Citrix Cloud

Contents

Citrix Cloud

July 2, 2024

> **Nota:**
>
> Citrix Virtual Apps Essentials y Citrix Virtual Desktops Essentials han llegado al fin de ventas y de vida. Para obtener más información, consulte CTX583004.

Citrix Cloud es una plataforma que aloja y administra servicios de la nube de Citrix. Conecta con sus recursos a través de conectores, en cualquier nube o infraestructura que usted elija (infraestructura local, nube pública, nube privada o nube híbrida). Le permite crear, administrar e implementar espacios de trabajo con aplicaciones y datos para usuarios finales, desde una única consola.

Novedades

Visite Citrix Cloud Updates para estar al día de funciones nuevas y futuras de Citrix Cloud y de estos servicios:

- Citrix Analytics
- Citrix DaaS
- Citrix Workspace

Probar Citrix Cloud

Pruebe un entorno de producción completo en una prueba de concepto de uno o varios de los servicios de Citrix Cloud. Después de registrarse en Citrix Cloud, puede solicitar pruebas de cada uno de los servicios desde la consola. Cuando finaliza la versión de prueba, puede convertirla directamente en un entorno de producción para conservar todas las configuraciones que haya aplicado durante la prueba. Para obtener más información, consulte Pruebas de servicio de Citrix Cloud.

Documentación de los servicios de Citrix Cloud

¿Busca información sobre la configuración o la administración de servicios de Citrix Cloud? Vaya a Citrix Cloud Services para ver enlaces a la documentación del producto de todos los servicios de la nube.

Recursos de arquitectura e implementación

Citrix Tech Zone contiene una gran cantidad de información para conocer más sobre Citrix Cloud y otros productos Citrix. Aquí encontrará arquitecturas de referencia, diagramas y documentos técnicos que contienen información sobre el diseño, la creación y la implementación de tecnologías Citrix.

Para obtener más información sobre los componentes principales de Citrix Cloud, consulte los siguientes recursos:

- Diagrama conceptual de Citrix Workspace: Proporciona una descripción general de áreas clave, como la identidad, las funciones inteligentes de los espacios de trabajo y Single Sign-On.
- Arquitecturas de referencia: Proporciona guías completas para planificar la implementación de Citrix Workspace, incluidos casos de uso, recomendaciones y recursos relacionados.
- Citrix DaaS reference architectures: Proporciona una guía exhaustiva para implementar Citrix DaaS (antes denominado Virtual Apps and Desktops Service) con servicios relacionados.

Recursos educativos

El portal de la serie Citrix Cloud Learning ofrece módulos educativos para ponerle al día de Citrix Cloud y sus servicios. Puede ver todos los módulos seguidos, desde las presentaciones generales hasta la planificación y creación de los servicios. Comience su viaje en la nube con los siguientes cursos:

- Fundamentals of Citrix Cloud
- Intro to Citrix Identity and Authentication
- Moving from StoreFront to Workspace

La biblioteca de vídeos de Citrix Education ofrece lecciones en vídeo en línea que le guiarán a través de las tareas clave de implementación y la solución de problemas de los componentes que utiliza con los servicios de Citrix Cloud. Obtenga más información sobre tareas, como la instalación de Cloud Connectors y el registro de agentes VDA, así como la solución de problemas con estos componentes.

Contrato de nivel de servicio

July 2, 2024

Fecha de entrada en vigor: 30 de octubre de 2020

Citrix Cloud ha sido diseñado teniendo en cuenta las prácticas recomendadas del sector con el fin de lograr un alto grado de disponibilidad de los servicios.

Este Contrato de nivel de servicio (SLA) describe el compromiso de Citrix con la disponibilidad de Citrix Cloud Service. Este SLA forma parte del contrato de usuario final (EULA o CLUF) de Cloud Software Group para los servicios que se cubren ("Servicios").

El compromiso de servicio de Citrix ("Compromiso de servicio") es mantener al menos un 99,9 % de tiempo de actividad mensual ("Tiempo de actividad mensual") en los Servicios. El Tiempo de actividad mensual se calcula restando del 100% el porcentaje de minutos en el que la instancia del Servicio se encontraba en estado "No disponible"durante un mes completo. Los servicios y la medida de disponibilidad para cada uno se establecen en la siguiente tabla. Los porcentajes de Tiempo de actividad mensual excluyen el tiempo de inactividad resultante de:

- Las ventanas de mantenimiento programadas regularmente.
- Casos en los que el cliente no cumple los requisitos de configuración del servicio documentados en https://docs.citrix.com, o casos de comportamientos abusivos o entradas defectuosas.
- Casos en los que el cliente ha ignorado los consejos de Citrix de modificar su uso del Servicio.
- A causa de un componente que no administre Citrix, incluidos, entre otros: máquinas físicas y virtuales que controle el cliente, sistemas operativos que controle y administre el cliente, equipos de red u otro hardware que instale y controle el cliente; parámetros de seguridad que defina y controle el cliente, directivas de grupo y otras directivas de configuración; fallos del proveedor de nube pública, fallos del proveedor de servicios de Internet u otros factores de asistencia al cliente externos al control de Citrix.
- Empleados, agentes, contratistas o proveedores del cliente, o cualquier persona que tenga acceso mediante contraseñas o equipos del cliente, o que de otro modo resulten del incumplimiento por parte del cliente de las prácticas de seguridad adecuadas.
- Los intentos del cliente de realizar operaciones que exceden los derechos del Servicio.
- La interrupción del servicio debida a causas de fuerza mayor, incluidos, entre otros, desastres naturales, guerras o actos de terrorismo o acciones gubernamentales.

No se ofrece ningún compromiso de servicio para ninguna prueba de Citrix, Tech Preview Labs o servicio Beta.

Citrix ofrece compromisos de servicio a los clientes que:

- Hayan comprado los servicios mediante una suscripción por períodos (de un período de suscripción mínimo de 1 año).
- Tengan al menos una suscripción de 100 unidades (1000 unidades como mínimo para los CSP) según el modelo de licencia aplicable al servicio durante el período de reclamación.

Los proveedores de servicios de Citrix (CSP) pueden participar desde el 1 de octubre de 2018.

Medidas de disponibilidad por servicio

Servicio	Medida para el tiempo de actividad mensual
Citrix Analytics for Performance	Tiempo que los usuarios pueden acceder y mejorar el rendimiento de aplicaciones y escritorios.
Citrix Analytics for Security	Tiempo que los usuarios pueden detectar y mitigar el acceso de los usuarios y los riesgos en la actividad.
Servicio NetScaler Console	Tiempo medio que el servicio está disponible en todos los puntos de presencia.
Citrix Endpoint Management	Los usuarios gestores de horas pueden acceder a sus aplicaciones móviles entregadas por Citrix y a los dispositivos inscritos a través del servicio.
Citrix Gateway Service para HDX Proxy	Los usuarios gestores de horas pueden acceder a su aplicación o sesión de escritorio a través del servicio.
NetScaler Intelligent Traffic Management	Tiempo durante el que los usuarios pueden acceder a la funcionalidad de administración de tráfico a través de consultas DNS o llamadas API HTTP
NetScaler SD-WAN Orchestrator	Los usuarios gestores de horas pueden acceder a su cuenta de SD-WAN Orchestrator y administrar su red de SD-WAN a través del servicio.
Citrix Secure Private Access	El tiempo durante el que los usuarios pueden acceder a su aplicación web interna o SaaS a través del servicio.
Citrix DaaS	Los usuarios gestores de horas pueden acceder a su aplicación o sesión de escritorio a través del servicio.
Citrix Workspace	Sucede igual que en el caso anterior para los servicios de componentes, pero incluye disponibilidad para cada uno. Los créditos pueden prorratearse si la notificación no está relacionada con todos los componentes.

> **Nota:**
>
> Citrix DaaS es el nuevo nombre de Citrix Virtual Apps Service, Citrix Virtual Desktops Service y Citrix Virtual Apps and Desktops Service.

Compromiso de servicio y compensaciones

En el caso de que Citrix no cumpla con el Compromiso de servicio en al menos 3 de cada 5 meses consecutivos en la Fecha de entrada en vigor de SLA o después de la misma, la compensación exclusiva consiste en un 10 % de crédito de servicio, con frecuencia mensual durante aquellos meses que Citrix no cumple el Compromiso de servicio, se aplica a la próxima extensión de servicio anual del cliente, durante el período de renovación inmediata para el mismo servicio y con la misma cantidad de unidades afectadas.

- Porcentaje mensual de tiempo de actividad: > 99,9%
- Crédito de servicio: 10% de descuento para los meses a los que se aplica (presentado al cliente en forma de vale)

Para recibir la compensación anterior, el cliente debe cumplir con los términos del Contrato de licencia del usuario final (EULA o CLUF) y debe informar del fallo en los treinta (30) días posteriores al último mes del período consecutivo de cinco meses para el que se presenta una solicitud de crédito. Para obtener instrucciones sobre posibles infracciones de este SLA, consulte CTX237141.

La solicitud debe identificar los servicios, definir las fechas, horas y duraciones de la indisponibilidad, junto con los registros de apoyo que corroboren la indisponibilidad, e identificar a los usuarios afectados y sus ubicaciones, así como cualquier asistencia técnica solicitada o implementación de correcciones. Solo se emitirá un crédito de servicio por cada servicio, para la cantidad correspondiente de meses, con un máximo de 10% de crédito de servicio para todos los meses de la extensión. El cliente debe presentar el vale al comprar la extensión.

Si compra la extensión a través de un revendedor, recibirá el crédito a través del revendedor. El crédito que aplicamos en caso de compra directa o que transferimos a su revendedor en caso de compra indirecta se basará en el precio recomendado y prorrateado de la extensión para el mismo número de unidades. Citrix no controla el precio de reventa ni los créditos de reventa. Los créditos no incluyen un derecho de compensación en los pagos debidos a Citrix o a un revendedor. Citrix actualizará estos términos ocasionalmente. Cuando se produzcan dichas actualizaciones, Citrix revisará también la fecha de publicación en la parte superior del Contrato de nivel de servicio. Todos los cambios se aplican solo a sus nuevas compras de servicios o extensiones de servicio a partir de la fecha de publicación actual.

Notificaciones de terceros

November 2, 2023

- Citrix Cloud - Avisos legales de terceros (PDF)
- Citrix Analytics Service - Avisos legales de terceros (PDF)

- Citrix DaaS Third Party Notifications (PDF)
- Citrix DaaS Standard for Azure Third Party Notifications (PDF)
- Remote Browser Isolation (antes denominado Secure Browser) (PDF)
- Citrix Endpoint Management - Avisos legales de terceros(PDF)
- Citrix Cloud Linux VDA Image Service - Avisos legales de terceros (PDF)
- Connector Appliance para Cloud Services - Avisos legales de terceros (PDF)
- Citrix Gateway Service - Avisos legales de terceros (PDF)
- Servicio de posición de dispositivos de Citrix - Avisos legales de terceros (PDF)

> **Nota:**
>
> Citrix DaaS se llamaba Citrix Virtual Apps and Desktops Service. Citrix DaaS Standard para Azure se llamaba Citrix Virtual Apps and Desktops Standard para Azure.

Cómo obtener ayuda y asistencia técnica

July 2, 2024

Este artículo describe cómo solucionar problemas y obtener ayuda si tiene problemas al crear una cuenta o iniciar sesión en Citrix Cloud u otro sitio web de Citrix. Este artículo también incluye otros recursos de autoayuda y opciones de asistencia guiada.

> **Importante:**
>
> Si tiene algún problema al iniciar sesión en el sitio web de Citrix o al inscribirse en la autenticación de varios factores (MFA), consulte primero este artículo para obtener recursos de solución de problemas. Si estos recursos no le ayudan a resolver el problema, contacte con el Servicio de atención al cliente de Citrix en https://www.citrix.com/contact/customer-service.html.

Crear una cuenta

Se necesita una cuenta de Citrix para acceder a ciertos recursos del sitio web de Citrix, como los foros de debate de Citrix, los cursos de formación, determinadas descargas de productos y la asistencia técnica de Citrix.

Para crear una cuenta de Citrix para su empresa, contacte con Citrix mediante uno de estos métodos:

- Ponerse en contacto con el Servicio de atención al cliente de Citrix.
- Contacte con un Citrix Partner o un agente de Ventas de Citrix de su zona.

Si ya tiene una cuenta de Citrix, puede crear una cuenta de Citrix Cloud y completar el proceso de incorporación tras realizar las tareas descritas en Crear una cuenta de Citrix Cloud.

Si tiene algún problema al registrarse en Citrix Cloud, contacte con el Servicio de atención al cliente de Citrix.

Iniciar en sitios web de Citrix y Citrix Cloud

Si tiene problemas para iniciar sesión en un sitio web de Citrix con su cuenta de Citrix, utilice estos recursos para solucionarlos:

- CTX228792: Troubleshooting login issues on Citrix websites
- CTX283814: Problema de inicio de sesión después de configurar la cuenta de Citrix

No puedo configurar MFA o no puedo autenticarme con MFA al iniciar sesión en mi cuenta de Citrix

Consulte estos artículos para obtener información sobre cómo solucionar problemas:

- CTX461297: Cómo inscribirse en la autenticación de varios factores (MFA)
- CTX463758: Cómo recuperar el acceso a su cuenta

Si sigue sin poder iniciar sesión con MFA, contacte con el Servicio de atención al cliente de Citrix en https://www.citrix.com/contact/customer-service.html.

¿Dónde está el nombre de usuario de mi cuenta de Citrix o cómo restablezco mi contraseña de Citrix?

Siga estos pasos para verificar el nombre de usuario de su cuenta de Citrix y restablecer la contraseña.

1. Vaya a https://www.citrix.com/welcome/request-password.html.
2. Para verificar el nombre de usuario de su cuenta de Citrix:
    a) En **Find my account by**, seleccione **Email**.
    b) Introduzca la dirección de correo electrónico asociada a su cuenta de Citrix.
3. Para restablecer la contraseña de su cuenta de Citrix:
    a) En **Find my account by**, seleccione **User name**.
    b) Introduzca el nombre de usuario de su cuenta de Citrix.
4. Haga clic en **Find my account**.

Si Citrix encuentra su cuenta con su dirección de correo electrónico, Citrix le envía un correo electrónico con los nombres de usuario y de empresa asociados a su dirección de correo electrónico. Si Citrix encuentra su cuenta con su nombre de usuario de Citrix, Citrix le envía un correo electrónico con instrucciones para restablecer la contraseña.

Si no recibe ningún correo electrónico transcurridos unos minutos, consulte No veo correos de Citrix en mi bandeja de entrada en este artículo.

No puedo iniciar sesión en Citrix Cloud

- Asegúrese de iniciar sesión con las credenciales de cuenta correctas. Para verificar el nombre de usuario de su cuenta, vaya a https://citrix.cloud.com/ y seleccione **¿Ha olvidado su nombre de usuario?** e introduzca su dirección de correo electrónico. Citrix le envía un correo electrónico con el nombre de usuario de su cuenta.
- Es posible que deba restablecer la contraseña. Citrix Cloud le pide que cambie la contraseña si no inició sesión recientemente o si la contraseña no es lo suficientemente segura. Para obtener más información, consulte Cambiar la contraseña en este artículo.
- Es posible que deba iniciar sesión con una URL de inicio de sesión personalizada. Si su cuenta de Citrix Cloud usa Azure AD, Google Cloud Identity o SAML para autenticar a administradores, seleccione **Sign in with my company credentials** e introduzca la URL de inicio de sesión de su empresa. Después, introduzca sus credenciales de empresa para acceder a la cuenta de Citrix Cloud de su empresa. Si no conoce la URL de inicio de sesión de su empresa, póngase en contacto con el administrador de su empresa para obtener ayuda.

Si sigue sin poder iniciar sesión en Citrix Cloud, contacte con el Servicio de atención al cliente de Citrix.

No veo correos de Citrix en mi bandeja de entrada

Cuando Citrix le envía correos para verificar su identidad para MFA, al buscar su cuenta de Citrix o cambiar su contraseña, el correo suele llegar poco después. Si no recibe estos correos:

- Compruebe la dirección de correo electrónico que está registrada para su cuenta de Citrix y compruebe que es correcta. Si cambió recientemente su dirección de correo electrónico, es posible que el correo de verificación se envíe a su antigua dirección.
- Es posible que el correo electrónico se haya filtrado por accidente. Revise las carpetas de correo no deseado y de la papelera de su cliente de correo electrónico. También puede buscar en su cuenta de correo electrónico los correos electrónicos de `donotreplynotifications@citrix.com` o `cloud@citrix.com`.

- Es posible que el firewall haya bloqueado el correo electrónico. Asegúrese de que estas direcciones aparezcan como remitentes de confianza:
  - `donotreplynotifications@citrix.com`
  - `cloud@citrix.com`
  - `CustomerService@citrix.com`

Si no recibe el correo electrónico después de varios minutos o tiene otro problema al iniciar sesión, contacte con el Servicio de atención al cliente de Citrix.

Autenticación de varios factores para cuentas de Citrix y Citrix Cloud

Los clientes de Citrix deben iniciar sesión en su cuenta de Citrix y en Citrix Cloud mediante MFA. La inscripción en MFA se produce cuando:

- Un cliente nuevo inicia sesión en su cuenta de Citrix por primera vez.
- Un cliente de Citrix incorpora una nueva cuenta de Citrix Cloud, pero esta aún no se ha inscrito en MFA.
- Un nuevo administrador se une a una cuenta de Citrix Cloud existente.

Si se le pide que se inscriba en MFA al iniciar sesión en su cuenta de Citrix o Citrix Cloud, siga los pasos que se indican en CTX461297: How to Enroll into Multi Factor Authentication (MFA).

Para obtener más información sobre MFA para cuentas de Citrix, consulte CTX463482: Frequently asked questions when setting up Multi-Factor Authentication (MFA) on Citrix properties.

Recuperación de cuentas

Si necesita ayuda para recuperar las credenciales de su cuenta de Citrix, consulte ¿Dónde está el nombre de usuario de mi cuenta de Citrix o cómo restablezco mi contraseña de Citrix? en este artículo.

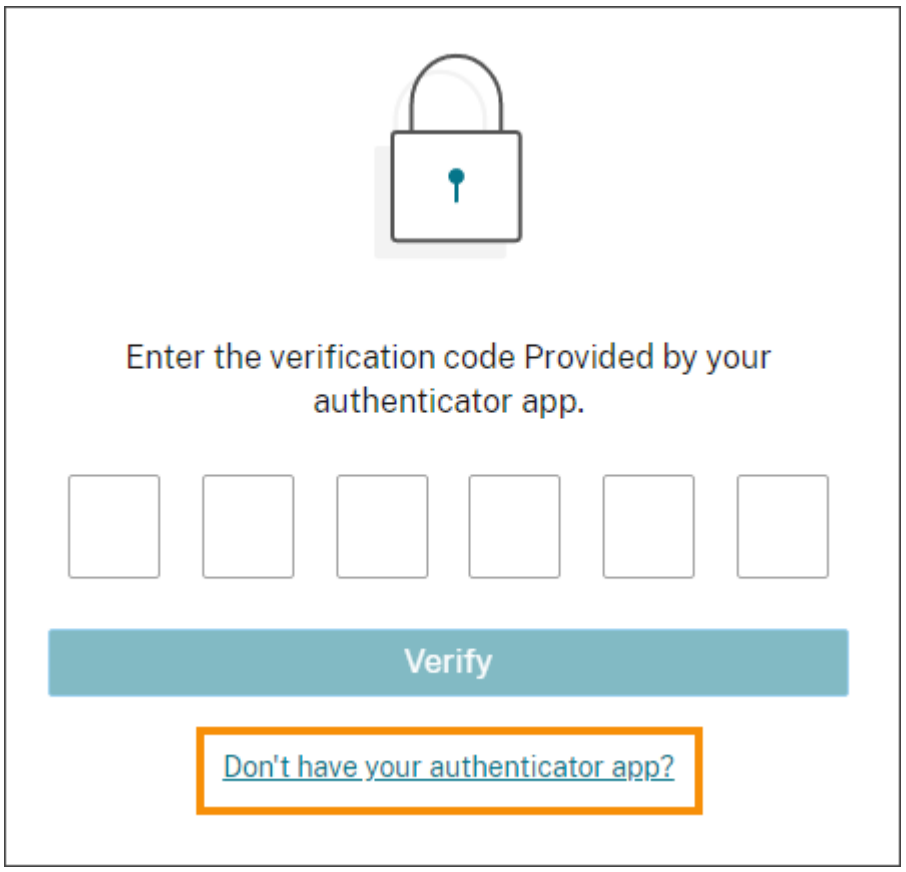
Si necesita ayuda para recuperar el acceso a su cuenta de Citrix Cloud, puede usar los métodos de recuperación que configuró al inscribirse en MFA. Estos métodos de recuperación incluyen:

- Un código de un solo uso que Citrix envía a su dirección de correo electrónico de recuperación.
- Un código de reserva de la lista generada durante la inscripción en MFA.
- Una llamada telefónica de Citrix Support a su número de teléfono de recuperación para verificar su identidad y ayudarle a acceder a su cuenta. Es necesario configurar un número de teléfono de recuperación durante la inscripción en MFA.

Para iniciar sesión con un método de recuperación:

1. En la página de inicio de sesión de la cuenta de Citrix o de Citrix Cloud, introduzca su nombre de usuario y su contraseña y, a continuación, seleccione **Iniciar sesión**.

2. Cuando se le solicite el código de su método de MFA principal, seleccione **Usar un método de recuperación**.



3. Seleccione el método de recuperación que quiera usar, si corresponde. Si solo tiene configurado un método de recuperación, además de un número de teléfono de recuperación, Citrix le pedirá que utilice ese método automáticamente.
4. Si usa su dirección de correo electrónico de recuperación, introduzca el código de un solo uso que envía Citrix y seleccione **Verificar**. Si no recibe el código pasado un tiempo, seleccione **Reenviar correo**. Tras la verificación, consigue iniciar sesión en Citrix Cloud.
5. Si usa un código de reserva, introdúzcalo cuando se le solicite y seleccione **Verificar y continuar**. Inicia sesión en Citrix Cloud y recibirá un correo electrónico para notificarle que se utilizó un código de reserva y la cantidad de códigos de reserva válidos que le quedan. Anote o elimine el código de reserva usado para asegurarse de no usarlo de nuevo.
6. Si no puede usar la dirección de correo de recuperación o los códigos de reserva:

    a) Seleccione **Contactar con Citrix Support**.
    b) Complete el formulario con los detalles de su problema. Un representante de Citrix Support le contactará mediante su número de teléfono de recuperación para verificar su identidad. Después, el representante le enviará un código de recuperación que puede usar

para iniciar sesión.

c) Regrese a la página de inicio de sesión de Citrix Cloud e inicie sesión con sus credenciales de Citrix Cloud.
d) Cuando se le solicite un código, introduzca el código de recuperación que recibió de Citrix Support y seleccione **Verificar**.

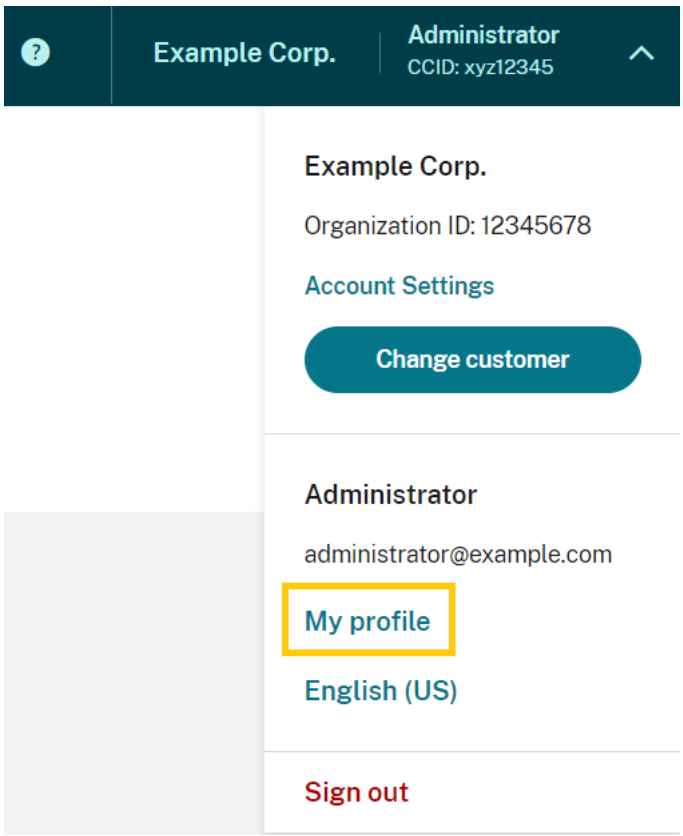
Después de iniciar sesión, asegúrese de actualizar los métodos de recuperación de la cuenta para evitar futuras demoras en el inicio de sesión.

Actualizar los parámetros de MFA

Puede actualizar los parámetros de acceso y recuperación de MFA a través de la página **Mis parámetros**. Puede acceder a esta página a través de su cuenta de Citrix o de Citrix Cloud.

Para acceder a la página **Mis parámetros**:

1. Inicie sesión en su cuenta de Citrix o en Citrix Cloud.
2. Desde su cuenta de Citrix, visite https://accounts.cloud.com/core/profile.
3. En Citrix Cloud, seleccione **Mis parámetros** en el menú superior derecho.



Para cambiar los parámetros de MFA, consulte estas secciones:

- Administrar el método de autenticación MFA principal
- Administrar los métodos de recuperación de la autenticación MFA

Cambiar la contraseña

Si olvidó la contraseña de su cuenta, seleccione **¿Olvidó la contraseña?** e introduzca el nombre de usuario de su cuenta cuando se le solicite. Citrix envía un correo electrónico a la dirección de correo electrónico de su cuenta con un enlace para configurar una nueva contraseña. Si no recibe este correo electrónico después de varios minutos o si necesita más ayuda, contacte con el Servicio de atención al cliente de Citrix.

Es posible que Citrix Cloud le pida que restablezca la contraseña cuando intente iniciar sesión. Este mensaje se produce si:

- Su contraseña no cumple los requisitos de complejidad de Citrix Cloud.
- Su contraseña incluye palabras del diccionario.
- Su contraseña aparece en una base de datos conocida de contraseñas desveladas.
- No ha iniciado sesión en Citrix Cloud en los últimos 60 días.

Las contraseñas deben tener entre 8 y 128 caracteres e incluir lo siguiente:

- Al menos un número
- Al menos una letra mayúscula
- Al menos un símbolo: ! @ # $ % ^ * ? + = -

Cuando se le solicite, seleccione **Restablecer contraseña** para crear una nueva contraseña segura para su cuenta.

Estado del servicio de Cloud

El panel de estado de Citrix Cloud (https://status.cloud.com) proporciona una visión general de la disponibilidad en tiempo real de la plataforma y los servicios de Citrix Cloud en cada región geográfica. Si experimenta algún problema con Citrix Cloud, consulte el panel de estado de Cloud para verificar que Citrix Cloud o servicios específicos funcionan normalmente.

Para obtener más información sobre el panel de mandos de estado de Cloud, consulte Estado del servicio.

Foros de asistencia de Citrix Cloud

En los Foros de asistencia de Citrix Cloud puede obtener ayuda, publicar comentarios y sugerencias de mejoras, ver conversaciones de otros usuarios o iniciar nuevas conversaciones con sus propios temas.

Los miembros del personal de asistencia de Citrix realizan un seguimiento de estos foros y pueden responder a sus preguntas. Otros miembros de la comunidad de Citrix Cloud también pueden ofrecer ayuda o unirse al debate.

No es necesario iniciar sesión para poder leer las cuestiones del foro. Sin embargo, debe iniciar sesión para publicar un tema o responder en un tema. Para iniciar sesión, use las credenciales existentes de su cuenta de Citrix o use la dirección de correo electrónico y la contraseña que proporcionó al crear la cuenta de Citrix Cloud.

Artículos y documentación de asistencia

Citrix ofrece mucho contenido sobre productos y de asistencia para ayudarle a sacar el máximo partido de Citrix Cloud y resolver problemas que pueda encontrar al usar los productos Citrix.

Citrix Support Knowledge Center

El Knowledge Center proporciona contenido para la solución de problemas, así como boletines de seguridad y avisos de actualización de software para todos los productos de Citrix. Solo necesita introducir una cadena de búsqueda para buscar el contenido relevante. Puede filtrar los resultados según el producto y el tipo de artículo.

Citrix Tech Zone

Citrix Tech Zone contiene información para conocer más sobre Citrix Cloud y otros productos Citrix. Aquí puede encontrar arquitecturas de referencia, diagramas, vídeos y documentos técnicos que contienen información sobre el diseño, la creación y la implementación de tecnologías Citrix.

Centro de ayuda para usuarios

El Centro de ayuda para usuarios de Citrix proporciona documentación de productos Citrix específica para los usuarios finales de su organización. El Centro de ayuda para el usuario proporciona instrucciones en un formato fácil de leer sobre los productos orientados al usuario final, como la aplicación Citrix Workspace y Citrix SSO. Para obtener documentación para usuarios finales sobre ShareFile, consulte Aplicaciones de Citrix Files en el sitio web de la documentación de producto de ShareFile.

Asistencia técnica

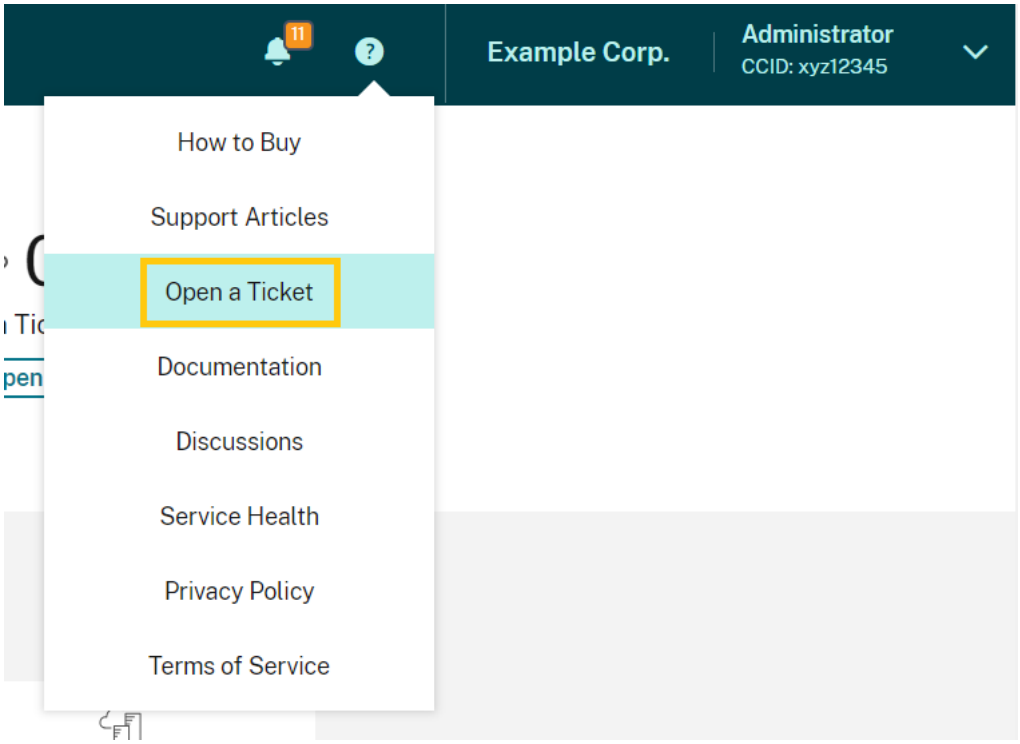
Si experimenta un problema que requiere asistencia técnica, puede acceder al portal My Support para abrir un caso o hablar con un representante de asistencia técnica de Citrix.

Para acceder al portal My Support, visite https://support.citrix.com/case/manage.

