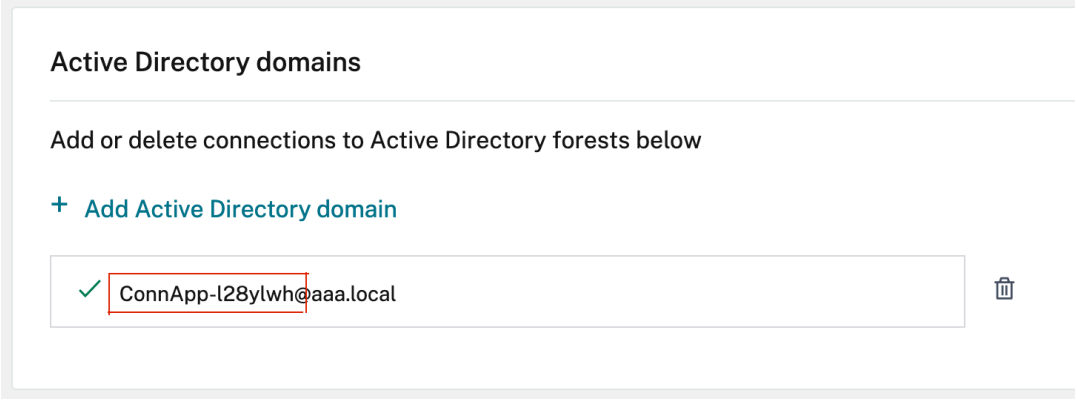
      Unirse a un bosque de Active Directory le permite usar la delegación limitada de Kerberos (KCD) al configurar Secure Private Access, pero no permite las solicitudes de identidad ni la autenticación para usar el Connector Appliance.

      - 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**.

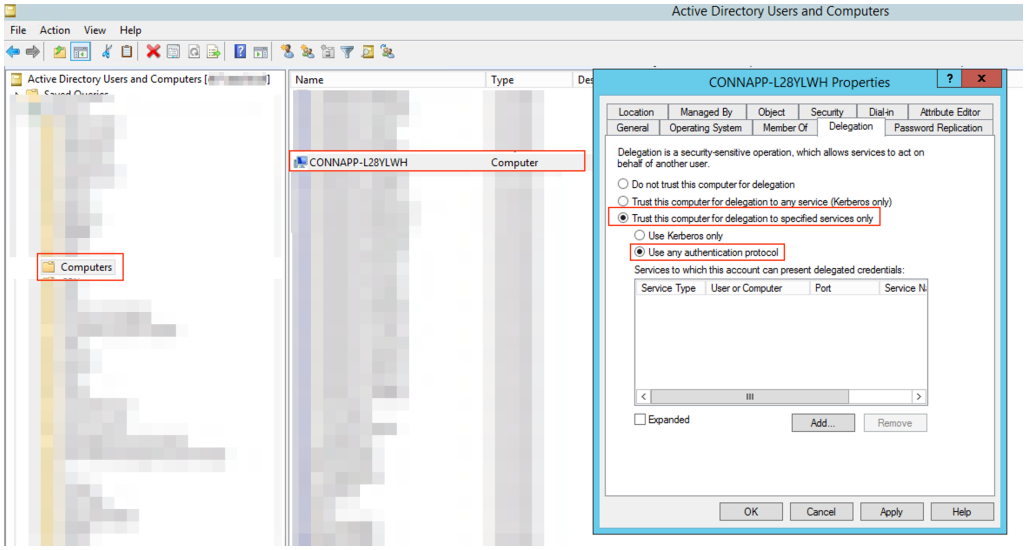
        Si no tiene una sección de **dominios de Active Directory** en la página de administración, contacte con Citrix para solicitar la inscripción en la función Tech Preview.
      - Introduzca el nombre de dominio en el campo **Nombre de dominio**. Haga clic en **Agregar**.
      - Connector Appliance comprueba 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**.

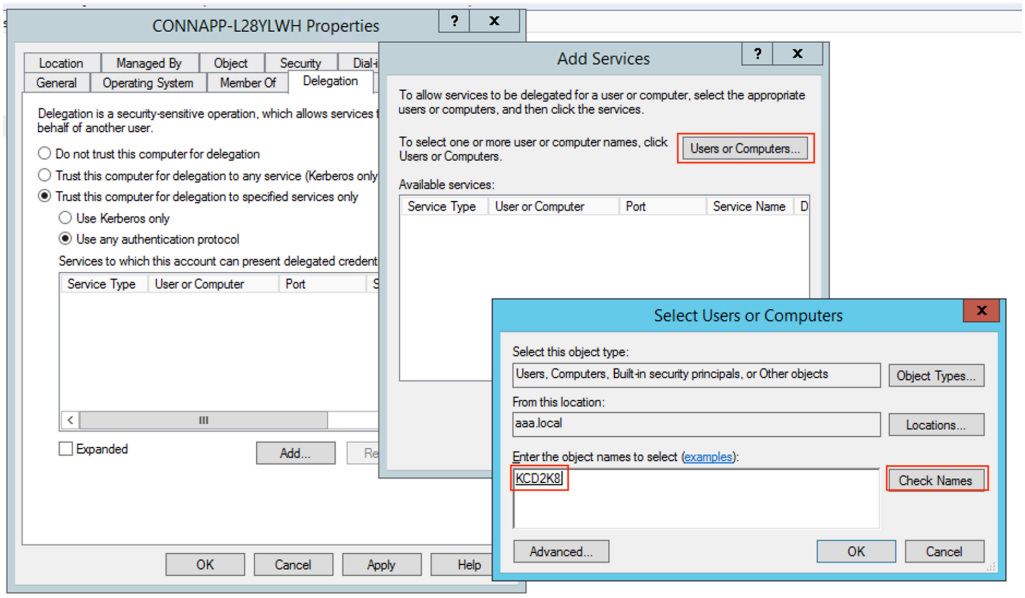
b) Configure la delegación de restricciones Kerberos para el servidor web sin un equilibrador de carga.



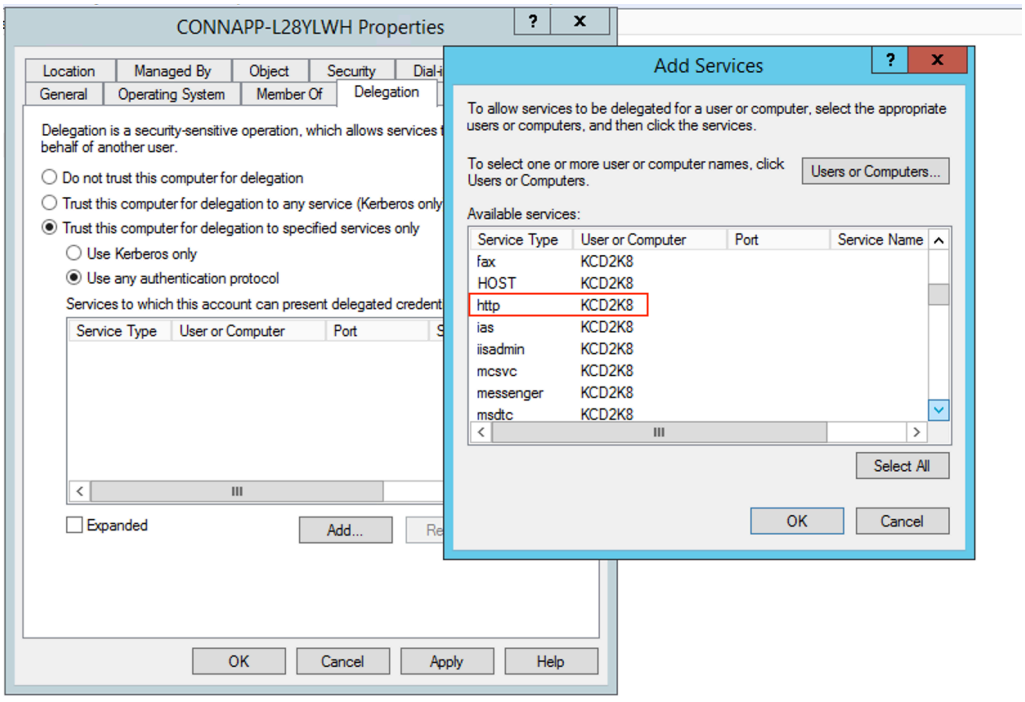
- Identifique el nombre del equipo del dispositivo conector. Puede obtener este nombre desde el lugar donde lo alojó o simplemente desde la interfaz de usuario del conector.
- En la controladora de Active Directory, busque el equipo del dispositivo conector.
- Vaya a las propiedades de la cuenta de equipo 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, seleccione **Usar cualquier protocolo de autenticación.**



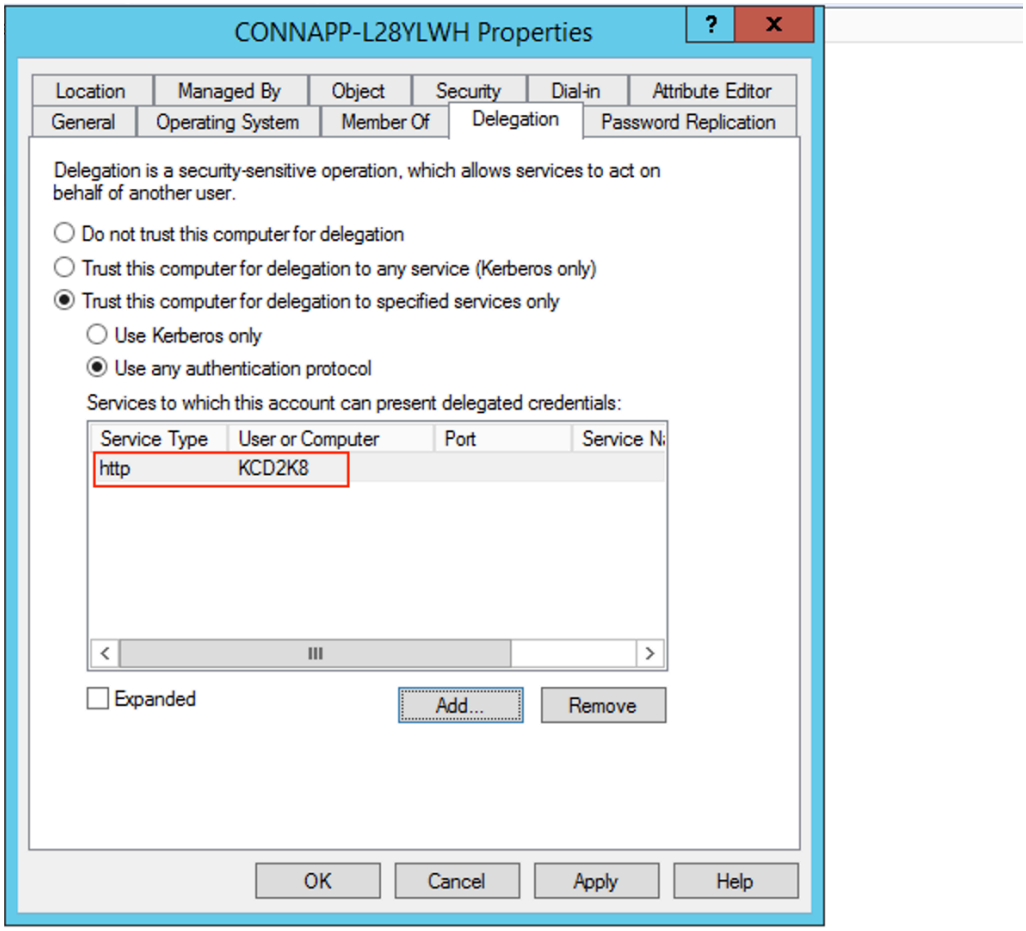
- Haga clic en **Agregar.**
- Haga clic en **Usuarios o equipos.**
- Introduzca el nombre del equipo del servidor web de destino y después haga clic en **Comprobar nombres.** En la imagen anterior, **KCD2K8** es el servidor web.



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



- Haga clic en **Aceptar**.
- Haga clic en **Aplicar** y después en **Aceptar**.



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

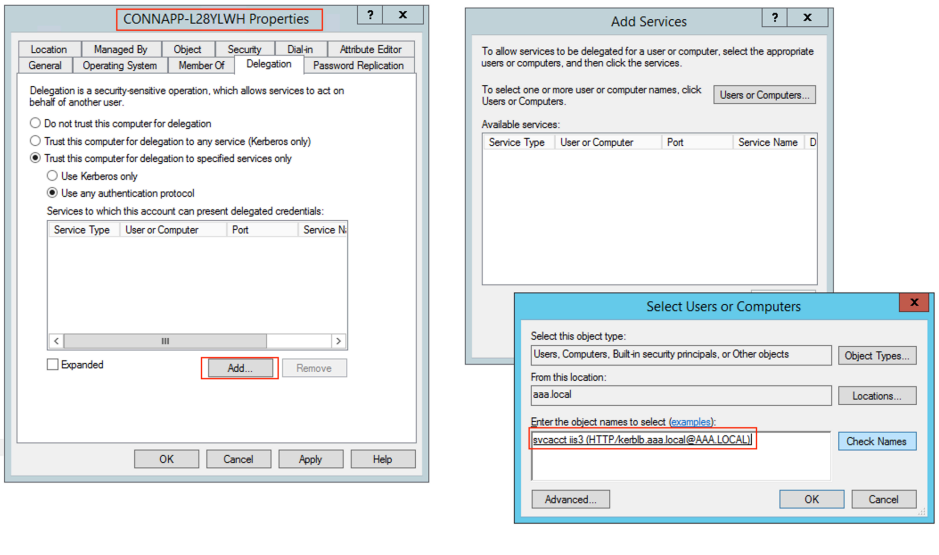
c) Configure la delegación de restricciones Kerberos (KCD) para un servidor web detrás de un equilibrador de carga.

- Agregue el SPN del equilibrador de cargas a la cuenta de servicio mediante este comando `setspn`.
  `setspn -S HTTP/<web_server_fqdn> <service_account>`

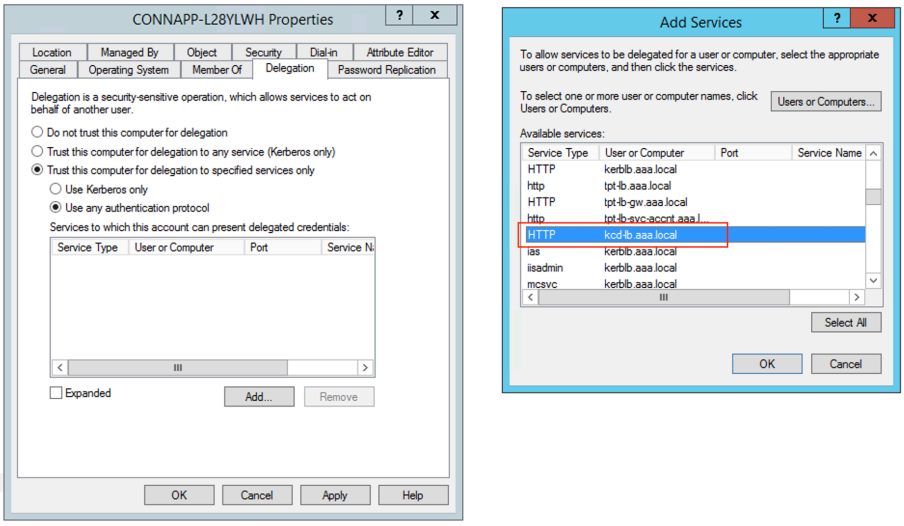
```
C:\Windows\system32>setspn -s HTTP/kcd-lb.aaa.local aaa\svc_iis3
Checking domain DC=aaa,DC=local

Registering ServicePrincipalNames for CN=svcacct iis3,OU=Users,OU=KCD,DC=aaa,DC=local
        HTTP/kcd-lb.aaa.local
Updated object

C:\Windows\system32>_
```

- Confirme los SPN de la cuenta de servicio mediante el siguiente comando.
  `setspn -l <service_account>`

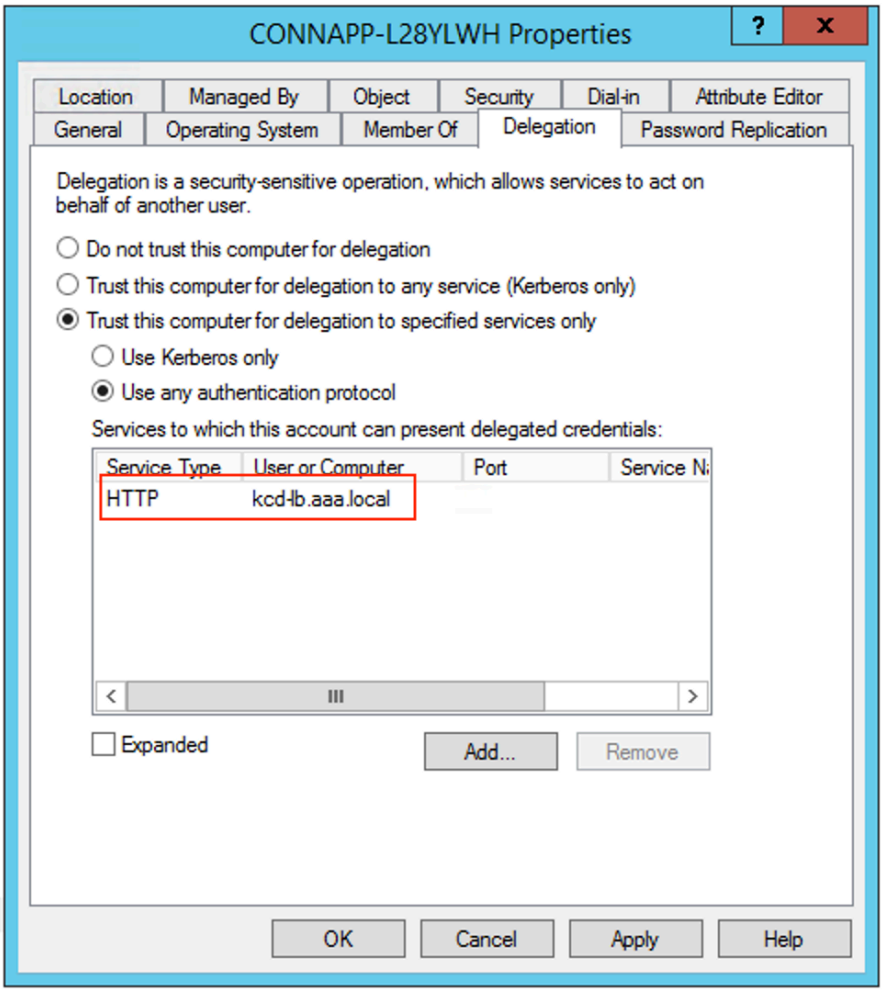
- Cree una delegación para la cuenta de equipo del dispositivo conector.
  - Siga los pasos para *configurar la delegación de restricciones Kerberos para el servidor web* sin un equilibrador de carga para identificar la máquina de CA y navegar hasta la interfaz de usuario de delegación.
  - En Seleccionar **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 después en **Aceptar**.

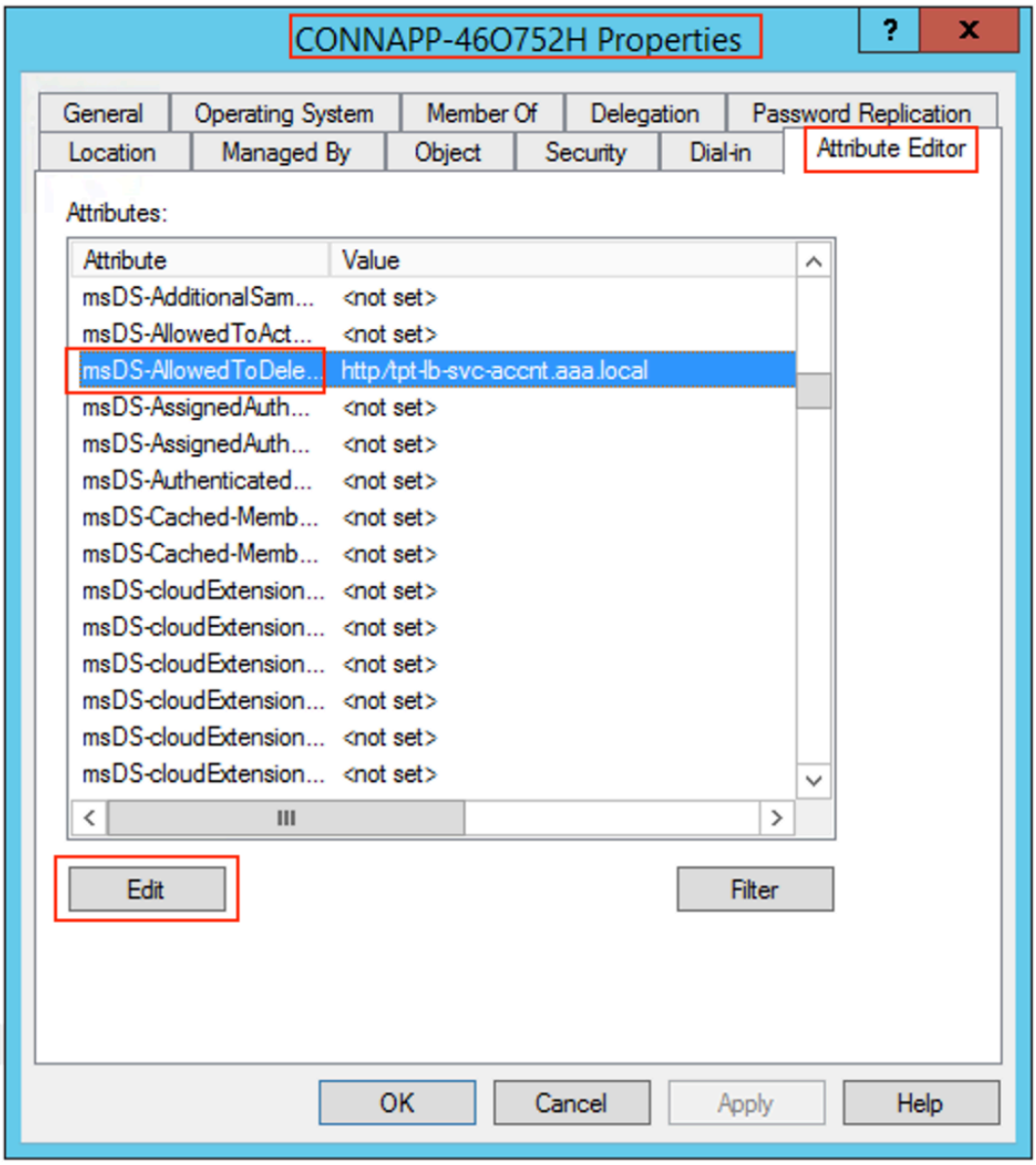


d) Configure la delegación restringida de Kerberos (KCD) para una cuenta de servicio administrada por grupo.

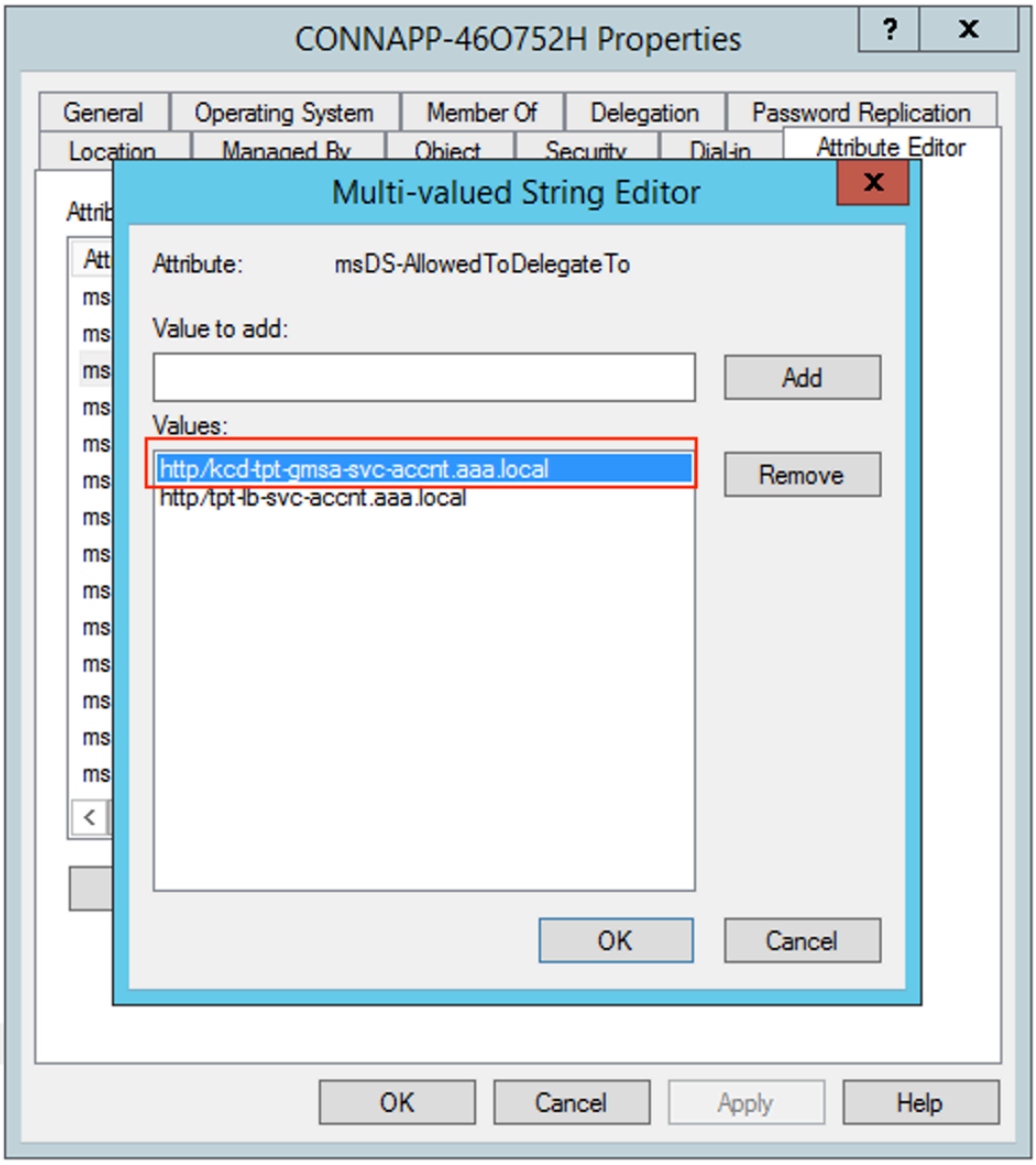
- Agregue SPN a la cuenta de servicio administrado del grupo si aún no lo ha hecho.
  `setspn -S HTTP/<web_server_fqdn> <group_manged_service_account>`
- Confirme el SPN con el siguiente comando.
  `setspn -l <group_manged_service_account>`

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 después agregue el SPN.



)

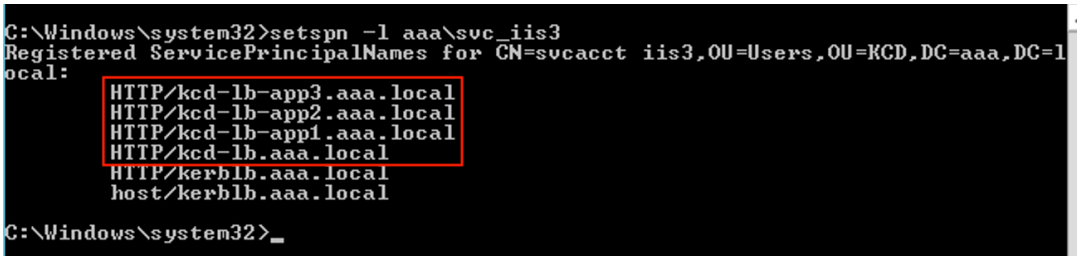


)

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

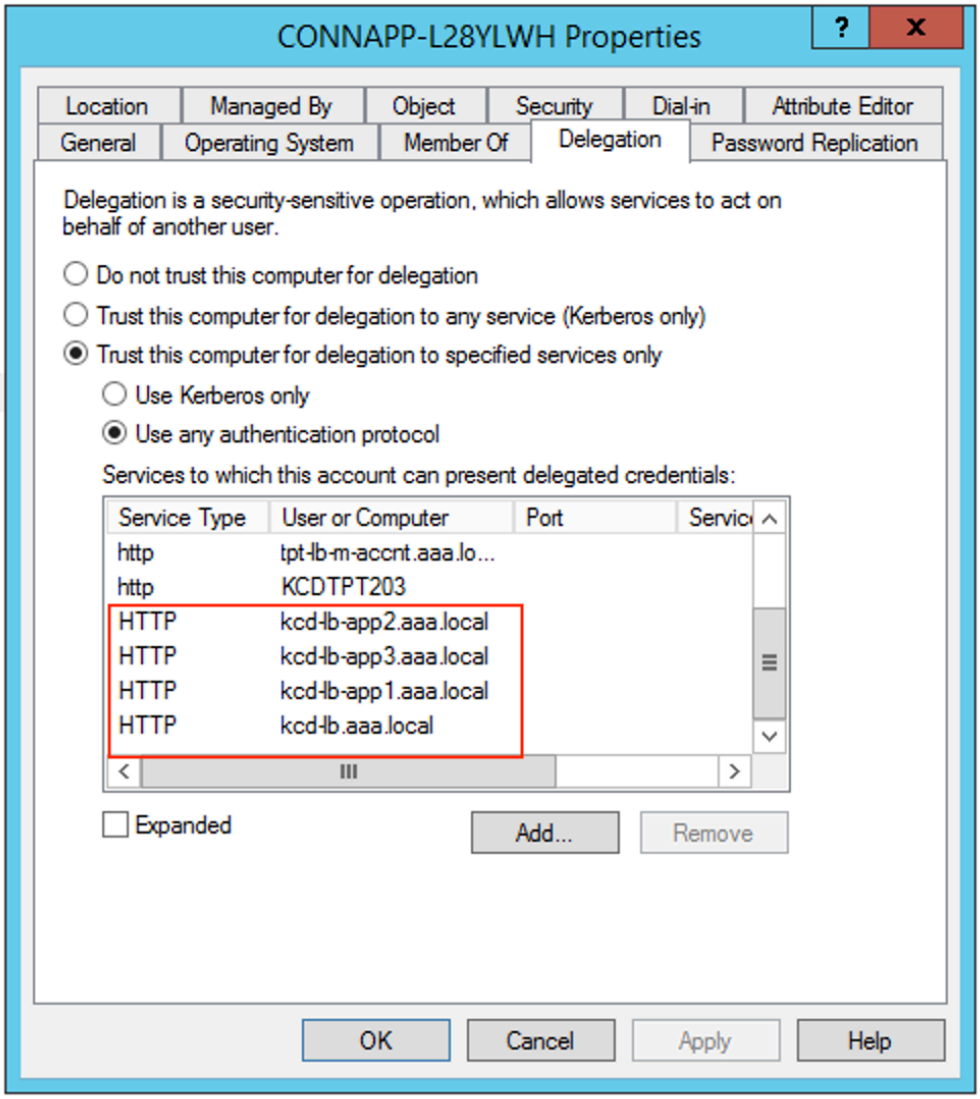
- Como los SPN ya están configurados en la cuenta de servicio al configurar el conector de puerta de enlace, no es necesario agregar más SPN para la cuenta de servicio si no se ha configurado una nueva aplicación kerberos. Puede ver la lista de todos los SPN asignados a la cuenta de servicio siguiendo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

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

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

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>

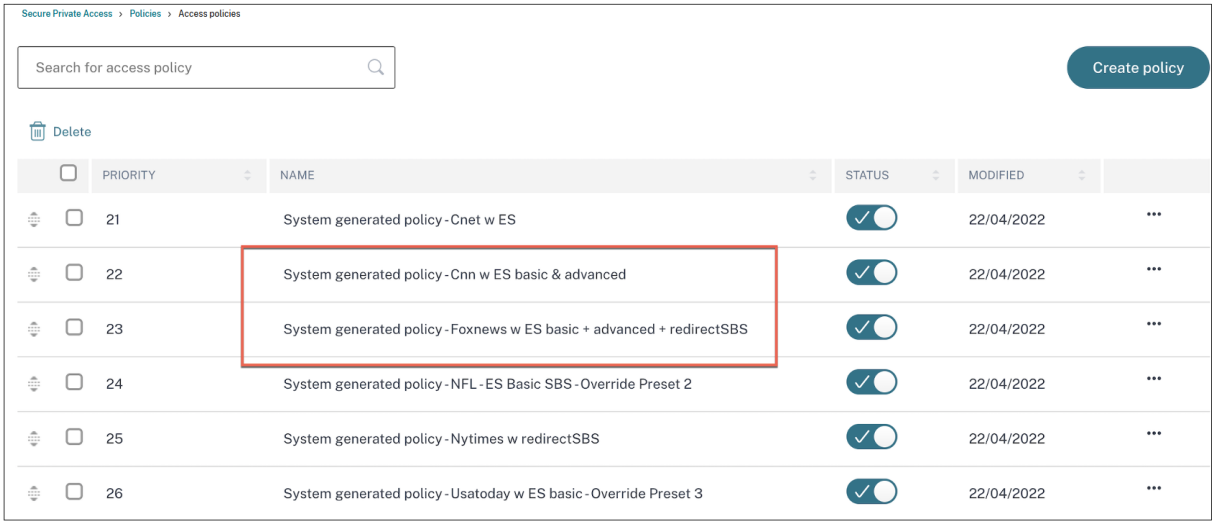
> **Nota:**
>
> Si las aplicaciones no tienen usuarios o grupos agregados, no se crean nuevas directivas.

En la siguiente tabla se resumen los cambios.