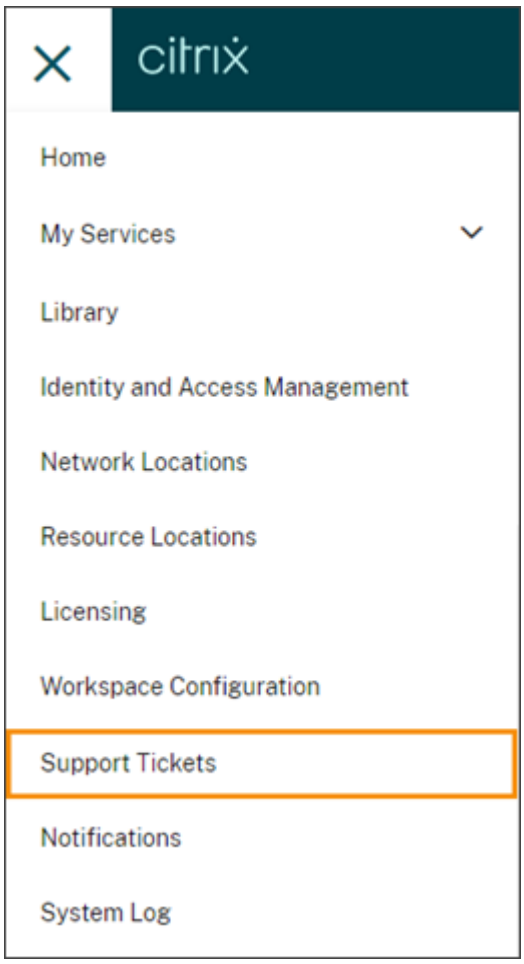
Para acceder al portal desde Citrix Cloud, debe tener el permiso de **Tíquets de asistencia**. Para obtener más información sobre los permisos de administrador, consulte Modificar permisos de administrador.

Desde la consola de administración de Citrix Cloud, puede acceder a My Support de estas maneras:

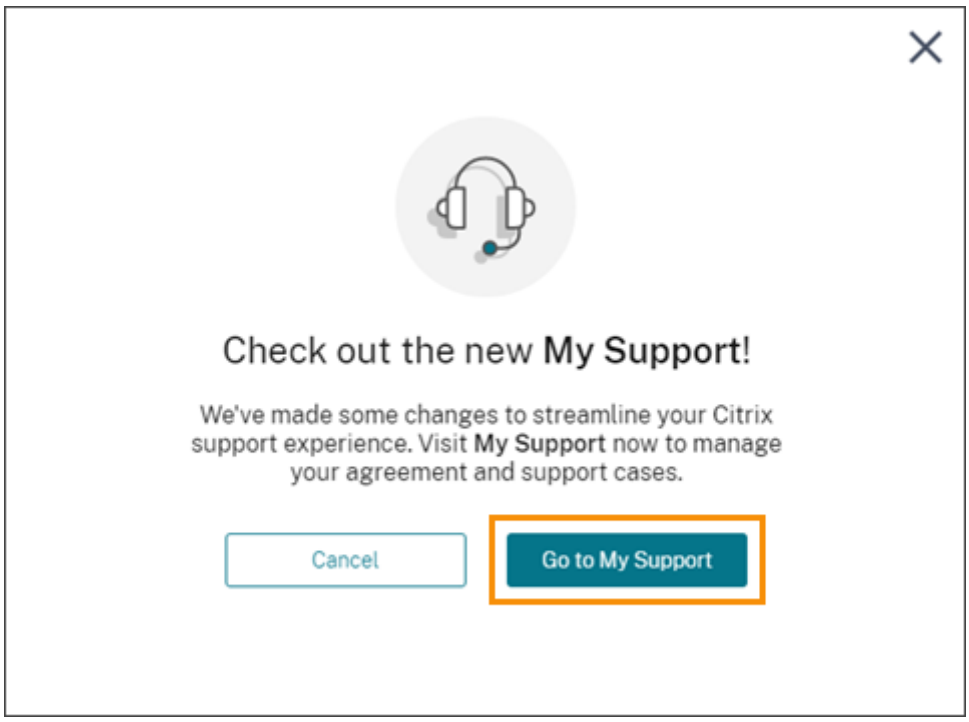
- En el icono de **Ayuda** situado en la parte superior derecha de la pantalla, seleccione **Abrir un tíquet**.



- En el menú de Citrix Cloud de la parte superior izquierda de la pantalla, seleccione **Tíquets de asistencia**.

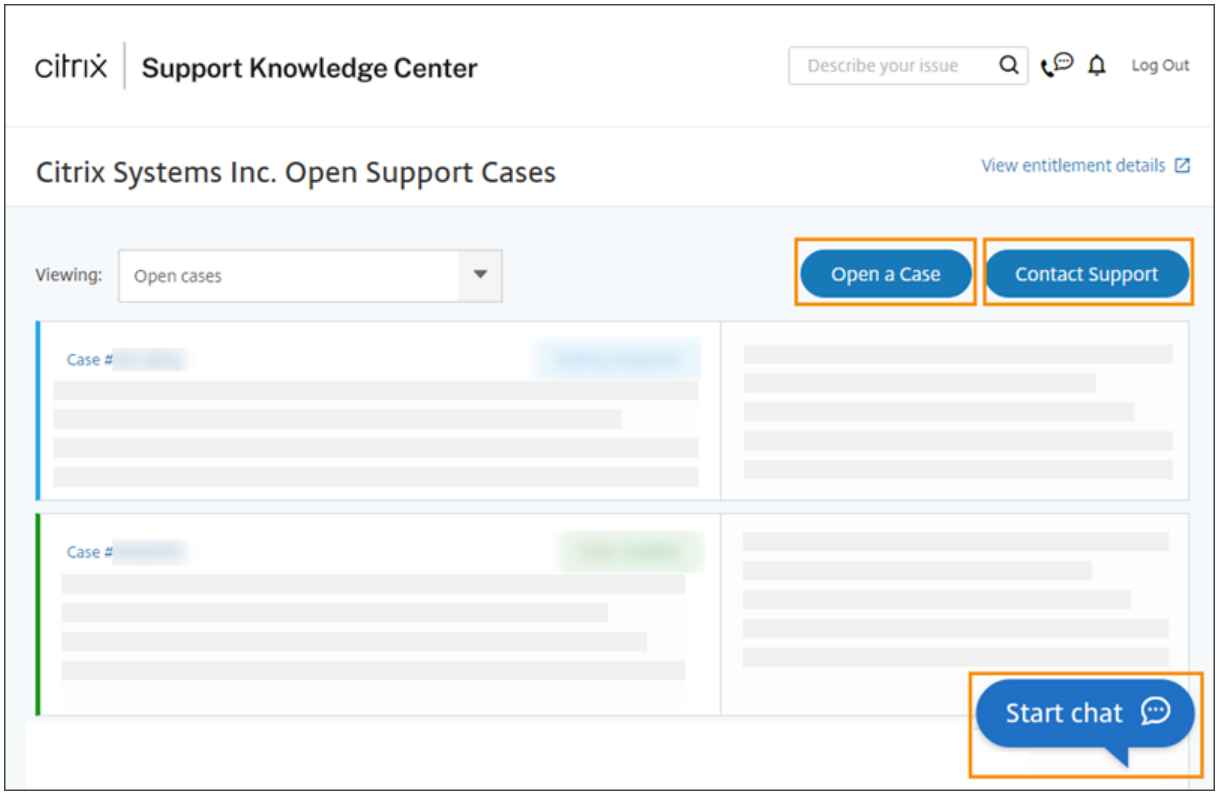


Después de seleccionar cualquiera de estas opciones, seleccione **Ir a My Support** y, a continuación, inicie sesión con las credenciales de su cuenta de Citrix.



Después de iniciar sesión, póngase en contacto con la asistencia técnica de Citrix mediante uno de los métodos siguientes:

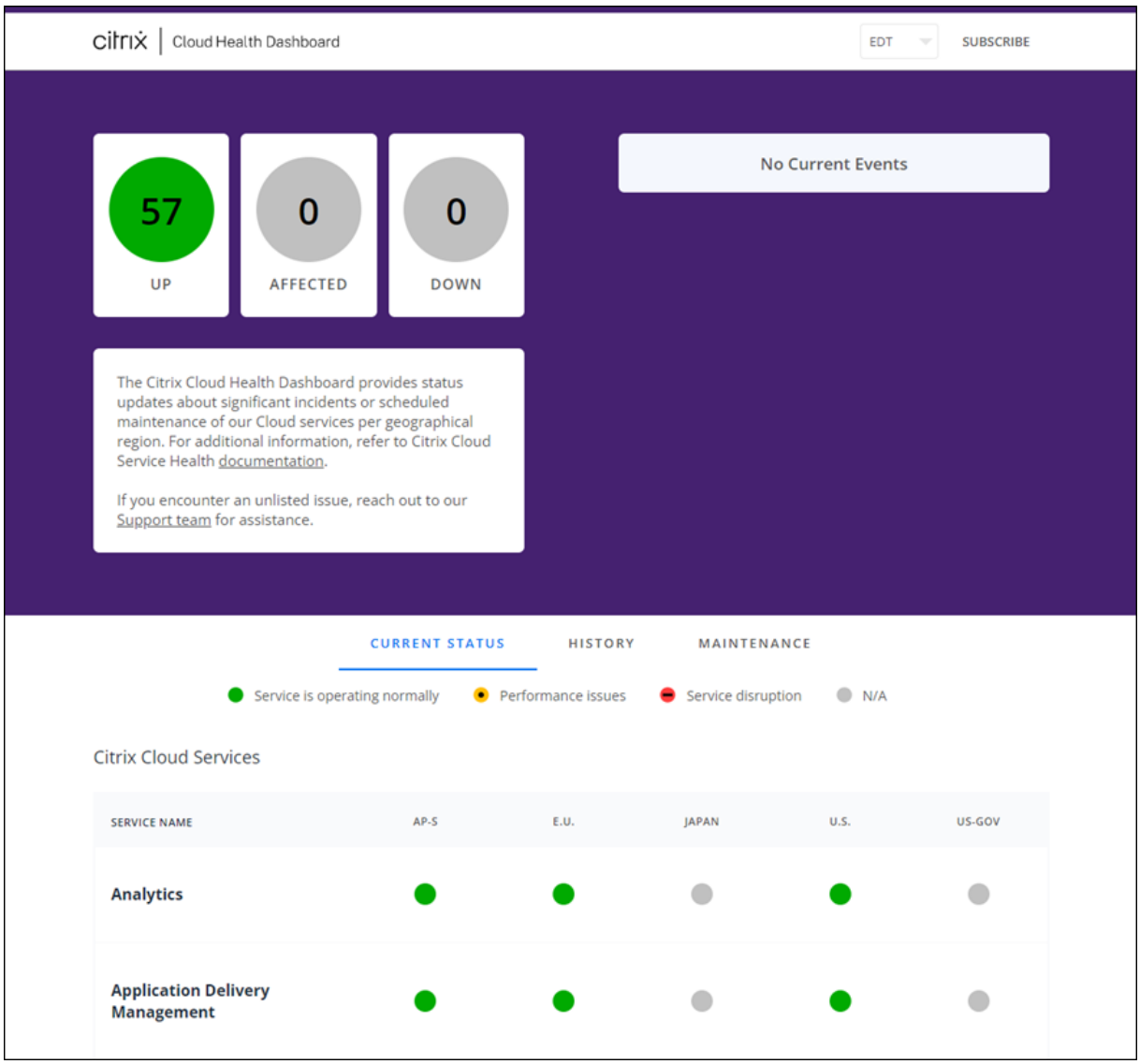
- Iniciar un caso de asistencia técnica: Seleccione **Abrir un caso** y proporcione los detalles del problema.
- Por teléfono: Seleccione **Llame a Soporte técnico** para ver una lista de números de teléfono locales con los que ponerse en contacto con la asistencia técnica de Citrix.
- Chat en directo: Seleccione **Iniciar un chat** en la esquina inferior derecha de la página para conversar con un representante de asistencia técnica de Citrix.



Estado del servicio de Citrix Cloud

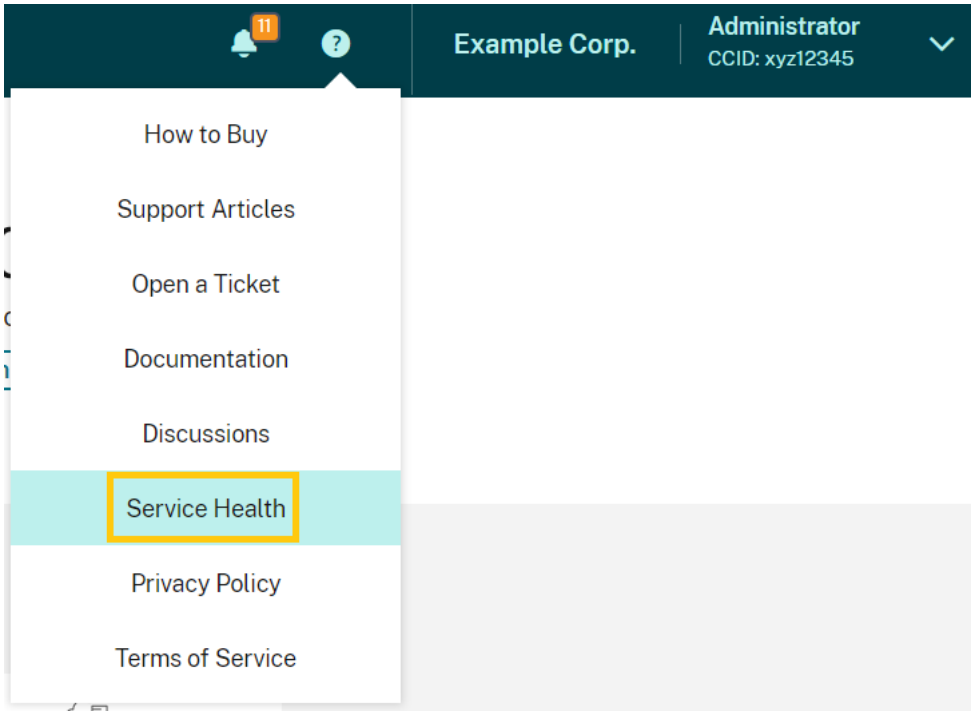
November 27, 2023

El panel de estado de Citrix Cloud proporciona una visión general de la disponibilidad en tiempo real de la plataforma y los servicios de Citrix Cloud en cada región geográfica. Si experimenta algún problema con Citrix Cloud, consulte el panel de estado de Cloud para verificar que Citrix Cloud o servicios específicos funcionan normalmente.



Puede acceder al panel de estado de Cloud de estas maneras:

- Vaya a https://status.cloud.com desde su explorador web.
- Seleccione **Estado del servicio** en el menú Ayuda de Citrix Cloud.



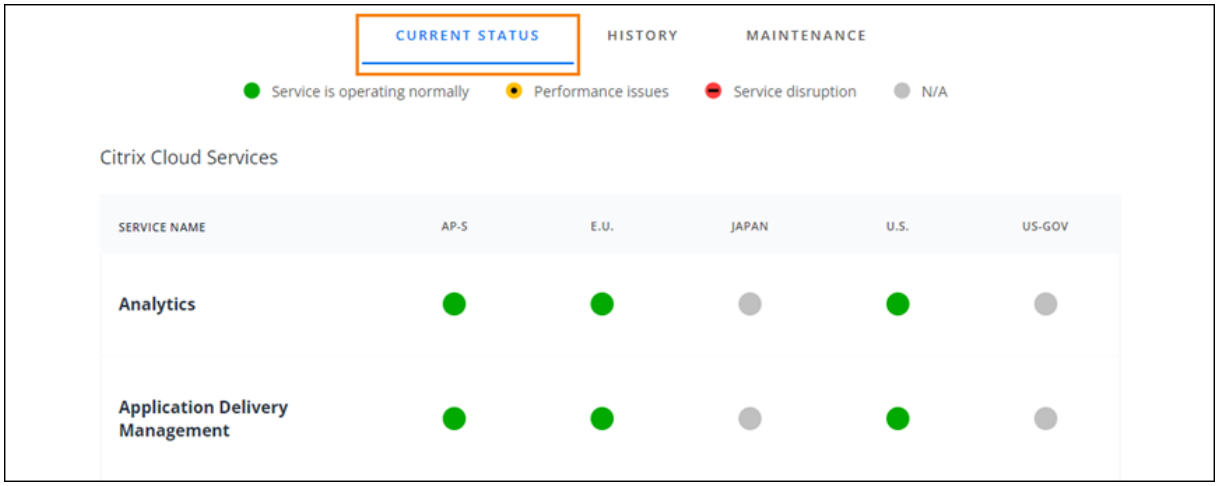
Utilice el panel para obtener más información sobre las siguientes condiciones:

- El estado actual de todos los servicios de Citrix Cloud, agrupados por región geográfica
- Historial de estado de cada servicio durante los últimos siete días
- Períodos de mantenimiento para servicios específicos

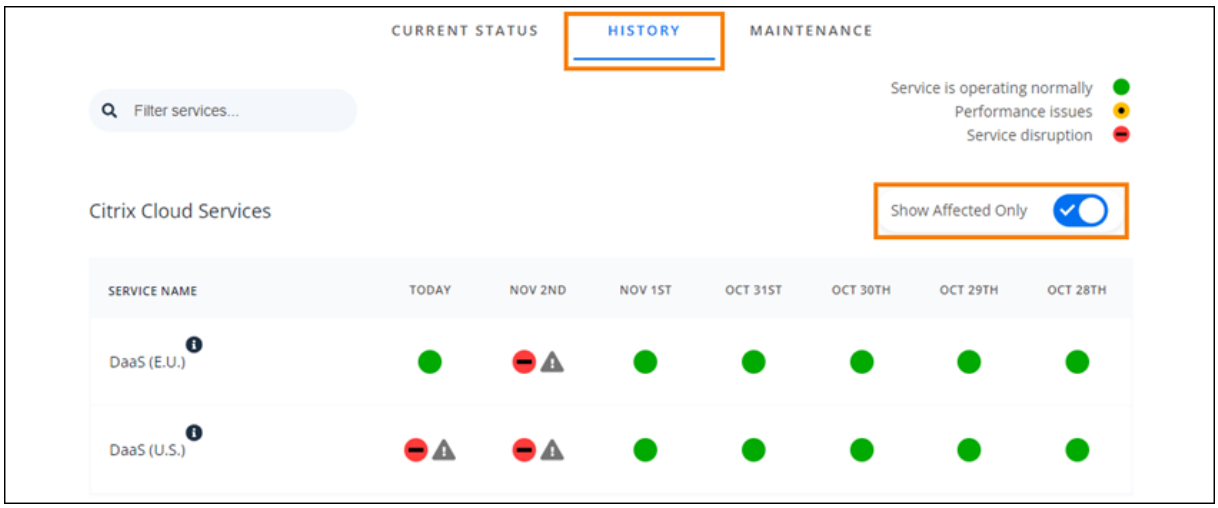
También puede suscribirse a notificaciones sobre eventos como períodos de mantenimiento e incidentes de servicio.

Ver estado y condiciones de mantenimiento

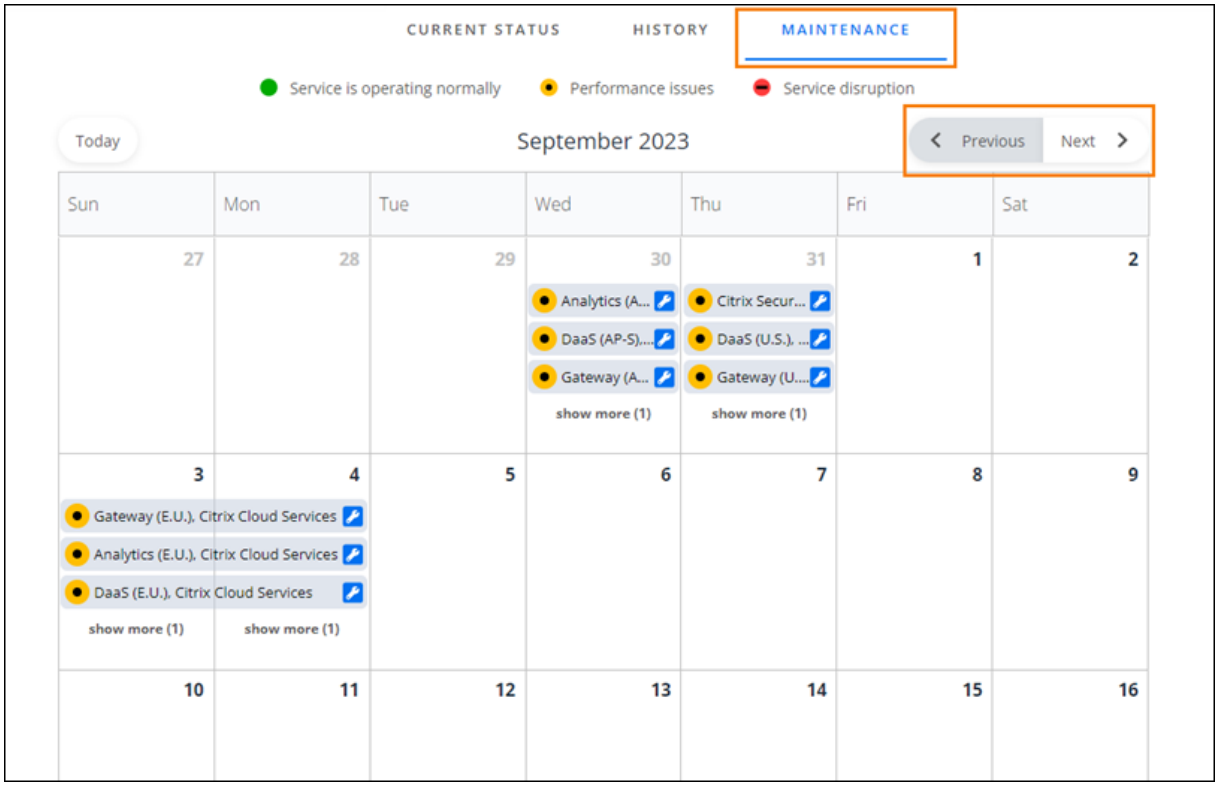
Seleccione **Current Status** para mostrar el estado actual de todos los servicios y componentes de plataforma de Citrix Cloud en cada región geográfica.



Seleccione **Historial** para mostrar el estado de todos los servicios y componentes de plataforma de Citrix Cloud durante los últimos siete días. Seleccione **Show Affected Only** para mostrar solo los servicios que han tenido eventos de mantenimiento relativos a su estado en los últimos siete días.



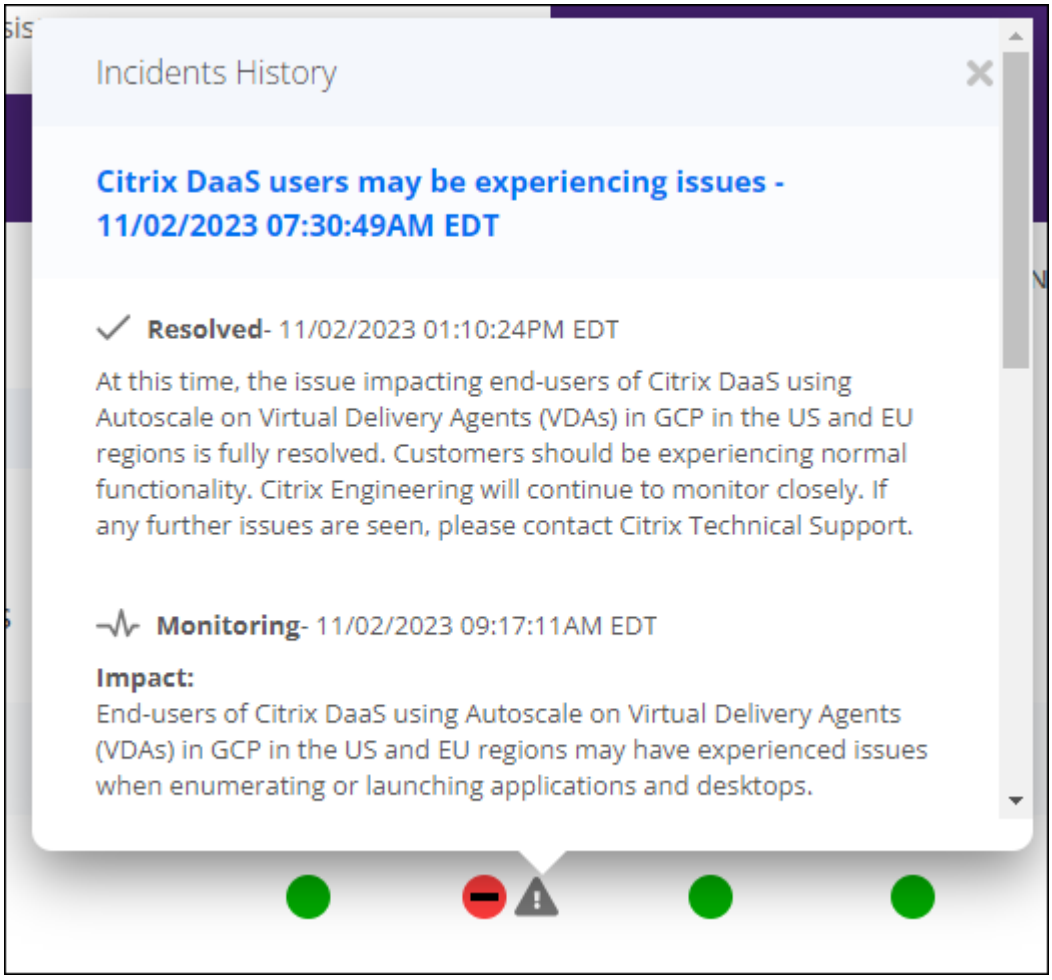
Seleccione **Mantenimiento** para mostrar una vista de calendario de las ventanas de mantenimiento de servicio. Seleccione **Siguiente** para ver eventos de mantenimiento programados para los próximos meses. Seleccione **Anterior** para volver a los eventos del mes actual.



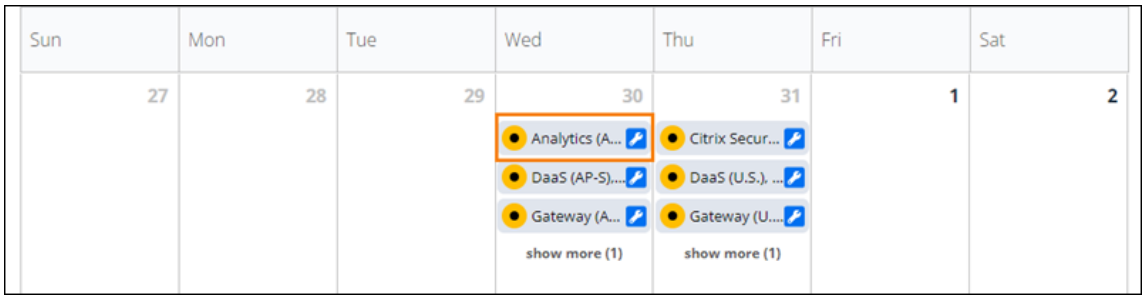
Ver detalles de incidentes de servicio

Para ver información más detallada sobre un incidente con relación a un servicio afectado:

- En la vista de historial, haga clic en el icono situado junto al indicador de servicio para ver información más detallada sobre el incidente.



- En la vista de mantenimiento, haga clic en la entrada de servicio para ver la página de estado de la ventana de mantenimiento programado.



Frecuencia de notificaciones de incidentes

Si se produce un incidente de estado del servicio, Citrix tiene en cuenta estas características al publicar notificaciones en status.cloud.com:

- Duración del impacto
- Frecuencia del impacto

Mientras se trata el incidente, Citrix publica estos tipos de notificaciones en el panel de estado de Cloud:

- **Investigating:** Esta notificación indica que Citrix ha identificado el problema como urgente y lo está investigando.
- **Monitoring:** Esta notificación indica que Citrix ha identificado la causa principal y está mitigando el problema.
- **Resolved:** Esta notificación indica que Citrix ha resuelto el problema y que el servicio se ha restablecido correctamente.

Mientras Citrix investiga y supervisa incidentes, publica actualizaciones en intervalos de 60 a 120 minutos. Estas actualizaciones pueden incluir información como:

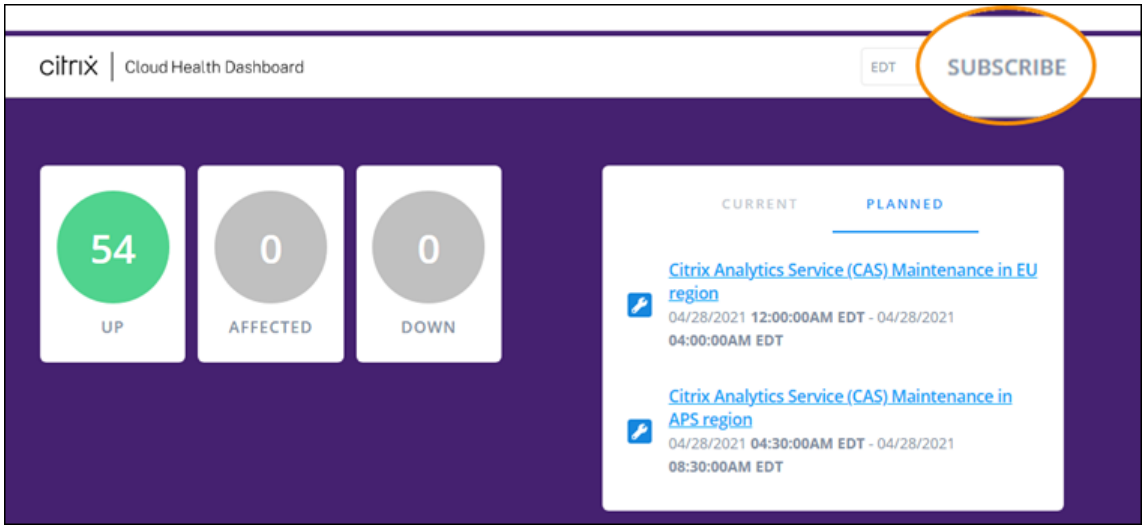
- Detalles adicionales sobre el incidente.
- Una descripción de las medidas que Citrix está tomando para resolver el incidente.
- Una indicación de que no se han producido cambios nuevos desde la última actualización.

Cuando se resuelve un incidente, Citrix publica una actualización final. Esta actualización puede indicar que el incidente se ha resuelto y que el servicio se ha restablecido correctamente.

Suscríbase a las notificaciones

Para recibir notificaciones sobre eventos de mantenimiento del servicio, utilice los métodos siguientes:

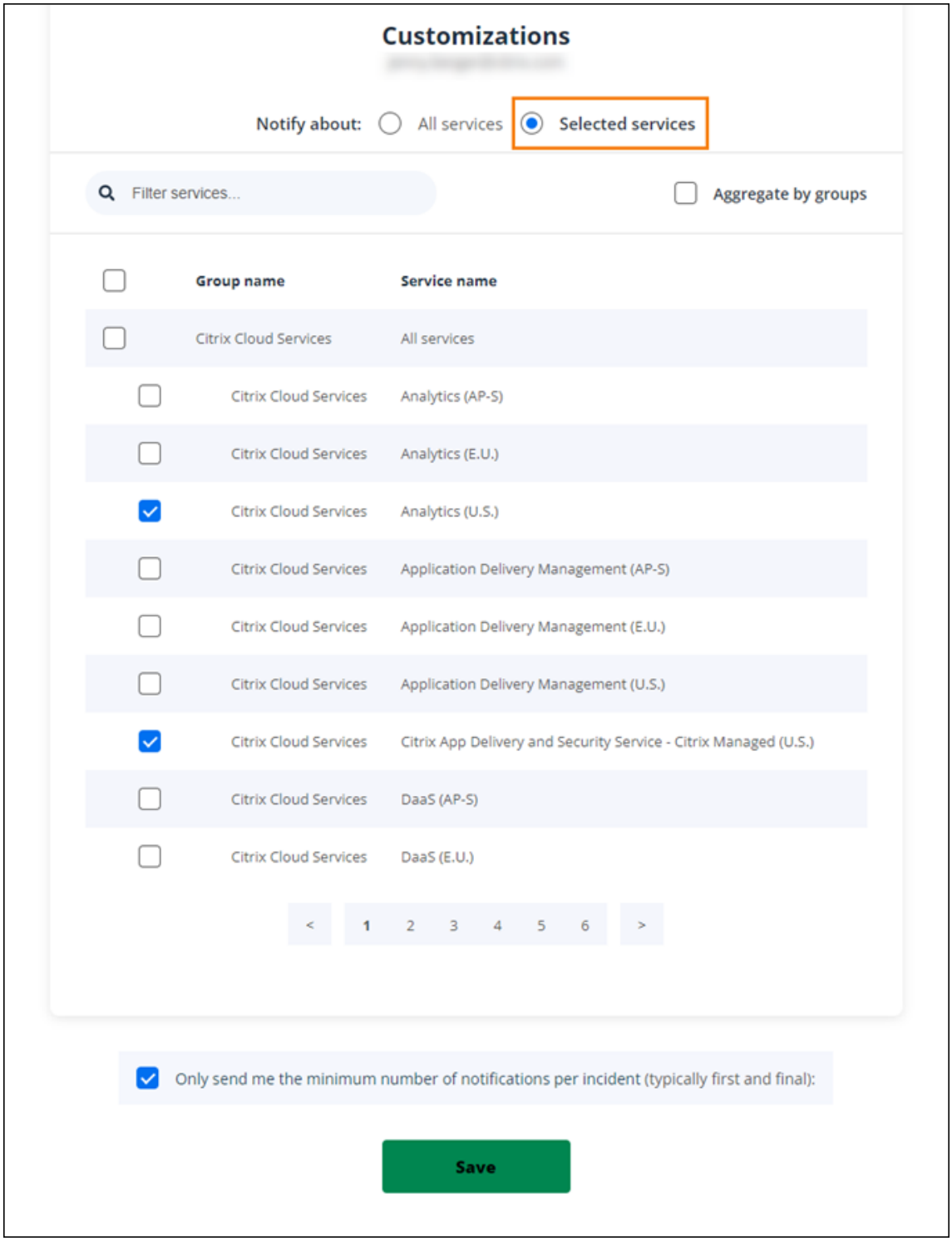
- Seleccione **Suscribe** en la parte superior derecha del panel y seleccione el método de notificación que quiere utilizar. Puede elegir entre varios métodos, incluidos por correo electrónico y por teléfono (con mensajes de texto).



- Introduzca las siguientes URL en su lector RSS para suscribirse al feed RSS de Estado de Citrix Cloud:
  - Para recibir notificaciones de incidentes de servicio y mantenimiento en un único feed, suscríbase a `https://status.cloud.com/?format=atom`.
  - Para recibir únicamente notificaciones de incidentes de servicio, suscríbase a `https://status.cloud.com/atom/incidents`.
  - Para recibir únicamente notificaciones de mantenimiento, suscríbase a `https://status.cloud.com/atom/maintenances`.

Suscribirse a servicios específicos de una región

1. Seleccione **Suscribe** en la esquina superior derecha del panel y, a continuación, seleccione el método de notificación que quiere utilizar.
2. Introduzca los detalles de contacto o la URL del método de suscripción elegido y seleccione **Acepto las condiciones y servicios**. Seleccione **Siguiente**. La página **Personalizaciones** aparece con **Servicios seleccionados** seleccionado de forma predeterminada.
3. En la página **Customizations**, seleccione los servicios de las regiones que quiera de la lista de varias páginas.

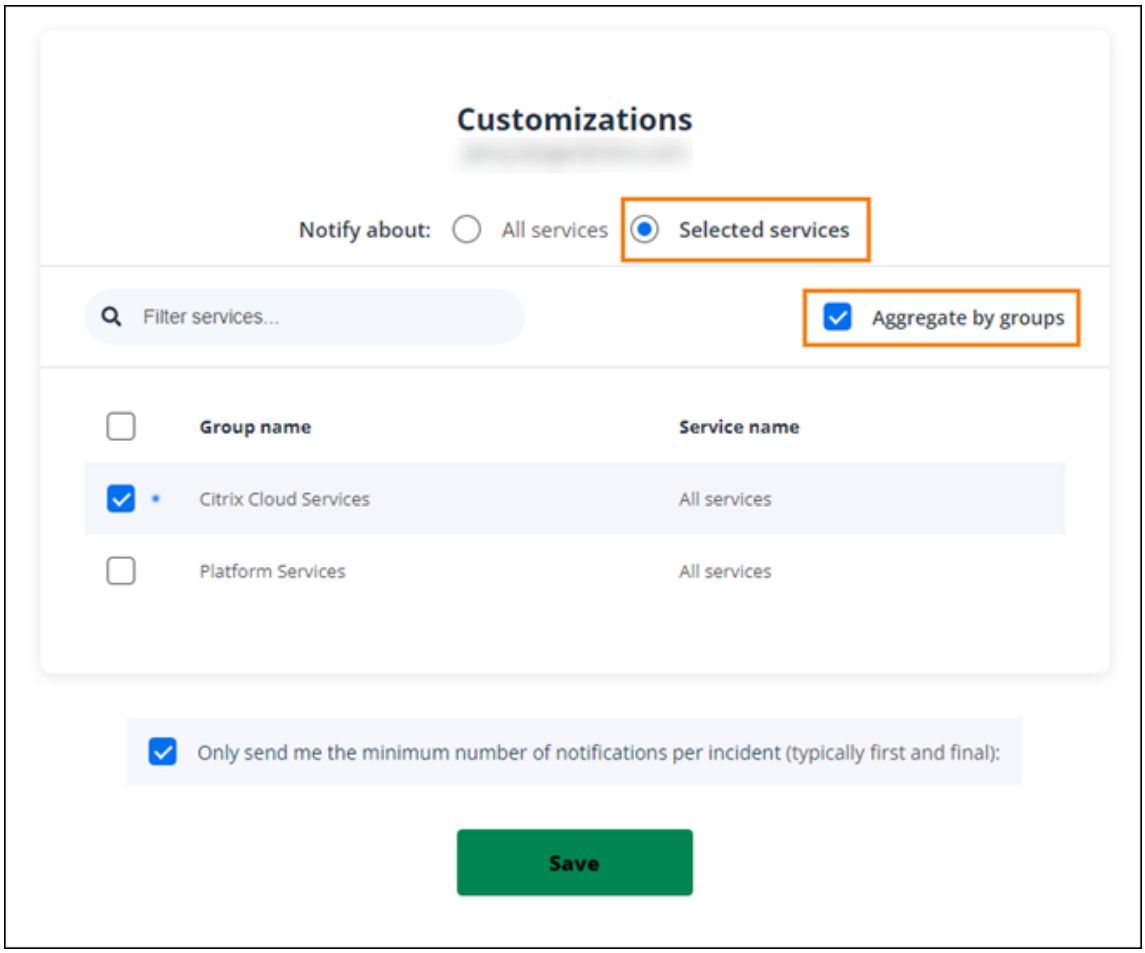


4. Para recibir solo la primera y la última notificación de cada incidente, seleccione **Only send me the minimum number of notifications per incident** (Enviarme solo la cantidad mínima de notificaciones por incidente).
5. Haga clic en **Guardar**.

Suscribirse a grupos específicos de servicios

Puede suscribirse a notificaciones de todos los servicios de la nube (por ejemplo, Analytics y DaaS) o de todos los servicios de plataforma (por ejemplo, el plano de control y las API de la nube) en todas las regiones.

1. Seleccione **Suscribe** en la esquina superior derecha del panel y, a continuación, seleccione el método de notificación que quiere utilizar.
2. Introduzca los detalles de contacto o la URL del método de suscripción elegido y seleccione **Acepto las condiciones y servicios**. Seleccione **Siguiente**. La página **Personalizaciones** aparece con **Servicios seleccionados** seleccionado de forma predeterminada.
3. En la página **Customizations**, seleccione **Aggregate by groups**.
4. Seleccione **Citrix Cloud Services** o **Platform Services**.

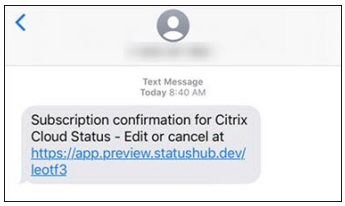


5. Para recibir solo la primera y la última notificación de cada incidente, seleccione **Only send me the minimum number of notifications per incident** (Enviarme solo la cantidad mínima de notificaciones por incidente).
6. Haga clic en **Guardar**.

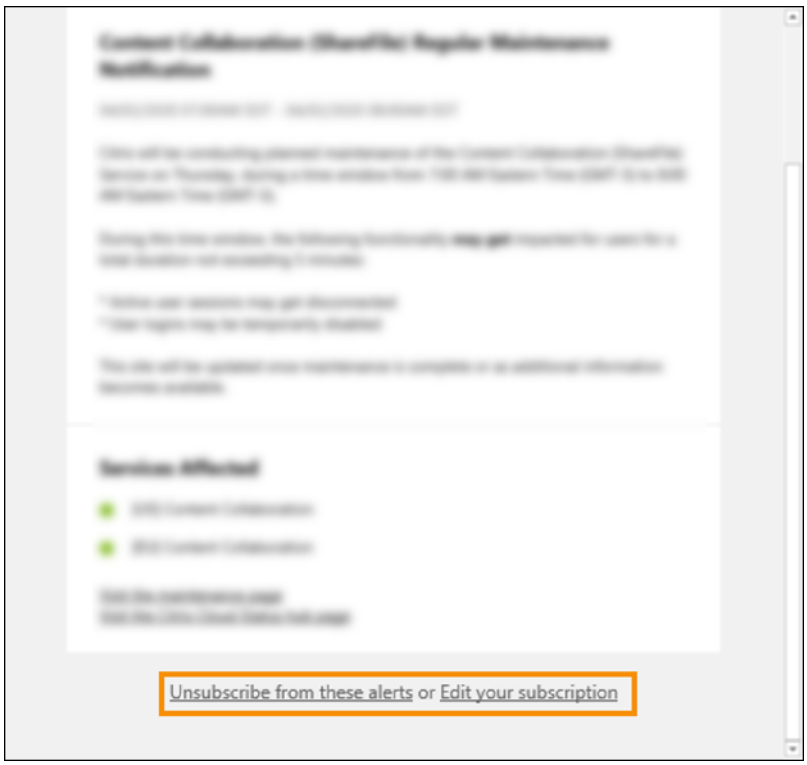
Cancelar la suscripción a las notificaciones

Dependiendo del método de suscripción, los enlaces para cancelar o cambiar la suscripción se incluyen en el mensaje de confirmación que recibe (por ejemplo, al suscribirse a notificaciones telefónicas) o en cada mensaje de notificación (por ejemplo, cuando se suscribe a notificaciones por correo electrónico). Por ejemplo:

- Notificación telefónica con opciones de suscripción:



- Correo electrónico de notificación con opciones de suscripción



Para cancelar la suscripción a todas las notificaciones y eliminar todos los métodos de suscripción:

1. Localice su mensaje de confirmación de suscripción o una notificación existente y seleccione el enlace para darse de baja. Algunos métodos de suscripción pueden proporcionar un único enlace para modificar o cancelar la suscripción.
2. Dependiendo del método de suscripción, utilice una de las siguientes opciones en la página **Edit Subscriptions**:
    - Seleccione **Remove all subscriptions**.

- Seleccione **Unsubscribe**. En la página **Unsubscribe methods**, seleccione **Remove all subscriptions**.

Para cancelar la suscripción a todas las notificaciones de un método de suscripción específico:

1. Localice su mensaje de confirmación de suscripción o una notificación existente y seleccione el enlace para darse de baja. Algunos métodos de suscripción pueden proporcionar un único enlace para modificar o cancelar la suscripción.
2. Dependiendo del método de suscripción, utilice una de las siguientes opciones en la página **Edit Subscriptions**:
   - Seleccione el método de suscripción que quiere eliminar. Su suscripción se eliminará inmediatamente.
   - Seleccione **Unsubscribe**. En la página **Unsubscribe Methods**, seleccione el método de suscripción que quiere quitar. Su suscripción se eliminará inmediatamente.

Cambiar notificaciones de servicio

1. Localice su mensaje de confirmación de suscripción o una notificación existente y seleccione el enlace para modificar su suscripción. Algunos métodos de suscripción pueden proporcionar un único enlace para modificar o cancelar la suscripción.
2. En la **página Edit Subscriptions**, seleccione el método de suscripción que quiere administrar.
3. En la página **Customizations**, seleccione los servicios sobre los que quiere que se le notifique o desactive los servicios para los que ya no quiere recibir notificaciones, según corresponda.
4. Seleccione **Guardar**.

Requisitos del sistema y de conectividad

July 2, 2024

Citrix Cloud ofrece funciones administrativas (a través de un explorador web) y solicitudes de funcionamiento (desde otros componentes instalados) que se conectan a los recursos que se encuentren dentro de su implementación. En este artículo se describen los requisitos del sistema, las direcciones de Internet necesarias a las que se puede contactar y los aspectos a tener en cuenta al establecer la conectividad entre su recursos y Citrix Cloud.

Requisitos del sistema

Citrix Cloud requiere la siguiente configuración mínima:

- Un dominio de Active Directory
- Dos máquinas físicas o virtuales, unidas a su dominio, para Citrix Cloud Connector. Para obtener más información, consulte Citrix Cloud Connector - Detalles técnicos.
- Máquinas físicas o virtuales, unidas a su dominio, para alojar cargas de trabajo y otros componentes como StoreFront. Para obtener más información sobre los requisitos del sistema para servicios específicos, consulte la documentación de Citrix para cada servicio.

Para obtener información sobre los requisitos de escala y tamaño, consulte Consideraciones sobre la escala y el tamaño de Cloud Connectors.

Exploradores web compatibles

- La versión más reciente de Google Chrome
- La versión más reciente de Mozilla Firefox
- La versión más reciente de Microsoft Edge
- La versión más reciente de Apple Safari

Requisitos de Transport Layer Security (TLS)

Citrix Cloud admite Transport Layer Security (TLS) 1.2 para las conexiones por TCP entre los componentes. Citrix Cloud no permite la comunicación a través de TLS 1.0 o TLS 1.1.

Para acceder a Citrix Cloud, debe usar un explorador compatible con TLS 1.2 y haber aceptado conjuntos de cifrado configurados. Para obtener más información, consulte Cifrado y administración de claves.

Consola de administración de Citrix Cloud

La consola de administración de Citrix Cloud es una consola web a la que se puede acceder después de iniciar sesión en https://citrix.cloud.com. Las páginas web que conforman la consola pueden necesitar otros recursos de Internet, ya sea al iniciar sesión, o en otro momento, al realizar operaciones específicas.

Configuración de proxy

Si se conecta a través de un servidor proxy, la consola de administración funciona con la misma configuración que se aplica a su explorador web. La consola funciona en el contexto del usuario, por lo que cualquier configuración de servidores proxy que requiera la autenticación del usuario también la requerirá para la consola.

Configuración de firewall

Para que funcione la consola de administración, es necesario que el puerto 443 esté abierto para conexiones de salida. Puede navegar por la consola para probar la conectividad general. Para obtener más información sobre los puertos necesarios, consulte Configurar puertos de entrada y salida.

Notificaciones de la consola

La consola de administración utiliza Pendo para mostrar alertas críticas, notificaciones sobre nuevas funciones e instrucciones en los productos para algunas funciones y servicios. Para asegurarse de que puede ver el contenido de Pendo en la consola de administración, Citrix recomienda que se pueda contactar con la dirección `https://citrix-cloud-content.customer.pendo.io/`.

Los servicios que muestran contenido de Pendo incluyen:

- Citrix Analytics
- Citrix DaaS
- Citrix Workspace

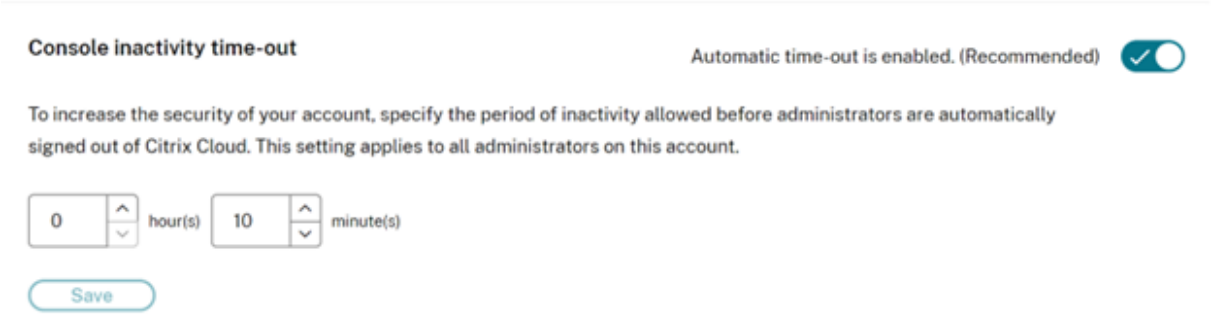
Pendo es un subprocesador de terceros que Citrix utiliza para proporcionar servicios de la nube y de asistencia a los clientes de Citrix. Para obtener una lista completa de estos subprocesadores, consulte Sub processors for Citrix Cloud & Support Services and Citrix Processors.

Tiempos de espera de la sesión

Después de que un administrador inicie sesión en Citrix Cloud, la consola de administración se cierra transcurridas 72 horas. Este tiempo de espera se produce independientemente de la actividad de la consola.

Tiempo de espera de inactividad configurable para la consola

Como administrador con acceso total, puede configurar la duración de la inactividad en la consola de Citrix Cloud antes de que los administradores cierren sesión automáticamente. Una vez configurado, el período de tiempo de espera especificado se aplicará a todos los administradores de la cuenta de Citrix Cloud.



Cuando la función esté habilitada, se cerrará la sesión de los administradores después del período de inactividad configurado y el tiempo de espera de la sesión se restablecerá en cada inicio de sesión posterior.

Cuando la función está inhabilitada, no hay un temporizador de inactividad y los administradores cerrarán sesión solo cuando se alcance el límite de 72 horas.

> **Nota:**
>
> - De forma predeterminada, esta función está inhabilitada.
> - El tiempo de espera de inactividad configurable es de 10 minutos a 12 horas.
> - El valor predeterminado de tiempo de espera de inactividad es 60 minutos.

Registro del servidor de licencias en Citrix Cloud

Si quiere registrar su servidor de licencias Citrix local en Citrix Cloud para supervisar el uso de las implementaciones locales, asegúrese de que se pueda contactar con las siguientes direcciones:

- `https://trust.citrixnetworkapi.net` (para obtener un código)
- `https://trust.citrixworkspacesapi.net/` (para confirmar que el servidor de licencias está registrado)
- `https://cis.citrix.com` (para cargar datos)
- `https://core-eastus-release-a.citrixworkspacesapi.net`
- `https://core.citrixworkspacesapi.net`
- `ocsp.digicert.com port 80`
- `crl3.digicert.com port 80`
- `crl4.digicert.com port 80`
- `ocsp.entrust.net port 80`
- `crl.entrust.net port 80`

Si utiliza un servidor proxy con Citrix License Server, asegúrese de que el servidor proxy esté configurado tal y como se describe en Configurar un servidor proxy, en la documentación de producto de las licencias.

Citrix Cloud Connector

Citrix Cloud Connector es un paquete de software que implementa un conjunto de servicios que se ejecutan en servidores Windows de Microsoft. La máquina que aloje el Cloud Connector se encuentra dentro de la red donde residen los recursos que se usan con Citrix Cloud. El Cloud Connector se conecta a Citrix Cloud para funcionar y administrar sus recursos según sea necesario.

Si quiere conocer los requisitos para instalar Cloud Connector, consulte Requisitos del sistema. Para funcionar, el Cloud Connector requiere conectividad de salida en el puerto 443. Después de la instalación, Cloud Connector pueden tener requisitos adicionales de acceso, en función del servicio de Citrix Cloud con el que se esté utilizando.

La máquina que aloja el Cloud Connector debe tener una conectividad de red estable con Citrix Cloud. Los componentes de la red deben admitir HTTPS y sockets web seguros de larga duración. Si se configura un tiempo de espera en los componentes de la red, el tiempo de espera debe ser superior a 2 minutos.

Para obtener ayuda para la solución de problemas de conectividad entre Cloud Connector y Citrix Cloud, use la utilidad de comprobación de la conectividad de Cloud Connector. Esta utilidad realiza una serie de comprobaciones en la máquina con Cloud Connectors para comprobar que puede contactar con Citrix Cloud y servicios relacionados. Si utiliza un servidor proxy en su entorno, todas las comprobaciones de conectividad se canalizan a través del servidor proxy. Para descargar la utilidad, consulte CTX260337 en Knowledge Center de Citrix Support.

Requisitos de conectividad con el servicio común de Cloud Connector

La conexión a Internet desde los centros de datos requiere que el puerto 443 esté abierto para las conexiones salientes. Sin embargo, para poder funcionar en entornos que contienen restricciones de firewall o un servidor proxy de Internet, se necesitan más parámetros. Para obtener más información, consulte Configurar el proxy y el firewall de Cloud Connector.

Debe poderse establecer contacto con las direcciones de cada servicio de este artículo para operar y utilizar correctamente el servicio. En la siguiente tabla, se ofrece una lista de las direcciones comunes a la mayoría de los servicios de Citrix Cloud:

- `https://*.citrixworkspacesapi.net` (proporciona acceso a las API de Citrix Cloud de las que hacen uso los servicios)
- `https://*.cloud.com` (proporciona acceso a la interfaz de inicio de sesión de Citrix Cloud)
- `https://*.blob.core.windows.net` (proporciona acceso a Azure Blob Storage, que almacena actualizaciones para Citrix Cloud Connector)
- `https://*.servicebus.windows.net` (proporciona acceso a Azure Service Bus, que se usa para los registros y el agente de Active Directory)

Estas direcciones solo se proporcionan como nombres de dominio porque Citrix Cloud Services son dinámicos y sus direcciones IP están sujetas a cambios de rutina.

Como recomendación, utilice Directiva de grupo para configurar y administrar estas direcciones. Además, configure únicamente las direcciones aplicables a los servicios que usted y sus usuarios finales utilizan.

Si utiliza Citrix Cloud con Citrix License Server para registrar sus productos locales, consulte Registro del servidor de licencias en Citrix Cloud en este artículo para ver las direcciones de contacto adicionales necesarias.

FQDN permitidos para Cloud Connector

Para ayudarle a garantizar que todos los nombres de dominio completos (FQDN) necesarios pasen por el firewall, Citrix proporciona los siguientes recursos:

- allowlist.json
- CTX270584: Citrix Gateway Service: puntos de presencia (PoP)

Al configurar el firewall, consulte estos dos recursos para verificar que los FQDN que requiere la implementación del servicio estén permitidos.

Caché de host local (High Availability Service) Cuando use la caché de host local (LHC) en los conectores, asegúrese de que pueden llegar al punto final de la elección de todos los demás conectores de la ubicación de recursos. El punto final de la elección está en el puerto 80 y se puede acceder a él mediante la siguiente URL: `http://<FQDN_OR_IP_OF_PEER_CONNECTOR>/Citrix/CdsController/ISecondaryBrokerElection`.

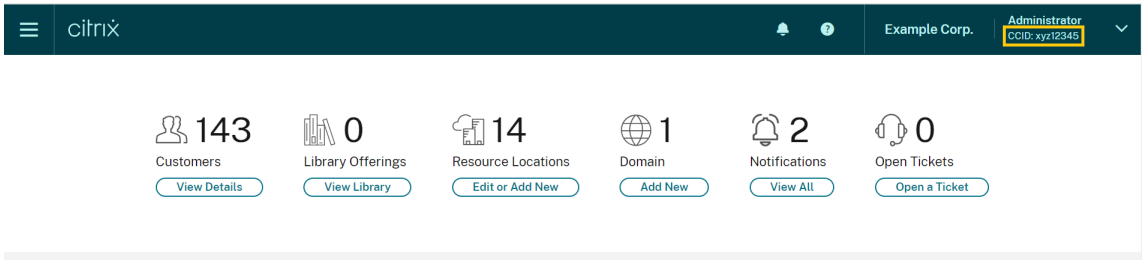
Si los conectores no pueden comunicarse en esta dirección, se eligen varios agentes durante un evento de LHC, lo que puede provocar errores intermitentes al iniciar aplicaciones y escritorios virtuales. Para obtener más información, consulte Ubicaciones de recursos con varios Cloud Connectors.

Autenticación adaptable Cuando utilice el Cloud Connector para la conectividad con un servicio de autenticación adaptable, debe permitir que el Citrix Cloud Connector acceda al dominio o a la URL que haya reservado para la instancia de autenticación adaptable. Por ejemplo, permita `https://aauth.xyz.com`. Para obtener más información, consulte Autenticación adaptable.

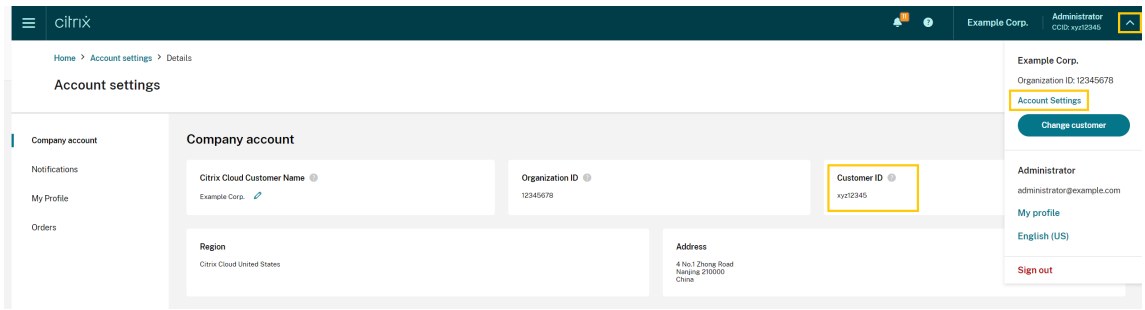
Allowlist.json El archivo allowlist.json se encuentra en https://fqdnallowlistsa.blob.core.windows.net/fqdnallowlist-commercial/allowlist.json y muestra los FQDN a los que accede Cloud Connector. Esta lista se agrupa por producto e incluye un registro de cambios para cada grupo de FQDN.

Algunos de estos FQDN son específicos de un cliente e incluyen secciones con plantillas entre corchetes angulares. Estas secciones con plantillas deben reemplazarse por los valores reales antes de usarlas. Por ejemplo, en el caso de `<CUSTOMER_ID>.xendesktop.net`, `<CUSTOMER_ID>` se reemplaza por el ID de cliente real de la cuenta de Citrix Cloud. Puede encontrar el ID de cliente en las siguientes ubicaciones de la consola:

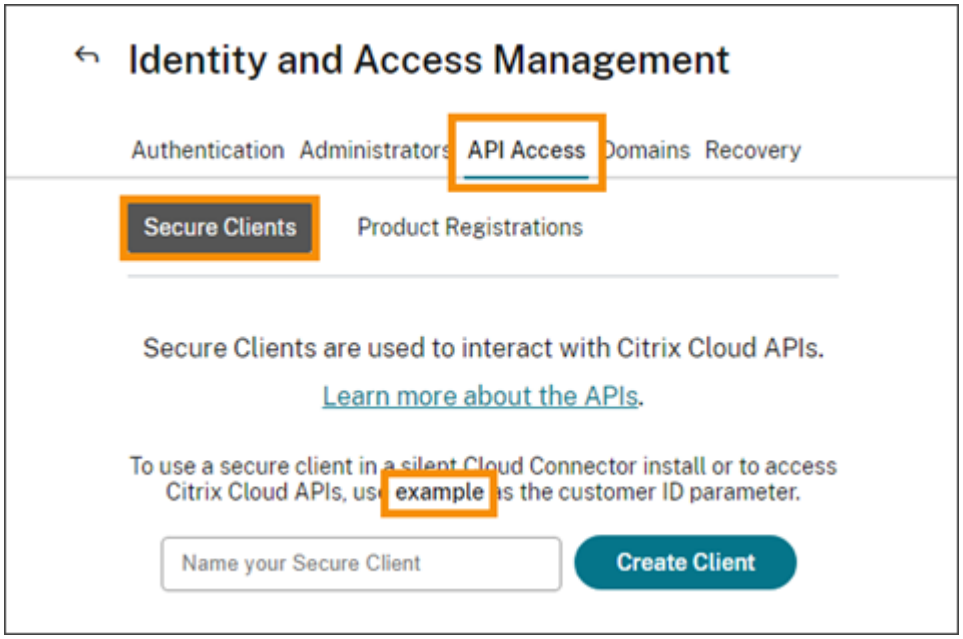
- En la esquina superior derecha de la pantalla, debajo del nombre del cliente de la cuenta de Citrix Cloud.



- En la página Parámetros de cuenta, bajo el **ID de cliente de Citrix Cloud (CCID)**.



- En la ficha **Clientes seguros Administración de acceso e identidad > Acceso a API > Clientes seguros**.



Puntos de presencia de Gateway Service Algunos de los FQDN incluidos en el archivo allowlist.json también se incluyen en CTX270584: Citrix Gateway Service –Points of Presence (PoPs). Sin embargo, CTX270584 también incluye los FQDN a los que acceden los clientes, como los siguientes:

- global-s.g.nssvc.net
- azure-s.g.nssvc.net

Validación de certificados

Binarios y dispositivos de punto final de Cloud Connector cuyos contactos de Cloud Connector están protegidos por certificados X.509 que se verifican cuando el software se instala. Para validar estos certificados, cada máquina con Cloud Connectors debe cumplir ciertos requisitos. Para obtener una lista completa de estos requisitos, consulte Requisitos de validación de certificados.

Descifrado SSL

Habilitar el descifrado SSL en algunos servidores proxy puede impedir que Cloud Connector se conecte a Citrix Cloud. Para obtener más información sobre cómo resolver este problema, consulte CTX221535.

Dispositivo Citrix Connector para Cloud Services

Connector Appliance es un dispositivo que puede implementar en el hipervisor. El hipervisor que aloja el Connector Appliance se encuentra en la red donde residen los recursos que se usan con Citrix Cloud. Connector Appliance se conecta a Citrix Cloud para funcionar y administrar sus recursos según sea necesario.

Para ver los requisitos de instalación de Connector Appliance, consulte Requisitos del sistema.

Para funcionar, el Connector Appliance requiere conectividad de salida en el puerto 443. Sin embargo, para poder funcionar en entornos que contienen restricciones de firewall o un servidor proxy de Internet, se necesitan más parámetros.

Para operar y utilizar correctamente los servicios de Citrix Cloud, debe poder establecerse contacto con las siguientes direcciones:

- `https://*.cloud.com`
- `https://*.citrixworkspacesapi.net`
- `https://*.citrixnetworkapi.net`

- `https://*.*.nssvc.net`

  Los clientes que no pueden habilitar todos los subdominios pueden utilizar las siguientes direcciones

  - `https://*.g.nssvc.net`
  - `https://*.c.nssvc.net`

- `https://*.servicebus.windows.net`
- `https://iwsprodeastusuniconacr.azurecr.io`
- `https://iwsprodeastusuniconacr.eastus.data.azurecr.io`

Requisitos de la red

Compruebe que el entorno de su Connector Appliance tenga esta configuración:

- La red permite que el Connector Appliance utilice DHCP para obtener servidores DNS y NTP, una dirección IP, un nombre de host y un nombre de dominio, o bien puede configurar manualmente los parámetros de red en la consola de Connector Appliance.
- La red no está configurada para utilizar los rangos IP locales de enlace 169.254.0.1/24, 169.254.64.0/18 o 169.254.192.0/18, que el Connector Appliance utiliza internamente.
- El reloj del hipervisor se establece en la hora universal coordinada (UTC) y se sincroniza con un servidor horario o DHCP proporciona información del servidor NTP a Connector Appliance.
- Si utiliza un proxy con un Connector Appliance, el proxy debe estar sin autenticar o usar autenticación básica.

Conectividad con Citrix Analytics Service

- Para mensajes dentro del producto, incluidas nuevas funciones y comunicaciones críticas: `https://citrix-cloud-content.customer.pendo.io/`
- Requisitos adicionales: Requisitos previos

Para obtener más información sobre cómo incorporar orígenes de datos al servicio, consulte Orígenes de datos compatibles.

Conectividad del servicio Console

Para obtener todos los requisitos de conectividad a Internet, consulte Puertos compatibles en la documentación de producto de NetScaler.

Conectividad de servicio de Citrix DaaS

Ubicación de recursos de Citrix / Cloud Connector:

- Requisitos de conectividad con el servicio común de Cloud Connector
- `https://[customerid].xendesktop.net`, donde `[customerid]` es el parámetro del ID de cliente que se muestra en la ficha **Clientes seguros** (**Administración de acceso e identidad > Acceso a API > Clientes seguros**) de la consola de administración de Citrix Cloud.
  - Los clientes que utilizan Citrix Virtual Apps Essentials necesitan utilizar `https://*.xendesktop.net` en su lugar.
- Los clientes que utilizan Distribución rápida para instalar Citrix DaaS deben configurar estas direcciones adicionales para que se pueda contactar con ellas:
  - `https://*.apps.cloud.com`
  - La `AzureCloud` etiqueta de servicio
- `https://*.*.nssvc.net`
  - Los clientes que no pueden habilitar todos los subdominios pueden utilizar las siguientes direcciones:
    - `https://*.g.nssvc.net`
    - `https://*.c.nssvc.net`

Para obtener información general sobre cómo Cloud Connector se comunica con el servicio, consulte el diagrama de Citrix DaaS en el sitio web de Citrix Tech Zone.