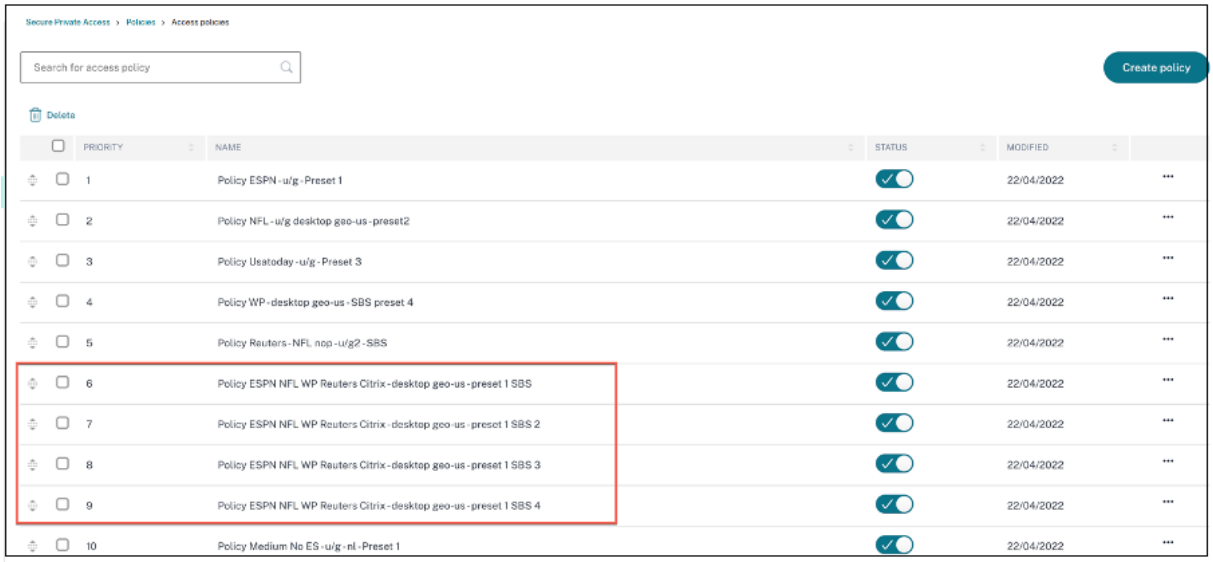
Si hubiera configurado un…	Entonces…
Aplicación sin condiciones de seguridad mejoradas	Se crea una nueva directiva con usuarios y grupos como condición obligatoria. Los usuarios o grupos se derivan de las directivas de acceso. La acción se establece en **Permitir acceso**.
Aplicación con condiciones 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>.

Si hubiera configurado un…	Entonces…
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.



Iniciar una aplicación configurada: flujo de trabajo del usuario final

December 27, 2023

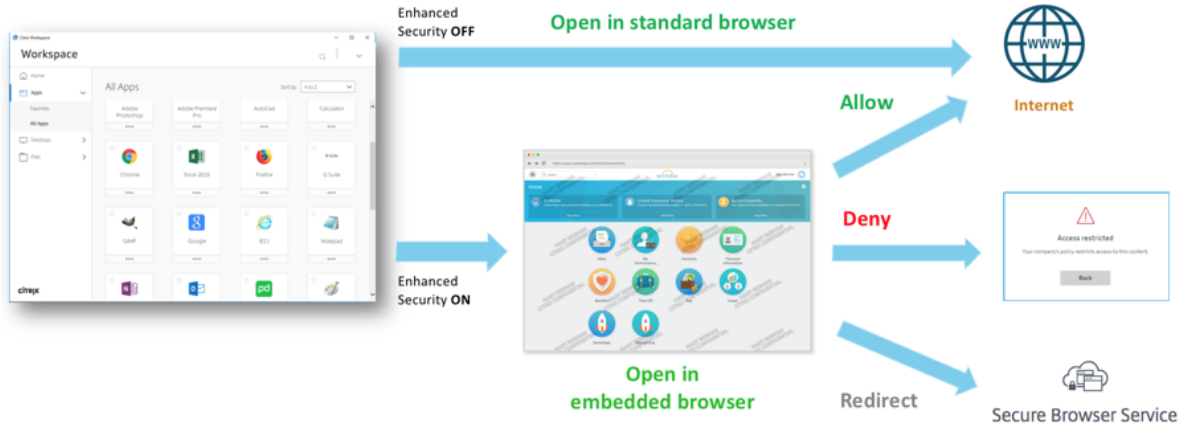
Como usuario final, debe hacer lo siguiente:

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.

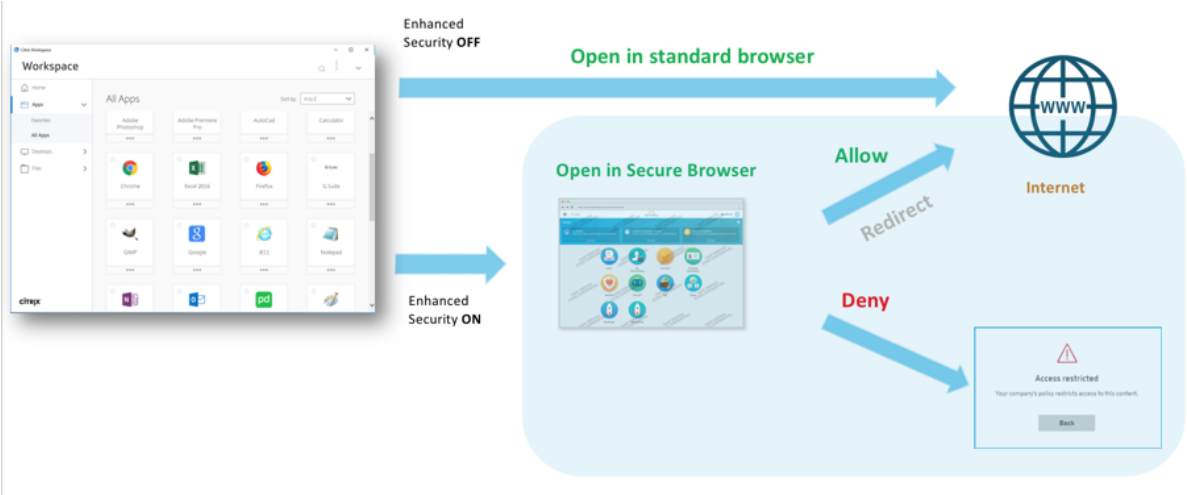
Ahora puede usar la aplicación SaaS desde la aplicación Citrix Workspace o desde el portal web de Citrix Workspace.

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.



Descubra dominios o direcciones IP a los que acceden los usuarios finales

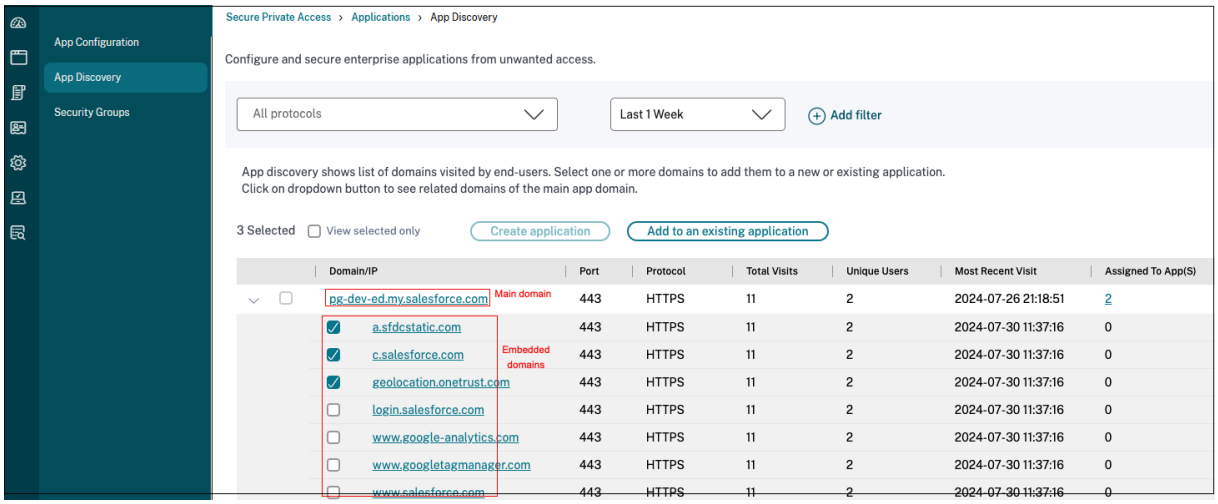
October 21, 2024

La función de descubrimiento de aplicaciones ayuda al administrador a obtener visibilidad de las aplicaciones internas y externas (aplicaciones HTTP/HTTPS y TCP/UDP) a las que se accede en una organización. Esta función descubre y enumera todos los dominios/direcciones IP, publicados o no publicados. De esta forma, los administradores pueden ver qué dominios/direcciones IP están siendo accedidos, quién los está accediendo y decidir si quieren publicarlos como aplicaciones, brindando acceso a esos usuarios.

La función de descubrimiento de aplicaciones proporciona las siguientes capacidades a los administradores:

- Proporciona visibilidad de las direcciones IP/dominios internos o externos a los que acceden los usuarios finales.
- Proporciona una visibilidad completa de todos los tipos de aplicaciones a las que se accede (HTTP, HTTPS, TCP y UDP). Se admiten todos los métodos de acceso, es decir, acceso a través de Citrix Enterprise Browser, Secure Access Agent, Direct Access o Workspace for Web.
- Muestra dominios/direcciones IP publicados o no publicados a los que acceden los usuarios finales.
- Muestra tanto el dominio principal como sus dominios integrados subyacentes que deben configurarse como dominios relacionados al publicar las aplicaciones para el acceso realizado a través de Citrix Enterprise Browser.
- Muestra los dominios integrados en una estructura de árbol. Los administradores pueden hacer clic en el signo de expansión (**>**) en línea con el dominio principal para ver los dominios integrados.
- Permite a los administradores crear nuevas aplicaciones o agregar esos dominios a una aplicación existente si un dominio principal o un dominio integrado (HTTP/HTTPS) o la dirección IP de destino (TCP/UDP) no está asociado con una aplicación.

La siguiente figura muestra un ejemplo de página de descubrimiento de aplicaciones ** . **La página de descubrimiento de aplicaciones**** permite filtrar dominios según el protocolo (HTTP/HTTPS, TCP/UDP) y la dirección IP/dominio y los números de puerto. También muestra los dominios no publicados (no asignados a ninguna aplicación) a los que acceden los usuarios finales. Puede ver un dominio principal con una lista desplegable de dominios integrados debajo de él. Estos dominios deben configurarse como dominios relacionados al publicar la aplicación.



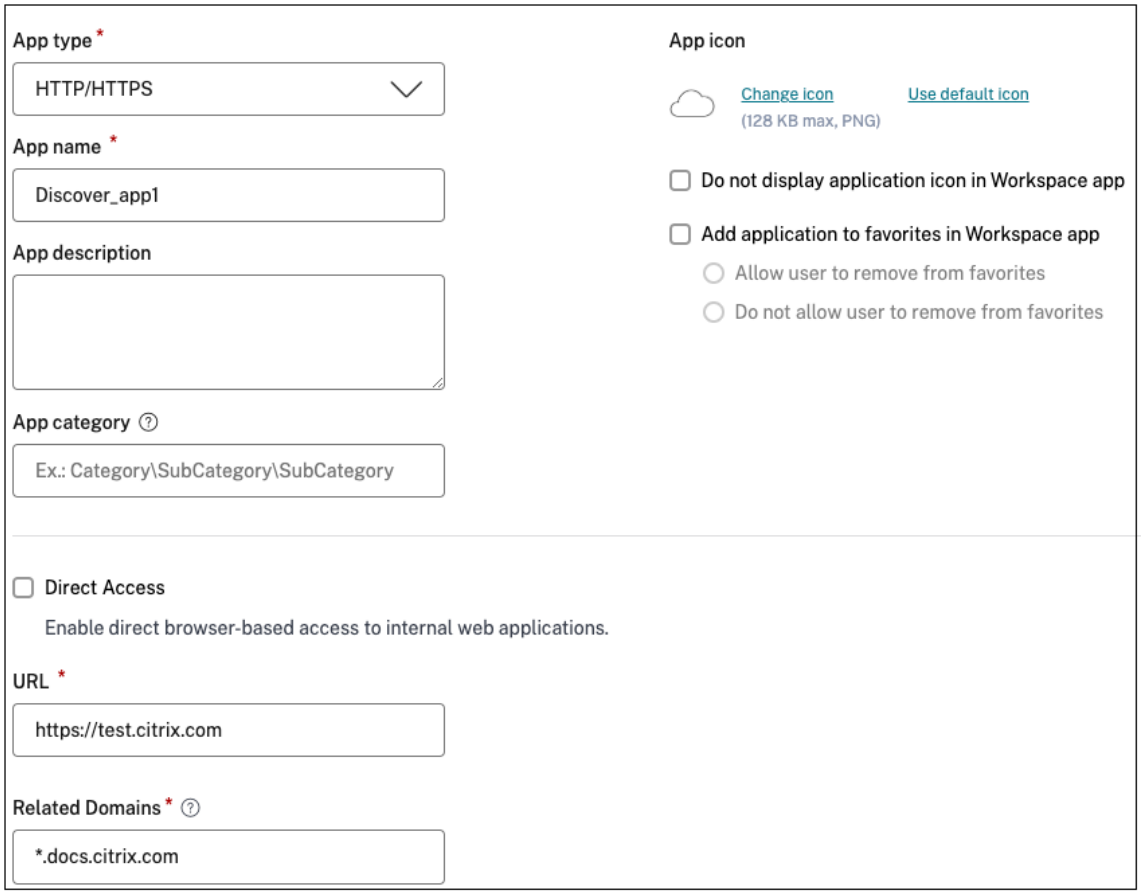
> **Nota**
>
> - Los dominios integrados se agrupan bajo el dominio principal solo para las aplicaciones HTTP/HTTPS a las que se accede a través de Citrix Enterprise Browser. Los dominios TCP/UDP no están agrupados bajo un dominio principal.
> - La agrupación de dominios integrados solo está disponible para aplicaciones a las que se accede desde Citrix Enterprise Browser (v119 y posteriores).

Descubrimiento de aplicaciones para dominios internos en un nuevo entorno

La función de descubrimiento de aplicaciones se puede utilizar si está configurando un nuevo entorno de acceso privado seguro y desea tener visibilidad de las aplicaciones que se configurarán. Esta función descubre y enumera todos los dominios/direcciones IP a los que acceden sus usuarios finales para que pueda configurarlos como aplicaciones. Utilice los siguientes pasos para habilitar la función de descubrimiento de aplicaciones cuando configure su entorno de acceso privado seguro:

- Para descubrir aplicaciones web internas, configure una aplicación dentro de Secure Private Access y especifique el dominio comodín relacionado que pertenece al dominio/subdominio de las aplicaciones que desea descubrir.

  Por ejemplo, si desea descubrir todas las aplicaciones con el dominio citrix.com, cree una aplicación con un dominio comodín relacionado como `*.citrix.com`. Para permitir completar la configuración de la aplicación, agregue cualquier URL de prueba como la sección URL de la aplicación web principal.

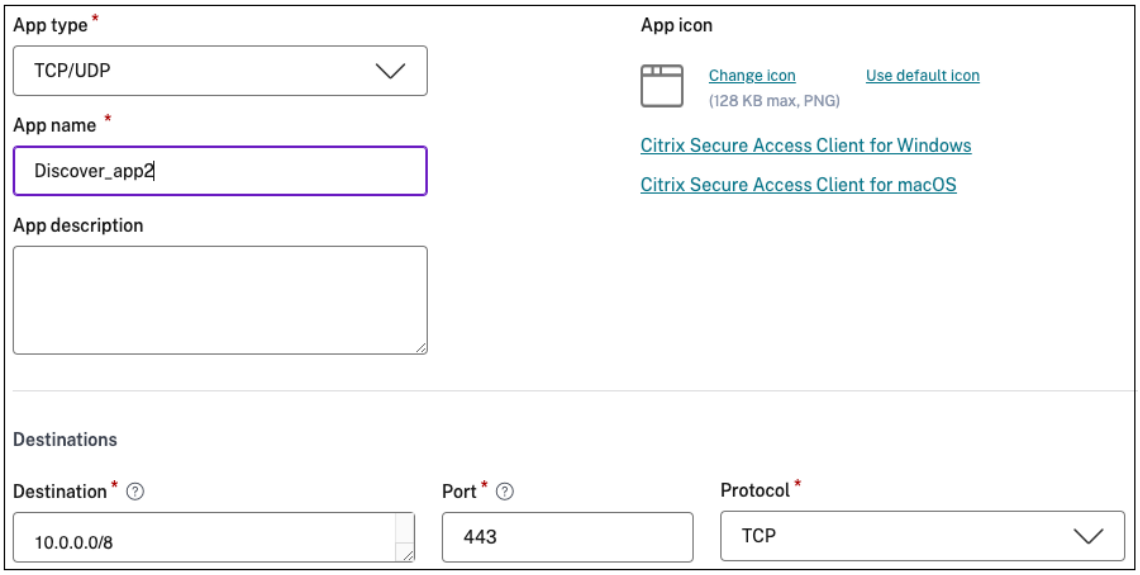


URL de la aplicación web: `https://test.citrix.com/` Dominio relacionado: `*.citrix.com`

- Para aplicaciones TCP/UDP internas, configure una aplicación dentro de Secure Private Access y especifique la subred junto con el protocolo TCP/UDP y el rango de puertos (ingrese * para incluir el rango completo). Esto permite descubrir todas las aplicaciones TCP y UDP desde el agente de Citrix Secure Access. Por ejemplo, si desea descubrir todas las aplicaciones dentro de la subred 10.0.0.0/8, configure la aplicación con los siguientes detalles: Ejemplo: 10.0.0.0/8:

  Puerto: (*)

  Protocolo: TCP



- Una vez que haya creado las aplicaciones, también debe definir los usuarios que tienen permitido el acceso a las aplicaciones con los dominios y las subredes IP configurados. Cree una política de acceso y asigne los usuarios a quienes desea permitir el acceso a los FQDN/direcciones IP configurados en las aplicaciones creadas. Estos pueden ser un conjunto inicial de usuarios de prueba o un número limitado de usuarios a los que desea dar acceso inicialmente.
- Después de crear las aplicaciones y las políticas de acceso correspondientes, los usuarios pueden seguir accediendo a las aplicaciones desde la aplicación Citrix Workspace y acceder a diferentes dominios. Todas las direcciones FQDN/IP a las que acceden los usuarios finales comienzan a aparecer en la página de Descubrimiento de aplicaciones.

> **Nota**
>
> - Una vez que haya descubierto e identificado la mayoría de las aplicaciones durante unos días o semanas, recomendamos eliminar las aplicaciones creadas inicialmente para que se pueda cerrar el acceso más amplio otorgado a través de los dominios comodín y las subredes IP, y solo se pueda permitir el acceso a las URL de aplicaciones específicas y las direcciones IP que se descubran a través de nuevas aplicaciones.
> - Agregue el prefijo `Discover` en el nombre de la aplicación para indicar que esta es una configuración de aplicación especial para habilitar el monitoreo y los informes de descubrimiento. 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 de la aplicación solo a los FQDN específicos y las combinaciones de IP/puerto más adelante en semanas o un mes.
> - Para acceder a las aplicaciones TCP/UDP, los usuarios deben utilizar 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 dentro

de la página **Descubrimiento de aplicaciones** .
- Incluso después de haber eliminado las aplicaciones descubiertas, esta función sigue descubriendo dominios/direcciones IP a los que acceden sus usuarios. Entonces, en cualquier momento, puedes regresar a la página **Descubrimiento de aplicaciones** para ver a qué se está accediendo y si hay nuevos dominios o direcciones IP descubiertos que deben configurarse como aplicaciones.

Para obtener detalles sobre cómo agregar dominios, FQDN o direcciones IP, consulte los siguientes temas.

- Compatibilidad con aplicaciones web empresariales
- Soporte para aplicaciones de software como servicio
- Soporte para aplicaciones cliente-servidor

Crear una aplicación desde la página de descubrimiento de aplicaciones

Para crear una aplicación para dominios integrados o dominios no publicados desde la página de descubrimiento de aplicaciones ** , realice los siguientes pasos:

1. Vaya a **Aplicaciones > Descubrimiento de aplicaciones**.
2. Seleccione un dominio de la lista. Si el dominio tiene dominios integrados, haga clic en el signo de expansión (**>**) en línea con el dominio principal y seleccione los dominios integrados.

Nota

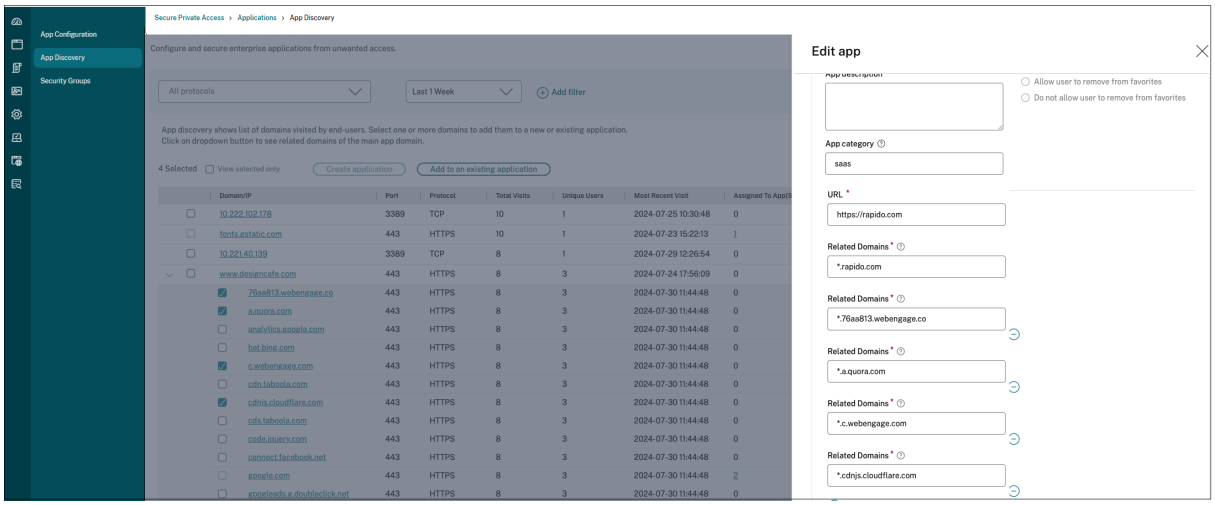
- No puede seleccionar dominios que pertenezcan a diferentes protocolos para crear una aplicación. Se muestra un mensaje de error cuando selecciona dominios que pertenecen a protocolos diferentes.
- Si un dominio ya está asociado a una aplicación, no podrás volver a seleccionar ese dominio para crear una aplicación. La casilla de verificación correspondiente a ese dominio aparece en gris y cuando pasa el mouse sobre la casilla de verificación, aparece una información sobre herramientas.
- No puede seleccionar y agregar dominios integrados agrupados bajo diferentes dominios principales a una aplicación. La función de descubrimiento de aplicaciones solo permite que los dominios integrados agrupados bajo un único dominio principal se agreguen a una aplicación. Aparece un mensaje de error si se seleccionan dominios integrados de diferentes dominios principales y se agregan a la misma aplicación.

1. Haga clic en **Crear aplicación**. Para obtener detalles sobre la creación de una aplicación, consulte Soporte para aplicaciones web empresariales, Soporte para aplicaciones de software como servicioy Soporte para aplicaciones cliente-servidor](/es-es/citrix-secure-private-access/service/spa-support-for-client-server-apps).

Actualizar una aplicación existente

Para agregar un dominio a una aplicación existente, seleccione el dominio de la lista. Si el dominio tiene dominios integrados, haga clic en el signo de expansión (**>**) en línea con el dominio principal y seleccione los dominios integrados.

1. Seleccione el dominio integrado que debe agregarse a una aplicación.
2. Haga clic en **Agregar a una aplicación existente**.
3. En **Aplicaciones**, seleccione la aplicación a la que desea agregar estos dominios.
4. Haga clic en **Obtener detalles de la aplicación**.
5. El campo **Dominios relacionados** muestra todos los dominios integrados que seleccionó anteriormente en filas separadas.
6. Haga clic en **Finish**.

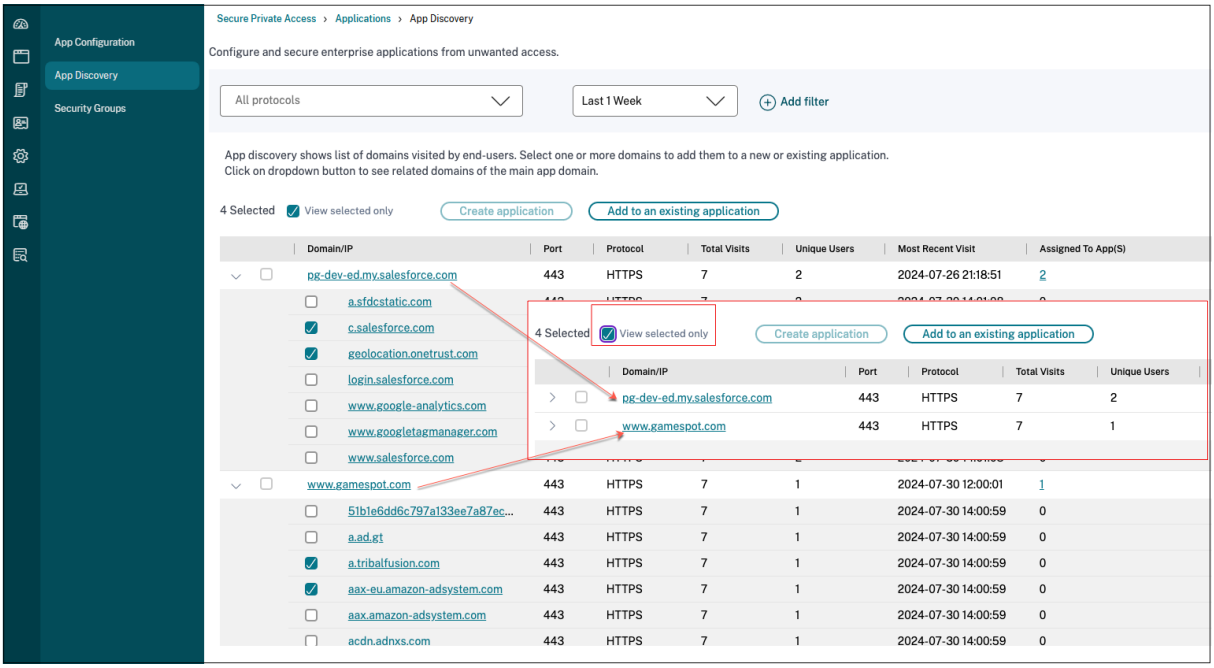


> **Nota**
>
> - Solo puede agregar una dirección IP de destino TCP/UDP a una aplicación TCP/UDP existente. El campo Aplicaciones enumera solo las aplicaciones TCP/UDP configuradas en el sistema.
> - Puede seleccionar una aplicación HTTP/HTTPS o TCP/UDP existente para agregar dominios (principal, de entrada única o integrado) cuyo protocolo sea HTTP/HTTPS.
> - No puede seleccionar un dominio que ya esté asociado a una aplicación.

Ver todos los dominios integrados seleccionados

Después de seleccionar los dominios, puede hacer clic en la casilla de verificación **Ver solo los seleccionados** y continuar con la creación o actualización de la aplicación. Además, si la lista de direcciones FQDN/IP en la página de descubrimiento de aplicaciones se extiende a lo largo de varias

páginas, puede usar la casilla de verificación **Ver solo los seleccionados** para ver todos los dominios principales e integrados que ha seleccionado para crear o actualizar la aplicación. Cuando se selecciona esta casilla de verificación, se muestran todos los dominios principales de los dominios integrados seleccionados.



Limitaciones conocidas

- Aunque las opciones **Crear aplicación** y **Agregar a aplicación existente** están disponibles en el panel de acceso privado seguro (gráfico**Principales aplicaciones descubiertas por visitas totales**), se recomienda crear o actualizar una aplicación desde la pestaña **Descubrimiento de aplicaciones** (gráfico**Aplicaciones > Descubrimiento de aplicaciones**). Esto se debe a que, al agregar o actualizar una aplicación desde el panel de control y cancelas la operación, la página se vuelve a cargar y, como resultado, se restablecen todas las configuraciones.
- A veces, es posible que notes el signo de expansión (>) junto a un dominio principal, pero los dominios integrados no se obtienen para ese FQDN específico. Este problema puede ocurrir en los siguientes casos:
  - Error al cargar la página principal debido a algunas restricciones de acceso para los usuarios.
  - Un error que impide la carga de la página web.
  - El almacenamiento en caché de los recursos de dominio integrados por parte de Citrix Enterprise Browser, lo que provoca que los dominios integrados no se obtengan de la fuente.

Mejores prácticas para configuraciones de aplicaciones web y SaaS

June 19, 2024

El acceso a las aplicaciones publicadas y no publicadas depende de las aplicaciones y directivas de acceso configuradas en el servicio Secure Private Access.

Acceso a aplicaciones dentro de Secure Private Access para aplicaciones publicadas y no publicadas

- **Acceso a aplicaciones web publicadas y dominios relacionados:**
  - Cuando un usuario final accede a un FQDN asociado a una aplicación web publicada, el acceso solo se permite si se configura una directiva de acceso de forma explícita con la acción **Permitir** o **Permitir con restricciones** para el usuario.

    > **Nota:**
    >
    > Se recomienda que varias aplicaciones no compartan el mismo dominio URL de la aplicación o dominios relacionados para obtener una coincidencia exacta. Si varias aplicaciones comparten el mismo dominio URL de la aplicación o dominios relacionados, el acceso se proporciona en función de la coincidencia exacta del FQDN y de la priorización de las directivas. Para más información, consulte Equiparación y priorización de directivas de acceso.

  - Si ninguna directiva de acceso coincide con la aplicación publicada o si una aplicación no está asociada a ninguna 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 web internas no publicadas y URL de Internet externas:**

  Para habilitar la confianza cero, Secure Private Access niega el acceso a las direcciones URL de intranet o aplicaciones web internas que no estén asociadas a una aplicación y que no tengan una directiva de acceso configurada para la aplicación. Para permitir el acceso a usuarios específicos, asegúrese de tener una directiva de acceso configurada para las aplicaciones web de la intranet.

  Para cualquier URL que no esté configurada como una aplicación en Secure Private Access, el tráfico fluye directamente a Internet.

  - En estos casos, el acceso a los dominios URL de las aplicaciones web de la intranet se enruta directamente y, por lo tanto, se deniega el acceso (a menos que el usuario ya esté dentro de la intranet).

- En el caso de las URL de Internet no publicadas, el acceso se basa en las reglas configuradas para las aplicaciones no autorizadas, si están habilitadas. De forma predeterminada, este acceso está permitido en Secure Private Access. Para obtener más información, consulte Configurar reglas para sitios web no autorizados.

Equiparación y priorización de directivas de acceso

Secure Private Access hace lo siguiente al hacer coincidir una solicitud de acceso:

1. Haga coincidir el dominio al que se accede con el dominio de la URL de la aplicación o con los dominios relacionados para obtener una coincidencia exacta.
2. Si se encuentra una aplicación de Secure Private Access configurada con un FQDN exacto, Secure Private Access evalúa todas las directivas configuradas para esa aplicación.
   - Las directivas se evalúan en orden de prioridad hasta que el contexto del usuario coincida. La acción (permitir/denegar) se aplica según la primera directiva que coincida en el orden de prioridad.
   - Si ninguna directiva coincide, se deniega el acceso de forma predeterminada.
3. Si no se encuentra una coincidencia exacta de FQDN, Secure Private Access busca el dominio basándose en la coincidencia más larga (por ejemplo, una coincidencia de caracteres comodín) para buscar las aplicaciones y las directivas correspondientes.

   Ejemplo 1: Tenga en cuenta las siguientes configuraciones de aplicaciones y directivas:

Aplicación	URL de la aplicación	Dominio relacionado
Intranet	`https://app.intranet.local`	*.cdn.com
wiki	`https://wiki.intranet.local`	*.intranet.local

Nombre de directiva	Prioridad	Aplicaciones de usuario y asociadas
PolicyA	Alto	Eng-User5 (Intranet)
PolicyB	Bajo	HR-User4 (Wiki)

Si `HR-User4` accede `app.intranet.local`, ocurre lo siguiente:

a) Secure Private Access busca en todas las directivas una coincidencia exacta con el dominio al que se accede, `app.intranet.local` en este caso.
b) Secure Private Access busca `PolicyA` y comprueba si las condiciones coinciden.
c) Como las condiciones no coinciden, Secure Private Access se detiene aquí y no continúa comprobando las coincidencias de los comodines, aunque `PolicyB` habría coincidido (ya que `app.intranet.local` coincide en el dominio relacionado de la aplicación Wiki de `*.intranet.local`) y habría dado acceso.
d) Por lo tanto, `HR-User4` se niega el acceso a la aplicación Wiki.

Ejemplo 2: Considere la siguiente configuración de aplicaciones y directivas en las que se usa el mismo dominio en varias aplicaciones:

Aplicación	URL de la aplicación	Dominio relacionado
App1	xyz.com	app.intranet.local
App2	app.intranet.local	-

Nombre de directiva	Prioridad	Aplicaciones de usuario y asociadas
PolicyA	Alto	Eng-User 5 (Aplicación 1)
PolicyB	Bajo	HR-User7 (Aplicación 2)

Cuando el usuario `Eng-User5` acceda a `app.intranet.local`, tanto la App1 como la App2 coincidirán en función de la coincidencia exacta del FQDN y, por lo tanto, el usuario `Eng-User5` tendrá acceso a través de `PolicyA`.