Consola de administración:

- `https://*.citrixworkspacesapi.net` (No es necesario para el protocolo Rendezvous)
- `https://*.citrixnetworkapi.net` (No es necesario para el protocolo Rendezvous)
- `https://*.cloud.com` (No es necesario para el protocolo Rendezvous)
- `https://[customerid].xendesktop.net`, donde `[customerid]` es el parámetro del ID de cliente que se muestra en la ficha **Clientes seguros** (**Administración de acceso e identidad > Acceso a API > Clientes seguros**) de la consola de administración de Citrix Cloud.
  - Los clientes que utilizan Citrix Virtual Apps Essentials necesitan utilizar `https://*.xendesktop.net` en su lugar.
- `https://*.*.nssvc.net` (no se necesita para Citrix DaaS Standard para Azure)
  - Los clientes que no pueden habilitar todos los subdominios pueden utilizar las siguientes direcciones:
    - `https://*.g.nssvc.net`

    * https://*.c.nssvc.net

- Para mensajes dentro del producto, incluidas nuevas funciones y comunicaciones críticas: https://citrix-cloud-content.customer.pendo.io/

Protocolo Rendezvous

Cuando se utiliza Citrix Gateway Service, el protocolo Rendezvous permite que los VDA omitan los Citrix Cloud Connectors para conectarse de forma directa y segura con el plano de control de Citrix Cloud.

Independientemente de la versión del protocolo que utilice, los VDA deben poder contactar con las direcciones de la consola de administración indicadas anteriormente, a menos que se indique lo contrario. Para obtener una lista completa de los requisitos del protocolo Rendezvous, consulte las siguientes secciones de la documentación del producto Citrix DaaS:

- Rendezvous V1
- Rendezvous V2

Requisito de caché de host local

Si el firewall realiza una inspección de paquetes y quiere utilizar la función Caché de host local, asegúrese de que el firewall acepte el tráfico XML y SOAP. Esta función requiere la capacidad de descargar archivos MDF, lo que ocurre cuando Cloud Connector sincroniza los datos de configuración con Citrix Cloud. Estos archivos se entregan al Cloud Connector a través del tráfico XML y SOAP. Si el firewall bloquea este tráfico, se produce un error en la sincronización entre el Cloud Connector y Citrix Cloud. Si se interrumpe la conexión, los usuarios no pueden seguir trabajando porque los datos de configuración que residen en el Cloud Connector no están actualizados.

Para obtener más información sobre esta función, consulte Caché de host local en la documentación de producto de Citrix DaaS.

Requisito de actualización de versiones de VDA

Con la interfaz de Configuración completa de Citrix DaaS, puede actualizar la versión de los VDA por catálogo o por máquina. Puede actualizarlos inmediatamente o en un momento programado. Para obtener más información sobre la función de actualización de versiones de VDA, consulte Actualizar la versión de los VDA mediante la interfaz de Configuración completa.

Al utilizar la función, asegúrese de cumplir estos requisitos de conectividad:

- Se agregaron estas URL de Azure CDN a la lista de permitidos. La función descarga los instaladores de VDA desde los dispositivos de punto final de Azure CDN.

  - Producción: Estados Unidos (US): `https://prod-us-vus-storage-endpoint.azureedge.net/*`
  - Producción: Unión Europea (UE): `https://prod-eu-vus-storage-endpoint.azureedge.net/*`
  - Producción: Asia-Pacífico Sur (APS): `https://prod-aps-vus-storage-endpoint.azureedge.net/*`
  - Producción: Japón (JP): `https://prod-jp-vus-storage-endpoint.azureedge.net/*`

- La función verifica que el instalador de VDA esté firmado por un certificado válido. Asegúrese de que se hayan agregado estas URL a la lista de permitidos para comprobar la validez y la revocación de certificados:

  - `http://crl3.digicert.com/*`
  - `http://crl4.digicert.com/*`
  - `http://ocsp.digicert.com/*`
  - `http://cacerts.digicert.com/*`

- La función requiere el agente de actualización de versiones de VDA para funcionar. El agente de actualización de versiones de VDA que se ejecuta en el VDA se comunica con Citrix DaaS. Asegúrese de que se hayan agregado estas URL a la lista de permitidos:

  - `https://[customerId].xendesktop.net/citrix/VdaUpdateService/*`, donde `[customerid]` es el parámetro del ID de cliente que se muestra en la ficha **Clientes seguros** (**Administración de acceso e identidad > Acceso a API > Clientes seguros**) de la consola de administración de Citrix Cloud.
  - `http://xendesktop.net/citrix/VdaUpdateService/*`

Conectividad con Endpoint Management Service

Ubicación de recursos de Citrix / Cloud Connector:

- Requisitos de conectividad con el servicio común de Cloud Connector
- Requisitos adicionales: /es-es/citrix-endpoint-management/endpoint-management.html

Consola de administración:

- `https://*.citrix.com`
- `https://*.citrixworkspacesapi.net`
- `https://*.cloud.com`
- `https://*.blob.core.windows.net`
- Requisitos adicionales: /es-es/citrix-endpoint-management/endpoint-management.html

Conectividad con Citrix Gateway Service

- Requisitos de conectividad con el servicio común de Cloud Connector
- `https://*.*.nssvc.net`
  - Los clientes que no pueden habilitar todos los subdominios pueden utilizar las siguientes direcciones:
    - `https://*.g.nssvc.net`
    - `https://*.c.nssvc.net`

> **Importante:**
>
> La interceptación SSL no se puede realizar en direcciones de Citrix Gateway. Es posible que, al habilitar la interceptación SSL en algunos proxies, se impida que Cloud Connector se conecte correctamente a Citrix Cloud.

Conectividad con NetScaler Intelligent Traffic Management Service

- `https://*.cedexis-test.com`
- `https://*.citm-test.com`
- `https://cedexis.com`
- `https://cedexis-radar.net`

Conectividad con SD-WAN Orchestrator Service

Para obtener toda la información sobre los requisitos de conectividad a Internet, consulte Prerequisites for Citrix SD-WAN Orchestrator service usage.

Conectividad de servicio de Remote Browser Isolation (antes denominado Secure Browser)

Ubicación de recursos de Citrix / Cloud Connector:

Requisitos de conectividad con el servicio común de Cloud Connector

Consola de administración:

- `https://*.cloud.com`
- `https://*.citrixworkspacesapi.net`
- `https://browser-release-a.azureedge.net`
- `https://browser-release-b.azureedge.net`

Conectividad con Citrix Secure Private Access Service

- https://*.netscalergateway.net
- https://*.*.nssvc.net
  - Los clientes que no pueden habilitar todos los subdominios pueden utilizar las siguientes direcciones:
    * https://*.g.nssvc.net
    * https://*.c.nssvc.net

Conectividad con Citrix Workspace Service

- https://*.cloud.com
- https://*.citrixdata.com
- Para mensajes dentro del producto, incluidas nuevas funciones y comunicaciones críticas: https://citrix-cloud-content.customer.pendo.io/

Conectividad de Global App Configuration Service

https://discovery.cem.cloud.us

Para obtener más información sobre este servicio, consulte estos recursos:

- Personalización de parámetros de la aplicación Workspace: Documentación del producto Citrix Workspace
- Global App Configuration Service: Documentación de Citrix Developer

Conectividad de la aplicación Citrix Workspace

Agregue estas URL a su lista de direcciones permitidas:

- https://*.cloud.com
- Dirección del proveedor de identidades. Consulte las instrucciones de la documentación del IDP correspondiente.
- https://*.wsp.cloud.com

En el caso de direcciones URL específicas, permita el acceso a estas direcciones:

- <yourcustomer>.cloud.com

Citrix Secure Private Access

- ngspolicy.netscalergateway.net
- config.netscalergateway.net
- app.netscalergateway.net
- http://tunnel.netscalergateway.net/

Global App Configuration Service

Consulte Conectividad de Global App Configuration Service en este artículo.

Autenticación

- accounts.cloud.com
- accounts-dsauthweb.cloud.com

Asegúrese de que las URL de su proveedor de identidades también sean accesibles desde los dispositivos de los usuarios finales.

Citrix Analytics Service

- locus.analytics.cloud.com

Habilite el acceso a la URL correspondiente de esta lista, según su ubicación:

- EE. UU.: citrixanalyticseh.servicebus.windows.net
- UE: citrixanalyticseheu.servicebus.windows.net
- APS: citrixanalyticsehaps.servicebus.windows.net

Recursos de la interfaz gráfica de Workspace

- ctx-ws-assets.cloud.com

Personalización, notificaciones e implantación de funciones

- customer-**interface**-personalization.us.wsp.cloud.com
- user-personalization.us.wsp.cloud.com
- admin-notification.us.wsp.cloud.com
- customer-**interface**-personalization.eu.wsp.cloud.com
- user-personalization.eu.wsp.cloud.com

- admin-notification.eu.wsp.cloud.com
- customer-interface-personalization.ap-s.wsp.cloud.com
- user-personalization.ap-s.wsp.cloud.com
- admin-notification.ap-s.wsp.cloud.com
- feature-rollout.us.wsp.cloud.com
- feature-rollout.eu.wsp.cloud.com
- feature-rollout.ap-s.wsp.cloud.com

Servicio de registro de dispositivos

- device-registration.us.wsp.cloud.com
- device-registration.eu.wsp.cloud.com
- device-registration.ap-s.wsp.cloud.com

Servicio de notificaciones push

- push-events-signalr.us.wsp.cloud.com
- push-events-signalr.eu.wsp.cloud.com
- push-events-signalr.ap-s.wsp.cloud.com

Citrix Gateway Service

- https://*.g.nssvc.net

Single Sign-On para espacios de trabajo con el Servicio de autenticación federada (FAS) de Citrix

La consola y el servicio FAS acceden a las siguientes direcciones con la cuenta del usuario y la cuenta del servicio de red, respectivamente.

- Consola de administración de FAS, en la cuenta del usuario:
  - https://*.cloud.com
  - https://*.citrixworkspacesapi.net
  - https://*.citrixnetworkapi.net/
  - Direcciones requeridas por un proveedor de identidades tercero, si se utiliza uno en su entorno
- Servicio FAS, en la cuenta del servicio de red:
  - https://*.citrixworkspacesapi.net


```
- https://*.citrixnetworkapi.net/
```

Si su entorno incluye servidores proxy, configure el proxy de usuario con las direcciones de la consola de administración FAS. Además, asegúrese de que la dirección de la cuenta de servicio de red esté configurada como apropiada para su entorno.

Si utiliza Active Directory o Active Directory y una contraseña temporal de un solo uso (TOTP) como proveedor de identidades de la aplicación Citrix Workspace, también debe incluir `login.cloud.com` en la lista de permitidos. Si utiliza otros proveedores de identidades, permita las URL de cada proveedor de identidades por separado.

Las URL del centro de eventos de CAS también son geoespecíficas. citrixanalyticseh-alias.servicebus.windows.net

Conectividad con Workspace Environment Management Service

Ubicación de recursos de Citrix / Cloud Connector / Agente:

`https://*.wem.cloud.com`

Para ver todos los requisitos, consulte Requisitos previos de conectividad en la documentación de Workspace Environment Management Service.

Planificar su implementación

July 2, 2024

Para obtener una guía desde el punto de vista del cliente, vaya a Citrix Success Center. Success Center le ofrece una guía para las cinco etapas clave de lo que puede hacer con Citrix: planificación, construcción, implementación, administración y optimización. Los artículos y las guías de Success Center complementan esta documentación y ofrecen un panorama general de las soluciones disponibles.

Suscripciones y pruebas de los servicios

Citrix Cloud ofrece pruebas para la mayoría de los servicios de nube. Las pruebas tienen las mismas características y funciones que los servicios de pago, lo que las convierte en aptas para una prueba de concepto o una implementación piloto. Para obtener más información, consulte Pruebas de servicio de Citrix Cloud.

En general, los derechos relativos a los servicios de pago pueden tener una duración mensual, anual o determinada. A medida que el plazo de suscripción se acerca a su fin, Citrix Cloud envía recordatorios y proporciona un período de gracia para que pueda renovarla sin interrupciones indebidas

del servicio. Para obtener más información sobre la renovación de sus derechos, consulte Ampliar suscripciones de Citrix Cloud Services.

Regiones y presencia de los servicios

Citrix Cloud ofrece servicios en tres regiones: Estados Unidos, Unión Europea y Asia Pacífico Sur. Al suscribirse a Citrix Cloud, debe elegir la región que mejor se adapte a sus necesidades empresariales y de rendimiento.

Para obtener más información sobre cómo seleccionar una región y sobre los servicios disponibles en cada región, consulte Consideraciones geográficas.

Recursos de implementación

- Resiliencia de Citrix Cloud
- Guías de prueba de concepto de Tech Zone
- Arquitecturas de referencia de Tech Zone
- Consideraciones de escala y tamaño para los Cloud Connectors
- Consideraciones sobre la escala y el tamaño de la caché de host local
- Arquitecturas de referencia de autenticación de almacenes locales de StoreFront para Citrix DaaS

Recursos de migración

- Proof of Concept: Automated Configuration Tool
- Migración de Citrix Virtual Apps and Desktops desde el entorno local a Citrix Cloud
- Migración de Citrix Virtual Apps and Desktops desde VMware vSphere a Citrix DaaS en Microsoft Azure
- migración desde Administrador de dispositivos Android a Android Enterprise con Citrix Endpoint Management

Más información

- Citrix Discussions: Citrix Cloud: Foros de asistencia de la comunidad para Citrix Cloud y Citrix Cloud Services
- Formación de Citrix:
  - Fundamentals of Citrix Cloud
  - Introduction to Citrix Identity and Authentication

Pruebas de servicios en Citrix Cloud

July 2, 2024

Las pruebas de cada uno de los servicios de Citrix Cloud se entregan a través de la consola de administración de Citrix Cloud. La funcionalidad de las pruebas de los servicios es la misma que la de los servicios de pago, por lo que dichas pruebas pueden utilizarse para llevar a cabo pruebas de concepto (POC) o implementaciones piloto.

Cuando esté listo para comprar los servicios de Citrix Cloud, la versión de prueba se convierte en un servicio de producción. No es necesario volver a configurar nada ni crear una cuenta de producción aparte.

Descripción general de la prueba del servicio

La información incluida en esta sección es aplicable a la mayoría de las pruebas de servicios de Citrix Cloud. Los servicios con términos de prueba diferentes se describen en secciones aparte.

		Prueba de Citrix Cloud
	Cantidad de suscriptores permitida	25
	Duración máxima de la prueba	60 días naturales
	Período de gracia	14 días después del vencimiento de la prueba
	Período de retención de datos	90 días naturales después del vencimiento de la prueba
	Disponibilidad	Disponibilidad restringida
	Ubicación de recursos	Proporcionada y configurada por el cliente
	Duración de las sesiones de usuario	Sin límite
	Integración de Microsoft Active Directory local	Sí
	Elección de ubicaciones de recursos	Sí
	Implementación local (On-premises)	Sí

		Prueba de Citrix Cloud
	Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service)	Conjunto completo de funciones
	Endpoint Management	Conjunto completo de funciones
	Personalizable	Sí

Solicitar una prueba del servicio

El acceso a la prueba de Citrix Cloud se administra servicio por servicio. Para algunos servicios, puede solicitar una prueba como se describe en la sección Solicitar una prueba del servicio de este artículo. Para otros servicios, debe solicitar una demostración antes de recibir acceso a la prueba, como se describe en Solicitar una demostración del servicio en este artículo.

Período de prueba del servicio

En el caso de la mayoría de los servicios, tiene 60 días para probarlo después de que se apruebe su solicitud de prueba. Puede solicitar la prueba de un servicio una sola vez.

Compra de suscripciones a servicios

Puede comprar una suscripción al servicio en cualquier momento durante la prueba o durante el período de retención de datos. Para obtener más información, consulte Comprar los servicios de Citrix Cloud.

Después de comprar una suscripción, la versión de prueba se convierte en un servicio de producción. Los administradores y los usuarios pueden acceder al servicio y los datos que haya agregado durante la prueba permanecen intactos.

Citrix DaaS Standard para Azure

En esta sección se describen estos tipos de pruebas de Citrix DaaS Standard para Azure (antes denominado Citrix Virtual Apps and Desktops Standard para Azure):

- **Prueba aprobada automáticamente:** Después de solicitar la prueba a través de la consola de administración de Citrix Cloud, la prueba se autoriza automáticamente y está lista para usarse.

- **Prueba aprobada por Ventas:** Después de ponerse en contacto con un representante de Ventas de Citrix para solicitar una prueba, el representante autoriza la prueba. Después de la aprobación, la prueba está lista para usarse.

		Prueba aprobada automáticamente	Prueba aprobada por ventas
	Duración máxima de la prueba	7 días naturales	14 días naturales
	Período de gracia	1 día natural después del vencimiento de la prueba	14 días naturales después del vencimiento de la prueba
	Período de retención de datos	30 días naturales después del vencimiento de la prueba	90 días naturales después del vencimiento de la prueba

Según el tipo de prueba, tiene siete o 14 días para usar el servicio. Puede solicitar la prueba de un servicio una sola vez.

Las pruebas incluyen un período de gracia para acceder al servicio después de que venza el período de prueba. Este período de gracia le permite comprar una suscripción al servicio o eliminar los datos que haya agregado. Una vez finalizado el período de gracia, Citrix bloquea el acceso al servicio tanto para los administradores como para los usuarios.

Según el tipo de prueba, Citrix retiene los datos que agregue al servicio durante los 30 o 90 días posteriores al vencimiento de la prueba. Si compra una suscripción al servicio durante este período de retención, los administradores y los usuarios pueden acceder al servicio con sus datos intactos.

Puede comprar una suscripción al servicio a través de Azure Marketplace o poniéndose en contacto con su representante de Ventas de Citrix.

Solicitar una demostración del servicio

Para algunos servicios, debe solicitar una demostración a un representante de Ventas de Citrix para poder probar el servicio. Solicitar una demostración le permite analizar las necesidades que pueda tener su organización de un servicio en la nube con un representante de Ventas de Citrix. Además, el representante de Ventas se asegura de que disponga de toda la información necesaria para aprovechar al máximo el servicio.

1. Inicie sesión en su cuenta de Citrix Cloud.

2. En la consola de administración, seleccione **Solicitar demostración** para el servicio correspondiente. Aparece la página de solicitud de demostración del servicio.
3. Rellene el formulario y envíelo. Un representante de Ventas de Citrix se pondrá en contacto con usted para proporcionarle más información y guiarle a través del servicio.

Solicitar una prueba de servicio

1. Inicie sesión en su cuenta de Citrix Cloud.
2. En la consola de administración, seleccione **Solicitar prueba** para el servicio que quiere probar.

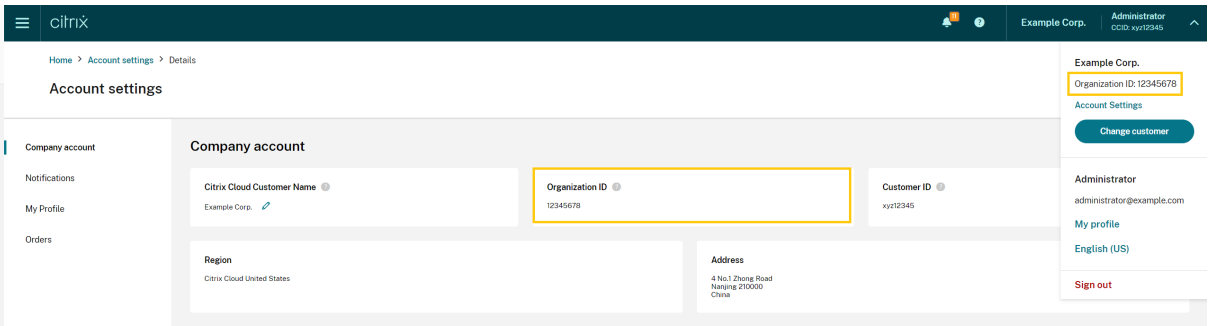
Cuando la prueba ha sido aprobada y está lista para usarse, Citrix le envía una notificación por correo electrónico.

> **Nota:**
>
> Para ofrecer una experiencia óptima al cliente, Citrix se reserva el derecho de autorizar las pruebas para un número limitado de participantes simultáneamente.

Comprar los servicios de Citrix Cloud

Cuando tenga todo listo para convertir el servicio de prueba en un servicio de producción, visite https://www.citrix.com/buy/ para buscar un Citrix Partner local.

Para comprar el servicio, necesitará su ID de organización (OrgID). Su OrgID aparece en el menú del cliente, en la esquina superior derecha de la consola de administración de Citrix Cloud. Su OrgID también aparece en la página **Parámetros de cuenta**.



Más información

- Condiciones de servicio de los servicios de Citrix Cloud
- El curso Fundamentals of Citrix Cloud incluye un breve vídeo en el que se explica cómo solicitar una prueba. El curso completo también cubre los componentes de la plataforma Citrix Cloud y sus servicios.

Ampliar suscripciones de Citrix Cloud Services

July 2, 2024

Este artículo describe cómo caducan las suscripciones adquiridas para los servicios de Citrix Cloud y cómo puede extender su suscripción.

En este artículo, las *suscripciones mensuales* se refieren a los servicios que se contratan mes a mes. Las *suscripciones anuales* se refieren a los servicios que se contratan anualmente. Las *suscripciones plurianuales* se refieren a los servicios que se contratan con carácter plurianual.

> **Nota:**
>
> Los Citrix Service Providers (CSP) pueden ampliar sus suscripciones enviando una orden de compra por valor de cero euros a su distribuidor de CSP. Para obtener más información sobre las renovaciones y las licencias de productos CSP, consulte *Citrix Service Provider Licensing Guide for Citrix Cloud*, disponible en el sitio web de Citrix Partner Central.

Antes del vencimiento

En el caso de las suscripciones mensuales, Citrix Cloud no envía notificaciones antes del vencimiento.

En el caso de las suscripciones anuales y plurianuales, Citrix Cloud le notifica a determinados intervalos cuando la suscripción se acerca a la fecha de vencimiento. Estas notificaciones le avisan por si quiere ampliar la suscripción o evitar la interrupción del servicio. Las siguientes notificaciones aparecen en la consola de administración de Citrix Cloud:

- 90 días antes de la fecha de vencimiento: aparece una pancarta amarilla que muestra los servicios que deben extenderse y sus fechas de vencimiento. Esta notificación aparece en la consola cada siete días o hasta que se extienda el servicio.
- 7 días antes de la fecha de vencimiento aparece una pancarta amarilla que muestra los servicios que deben extenderse y sus fechas de vencimiento. Esta notificación aparece en la consola hasta que se extienda el servicio o transcurra el período de gracia de vencimiento de 30 días.

Puede descartar estas notificaciones cuando aparezcan; sin embargo, reaparecerán después de siete días.

Citrix también le envía una notificación por correo electrónico que incluye una lista de los servicios que deben extenderse y sus fechas de vencimiento. Citrix envía esta notificación en los siguientes intervalos:

- 90 días antes de la fecha de vencimiento

- 60 días antes de la fecha de vencimiento
- 30 días antes de la fecha de vencimiento
- Siete días antes de la fecha de vencimiento
- Un día antes de la fecha de vencimiento

Después del vencimiento: bloqueo del servicio y retención de datos

Si la suscripción de servicio no se amplía durante el período de gracia, Citrix bloquea el acceso al servicio en cuestión de la siguiente manera:

- En el caso de las suscripciones mensuales caducadas, se bloquea el acceso a administradores y usuarios transcurridos cinco días a partir de la fecha de caducidad.
- En el caso de las suscripciones anuales y plurianuales caducadas, se bloquea el acceso a administradores y usuarios transcurridos 30 días a partir de la fecha de caducidad.

Citrix conserva los datos que haya agregado al servicio durante los 90 días posteriores a la fecha de vencimiento del servicio. Si extiende su suscripción antes de que termine el período de retención de 90 días, sus administradores y usuarios pueden acceder al servicio con sus datos intactos. Su suscripción extendida comienza de la siguiente manera:

- Para las suscripciones mensuales, la fecha de inicio de la suscripción del primer mes será la fecha en la que compró la extensión. Después, su suscripción se renueva automáticamente el primer día de cada mes siguiente.
- En el caso de suscripciones anuales y plurianuales, la fecha de inicio de la suscripción extendida es el día siguiente a la fecha de caducidad. Por ejemplo, si la suscripción caduca el 30 de septiembre y la extiende el 23 de octubre, la fecha de inicio de la suscripción extendida es el 1 de octubre.

Si no extiende su suscripción antes de que termine el período de retención de 90 días, Citrix restablece el servicio y elimina cualquier dato que haya agregado. Si aceptó permitir que Citrix administre la implementación en la nube (por ejemplo, al usar los servicios de Citrix Essentials o la opción de distribución rápida de Azure en Citrix DaaS), Citrix hace lo siguiente tras finalizar el período de retención de 90 días:

- Elimina todos los datos relacionados con el cliente de las bases de datos de Citrix.
- Elimina todos los recursos relacionados con los servicios de Citrix Cloud, incluidas las máquinas virtuales administradas por Citrix, que Citrix aprovisionó en su entorno de nube. Para obtener una descripción de los componentes administrados por Citrix que se incluyen en servicios específicos de Citrix Cloud, consulte la documentación del servicio correspondiente.

Suscripciones de Azure administradas por el cliente

Si utiliza su propia suscripción de Azure con un servicio de Citrix Cloud, el servicio instala una aplicación cuando conecta la suscripción de Azure al servicio. Si no amplía la suscripción al servicio de Citrix Cloud, Citrix no quita esta aplicación de la suscripción de Azure una vez finalizado el período de retención de 90 días. Debe eliminar esta aplicación para quitar el servicio completamente de su suscripción de Azure. Puede eliminar la aplicación mediante uno de los métodos siguientes:

- Si los administradores todavía no han bloqueado el acceso al servicio, elimine esta aplicación del servicio.
- Si los administradores tienen bloqueado el acceso al servicio, elimine esta aplicación desde Azure Portal.

Adquisición de extensiones de servicio

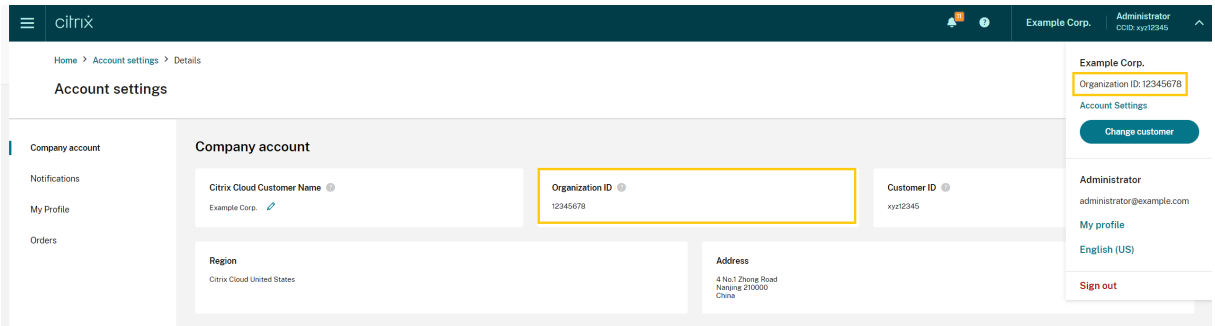
Para ampliar su suscripción a los servicios de Citrix Cloud, contacte con un representante de ventas de Citrix. Para buscar a un representante de ventas, siga estos pasos:

1. Inicie sesión en su cuenta de Citrix.
2. Seleccione **Quoting (DOTI)** y, a continuación, **Transactions**. Su representante de ventas y su dirección de correo electrónico aparecerán en la parte superior de esta vista.

También puede visitar la página Citrix Customer Service para obtener la información de contacto de su región geográfica.

Para completar la compra, su representante de ventas necesitará el ID de organización de su cuenta de Citrix Cloud. Para ver el ID de su organización, inicie sesión en su cuenta de Citrix Cloud. El ID de su organización se muestra en estos lugares:

- En el menú del cliente, en la esquina superior derecha de la consola de Citrix Cloud.
- En la página **Parámetros de cuenta**.



Consideraciones geográficas

July 2, 2024

En este artículo se describen las regiones comerciales que utiliza Citrix Cloud y la presencia de los servicios comerciales de Citrix Cloud en cada región.

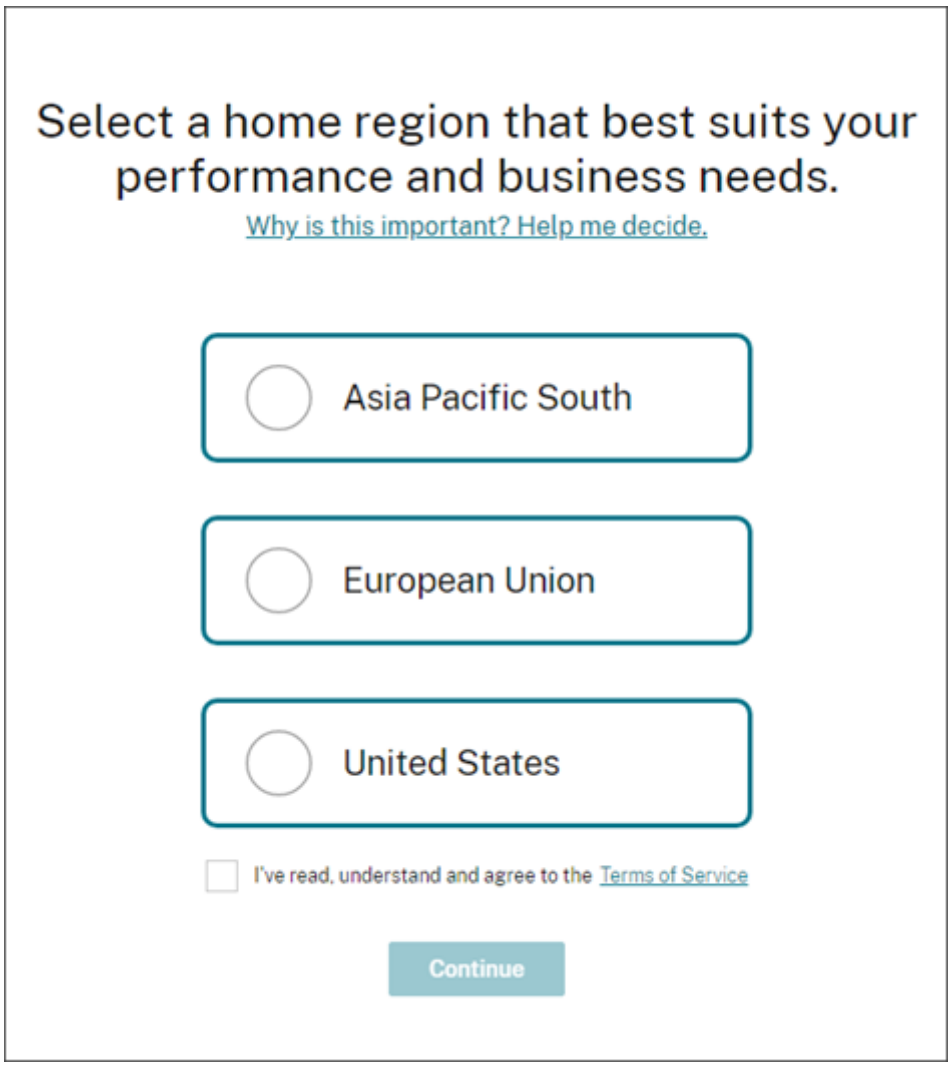
Para obtener más información sobre las regiones geográficas y la presencia de servicios para las plataformas en la nube dedicadas y las plataformas en la nube orientadas al sector público de Citrix, consulte Otras plataformas de la nube de Citrix.

Elegir una región

Cuando su organización se incorpora a Citrix Cloud y usted inicia sesión por primera vez, se le pide que seleccione una de las regiones siguientes:

- Estados Unidos
- Unión Europea
- Asia-Pacífico Sur

Al seleccionar una región, los servicios alojados en esa región geográfica se utilizan para las acciones asociadas a la organización siempre que sea posible. Elija una región asignada a la ubicación de la mayoría de los usuarios y recursos.