Sin embargo, si App1 tuviera `*.intranet.local` como dominio relacionado, se habría denegado el acceso para `Eng-User5`, ya que `app.intranet.local` habría coincidido exactamente con `PolicyB`, a la cual el usuario `Eng-User5` no tiene acceso.

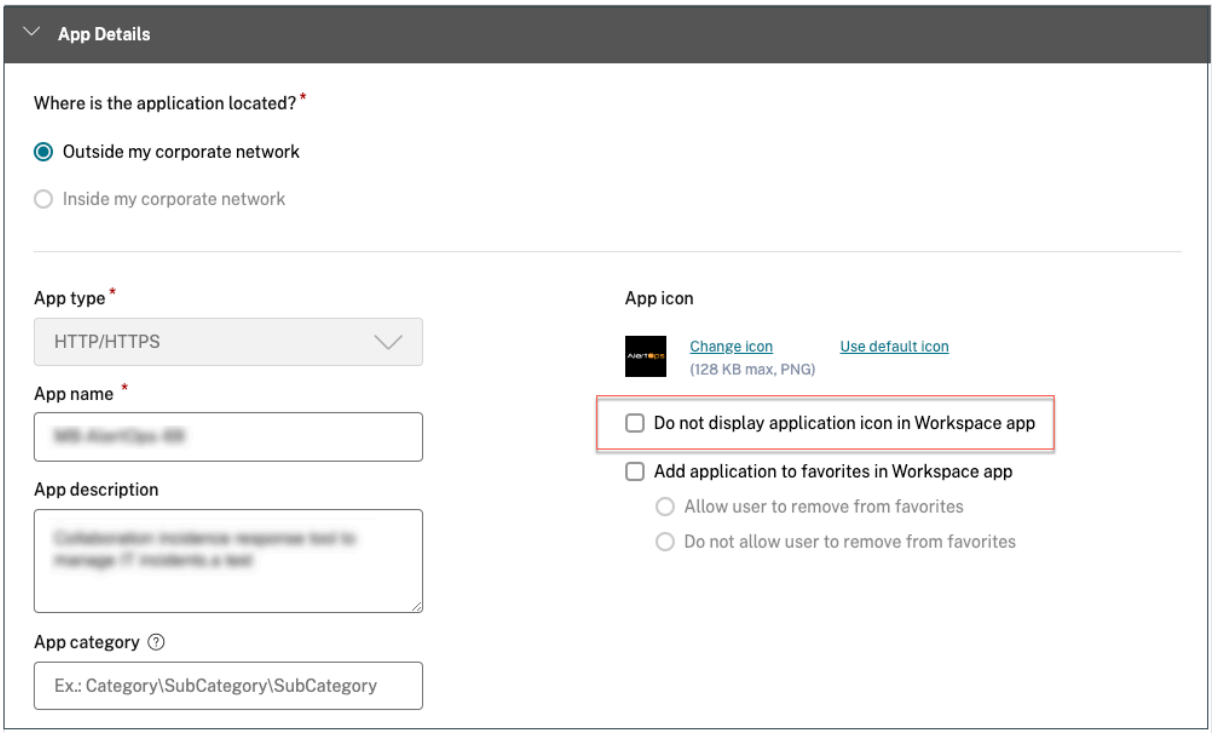
Mejores prácticas de configuración de aplicaciones

Los dominios IDP deben tener una aplicación propia

En lugar de agregar dominios de IDP como dominios relacionados en las configuraciones de las aplicaciones de intranet, le recomendamos lo siguiente:

- Cree aplicaciones independientes para todos los dominios de IDP.

- Cree una directiva para permitir el acceso a todos los usuarios que necesitan acceder a la página de autenticación de IDP y mantenga la directiva como la máxima prioridad.
- Oculte esta aplicación (seleccionando la opción **No mostrar el icono de la aplicación a los usuarios**) de la configuración de la aplicación para que no aparezca en el espacio de trabajo. Para obtener más información, consulte Configurar los detalles de la aplicación.



> **Nota:**
>
> La configuración de esta aplicación solo permite el acceso a la página de autenticación de IDP. El acceso adicional a las aplicaciones individuales sigue dependiendo de las configuraciones de las aplicaciones individuales y de sus respectivas directivas de acceso.

Ejemplo de configuración:

1. Configure todos los FQDN comunes en sus propias aplicaciones, agrupándolos cuando corresponda.

   Por ejemplo, si tiene algunas aplicaciones que usan Azure AD como IdP y necesita configurar `login.microsoftonline.com` y otros dominios relacionados (`*.msauth.net`), haga lo siguiente:

   - Cree una única aplicación común con `https://login.microsoftonline.com` como URL de la aplicación y `*.login.microsoftonline.com` y `*.msauth.net` como dominios relacionados.

2. Seleccione la opción **No mostrar el icono de la aplicación a los usuarios** al configurar la aplicación. Para obtener más información, consulte Configurar los detalles de la aplicación.
3. 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.
4. Asigne la máxima prioridad a la directiva de acceso. Para obtener más información, consulte Orden prioritario.
5. Verifique los registros de diagnóstico para confirmar que el FQDN coincide con la aplicación y que la directiva se aplica según lo previsto.

Los mismos dominios relacionados no deben formar parte de varias aplicaciones

El dominio relacionado debe ser exclusivo de una aplicación. Las configuraciones conflictivas pueden provocar problemas de acceso a las aplicaciones. Si se configuran varias aplicaciones con el mismo FQDN o alguna variación del FQDN comodín, es posible que surjan 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.

Por lo tanto, recomendamos tener un dominio relacionado único para configurarlo en una sola aplicación.

Ejemplos de configuración incorrectos:

- **Ejemplo: dominios relacionados duplicados en varias aplicaciones**

  Supongamos que tiene 2 aplicaciones en las que ambas necesitan acceder a Okta (example.okta.com):

Aplicación	dominio URL de la aplicación	Dominio relacionado
App1	`https://code.example.net`	example.okta.com
App2	`https://info.example.net`	example.okta.com

Nombre de directiva	Prioridad	Aplicaciones de usuario y asociadas
Denegar App1 a HR	Alto	Grupo de usuarios HR para App1
Otorgar a todos el acceso a la aplicación 1	Medio	Habilitar el acceso al grupo de usuarios Everyone to App1
Otorgue a todos el acceso a App2	Bajo	Habilitar el acceso al grupo de usuarios "Todos"a App2

Problema con la configuración: aunque la intención era dar acceso a todos los usuarios a App2, el grupo de usuarios HR no puede acceder a App2. El grupo de usuarios HR se redirige a Okta, pero se bloquea debido a la primera directiva que denegó el acceso a la App1 (que también tiene el mismo dominio relacionado `example.okta.com` que App2).

Este escenario es muy común para los proveedores de identidad como Okta, pero también puede ocurrir con otras aplicaciones estrechamente integradas con dominios relacionados comunes. Para obtener más información sobre la coincidencia y priorización de directivas, consulte Equiparación y priorización de directivas de acceso.

Recomendación para la configuración anterior:

1. Elimine example.okta.com como dominio relacionado de todas las aplicaciones.
2. Crea una nueva aplicación solo para Okta (con la URL de la aplicación `https://example.okta.com` y un dominio relacionado de `*.okta.com`).
3. Oculta esta aplicación del espacio de trabajo.
4. Asigne la máxima prioridad a la directiva para eliminar cualquier conflicto.

Práctica óptima:

- Los dominios relacionados de una aplicación no deben superponerse con los dominios relacionados de otra aplicación.
- Si esto ocurre, se debe crear una nueva aplicación publicada para cubrir el dominio relacionado compartido y después el acceso debe configurarse en consecuencia.
- Los administradores deben evaluar si este dominio relacionado compartido debe aparecer como una aplicación real en Workspace.
- Si la aplicación no debe aparecer en Workspace, al publicarla, seleccione la opción **No mostrar el icono de la aplicación a los usuarios** para ocultarla de Workspace.

URL de enlace profundo

Para las URL de enlace profundo, se debe agregar el dominio URL de la aplicación de intranet como dominio relacionado:

Ejemplo:

La aplicación de intranet tiene una URL configurada con `https://example.okta.com/deep-link-app-1` como dominio URL de la aplicación principal y el dominio relacionado tiene el dominio URL de la aplicación de intranet, es decir, `*.issues.example.net`.

En este caso, cree por separado una aplicación de IdP con la URL `https://example.okta.com` y después el dominio relacionado como `*.example.okta.com`.

Terminar sesiones de usuarios activos y agregar usuarios a la lista de bloqueo de usuarios

October 21, 2024

Los administradores pueden finalizar todas las sesiones de usuarios finales activos inmediatamente y agregarlos a la lista de bloqueo de usuarios. Agregar un usuario a esta lista de bloqueo de usuarios finaliza todas las sesiones activas de la aplicación Secure Private Access y bloquea el acceso futuro a la aplicación.

Se finalizan y bloquean todas las sesiones de aplicaciones activas a través de Citrix Enterprise Browser, acceso directo, CWA para HTML5 y el agente de acceso seguro. Todos los recursos conectados a través del agente de acceso seguro, como recursos compartidos de archivos, RDP y sesiones SSH, también se finalizan y bloquean. Los usuarios bloqueados no pueden iniciar ninguna aplicación nueva hasta que se los elimine de la lista de usuarios bloqueados.

> **Nota**
>
> - Agregar un usuario a la lista de bloqueo de usuarios no cambia ni edita la política de acceso privado seguro configurada. La terminación y el bloqueo del acceso ocurren independientemente de la política de acceso configurada. Una vez que se elimina al usuario de la lista, se restablecen las políticas de acceso privado seguro existentes para el usuario.
> - Sólo se bloquea el acceso a las aplicaciones publicadas de Secure Private Access. El acceso a Internet a través de Citrix Enterprise Browser se permite o se deniega incluso después de que se agrega un usuario a la lista de bloqueo según su configuración de filtrado web .

Casos de uso

Puede utilizar esta función en los siguientes escenarios.

- Un empleado abandona la organización o es despedido de la misma. En este caso, el administrador revoca todo acceso a la aplicación Secure Private Access finalizando las sesiones activas de Secure Private Access y bloqueando cualquier acceso futuro a la aplicación.
- Se pierde o se roba un dispositivo. En este caso, se bloquea el acceso y se finalizan todas las sesiones actuales. El usuario puede ser eliminado de la lista de bloqueo de usuarios después de que la situación esté bajo control.
- Un usuario hace mal uso del acceso a la aplicación. En este caso, el acceso al usuario podrá ser revocado inmediatamente. El acceso está bloqueado hasta que el usuario se agregue a la lista.

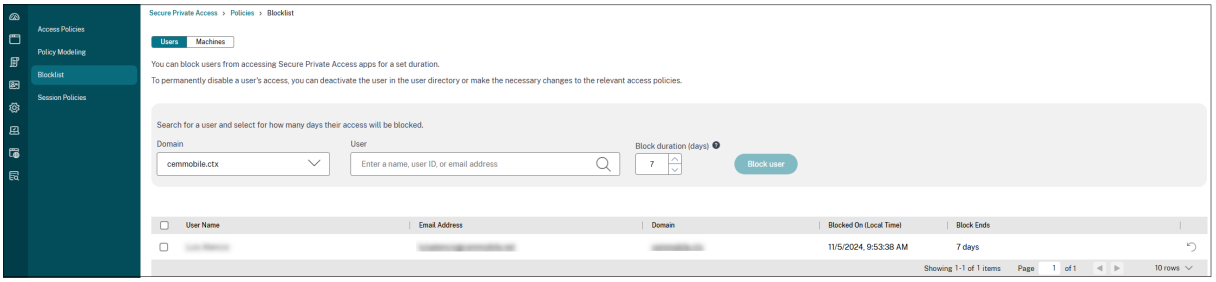
Agregar usuarios a la lista de bloqueo de usuarios

1. Vaya a **Acceso privado seguro > Políticas de acceso** y luego haga clic en la pestaña **Lista de bloqueo de usuarios** .
2. En **Dominio**, seleccione el dominio para el cual se debe deshabilitar el acceso.
3. En **Usuario**, busque el nombre de usuario que debe agregarse a la lista de bloqueo de usuarios. Se muestran todos los nombres de usuario que coinciden con los criterios de búsqueda. Si se elimina al usuario del servicio de directorio, ese nombre de usuario no aparece en la lista **Usuario** .
4. En **Duración del bloqueo (días)**, ingrese la cantidad de días durante los cuales este usuario debe estar bloqueado. Una vez que agregas al usuario a la lista de bloqueados, quedará bloqueado durante 7 días de forma predeterminada. Sin embargo, puedes cambiar la duración a cualquier valor entre 1 y 99 días. Una vez finalizada la duración, el acceso del usuario se restablece según el directorio de usuarios y la configuración de políticas. Además, este valor permanece persistente para el usuario para futuras adiciones. Por ejemplo, si un administrador establece la duración del bloqueo para un usuario en 30 días, esta configuración persistirá para el usuario en el futuro.
5. Haga clic en **Bloquear usuario**.

   El usuario se agrega a la lista de usuarios bloqueados. Las siguientes acciones ocurren una vez que el usuario se agrega a la lista de bloqueo de usuarios:

   - Todas las sesiones activas de acceso privado seguro se finalizan inmediatamente.
   - El acceso futuro a todas las aplicaciones publicadas de Secure Private Access está bloqueado.

- El acceso a Internet a través de Citrix Enterprise Browser está permitido incluso después de que un usuario se agregue a la lista de usuarios bloqueados. Sólo se bloquea el acceso a las aplicaciones publicadas de Secure Private Access.



Puede restaurar el acceso incluso antes de que finalice la duración del bloqueo realizando uno de los siguientes pasos.

- Seleccione el acceso para el cual debe restaurar el acceso y luego haga clic en **Restaurar acceso**.
- Haga clic en el icono de restauración correspondiente al usuario para el cual desea restaurar el acceso.

En ambos casos, aparece un cuadro de diálogo de confirmación.

> **Recomendaciones:**
>
> - Para revocar el acceso de un usuario de forma indefinida, elimine al usuario de su servicio de directorio respectivo, como Active Directory, y luego agréguelo a la lista de bloqueo de usuarios. Esto finaliza la sesión activa de acceso privado seguro del usuario, bloquea el acceso futuro a la aplicación y, una vez que el usuario cierra sesión en Workspace, no puede iniciar sesión nuevamente debido a credenciales de directorio inactivas.

Tiempos de espera para las sesiones de usuario

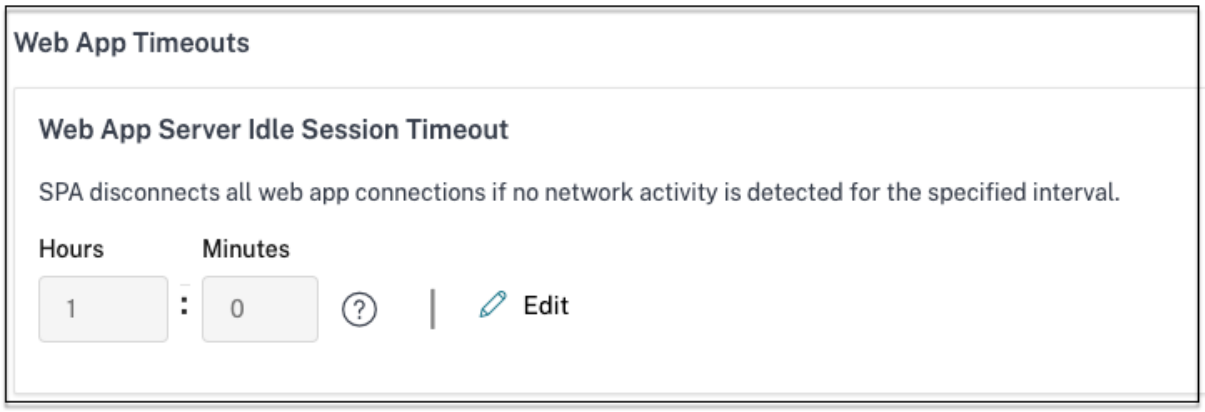
December 27, 2023

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.

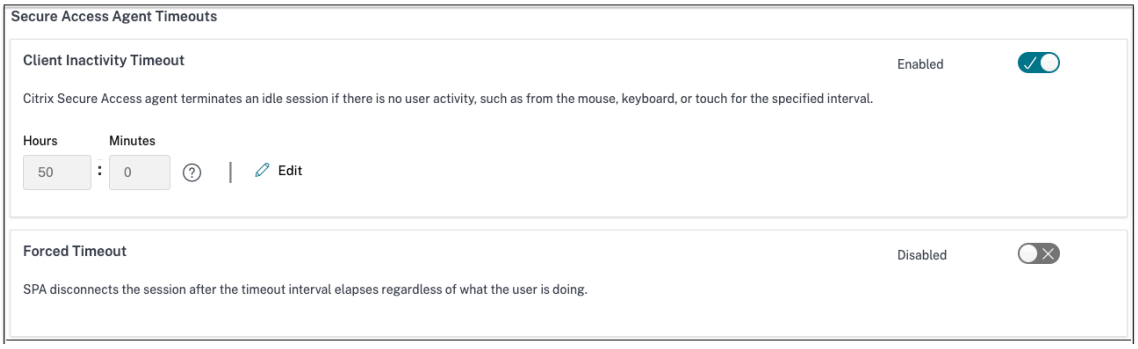


Tiempos de espera para el cliente Citrix Secure Access

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.

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.

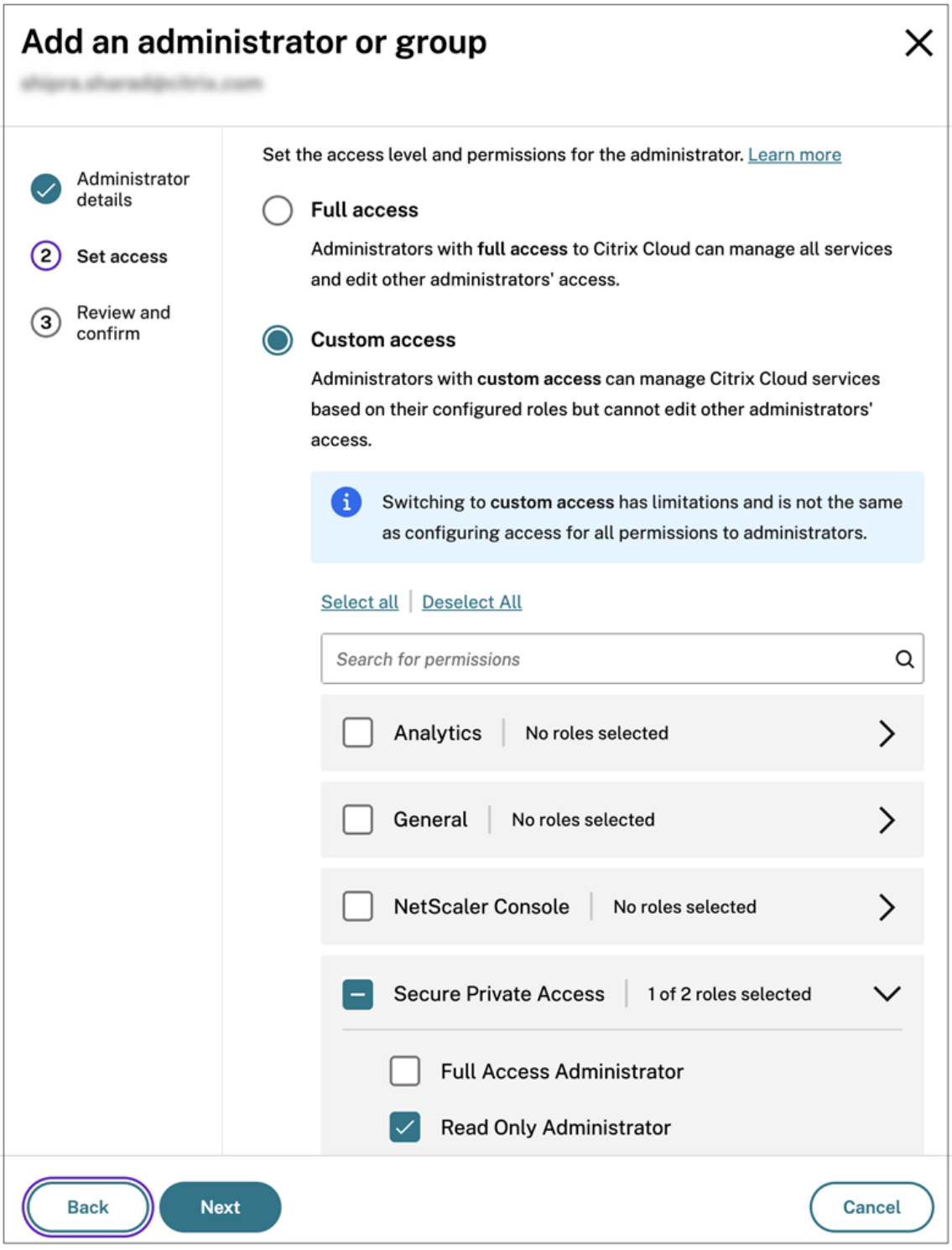
- Agregue aplicaciones web o SaaS empresariales.
- Agregue nuevos dispositivos de conector en ubicaciones de recursos nuevas o existentes.

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**.

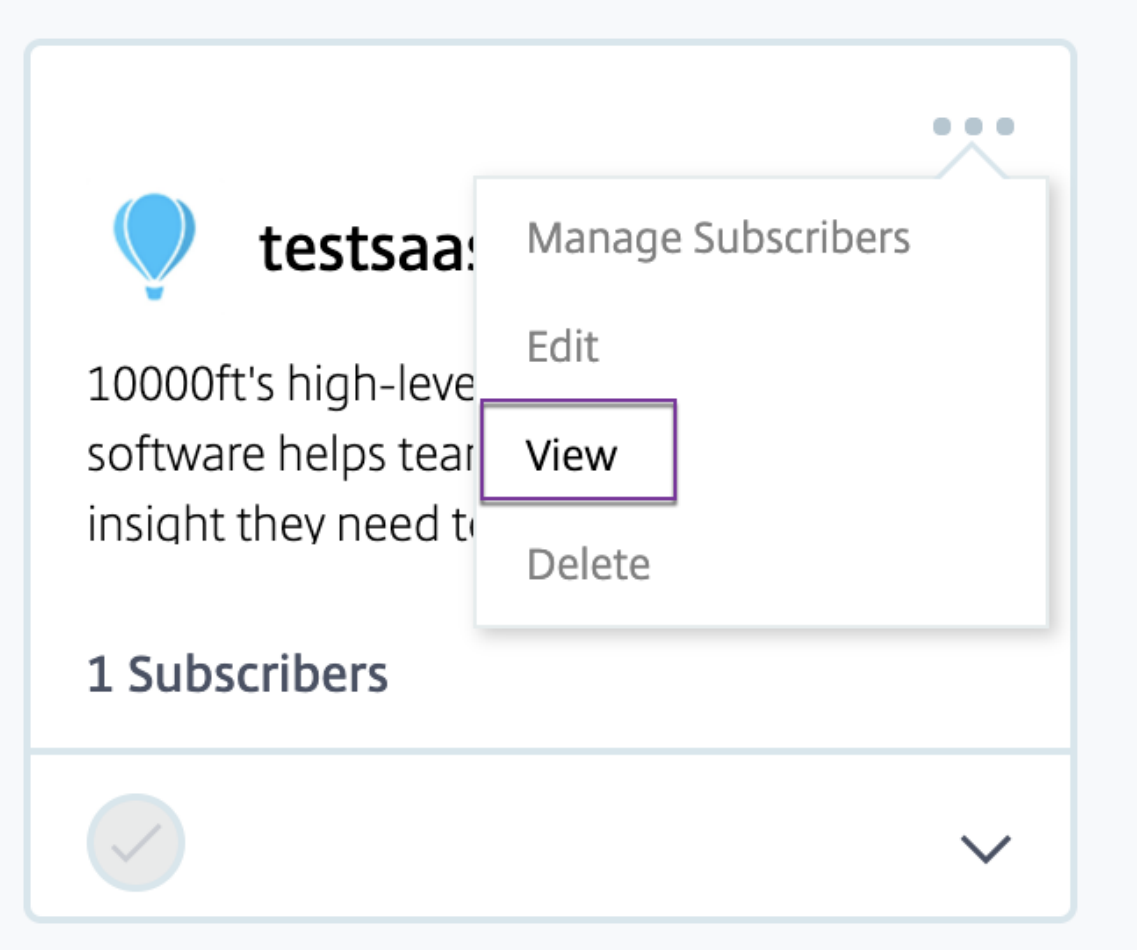
> **Importante:**
>
> - Cuando proporciona acceso de **administrador de solo lectura** a los administradores del

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.

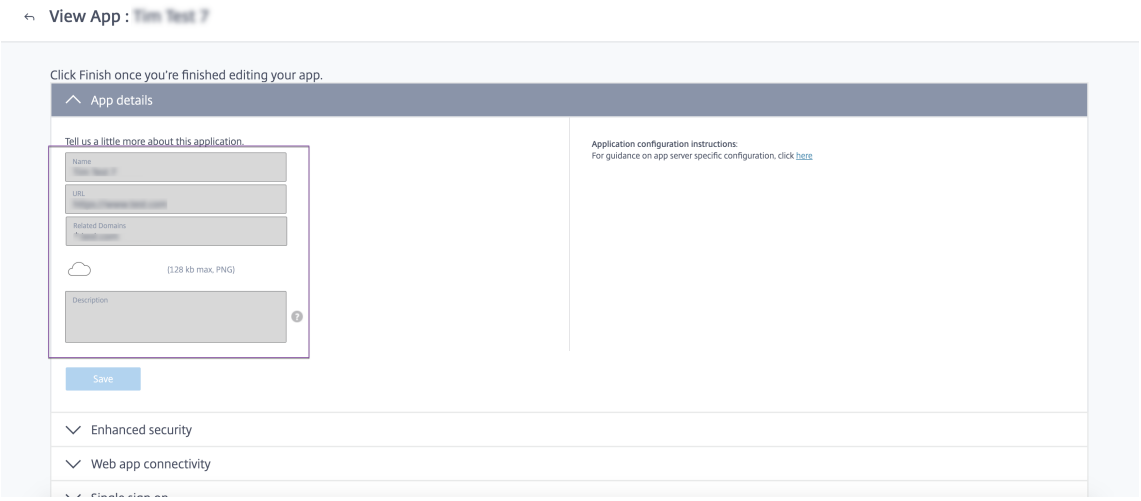
- El botón **Agregar una aplicación web/SaaS** está inhabilitado para los usuarios con acceso de **administrador de solo lectura**.

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**.



Descripción general del panel de control

October 21, 2024

El panel del servicio de acceso privado seguro muestra los datos de diagnóstico y uso de las aplicaciones SaaS, web, TCP y UDP. El panel proporciona a los administradores visibilidad completa de sus aplicaciones, usuarios, estado de los conectores y uso del ancho de banda en un solo lugar para el consumo. Estos datos se obtienen de Citrix Analytics. Los datos de las distintas entidades se pueden visualizar para el tiempo preestablecido o para una línea de tiempo personalizada. Para algunas de las entidades, puedes desglosarlas para ver más detalles.

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

- **Registro y resolución de problemas**
  - Registros de diagnóstico: registros relacionados con la autenticación, el inicio de aplicaciones, la enumeración de aplicaciones y las comprobaciones de la postura del dispositivo.
- **Usuarios**
  - Usuarios activos: Número total de usuarios únicos que acceden a las aplicaciones (SaaS, Web y TCP) durante el intervalo de tiempo seleccionado.
  - Cargas: Datos de volumen total cargados a través del servicio de acceso privado seguro durante el intervalo de tiempo seleccionado.
  - Descargas: Volumen total de datos descargados a través del servicio de Acceso Privado Seguro durante el intervalo de tiempo seleccionado.
- **Aplicaciones:**

  - Aplicaciones: Número total de aplicaciones (independiente del intervalo de tiempo) configuradas actualmente.
  - Recuento de lanzamientos de aplicaciones: número total de aplicaciones (sesiones de aplicaciones) iniciadas por cada usuario durante el intervalo de tiempo seleccionado.
  - Dominios configurados: Número total de dominios configurados para el intervalo de tiempo seleccionado.
  - Aplicaciones descubiertas: Número total de dominios individuales y únicos a los que se ha accedido pero que no están asociados con ninguna aplicación

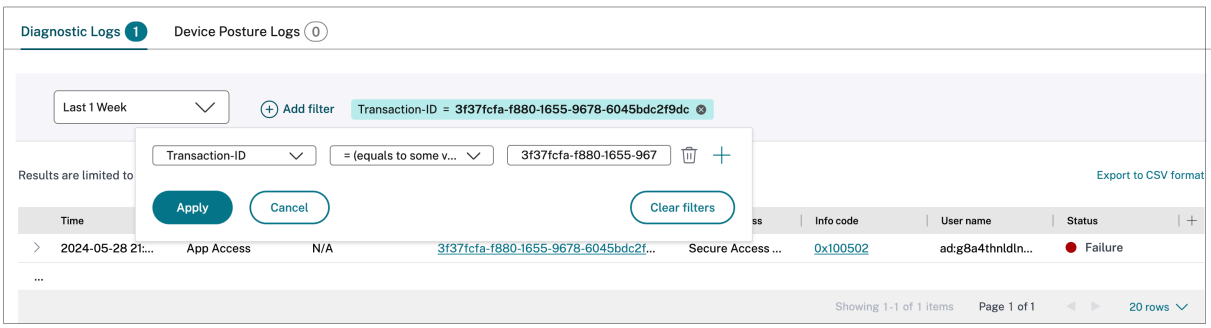
- **Políticas de acceso**

  - Políticas de acceso: Número total de políticas de acceso (independientes del intervalo de tiempo) configuradas actualmente.

Registros de diagnóstico

Utilice el gráfico **Registros de diagnóstico** para ver los registros relacionados con la autenticación, el inicio de aplicaciones, 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 del tiempo preestablecido o de una línea de tiempo personalizada. Puede agregar columnas al gráfico haciendo clic en el signo + según la información que desee ver en el panel. Puede exportar los registros de usuario en formato CSV.

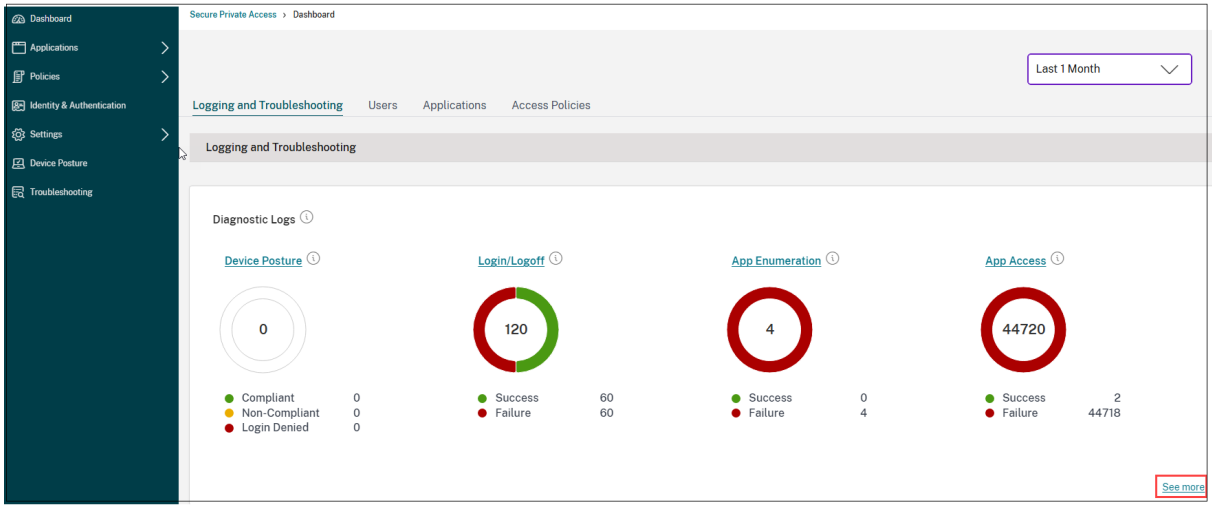
- Puede utilizar la opción **Agregar filtro** para refinar su búsqueda en función de diversos criterios, como el tipo de aplicación, la categoría y la descripción. Por ejemplo, en los campos de búsqueda, puede seleccionar `ID de transacción`, `= (es igual a algún valor)` e ingresar `7456c0fb-a60d-4bb9-a2a2-edab8340bb15`en esta secuencia, para buscar todos los registros relacionados con este ID de transacción. Para obtener detalles sobre los operadores de búsqueda que se pueden utilizar con la opción de filtro, consulte Operadores de búsqueda.



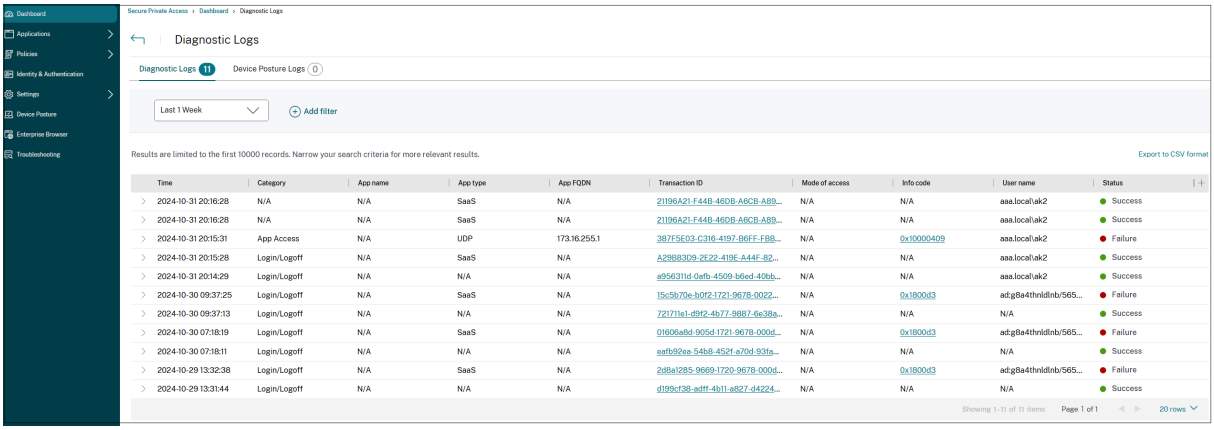
- **Registros de postura del dispositivo:** Puede refinar su búsqueda en función de los resultados

de la política (**Cumple, No cumple e inicio de sesión denegado**). Para obtener detalles sobre la postura del dispositivo, consulte Postura del dispositivo.

> **Nota**
>
> - Cada evento de falla dentro del panel de registros de diagnóstico de Secure Private Access tiene un código de información asociado. Para obtener más detalles, consulte el código de información .
> - El ID de transacción correlaciona todos los registros de acceso privado seguro para una solicitud de acceso. Para obtener más detalles, consulte ID de transacción.



- Puede hacer clic en el icono de expansión (>) para ver los detalles completos de los registros.
- La página **Registros de diagnóstico** muestra los dominios integrados para cada una de las URL principales a las que se accede. Los administradores pueden ver los dominios integrados haciendo clic en el ícono de expansión (>) desde la URL principal. Los administradores pueden usar la lista de dominios integrados para abordar problemas relacionados con el acceso a las aplicaciones o la representación de las aplicaciones. Por ejemplo, si se omitió un dominio en la configuración de la aplicación, el usuario final no podrá acceder a la aplicación específica. En este caso, el administrador puede ver la lista de dominios integrados, identificar el dominio faltante y luego actualizar la configuración de la aplicación con el dominio faltante.

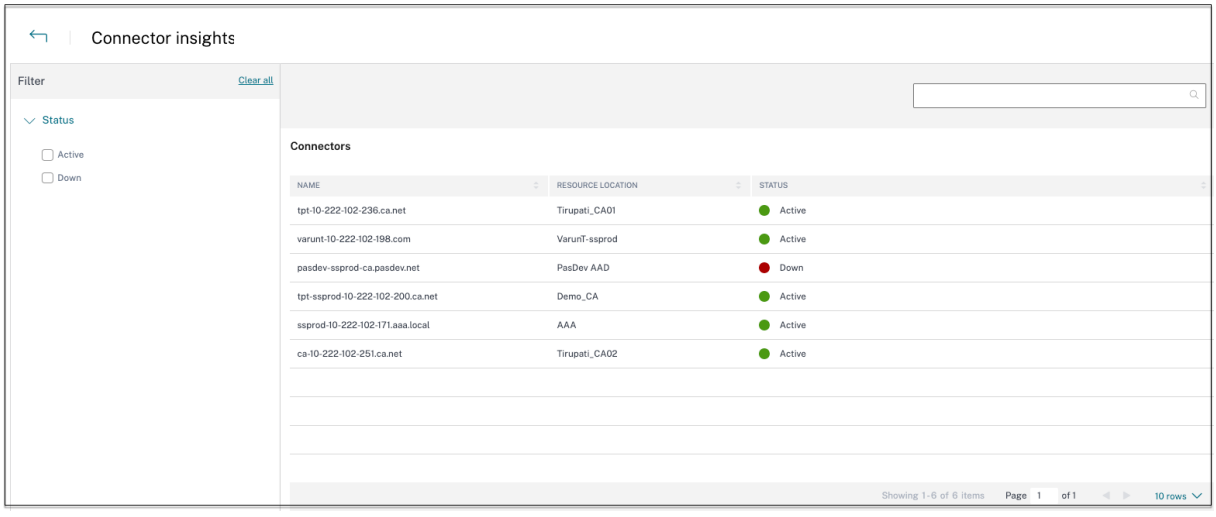


Nota

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

Estado del conector

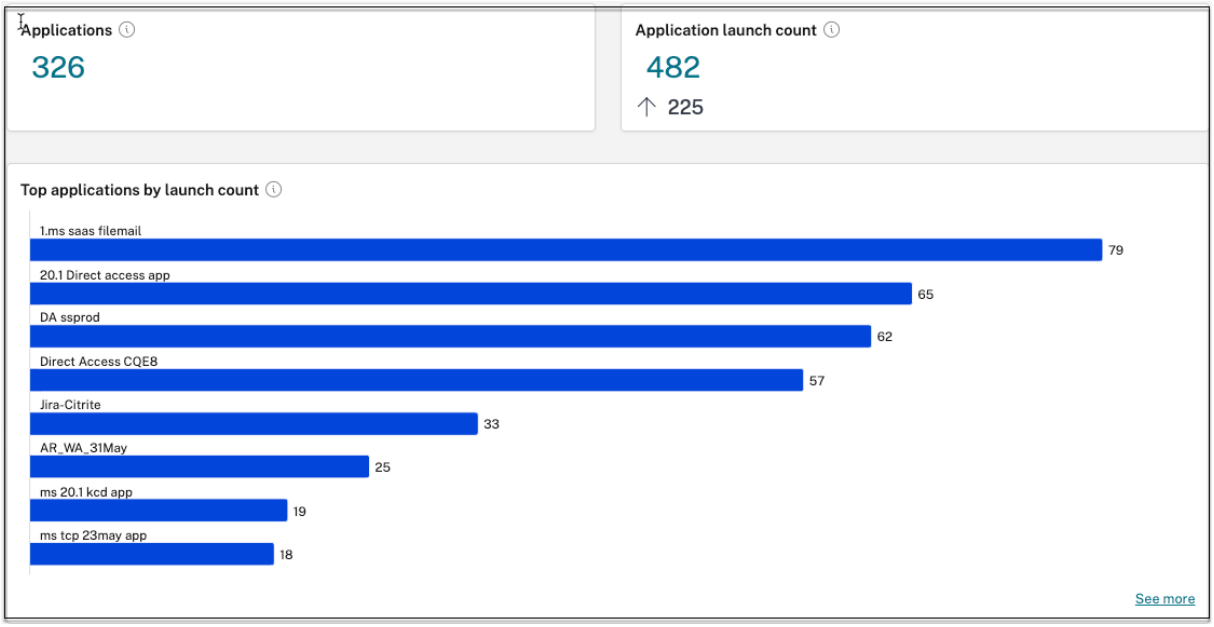
Utilice el gráfico **Estado del conector** para ver el estado de los conectores y las ubicaciones de recursos donde están implementados los conectores. Haga clic en el enlace **Ver más** para ver los detalles. En la página **Información del conector** , puedes usar los filtros **Activo** o **Inactivo** para filtrar los conectores según su estado.



Principales aplicaciones por número de lanzamientos

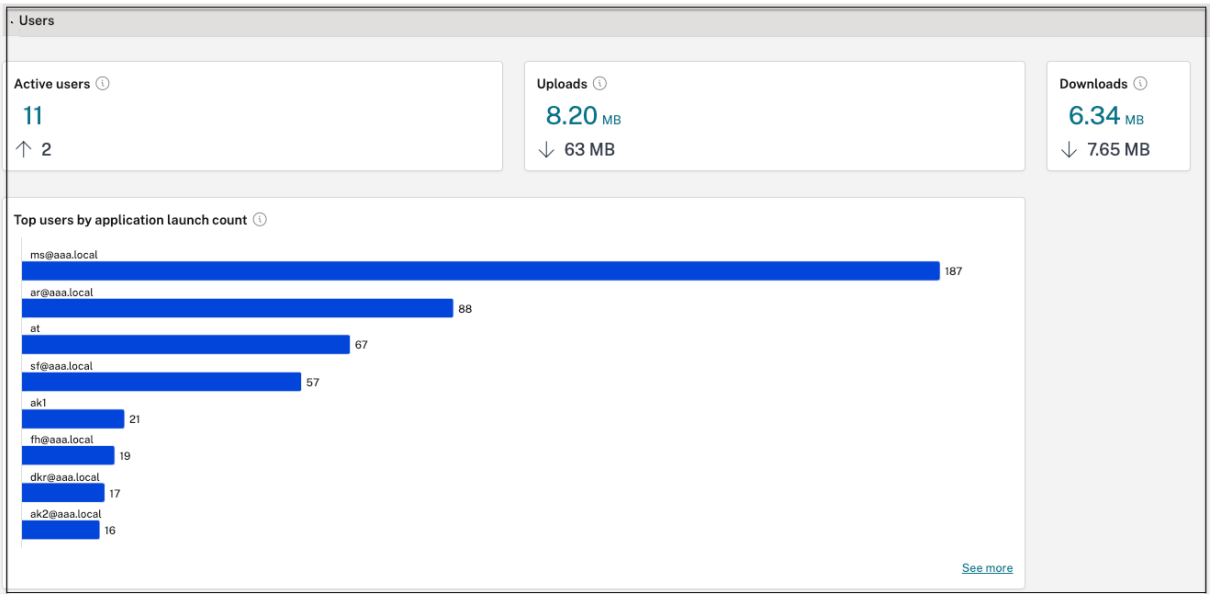
Utilice el gráfico **Principales aplicaciones por cantidad de lanzamientos** para ver la lista de las principales aplicaciones según la cantidad de veces que se lanzó la aplicación, el volumen total de datos

cargados al 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 su búsqueda a aplicaciones específicas. Puede filtrar los datos para una línea de tiempo preestablecida o para una línea de tiempo personalizada.



Principales usuarios por número de lanzamientos de aplicaciones

Utilice el gráfico **Principales usuarios por conteo de lanzamiento de aplicaciones** para ver los datos por usuario. Por ejemplo, la cantidad de veces que un usuario inició la aplicación TCP, el volumen total de datos cargados al servidor de aplicaciones y el volumen total de datos descargados del servidor de aplicaciones. Puede filtrar los datos para una línea de tiempo preestablecida o para una línea de tiempo personalizada.

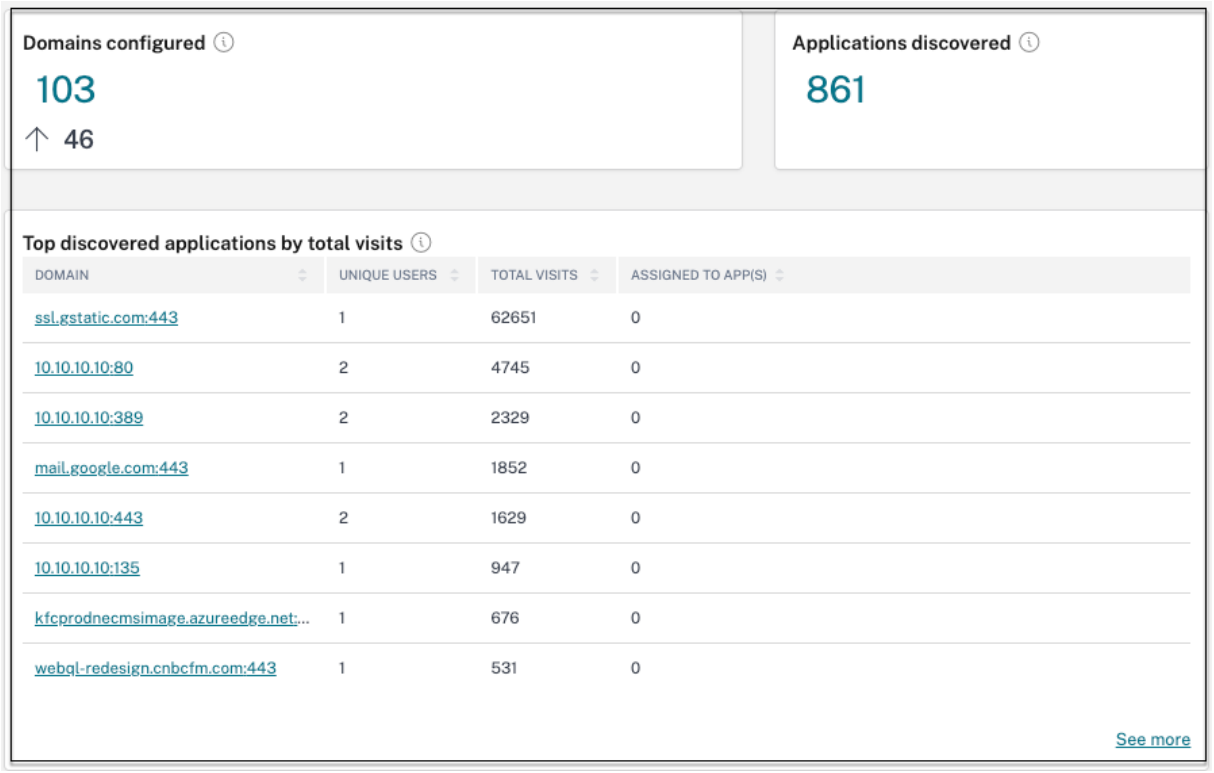


Principales políticas de acceso por aplicación

Utilice el gráfico **Principales políticas de acceso por aplicación** para ver la lista de políticas de acceso que se aplican en las aplicaciones. Haga clic en el enlace **Ver más** para ver la lista de políticas asociadas con las aplicaciones y la cantidad de veces que se aplican las políticas. También puede utilizar la opción **Buscar** en la página Políticas de acceso para filtrar las políticas según el nombre de la política. También puede buscar políticas específicas utilizando los operadores de búsqueda para refinar aún más su búsqueda. Para obtener más detalles, consulte Operadores de búsqueda.

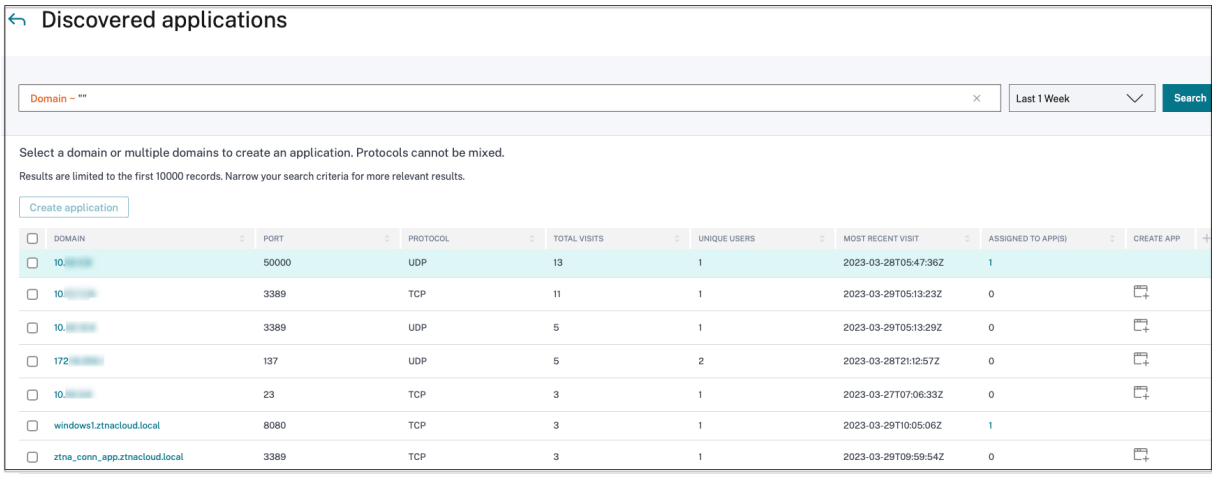
Principales aplicaciones descubiertas

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



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

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



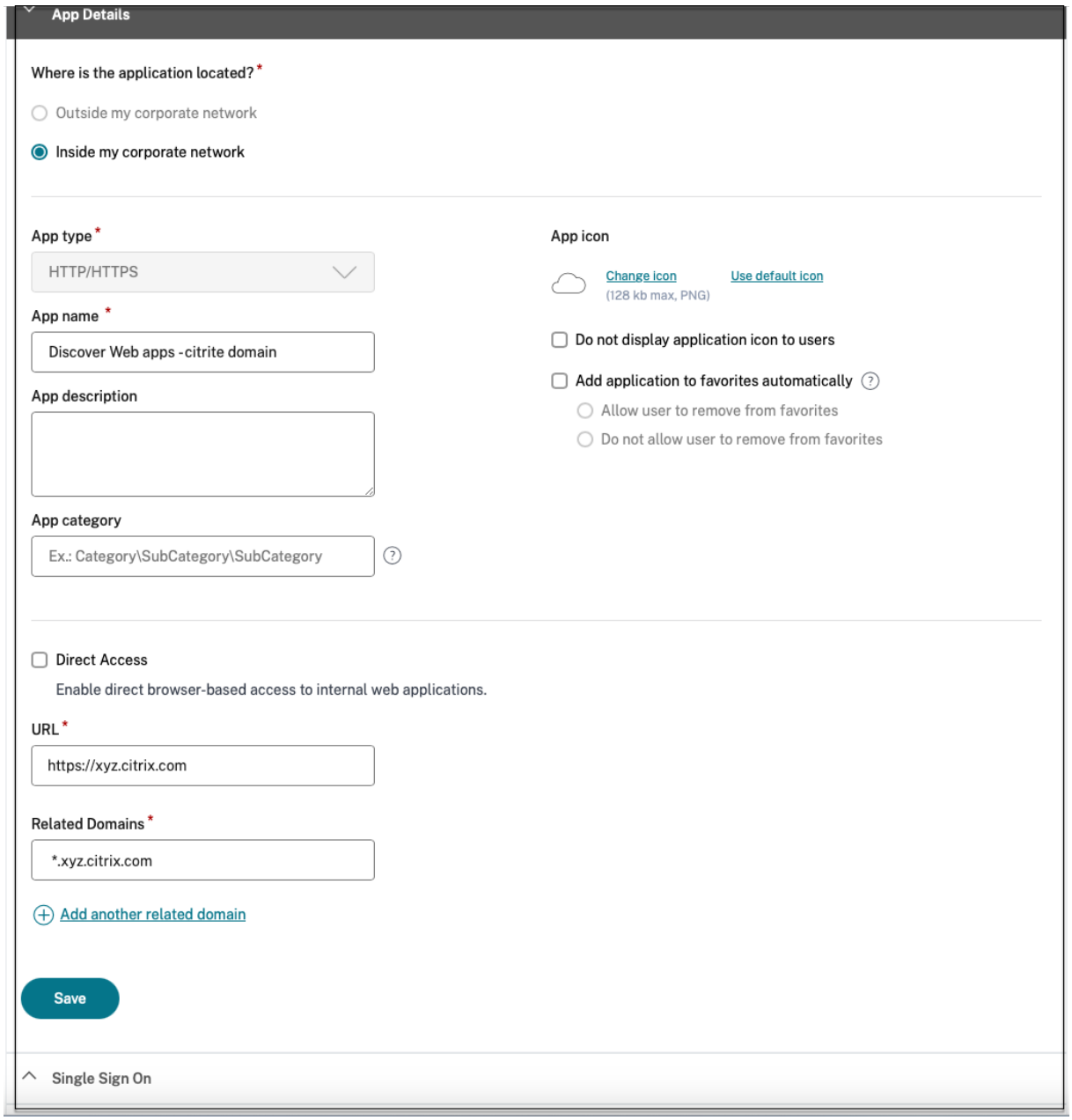
La página **Aplicaciones descubiertas** muestra los detalles de los dominios, como el nombre de dominio, el puerto, el protocolo, las visitas totales, los usuarios únicos y la fecha de visita más reciente. Todas las columnas del gráfico se pueden ordenar. Puede utilizar la barra de búsqueda para buscar según el dominio.

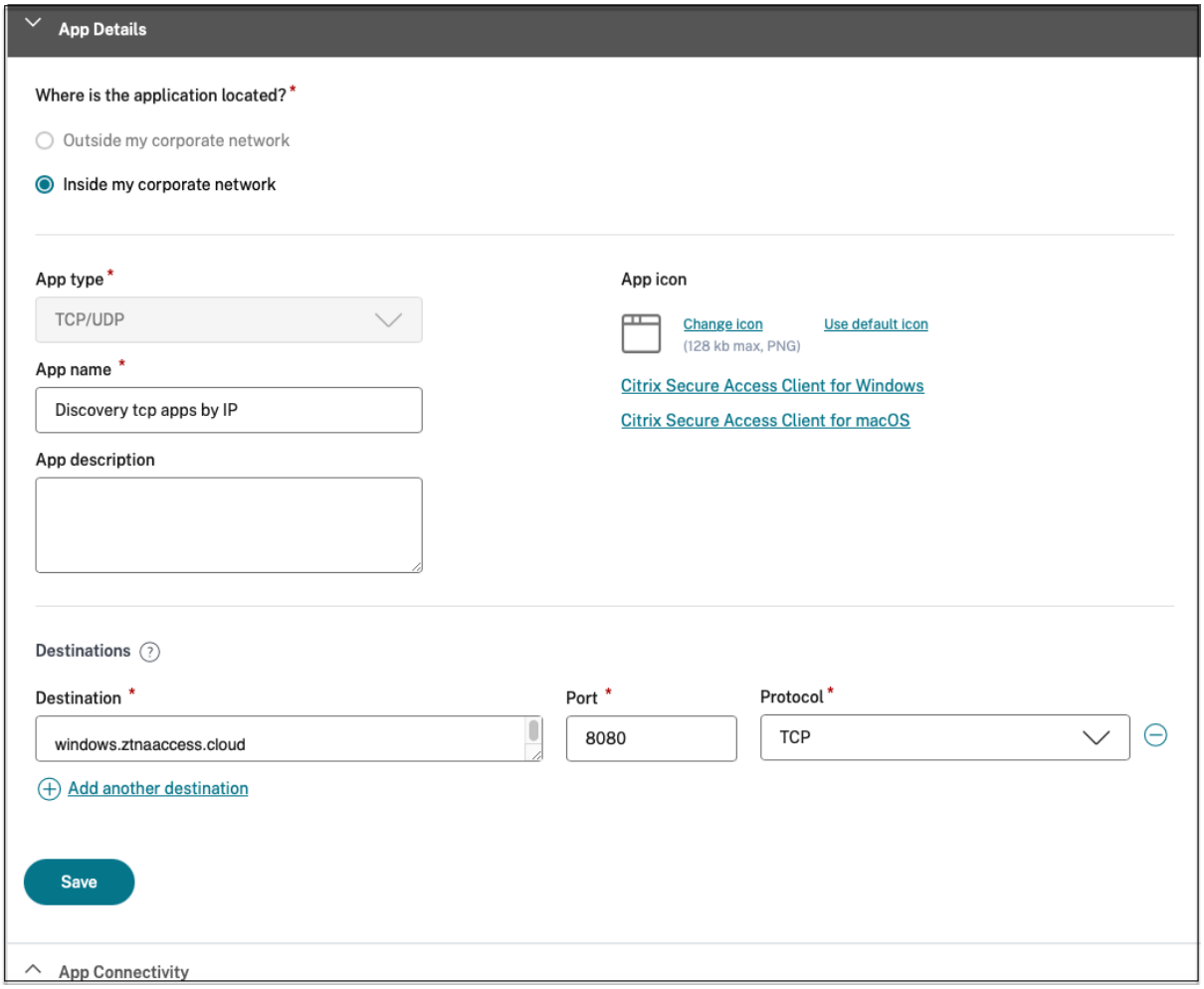
> **Nota**
>
> - Los protocolos se derivan de los puertos estándar utilizados por los clientes.
> - La lista de dominios descubiertos está limitada a 10000 registros.

Creación de una aplicación a partir del gráfico

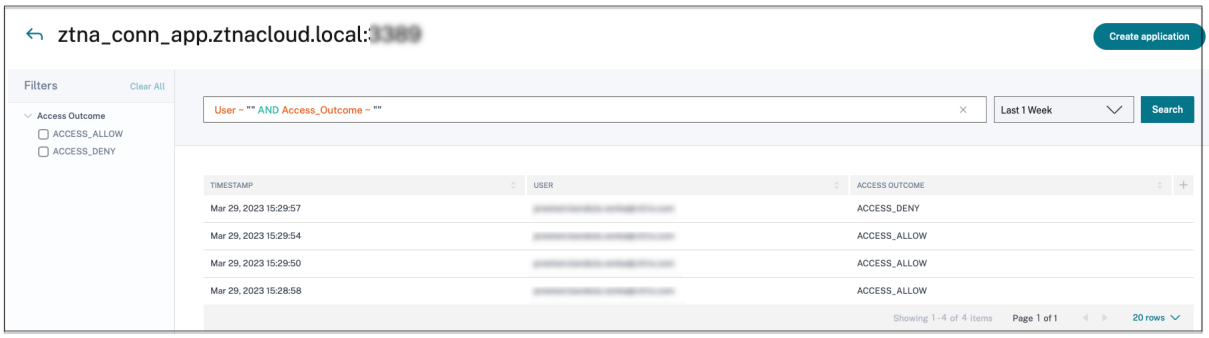
Haga clic en el ícono **+** en línea con el dominio correspondiente para crear una aplicación. Aparece el asistente de configuración de la aplicación. El ícono de creación de aplicaciones no aparece en las filas en las que ya se creó una aplicación con la misma combinación de dominio, puerto y protocolo,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

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





También puede hacer clic en el enlace de dominio único para ver más detalles y crear una solicitud para ese dominio. Al hacer clic en un enlace de dominio, se muestran los registros de autenticación de usuario para ese 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 su búsqueda:

- **= (es igual a algún valor)**: Para buscar los registros/políticas que coincidan exactamente con los criterios de búsqueda.
- **!= (no es igual a algún valor)**: Para buscar registros/políticas que no contengan los criterios especificados.
- **~ (contiene algún valor)**: Para buscar los registros/políticas que coincidan parcialmente con los criterios de búsqueda.
- **!~ (no contiene algún valor)**: Para buscar registros/políticas que no contengan algunos de los criterios especificados.

Registro y resolución de problemas

October 21, 2024

Utilice este tema para solucionar algunos problemas relacionados con la configuración de la aplicación, la autenticación y el inicio de sesión único (SSO) o el acceso a la aplicación. Copie el código de información de la columna 'Código de información' dentro de los registros de diagnóstico de Secure Private Access y luego busque ese código en esta página para encontrar los pasos de solución de problemas correspondientes. A continuación se presentan algunas preguntas frecuentes que le ayudarán a utilizar mejor este tema.

Preguntas frecuentes?

¿Qué son los registros de diagnóstico de acceso privado seguro?

¿Dónde puedo encontrar los registros de acceso privado seguro?

¿Qué widget muestra los registros de diagnóstico de acceso privado seguro?

¿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 filtro los registros de diagnóstico?

¿Cómo uso el tema de solución de problemas de acceso privado seguro para resolver una falla que he encontrado?

¿Qué es un código de información? ¿Donde los encuentro?

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

¿Cuáles son todas las ubicaciones de PoP de acceso privado seguro?

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

Tabla de consulta de códigos de información

La siguiente tabla de búsqueda de errores proporciona una descripción general completa de los diversos errores que los usuarios pueden encontrar al utilizar el servicio de acceso privado seguro.

Código de información	Descripción	La resolución
0x180006, 0x1800B7	El inicio de la aplicación falló porque se excedió la longitud del FQDN de la aplicación	El inicio de la aplicación falló porque se excedió la longitud del FQDN de la aplicación
0x180022	El inicio de la aplicación falló porque el servicio de autenticación no funciona	El inicio de la aplicación falló porque el servicio de autenticación no funciona
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 inicio de sesión único SAML, FQDN de aplicación no válido	Se deniega el acceso a la aplicación
0x1800EF	Problema al conectarse al dispositivo Connector	Problema al conectarse al dispositivo Connector
0x18009D	Búsqueda de DNS/Conexión fallida	Servicio de navegación segura: errores de conexión/búsqueda de DNS
0x1800A0, 0x1800A2, 0x1800A3, 0x1800A5 0x1800A6, 0x1800A7	El inicio de la aplicación web falló porque no se pudo conectar con la aplicación web de back-end	El inicio de la aplicación web falló porque no se pudo conectar a la aplicación web de back-end
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

Código de información	Descripción	La resolución
0x1800D0	El inicio de la sesión del agente de Citrix Secure Access falló al obtener la configuración de la aplicación	El inicio de la sesión del agente de Citrix Secure Access falló al obtener la configuración de la aplicación
0x1800CD, 0x1800CE, 0x1800D6, 0x1800EA	El inicio de la sesión del agente de Citrix Secure Access ha fallado al obtener la configuración de la aplicación, el inicio de la aplicación del agente de Citrix Secure Access ha fallado durante la evaluación de la política, el inicio de la aplicación del agente de Citrix Secure Access ha fallado	Solicitudes de cliente mal formadas
0x1800DE	El inicio de la aplicación del agente de Citrix Secure Access falló durante la evaluación de la política	El inicio de la aplicación del agente de Citrix Secure Access falló durante la evaluación de la política
0x180055, 0x1800DF, 0x1800E3	Aplicaciones restringidas por política contextual, acceso denegado debido a la configuración de la política	Una o más aplicaciones no figuran en el panel de usuario
0x1800EB	El inicio de la aplicación del agente de Citrix Secure Access ha fallado porque no se admite IPv6	El inicio de la aplicación del agente de Citrix Secure Access ha fallado porque no se admite IPv6
0x1800EC, 0x1800ED	La aplicación del agente de Citrix Secure Access no se inició debido a una dirección IP no válida	La aplicación del agente de Citrix Secure Access no se inició debido a una dirección IP no válida
0x10000001, 0x10000002, 0x10000003, 0x10000004	Error de inicio de sesión del cliente de Citrix Secure Access debido a un problema de red	Problema de accesibilidad de conectividad de red con el cliente Citrix Secure Access

Código de información	Descripción	La resolución
0x10000006	Error de inicio de sesión del cliente de 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 de Citrix Secure Access debido a una autoridad de certificación que no es de confianza	Se observa un problema de certificado de servidor no confiable
0x10000008	Error de inicio de sesión del cliente de Citrix Secure Access debido a un certificado no válido	Se observa un problema de certificado de servidor no válido
0x1000000A	Error de inicio de sesión del cliente de Citrix Secure Access debido a un problema de configuración	El inicio de sesión falló porque la configuración está vacía para el usuario
0x1000000B	Error de inicio de sesión del cliente de Citrix Secure Access debido a un error de conexión	Conexión finalizada por la red o el usuario final
0x10000010	Error de inicio de sesión del cliente de Citrix Secure Access debido a que la sesión expiró	La descarga de configuración falló porque la sesión expiró
0x10000013	Error de inicio de sesión del cliente de Citrix Secure Access debido a una lista de configuraciones enorme	El cliente de Citrix Secure Access no pudo iniciar sesión
0x11000003	Error de inicio de sesión del cliente de Citrix Secure Access debido a un error en la creación del canal de control	El establecimiento del canal de control falló porque la sesión expiró
0x11000004	Error de inicio de sesión del cliente de Citrix Secure Access debido a un error en la creación del canal de control	Falló el establecimiento del canal de control
0x11000005	Error de inicio de sesión del cliente de Citrix Secure Access debido a un error en la creación del canal de control	Falló el establecimiento del canal de control

Código de información	Descripción	La resolución
0x11000006	Error de inicio de sesión del cliente de Citrix Secure Access debido a un error en la creación del canal de control	El establecimiento del canal de control falló debido a un problema de red
0x12000001	Error al cerrar sesión en el cliente de Citrix Secure Access porque la sesión ya expiró	No se puede cerrar la sesión porque la sesión ha finalizado
0x12000002	Error al cerrar sesión en el cliente de Citrix Secure Access porque la sesión ya agotó el tiempo de espera	La sesión se ha terminado forzosamente
0x13000001	El acceso a la aplicación falló porque la sesión expiró	El inicio de la aplicación falló porque la sesión expiró
0x13000002	El acceso a la aplicación falló debido a una licencia inadecuada	El inicio de la aplicación falló debido a un problema de licencia
0x13000003, 0x13000008, 0x001800DF	El acceso a la aplicación falló porque está prohibido. Se niega el inicio de la aplicación TCP/UDP según la política	El inicio de la aplicación falló porque el servicio denegó el acceso
0x13000004, 0x13000005	El acceso a la aplicación falló porque el servidor no está disponible	El inicio de la aplicación falló porque el cliente no puede acceder al servicio
0x13000007	El acceso a la aplicación falló porque la política de acceso está deshabilitada o el usuario no está suscrito	El inicio de la aplicación falló debido a que la evaluación de políticas y la validación de configuración fallaron
0x13000009	El acceso a la aplicación falló porque falta la entrada de ruta	El inicio de la aplicación falló debido a problemas en la tabla de dominio de la aplicación
0x1300000B	El cliente cerró la conexión	El cliente cerró la conexión con el servicio Secure Private Access
0x1300000C	La resolución de FQDN sobre ZTNA falló	El servidor DNS no puede resolver el FQDN

Código de información	Descripción	La resolución
0x001800D3	Error en la descarga de la configuración de aplicaciones al iniciar sesión	No se pudo obtener la lista de destinos de aplicaciones configuradas
0x001800D9, 0x001800DA	El inicio de la aplicación TCP/UDP ha fallado durante el análisis de la respuesta de evaluación de la política. El inicio de la aplicación TCP/UDP ha fallado con un resultado no válido durante la evaluación de la política	Problema de configuración de la aplicación
0x001800DB	El inicio de la aplicación TCP/UDP ha fallado debido a una configuración de ubicación de recurso no válida	Problema con la ubicación de los recursos
0x13000006, 0x001800DC, 0x001800DD	El inicio de la aplicación TCP ha fallado debido a una política de seguridad mejorada no compatible configurada para la aplicación. El inicio de la aplicación TCP ha fallado debido a una redirección del servicio de navegador seguro no compatible configurada para la aplicación TCP.	La política de seguridad mejorada está vinculada a la aplicación HTTP
0x001800DE	El inicio de la aplicación TCP/UDP ha fallado porque no se encontró ninguna configuración de aplicación para el destino	No se puede localizar la aplicación
0x001800EA	El inicio de la aplicación TCP ha fallado 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 ha fallado debido a una IP de destino no válida	Dirección IP no válida