Notas importantes:

- Solo puede elegir la región una vez: cuando su organización empieza a utilizar Citrix Cloud. No podrá cambiarla más adelante.
- Si se encuentra en una región y utiliza un servicio en otra región, todo impacto en el rendimiento es mínimo. Los servicios de Citrix Cloud están diseñados para utilizarse de forma global. Por ejemplo, el impacto en la latencia de clientes ubicados en EE. UU. que tengan usuarios y conectores en Australia será mínimo.
- Si Citrix Cloud no está disponible en su región, elija la región que esté más cerca de donde se encuentran la mayoría de sus usuarios y recursos.

Presencia de servicios en cada región

La mayoría de los servicios de Citrix Cloud se replican en todas las regiones. La región que seleccione indica una preferencia en cuanto al lugar donde se deben realizar las conexiones. No obstante, es

posible que aún se establezcan conexiones con otras regiones geográficas. Si un servicio se replica en todas las regiones, todos los datos de ese servicio se almacenan en todas las regiones.

Del mismo modo, sus datos podrían ser procesados en cualquier región por afiliados o subprocesadores de Citrix según sea necesario para prestar los servicios.

Ciertos servicios tienen instancias regionales dedicadas. Algunos servicios solo tienen instancias basadas en EE. UU. En estos casos, las conexiones y los datos se encuentran confinados dentro de esa región geográfica.

Cuando un servicio no esté disponible en la región que haya seleccionado para la organización, es posible que cierta información (como datos de autenticación) se transfiera entre regiones según sea necesario.

Servicio	EE. UU.	UE	Asia-Pacífico Sur	Notas
Plano de control de Citrix Cloud	Sí	Sí	Sí	
Citrix Analytics for Security	Sí	Sí	Sí	
Citrix Analytics for Performance	Sí	Sí	Sí	
NetScaler Console (anteriormente Application Delivery Management)	Sí	Sí	Sí	Consulte Incorporación con baja interacción de instancias de NetScaler mediante Console Advisory Connect en este artículo. Para ver el programa de telemetría local de Console, consulte aquí.
Citrix DaaS (antes denominado Virtual Apps and Desktops Service)	Sí	Sí	Sí	El servicio usa la región de Citrix Cloud.

Servicio	EE. UU.	UE	Asia-Pacífico Sur	Notas
Citrix DaaS Standard para Azure (antes denominado Virtual Apps and Desktops Standard para Azure)	Sí	Sí	Sí	El servicio usa la región de Citrix Cloud.
Citrix DaaS Standard para Google Cloud (antes denominado Virtual Apps and Desktops Standard para Google Cloud)	Sí	No (usa la región de EE. UU.)	No (usa la región de EE. UU.)	
Citrix DaaS Premium para Google Cloud (antes denominado Virtual Apps and Desktops Premium para Google Cloud)	Sí	No (usa la región de EE. UU.)	No (usa la región de EE. UU.)	
Citrix Endpoint Management	Sí	Sí	Sí	Seleccionar desde múltiples ubicaciones en múltiples regiones. Consulte Ubicaciones del servicio de Endpoint Management en este artículo.

Servicio	EE. UU.	UE	Asia-Pacífico Sur	Notas
Remote Browser Isolation Service	Sí	Sí	Sí	El servicio usa la región de Citrix Cloud.
SD-WAN Orchestrator	Sí	Sí	Sí	
Citrix Secure Internet Access Nodes/POP	Varios nodos globales; tráfico redirigido según sea necesario para garantizar la mejor experiencia posible	Varios nodos globales; tráfico redirigido según sea necesario para garantizar la mejor experiencia posible	Varios nodos globales; tráfico redirigido según sea necesario para garantizar la mejor experiencia posible	Consulte Ubicaciones de Secure Internet Access Service en este artículo.
Citrix Secure Private Access	Todas las regiones	Todas las regiones	Todas las regiones	Consulte Puntos de presencia de Secure Private Access en este artículo.
Servicio de grabación de sesiones	Sí	Sí	Sí	
Citrix Virtual Apps Essentials	Sí	Sí	Sí	El servicio usa la región de Citrix Cloud.
Citrix Virtual Desktops Essentials	Sí	Sí	Sí	El servicio usa la región de Citrix Cloud.
Web App Firewall	Sí	Sí	No (usa la región de EE. UU.)	
Workspace Environment Management; Citrix Optimization Pack	Sí	Sí	Sí	
Servicios de red	Sí	No (usa la región de EE. UU.)	No (usa la región de EE. UU.)	

Servicio	EE. UU.	UE	Asia-Pacífico Sur	Notas
License Usage Insights (solo CSP)	Todas las regiones	Todas las regiones	Todas las regiones	
PoP/Nodos de acceso de Citrix Gateway Service	Varios nodos globales; tráfico redirigido según sea necesario para garantizar la mejor experiencia posible	Varios nodos globales; tráfico redirigido según sea necesario para garantizar la mejor experiencia posible	Varios nodos globales; tráfico redirigido según sea necesario para garantizar la mejor experiencia posible	Puede configurar las ubicaciones de recursos para permitir que el tráfico de usuarios se redirija a regiones específicas. Para obtener más información, consulte Redirección de geolocalización: Technical Preview

> **Nota:**
>
> Es posible que ciertos servicios regionales se entreguen con derechos a servicios de componentes no regionales que se indican en otra parte de la tabla anterior, y se pueden utilizar si el cliente lo quiere.
>
> Citrix Cloud Services utiliza la región designada por el cliente para almacenar contenido y registros de los clientes, excepto en el caso de determinados registros recopilados por subprocesadores de Citrix o para los que es necesario un almacenamiento no regional para el rendimiento del servicio, lo que incluye la asistencia o la solución de problemas, la supervisión del rendimiento, la seguridad, la auditoría y permitir la autenticación entre regiones (por ejemplo, cuando un ingeniero de asistencia situado la UE necesita acceder a un entorno situado en EE. UU.). Se puede acceder al contenido y a los registros de los clientes a nivel global según sea necesario para prestar los servicios.

Para obtener más información acerca de los datos que almacenan servicios concretos, consulte el apartado Visión general técnica de la seguridad referente a cada servicio.

Incorporación con baja interacción de instancias de NetScaler Console mediante Console Advisory Connect

Como parte de Incorporación con baja interacción de instancias de NetScaler Console basada en Console Advisory Connect:

- Si ya es cliente de Citrix Cloud, el arrendatario del servicio Console se crea en la misma región geográfica que seleccionó al crear su cuenta de Citrix Cloud.
- Si no es cliente de Citrix Cloud, se hace referencia a la dirección mencionada para ese cliente en el portal de Citrix.com. Se crea un arrendatario del servicio Console como marcador de posición en la región geográfica correspondiente a esta dirección de referencia. Si decide incorporar Citrix Cloud en el futuro, se creará un nuevo arrendatario del servicio Console en la misma región que seleccionó al crear su cuenta de Citrix Cloud. Además, se migran los datos del marcador de posición "arrendatario del servicio Console"al nuevo arrendatario del servicio Console.

Ubicaciones del servicio de Endpoint Management

Puede seleccionar una de las siguientes ubicaciones del servicio de Endpoint Management desde su región de origen:

- Este de EE. UU.
- Oeste de EE. UU.
- UE Occidental
- Sureste de Asia
- Sídney

Ubicaciones de Secure Internet Access Service

El tráfico se redirige a las siguientes ubicaciones de Secure Internet Access Service en función de la disponibilidad y la proximidad del usuario final a fin de garantizar la mejor experiencia posible.

Norteamérica

- Sterling, VA, EE. UU.
- Toronto, Canadá
- Los Ángeles, CA, EE. UU.
- Irvine, CA, EE. UU.
- Seattle, WA, EE. UU.
- Denver, CO, EE. UU.
- Charlotte, NC, CA, EE. UU.

- Dallas, TX, EE. UU.
- Allen, TX, EE. UU.
- Miami, FL, EE. UU.
- Chicago, IL, EE. UU.
- Nueva York, NY, EE. UU.
- Boston, MA, EE. UU.
- Vancouver, Canadá

Sudamérica

- Querétaro, México
- Sao Paulo, Brasil
- Buenos Aires, Argentina
- Bogotá, Colombia

Asia-Pacífico

- Perth, Australia
- Sídney, Australia
- Tokio, Japón
- Singapur, Singapur
- Mumbai, India
- Delhi, India

África

Johannesburgo, Sudáfrica

Medio Oriente

- Dubái, Emiratos Árabes Unidos
- Estambul, Turquía

Europa Occidental

- Londres, Reino Unido
- Manchester, Reino Unido
- Fráncfort, Alemania

- Düsseldorf, Alemania
- Mannheim, Alemania
- París, Francia

Europa

- Helsinki, Finlandia
- Ámsterdam, Países Bajos
- Estocolmo, Suecia
- Varsovia, Polonia
- Madrid, España
- Sofía, Bulgaria
- Zúrich, Suiza
- Milán, Italia

Puntos de presencia de Secure Private Access

Para obtener una lista de los puntos de presencia (PoP) que utiliza Secure Private Access para garantizar la continuidad y la calidad de servicio a los clientes, consulte ¿Cuáles son las ubicaciones PoP de acceso privado seguro? en la documentación de Secure Private Access Service.

Otras plataformas de la nube de Citrix

Además de Citrix Cloud, Citrix ofrece otras nubes aisladas y separadas de Citrix Cloud.

Citrix Cloud Government

Citrix Cloud Government permite a las agencias gubernamentales de los Estados Unidos y a otros clientes del sector público en los Estados Unidos utilizar los servicios en la nube de Citrix de acuerdo con los requisitos normativos. Citrix Cloud Government es una zona geográfica dentro de la cual Citrix opera, almacena y replica servicios y datos para la entrega de los servicios de Citrix Cloud Government. Citrix puede utilizar varias nubes públicas o privadas ubicadas en uno o varios estados dentro de los Estados Unidos para proporcionar los servicios.

Citrix Cloud Government y los servicios ofrecidos solo están disponibles en la región de Estados Unidos.

Para obtener más información, consulte la documentación del producto Citrix Cloud Government.

Citrix Cloud Japan

Citrix Cloud Japan permite a los clientes japoneses utilizar ciertos servicios de Citrix Cloud en un entorno dedicado administrado por Citrix. Citrix Cloud Japan y los servicios ofrecidos solo están disponibles en Japón.

Para obtener más información, consulte la documentación del producto Citrix Cloud Japan.

Guía de implementación segura para la plataforma Citrix Cloud

July 2, 2024

La Guía de implementación segura para Citrix Cloud ofrece una visión general de las prácticas recomendadas al utilizar Citrix Cloud, y describe la información que Citrix Cloud recopila y administra.

Información técnica general sobre la seguridad para los servicios

Consulte los siguientes artículos para obtener más información sobre la seguridad de los datos en los servicios de Citrix Cloud:

- Información técnica general sobre la seguridad de Analytics
- Información técnica general sobre la seguridad de Endpoint Management
- Información técnica general sobre la seguridad de Remote Browser Isolation
- Información técnica general sobre la seguridad de Citrix DaaS
- Información técnica general sobre la seguridad de Citrix DaaS Standard para Azure

Instrucciones para administradores

- Use contraseñas seguras y cámbielas con regularidad.
- Todos los administradores de una cuenta de cliente pueden agregar y quitar otros administradores. Solo los administradores de confianza deben tener acceso a Citrix Cloud.
- Los administradores de un cliente tienen, de forma predeterminada, acceso completo a todos los servicios. Algunos servicios ofrecen la posibilidad de restringir el acceso de un administrador. Para obtener más información, consulte la documentación de cada servicio.
- La autenticación de dos factores para los administradores de Citrix Cloud se logra mediante el proveedor de identidades predeterminado de Citrix. Cuando los administradores se registran en Citrix Cloud o se les invita a una cuenta de Citrix Cloud, deben inscribirse en la autenticación de varios factores (MFA). Si un cliente usa Microsoft Azure para autenticar a los administradores

de Citrix Cloud, la autenticación de varios factores se puede configurar como se describe en Configuración de Azure AD Multi-Factor Authentication en el sitio web de Microsoft.
- De forma predeterminada, Citrix Cloud finaliza automáticamente las sesiones de administrador transcurridas 24 horas, independientemente de la actividad de la consola. Este tiempo de espera no se puede cambiar.
- Las cuentas de administrador pueden estar asociadas a un máximo de 100 cuentas de clientes. Si un administrador necesita administrar más de 100 cuentas de clientes, debe crear una cuenta de administrador independiente con una dirección de correo electrónico diferente para administrar cuentas de clientes adicionales. También se pueden quitar como administrador de las cuentas de clientes que ya no necesiten administrar.

Cumplimiento de normas para las contraseñas

Citrix Cloud solicita a los administradores que cambien sus contraseñas si se da una de las siguientes condiciones:

- La contraseña actual no se ha utilizado para iniciar sesión durante más de 60 días.
- La contraseña actual se ha incluido en una base de datos conocida de contraseñas desveladas.

Las nuevas contraseñas deben cumplir todos los criterios siguientes:

- Longitud mínima de 8 caracteres (128 caracteres como máximo)
- Incluir al menos una letra mayúscula y una minúscula
- Incluir al menos un número
- Incluir al menos un carácter especial: ! @ # $ % ^ * ? + =-

Reglas para cambiar contraseñas:

- La contraseña actual no se puede utilizar como la nueva contraseña.
- Las 5 contraseñas anteriores no se pueden reutilizar.
- La nueva contraseña no puede parecerse al nombre de usuario de la cuenta.
- La nueva contraseña no debe figurar en una base de datos conocida de contraseñas desveladas. Citrix Cloud utiliza una lista que proporciona https://haveibeenpwned.com/ para determinar si las contraseñas nuevas infringen esta condición.

Cifrado y administración de claves

El plano de control de Citrix Cloud no almacena información confidencial de los clientes. En su lugar, Citrix Cloud obtiene la información (tal como las contraseñas de administrador) a demanda (pidiéndoselo explícitamente al administrador).

Para los datos en reposo, el almacenamiento de Citrix Cloud se cifra mediante claves AES de 256 bits o más. Citrix administra estas claves.

Para los datos en proceso, Citrix utiliza los estándares TLS 1.2 del sector con los conjuntos de cifrado más robustos. Los clientes no pueden controlar el certificado TLS que se usa, ya que Citrix Cloud está alojado en el dominio cloud.com, que es propiedad de Citrix. Para acceder a Citrix Cloud, los clientes deben usar un explorador que funcione con TLS 1.2 y deben haber aceptado conjuntos de cifrado configurados.

- Si accede al plano de control de Citrix Cloud desde Windows Server 2016, Windows Server 2019 o Windows Server 2022, se recomiendan los siguientes cifrados seguros: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- Si accede al plano de control de Citrix Cloud desde Windows Server 2012 R2, los cifrados seguros no están disponibles, por lo que deberán utilizarse los siguientes cifrados: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Para obtener más información sobre cómo se protegen los datos en los servicios de Citrix Cloud, consulte Citrix Cloud Services Data Protection Overview en el sitio web de Citrix.

Para obtener más información sobre el cifrado y la administración de claves dentro de cada servicio en la nube, consulte la documentación de los correspondientes servicios.

Para obtener más información sobre la configuración de TLS 1.2, consulte los siguientes artículos:

- Exigir el uso de TLS 1.2 en máquinas cliente: CTX245765, Error: "Se cerró la conexión subyacente: Ocurrió un error inesperado en un envío."al consultar el dispositivo de punto final OData de Monitoring Service
- Update and configure the .NET Framework to support TLS 1.2 en el sitio web de documentación de Microsoft.

Soberanía de los datos

El plano de control de Citrix Cloud está alojado en los Estados Unidos de América, en la Unión Europea y en Australia. Los clientes no tienen control sobre ello.

El cliente posee y administra las ubicaciones de recursos que utiliza con Citrix Cloud. Las ubicaciones de recursos pueden crearse en cualquier centro de datos, infraestructura de nube, ubicación o región geográfica que quiera el cliente. Todos los datos importantes de la empresa (por ejemplo, documentos, hojas de cálculo, etc.) se almacenan en las ubicaciones de recursos y están bajo el control del cliente.

Otros servicios pueden tener una opción para almacenar datos en diferentes regiones. Consulte el

tema titulado Consideraciones geográficas o los temas de Visión general técnica de la seguridad (indicados al comienzo de este artículo) para cada servicio.

Detección de problemas de seguridad

El sitio Web status.cloud.com permite ver con claridad los problemas de seguridad que tienen un impacto constante en el cliente. El sitio registra información del estado y del tiempo de actividad. Existe la opción de suscribirse a actualizaciones de la plataforma o de servicios individuales.

Citrix Cloud Connector

Instalar Cloud Connector

Por razones de seguridad y rendimiento, Citrix recomienda no instalar el software de Cloud Connector en un controlador de dominio.

Además, Citrix recomienda encarecidamente que las máquinas donde se ha instalado el software de Cloud Connector estén dentro de la red privada del cliente, no en la zona desmilitarizada (DMZ). Para ver las instrucciones de instalación de Cloud Connector y los requisitos de sistema y de red, consulte Citrix Cloud Connector.

Configurar Cloud Connector

El cliente es el responsable de mantener las máquinas donde está instalado Cloud Connector al día con las actualizaciones de seguridad de Windows necesarias.

Los clientes pueden usar un antivirus junto a Cloud Connector. Citrix realiza pruebas con McAfee VirusScan Enterprise + AntiSpyware Enterprise 8.8. Citrix ofrece asistencia a los clientes que utilicen otros productos antivirus estándares del sector.

En el Active Directory (AD) del cliente, Citrix recomienda encarecidamente que la cuenta de la máquina de Cloud Connector tenga restricción de acceso de solo lectura. Esta es la configuración predeterminada en Active Directory. Asimismo, el cliente puede habilitar la captura de registros y auditoría de AD en la cuenta de la máquina de Cloud Connector para supervisar toda la actividad de acceso de AD.

Iniciar sesión en la máquina que aloja Cloud Connector

Cloud Connector permite que la información confidencial de seguridad pase a otros componentes de la plataforma en los servicios de Citrix Cloud, pero también almacena la siguiente información confidencial:

- Claves de servicio para comunicarse con Citrix Cloud
- Credenciales del servicio de hipervisor para la administración de energía en Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service)

Esta información confidencial se cifra mediante la API de protección de datos (DPAPI) en el servidor Windows que aloja Cloud Connector. Citrix recomienda encarecidamente permitir únicamente el inicio de sesión en las máquinas que alojan Cloud Connector a los administradores con privilegios superiores (por ejemplo, para realizar operaciones de mantenimiento). En general, un administrador no necesita iniciar sesión en estas máquinas para administrar los productos Citrix. En ese sentido, Cloud Connector se autoadministra.

No permita que los usuarios finales inicien sesión en las máquinas que alojan Cloud Connector.

Instalar otro software en máquinas de Cloud Connector

Los clientes pueden instalar software antivirus y herramientas de hipervisor (si se ha instalado en una máquina virtual) en las máquinas donde está instalado Cloud Connector. No obstante, Citrix recomienda a los clientes no instalar ningún otro software en esas máquinas. Cualquier otro software puede crear vectores de ataque de seguridad y puede reducir la seguridad global de la solución Citrix Cloud.

Configurar puertos de entrada y salida

Cloud Connector requiere que el puerto de salida 443 esté abierto con acceso a Internet. Citrix recomienda encarecidamente que Cloud Connector no tenga puertos de entrada accesibles desde Internet.

Los clientes pueden ubicar Cloud Connector detrás de un proxy Web para supervisar sus comunicaciones salientes de Internet. No obstante, ese proxy Web debe admitir comunicación cifrada por SSL/TLS.

Cloud Connector puede tener otros puertos de salida con acceso a Internet. Cloud Connector negocia en una amplia gama de puertos para optimizar el ancho de banda y el rendimiento de la red si hay otros puertos disponibles.

Cloud Connector debe tener una amplia gama de puertos de entrada y salida abiertos dentro de la red interna. En la siguiente tabla, se muestra el conjunto de base de puertos abiertos necesarios.

Puerto del cliente	Puerto del servidor	Servicio
49152 -65535/UDP	123/UDP	W32Time
49152 -65535/TCP	135/TCP	Asignador de extremos de RPC

Puerto del cliente	Puerto del servidor	Servicio
49152 -65535/TCP	464/TCP/UDP	Cambio de contraseña de Kerberos
49152 -65535/TCP	49152-65535/TCP	RPC para LSA, SAM, Netlogon (*)
49152-65535/TCP/UDP	389/TCP/UDP	LDAP
49152 -65535/TCP	3268/TCP	LDAP GC
53, 49152-65535/TCP/UDP	53/TCP/UDP	DNS
49152 -65535/TCP	49152 -65535/TCP	FRS RPC (*)
49152-65535/TCP/UDP	88/TCP/UDP	Kerberos
49152-65535/TCP/UDP	445/TCP	SMB

Cloud Connector usa la firma y el sellado de LDAP para proteger las conexiones al controlador de dominio. Esto significa que no se requiere LDAP por SSL (LDAPS). Para obtener más información sobre la firma de LDAP, consulte How to enable LDAP signing in Windows Server y Microsoft Guidance for Enabling LDAP Channel Binding and LDAP Signing.

Cada uno de los servicios utilizados dentro de Citrix Cloud ampliará la lista de los puertos abiertos necesarios. Para obtener más información, consulte los recursos siguientes:

- Visión general técnica de la seguridad para cada servicio (artículos indicados al comienzo de este tema)
- Requisitos de conectividad con Internet de los servicios de Citrix Cloud
- Requisitos de puertos del servicio Console
- Requisitos de puertos de Endpoint Management

Supervisar la comunicación de salida

Cloud Connector se comunica con el exterior vía Internet por el puerto 443; se conecta tanto a servidores Citrix Cloud como a servidores Microsoft Azure Service Bus.

Cloud Connector se comunica con los controladores de dominio en la red local que están dentro del bosque de Active Directory donde residen las máquinas que alojan Cloud Connector.

Durante el funcionamiento normal, Cloud Connector solo se comunica con los controladores de dominio en los dominios que no están inhabilitados en la página **Administración de acceso e identidad** de la interfaz de usuario de Citrix Cloud.

Cada servicio de Citrix Cloud ampliará la lista de servidores y recursos internos con los que Cloud Connector puede ponerse en contacto durante las operaciones habituales. Además, los clientes no

pueden controlar los datos que Cloud Connector envía a Citrix. Para obtener más información acerca de los recursos internos de los servicios y los datos que se envían a Citrix, consulte lo siguiente:

- Visión general técnica de la seguridad para cada servicio (artículos indicados al comienzo de este tema)
- Requisitos de conectividad con Internet de los servicios de Citrix Cloud

Ver los registros de Cloud Connector

Toda información relevante o acción asociada a un administrador está disponible en el Registro de eventos de Windows de la máquina de Cloud Connector.

Revise los registros de instalación para Cloud Connector en los siguientes directorios:

- %AppData%\Local\Temp\CitrixLogs\CloudServicesSetup
- %windir%\Temp\CitrixLogs\CloudServicesSetup

Los registros de lo que Cloud Connector envía a la nube se encuentran en: %ProgramData%\Citrix\WorkspaceCloud

Los registros del directorio "WorkspaceCloud\Logs"se eliminan cuando superan el tamaño especificado. El administrador puede controlar este tamaño máximo ajustando el valor de clave de Registro HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CloudServices\AgentAdministration\MaximumLogSpaceMegabytes.

Configuración de SSL/TLS

El servidor Windows Server que aloja el Cloud Connector debe tener habilitados los cifrados que se indican en Cifrado y administración de claves.

Cloud Connector debe confiar en la entidad de certificación (CA) que utilizan los certificados SSL/TLS de Citrix Cloud y los certificados SSL/TLS de Microsoft Azure Service Bus. Citrix y Microsoft pueden cambiar los certificados y las entidades de certificación en el futuro, pero siempre usan entidades de certificación que constan en la lista de publicadores de confianza estándar de Windows.

Cada servicio de Citrix Cloud podría presentar requisitos diferentes de configuración de SSL. Para obtener más información, consulte los artículos de Visión general técnica de la seguridad para cada servicio (artículos indicados al comienzo de este tema).

Cumplimiento de directrices de seguridad

Para garantizar el cumplimiento de las directrices de seguridad, Cloud Connector se autoadministra. No inhabilite los reinicios de sistema ni ponga otras restricciones a Cloud Connector. Esas acciones impedirían que Cloud Connector se actualice cuando haya una actualización importante.

El cliente no necesita tomar ninguna otra medida para reaccionar frente a los problemas de seguridad que surjan. Cloud Connector aplica automáticamente las correcciones de seguridad.

Dispositivo Citrix Connector para Cloud Services

Instalar el Connector Appliance

El Connector Appliance está alojado en un hipervisor. Este hipervisor debe estar en su red privada y no en la zona desmilitarizada.

Compruebe que el Connector Appliance esté dentro de un firewall que bloquea el acceso de forma predeterminada. Utilice una lista de permitidos para permitir solamente el tráfico esperado procedente del Connector Appliance.

Compruebe que los hipervisores que alojan los Connector Appliances están instalados con las actualizaciones de seguridad más recientes.

Para ver las instrucciones de instalación del Connector Appliance y los requisitos de sistema y de red, consulte Connector Appliance para Cloud Services.

Iniciar sesión en el hipervisor que aloja un Connector Appliance

El Connector Appliance contiene una clave de servicio para comunicarse con Citrix Cloud. Solamente debe permitir que los administradores con privilegios superiores inicien sesión en un hipervisor que aloje el Connector Appliance (por ejemplo, para realizar operaciones de mantenimiento). En general, un administrador no necesita iniciar sesión en estos hipervisores para administrar los productos Citrix. El Connector Appliance se administra automáticamente.

Configurar puertos de entrada y salida

El Connector Appliance requiere que el puerto de salida 443 esté abierto con acceso a Internet. Citrix recomienda encarecidamente que el Connector Appliance no tenga puertos de entrada accesibles desde Internet.

Puede ubicar el Connector Appliance detrás de un proxy web para supervisar sus comunicaciones salientes de Internet. No obstante, ese proxy Web debe admitir comunicación cifrada por SSL/TLS.

El Connector Appliance puede tener otros puertos de salida con acceso a Internet. El Connector Appliance negocia en una amplia gama de puertos para optimizar el ancho de banda y el rendimiento de la red si hay otros puertos disponibles.

El Connector Appliance debe tener una amplia gama de puertos de entrada y salida abiertos dentro de la red interna. En la siguiente tabla, se muestra el conjunto de base de puertos abiertos necesarios.

Dirección de la conexión	Puerto del Connector Appliance	Puerto externo	Servicio
Entrante	443/TCP	Cualquiera	IU web local
Saliente	49152-65535/UDP	123/UDP	NTP
Saliente	53, 49152-65535/TCP/UDP	53/TCP/UDP	DNS
Saliente	67/UDP	68/UDP	DHCP y difusión
Saliente	49152 -65535/UDP	123/UDP	W32Time
Saliente	49152 -65535/TCP	464/TCP/UDP	Cambio de contraseña de Kerberos
Saliente	49152-65535/TCP/UDP	389/TCP/UDP	LDAP
Saliente	49152 -65535/TCP	3268/TCP	LDAP GC
Saliente	49152-65535/TCP/UDP	88/TCP/UDP	Kerberos
Saliente	49152-65535/TCP/UDP	445/TCP	SMB
Saliente	137/UDP	137/UDP	Servicio de nombres de NetBIOS
Saliente	138/UDP	138/UDP	Datagrama de NetBIOS
Saliente	139/TCP	139/TCP	Sesión de NetBIOS

Cada uno de los servicios utilizados dentro de Citrix Cloud ampliará la lista de los puertos abiertos necesarios. Para obtener más información, consulte los recursos siguientes:

- Visión general técnica de la seguridad para cada servicio (artículos indicados al comienzo de este tema)
- Requisitos del sistema y de conectividad de los servicios de Citrix Cloud

Supervisar la comunicación de salida

El Connector Appliance se comunica con el exterior vía Internet por el puerto 443 con los servidores de Citrix Cloud.

Cada servicio de Citrix Cloud ampliará la lista de servidores y recursos internos con los que el Connector Appliance puede ponerse en contacto durante las operaciones habituales. Además, los clientes no pueden controlar los datos que el Connector Appliance envía a Citrix. Para obtener más información acerca de los recursos internos de los servicios y los datos que se envían a Citrix, consulte lo siguiente:

- Visión general técnica de la seguridad para cada servicio (artículos indicados al comienzo de este tema)
- Requisitos del sistema y de conectividad de los servicios de Citrix Cloud

Ver los registros del Connector Appliance

Puede descargar un informe de diagnóstico sobre el Connector Appliance que incluye varios archivos de registro. Para obtener más información sobre cómo obtener este informe, consulte Connector Appliance para Cloud Services.

Configuración de SSL/TLS

El Connector Appliance no necesita ninguna configuración especial de SSL/TLS.

El Connector Appliance confía en la entidad de certificación (CA) utilizada por los certificados SSL/TLS de Citrix Cloud. Es posible que, en el futuro, Citrix cambie certificados y entidades de certificación, pero siempre utilizará entidades en las que el Connector Appliance confía.

Cada servicio de Citrix Cloud podría presentar requisitos diferentes de configuración de SSL. Para obtener más información, consulte los artículos de Visión general técnica de la seguridad para cada servicio (artículos indicados al comienzo de este tema).

Cumplimiento de directrices de seguridad

Para garantizar el cumplimiento de directrices de seguridad, el Connector Appliance se autoadministra y usted no puede iniciar sesión en él a través de la consola.

No es necesario tomar ninguna otra medida para reaccionar frente a los problemas de seguridad del conector. El Connector Appliance aplica automáticamente las correcciones de seguridad.

Compruebe que los hipervisores que alojan los Connector Appliances están instalados con las actualizaciones de seguridad más recientes.

En su Active Directory (AD), recomendamos que la cuenta de la máquina del Connector Appliance esté restringida al acceso de solo lectura. Esta es la configuración predeterminada en Active Directory. Asimismo, el cliente puede habilitar la captura de registros y auditoría de AD en la cuenta de la máquina del Connector Appliance para supervisar toda la actividad de acceso de AD.

Instrucciones para la gestión de cuentas en situación de riesgo

- Audite la lista de administradores de Citrix Cloud y quite los que no sean de confianza.
- Inhabilite las cuentas en peligro que haya en el directorio Active Directory de su empresa.

- Póngase en contacto con Citrix y solicite rotar los secretos de autorización almacenados para todos los Cloud Connectors del cliente. Según la gravedad de la infracción, realice lo siguiente:
  - **Riesgo leve:** Citrix puede rotar los secretos con regularidad. Los Cloud Connectors siguen funcionando normalmente. Los secretos de autorización antiguos dejan de ser válidos entre 2 y 4 semanas después. Supervise Cloud Connector durante este tiempo para asegurarse de que no haya operaciones inesperadas.
  - **Riesgo serio continuo:** Citrix puede revocar todos los secretos antiguos. Los Cloud Connectors existentes ya no funcionarán. Para reanudar el funcionamiento normal, el cliente debe desinstalar y volver a instalar Cloud Connector en todas las máquinas afectadas.

Crear una cuenta de Citrix Cloud

December 12, 2023

En este artículo, se explica el proceso de creación de una cuenta de Citrix Cloud y se completan las tareas necesarias para incorporar cuentas correctamente.

Los clientes que ya tienen una relación con Citrix y que son nuevos en los servicios de la nube de Citrix pueden utilizar las tareas de este artículo para completar el proceso de incorporación.

Proceso de registro para nuevos clientes de Citrix

Si es la primera vez que usa Citrix y Citrix Cloud, contacte con Citrix para crear una cuenta de Citrix para su empresa. Use uno de estos métodos de contacto:

- Ponerse en contacto con el Servicio de atención al cliente de Citrix.
- Contacte con un Citrix Partner o un agente de Ventas de Citrix de su zona.

Cuando contacte con Citrix, podrá analizar sus necesidades empresariales con un representante de Citrix. El representante le ayudará a completar el proceso de registro y le proporcionará sus credenciales de inicio de sesión de Citrix.

Tras recibir las credenciales de su cuenta de Citrix, puede usar las tareas de este artículo para iniciar sesión y empezar a utilizar Citrix Cloud.

¿Qué es una cuenta de Citrix?