Código de información	Descripción	La resolución
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	El inicio de la aplicación UDP falló 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	El tráfico UDP no se pudo entregar
0x001800FF	Error en la entrega del tráfico de datos UDP	Error en la entrega del tráfico de datos UDP
0x10000401	Error en la marcación del servidor de encuentro de Citrix	El inicio de la aplicación falló debido a problemas de conectividad de red
0x10000402, 0x1000040C	No se puede registrar el dispositivo conector, falla en la inicialización de la conexión de red UDP	El dispositivo conector no pudo registrarse en el servicio de acceso privado seguro
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 al analizar el paquete de control,	Problema de conectividad con el dispositivo Connector
0x10000405, 0x10000408, 0x10000409, 0x1000040D 0x1000040E, 0x10000412	Back-end inaccesible, falla en la transmisión del paquete UDP, falla en la recepción de paquete UDP, error al escribir	Problemas de conectividad con el dispositivo Connector y los servidores TCP/UDP privados de back-end
0x10000406	La resolución de DNS falló en el back-end, el back-end cerró la conexión	El dispositivo conector no puede resolver el DNS para los FQDN
0x10000411	El servicio de puerta de enlace cerró la conexión	La conexión al servidor privado ha finalizado
0x10000413	Error al determinar el motivo de la interrupción de la conexión	No se pudo conectar ni enviar datos a la dirección IP o FQDN del servicio privado
0x100508	El contexto del usuario no coincide con las condiciones de la regla de acceso	No hay ninguna condición de política coincidente

Código de información	Descripción	La resolución
0x100509	Política de acceso no asociada a la aplicación	No hay ninguna política de acceso asociada a la aplicación
0x10050C	Resultados de la evaluación de políticas de múltiples aplicaciones a las que el usuario podría tener derecho	Información de enumeración de la aplicación
0x00180101	El inicio de la aplicación TCP/UDP falló porque falta una entrada de enrutamiento en la tabla de dominio de la aplicación	El inicio de la aplicación TCP/UDP falló porque falta una entrada de enrutamiento en la tabla de dominio de la aplicación
0x00180102	El inicio de la aplicación TCP/UDP falló porque los conectores no están en buen estado	El inicio de la aplicación TCP/UDP falló porque los conectores no están en buen estado
0x00180103	La solicitud UDP/DNS falló porque el conector no está disponible	La solicitud UDP/DNS falló porque el conector no está disponible
0x20580001	No se pudo cargar la página porque la cookie NGS ha expirado	No se pudo cargar la página porque la cookie NGS ha expirado
0x20580002	La obtención de la política de acceso falló debido a una falla de la red	La obtención de la política de acceso falló debido a una falla de la red
0x20580003	Error en la obtención de la política de acceso al analizar el token web JSON	Error en la obtención de la política de acceso al analizar el token web JSON
0x20580004	Error en la red al obtener los detalles de la política de acceso	Error en la red al obtener los detalles de la política de acceso
0x20580005	Error en la obtención de la política al obtener el certificado público	Error en la obtención de la política al obtener el certificado público

Código de información	Descripción	La resolución
0x20580007	Error en la obtención de la política al validar la firma de JWT	Error en la obtención de la política al validar la firma de JWT
0x20580008	La obtención de la política falló al validar el certificado público	La obtención de la política falló al validar el certificado público
0x2058000A	No se pudo determinar el entorno de la tienda para formar una URL de política	No se pudo determinar el entorno de la tienda para formar una URL de política
0x2058000B	No se pudo obtener respuesta de la solicitud de obtención de política de acceso	No se pudo obtener respuesta de la solicitud de obtención de política de acceso
0x2058000C	La obtención de la política de acceso falló debido a un token de autenticación DS secundario vencido	La obtención de la política de acceso falló debido a un token de autenticación DS secundario vencido
0x10200002	El dispositivo conector no está registrado	El dispositivo conector no está registrado
0x10200003	No se puede conectar al dispositivo conector	No se puede conectar al dispositivo conector
0x10000301	La conexión al servicio SPA de Citrix falló	La conexión al servicio Citrix Secure Private Access falló
0x10000303, 0x10000304	El servidor proxy no es accesible	El servidor proxy no es accesible
0x10000305	Error en la autenticación del servidor proxy	Error en la autenticación del servidor proxy
0x10000306	Los servidores proxy configurados no son accesibles	Los servidores proxy configurados no son accesibles
0x10000307	Se recibió una respuesta de error del servidor backend	Se recibió una respuesta de error del servidor backend
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

Código de información	Descripción	La resolución
0x10000108, 0x1000010B	No se pudo procesar el SSO, no se pueden determinar las configuraciones del SSO	No se pudo procesar el SSO, no se pueden determinar las configuraciones del SSO
0x10000101, 0x10000102, 0x10000103, 0x10000104	Error de inicio de sesión único (SSO) de FormFill: configuración incorrecta de la aplicación de formulario	Error de inicio de sesión único (SSO) de FormFill: configuración incorrecta de la aplicación de formulario
0x1000010A	Error de inicio de sesión único (SSO) de FormFill: configuración incorrecta de la aplicación de formulario	Error de inicio de sesión único (SSO) de FormFill: configuración incorrecta de la aplicación de formulario
0x10000202	Error en el inicio de sesión único de Kerberos	Error en el inicio de sesión único de Kerberos
0x10000203	No se pudo procesar el SSO para el tipo de autenticación	No se pudo procesar el SSO para el tipo de autenticación
0x10000204	El SSO de Kerberos falló y se vuelve a utilizar NTLM	El SSO de Kerberos falló y se vuelve a utilizar NTLM
0x14000001	Varias cuentas autorizadas a ZTNA configuradas en la aplicación Citrix Workspace	Varias cuentas autorizadas de ZTNA configuradas en la aplicación Citrix Workspace

Pasos de resolución

Las siguientes secciones proporcionan pasos de resolución para la mayoría de los códigos de información. Para los códigos que no tienen capturados los pasos de resolución, comuníquese con el soporte de Citrix.

Una o más aplicaciones no figuran en el panel de usuario

Código de información: 0x180055, 0x1800DF, 0x1800E3

Debido a la configuración de la política contextual, es posible que algunas aplicaciones no sean vistas por algunos usuarios o dispositivos. Parámetros como factores de confianza (postura del dispositivo o puntuación de riesgo) pueden afectar la accesibilidad de las aplicaciones.

1. Copie el ID de transacción de la columna `motivos` para el código de error `0x18005C` en el archivo csv de Registros de diagnóstico.
2. Modifique el filtro de columna `prod` en el archivo csv para mostrar eventos del componente llamado `SWA.PSE` o `SWA.PSE.EVENTS`. Este filtro muestra únicamente los registros relacionados con la evaluación de políticas.
3. Busque la carga útil de la política evaluada en la columna `motivo` . Esta carga útil muestra la política evaluada para el contexto del usuario para todas las aplicaciones a las que el usuario está suscrito.
4. Si la evaluación de la política indica que la aplicación fue denegada para el usuario, las posibles razones pueden ser:

    - Condiciones de coincidencia incorrectas en la política: verifique la configuración de la política de la aplicación en Citrix Cloud
    - Reglas de coincidencia incorrectas en la política: verifique la configuración de la política de la aplicación en Citrix Cloud
    - Regla predeterminada de coincidencia incorrecta en la política: este es un caso de solución provisional. 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 cual no tiene una suscripción.

Asegúrese de que el usuario tenga una suscripción a las aplicaciones.

1. Vaya a la aplicación en el portal de gestión.
2. Edite la aplicación y vaya a la pestaña **Suscripción** .
3. Asegúrese de que el usuario objetivo tenga una entrada en la lista de suscripciones.

Rendimiento lento de la aplicación back-end

Código de información:0x18000F

Hay casos en los que la red del cliente es inestable debido a que los conectores en una ubicación de recursos pueden estar inactivos o el servidor back-end en sí puede no responder.

1. Asegúrese de que el dispositivo conector esté ubicado geográficamente cerca del servidor back-end para descartar latencias de red.
2. Compruebe si el firewall del servidor back-end no está bloqueando el dispositivo conector.

3. Verifique 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 en la respuesta indica el servidor geoespecífico como `aws-us-wgnssvc.net`.

El inicio de la aplicación falló porque se excedió la longitud del FQDN de la aplicación

Código de información: 0x180006, 0x1800B7

Los FQDN de la aplicación no deben superar los 512 caracteres de longitud. Verifique el FQDN de la aplicación en la página de configuración de la aplicación. Asegúrese de que la longitud no exceda los 512 bytes.

1. Vaya a la pestaña **Aplicaciones** en la consola de administración.
2. Busque la aplicación cuyo FQDN supere los 512 caracteres.
3. Edite la aplicación y corrija la longitud del FQDN de la aplicación.

Se ha excedido la longitud de los detalles de la aplicación

Código de información: 0x18000E

Verifique las políticas si están bloqueando el acceso a la aplicación.

1. Vaya a **Políticas de acceso**.
2. Busque las políticas sobre las cuales la aplicación tiene derechos.
3. Revise las reglas y condiciones de la política para el usuario final.

Se deniega 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, donde las políticas niegan la aplicación a un usuario determinado.

Revisa las políticas si están bloqueando el acceso a la aplicación

1. Vaya a **Políticas de acceso**.
2. Busque las políticas sobre las cuales la aplicación tiene derechos.
3. Revise las reglas y condiciones de la política para el usuario final.

Aplicaciones no enumeradas

Es posible que falten aplicaciones en la lista enumerada debido a denegaciones de políticas o si la integración de acceso privado seguro no está habilitada.

- Si se debe habilitar el acceso para algunas de las aplicaciones pero no ve ninguna aplicación, intente habilitar la integración de Acceso privado seguro.
  - Inicie sesión en Citrix Cloud.
  - Seleccione **Configuración del espacio de trabajo** en el menú de hamburguesa y, luego, haga clic en **Integraciones de servicios**.
  - Haga clic en el botón de puntos suspensivos en Acceso privado seguro y luego haga clic en **Habilitar**.
- Si la integración de Acceso Privado Seguro ya está habilitada, deshabilítela y luego habilítela nuevamente para ver si tiene alguna aplicación.

Problema al conectarse al dispositivo Connector

Código de información: 0x1800EF

El enrutamiento de la aplicación falla debido a la falta de disponibilidad de conexiones TCP con conectores locales.

Revisar eventos desde el componente controlador

1. Busque el ID de transacción “ para el código de error `0x1800EF` en el archivo csv de registros de diagnóstico.
2. Filtrar todos los eventos que coincidan con el ID de transacción en el archivo csv.
3. Además, filtre la columna `prod` en el archivo csv que coincida con `SWA.GOCTRL`.

   Si ve eventos con el mensaje `connectType multiconnect::success`? entonces;

   - Esto indica que la solicitud de establecimiento del túnel se transmitió correctamente al controlador.
   - Verifique si la ubicación del recurso “ en el mensaje de registro es correcta. Si es incorrecto, corrija la ubicación del recurso en la sección de configuración de la aplicación en el portal de administración de Citrix.
   - Verifique si la IP de VDA `y el puerto` en el mensaje de registro son correctos. La IP y el puerto de VDA indican la IP y el puerto de la aplicación back-end. Si es incorrecto, corrija el FQDN o la dirección IP de la aplicación en la sección de configuración de la aplicación en el portal de administración de Citrix.

- Continúe revisando los eventos del conector si no encuentra ninguno de los problemas mencionados anteriormente.

Si ve eventos con el mensaje `connectType connect::failure` o `multiconnect::success`, entonces;

- Verifique si la solución recomendada para este mensaje de registro indica: `Verifique si el conector todavía estáconectado al mismo pop`. Esto indica que es posible que el conector en la ubicación del recurso se haya caído. Proceda a revisar los eventos del conector .
- Comuníquese con el servicio de atención al cliente de Citrix si no ve los mensajes mencionados anteriormente.

Si ve eventos con el mensaje `connectType IntraAll::failure`, comuníquese con el servicio de atención al cliente de Citrix.

Revisar eventos del componente conector

1. Busque el ID de transacción “ para el código de error `0x1800EF` en el archivo csv de registros de diagnóstico.
2. Filtrar todos los eventos que coincidan con el ID de transacción en el archivo csv.
3. También filtre la columna `prod` en el archivo csv que coincida con `SWA.ConnectorAppliance.WebApps`.
4. Si ve eventos con estado `como error`, entonces;

   - Revise el mensaje de motivo “ para cada uno de estos eventos de falla.
   - `UnableToRegister` indica que el conector no pudo registrarse en Citrix Cloud correctamente. Contactar con Citrix Support.
   - `IsProxyRequiredCheckError` o `ProxyDialFailed` o `ProxyConnectionFailed` o `ProxyAuthenticationFailure` o `ProxiesUnReachable` indica que el conector no pudo resolver la URL del back-end a través de la configuración del proxy. Verifique que la configuración del proxy sea correcta.
   - Para obtener más información sobre la depuración, consulte Eventos SSO del conector.

Errores de inicio de sesión único

Para el inicio de sesión único, se extraen diferentes atributos SSO de la configuración de la aplicación y se aplican durante el inicio de la aplicación. Si ese usuario en particular no tiene los atributos o si los atributos son incorrectos, el inicio de sesión único podría fallar. Asegúrese de que la configuración parezca correcta.

1. Vaya a **Políticas de acceso.**

2. Busque las políticas sobre las cuales la aplicación tiene derechos.
3. Revise las reglas y condiciones de la política para el usuario final.

Los métodos SSO, como Form SSO, Kerberos y NTLM, los realiza el conector local. Revise los siguientes registros de diagnóstico del conector.

Revisar eventos SSO desde el componente conector

1. Filtra el nombre del componente " en el archivo csv que coincida con `SWA.ConnectorAppliance.WebApps`.
2. ¿Ves eventos con estatus de "fracaso"?

    - Revise el mensaje de cada uno de estos eventos de falla.
    - `IsProxyRequiredCheckError` o `ProxyDialFailed` o `ProxyConnectionFailed` o `ProxyAuthenticationFailure` o `ProxiesUnReachable` indica que el conector no pudo resolver la URL del back-end a través de la configuración del proxy. Verifique que la configuración del proxy sea correcta.
    - `FailedToReadRequest` o `RequestReceivedForNonSecureBrowse` o `UnableToRetrieveUserCredentials` o `CCSPolicyIsNotLoaded` o `FailedToLoadBaseC` o `ProcessConnectionFailure` o `WebAppUnSupportedAuthType` indica un error de tunelización. Contactar con Citrix Support.
    - `UnableToConnectTargetServer` indica que el servidor back-end no es accesible desde el conector. Verifique nuevamente la configuración del back-end.
    - `IncorrectFormAppConfiguration` o `NoLoginFormFound` o `FailedToConstructForLog` o `FailedToLoginViaFormBasedAuth` indica un error de autenticación basada en formulario. Consulte la sección de configuración de SSO del formulario en Configuración de la aplicación en el portal de administración de Citrix.
    - `NTLMAuthNotFound` indica un error de autenticación basado en NTLM. Consulte la sección de configuración de SSO NTLM en la configuración de la aplicación en el portal de administración de Citrix.
    - Para una mayor depuración, consulte Eventos del conector.

El inicio de la aplicación falló porque el servicio de autenticación no funciona

Código de información: 0x180022

El acceso privado seguro permite a los administradores configurar un servicio de autenticación de terceros, como el directorio activo tradicional, AAD, Okta o SAML. Las interrupciones en estos servicios de autenticación pueden causar este problema.

Verifique si los servidores de terceros están activos y son accesibles.

Error de inicio de sesión único (SSO) de SAML

Código de información: 0x18008A, 0x1800A9, 0x1800AA, 0x1800AB, 0x1800AC, 0x1800AD, 0x1800AE, 0x1800AF, 0x1800B0, 0x1800B1, 0x1800B2, 0x1800B3

Los usuarios enfrentan una falla de autenticación durante el inicio de la aplicación cuando la inicia un IdP o pueden ver enlaces inaccesibles cuando la inicia un SP. Verifique la configuración de la aplicación SAML en el lado del servicio de acceso privado seguro y también la configuración del proveedor de servicios.

Configuración de acceso privado seguro:

1. Vaya a la pestaña **Aplicaciones** .
2. Busque la aplicación SAML problemática.
3. Edite la aplicación y vaya a la pestaña **Inicio de sesión único** .
4. Compruebe los siguientes campos.
    - URL de afirmación
    - Estado del relé
    - Audiencia
    - Formato de identificación de nombre, identificación de nombre y otros atributos

Configuración del proveedor de servicios:

1. Inicie sesión en el proveedor de servicios.
2. Vaya a la configuración de SAML **.**
3. Verifique el certificado IdP, la audiencia y la URL de inicio de sesión del IdP.

Si la configuración parece correcta, comuníquese 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 back-end.

En este caso, el usuario final ve un error en la página web. Verifique 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 pestaña **Aplicaciones** .

2. Edite la aplicación problemática.
3. Vaya a la página **Detalles de la aplicación** .
4. Compruebe la URL. La URL debe ser accesible en intranet o Internet.

Servicio de navegación segura: error en la búsqueda/conexión de DNS

Código de información: 0x18009D

Experiencia de navegación interrumpida a través del servicio de aislamiento remoto del navegador. Verifique el servidor back-end al que el usuario final está intentando conectarse.

1. Vaya al servidor back-end y verifique si está en funcionamiento y puede recibir las solicitudes.
2. Verifique la configuración del proxy para ver si está deteniendo la conexión al servidor back-end.

> **Nota**
>
> El servicio de aislamiento de navegador remoto de Citrix se conocía anteriormente como servicio de navegador seguro.

CWA Web: errores de conexión/búsqueda de DNS para aplicaciones web

Código de información: 0x1800A0, 0x1800A2, 0x1800A3, 0x1800A5, 0x1800A6, 0x1800A7

Experiencia de navegación interrumpida en aplicaciones web que se ejecutan dentro de una red corporativa.

1. Filtra los registros de diagnóstico para los FQDN que no se pueden resolver.
2. Verifique la accesibilidad del servidor back-end desde dentro de la red corporativa.
3. Verifique la configuración del proxy para ver si el conector no puede llegar al servidor back-end.

Acceso directo: mal configurado como aplicación web

Dado que el tráfico de aplicaciones web siempre se enruta a través del conector, configurar el acceso directo a ellas genera un error de acceso a la aplicación.

Verifique la configuración conflictiva entre la tabla de dominio de enrutamiento y la configuración de la aplicación.

1. Vaya a la aplicación en el portal de gestión.
2. Edite la aplicación y verifique si el acceso directo está habilitado.
3. Verifique el FQDN de la aplicación dentro de la tabla de dominio de enrutamiento si se ha 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 deshabilita el acceso directo al tráfico que se origina en clientes basados en navegador.

Asegúrese de que el usuario tenga una suscripción a las aplicaciones.

1. Vaya a la aplicación en el portal de gestión.
2. Edite la aplicación y verifique la configuración de acceso sin agente.

Políticas de seguridad mejoradas: configuración incorrecta del servicio de navegación segura

Código de información: 0x1800C3

Se observó un comportamiento incorrecto al previsto por las reglas de la política. Verifique las políticas de acceso contextual.

1. Vaya a la pestaña **Políticas** .
2. Consulte las políticas asociadas a la aplicación.
3. Consulte las reglas para esas políticas.

Políticas de seguridad mejoradas: configuración incorrecta de políticas

Se observó un comportamiento incorrecto al previsto por las reglas de la política. Verifique la configuración de seguridad mejorada.

1. Vaya a la aplicación.
2. Haga clic en la pestaña **Políticas de acceso** .
3. Verifique la configuración en la sección **Restricciones de seguridad disponibles:** .

El inicio de la sesión del agente de Citrix Secure Access falló al obtener la configuración de la aplicación

Código de información: 0x1800D0

La aplicación Citrix Secure Access no logra establecer con éxito un túnel completo a Citrix Cloud.

1. Revise la configuración del dominio de enrutamiento 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 cliente mal formadas

Código de información: 0x1800CD, 0x1800CE, 0x1800D6, 0x1800EA

O bien el túnel VPN no está establecido o es posible que ciertos FQDN no estén tunelizados.

1. Asegúrese de que las solicitudes no sean fabricadas ni reconstruidas por servidores proxy en el medio.
2. Sospechosos de ataques tipo "man-in-middle".

Aplicaciones TCP/UDP: configuración incorrecta de la redirección del servicio de navegación segura

Código de información: 0x1800DD

Las redirecciones del servicio de aislamiento del navegador remoto solo se pueden aplicar a aplicaciones web y no a aplicaciones TCP/UDP. Revise la configuración de la aplicación en la GUI del servicio de acceso privado seguro.

> **Nota**
>
> El servicio de aislamiento de navegador remoto de Citrix se conocía anteriormente como servicio de navegador seguro.

El inicio de la aplicación del agente de Citrix Secure Access falló durante la evaluación de la política

Código de información: 0x1800DE

Asegúrese de que todos los FQDN internos que el cliente Citrix Secure Access debe tunelizar tengan una entrada correspondiente en la tabla de dominio de enrutamiento.

El inicio de la aplicación del agente de Citrix Secure Access ha fallado porque no se admite IPv6

Código de información: 0x1800EB

Revise las entradas del dominio de enrutamiento. Asegúrese de que no haya entradas IPV6 en la tabla.

El inicio de la aplicación del agente de Citrix Secure Access falló debido a una dirección IP no válida

Código de información:0x1800EC, 0x1800ED

Revise las entradas del dominio de enrutamiento. Asegúrese de que las direcciones IP sean válidas y apunten al back-end correcto.

Problema de accesibilidad de conectividad de red con el cliente Citrix Secure Access

Código de información: 0x10000001, 0x10000002, 0x10000003, 0x10000004

1. Compruebe si la red de la máquina cliente es accesible. Si la red es accesible, comuníquese 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 registros de depuración del cliente, consulte Cómo recopilar registros del cliente.

El servidor proxy interfiere en la conectividad del cliente con el servicio

Código de información: 0x10000006

1. Compruebe si la red de la máquina cliente es accesible.
2. Verifique si el proxy está configurado correctamente en el cliente.
3. Si no hay problemas con ambos, comuníquese con el soporte de Citrix con los registros de depuración del cliente.

Para recopilar registros de depuración del cliente, consulte Cómo recopilar registros del cliente.

Se observa un problema de certificado de servidor no confiable

Código de información: 0x10000007

Comuníquese con el soporte de Citrix para verificar si el certificado del servidor fue generado correctamente por una CA válida.

Se observa un problema de certificado de servidor no válido

Código de información: 0x10000008

Comuníquese con el soporte de Citrix para verificar si el certificado del servidor está autofirmado, vencido o proviene de una fuente no confiable.

El inicio de sesión falló porque la configuración está vacía para el usuario

Código de información: 0x1000000A

1. Asegúrese de que al menos una aplicación TCP/UDP/HTTP esté configurada. Para obtener más detalles, consulte Agregar y administrar aplicaciones.
2. Asegúrese de que la tabla Dominio de aplicación (**Acceso privado seguro > Configuración > Dominio de aplicación**) no esté vacía o que todas las entradas no estén deshabilitadas. Los destinos configurados en la aplicación TCP/UDP/HTTP se agregan automáticamente a esta tabla.

Se recomienda no eliminar ni deshabilitar los destinos o URL de una aplicación TCP/UDP/HTTP activa.

Conexión finalizada por la red y/o el usuario final

Código de información: 0x1000000B

Verifique si la red está interrumpida o si el usuario final canceló la conexión durante la conexión de la sesión ZTNA.

La descarga de configuración falló porque la sesión expiró

Código de información: 0x10000010

Es posible que la sesión VPN haya expirado durante la solicitud de descarga de configuración de la sesión ZTNA. Intente volver a iniciar sesión en el cliente Citrix Secure Access.

El cliente de 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 excede el límite máximo de configuración.

1. Revise la configuración del dominio de enrutamiento para las aplicaciones TCP/UDP en **Acceso privado seguro > Configuración > Dominio de aplicación**
2. Asegúrese de que el número de entradas no sea enorme. Si la lista de entradas es enorme, deshabilite o elimine los destinos no utilizados.

   Si se espera que la lista de destinos tenga más de 1000 segundos, intente aumentar el tamaño máximo de descarga de configuración actualizando la clave de registro ConfigSize. Para obtener más detalles, consulte Claves de registro del cliente VPN de Citrix Gateway.

El establecimiento del canal de control falló porque la sesión expiró

Código de información: 0x11000003

El canal de control para el establecimiento de la solicitud DNS ha fallado porque la sesión ha expirado.

Es posible que la sesión ZTNA haya expirado durante la configuración del canal de control.

Intente volver a iniciar sesión en el cliente Citrix Secure Access.

Falló el establecimiento del canal de control

Código de información: 0x11000004

El canal de control para el establecimiento de la solicitud DNS ha fallado.

- **Mantenga la ubicación del recurso en buen estado:**

1. Inicie sesión en Citrix Cloud.
2. Haga clic en **Ubicación del recurso** en el menú de hamburguesas.
3. Ejecute una verificación de estado de los dispositivos conectores en la ubicación del recurso respectivo.
4. Si esto no soluciona el problema, intente reiniciar la máquina virtual del conector.

- **Mantener el dispositivo conector HA:**

1. Inicie sesión en Citrix Cloud.
2. Haga clic en **Ubicación del recurso** en el menú de hamburguesas.
3. Asegúrese de que la ubicación del recurso esperada tenga al menos dos dispositivos conectores.

Asegúrese de lo siguiente:

- La ubicación del recurso LAN está en condiciones de funcionamiento.
- No hay ningún firewall o proxy en el medio que bloquee el acceso del Connector Appliance al servicio o a los servidores back-end.
- La red del cliente está saludable.
- Los servidores privados back-end 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 para este error.
2. Filtra todos los eventos que coincidan con el ID de transacción en el panel de acceso privado seguro.

3. Verifique si se produjo algún error en los registros de diagnóstico del cliente o del dispositivo o servicio del conector, que coincida con el ID de la transacción. Luego tome las medidas apropiadas según corresponda.
4. Verifique si la ubicación del recurso está elegida correctamente para el destino en la tabla de dominio de la aplicación (**Acceso privado seguro > Configuración > Dominio de la aplicación**).
5. Verifique si la aplicación está configurada con el puerto, rangos de IP y dominios correctos. Para obtener más detalles, consulte Agregar y administrar aplicaciones.

Si aún no puede resolver el problema, comuníquese con el soporte técnico de Citrix con el código de error correspondiente al ID de transacción y los registros del cliente.

Para recopilar registros de depuración del cliente, consulte Cómo recopilar registros del cliente.

Falló el establecimiento del canal de control

Código de información: 0x11000005

Error en el establecimiento del canal de control (para solicitud DNS).

1. Verifique la titularidad de la licencia del servicio de acceso privado seguro.
2. Si no tiene derecho, comuníquese con el soporte técnico de Citrix para verificar la licencia.

Para obtener información detallada, consulte https://www.citrix.com/buy/licensing/product.html.

El establecimiento del canal de control falló debido a un problema de red

Código de información: 0x11000006

El establecimiento del canal de control (para solicitud de DNS) falló debido a un problema de red.

1. Compruebe si el servicio de acceso privado seguro está disponible.
2. Si no puede comunicarse, comuníquese con el soporte técnico de Citrix con el código de error y los registros del cliente.

Para recopilar registros de depuración del cliente, consulte Cómo recopilar registros del cliente.

El establecimiento del canal de control falló debido a IIP insuficientes

Código de información: 0x11000007

El establecimiento del canal de control (para solicitud DNS) falló debido a IIP insuficientes.

Comuníquese con el soporte técnico de Citrix con el código de error y los registros del cliente.

Para recopilar registros de depuración del cliente, consulte Cómo recopilar registros del cliente.

No se puede cerrar la sesión porque la sesión ha finalizado

Este problema podría haber ocurrido porque la máquina cliente (teclado o mouse) estuvo inactiva durante más tiempo que el período de espera 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 finaliza 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.

El inicio de la aplicación falló porque la sesión expiró

Código de información: 0x13000001

1. La sesión de ZTNA ha expirado durante el inicio de la aplicación.
2. Intente volver a iniciar sesión en el cliente Citrix Secure Access.

El inicio de la aplicación falló debido a un problema de licencia

Código de información: 0x13000002

1. Verifique que la licencia del servicio de Acceso Privado Seguro sea válida.
2. Si no tiene derecho, comuníquese con el soporte técnico de Citrix para verificar la licencia.

Para obtener información detallada, consulte https://www.citrix.com/buy/licensing/product.html.

El inicio de la aplicación falló porque el servicio denegó el acceso

Código de información: 0x13000003, 0x13000008, 0x001800DF

Se deniega el inicio de la aplicación según la configuración de políticas para el usuario y la aplicación.

Asegúrese de lo siguiente.

- No se utilizan los mismos destinos en múltiples aplicaciones (HTTP, HTTPS, TCP, UDP)
- No hay destinos superpuestos en múltiples aplicaciones.

- Las políticas de acceso están ligadas a las aplicaciones.

Verifique también las condiciones y acciones de las políticas configuradas para la aplicación denegada. Luego revise las condiciones y acciones de la política.

Para obtener más detalles, consulte Políticas de acceso.

El inicio de la aplicación falló porque el cliente no puede acceder al servicio

Código de información: 0x13000004, 0x13000005

1. Compruebe si el servicio de acceso privado seguro está accesible.
2. Inicie la aplicación nuevamente.
3. Si la aplicación no está disponible durante mucho tiempo, comuníquese con el soporte técnico de Citrix con el código de error y los registros del cliente.

Para recopilar registros de depuración del cliente, consulte Cómo recopilar registros del cliente.

El inicio de la aplicación falló debido a que la evaluación de políticas y la validación de configuración fallaron

Código de información: 0x13000007

El inicio de la aplicación falló debido a que el servicio de acceso privado seguro falló en la evaluación de políticas y la validación de configuración.

No se puede detectar la aplicación para el destino accedido.

El inicio de la aplicación falló porque el servicio denegó el acceso.

El inicio de la aplicación falló debido a problemas en la tabla de dominio de la aplicación

Código de información: 0x13000009

El inicio de la aplicación falló porque la tabla de dominio de la aplicación no tiene una entrada para el destino al que se accedió.

Verifique que la entrada de ruta esté configurada correctamente para la aplicación en **Acceso privado seguro > Configuración > Dominio de aplicación**.

El cliente cerró la conexión con el servicio Secure Private Access

Código de información: 0x1300000B

1. Verifique si el usuario final cerró manualmente la conexión.
2. De lo contrario, comuníquese con el soporte técnico de Citrix con el código de error y los registros del cliente.

Para recopilar registros de depuración del cliente, consulte Cómo recopilar registros del cliente.

El servidor DNS no puede resolver el FQDN

Código de información: 0x1300000C

Este problema ocurre cuando el dispositivo conector no puede resolver el DNS para los FQDN.

1. Verifique la entrada DNS para el FQDN de la aplicación respectiva en el servidor DNS.
2. Asegúrese de que haya un servidor DNS apropiado configurado en los dispositivos conectores. Para obtener más detalles, consulte Configuración de ajustes de red en la página de administración del dispositivo Connector.

No se puede localizar la aplicación

Código de información: 0x001800DE

Es posible que no pueda encontrar la aplicación para el destino al que accedió el usuario. Esto puede ocurrir si la asignación de la ubicación del destino al recurso falta en la tabla de dominio de 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 accede.

1. Vaya a la aplicación en el portal de gestión.
2. Edite la aplicación y vaya a la pestaña **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 aplicación ** tenga el destino y la ubicación del recurso adecuados.

No se pudo obtener la lista de destinos de aplicaciones configuradas

Código de información: 0x001800D3

- Asegúrese de que al menos una aplicación TCP/UDP/HTTP esté configurada. Para obtener más detalles, consulte Agregar y administrar aplicaciones.

- Asegúrese de que la página de la tabla Dominio de aplicación (**Acceso privado seguro > Configuración > Dominio de aplicación**) no esté vacía o que no todas las entradas estén deshabilitadas. Los destinos configurados en la aplicación TCP/UDP/HTTP se agregan automáticamente a esta tabla. Se recomienda no eliminar ni deshabilitar los destinos o URL de las aplicaciones TCP/UDP/HTTP activas en la tabla de dominio de aplicación.

Problema de configuración de la aplicación

La configuración de la aplicación contiene un carácter especial o algún problema de configuración de política.

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 rango de direcciones IP o el CIDR de IP son válidos.
- El destino de la aplicación está habilitado en la tabla Dominio de la aplicación (**Acceso privado seguro > Configuración > Dominio de la aplicación**).
- Las políticas se configuran y vinculan a la aplicación respectiva.
- La configuración de la política de acceso es correcta.

Problema con la ubicación de los recursos

Código de información: 0x001800DB

- Asegúrese de que una ubicación de recurso esté configurada.

  1. En el menú de hamburguesa de Citrix Cloud, seleccione **Ubicación del recurso**.
  2. Asegúrese de que la ubicación del recurso esperada esté configurada y que la ubicación del recurso esté en estado activo.

- Asegúrese de que se seleccione una ubicación de recurso correcta para el destino en la tabla Dominio de aplicación (**Acceso privado seguro > Configuración > Dominio de aplicación**).

Los destinos configurados en la aplicación TCP/UDP/HTTP se agregan automáticamente a esta tabla. Se recomienda no eliminar ni deshabilitar los destinos o URL de las aplicaciones TCP/UDP/HTTP activas en la tabla de dominio de aplicación.

La política de seguridad mejorada está vinculada a la aplicación HTTP

Código de información: 0x001800DC, 0x001800DD, 0x13000006

Se accede a la aplicación HTTP que tiene una política de seguridad mejorada 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 política 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.
- Deshabilite 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 acceso privado seguro.
  - Haga clic en la pestaña **Aplicaciones** y busque el nombre de la política para la aplicación HTTP/HTTPS de destino a la que se accedió.
  - Haga clic en la pestaña **Políticas de acceso** y busque el nombre de la política identificada anteriormente.
  - Seleccione la política y haga clic en **Editar**.
  - Cambie la acción de **Permitir acceso con restricción** a **Permitir acceso.**

Para obtener detalles sobre la configuración, consulte Agregar y administrar aplicaciones.

> **Nota**
>
> El servicio de aislamiento de navegador remoto de Citrix se conocía anteriormente como servicio de navegador seguro.

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 FDQN no excedan los 256 caracteres.

Dirección IP no válida

Código de información: 0x001800ED

La dirección IP recibida en la solicitud de inicio de la aplicación no es válida.

Se recomienda acceder únicamente 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 del recurso.

- Asegúrese de que la ubicación del recurso esté en estado activo.
  - En el menú de hamburguesa de Citrix Cloud, seleccione **Ubicación del recurso**.
  - Ejecute una verificación de estado de los dispositivos conectores en la ubicación del recurso correspondiente.
  - Si esto no soluciona el problema, reinicie la máquina virtual del conector.
- Mantener un dispositivo conector de alta disponibilidad
  - En el menú de hamburguesa de Citrix Cloud, seleccione **Ubicación del recurso**.
  - Asegúrese de que la ubicación del recurso tenga al menos dos dispositivos conectores.
- Asegúrese de lo siguiente:
  - La ubicación del recurso LAN está en condiciones de funcionamiento.
  - No hay firewalls ni servidores proxy en el medio que bloqueen el acceso del dispositivo Connector al servicio o a los servidores back-end.
  - La red de clientes está saludable.
  - Los servidores privados back-end están en buen estado.
  - Los servidores DNS están en buen estado.
  - Los FQDN se pueden resolver.

Si no hay problemas con esto, haga lo siguiente:

1. Obtenga el ID de transacción de los registros de diagnóstico para este error.
2. Filtrar todos los eventos que coincidan con el ID de transacción en el panel del servicio de acceso privado seguro.
3. Verifique los registros de diagnóstico correspondientes al ID de transacción desde el panel del servicio Secure Private Access y luego tome las medidas adecuadas según corresponda.
4. Verifique que se haya seleccionado una ubicación de recurso correcta como destino en la tabla Dominio de aplicación (**Acceso privado seguro > Configuración > Dominio de aplicación**).
5. Verifique si la aplicación está configurada (**Acceso privado seguro > Aplicaciones**) con la dirección IP, el puerto y el FQDN correctos.

Si ninguno de estos pasos resuelve el problema, comuníquese con el soporte técnico de Citrix con el código de error correspondiente al ID de transacción y recopile los registros del cliente.

Para recopilar registros de depuración del cliente, consulte Cómo recopilar registros del cliente.

IPv6 recibido en la solicitud de la aplicación

Código de información: 0x001800F5

Se recibe en la solicitud de la aplicación una IPv6 que no es compatible. Actualmente, sólo se admite IPv4.

Edite la aplicación para solucionar el problema de la dirección IP de la aplicación.

1. Vaya al portal de administración de acceso privado seguro.
2. Haga clic en la ficha **Aplicaciones**.
3. Busque la aplicación y haga clic en **Editar**.

Para obtener más detalles, consulte Agregar y administrar aplicaciones.

El tráfico UDP no se pudo entregar

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 la sesión y vuelva a iniciarla.

Error en la entrega del tráfico de datos UDP

Código de información: 0x001800FF

- Busque el ID de transacción para el código de error y filtre todos los eventos que coincidan con el ID de transacción en el panel del servicio de acceso privado seguro.
- Verifique si ocurrió algún error en el otro componente que coincide con el ID de transacción. Si se encuentra un problema en otros componentes, tome las medidas adecuadas.
- Si esto no resuelve el problema, comuníquese con el soporte de Citrix con el código de error junto con el ID de transacción correspondiente.

El inicio de la aplicación falló debido a problemas de conectividad de red

Código de información: 0x10000401

Error en el inicio de la aplicación debido a problemas de conectividad de red entre el dispositivo Conector y el servicio de acceso privado seguro

1. Verifique la conectividad a Internet pública del dispositivo conector.
2. Compruebe si alguna regla de proxy o firewall está bloqueando la conexión.

3. Si algún proxy está causando el problema, omítalo e intente iniciar la aplicación nuevamente.
4. Verifique el estado de salud del dispositivo Connector (**Citrix Cloud > Ubicación del recurso**).

Para obtener detalles sobre la configuración de red, consulte Configuración de red para su dispositivo Connector.

El dispositivo conector no pudo registrarse en el servicio de acceso privado seguro

Código de información: 0x10000402, 0x1000040C

1. Vaya a la página de administración de dispositivos del conector y consulte el Resumen del conector.
2. Si el estado del conector no es bueno, vaya a la ubicación del recurso en el portal de administración.
3. Ejecute una verificación de estado de los dispositivos conectores en la ubicación del recurso correspondiente.
4. Si la comprobación de estado falla, reinicie la máquina virtual del conector.
5. Verifique el resumen del conector y ejecute la verificación de estado nuevamente.

Para obtener detalles sobre la configuración de red, consulte Configuración de red para su dispositivo Connector.

Problema de conectividad con el dispositivo Connector

Código de información: 0x10000403, 0x10000404, 0x10000407, 0x1000040A, 0x1000040B, 0x1000040F, 0x10000410

- Busque el ID de transacción para obtener el código de error.
- Filtra todos los eventos que coincidan con el ID de transacción en el panel de acceso privado seguro.
- Verifique si ocurrió algún error en el otro componente que coincida con el ID de transacción; si lo encuentra, realice la solución alternativa correspondiente a 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.
  - Descargar el informe de diagnóstico. Para obtener más detalles, consulte Generación de un informe de diagnóstico.
  - Capturar el rastro del paquete. Para obtener más detalles, consulte Verificar su conexión de red.
- Comuníquese con el soporte técnico de Citrix con este informe de diagnóstico y el seguimiento de paquetes junto con el código de error y el ID de transacción.

Problemas de conectividad con el dispositivo Connector y los servidores TCP/UDP privados de back-end

Código de información: 0x10000405, 0x10000408, 0x10000409, 0x1000040D, 0x1000040E, 0x10000412

El dispositivo conector tiene problemas de conectividad con los servidores TCP/UDP privados de back-end.

- Verifique si el servidor back-end al que el usuario final intenta conectarse está en funcionamiento y puede recibir las solicitudes.
- Verifique la accesibilidad de los servidores back-end desde dentro de la red corporativa.
- Verifique la configuración del proxy para ver si el conector no puede llegar al servidor back-end.
- Si la solicitud es para una aplicación basada en FQDN, verifique la entrada DNS de la aplicación respectiva en el servidor DNS.

El dispositivo conector no puede resolver el DNS para los FQDN

Código de información: 0x10000406

- Verifique la entrada DNS para el FQDN de la aplicación respectiva en el servidor DNS.
- Asegúrese de que haya un servidor DNS apropiado configurado en los dispositivos conectores. Para obtener más detalles, consulte Configuración de ajustes de red en la página de administración del dispositivo Connector.

La conexión al servidor privado ha finalizado

Código de información: 0x10000411

La conexión al servidor privado es finalizada por el cliente o el servicio de acceso privado seguro.

1. Verifique si el usuario final ha cerrado la aplicación.
2. Verifique otros registros de diagnóstico que coincidan con el ID de transacción de este registro y tome las medidas apropiadas según corresponda.
3. Inicie la aplicación nuevamente.
4. Si esto no resuelve el problema, comuníquese con el soporte técnico de Citrix con el código de error y el ID de transacción.

No se pudo conectar ni enviar datos a la dirección IP o FQDN del servicio privado

Código de información: 0x10000413

- La conexión al servidor privado ha finalizado
- [Problemas de conectividad con el dispositivo Connector y los servidores TCP/UDP privados de back-end](/es-es/citrix-secure-private-access/service/secure-private-access-troubleshooting.html#problemas-de-conectividad-con-el-dispositivo-conector-y-servidores-tcpudp-privados-de-backend). Revise las entradas del dominio de enrutamiento. Asegúrese de que las direcciones IP sean válidas y apunten al back-end correcto.

No hay ninguna condición de política coincidente

Código de información: 0x100508

El contexto del usuario no coincide con las condiciones de la regla de acceso definidas en las políticas asignadas a la aplicación.

Actualice la configuración de la política para que coincida con el contexto del usuario.

No hay ninguna política de acceso asociada a la aplicación

Código de información: 0x100509

1. En la GUI del servicio Citrix Secure Private Access, haga clic en **Políticas de acceso** en la navegación izquierda.
2. Asegúrese de que una política de acceso esté asociada con la aplicación respectiva.
3. Si una política de acceso no está asociada con la aplicación, cree una política de acceso para la aplicación. Para obtener más detalles, consulte Crear políticas de acceso.
4. Si esto no resuelve el problema, comuníquese con el soporte técnico 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 no publicada. Si esto no es lo esperado, haga lo siguiente.

1. Vaya al portal de administración del servicio de acceso privado seguro.
2. Haga clic en **Aplicaciones** en la navegación izquierda.
3. Busque la aplicación y haga clic en **Editar**.

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 **Acceso privado seguro > Configuración > Dominio de aplicación** no resuelve este problema. Debe agregarse como parte de la configuración de la aplicación.

Información de enumeración de la aplicación

Código de información: 0x10050C

Este código captura los resultados de la evaluación de políticas de múltiples aplicaciones a las que el usuario podría tener derecho. El acceso a la aplicación podría ser denegado por los siguientes motivos:

- El contexto del usuario no coincide con las condiciones de la regla de acceso definidas en las políticas asignadas a la aplicación. Para obtener más detalles, consulte No hay condición de política coincidente.
- No hay ninguna política de acceso asociada con la aplicación. Para obtener más detalles, consulte No hay ninguna política de acceso asociada con la aplicación.
- Se configura una política asociada con la aplicación para denegar el acceso. En este caso, no se requiere ninguna acción ya que esa es la intención.
- Error interno inesperado al aplicar la política de acceso. Para obtener más detalles, comuníquese con el soporte de Citrix.

El inicio de la aplicación TCP/UDP falló porque falta una entrada de enrutamiento en la tabla de dominio de la aplicación

Código de información: 0x00180101

Este problema puede ocurrir si la configuración de la aplicación está presente pero la entrada de enrutamiento falta o se eliminó previamente.

Agregue una entrada de enrutamiento (**Acceso privado seguro > Configuración > Dominio de aplicación**) para el destino al que se accede.

El inicio de la aplicación TCP/UDP falló porque los conectores no están en buen estado

Código de información: 0x00180102

Este problema puede ocurrir si ninguno de los conectores está activo o responde a la nueva conexión.

Ejecute una verificación de estado de los dispositivos conectores en la ubicación del recurso correspondiente.

La solicitud UDP/DNS falló porque el conector no está disponible

Código de información: 0x00180103

Este problema puede ocurrir si el tráfico UDP/DNS no puede llegar al conector.

Ejecute una verificación de estado de los dispositivos conectores en la ubicación del recurso correspondiente.

No se pudo cargar la página porque la cookie NGS ha expirado

Código de información: 0x20580001

1. Reinicie el navegador e intente abrir la aplicación nuevamente.
2. Si esto no resuelve el problema, comuníquese con el soporte técnico de Citrix.

La obtención de la política de acceso falló debido a una falla de la red

Código de información: 0x20580002

1. Verifique la URL y la conexión de red.
2. Reinicie el navegador e intente abrir la aplicación nuevamente.
3. Si esto no resuelve el problema, comuníquese con el soporte técnico de Citrix.

Error en la obtención de la política de acceso al analizar el token web JSON

Código de información:0x20580003

1. Reinicie el navegador e intente abrir la aplicación nuevamente.
2. Si esto no resuelve el problema, comuníquese con el soporte técnico de Citrix.

Error en la red al obtener detalles de la política de acceso

Código de información:0x20580004

1. Verifique si la política de acceso está habilitada.
2. Reinicie el navegador e intente abrir la aplicación nuevamente.
3. Si esto no resuelve el problema, comuníquese con el soporte técnico de Citrix.

La obtención de la política falló al obtener el certificado público

Código de información: 0x20580005

1. Reinicie el navegador e intente abrir la aplicación nuevamente.
2. Si esto no resuelve el problema, comuníquese con el soporte técnico de Citrix.

Error en la obtención de la política al validar la firma del token web JSON

Código de información: 0x20580007

1. Verifique si la hora de la red y la hora del dispositivo del usuario están sincronizadas.
2. Reinicie el navegador e intente abrir la aplicación nuevamente.
3. Si esto no resuelve el problema, comuníquese con el soporte técnico de Citrix.

La obtención de la política falló al validar el certificado público

Código de información: 0x20580008

1. Reinicie el navegador e intente abrir la aplicación nuevamente.
2. Si esto no resuelve el problema, comuníquese con el soporte técnico de Citrix.

No se pudo determinar el entorno de la tienda para formar una URL de política

Código de información: 0x2058000A

1. Reinicie el navegador e intente abrir la aplicación nuevamente.
2. Si esto no resuelve el problema, comuníquese con el soporte técnico de Citrix.

No se pudo obtener una respuesta para la solicitud de obtención de la política de acceso

Código de información: 0x2058000B

1. Reinicie el navegador e intente abrir la aplicación nuevamente.
2. Si esto no resuelve el problema, comuníquese con el soporte técnico de Citrix.

La obtención de la política de acceso falló debido a un token de autenticación DS secundario vencido

Código de información: 0x2058000C

1. Reinicie el navegador e intente abrir la aplicación nuevamente.
2. Si esto no resuelve el problema, comuníquese con el soporte técnico de Citrix.

El dispositivo conector no está registrado

Código de información: 0x10200002

Verifique el registro del dispositivo conector.

Para obtener más detalles, consulte Registrar su dispositivo Connector con Citrix Cloud.

No se puede conectar al dispositivo conector

Código de información: 0x10200003

El dispositivo Connector no puede comunicarse entre Citrix Cloud y las ubicaciones de recursos.

Verifique el registro del conector.

Para obtener más detalles, consulte Registrar su dispositivo Connector con Citrix Cloud.

La conexión al servicio Citrix Secure Private Access falló

Código de información: 0x10000301

Verifique la configuración de red del dispositivo conector. Para obtener más detalles, consulte Configuración de red para su dispositivo conector.

El servidor proxy no es accesible

Código de información: 0x10000303, 0x10000304

Verifique la configuración del servidor proxy y asegúrese de que el dispositivo Connector pueda acceder a él. Para obtener más detalles, consulte Registrar su dispositivo Connector con Citrix Cloud.

Error en la autenticación del servidor proxy

Código de información: 0x10000305

Verifique las credenciales del servidor proxy y asegúrese de que estén configuradas correctamente en Connector Appliance. Para obtener más detalles, consulte Después de registrar su dispositivo conector.

Los servidores proxy configurados no son accesibles

Código de información: 0x10000306

Verifique la configuración de red del dispositivo conector, la configuración del firewall o la configuración del servidor proxy. Para obtener más detalles, 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 backend

Código de información: 0x10000307

Verifique el código de estado HTTP del servidor web backend, si no es el código esperado.

No se puede enviar la solicitud a la URL de destino

Código de información: 0x10000005

Verifique la URL de destino o verifique la configuración de red del dispositivo conector. Para obtener más detalles, consulte Configuración de red para su dispositivo conector.

No se pudo procesar el SSO

Código de información: 0x10000107

Error al recuperar los datos de configuración de la aplicación de Citrix Cloud.

Verifique la configuración de red del dispositivo conector y asegúrese de que el servidor NTP esté configurado y que no haya problemas con las franjas horarias. Para obtener más detalles, consulte Configuración de red para su dispositivo conector.

La conexión al servicio Citrix Secure Private Access falló

Código de información: 0x10000108, 0x1000010B

Verifique la configuración de red del dispositivo conector. Para obtener más detalles, consulte Configuración de red para su dispositivo conector.

No se pudo procesar el SSO, no se pueden determinar las configuraciones del SSO

Código de información: 0x1000010A

Verifique la configuración de SSO y asegúrese de que el servidor sea accesible para el dispositivo Connector.

Error de inicio de sesión único (SSO) de FormFill: configuración incorrecta de la aplicación de formulario

Código de información: 0x10000101, 0x10000102, 0x10000103, 0x10000104

Verifique la configuración de la aplicación del formulario SSO y asegúrese de que los campos de nombre de usuario, contraseña, acción y URL de inicio de sesión estén configurados correctamente en la configuración de la aplicación.

Error en el inicio de sesión único de Kerberos

Código de información: 0x10000202

Verifique la configuración de SSO de Kerberos en el servidor back-end y el controlador de dominio. Verifique también la configuración de autenticación NTLM de respaldo.

Para conocer la configuración de SSO de Kerberos, consulte Validación de su configuración de Kerberos.

No se pudo procesar el SSO para el tipo de autenticación

Código de información: 0x10000203

Verifique la configuración de SSO en el servicio de acceso privado seguro y el servidor backend. Para el servicio de acceso privado seguro, consulte Establecer el método de inicio de sesión preferido.

El SSO de Kerberos falló y se vuelve a utilizar NTLM

Código de información: 0x10000204

La recuperación del ticket Kerberos del controlador de dominio ha fallado. Como autenticación secundaria, Connector Appliance ha probado la autenticación NTLM de respaldo.

Para habilitar una autenticación Kerberos exitosa, verifique la configuración de SSO de Kerberos en el servidor back-end y el controlador de dominio.

Para obtener más detalles, consulte Validación de su configuración de Kerberos.

Varias cuentas autorizadas a ZTNA configuradas en la aplicación Citrix Workspace

Código de información: 0x14000001

Configure solo una cuenta autorizada ZTNA en la aplicación Citrix Workspace.

Cómo recopilar registros de clientes

- **Cliente Windows:**
  1. Abra la aplicación y asegúrese de que el registro esté habilitado.
  2. Ahora conéctese al servicio de acceso privado seguro y duplique el problema que está enfrentando.
  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 de la máquina cliente.
- **Cliente Mac:**
  1. Abra la aplicación y vaya a **Registros > Verbose**.
  2. Borre los registros y proceda a reproducir el problema.
  3. Regresar a **Registros > Exportar registros**. Esto crea un archivo zip que contiene archivos de registro.

Respuestas a preguntas frecuentes

¿Qué son los registros de diagnóstico de acceso privado seguro?

Los registros de diagnóstico de acceso privado seguro capturan todos los eventos que ocurren 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 la aplicación y los registros de acceso a la aplicación. Los detalles se presentan en formato tabular. Puede ver los registros del tiempo preestablecido o de una línea de tiempo personalizada. Puede agregar columnas al gráfico haciendo clic en el signo + según la información que desee ver en el panel. Puede exportar los registros de usuario en formato CSV.

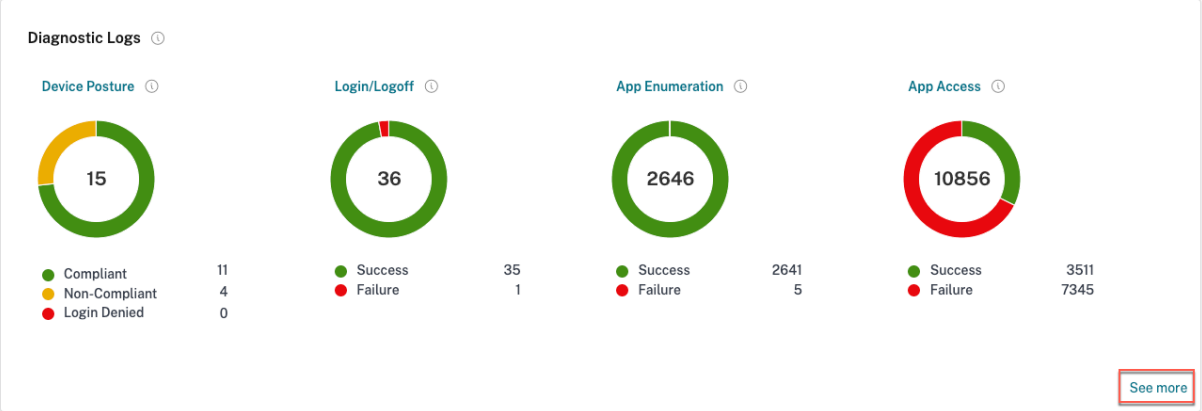
¿Dónde puedo encontrar los registros de acceso privado seguro?

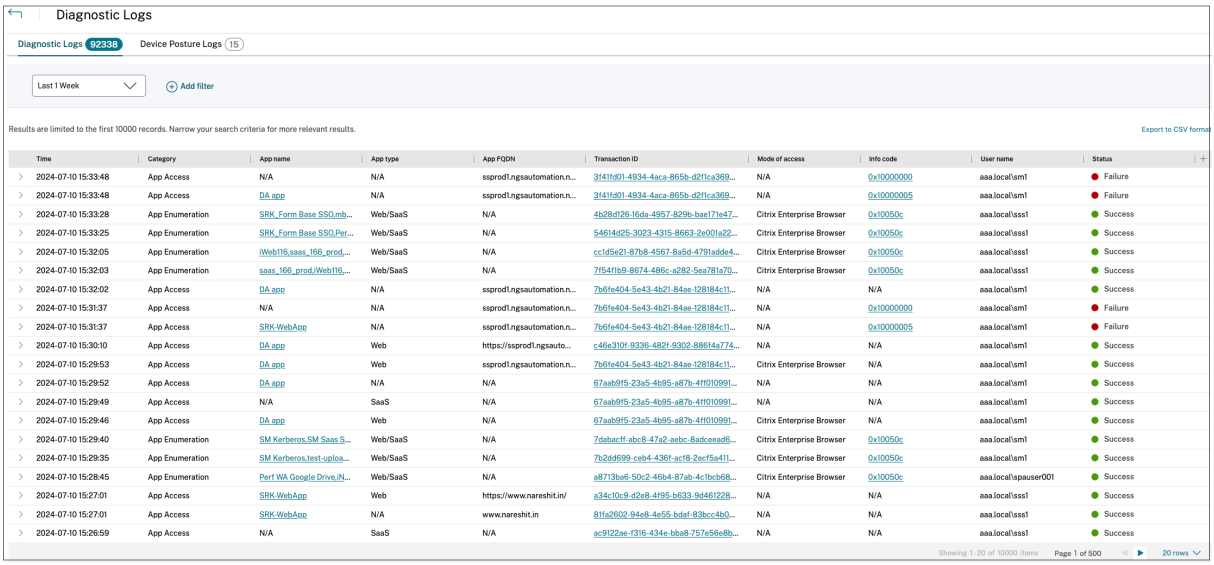
1. Inicie sesión en Citrix Cloud.
2. En el mosaico del servicio Acceso privado seguro, haga clic en **Administrar**.

3. Haga clic en **Panel de control** en la navegación izquierda de la interfaz de usuario de administrador.
4. En el gráfico **Registros de diagnóstico** , haga clic en el enlace **Ver más** .

¿Qué widget muestra los registros de diagnóstico de acceso privado seguro?

Los widgets **Registros de diagnóstico** en la sección **Registro y solución de problemas** muestran una vista de gráfico circular de todos los eventos de acceso privado seguro relacionados con la autenticación, el inicio de aplicaciones, la enumeración de aplicaciones y también los registros relacionados con la postura del dispositivo. Los registros de diagnóstico de acceso privado seguro obtienen eventos de varios componentes internos, cada uno de los cuales envía un evento cuando un usuario final accede a una aplicación. Estos eventos se dividen en categorías; **Inicio de sesión/Cierre de sesión**, **Enumeración de aplicaciones**y **Acceso a aplicaciones**. El gráfico circular muestra la relación general de éxito/fracaso de cada categoría. Al hacer clic en el gráfico circular de color en cualquier gráfico, accederá a los registros de diagnóstico donde podrá encontrar los eventos correspondientes. También hay registros de postura del dispositivo si tiene habilitado el servicio de Postura del dispositivo. También puede hacer clic en el enlace **Ver más** para ver los registros de diagnóstico completos.





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

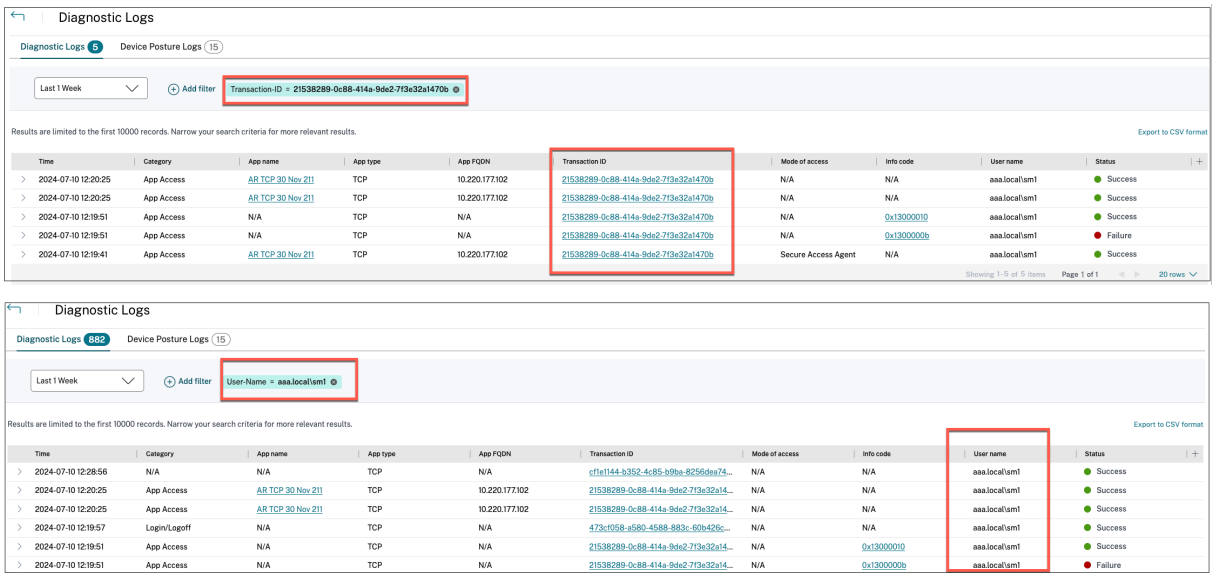
El panel de registros de usuario de Secure Private Access proporciona los siguientes detalles, de forma predeterminada.

- **Marca de tiempo** - 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(s) aplicación(es) a las que se accedió.
- **Información de política** : muestra el nombre de la política o políticas de acceso que se activaron durante el evento.
- **Estado** - Muestra el estado del evento, éxito o fracaso.
- **Código de información** : cada evento de falla dentro del panel de registros de diagnóstico de acceso privado seguro tiene un código de información asociado. Ver más información en 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 con la operación realizada.
- **Tipo de operación** : muestra la operación para la que se genera el registro.
- **Categoría** - Hay tres categorías disponibles según el tipo de evento. Esto es autenticación de aplicaciones, enumeración de aplicaciones o acceso a aplicaciones. Estas opciones también están disponibles como opciones de filtro. Puede utilizar estas opciones para filtrar registros según el tipo de problema que esté enfrentando.
- **ID de transacción** : el ID de transacción correlaciona todos los registros de acceso privado seguro para una solicitud de acceso. Aprenda a utilizar un ID de transacción. Los siguientes detalles se pueden obtener haciendo clic en el botón + en el lado más a la derecha del panel:

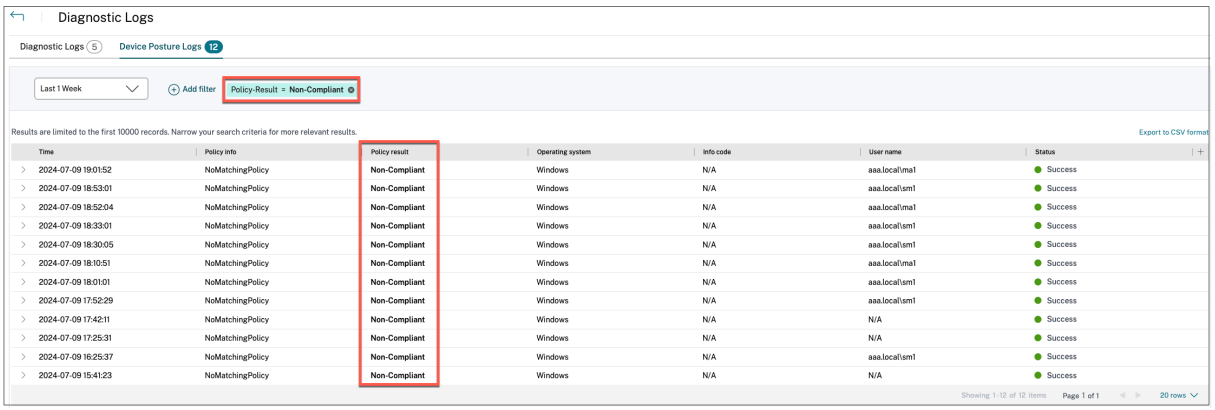
- **Ubicación PoP de SPA** : muestra el nombre/ID de la ubicación PoP del servicio de acceso privado seguro que se utilizó durante el acceso a la aplicación. Consulte Ubicaciones de PoP de acceso privado seguro.

¿Cómo filtro los registros de diagnóstico?

Puede utilizar la opción **Agregar filtro** para refinar su búsqueda en función de diversos criterios, como el tipo de aplicación, la categoría y la descripción. Por ejemplo, en el campo de búsqueda, puede hacer clic en ID de transacción, = (es igual a algún valor) e ingresar 21538289-0c88-414a-9de2-7f3e32a1470b, para buscar todos los registros relacionados con este ID de transacción. Para obtener detalles sobre los operadores de búsqueda que se pueden utilizar con la opción de filtro, consulte Operadores de búsqueda.



También puede utilizar las distintas opciones de filtro para refinar su búsqueda en los registros de postura del dispositivo.



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

Los registros de diagnóstico de acceso privado seguro 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 se le negó el acceso según su política de postura del dispositivo.
- **Inicio de sesión/Cierre de sesión**: Eventos sobre el estado de inicio de sesión 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 de acceso privado seguro, 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 dentro de la aplicación Citrix Workspace. Estos eventos le ayudan a saber a qué aplicaciones se les permitió o denegó el acceso a un usuario según las políticas de acceso configuradas dentro del servicio de acceso privado seguro.
- **Acceso a la aplicación**: Eventos de acceso a la aplicación/punto final del usuario final, estado de permitir/denegar, estado de inicio de sesión único y estado de conectividad según las políticas de acceso configuradas para el intervalo de tiempo seleccionado.

¿Cómo uso el tema de solución de problemas de acceso privado seguro para resolver una falla que he encontrado?

1. Obtenga el código de información para la falla que está intentando resolver.
2. Encuentre 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? ¿Donde los encuentro?

Algunos eventos de registro, como fallas, tienen un código de información asociado. Busque este código de información dentro de la tabla de búsqueda de errores para encontrar los pasos de resolución o más información sobre ese evento.

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

Los errores o problemas de acceso a través de Citrix Enterprise Browser muestran un ID de transacción al usuario final. Los administradores pueden obtener este ID de transacción de los usuarios finales y usarlo para filtrar los registros exactos que causaron el problema, lo que les permite identificar el problema exacto. Una vez que los administradores filtran eventos con el ID de transacción, solo se

muestran los eventos relacionados con el problema en cuestión, lo que proporciona todos los detalles a los administradores sobre por qué ocurrió la falla o el problema. Los administradores pueden luego usar el código de error en esos registros para resolver aún más los problemas.

¿Cuáles son todas las ubicaciones de PoP de acceso privado seguro?

La siguiente es la lista de ubicaciones de PoP de acceso privado seguro.

Nombre del PoP	Zona	Region
az-us-e	Este azul	Virginia
az-us-w	Azul oeste	California
az-us-sc	Azure surcentralus	Texas
az-a-e	Azul Australia del Este	Nueva Gales del Sur
az-eu-n	Azul norte de Europa	Irlanda
az-eu-w	Azul Europa occidental	Países Bajos
az-jp-e	Azul japaneast	Tokio, Saitama
az-bz-s	Azul Brasil Sur	Estado de Sao Paulo
az-asia-se	Sudeste asiático azul	Singapur
az-uae-n	Uaenorth azul	Dubái
az-en-s	Azul del sur de la India	Chennai
az-asia-hong kong	Azul del este de Asia	Hong Kong

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

Contactar con Citrix Support.