Una cuenta de Citrix, también conocida como cuenta Citrix.com o cuenta My Citrix, le permite administrar el acceso a las licencias que ha adquirido. Su cuenta de Citrix usa un ID de organización (OrgID)

como identificador exclusivo. Para acceder a su cuenta de Citrix, inicie sesión en https://www.citrix.com con un nombre de usuario (también conocido como credencial de inicio de sesión web) o su dirección de correo electrónico, si hay alguna vinculada a su cuenta.

> **Importante:**
>
> El nombre de usuario corresponde a una única cuenta de Citrix, pero una dirección de correo electrónico puede abarcar varias cuentas de Citrix.

¿Qué es un OrgID?

El ID de organización (OrgID) es un identificador asignado exclusivamente a su cuenta de Citrix. Su OrgID está asociado a una dirección física, que generalmente es el domicilio comercial de su empresa. Las empresas suelen tener un único OrgID. Sin embargo, en algunos casos (por ejemplo, si la empresa tiene varias sucursales o múltiples departamentos que gestionan activos de manera independiente), Citrix puede permitir que una misma empresa tenga varios OrgID.

Citrix hace una limpieza rutinaria de ciertos OrgID, y fusiona los ID duplicados en algunos casos. Si su empresa tiene varios OrgID que usted quiere fusionar con un OrgID válido y activo, puede contactar con el equipo de asistencia al cliente (Citrix Customer Support) para indicarle los OrgID que quiere fusionar.

> **Nota:**
>
> Las empresas tienen ya los OrgID configurados en función de cómo quieren administrar sus activos, de modo que si no está seguro de cuál es el OrgID que necesita usar, o de cuántos OrgID dispone, contacte con el departamento de TI o con el administrador de Citrix de su empresa. Si necesita ayuda, contacte con el Servicio de atención al cliente de Citrix en https://www.citrix.com/support/ para localizar su OrgID.

¿Qué es una cuenta de Citrix Cloud?

Una cuenta de Citrix Cloud permite usar uno o varios servicios de Citrix Cloud para entregar aplicaciones y datos de manera segura. Las cuenta de Citrix Cloud se identifican con un ID de cliente y se asocian a un OrgID. Un OrgID se puede asociar a varios ID de cliente de Citrix Cloud, pero un ID de cliente solo se puede asociar a un OrgID.

Es importante usar la cuenta correcta de Citrix Cloud, en función de cómo haya configurado su organización los OrgID, para que sus compras y su acceso de administrador puedan continuar usando los mismos OrgID. Por ejemplo, si el departamento de Diseño de una empresa que usa el OrgID 1234 ha estado usando el producto Virtual Apps and Desktops en entorno local y ahora quiere probar Citrix Cloud, uno de los administradores de OrgID 1234 puede registrarse en Citrix Cloud con ese OrgID mediante las credenciales de una cuenta de Citrix o mediante una dirección de correo electrónico

asociada a dicho OrgID. Cuando la empresa decide adquirir una suscripción a Citrix DaaS, el pedido se puede realizar correctamente en OrgID 1234.

> **Importante:**
>
> Los usuarios que tienen acceso a una cuenta de Citrix concreta no tienen acceso automático a la cuenta de Citrix Cloud asociada al OrgID de esa cuenta de Citrix. El acceso a Citrix Cloud permite realizar acciones que pueden afectar a los servicios, por lo que es importante controlar quién tiene acceso a la cuenta de Citrix Cloud.

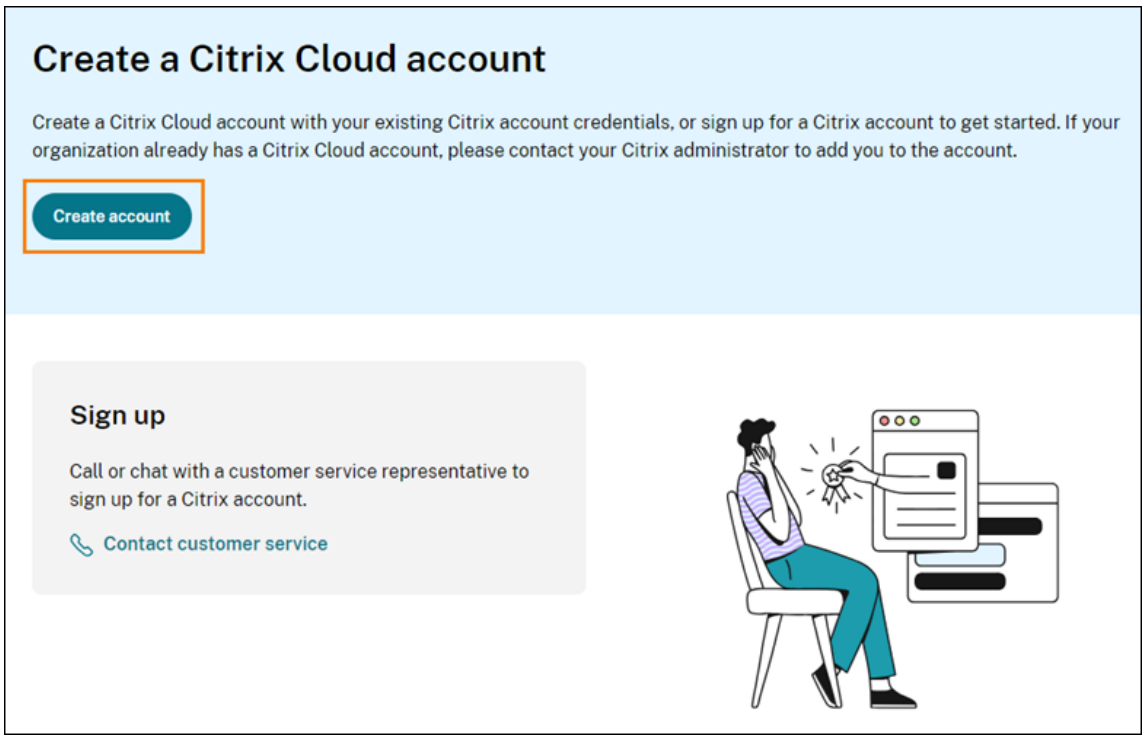
Autenticación de varios factores

Para mantener su cuenta de Citrix Cloud segura, Citrix exige que todos los clientes se inscriban en la autenticación de varios factores (MFA). Para inscribirse, solo necesita un dispositivo, como un equipo o dispositivo móvil, y una aplicación de autenticación instalada, como Citrix SSO. Si no es posible usar un dispositivo con una aplicación de autenticación, puede usar una dirección de correo electrónico en su lugar.

Si aún no se ha inscrito en MFA, Citrix le pedirá que se inscriba cuando inicie sesión con las credenciales de su cuenta de Citrix. Para ver los requisitos y las instrucciones, consulte el Paso 2: Configurar la autenticación de varios factores en este artículo.

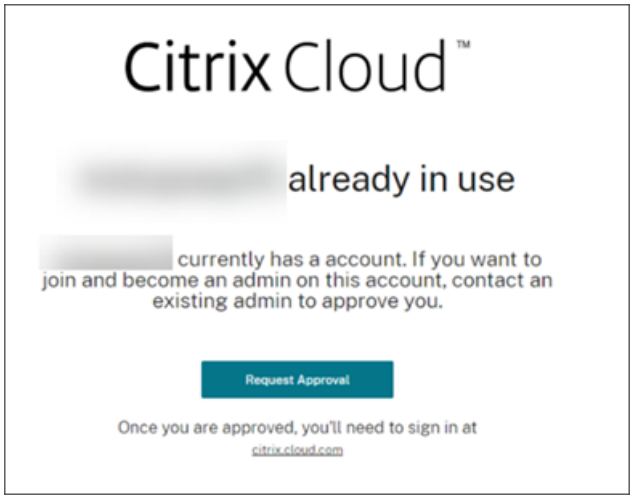
Paso 1: Visitar el sitio web de Citrix Cloud

1. Con un explorador web, diríjase a https://onboarding.cloud.com.
2. Seleccione **Crear cuenta**.



3. Introduzca su nombre de usuario y contraseña o la dirección de correo electrónico y contraseña asociados a su cuenta de Citrix.com.

¿Qué sucede si la cuenta ya está en uso?



Si aparece un mensaje que indica que ya se está utilizando una cuenta de Citrix Cloud para su organización, significa que otro administrador de su cuenta de Citrix ya ha creado la cuenta de Citrix Cloud. Antes de poder acceder a la cuenta, un administrador debe invitarlo a ser administrador, incluso si ya es miembro de la cuenta de Citrix.

Una cuenta de Citrix Cloud ofrece a los administradores un control mucho mayor sobre los servicios,

y por eso, el primer administrador que crea la cuenta de Citrix Cloud debe conceder explícitamente el acceso a otro administrador, incluso aunque dicho administrador ya sea miembro de la cuenta de Citrix.

Para solicitar una invitación para unirse a la cuenta de Citrix Cloud, seleccione **Solicitar aprobación**. Todos los administradores de la cuenta reciben un correo electrónico en el que se les notifica su solicitud. Si los administradores ya no están en su organización, contacte con Citrix Support.

Cuando un administrador recibe su solicitud de aprobación, le invita a convertirse en administrador, tal y como se describe en Invitar a administradores individuales.

Cuando reciba el correo electrónico de invitación, haga clic en el enlace **Iniciar sesión** para aceptar la invitación. Cuando el explorador se abra, Citrix Cloud le pedirá que cree una contraseña e inicie sesión en la cuenta de Citrix Cloud.

Paso 2: Configurar la autenticación de varios factores

Si no se ha inscrito en la autenticación MFA, Citrix Cloud le pedirá que se inscriba antes de iniciar sesión. Puede inscribirse en la autenticación MFA mediante una aplicación de autenticación (opción recomendada) o con su dirección de correo electrónico.

> **Notas:**
>
> - Solo los administradores del proveedor de identidades Citrix pueden configurar la autenticación MFA a través de Citrix Cloud. Si utiliza Azure AD para administrar administradores de Citrix Cloud, puede configurar la autenticación MFA a través de Azure Portal. Para obtener más información, consulte Configure Azure Multi-Factor Authentication settings en el sitio web de Microsoft.
> - Tras completar el proceso de configuración, la autenticación MFA se utilizará para todas las organizaciones de clientes a las que pertenezca en Citrix Cloud. La autenticación MFA no puede inhabilitarse una vez completado el proceso de configuración.
> - Solo puede inscribir un dispositivo. Si inscribe otro dispositivo más adelante, Citrix Cloud elimina la inscripción del dispositivo actual y la sustituye por la del nuevo dispositivo. Para obtener más información, consulte Administrar el método de autenticación MFA principal.

Correo electrónico como método de autenticación

Si no puede usar una aplicación de autenticación para acceder a Citrix Cloud, la autenticación MFA mediante correo electrónico es una alternativa práctica. Sin embargo, Citrix recomienda encarecidamente que tome precauciones para garantizar un acceso seguro a su dirección de correo electrónico.

Requisitos de la autenticación MFA

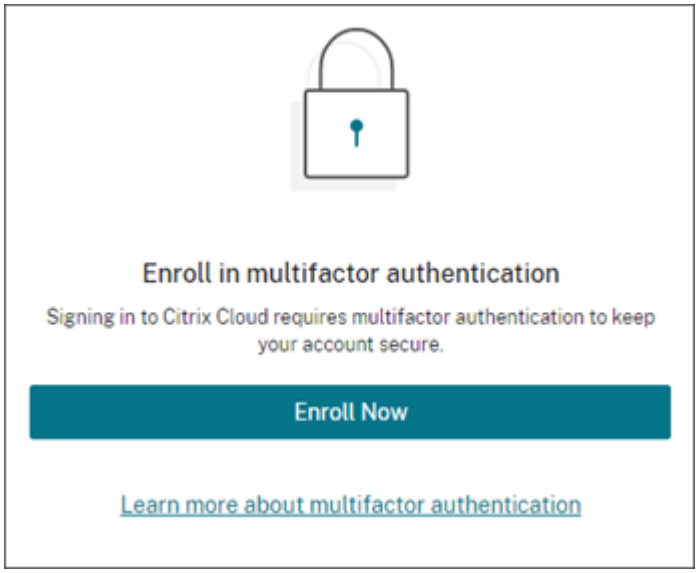
Para configurar la MFA con una aplicación de autenticación, debe instalar una aplicación que siga el estándar de contraseña temporal de un solo uso en su dispositivo, como un smartphone o un equipo de escritorio. Según el dispositivo que vaya a inscribir, es posible que la aplicación necesite acceder a la cámara de tal dispositivo para escanear un código QR. Si el dispositivo no tiene cámara, puede introducir la clave que proporciona Citrix Cloud.

Para configurar la autenticación MFA con una dirección de correo electrónico, debe utilizar una dirección de correo electrónico que cumpla los siguientes requisitos:

- La dirección de correo electrónico es distinta de la dirección de correo electrónico que utiliza para su cuenta de Citrix.
- La dirección de correo electrónico es una dirección a la que puede acceder para recibir correos electrónicos de verificación de Citrix.

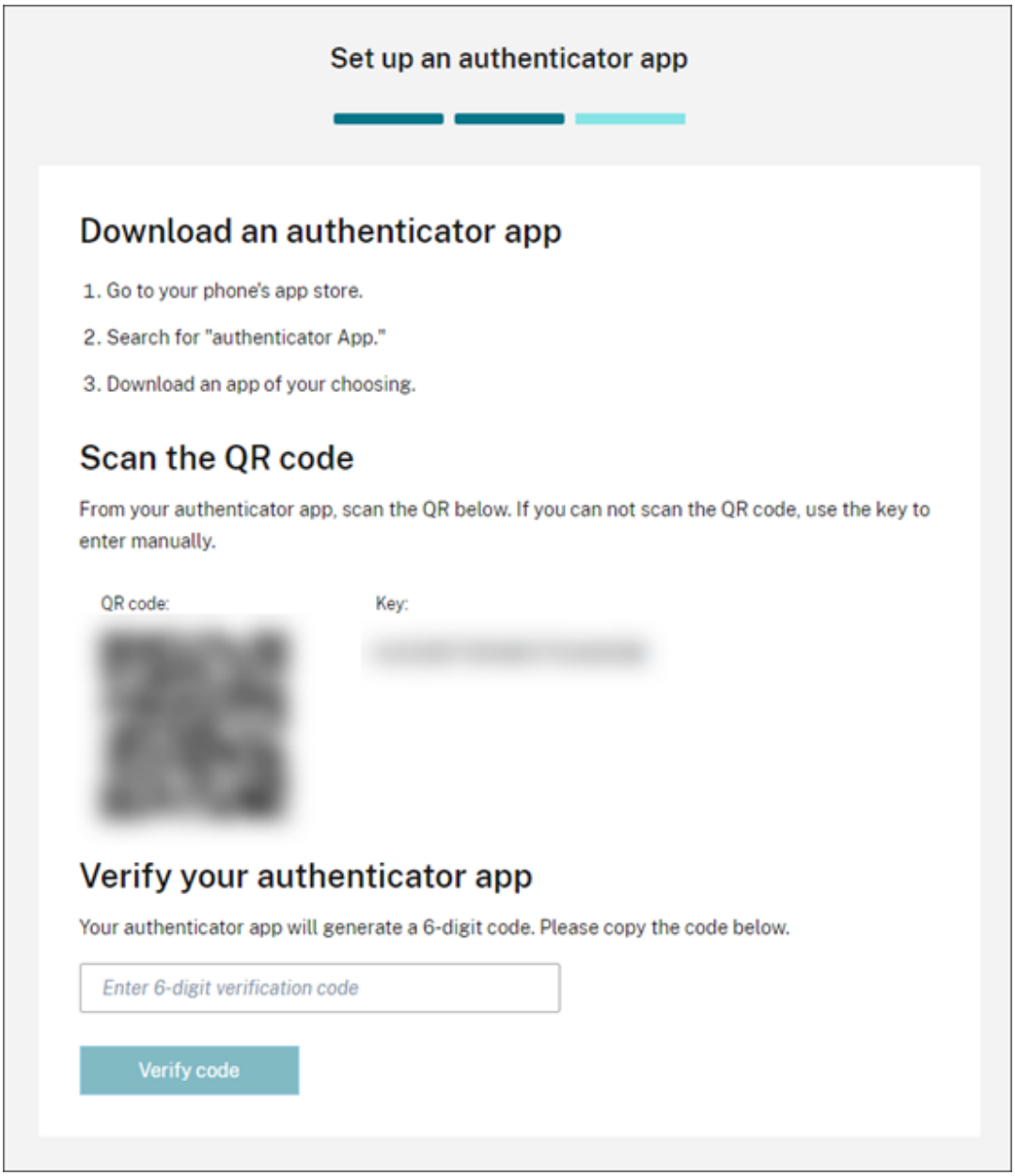
Inscribirse en la autenticación de varios factores

1. Cuando se le pida que se inscriba en la autenticación MFA, seleccione **Inscribirse**.



2. Cuando se le solicite, introduzca su dirección de correo electrónico y seleccione **Enviar correo**. Citrix Cloud le enviará un correo electrónico con un código de verificación.
3. Introduzca el código de verificación del correo electrónico y la contraseña de su cuenta de Citrix. Haga clic en **Verificar y continuar**.
4. Seleccione el método de autenticación que quiera usar, ya sea una aplicación de autenticación o una dirección de correo electrónico.
5. Si seleccionó **Aplicación de autenticación**, siga estos pasos:

a) Desde la aplicación de autenticación, escanee el código QR o introduzca la clave manualmente. La aplicación de autenticación muestra una entrada para Citrix Cloud y genera un código de 6 dígitos.



b) En **Compruebe su aplicación de autenticación**, introduzca el código de la aplicación de autenticación y seleccione **Verificar código**.

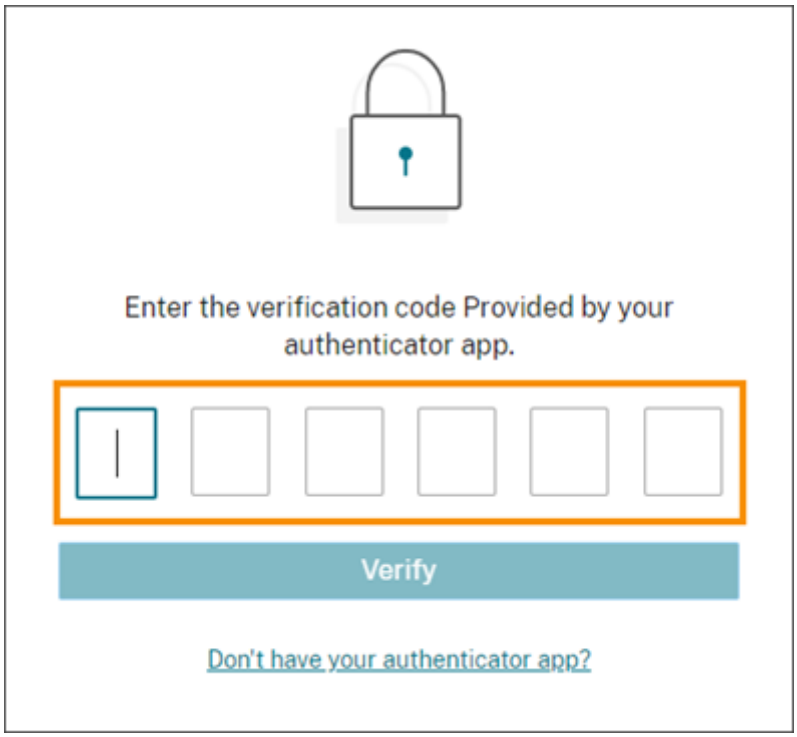
6. Haga clic en **Siguiente: Métodos de recuperación**.
7. Seleccione **Agregar teléfono de recuperación** e introduzca un número de teléfono de recuperación que Citrix Support pueda usar para contactar con usted y verificar su identidad. Citrix recomienda usar un número de teléfono fijo. Cuando haya terminado, haga clic en **Guardar**

número de teléfono de recuperación.

8. Seleccione **Siguiente**.
9. Seleccione **Agregar correo de recuperación** e introduzca una dirección de correo electrónico a la que pueda acceder y que sea diferente de la que usa con Citrix Cloud. Citrix usa esta dirección para enviarle un código de verificación a fin de verificar su identidad.

   Si no tiene otra dirección de correo electrónico, seleccione **¿No tiene ninguna dirección de correo de recuperación?** para generar, en su lugar, una lista de códigos de reserva. No se recomiendan los códigos de reserva porque se pueden perder fácilmente. Si elige esta opción, descargue los códigos y guárdelos en un lugar donde pueda acceder a ellos cuando los necesite.
10. Para completar la inscripción, seleccione **Finalizar**.

La próxima vez que inicie sesión con sus credenciales de administrador de Citrix Cloud, Citrix Cloud le pedirá el código de verificación procedente del método de autenticación MFA elegido.



Administrar su inscripción en la autenticación MFA

Para cambiar el dispositivo, cambiar a otro método de MFA o actualizar los métodos de recuperación, consulte estos artículos:

- Administrar el método de autenticación MFA principal
- Administrar los métodos de recuperación de la autenticación MFA

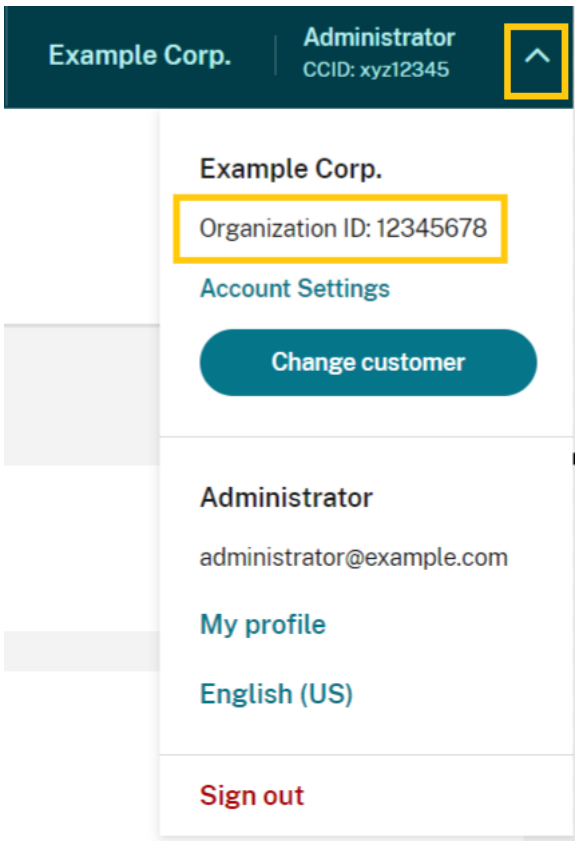
Paso 3: Verificar su OrgID

Antes de empezar a usar Citrix Cloud, tómese un momento para verificar su OrgID.

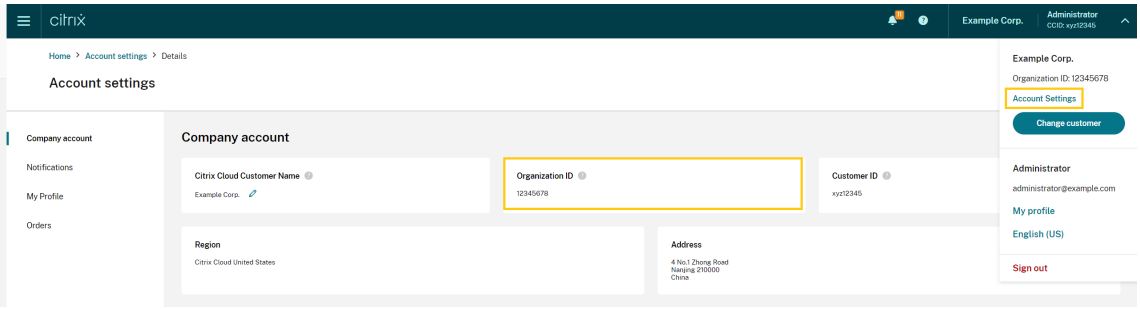
Compruebe que el OrgID de la cuenta coincide con el OrgID que usa para hacer pedidos. Una de las ventajas de Citrix Cloud es que si usted prueba un servicio y luego decide adquirirlo, todas las configuraciones que haya realizado durante la prueba se conservarán en el servicio adquirido, ya que la compra tiene lugar en la misma cuenta. Por lo tanto, se ahorrará trabajo cuando decida adquirir servicios si se registra con el OrgID correcto para las pruebas de servicio.

Su OrgID aparece en las siguientes ubicaciones de la consola de administración:

- En el menú situado debajo del nombre del cliente. Haga clic en el nombre del cliente en la esquina superior derecha para ver el menú.



- En la página **Parámetros de cuenta**. Seleccione **Parámetros de cuenta** en el menú del cliente.



Siguientes pasos

Tras la incorporación, puede pasar a estas tareas:

- Agregar un proveedor de identidades para autenticar a administradores o usuarios de espacios de trabajo.
- Agregar administradores a su cuenta de Citrix Cloud. Aunque los demás administradores tengan ya acceso a su cuenta de Citrix en Citrix.com, necesita agregarlos igualmente a su cuenta de Citrix Cloud.
- Solicitar pruebas de servicios de Cloud. Las pruebas están diseñadas para que usted pueda utilizarlas con su propia infraestructura (ya sea en sus instalaciones locales o nube pública), sus aplicaciones y su propia implementación de Microsoft Active Directory.

Más información

- Curso de Citrix: Fundamentals of Citrix Cloud
- Canal de Citrix en YouTube: Citrix Cloud Master Class

Verificar el correo electrónico de Citrix Cloud

October 19, 2023

De vez en cuando, Citrix puede pedirle que verifique su cuenta de Citrix Cloud. A continuación, se indican algunas de las razones por las que puede pedírsele que verifique su correo electrónico:

- Lleva un tiempo sin iniciar sesión en Citrix Cloud.
- Ha cambiado la dirección de correo electrónico.
- Ha agregado un nuevo administrador a su cuenta de Citrix Cloud.
- Debido a las actualizaciones del sistema de seguridad de Citrix Cloud, debe verificar de nuevo su cuenta de Citrix Cloud.

Preguntas frecuentes

¿Con qué frecuencia se me pedirá la verificación?

La verificación de su cuenta se hace una vez. Citrix Cloud no pedirá una verificación cada vez que usted inicie sesión o cuando cambie algo de su cuenta. Si se le pide que verifique la cuenta con frecuencia, póngase en contacto con el servicio de asistencia técnica de Citrix.

¿Ha pasado algo con mi cuenta?

No. Cuando se le solicita que verifique su cuenta, no significa que haya problemas con su cuenta ni con ninguno de los servicios de Citrix Cloud. Es simplemente una manera para Citrix de mantener la información segura.

No he recibido ningún correo electrónico de verificación. ¿Qué debo hacer?

Siga estos pasos:

1. Busque en su bandeja de entrada un correo electrónico de verificación de "Citrix". El correo electrónico de verificación caduca en 24 horas. Para recibir otro correo electrónico de verificación, inicie sesión de nuevo en Citrix Cloud. Es un proceso único para cada inicio de sesión web.
2. Si no está en la bandeja de entrada, consulte las carpetas. Si un filtro o una regla de correo no deseado ha movido el mensaje, es posible que esté en la carpeta de papelera o correo no deseado. Compruebe los firewalls.
3. Asegúrese de que se trata de la cuenta de correo electrónico correcta. Citrix envía el mensaje de verificación a la dirección de correo electrónico que conste en ese momento en su cuenta. Por lo general, esta es la dirección de correo electrónico con la que se registró en Citrix Cloud, o aquella con la que se le invitó a unirse a la cuenta de Citrix Cloud.
4. Para confirmar que la dirección de correo electrónico registrada es válida, inicie sesión en su cuenta de Citrix en https://www.citrix.com/account. Si la dirección de correo electrónico no es válida, actualice su dirección de correo electrónico e inicie sesión de nuevo en Citrix Cloud para recibir otro correo electrónico de verificación. Para obtener más información, consulte CTX126336 o CTX130452 en el Knowledge Center de Citrix Support.
5. Si aún no ha recibido ningún correo electrónico de verificación, contacte con Citrix Support para abrir un caso de asistencia. En el caso de sitios de formación (consulte **Partner Services Delivery > eLearning > Citrix Training**), abra un caso con el equipo de formación para que lo investigue más a fondo. Para abrir un caso, solicite **General Support** en la página Contact Us.

Si verificó correctamente su dirección de correo electrónico, pero sigue sin poder iniciar sesión en Citrix Cloud, consulte Troubleshooting login issues on Citrix websites.

Contactar con Citrix Support

Si tiene algún otro problema que no se ha indicado aquí, póngase en contacto con Citrix Support para que abran un caso de asistencia.

Conectarse a Citrix Cloud

April 5, 2024

La conexión de los recursos a Citrix Cloud implica la implementación de conectores en el entorno y la creación de *ubicaciones de recursos*.

Las ubicaciones de recursos contienen los recursos necesarios para prestar servicios de nube a los suscriptores. Estos recursos se administran desde la consola de Citrix Cloud. Las ubicaciones de recursos contienen distintos recursos dependiendo de los servicios de Citrix Cloud que se estén utilizando y de los servicios que se quiera proporcionar a los suscriptores.

Para crear una ubicación de recursos, instale al menos dos conectores en su dominio. Según los servicios de la nube que utilice, se necesitan Cloud Connectors o Connector Appliances para habilitar la comunicación entre Citrix Cloud y sus recursos. Para obtener más información sobre la implementación de conectores, consulte estos artículos:

- Detalles técnicos de Cloud Connector
- Connector Appliance para Cloud Services

Tipos de recursos

Las ubicaciones de recursos contienen distintos recursos dependiendo de los servicios de Citrix Cloud que se estén utilizando y de los servicios que se quiera proporcionar a los suscriptores. Los diferentes recursos utilizan diferentes tipos de conector. La mayoría de los servicios utilizan el Citrix Cloud Connector, pero algunos servicios específicos necesitan un Connector Appliance.

Servicios que usan Citrix Cloud Connector

- **Citrix DaaS** (antes denominado Citrix Virtual Apps and Desktops Service) necesita el Cloud Connector para publicar aplicaciones y escritorios y aprovisionar catálogos de máquinas en las ubicaciones de recursos. Para obtener información general sobre cómo Cloud Connector se comunica con este servicio, consulte el diagrama de Citrix DaaS en Citrix Tech Zone.

- **Citrix DaaS Standard para Azure** (antes denominado Citrix Virtual Apps and Desktops Standard para Azure) necesita el Cloud Connector para entregar aplicaciones y escritorios virtuales de Azure alojados en Citrix desde máquinas multisesión.
- **Endpoint Management** necesita Cloud Connector para administrar directivas de aplicaciones y dispositivos, y para entregar aplicaciones a los usuarios.

Servicios que utilizan Connector Appliances

- **Image Portability Service** simplifica la administración de imágenes en distintas plataformas. Esta funcionalidad es útil para administrar imágenes entre una ubicación de recursos local y otra en una nube pública. Las API de REST de Citrix Virtual Apps and Desktops sirven para automatizar la administración de recursos en un sitio de Citrix Virtual Apps and Desktops.

  El flujo de trabajo de Image Portability comienza cuando usa Citrix Cloud para iniciar la migración de una imagen desde su ubicación local a su suscripción de nube pública. Después de preparar la imagen, Image Portability Service le ayuda a transferir la imagen a su suscripción en la nube pública y a prepararla para su ejecución. Por último, Citrix Provisioning o Machine Creation Services aprovisionan la imagen en su suscripción a la nube pública.

  Para obtener más información, consulte Image Portability Service.

- **Citrix Secure Private Access** permite a los administradores proporcionar una experiencia coherente que integre el inicio de sesión único (SSO), el acceso remoto y la inspección de contenido en una única solución para el control de acceso de extremo a extremo. Para obtener más información, consulte Secure Private Access con Connector Appliance.

Es posible que haya otros servicios en Tech Preview que también dependan de Connector Appliance.

Ubicación de los recursos

Las ubicaciones de recursos se encuentran allí donde residen los recursos, ya sea una nube privada o una nube pública, una sucursal de oficina, o un centro de datos. Si ya tiene recursos en su propia nube o centro de datos, sus recursos permanecen donde están. No es necesario moverlos a ningún otro lugar para usarlos con Citrix Cloud.