Referencias

- **Agregar una aplicación web**
  - Compatibilidad con aplicaciones web empresariales
  - Configurar el acceso directo a las aplicaciones web
- **Agregar una aplicación SaaS**

  - Soporte para aplicaciones de software como servicio
  - Configuración específica del servidor de aplicaciones SaaS

- **Configurar aplicaciones cliente-servidor**
  - Soporte para aplicaciones cliente-servidor
- **Crear políticas de acceso**
  - Crear políticas de acceso
- **Tablas de redirecciones**
  - Tablas de redirecciones

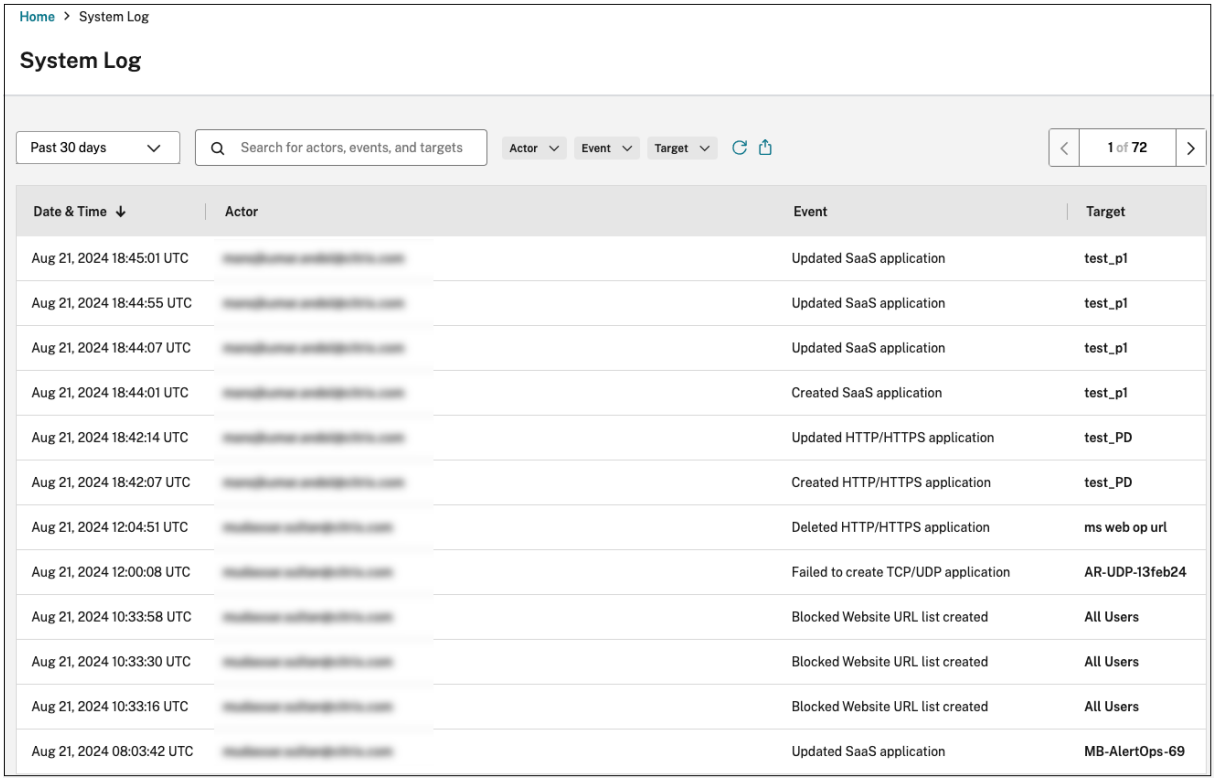
Registros de auditoría

October 21, 2024

Los eventos relacionados con el servicio de acceso privado seguro se capturan en el registro del sistema **de Citrix Cloud >**. 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:

- Crear o actualizar una aplicación
- Eliminar una aplicación
- Configurar o eliminar una política de acceso adaptativa
- Actualización del conector
- Creación de sitios web permitidos o bloqueados

La siguiente figura muestra los eventos relacionados con el acceso privado seguro 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

August 26, 2024

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 después 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)

- Device Posture (comprobación de Device Posture)
- 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 exploradores, 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 Restricciones de acceso disponibles.

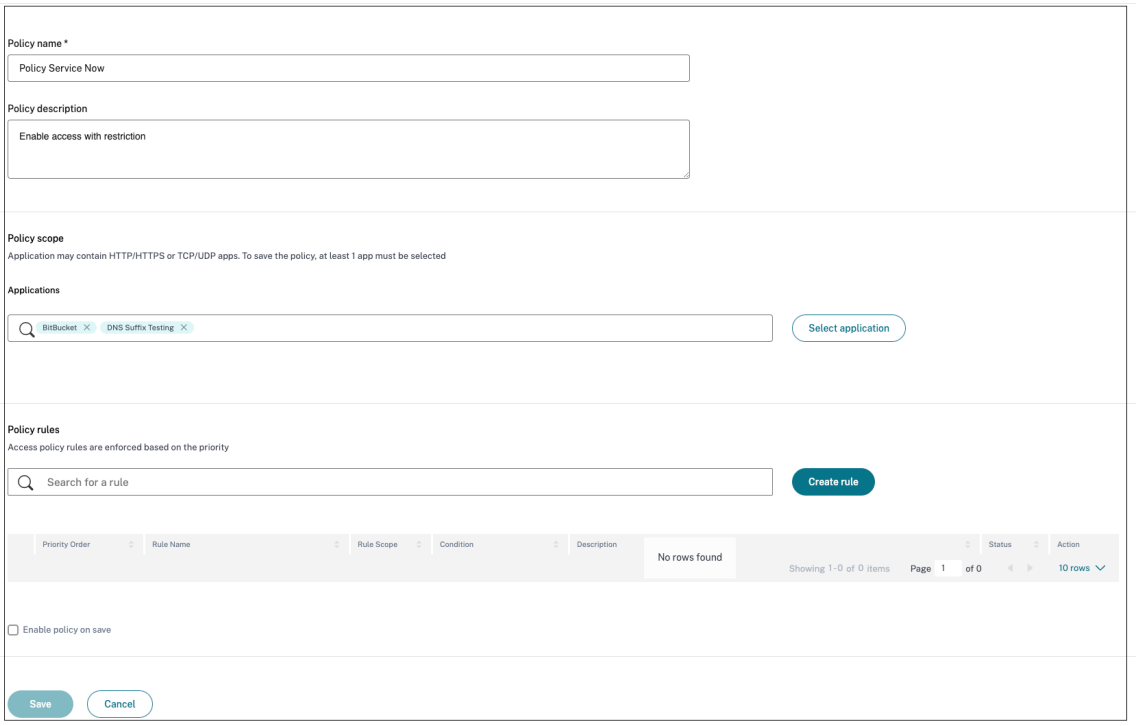
Asegúrese de haber completado las siguientes tareas antes de configurar una directiva de acceso.

- Configurar la identidad y la autenticación
- Aplicaciones configuradas

1. En el panel de navegación, haga clic en **Directivas de acceso** y después 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.

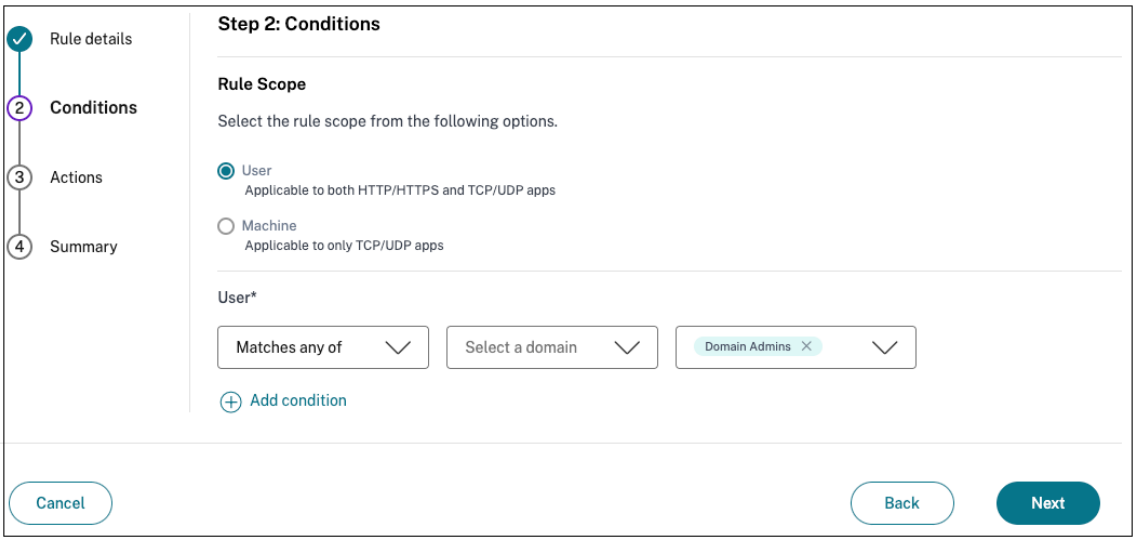


5. Introduzca el nombre de la regla y una breve descripción de la regla y después haga clic en **Siguiente**.

6. Seleccione 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.

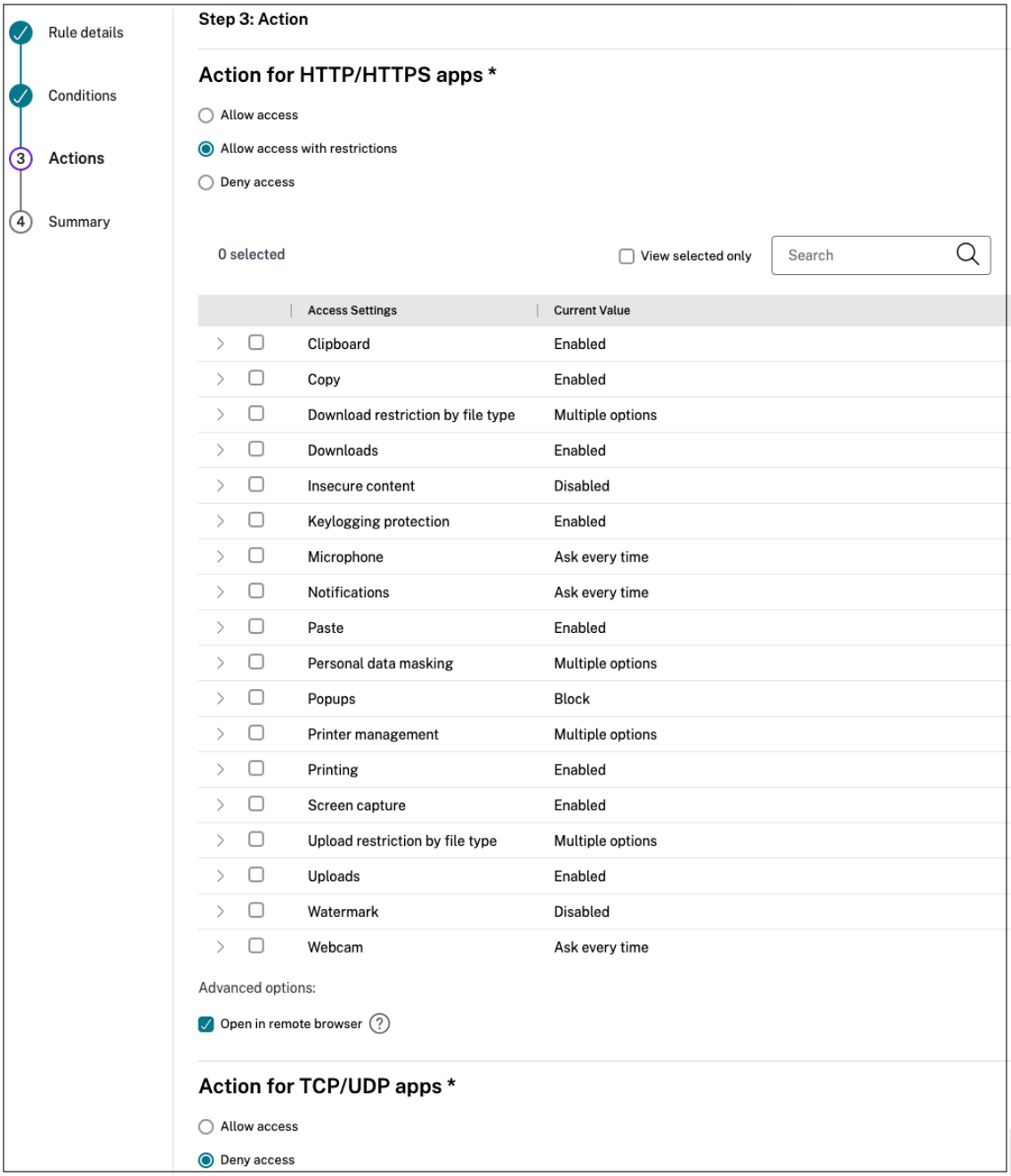
   - Dispositivo de **escritorio** o **móvil**: Seleccione el dispositivo para el que quiere habilitar el acceso a las aplicaciones.
   - **Ubicación geográfica**: Seleccione la condición y la ubicación geográfica desde donde los usuarios acceden a las aplicaciones.
   - **Ubicación de red**: Seleccione la condición y la red mediante la cual los usuarios acceden a las aplicaciones.
   - **Verificación de la Device Posture**: 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.

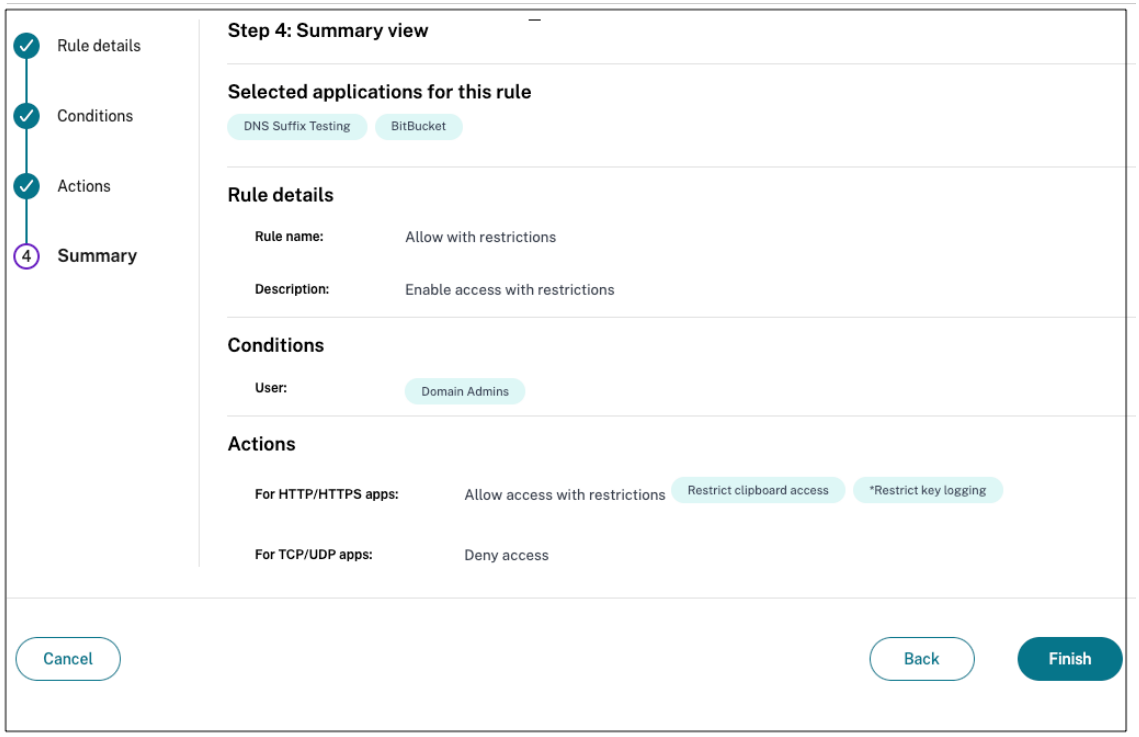
   - Para las aplicaciones HTTP/HTTPS, puede seleccionar lo siguiente:
     - **Permitir el acceso**
     - **Permitir el acceso con restricciones**
     - **Denegar el acceso**

> **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 después 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

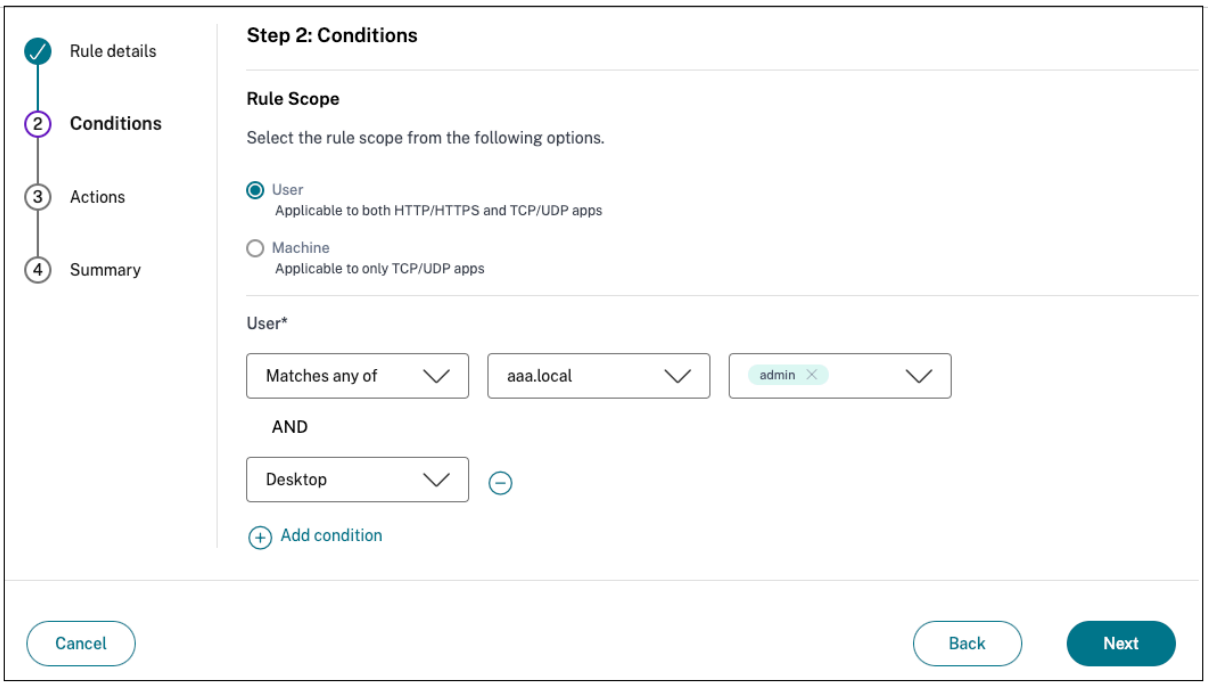
Al seleccionar la acción **Permitir el acceso con restricciones**, debe seleccionar al menos una de las restricciones de seguridad. Estas restricciones de seguridad están predefinidas en el sistema. Los administradores no pueden modificar ni agregar otras combinaciones. Para obtener más información, consulte Opciones de restricciones de acceso disponibles

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.**

- Seleccione **Escritorio** o **Dispositivo móvil**.
- Complete la configuración de la directiva.



Acceso adaptable según la ubicación

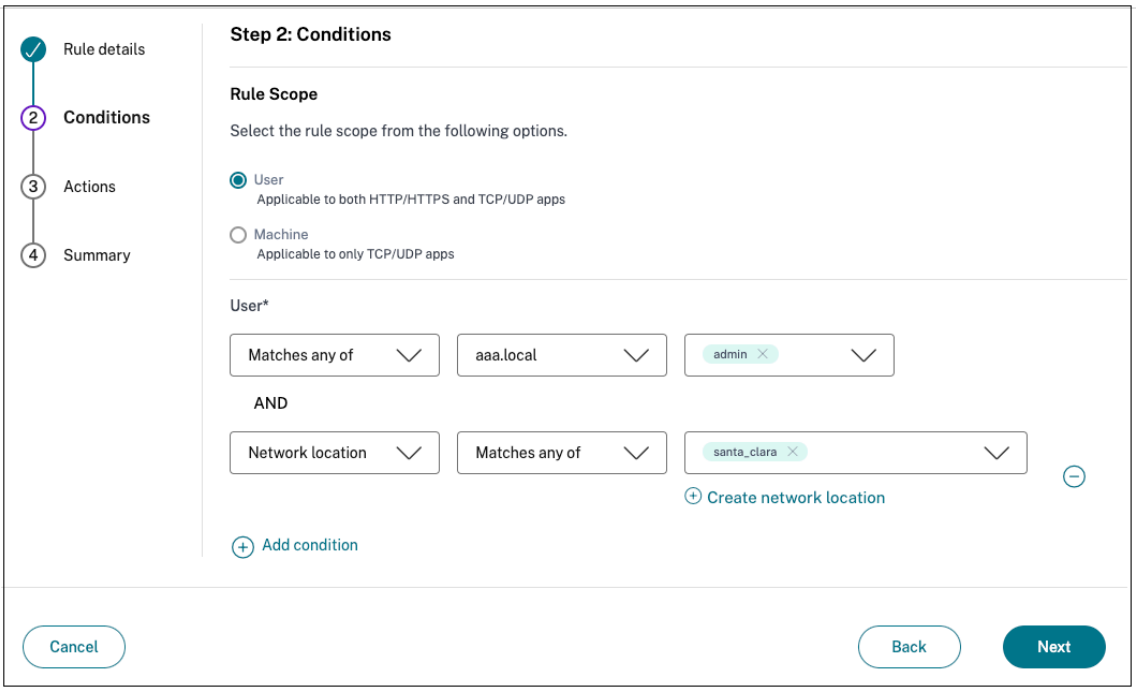
Un administrador puede configurar la directiva de acceso adaptable en función de la ubicación desde la que el usuario accede a la aplicación. La ubicación puede ser el país desde el que el usuario accede a la aplicación o la ubicación de red del usuario. La ubicación de la red se define mediante un rango 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.**
- Seleccione **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 seleccione **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 Device Posture

Puede configurar el servicio Secure Private Access para aplicar el control de acceso mediante etiquetas de Device Posture. Una vez que se permite que un dispositivo inicie sesión después de la verificación de la Device Posture, el dispositivo se puede clasificar como compatible o no compatible. Esta

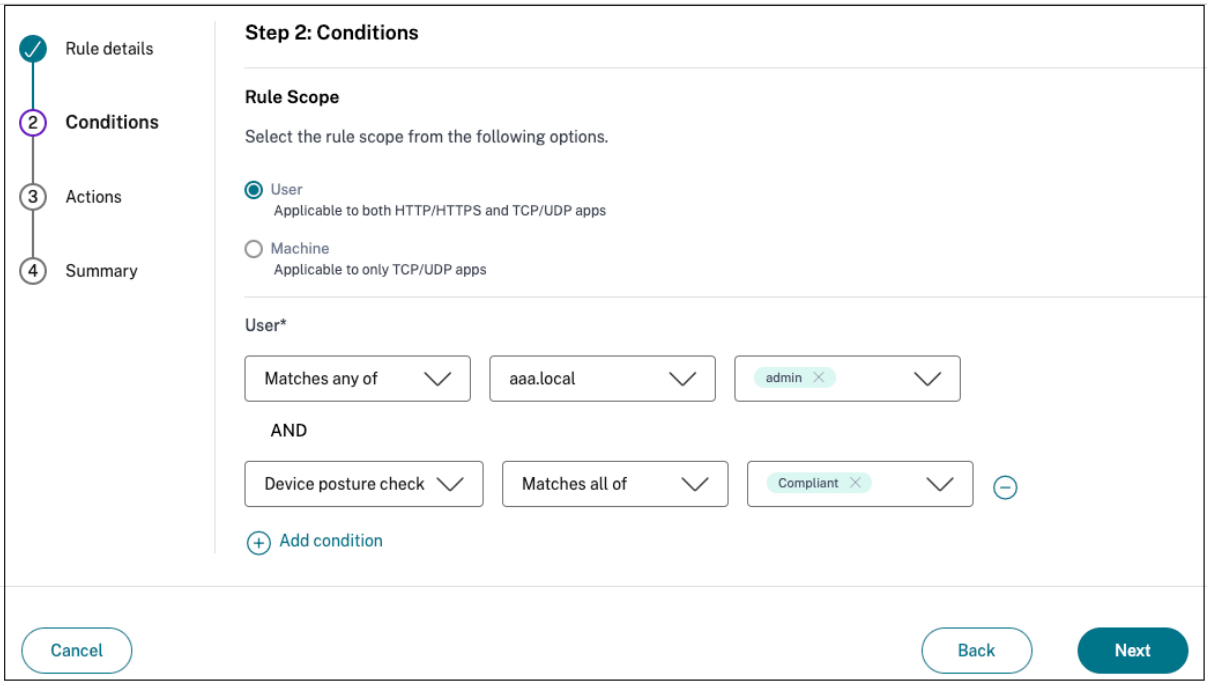
información está disponible como etiquetas para los servicios Citrix DaaS y Citrix Secure Private Access y se utiliza para proporcionar un acceso contextual en función de la Device Posture.

Para obtener información completa sobre Device Posture Service, consulte Device Posture.

Para configurar una directiva de acceso adaptable en función de la Device Posture, 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 Device Posture** y la expresión lógica en el menú desplegable.
- Introduzca uno de los siguientes valores en las etiquetas personalizadas:
  - **Conforme**: para dispositivos conformes
  - **No conforme**: para dispositivos no conformes

> **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 Device Posture no funcionan según lo previsto.



Acceso adaptable basado en la puntuación de riesgo del usuario

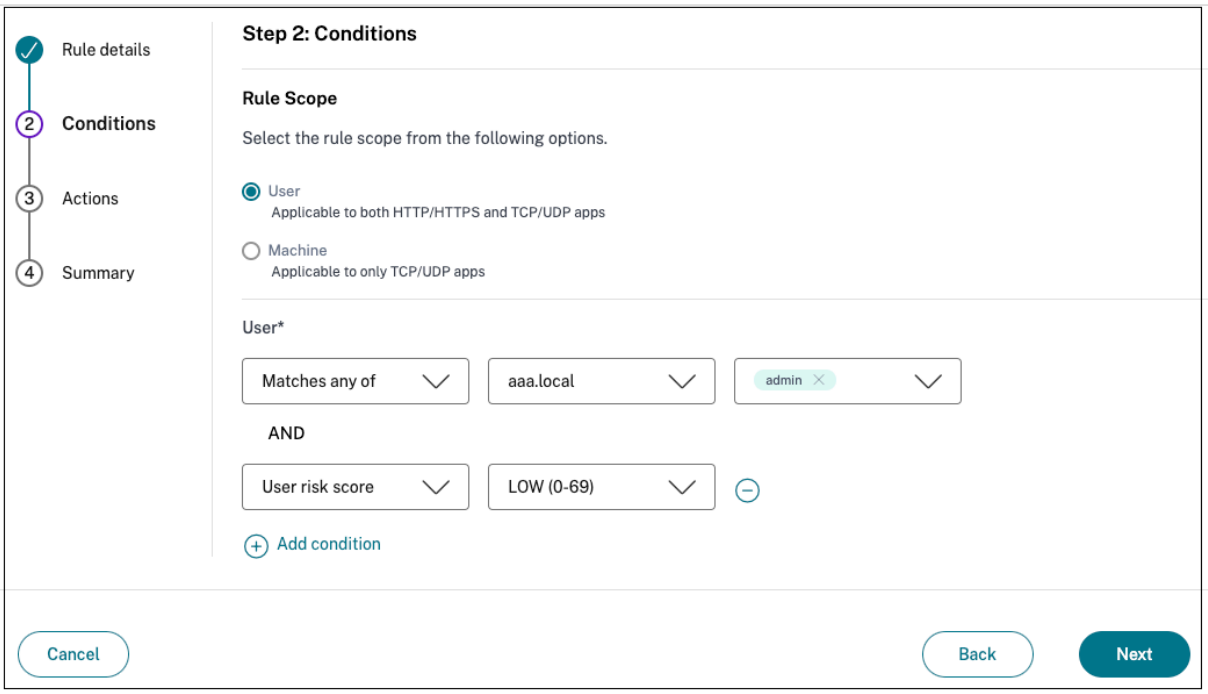
> **Importante:**
>
> Esta función solo está disponible para los clientes si tienen derecho a Security Analytics.

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 después 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 rutas para resolver conflictos resultantes de los mismos dominios relacionados

October 21, 2024

La función de dominios de aplicación del servicio Citrix Secure Private Access permite a los clientes tomar decisiones de enrutamiento que permiten que los dominios relacionados de las aplicaciones se enruten externa o internamente 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 IdP SAML tanto para Salesforce (aplicación SaaS) como para Jira (aplicación web interna), entonces el administrador podría configurar `*.okta.com` como un dominio relacionado en la configuración de ambas aplicaciones. Esto genera un conflicto y el usuario final experimenta un comportamiento inconsistente. En este escenario, el administrador puede definir reglas para enrutar estas aplicaciones de manera externa o interna a través de los dispositivos conectores, según los requisitos.

Cómo funciona la tabla de rutas

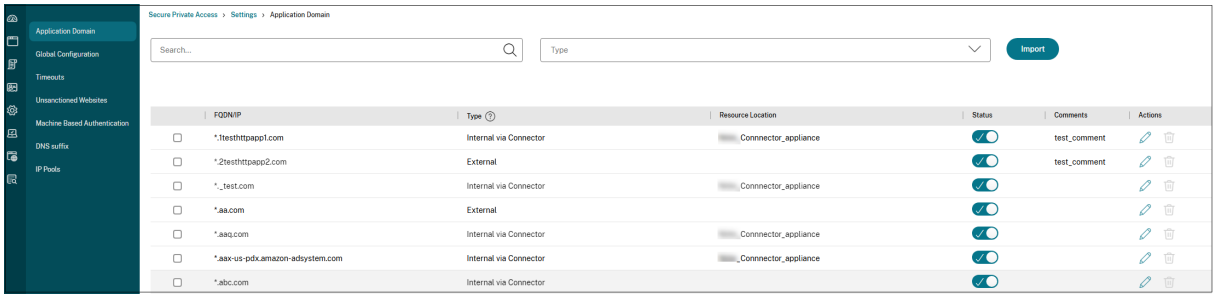
Los administradores pueden definir los siguientes tipos de rutas para las aplicaciones dependiendo de cómo quieran definir el flujo de tráfico.

- **Interno –Omitir proxy** : el tráfico del dominio se enruta a través de Citrix Cloud Connector, sin pasar por el proxy web del cliente configurado en el dispositivo Connector.
- **Interno a través del conector** : las aplicaciones son externas, pero el tráfico debe fluir a través del dispositivo conector hacia la red externa.
- **Externo** –El tráfico fluye directamente a Internet.

> **Nota**
>
> - Las entradas de ruta no afectan las políticas de seguridad configuradas en las aplicaciones.
> - Si los administradores no desean utilizar una entrada en la tabla de rutas o si las aplicaciones correspondientes no funcionan como se espera, los administradores pueden simplemente deshabilitar 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 para una aplicación en particular estaba vinculada a la ubicación de un recurso.

Tabla de ruta principal

La tabla de enrutamiento principal en la consola de Secure Private Access (**Configuración > Dominios de aplicación**) es un panel de solo lectura que le brinda todos los detalles sobre los dominios configurados en todas las aplicaciones. Esto se puede utilizar para ver la siguiente información de cualquier dominio:



La tabla de ruta principal se puede utilizar para ver la siguiente información de cualquier dominio:

- **FQDN/IP:** FQDN o la dirección IP para la que se desea configurar el tipo de enrutamiento de tráfico.
- **Tipo**: Tipo de aplicación. **Interno**, **Interno –Omitir proxy**o **Externo** según se seleccionó al agregar la aplicación.

> **Importante:**
>
> Si hay conflictos, se muestra un icono de alerta para la fila correspondiente en la tabla. Para

> resolver el conflicto, los administradores deben hacer clic en el ícono triangular y cambiar el tipo de aplicación desde la tabla principal.

- **Ubicación del recurso:** Ubicación del recurso para el enrutamiento de tipo **Interno**. Si no se asigna una ubicación de recurso, aparece un ícono triangular en la columna **Ubicación del recurso** para la aplicación respectiva. Al pasar el cursor sobre el icono, se muestra el siguiente mensaje.

  Falta ubicación del recurso. Asegúrese de que una ubicación de recurso esté asociada con este FQDN.

- **Estado:** El interruptor en la columna **Estado** se puede usar para deshabilitar la ruta de una entrada de ruta sin eliminar la aplicación. Cuando el interruptor está en la posición OFF (APAGADO), la entrada de ruta no tiene efecto. Además, si existen FQDN que coinciden exactamente, los administradores pueden seleccionar la ruta que se habilitará o deshabilitará.
- **Comentarios:** Muestra comentarios, si hay alguno.
- **Acciones:** El ícono de edición se utiliza para agregar una ubicación de recurso o cambiar el tipo de entrada de ruta. El icono de eliminar se utiliza para eliminar la ruta.

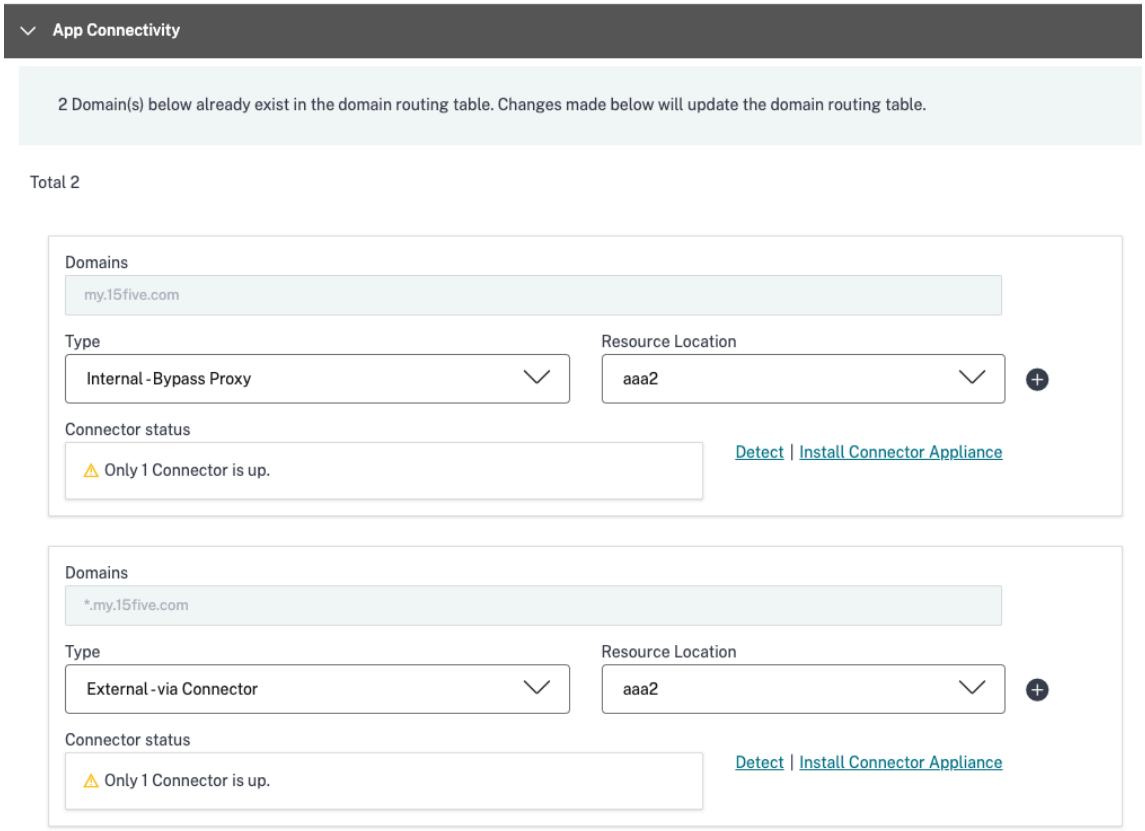
Mini tabla de ruta

Está disponible una versión mini de la tabla Dominios de aplicación para tomar decisiones de enrutamiento durante la configuración de la aplicación. La mini tabla de rutas disponible en la sección **Conectividad de aplicaciones** en la interfaz de usuario del servicio Citrix Secure Private Access.

Para agregar rutas a la mini tabla de rutas

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

1. Siga estos pasos:
   - Elija una plantilla.
   - Introduzca los detalles de la aplicación.
   - Seleccione detalles de seguridad mejorados, según corresponda.
   - Seleccione el método de inicio de sesión único, según corresponda.
2. Haga clic en **Conectividad de la aplicación**. - Está disponible una versión mini de la tabla de dominios de aplicación para tomar decisiones de enrutamiento durante la configuración de la aplicación.



- **Dominios:** La columna Dominios muestra una o más filas para una aplicación en particular. La primera fila muestra la URL real de la aplicación que el administrador ingresó al agregar los detalles de la aplicación. Las otras filas son todos dominios relacionados que se ingresan 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 afirmación SAML, si se selecciona SSO SAML.

- **Tipo:** Seleccione una de las siguientes opciones.
  - **Interno –Omitir proxy** : el tráfico del dominio se enruta a través de Citrix Cloud Connector, sin pasar por el proxy web del cliente configurado en el dispositivo Connector.
  - **Interno a través del conector** : las aplicaciones son externas, pero el tráfico debe fluir a través del dispositivo conector hacia la red externa.
  - **Externo** –El tráfico fluye directamente a Internet.
- **Ubicación del recurso:** Se completa automáticamente cuando selecciona el tipo Interno para una aplicación. Cámbielo si desea una ubicación de recurso diferente.
- **Estado del dispositivo conector:** Se completa automáticamente, junto con la ubicación del recurso, cuando selecciona el tipo Interno para una aplicación.

Sitios web no autorizados

October 21, 2024

Las aplicaciones (intranet o internet) que no estén configuradas dentro de Secure Private Access se consideran "Sitios web no autorizados". De forma predeterminada, Secure Private Access niega el acceso a todas las aplicaciones web de intranet si no hay aplicaciones y políticas de acceso configuradas para esas aplicaciones.

Para todas las demás URL de Internet o aplicaciones SaaS que no tienen una aplicación configurada, los administradores pueden usar la pestaña **Configuración > Sitios web no autorizados** de la consola de administración para permitir o denegar el acceso a través de Citrix Enterprise Browser. Los administradores también pueden redirigir el acceso a un entorno aislado del navegador remoto (RBI) para evitar ataques basados en el navegador. Si un administrador ha configurado la redirección de URL a RBI, se producen las siguientes acciones.

1. El acceso privado seguro convierte los dominios.
2. Luego, Citrix Enterprise Browser envía estas URL a Secure Private Access.
3. El acceso privado seguro redirige esas URL al servicio de aislamiento del navegador remoto.

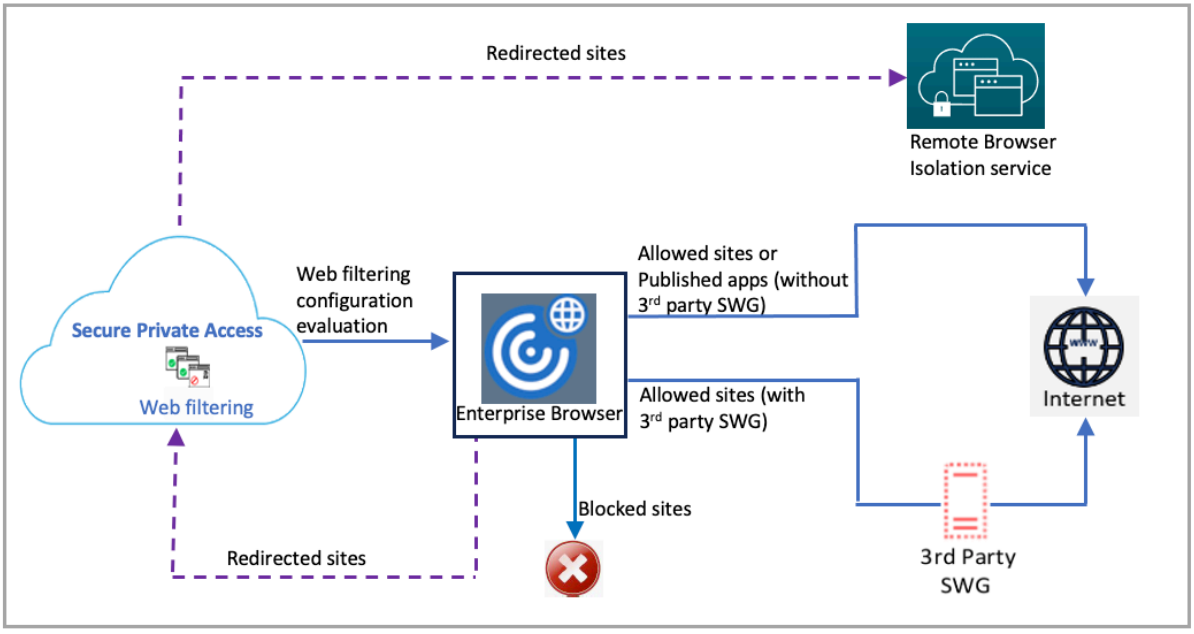
Puede utilizar caracteres comodín, como `*.example.com`, para controlar el acceso a todos los dominios de ese sitio web y a todas las páginas dentro de ese dominio.

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

Cómo funcionan los sitios web no autorizados

1. Se realiza una verificación de análisis de URL para determinar si la URL es una URL de servicio Citrix.
2. Luego se verifica la URL para determinar si se trata de una URL de una aplicación SaaS o una web empresarial.
3. Luego se verifica la URL para determinar si está identificada como una URL bloqueada, si debe redirigirse a una sesión de navegador segura o si se puede permitir el acceso a la URL.

La siguiente ilustración explica el flujo de tráfico del usuario final.

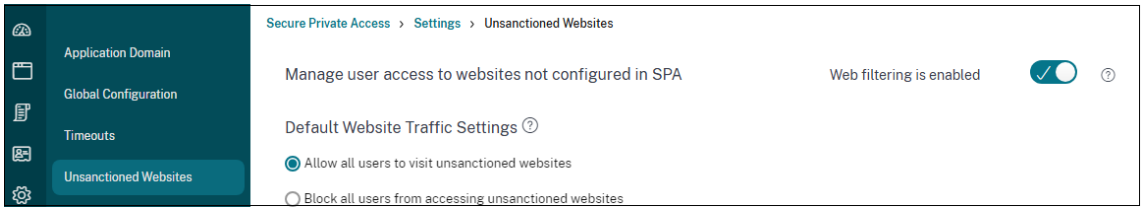


Cuando llega una solicitud, se realizan las siguientes comprobaciones y se toman las acciones correspondientes:

1. ¿La solicitud coincide con la lista global de permitidos?
    a) Si coincide, el usuario podrá acceder al sitio web solicitado.
    b) Si no coincide, se comprueban las listas de sitios web.
2. ¿La solicitud coincide con la lista de sitios web configurados?
    a) Si coincide, la siguiente secuencia determina la acción.
        i. Bloquear
        ii. Redirigir
        iii. Allow
    b) Si no coincide, se aplica la acción predeterminada (PERMITIR). La acción predeterminada no se puede cambiar.

Configurar reglas para sitios web no autorizados

1. En la consola de Acceso Privado Seguro, haga clic en **Configuración > Sitios web no autorizados**.



Nota

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

```
1  ![Configurar reglas](/en-us/citrix-secure-private-access/media/spa-
       enable-website-list-filtering.png)
2
3  También puede cambiar la configuración de URL específicas agregándolas
       a sitios web bloqueados, sitios web permitidos o redirigiéndolas a
       la lista de Aislamiento del navegador remoto.
4
5  Por ejemplo, si ha bloqueado el acceso a todas las URL no autorizadas
       de forma predeterminada y desea permitir el acceso solo a unas pocas
        URL de Internet específicas, puede hacerlo realizando los
       siguientes pasos:
6
7  1.  Haga clic en la pestaña **Sitios web permitidos** y luego haga clic
        en **Permitir un sitio web**.
8  1.  Agregue la dirección del sitio web al que se debe permitir el
       acceso. Puede agregar manualmente la dirección del sitio web o
       arrastrar y soltar un archivo CSV que contenga la dirección del
       sitio web.
9  1.  Haga clic en **Agregar una URL** y luego haga clic en **Guardar**.
10
11     La URL se agrega a la lista de sitios web permitidos.
```

Nota

Un cliente (organización) del servicio estándar de aislamiento remoto del navegador pago obtiene 5000 horas de uso por año de manera predeterminada. Para obtener más horas, deberán comprar los paquetes complementarios del navegador seguro. Puede realizar un seguimiento del uso del servicio de aislamiento remoto del navegador. Para obtener más información, consulte estos temas:

- Administrar y supervisar exploradores web aislados remotos
- Aislamiento del navegador remoto.

Puntos que tener en cuenta

Si los usuarios no tienen acceso a una aplicación SaaS, no pueden iniciar la aplicación desde Citrix Enterprise Browser. Sin embargo, es posible que aún puedan acceder a la aplicación escribiendo la URL directamente en Citrix Enterprise Browser.

- Si la política niega el acceso a una aplicación, la URL de la aplicación se agrega a la lista de bloqueados si la función de filtrado web ** está habilitada. Esto garantiza que se bloquee cualquier intento de acceder a la aplicación, ya sea a través de Citrix Enterprise Browser o directamente mediante URL.
- Para las aplicaciones no publicadas, incluso si el enrutamiento está configurado, se niega el acceso a estas aplicaciones. La URL de la aplicación no publicada se agrega a la lista de bloqueados si la función de filtrado web ** está habilitada, lo que evita cualquier intento de acceso.

Integración de ADFS con Secure Private Access

December 27, 2023

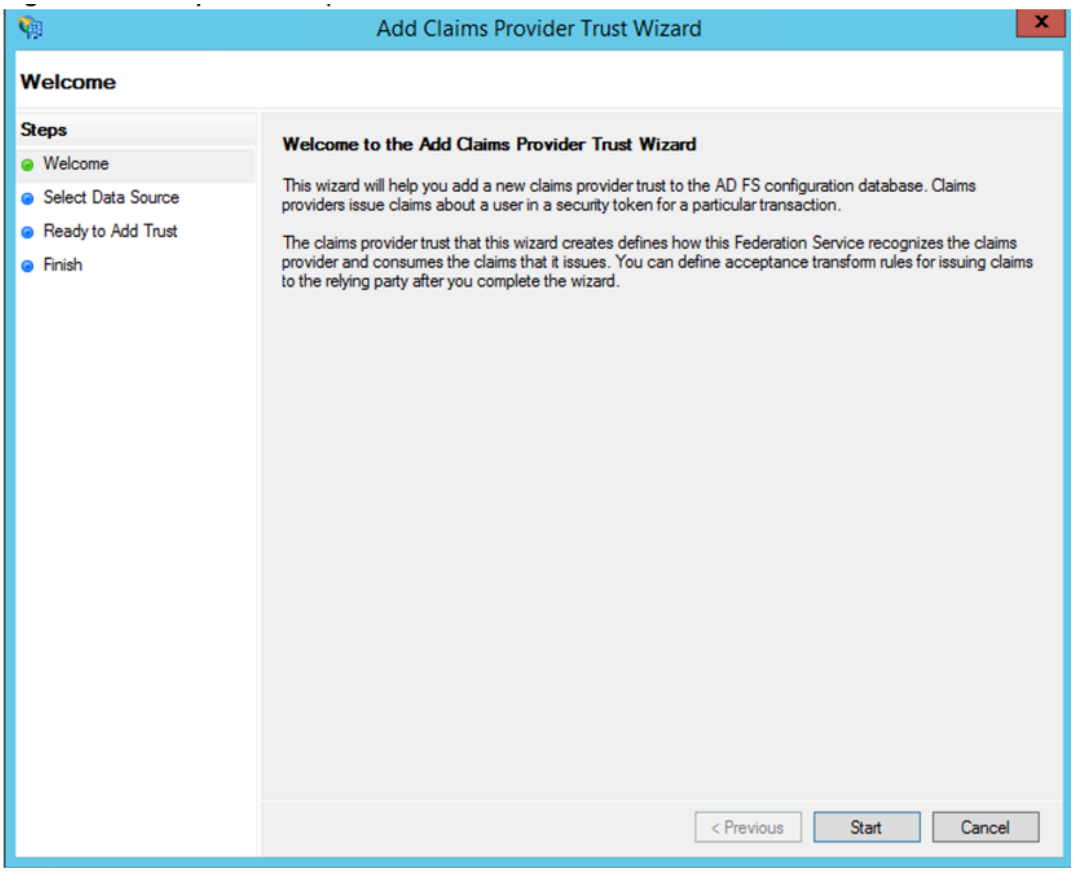
Las reglas de reclamos son necesarias para controlar el flujo de reclamos a través del proceso de reclamos. Las reglas de reclamación también se pueden utilizar para personalizar el flujo de reclamaciones durante el proceso de ejecución de la regla de reclamación. Para obtener más información sobre las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

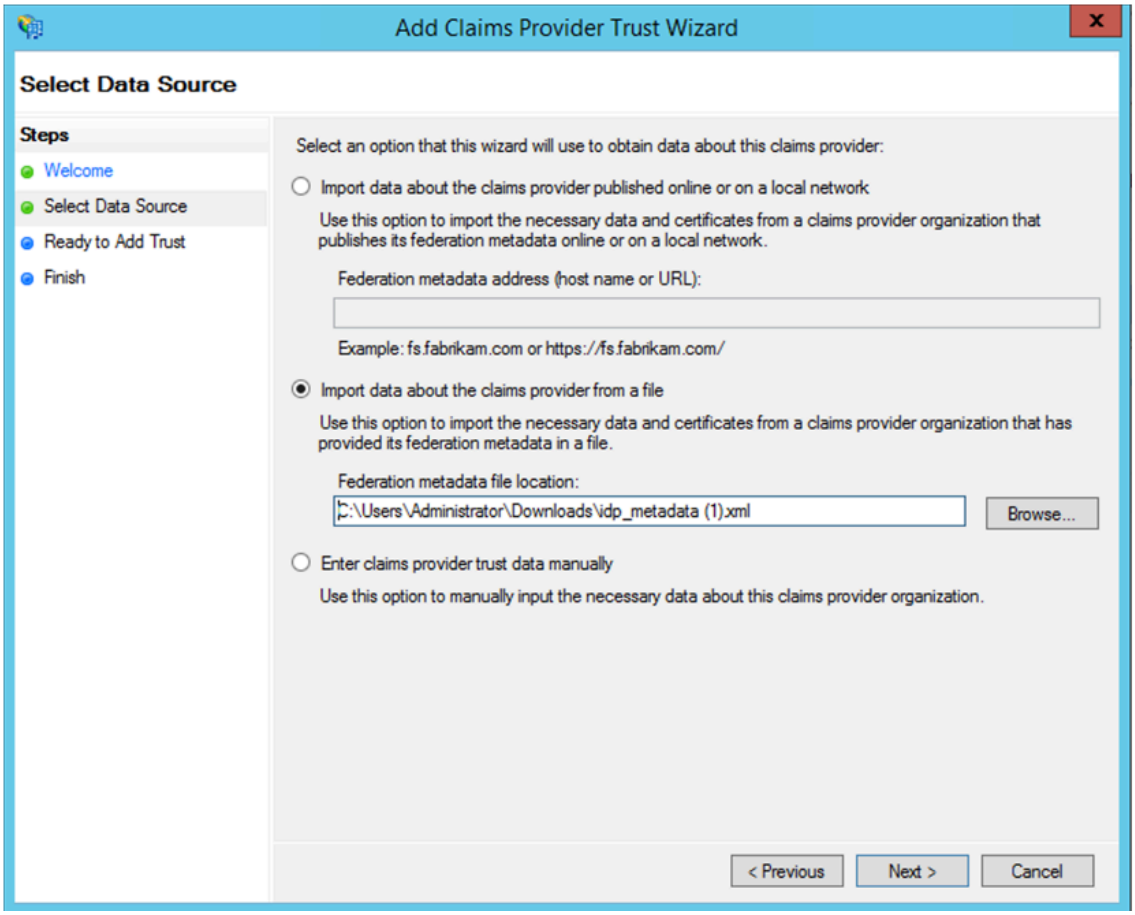
Agregue la confianza del proveedor de reclamos en ADFS

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**

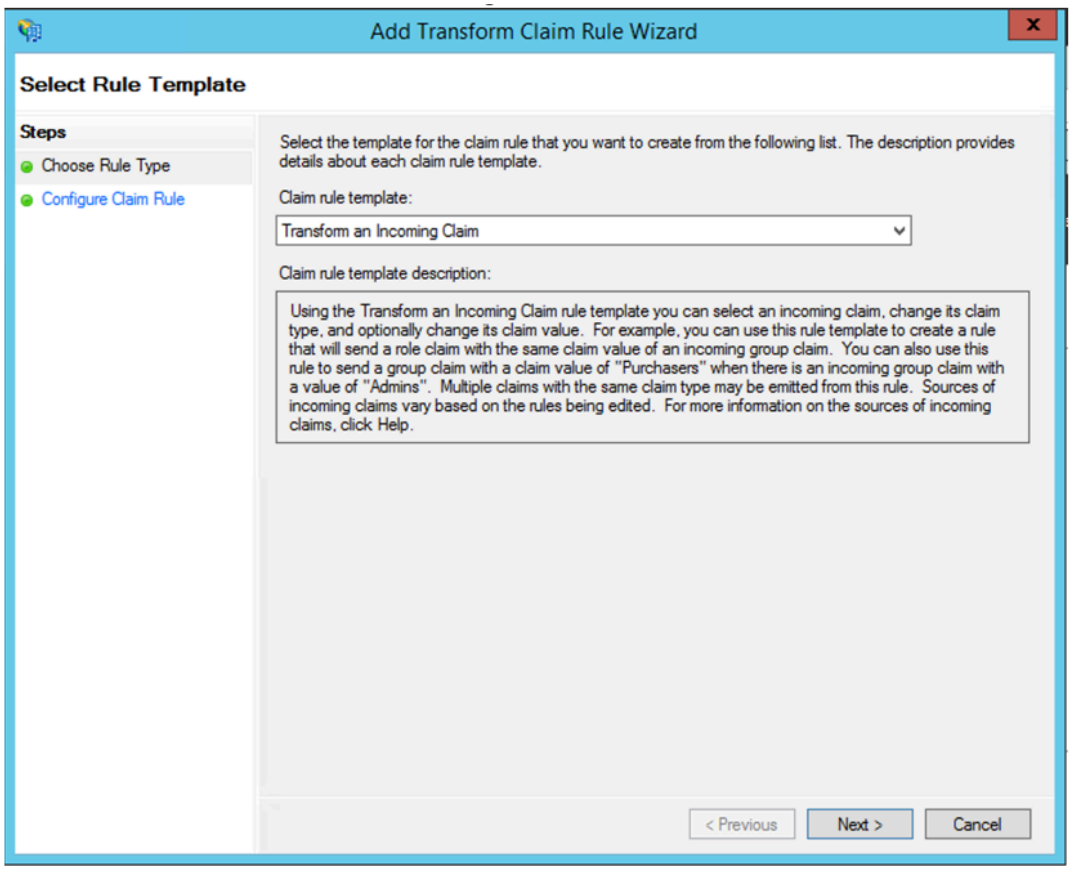


b) Agregue una aplicación en Secure Private Access que se utilice para federarse a ADFS. Para obtener más información, consulte Configuración de aplicaciones en Citrix Secure Private Access.

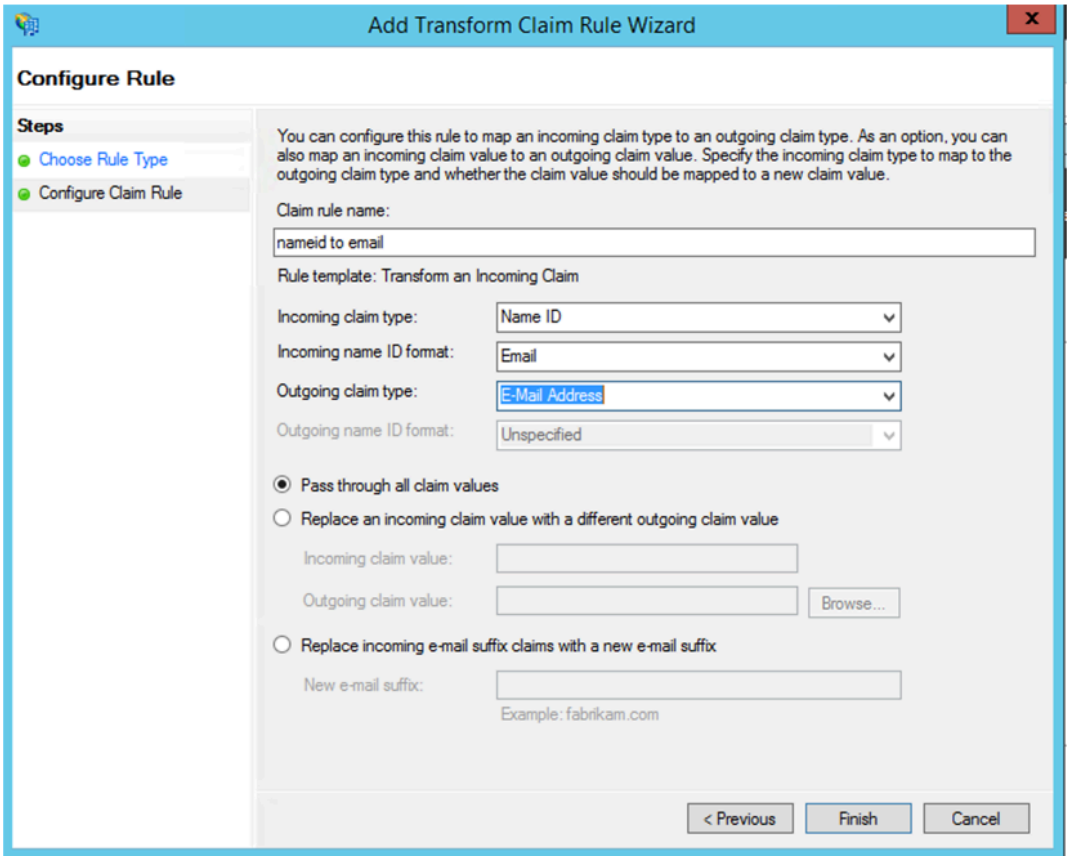
> **Nota:**
>
> Primero agregue la aplicación y, desde la sección de configuración de SSO de la aplicación, puede descargar el archivo de metadatos SAML y, a continuación, importar el archivo de metadatos en ADFS.



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**.



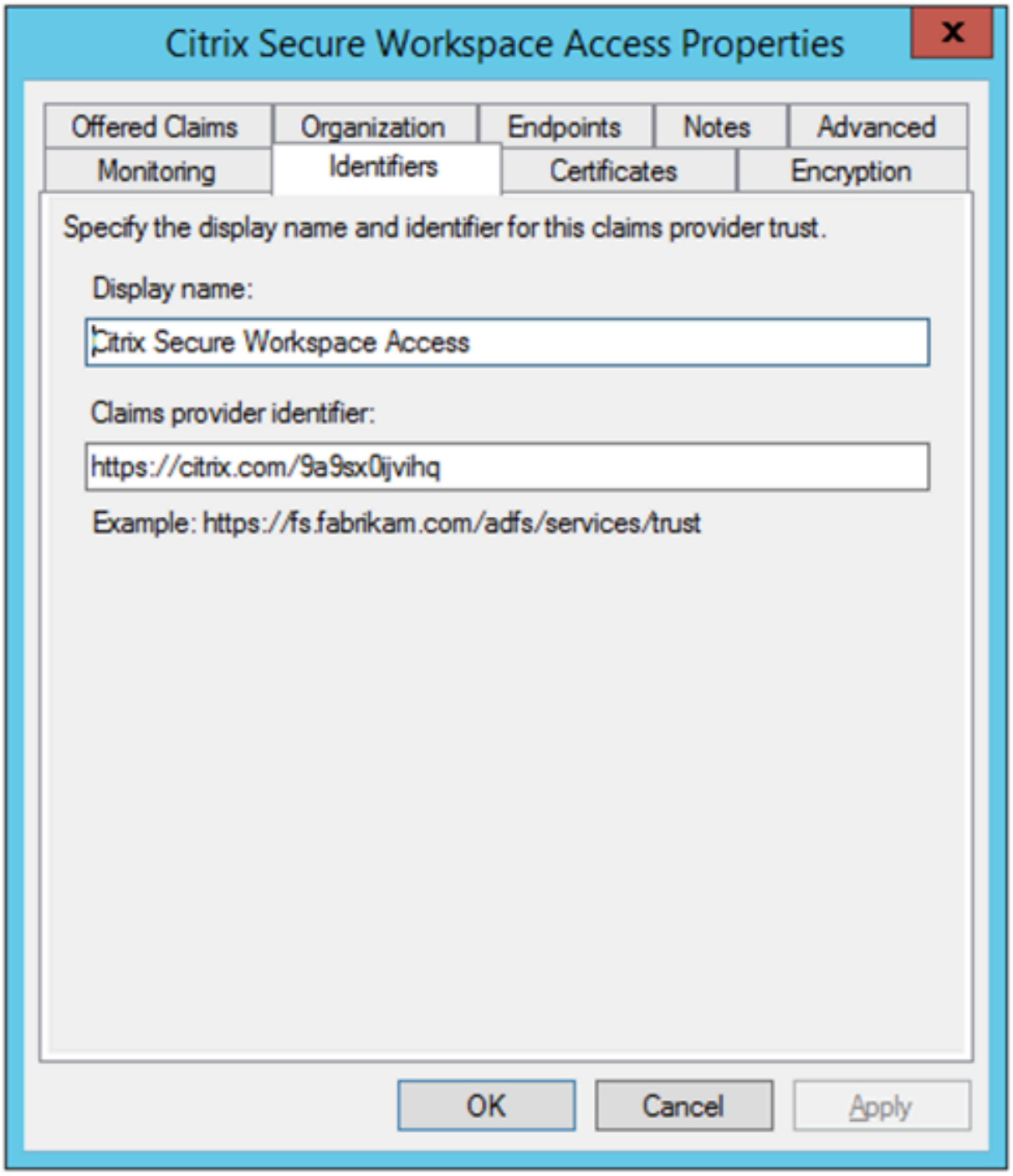
c) Complete los parámetros tal y como se muestra en la siguiente ilustración. Si su ADFS acepta otros reclamos, utilícelos y configure el SSO en Secure Private Access también en consecuencia.



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

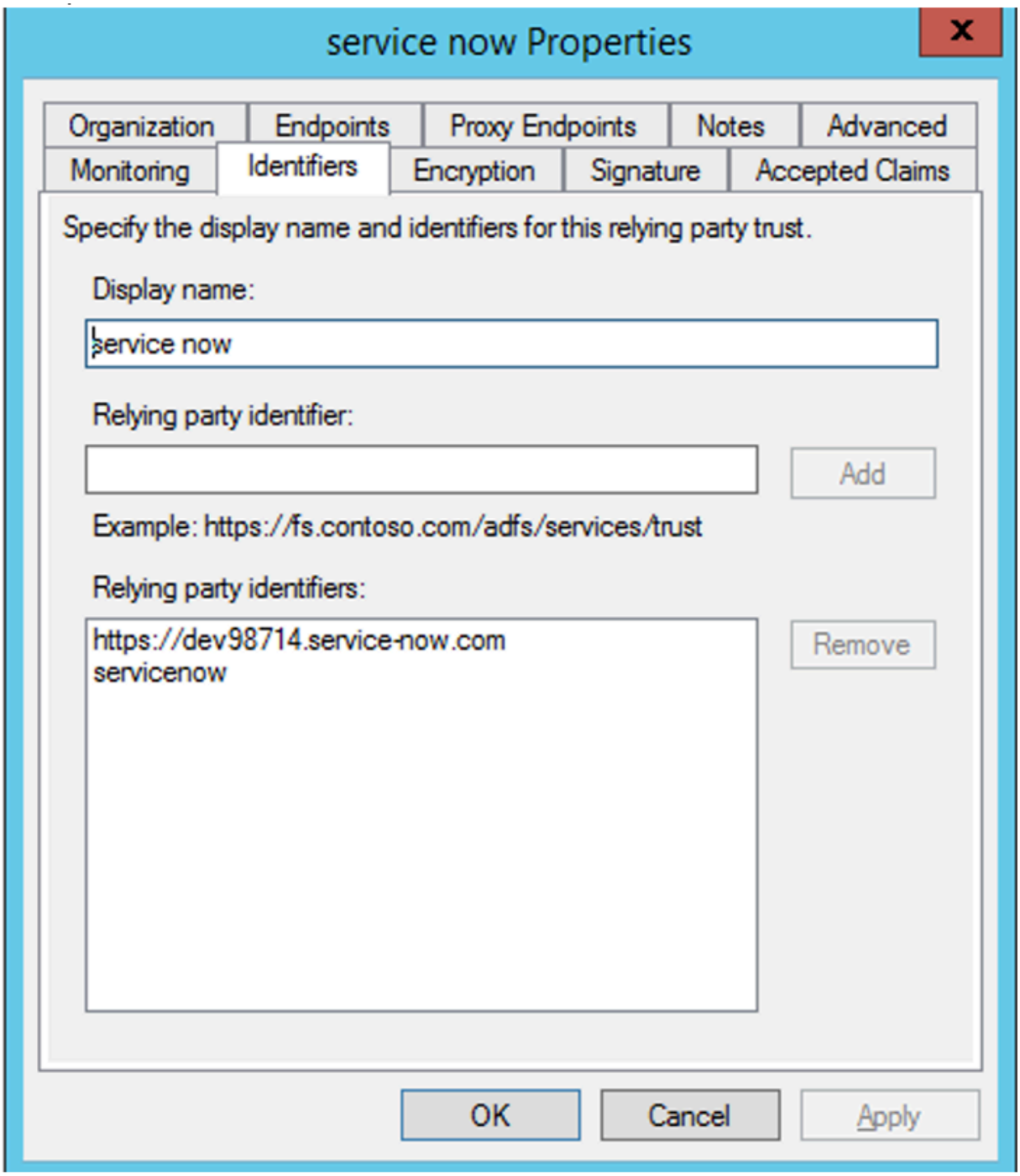
ID de confianza del proveedor de reclamaciones

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.

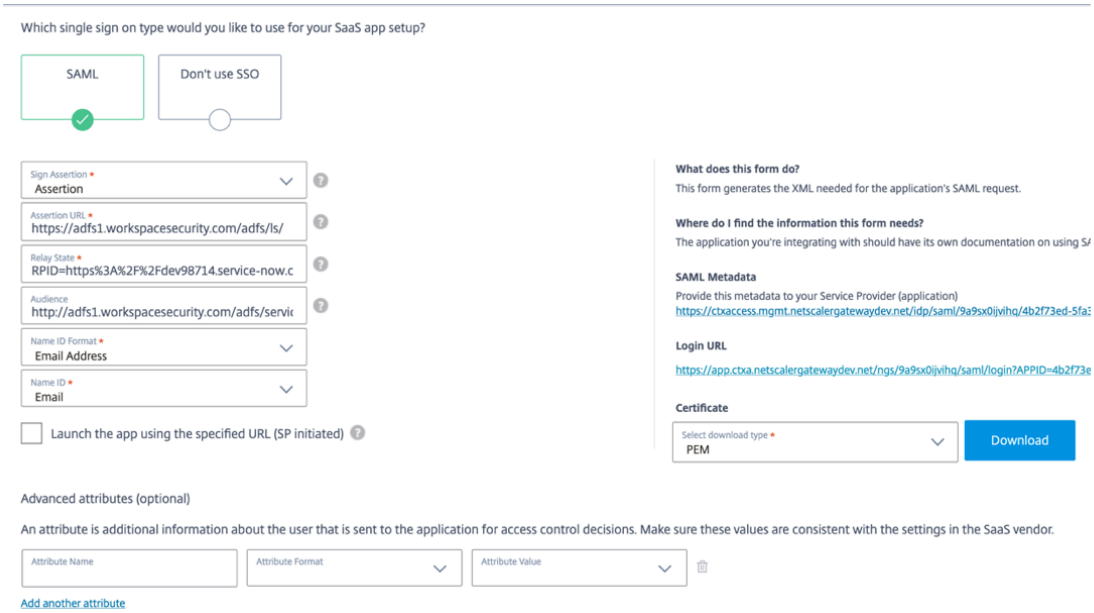
  Ejemplo: https://adfs1.workspacesecurity.com/adfs/ls/idpinitiatedsignon.aspx?LoginToRP=https%3A%2F%2Fdev98714.service-now.com&RedirectToIdentityProvider=https%3A%2F%2Fcitrix.com%2F9a9sx0ijvihq

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)**.

Funciones retiradas

August 26, 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.
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 medi-

ante 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.