La elección de la ubicación puede verse condicionada por estos factores:

- Proximidad a los suscriptores
- Proximidad a los datos
- Requisitos de escala
- Atributos de seguridad

Ejemplo de la implementación de una ubicación de recursos

- Cree su primera ubicación de recursos en su centro de datos para la oficina principal, en función de los suscriptores y las aplicaciones que necesitan situarse cerca de los datos.
- Agregue una segunda ubicación de recursos para usuarios globales en una nube pública. O crear ubicaciones de recursos independientes en cada una de las sucursales para entregar aplicaciones que funcionan mejor cuando se sitúan cerca de los trabajadores de las sucursales.
- Agregue una ubicación de recursos adicional en una red diferente que proporcione aplicaciones de carácter restringido. Esto restringe la visibilidad de otros recursos y suscriptores sin la necesidad de ajustar las otras ubicaciones de recursos.

Límites de ubicación de recursos

Puede tener un máximo de 50 ubicaciones de recursos en su cuenta de Citrix Cloud.

Restricciones de nombres

Los nombres que asigne a las ubicaciones de recursos deben cumplir las siguientes restricciones:

- Longitud máxima: 64 caracteres
- Caracteres no permitidos:
  - #, $, %, ^, &, ?, +
  - Llaves: [], { }
  - Barras verticales (|)
  - Símbolo menor que (<) y símbolo mayor que (>)
  - Barras diagonales (/, \)
- No debe coincidir con ningún otro nombre de ubicación de recursos (sin distinción entre mayúsculas y minúsculas) de la cuenta de Citrix Cloud

Ubicaciones de recursos principales

Una ubicación de recursos principal es una ubicación de recursos que se designa como "preferida" para ciertas comunicaciones entre el dominio y Citrix Cloud. Los Cloud Connectors de una ubicación de recursos principal se utilizan para los inicios de sesión de usuario y las operaciones de aprovisionamiento. La ubicación de recursos que se seleccione como "principal"debe tener Cloud Connectors que ofrezcan una conectividad con el dominio y un rendimiento óptimos. Esto permite que los usuarios inicien sesiones rápidamente en Citrix Cloud.

Para obtener más información, consulte [Seleccionar una ubicación de recursos principal].(/en-us/citrix-cloud/citrix-cloud-management/identity-access-management/primary-resource-locations.html)

Citrix Cloud Connector

April 5, 2024

Citrix Cloud Connector es un componente de Citrix que funciona como un canal de comunicaciones entre Citrix Cloud y las ubicaciones de los recursos, lo que permite administrar la nube sin necesidad de una configuración compleja de la red o de la infraestructura. Con él, se evitan muchos problemas a la hora de administrar la infraestructura de entrega de recursos. Le permite a usted administrar y centrarse en los recursos que ofrecen más valor a sus usuarios.

> **Nota:**
>
> No instale el SDK de PowerShell remoto en una máquina con Citrix Cloud Connector. Se puede instalar en cualquier máquina unida a un dominio dentro de la misma ubicación de recursos.
>
> Citrix recomienda no ejecutar los cmdlets de este SDK en los Cloud Connectors. El funcionamiento del SDK no concierne a los Cloud Connectors.

Servicios que requieren Cloud Connector

Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service) necesita el Cloud Connector. Para obtener información general sobre cómo Cloud Connector se comunica con el servicio, consulte el diagrama de Citrix DaaS en Citrix Tech Zone.

Citrix Endpoint Management necesita el Cloud Connector para la conectividad de la empresa con el servicio Endpoint Management. Remote Browser Isolation Service requiere Cloud Connector para aplicaciones web externas autenticadas.

Funciones de Cloud Connector

- **Active Directory (AD):** Habilita la administración de AD, lo que permite el uso de bosques y dominios de AD dentro de las ubicaciones de recursos. Elimina la necesidad de agregar más relaciones de confianza de AD.
- **Publicación de aplicaciones y escritorios virtuales:** Habilita la publicación de Citrix DaaS desde recursos situados en las ubicaciones de recursos.
- **Endpoint Management:** Habilita un entorno de administración de dispositivos móviles (MDM) y administración de aplicaciones móviles (MAM) para administrar directivas de dispositivo y aplicación, así como para entregar aplicaciones a los usuarios.
- **Aprovisionamiento de catálogos de máquinas**: Permite el aprovisionamiento de máquinas directamente en las ubicaciones de recursos.

> **Nota:**
>
> Aunque siga operativo, su funcionalidad puede verse reducida durante el período en que la conexión con Citrix Cloud no esté disponible. Puede supervisar el estado de Cloud Connector desde la consola de Citrix Cloud.

Comunicación de Cloud Connector

Cloud Connector autentica y cifra toda la comunicación entre Citrix Cloud y las ubicaciones de recursos. Una vez instalado, el Cloud Connector inicia la comunicación con Citrix Cloud a través de una conexión saliente. Todas las conexiones se establecen desde Cloud Connector hacia la nube mediante el puerto HTTPS estándar (443) y el protocolo TCP. No se aceptan conexiones entrantes.

Administración de carga y disponibilidad de Cloud Connector

Para administrar la carga de los conectores y conseguir una disponibilidad continuada de estos, instale varios Cloud Connectors en cada una de las ubicaciones de recursos. Se necesitan al menos dos Cloud Connectors en cada ubicación de recursos para garantizar una conexión de alta disponibilidad con Citrix Cloud. Si un Cloud Connector deja de estar disponible durante un tiempo, los demás Cloud Connectors pueden mantener la conexión. Puesto que los Cloud Connectors no guardan información de interacciones previas (son "stateless"), la carga puede distribuirse entre todos los conectores disponibles. No es necesario configurar la función de equilibrio de carga. Es completamente automática.

Mientras haya otro Cloud Connector disponible, no se perderá la comunicación con Citrix Cloud. Siempre que sea posible, la conexión del usuario final con los recursos de la ubicación de recursos no depende de una conexión con Citrix Cloud. Con esto, la ubicación de recursos puede ofrecer a los usuarios acceso a sus recursos, independientemente de si hay una conexión con Citrix Cloud.

Dónde obtener el Cloud Connector

Puede descargar el software de Cloud Connector desde dentro de Citrix Cloud.

1. Inicie sesión en Citrix Cloud.
2. En el menú de la esquina superior izquierda, seleccione **Ubicaciones de recursos**.
3. Si no tiene ubicaciones de recursos, haga clic en **Descargar** en la página Ubicaciones de recursos. Cuando se le solicite, guarde el archivo **cwcconnector.exe**.
4. Si dispone de una ubicación de recursos, pero no tiene Cloud Connectors instalados en ella, haga clic en la barra de Cloud Connectors y haga clic en **Descargar**. Cuando se le solicite, guarde el archivo **cwcconnector.exe**.

¿Cuántos Cloud Connectors necesito?

Se necesitan al menos dos (2) Cloud Connectors para crear una conexión de alta disponibilidad entre Citrix Cloud y la ubicación de recursos. Según su entorno y las cargas de trabajo que admita, es posible que necesite más Cloud Connectors para garantizar una experiencia de usuario óptima.

Como práctica recomendada, Citrix recomienda usar el modelo de redundancia N+1 para determinar la cantidad de Cloud Connectors que debe implementar. Determine la cantidad de Cloud Connectors que necesita en una ubicación de recursos en función del entorno, las cargas de trabajo, la configuración de Active Directory y los servicios. A esta cantidad, agréguele al menos un Cloud Connector más para ofrecer resiliencia. Por ejemplo, si determina que necesita cinco Cloud Connectors, agregue uno más al total e instale seis Cloud Connectors en su ubicación de recursos.

Para obtener pautas adicionales sobre el escalado y el tamaño, consulte Consideraciones sobre la escala y el tamaño de Cloud Connectors.

Dónde instalar el Cloud Connector

Revise Requisitos del sistema para conocer las versiones, las plataformas y los sistemas operativos compatibles.

Instale el Cloud Connector en una máquina dedicada con Windows Server 2016, Windows Server 2019 o Windows Server 2022. Esta máquina debe pertenecer a su dominio y poder comunicarse con los recursos que quiera administrar desde Citrix Cloud.

> **Importante:**
>
> - No instale el Cloud Connector ni ningún otro componente de Citrix en un controlador de dominio de Active Directory.
> - No instale el Cloud Connector en máquinas que ya forman parte de otras implementaciones de Citrix (por ejemplo, los Delivery Controllers de una implementación local de Virtual Apps and Desktops).

Para obtener más información sobre la implementación, consulte estos artículos:

- Casos de implementación de Cloud Connectors en Active Directory
- Instalación de Cloud Connector

Detalles técnicos de Citrix Cloud Connector

July 2, 2024

Citrix Cloud Connector es un componente que establece una conexión entre Citrix Cloud y las ubicaciones de recursos. En este artículo se describen los requisitos y casos de implementación, la compatibilidad con Active Directory y FIPS, y opciones para solucionar problemas.

Requisitos del sistema

Las máquinas que alojan al Cloud Connector deben cumplir estos requisitos: Se necesitan al menos dos Cloud Connectors en cada ubicación de recursos para garantizar la alta disponibilidad. Como práctica recomendada, Citrix recomienda usar el modelo de redundancia N+1 al implementar Cloud Connectors para mantener una conexión de alta disponibilidad con Citrix Cloud.

Requisitos de hardware

Cada Cloud Connector requiere, como mínimo:

- 2 CPU virtuales
- 4 GB de memoria
- 20 GB de espacio en disco

Más memoria de las CPU virtuales permite a Cloud Connector escalar verticalmente para sitios más grandes. Para ver las configuraciones recomendadas, consulte Consideraciones sobre la escala y el tamaño de Cloud Connectors.

Sistemas operativos

Están disponibles los siguientes sistemas operativos:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

El Cloud Connector no es compatible con Windows Server Core.

Requisitos de .NET

Se requiere Microsoft .NET Framework 4.7.2 o una versión posterior. Descargue la versión más reciente en el sitio web de Microsoft.

> **Nota:**
>
> No utilice Microsoft.NET Core con Cloud Connector. Si utiliza .NET Core en lugar de .NET Framework, es posible que falle la instalación de Cloud Connector. Utilice solo .NET Framework con

> Cloud Connector.

Requisitos del servidor

Si utiliza Cloud Connectors con Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service), consulte Consideraciones sobre la escala y el tamaño de Cloud Connectors para ver una guía sobre la configuración de las máquinas.

Los siguientes requisitos se aplican a todas las máquinas en las que está instalado el Cloud Connector:

- Utilice máquinas dedicadas para alojar al Cloud Connector. No instale ningún otro componente en estas máquinas.
- Las máquinas **no** deben configurarse como controladores de dominio de Active Directory. No se admite la instalación del Cloud Connector en un controlador de dominio.
- El reloj del servidor debe estar configurado con la hora UTC correcta.
- Si utiliza el instalador gráfico, debe tener un explorador web instalado y el explorador web del sistema predeterminado configurado.

Guía de Windows Update

Citrix recomienda habilitar Windows Update en todas las máquinas que alojan el Citrix Cloud Connector. El Citrix Cloud Connector comprueba periódicamente, cada cinco minutos, si hay reinicios pendientes, lo que puede deberse a diversos factores, incluidas las actualizaciones de Windows. Cualquier reinicio detectado se ejecuta con prontitud, independientemente de la programación diaria preferida establecida en la ubicación de recursos. Este enfoque proactivo garantiza que el Citrix Cloud Connector no quede en estado de actualización pendiente durante un período prolongado, manteniendo así la estabilidad del sistema.

La plataforma Citrix Cloud administra los reinicios para mantener la disponibilidad, permitiendo que solo se reinicie un Citrix Cloud Connector a la vez. Al configurar Windows Update, asegúrese de que Windows esté configurado para descargar e instalar automáticamente las actualizaciones fuera del horario laboral. Sin embargo, los reinicios automáticos no están permitidos durante al menos cuatro horas para que el Citrix Cloud Connector tenga tiempo suficiente para administrar el proceso de reinicio. Además, puede establecer un mecanismo de reinicio de reserva mediante una directiva de grupo o una herramienta de administración del sistema para situaciones en las que una máquina deba reiniciarse después de una actualización. Para obtener más información, consulte Administrar los reinicios de los dispositivos después de las actualizaciones.

> **Nota:**
>
> - Si el cliente no quiere que su Citrix Cloud Connector se reinicie durante el horario laboral, le

> sugerimos que programe las actualizaciones de Windows en consecuencia fuera de dicho horario.
> - Cada Citrix Cloud Connector tarda aproximadamente 10 minutos en reiniciarse, lo que incluye el tiempo necesario para sincronizarse con Citrix Cloud Platform para garantizar que solo se reinicie un Citrix Cloud Connector en un momento dado. Por lo tanto, la demora mínima recomendada de cuatro horas para los reinicios automáticos, como se mencionó anteriormente, se puede ajustar en consecuencia a una duración mayor o menor en función del número de Citrix Cloud Connectors del arrendatario.

Requisitos de validación de certificados

Binarios y dispositivos de punto final de Cloud Connector cuyos contactos de Cloud Connector están protegidos por certificados X.509 emitidos por una entidad de certificación (CA) empresarial de gran prestigio. La verificación de certificados en la infraestructura de clave pública (PKI) incluye la lista de revocación de certificados (CRL). Cuando un cliente recibe un certificado, el cliente comprueba si confía en la CA que emitió dicho certificado y si este se halla en una lista CRL. Si no está en ninguna lista CRL, el certificado se revoca y no se puede confiar en él, aunque parezca válido.

Los servidores CRL utilizan HTTP en el puerto 80 en lugar de HTTPS en el puerto 443. Los componentes de Cloud Connector, por sí mismos, no se comunican a través del puerto externo 80. La necesidad del puerto externo 80 es un subproducto del proceso de verificación de certificados que realiza el sistema operativo.

Los certificados X.509 se verifican durante la instalación de Cloud Connector. Por lo tanto, todas las máquinas con Cloud Connectors deben estar configuradas para que confíen en estos certificados de modo que el software de Cloud Connector se pueda instalar correctamente.

Los dispositivos de punto final de Citrix Cloud están protegidos por certificados emitidos por DigiCert o por una de las entidades de certificación raíz utilizadas por Azure. Para obtener más información sobre las CA raíz utilizadas por Azure, consulte https://docs.microsoft.com/es-es/azure/security/fundamentals/tls-certificate-changes.

Para validar los certificados, cada máquina con Cloud Connectors debe cumplir los requisitos siguientes:

- El puerto HTTP 80 está abierto para las siguientes direcciones. Este puerto se utiliza durante la instalación de Cloud Connector y durante las comprobaciones periódicas de las listas CRL. Para obtener más información sobre cómo probar la conectividad de las listas CRL y del programa OCSP, consulte https://www.digicert.com/kb/util/utility-test-ocsp-and-crl-access-from-a-server.htm en el sitio web de DigiCert.
  - `http://cacerts.digicert.com/`
  - `http://dl.cacerts.digicert.com/`

  - http://crl3.digicert.com
  - http://crl4.digicert.com
  - http://ocsp.digicert.com
  - http://www.d-trust.net
  - http://root-c3-ca2-2009.ocsp.d-trust.net
  - http://crl.microsoft.com
  - http://oneocsp.microsoft.com
  - http://ocsp.msocsp.com

- La comunicación con las direcciones siguientes está habilitada:

  - https://*.digicert.com

- Están instalados los siguientes certificados raíz:

  - https://cacerts.digicert.com/DigiCertAssuredIDRootCA.crt
  - https://cacerts.digicert.com/DigiCertGlobalRootG2.crt
  - https://cacerts.digicert.com/DigiCertGlobalRootCA.crt
  - https://cacerts.digicert.com/DigiCertTrustedRootG4.crt
  - https://cacerts.digicert.com/BaltimoreCyberTrustRoot.crt
  - https://www.d-trust.net/cgi-bin/D-TRUST_Root_Class_3_CA_2_2009.crt
  - https://www.microsoft.com/pkiops/certs/Microsoft%20RSA%20Root%20Certificate%20Authority%202017.crt
  - https://www.microsoft.com/pkiops/certs/Microsoft%20EV%20ECC%20Root%20Certificate%20Authority%202017.crt
  - https://www.microsoft.com/pkiops/certs/Microsoft%20ECC%20Root%20Certificate%20Authority%202017.crt

- Están instalados los siguientes certificados intermedios:

  - https://cacerts.digicert.com/DigiCertTrustedG4CodeSigningRSA4096SHA384.crt
  - https://cacerts.digicert.com/DigiCertSHA2AssuredIDCodeSigningCA.crt

Si falta algún certificado, el instalador de Cloud Connector lo descargará desde http://cacerts.digicert.com.

Para obtener instrucciones completas para descargar e instalar los certificados, consulte CTX223828.

Citrix DaaS El uso del Cloud Connector para la conectividad con recursos de DaaS requiere la instalación de certificados adicionales y la concesión de acceso a una infraestructura de PKI ampliada.

Cada máquina de Cloud Connector debe cumplir los siguientes requisitos:

- El puerto HTTP 80 está abierto para las siguientes direcciones:
  - crl.*.amazontrust.com
  - ocsp.*.amazontrust.com
  - *.ss2.us
- La comunicación con las direcciones siguientes está habilitada
  - https://*.amazontrust.com
  - https://*.ss2.us
- Están instalados los siguientes certificados raíz:
  - https://www.amazontrust.com/repository/AmazonRootCA1.cer
  - https://www.amazontrust.com/repository/AmazonRootCA2.cer
  - https://www.amazontrust.com/repository/AmazonRootCA3.cer
  - https://www.amazontrust.com/repository/AmazonRootCA4.cer
  - https://www.amazontrust.com/repository/SFSRootCAG2.cer
- Están instalados los siguientes certificados intermedios:
  - https://www.amazontrust.com/repository/G2-RootCA4.orig.cer
  - https://www.amazontrust.com/repository/R3-ServerCA3A.cer
  - https://www.amazontrust.com/repository/SFC2CA-SFSRootCAG2.cer
  - https://www.amazontrust.com/repository/SFC2CA-SFSRootCAG2.v2.cer
  - https://www.amazontrust.com/repository/G2-RootCA1.orig.cer
  - https://www.amazontrust.com/repository/R1-ServerCA1A.cer
  - https://www.amazontrust.com/repository/G2-RootCA3.cer
  - https://www.amazontrust.com/repository/R3-ServerCA3A.orig.cer
  - https://www.amazontrust.com/repository/G2-RootCA2.orig.cer
  - https://www.amazontrust.com/repository/G2-RootCA4.cer
  - https://www.amazontrust.com/repository/R2-ServerCA2A.cer
  - https://www.amazontrust.com/repository/R4-ServerCA4A.cer
  - https://www.amazontrust.com/repository/R1-ServerCA1A.orig.cer
  - https://www.amazontrust.com/repository/G2-RootCA1.cer
  - https://www.amazontrust.com/repository/G2-RootCA2.cer
  - https://www.amazontrust.com/repository/G2-RootCA3.orig.cer
  - https://www.amazontrust.com/repository/R4-ServerCA4A.orig.cer
  - https://www.amazontrust.com/repository/G2-ServerCA0A.cer
  - https://www.amazontrust.com/repository/G2-ServerCA0A.orig.cer

  - https://www.amazontrust.com/repository/SFSRootCA-SFSRootCAG2.cer

Si falta algún certificado, el Cloud Connector lo descargará desde https://www.amazontrust.com

Para obtener instrucciones completas para descargar e instalar los certificados, consulte CTX223828.

Requisitos de Active Directory

- La máquina debe estar unida a un dominio de Active Directory que contenga los recursos y los usuarios que se usan para crear ofertas para los usuarios. Para entornos de varios dominios, consulte Casos de implementación para Cloud Connectors en Active Directory en este artículo.
- Cada bosque de Active Directory que piense usar con Citrix Cloud debe ser siempre accesible desde dos Cloud Connectors.
- Cloud Connector debe poder llegar a los controladores de dominio, tanto en el dominio raíz del bosque como en los dominios que piensa utilizar con Citrix Cloud. Para obtener más información, consulte los siguientes artículos de asistencia de Microsoft:
  - Cómo configurar dominios y relaciones de confianza
  - Sección "Puertos de servicios de sistemas"en Introducción a los servicios y requisitos de puerto de red para Windows
- Use grupos de seguridad universales, en lugar de grupos de seguridad globales. Esta configuración garantiza que la pertenencia a grupos de usuarios pueda obtenerse de cualquier controlador de dominio del bosque.

Requisitos de la red

- Debe estar conectada a una red que pueda contactar con los recursos que se usan en la ubicación de recursos. Para obtener más información, consulte Configurar el proxy y el firewall de Cloud Connector.
- Debe estar conectada a Internet. Para obtener más información, consulte las siguientes secciones de Requisitos del sistema y de conectividad:
  - Requisitos de conectividad con el servicio común de Cloud Connector
  - FQDN permitidos para Cloud Connector

Niveles funcionales admitidos de Active Directory

Citrix Cloud Connector admite los siguientes niveles funcionales de bosque y dominio de Active Directory.

Nivel funcional de bosque	Nivel funcional de dominio	Controladores de dominio admitidos
Windows Server 2008 R2	Windows Server 2008 R2	Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016
Windows Server 2008 R2	Windows Server 2012	Windows Server 2012, Windows Server 2012 R2, Windows Server 2016
Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2012 R2, Windows Server 2016
Windows Server 2008 R2	Windows Server 2016	Windows Server 2016
Windows Server 2012	Windows Server 2012	Windows Server 2012, Windows Server 2012 R2, Windows Server 2016
Windows Server 2012	Windows Server 2012 R2	Windows Server 2012 R2, Windows Server 2016
Windows Server 2012	Windows Server 2016	Windows Server 2016
Windows Server 2012 R2	Windows Server 2012 R2	Windows Server 2012 R2, Windows Server 2016
Windows Server 2012 R2	Windows Server 2016	Windows Server 2016
Windows Server 2016	Windows Server 2016	Windows Server 2016, Windows Server 2019, Windows Server 2022

Soporte para FIPS

Cloud Connector admite actualmente los algoritmos criptográficos validados por FIPS que se utilizan en máquinas habilitadas para FIPS. Ahora bien, solo los admite la versión más reciente del software de Cloud Connector disponible en Citrix Cloud. Si tiene máquinas de Cloud Connector en el entorno (instaladas antes de noviembre de 2018) y quiere habilitar el modo FIPS en ellas, lleve a cabo estas acciones:

1. Desinstale el software de Cloud Connector que hubiera presente en cada máquina de la ubicación de recursos.
2. Habilite el modo FIPS en cada máquina.
3. Instale la versión más reciente del Cloud Connector en cada máquina habilitada para FIPS.

> **Importante:**
>
> - No intente actualizar las instalaciones existentes de Cloud Connector a la versión más reciente. Desinstale siempre el antiguo Cloud Connector primero y, a continuación, instale el más reciente.
> - No habilite el modo FIPS en una máquina que aloja una versión anterior del Cloud Connector. Los Cloud Connectors anteriores a la versión 5.102 no admiten el modo FIPS. Habilitar el modo FIPS en una máquina con un Cloud Connector anterior instalado impide que Citrix Cloud realice actualizaciones periódicas de mantenimiento para el Cloud Connector.

Para obtener instrucciones sobre cómo descargar la versión más reciente del Cloud Connector, consulte Dónde obtener el Cloud Connector.

Servicios instalados de Cloud Connector

En esta sección, se describen los servicios que se instalan con Cloud Connector y sus privilegios de sistema.

Durante la instalación, el archivo ejecutable de Citrix Cloud Connector instala y establece la configuración de servicio necesaria en la configuración predeterminada necesaria para funcionar. Si la configuración predeterminada se modifica manualmente, es posible que Cloud Connector no funcione de la manera prevista. En este caso, la configuración se restablece al estado predeterminado cuando tiene lugar la siguiente actualización de Cloud Connector, suponiendo que los servicios que manejan el proceso de actualización sigan funcionando.

Citrix Cloud Agent System facilita todas las llamadas elevadas necesarias para que los demás servicios de Cloud Connector funcionen y no se comunica directamente en la red. Cuando un servicio en Cloud Connector necesita realizar una acción que requiere permisos del sistema local, lo hace a través de un conjunto predefinido de operaciones que Citrix Cloud Agent System puede realizar.

Nombre del servicio	Descripción	Funciona como
Citrix Cloud Agent System	Gestiona las llamadas al sistema necesarias para los agentes locales. Incluye instalación, reinicios y acceso al registro. Solo le puede llamar Citrix Cloud Services Agent WatchDog.	Sistema local
Citrix Cloud Services Agent WatchDog	Supervisa y actualiza los agentes locales (permanentes).	Servicio de red

Nombre del servicio	Descripción	Funciona como
Citrix Cloud Services Agent Logger	Proporciona un marco de registro de soporte para los servicios de Citrix Cloud Connector.	Servicio de red
Citrix Cloud Services AD Provider	Permite a Citrix Cloud facilitar la administración de los recursos asociados a las cuentas del dominio de Active Directory donde está instalado.	Servicio de red
Citrix Cloud Services Agent Discovery	Permite a Citrix Cloud facilitar la administración de los productos Citrix locales antiguos de XenApp y XenDesktop.	Servicio de red
Citrix Cloud Services Credential Provider	Gestiona el almacenamiento y la recuperación de datos cifrados.	Servicio de red
Citrix Cloud Services WebRelay Provider	Permite que las solicitudes HTTP recibidas desde el servicio WebRelay Cloud puedan ser redirigidas a los servidores web locales.	Servicio de red
Citrix CDF Capture Service	Captura los rastros CDF de todos los productos y componentes configurados.	Servicio de red
Citrix Config Synchronizer Service	Copia la configuración de broker localmente para el modo de alta disponibilidad	Servicio de red
Servicio de intercambio de concesiones de conexión de Citrix	Habilita el intercambio de archivos de concesión de conexiones entre la aplicación Workspace y Cloud Connector para la continuidad del servicio para Workspace	Servicio de red
Citrix High Availability Service (Servicio de alta disponibilidad de Citrix)	Proporciona continuidad del servicio durante la interrupción del sitio central.	Servicio de red

Nombre del servicio	Descripción	Funciona como
Citrix ITSM Adapter Provider	Automatiza el aprovisionamiento y la administración de aplicaciones y escritorios virtuales.	Servicio de red
Citrix NetScaler CloudGateway	Proporciona conectividad a Internet a aplicaciones y escritorios locales sin necesidad de abrir reglas de firewall de entrada ni de implementar componentes en la DMZ.	Servicio de red
Citrix Remote Broker Provider	Permite la comunicación con Broker Service remoto desde los VDA locales y los servidores de StoreFront.	Servicio de red
Citrix Remote HCL Server	Sirve de proxy para las comunicaciones entre el Delivery Controller y los hipervisores.	Servicio de red
Citrix WEM Cloud Authentication Service	Proporciona un servicio de autenticación para que los agentes WEM de Citrix se conecten a servidores de infraestructura en la nube.	Servicio de red
Citrix WEM Cloud Messaging Service	Proporciona servicio para que el servicio en la nube de Citrix WEM reciba mensajes desde servidores de infraestructura en la nube.	Servicio de red

Casos de implementación de Cloud Connectors en Active Directory

Puede usar Cloud Connectors y Connector Appliances para conectarse a los controladores de Active Directory. El tipo de conector que se va a utilizar depende de la implementación.

Para obtener más información sobre el uso de Connector Appliances con Active Directory, consulte Casos de implementación para Connector Appliances en Active Directory.

Instale Cloud Connector dentro de su red interna segura.

Si tiene un solo dominio en un solo bosque, instalar Cloud Connectors en ese dominio es todo lo que necesita para establecer una ubicación de recursos. Si tiene varios dominios en el entorno, debe plantearse dónde instalar Cloud Connectors para que los usuarios puedan acceder a los recursos que ponga a su disposición.

Si la confianza entre los dominios no es del tipo principal/secundario, es posible que tenga que instalar Cloud Connectors para cada dominio o bosque por separado. Es posible que esta configuración sea necesaria para gestionar la enumeración de recursos cuando se utilizan grupos de seguridad para asignar recursos o para los registros de los VDA de cualquiera de los dominios.

> **Nota:**
>
> Estas ubicaciones de recursos forman un plano que tal vez deba repetir en otras ubicaciones físicas, en función de dónde estén alojados sus recursos.

Dominio único en un solo bosque con un único conjunto de Cloud Connectors

En este caso, un solo dominio contiene todos los objetos de usuario y recursos (forest1.local). Un conjunto de Cloud Connectors se implementa en una única ubicación de recursos y se une al dominio forest1.local.

- Relación de confianza: Ninguna, dominio único
- Dominios incluidos en **Administración de acceso e identidad**: forest1.local
- Inicios de sesión de usuario en Citrix Workspace: Se admiten todos los usuarios
- Inicios de sesión de usuario en una implementación local de StoreFront: Se admiten todos los usuarios

> **Nota:**
>
> Aun si tiene una instancia de hipervisor en otro dominio, puede implementar un único conjunto de Cloud Connectors, siempre que la instancia del hipervisor y los Cloud Connectors estén disponibles a través de la misma red. Citrix Cloud usa la conexión de alojamiento y una red disponible para establecer la comunicación con el hipervisor. Por lo tanto, aunque el hipervisor resida en un dominio diferente, no es necesario implementar otro conjunto de Cloud Connectors en ese dominio para garantizar que Citrix Cloud pueda comunicarse con el hipervisor.

Dominios primarios y secundarios en un solo bosque con un único conjunto de Cloud Connectors

En este caso, un dominio primario (forest1.local) y su dominio secundario (user.forest1.local) residen dentro de un solo bosque. El dominio primario actúa como dominio de recursos, mientras que el

dominio secundario es el dominio de usuarios. Un conjunto de Cloud Connectors se implementa en una única ubicación de recursos y se une al dominio forest1.local.

- Relación de confianza: Confianza entre dominios primarios y secundarios
- Dominios incluidos en **Administración de acceso e identidad**: forest1.local, user.forest1.local
- Inicios de sesión de usuario en Citrix Workspace: Se admiten todos los usuarios
- Inicios de sesión de usuario en una implementación local de StoreFront: Se admiten todos los usuarios

> **Nota:**
>
> Puede ser necesario reiniciar los Cloud Connectors para que Citrix Cloud registre el dominio secundario.

Usuarios y recursos en bosques independientes (con relación de confianza) con un único conjunto de Cloud Connectors

En este caso, un bosque (forest1.local) contiene el dominio de recursos, mientras que otro bosque (forest2.local) contiene el dominio de usuarios. Existe una confianza unidireccional en la que el bosque que contiene el dominio de recursos confía en el bosque que contiene el dominio de usuarios. Un conjunto de Cloud Connectors se implementa en una única ubicación de recursos y se une al dominio forest1.local.

- Relación de confianza: Confianza de bosque unidireccional
- Dominios incluidos en **Administración de acceso e identidad**: forest1.local
- Inicios de sesión de usuario en Citrix Workspace: Solo se admiten los usuarios de forest1.local
- Inicios de sesión de usuario en una implementación local de StoreFront: Se admiten todos los usuarios

> **Nota:**
>
> La relación de confianza entre los dos bosques debe permitir que el usuario que se encuentre en el bosque de usuarios inicie sesión en las máquinas del bosque de recursos.

Debido a que los Cloud Connectors no pueden atravesar las barreras que haya en las relaciones de confianza a nivel de bosque, el dominio forest2.local no se muestra en la página **Administración de acceso e identidad** de la consola de Citrix Cloud ni se puede usar en ninguna funcionalidad de la nube. Lo que conlleva las siguientes limitaciones:

- Los recursos solo se pueden publicar para usuarios y grupos ubicados en forest1.local en Citrix Cloud. Sin embargo, si usa almacenes de StoreFront, los usuarios de forest2.local se pueden anidar en los grupos de seguridad de forest1.local para mitigar este problema.
- Citrix Workspace no puede autenticar usuarios desde el dominio forest2.local.

- La consola Supervisar de Citrix DaaS no puede enumerar los usuarios del dominio forest2.local.

Para evitar estas limitaciones, implemente los Cloud Connectors como se describe en Usuarios y recursos en bosques independientes (con relación de confianza) con un conjunto de Cloud Connectors en cada bosque.

Usuarios y recursos en bosques independientes (con relación de confianza) con un único conjunto de Cloud Connectors en cada bosque

En este caso, un bosque (forest1.local) contiene el dominio de recursos, mientras que otro bosque (forest2.local) contiene el dominio de usuarios. Existe una confianza unidireccional en la que el bosque que contiene el dominio de recursos confía en el bosque que contiene el dominio de usuarios. Un conjunto de Cloud Connectors se implementa en el dominio forest1.local y un segundo conjunto se implementa en el dominio forest2.local.

- Relación de confianza: Confianza de bosque unidireccional
- Dominios incluidos en **Administración de acceso e identidad**: forest1.local, forest2.local
- Inicios de sesión de usuario en Citrix Workspace: Se admiten todos los usuarios
- Inicios de sesión de usuario en una implementación local de StoreFront: Se admiten todos los usuarios

En este caso, los Connector Appliances se pueden usar en lugar de Cloud Connectors en bosques de usuarios sin recursos para reducir los costes y los gastos generales de administración, especialmente si hay varios bosques de usuarios. Para obtener más información, consulte Usuarios y recursos en bosques separados (con confianza) con un único conjunto de Connector Appliances para todos los bosques.

Ver el estado de Cloud Connector

En Citrix Cloud, la página "Ubicaciones de recursos"muestra el estado de todos los conectores Cloud Connectors en las ubicaciones de recursos. También puede ver datos de comprobaciones avanzadas de estado de cada Cloud Connector. Para obtener más información, consulte Comprobaciones avanzadas de estado de Cloud Connector.

Mensajes de eventos

Cloud Connector genera ciertos mensajes de eventos que puede ver a través del Visor de eventos de Windows. Si quiere habilitar su software de monitorización preferido para buscar estos mensajes, puede descargarlos en formato de archivo ZIP. La descarga ZIP incluye estos mensajes en los siguientes archivos XML:

- Citrix.CloudServices.Agent.Core.dll.xml (Connector Agent Provider)
- Citrix.CloudServices.AgentWatchDog.Core.dll.xml (Connector AgentWatchDog Provider)

Descargue los mensajes de eventos de Cloud Connector.

Registros de eventos

De forma predeterminada, los registros de eventos se encuentran en el directorio C:\%ProgramData%\Citrix\Works
de la máquina donde se encuentra el Cloud Connector.

Solución de problemas

El primer paso para diagnosticar problemas de Cloud Connector es consultar los registros de eventos y los mensajes de eventos. Si el Cloud Connector no aparece en la ubicación de recursos o aparece como que "no está en contacto", los registros de eventos le proporcionan alguna información inicial.

Conectividad de Cloud Connector

Si Cloud Connector está "desconectado", la utilidad de comprobación de la conectividad de Cloud Connector puede ayudarle a verificar que Cloud Connector puede acceder a Citrix Cloud y sus servicios relacionados.

La utilidad de comprobación de la conectividad de Cloud Connector se ejecuta en la máquina que aloja el Cloud Connector. Si utiliza un servidor proxy en su entorno, la utilidad puede ayudarle a comprobar la conectividad a través del servidor proxy canalizando todas las comprobaciones de conectividad. Si es necesario, la utilidad también puede agregar los sitios de confianza de Citrix que falten a la zona Sitios de confianza de Internet Explorer.

Para obtener más información sobre la descarga y el uso de esta utilidad, consulte CTX260337 en Knowledge Center de Citrix Support.

Instalación

Si Cloud Connector se encuentra en estado de "error", es posible que exista algún problema relacionado con su alojamiento en la máquina. Instale Cloud Connector en una máquina nueva. Si el problema continúa, contacte con Citrix Support, el servicio de asistencia de Citrix. Para solucionar problemas habituales de instalación o de uso de Cloud Connector, consulte CTX221535.

Implementar Cloud Connectors como servidores Secure Ticket Authority

Si usa varios Cloud Connectors como servidores de Secure Ticket Authority (STA) con NetScaler Console, el ID de cada servidor de STA puede mostrarse como **CWSSTA** tanto en la consola de administración de NetScaler como en el archivo ICA para el inicio de aplicaciones y escritorios. Como consecuencia, los tíquets de STA no se redirigen correctamente y el inicio de sesiones falla. Este problema puede producirse si los Cloud Connectors se implementan en cuentas de Citrix Cloud separadas con ID de cliente distintos. En este caso, se produce una discordancia de tíquets entre las distintas cuentas que impide que se creen las sesiones.

Para resolver este problema, asegúrese de que los Cloud Connectors que enlaza como servidores STA pertenecen a la misma cuenta de Citrix Cloud con el mismo ID de cliente. Si necesita dar cabida a varias cuentas de clientes de una misma implementación de NetScaler Console, cree un servidor virtual de Citrix Gateway para cada cuenta. Para obtener más información, consulte los siguientes artículos:

- Creación de servidores virtuales de Citrix Gateway: Crear servidores virtuales
- Configurar Secure Ticket Authority en Citrix Gateway
- Guía de implementación: Migración de Citrix Virtual Apps and Desktops desde el entorno local a Citrix Cloud
- CTX232640: How do I configure Citrix Gateway to use a Cloud Connector as a STA

Configuración del proxy y del firewall de Cloud Connector

April 6, 2024

El Cloud Connector puede conectarse a Internet a través de un servidor proxy web sin autenticar. Tanto el instalador como los servicios que éste instala necesitan conexiones con Citrix Cloud.
El acceso a Internet debe estar disponible en estos dos puntos.

Requisitos de conectividad

Utilice el puerto 443 para el tráfico HTTP, solo de salida. Para obtener una lista de las direcciones de contacto necesarias, consulte los siguientes recursos:

- Requisitos del sistema y de conectividad
- Requisitos de conectividad con el servicio común de Cloud Connector

Las direcciones de contacto necesarias para Citrix Cloud se especifican como nombres de dominio, no direcciones IP. Como las direcciones IP pueden cambiar, el hecho de permitir los nombres de dominio garantiza la estabilidad de la conexión con Citrix Cloud.

Para obtener una lista de los puertos necesarios, consulte Configurar puertos de entrada y salida.

> **Importante:**
>
> - Es posible que, al habilitar la interceptación SSL en algunos proxies, se impida que Cloud Connector se conecte correctamente a Citrix Cloud.
> - La interceptación SSL no se puede realizar en direcciones de Citrix Gateway. Para obtener más información, consulte Requisitos de conectividad de Citrix Gateway Services.
> - La interceptación SSL no debe afectar a la conectividad ni a la estabilidad de la red. Para obtener más información, consulte Citrix Cloud Connector
> - Si usa un proxy, se recomienda que los siguientes flujos de tráfico omitan ese proxy:
>
> – Comunicación entre conectores (por ejemplo, durante eventos de LHC).
> – Comunicación entre conectores y VDA (conexión WCF).
> – Comunicación entre conectores y controladores de dominio (solicitudes de AD).

Además, es importante tener en cuenta que el conector utiliza los parámetros del proxy WinHTTP. Para más detalles sobre los parámetros de configuración, consulte CTX222727.

Comprobar la conectividad de Cloud Connector

La utilidad de comprobación de la conectividad de Cloud Connector ayuda a verificar la conectividad entre Cloud Connector y Citrix Cloud mediante una serie de comprobaciones de conectividad. Si utiliza un servidor proxy en su entorno, la utilidad puede ayudarle a configurar los parámetros del proxy en Cloud Connector y a probar la conectividad a través del servidor proxy. Cuando se configura un servidor proxy, las pruebas de conectividad se canalizan a través del servidor proxy.

> **Nota:**
>
> La utilidad de comprobación de la conectividad de Cloud Connector solo debe usarse con cuentas comerciales de Citrix Cloud. No la use con Citrix Cloud Government ni Citrix Cloud Japan.

Para obtener más información acerca de la descarga y el uso de la utilidad de comprobación de la conectividad de Cloud Connector, consulte CTX260337.

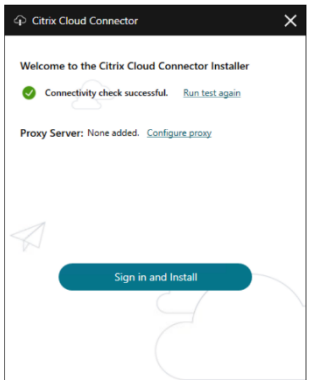
Instalador

El instalador utiliza los parámetros configurados para las conexiones a Internet. Si puede navegar por Internet desde la máquina, el instalador también debería funcionar.

Servicios en ejecución

El servicio en tiempo de ejecución funciona en el contexto de un servicio local. No utiliza los parámetros definidos para el usuario (como se describe más arriba).

Puede configurar los parámetros del proxy durante el proceso de instalación.



Una vez iniciado el instalador, antes de iniciar sesión en Citrix Cloud, haga clic en **Configurar proxy**. Se le pedirá que agregue la información del proxy y las direcciones que omitirán el proxy. Al especificar direcciones que omitirán el proxy, se admiten tanto nombres de dominio completos (FQDN) como direcciones comodín.

> **Nota:**
>
> Si utiliza un servidor proxy, debe utilizar la configuración manual del proxy. No se admite la configuración automática del proxy, tanto si es mediante la detección automática como si es mediante scripts PAC/Setup.

Instalación de Cloud Connector

July 2, 2024

Puede instalar el software de Cloud Connector de forma interactiva o mediante la línea de comandos.

La instalación tiene lugar con los privilegios del usuario que inicia la instalación. El Cloud Connector requiere acceso a la nube para:

- Autenticar al usuario que realiza la instalación
- Validar los permisos del instalador
- Descargar y configurar los servicios del Cloud Connector

Información que revisar antes de la instalación

- Requisitos del sistema: Para preparar las máquinas que alojarán al Cloud Connector.
- La sección Antivirus Exclusions del artículo Endpoint Security and Antivirus Best Practices de Tech Zone: Ofrece las directrices que le ayudarán a determinar el equilibrio adecuado entre la seguridad y el rendimiento de los Cloud Connectors en su entorno. Citrix recomienda encarecidamente revisar estas directrices con los equipos de seguridad y antivirus de su organización y realizar pruebas rigurosas en un entorno de pruebas antes de aplicarlas a un entorno de producción.
- Requisitos del sistema y de conectividad: Para garantizar que todas las máquinas que alojan al Cloud Connector puedan comunicarse con Citrix Cloud.
- Configurar el proxy y el firewall de Cloud Connector: Si está instalando el Cloud Connector en un entorno que tiene un proxy web o reglas estrictas de firewall.
- Consideraciones de escala y tamaño para Cloud Connectors: Ofrece detalles sobre las capacidades máximas probadas y prácticas recomendadas para configurar máquinas que alojarán al Cloud Connector.

Consideraciones y orientación sobre la instalación

- No instale Cloud Connector en un controlador de dominio de Active Directory ni en cualquier otra máquina de importancia crítica para la infraestructura de la ubicación de recursos. El mantenimiento periódico en el Cloud Connector incluye operaciones en la máquina que provocan una interrupción de estos recursos adicionales.
- No descargue ni instale otros productos de Citrix en las máquinas donde aloja Cloud Connector.
- No actualice la versión de componentes individuales del Cloud Connector por separado.
- No descargue ni instale Cloud Connector en máquinas que ya pertenecen a otras implementaciones de productos de Citrix (por ejemplo, los Delivery Controllers de una implementación local de Citrix Virtual Apps and Desktops).
- No actualice la versión de un Cloud Connector ya instalado a una versión más reciente. En su lugar, desinstale el Cloud Connector antiguo e instale el nuevo.
- El programa de instalación de Cloud Connector se descarga desde Citrix Cloud. Por lo tanto, el explorador web debe permitir la descarga de archivos ejecutables.
- Si utiliza el instalador gráfico, debe tener un explorador web instalado y el explorador web del sistema predeterminado configurado.

Guía posterior a la implementación

Después de la instalación, mantenga los Cloud Connectors siempre encendidos para una conexión permanente con Citrix Cloud.

Cambiar el nombre de las máquinas

Tras la instalación, no cambie el nombre de la máquina que aloja el Cloud Connector. Si necesita cambiar el nombre del servidor más adelante, haga estas tareas:

1. Quite la máquina de la ubicación de recursos:
    a) En el menú de Citrix Cloud, seleccione **Ubicaciones de recursos**.
    b) Busque la ubicación de recursos que quiere administrar y seleccione el mosaico de **Cloud Connectors**.
    c) Busque la máquina que quiere administrar y, a continuación, haga clic en el menú de tres puntos. Seleccione **Quitar conector**.
2. Desinstale el software de Cloud Connector.
3. Cambie el nombre de la máquina.
4. Instale la versión más reciente del software de Cloud Connector, tal y como se describe en este artículo.

Mover máquinas a otro dominio

Después de la instalación, no mueva la máquina donde se encuentra Cloud Connector a un dominio diferente. Si necesita unir la máquina a otro dominio más adelante, haga estas tareas:

1. Quite la máquina de la ubicación de recursos.
2. Desinstale el software de Cloud Connector.
3. Separe la máquina de su dominio actual y únala de nuevo al nuevo dominio.
4. Instale la versión más reciente del software de Cloud Connector, tal y como se describe en este artículo.

Consideraciones acerca de las máquinas clonadas

Cada máquina que aloja Cloud Connector debe tener un SID y un ID de conector únicos, para que Citrix Cloud pueda comunicarse con de manera fiable con las máquinas de la ubicación de recursos. Si va a alojar Cloud Connector en varias máquinas de la ubicación de recursos y quiere usar máquinas clonadas, siga estos pasos:

1. Prepare la plantilla de máquina según los requisitos de su entorno.
2. Aprovisione la cantidad de máquinas que vaya a usar como Cloud Connectors.
3. Instale Cloud Connector en cada una de las máquinas, ya sea manualmente, o mediante una instalación silenciosa.

No se admite la instalación de Cloud Connector directamente en una plantilla de máquina (antes de clonar). Si clona una máquina que ya tiene Cloud Connector instalado, los servicios de Cloud Connector no se podrán ejecutar y la máquina no podrá conectarse a Citrix Cloud.

Consideraciones sobre los servicios

En los pasos de instalación de este artículo se describe el proceso de implementación de Cloud Connectors, independientemente del servicio para el que se usen.

Al implementar Cloud Connectors para Citrix DaaS, verifique que los dominios de AD en los que residen los conectores estén activos y no aparezcan como "no utilizado"en la consola de Citrix Cloud. Si especifica un dominio no utilizado durante la configuración del catálogo de máquinas en Citrix DaaS, es posible que se produzca un error. Para obtener más información, consulte Agregar un tipo de recurso o activar un dominio no utilizado en Citrix Cloud en la documentación de producto de Citrix DaaS.

Para obtener más información sobre otros servicios, consulte la documentación del servicio.

Ubicaciones de recursos predeterminadas

Si no tiene ubicaciones de recursos en su cuenta de Citrix Cloud e instala Cloud Connectors en su dominio, la ubicación de recursos que Citrix Cloud crea se convierte en la ubicación de recursos predeterminada. Solo puede tener una ubicación de recursos predeterminada en su cuenta. Si es necesario, puede crear ubicaciones de recursos adicionales en Citrix Cloud y, a continuación, seleccionar la que quiera cuando instale Cloud Connectors en otros dominios.

Como alternativa, puede crear primero las ubicaciones de recursos que necesita en la consola, antes de instalar Cloud Connectors en sus dominios. Durante la instalación, el instalador de Cloud Connector le pide que seleccione la ubicación de recursos que quiere.

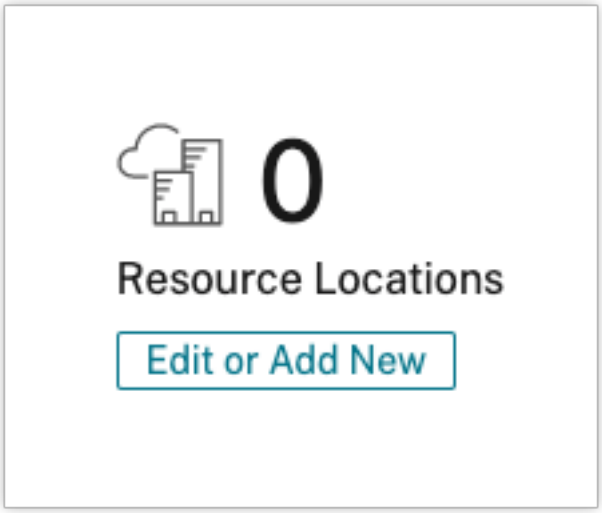
Instalación interactiva

Puede descargar e instalar Cloud Connectors a través de la interfaz gráfica del instalador. Antes de hacerlo, deberá crear una o varias ubicaciones de recursos en la consola de administración de Citrix Cloud donde implementar los Cloud Connectors. Para obtener más información sobre las ubicaciones de recursos, consulte Ubicación de recursos.

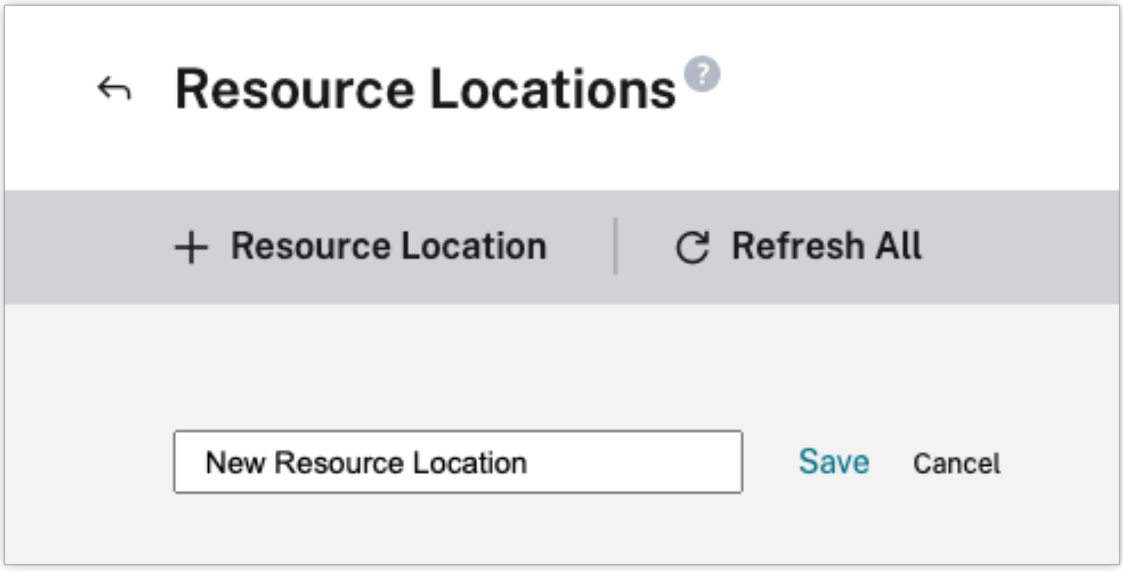
Para crear una ubicación de recursos

1. Inicie sesión como administrador de Windows en el equipo en el que quiere instalar Citrix Cloud Connectors.

2. Vaya a https://citrix.cloud.com e inicie sesión en su cuenta de administrador.
3. En la consola de Citrix Cloud, vaya a **Ubicaciones de recursos** en el menú principal o seleccione **Modificar o agregar** en **Ubicaciones de recursos**, en la parte superior de la página.



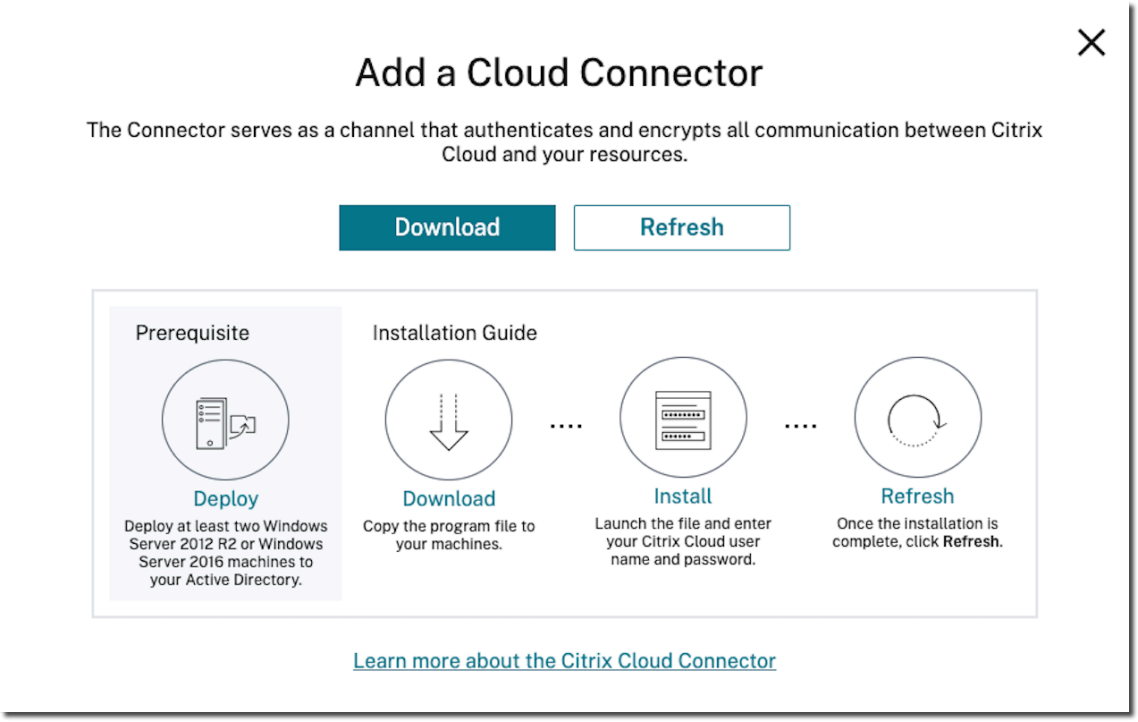
4. En Ubicaciones de recursos, seleccione **+ Ubicación de recursos** en la parte superior de la página y guárdela con un nombre representativo.



Descargar el software Citrix Cloud Connector

1. Busque la ubicación de recursos que quiere administrar y seleccione **+ Cloud Connectors**.

2. Seleccione **Descargar** en la ventana que se abre. Guarde el archivo **cwcconnector.exe** en una ubicación local de la máquina usada como conector.



Instalar el software Citrix Cloud Connector

1. Haga clic con el botón secundario en el archivo instalador **cwcconnector.exe** y seleccione **Ejecutar como administrador**. El instalador realiza una comprobación de conectividad inicial para asegurarse de que se puede conectar a Citrix Cloud.
2. (Opcional) Si fuera necesario, haga clic en **Configurar proxy** para agregar un servidor proxy. Se le pedirá que agregue la información del proxy y las direcciones que omitirán el proxy. Al especificar direcciones que omitirán el proxy, se admiten tanto nombres de dominio completos (FQDN) como direcciones comodín.
3. Haga clic en **Iniciar sesión e instalar** para iniciar sesión en Citrix Cloud.
4. Para instalar y configurar el Cloud Connector, siga las instrucciones del asistente. Cuando finaliza la instalación, el instalador realiza una última comprobación de conectividad para verificar la comunicación entre el Cloud Connector y Citrix Cloud.

5. Repita esos pasos en otras máquinas que quiera usar como Citrix Cloud Connectors. Para tener alta disponibilidad, Citrix recomienda instalar al menos dos Cloud Connectors para cada ubicación de recursos.

Citrix Cloud muestra el Cloud Connector recientemente instalado en la página **Conectores** de la ubicación de recursos.

Después de la instalación, Citrix Cloud registra su dominio en **Administración de acceso e identidad > Dominios**. Para obtener más información, consulte Administración de acceso e identidad.

Activar dominios no utilizados

Si piensa crear ubicaciones de recursos e implementar Cloud Connectors para Citrix DaaS, verifique que los dominios de AD que utiliza con Citrix DaaS estén activos y no se consideren no utilizados. Si especifica un dominio no utilizado al configurar los catálogos de máquinas en Citrix DaaS, es posible que se produzca un error.

Para obtener más información, consulte Agregar un tipo de recurso o activar un dominio no utilizado en Citrix Cloud en la documentación de producto de Citrix DaaS.

Crear ubicaciones de recursos adicionales

1. En la consola de administración de Citrix Cloud, haga clic en el botón de menú y seleccione **Ubicaciones de recursos**.
2. Haga clic en **+ Ubicación de recursos** e introduzca un nombre representativo.
3. Haga clic en **Guardar**. Citrix Cloud muestra un mosaico para la nueva ubicación de recursos.

4. Haga clic en **Cloud Connectors** y, a continuación, en **Descargar** para adquirir el software Cloud Connector.
5. En cada máquina preparada, instale el software Cloud Connector con el asistente de instalación o a través de la línea de comandos. Citrix Cloud le pedirá que seleccione la ubicación de recursos que quiere asociar al Cloud Connector.

Instalación con varios clientes y ubicaciones de recursos existentes

Si usted es un administrador de varias cuentas de cliente, Citrix Cloud le pedirá que seleccione la cuenta de cliente que quiere asociar con el Cloud Connector.

Si su cuenta de cliente ya tiene varias ubicaciones de recursos, Citrix Cloud le pedirá que seleccione la ubicación de recursos que quiere asociar con el Cloud Connector.

Instalación mediante línea de comandos

La instalación puede realizarse de manera silenciosa o automática. Sin embargo, no se recomienda usar el mismo instalador para instalaciones repetidas. Descargue un nuevo Cloud Connector desde la página Ubicaciones de recursos en la consola de Citrix Cloud.

Requisitos

Para utilizar la instalación a través de línea de comandos con Citrix Cloud, debe proporcionar esta información:

- El ID de cliente de la cuenta de Citrix Cloud para la que está instalando Cloud Connector. Este ID aparece en la parte superior de la ficha **Acceso a API** en **Administración de acceso e identidad**.
- El ID de cliente y el secreto del cliente de API seguro que quiere utilizar para instalar Cloud Connector. Para adquirir estos valores, primero debe crear un cliente seguro. El ID y el secreto de cliente garantizan que el acceso a la API de Citrix Cloud esté bien protegido. Al crear un cliente seguro, el cliente opera con el mismo nivel de permisos de administrador que usted tiene. Para instalar un Cloud Connector, debe utilizar un cliente seguro creado por un administrador con acceso total, lo que significa que el cliente seguro también tiene permisos de acceso total.
- El ID de la ubicación de recursos que quiere asociar al Cloud Connector. Para obtener este valor, seleccione el botón **ID** situado debajo del nombre de la ubicación de recursos en la página **Ubicaciones de recursos**. Si no proporciona este valor, Citrix Cloud utiliza el identificador de la ubicación de recursos predeterminada.

Crear un cliente seguro

Al crear un cliente seguro, Citrix Cloud genera un ID y un secreto de cliente únicos. Deberá proporcionar estos valores cuando invoque la API a través de la línea de comandos.

1. Desde el menú de Citrix Cloud, seleccione **Administración de acceso e identidad** y, luego, **Acceso a API**.
2. En la ficha **Clientes seguros**, introduzca un nombre para el cliente y seleccione **Crear cliente**. Citrix Cloud genera y muestra un ID y un secreto de cliente para el cliente seguro.
3. Seleccione **Descargar** para descargar el ID y el secreto de cliente en formato CSV y almacenarlo en una ubicación segura. También puede seleccionar **Copiar** para adquirir manualmente cada valor. Cuando haya terminado, seleccione **Cerrar** para volver a la consola.

Parámetros admitidos

Para garantizar la seguridad de los detalles del cliente seguro, se debe proporcionar un archivo de configuración JSON al instalador. Este archivo deberá eliminarse una vez finalizada la instalación. Los valores admitidos para el archivo de configuración son:

- **customerName:** Obligatorio. El ID de cliente que se muestra en la página Acceso a API de la consola de Citrix Cloud (dentro de Administración de acceso e identidad).
- **clientId:** Obligatorio. El ID de cliente seguro que puede crear un administrador, ubicado en la página Acceso a API.
- **clientSecret:** Obligatorio. El secreto de cliente seguro que puede descargarse después de crear el cliente seguro. Se encuentra en página Acceso a API.
- **resourceLocationId:** Recomendado. El identificador único de una ubicación de recursos existente. Seleccione el botón de ID para obtener el ID de la ubicación de recursos en la página Ubicaciones de recursos de la consola de Citrix Cloud. Si no se especifica ningún valor, Citrix Cloud utiliza el ID de la primera ubicación de recursos de la cuenta.
- **acceptTermsOfService:** Obligatorio. Debe establecerse en **true**.

Archivo de configuración de ejemplo

```
{

"customerName": "*CustomerID*",
"clientId": "*ClientID*",
"clientSecret": "*ClientSecret*",
"resourceLocationId": "*ResourceLocationId*",
"acceptTermsOfService": "true"
 }

<!--NeedCopy-->
```


Comando de ejemplo

El siguiente comando instala de forma silenciosa el software Cloud Connector mediante un archivo de configuración JSON:

```
CWCConnector.exe /q /ParametersFilePath:c:\cwcconnector_install_params.
   json
<!--NeedCopy-->
```

Utilice `/q` para especificar una instalación silenciosa.

Use **Start /Wait CWCConnector.exe /ParametersFilePath:value** para examinar posibles códigos de error en caso de fallo. Puede usar el mecanismo normal que consiste en ejecutar **echo %ErrorLevel%** una vez completada la instalación.

> **Nota:**
>
> El uso de parámetros para transmitir el ID de cliente y el secreto de cliente ya no es compatible; para instalaciones automatizadas, debe utilizarse el archivo de configuración.

Siguientes pasos

1. Configure la programación de actualizaciones de Citrix Cloud Connector. Para obtener información sobre las actualizaciones de Citrix Cloud Connector y cómo administrar programaciones de actualizaciones, consulte Novedades de Connector
2. Configure un proveedor de identidades para autenticar a los suscriptores del espacio de trabajo. Puede cambiar el proveedor de identidades predeterminado de Citrix por el de Active Directory u otros proveedores de identidades en la consola de **Administración de acceso e identidad**. Para obtener más información, vaya a Para conectar su Active Directory a Citrix Cloud.

Solución de problemas de instalación

En esta sección, se detallan algunas formas de diagnosticar y solucionar los problemas que podrían surgir durante la instalación. Para obtener más información sobre cómo solucionar problemas de instalación, consulte la Guía de solución de problemas de Citrix Cloud Connector.

Registros de la instalación

Puede solucionar los problemas encontrados durante la instalación consultando primero los archivos de registro disponibles.

Los eventos ocurridos durante la instalación están disponibles en el **Visor de eventos de Windows**. También puede revisar los registros de instalación de Cloud Connector, que se encuentran en **%LOCALAPPDATA%\Temp\CitrixLogs\CloudServicesSetup**.
También se agregan registros a **%ProgramData%\Citrix\WorkspaceCloud\InstallLogs** después de la instalación.

Códigos de salida

Dependiendo de si el proceso de instalación funciona correctamente o falla, podrían mostrarse los siguientes códigos de salida:

- 1603: Se ha producido un error inesperado.
- 2: Ha fallado algún requisito previo.
- 0: Instalación completada correctamente.

Error de instalación

Si instala el software Citrix Cloud Connector haciendo doble clic en el instalador, es posible que aparezca el siguiente mensaje de error:

```
Can't reach this page.
```

Este error puede producirse aunque haya iniciado sesión como administrador en la máquina donde se instalará Citrix Cloud Connector. Para evitar este error, ejecute el software de Citrix Cloud Connector como administrador; para ello, haga clic con el botón secundario en el instalador y seleccione Ejecutar como administrador.

Fallos de conexión

Para garantizar que el Cloud Connector pueda comunicarse con Citrix Cloud, confirme que los siguientes servicios de Citrix se encuentran en estado **Inicio**:

- Citrix Cloud AD Provider
- Citrix Cloud Agent Logger
- Citrix Cloud Agent System
- Citrix Cloud Agent Watchdog
- Citrix Cloud Credential Provider
- Citrix Config Synchronizer Service
- Citrix High Availability Service (Servicio de alta disponibilidad de Citrix):
- Citrix NetScaler CloudGateway
- Citrix Remote Broker Provider

- Citrix Remote HCL Server
- Citrix Session Manager Proxy

Para obtener más información sobre estos servicios, consulte Servicios instalados.

Si continúa experimentando fallos de conectividad, utilice la utilidad de comprobación de la conectividad de Cloud Connector disponible en Knowledge Center de Citrix Support. Para obtener más información, consulte CTX260337 en el sitio web de Knowledge Center.

La herramienta se puede utilizar para realizar las siguientes tareas:

- Probar si se puede acceder a Citrix Cloud y a los servicios relacionados.
- Comprobar si hay parámetros mal configurados.
- Configurar los parámetros de proxy en Citrix Cloud Connector.

Para obtener más información sobre cómo resolver una comprobación de conectividad fallida, consulte CTX224133: Cloud Connector Connectivity Check Failed.

Comprobaciones avanzadas de estado de Cloud Connector

December 12, 2023

Antes y después de las actualizaciones, Cloud Connector realiza comprobaciones de estado para garantizar que las actualizaciones no provoquen períodos de inactividad innecesarios a los proveedores. Puede ver el estado y la conectividad del conector y de cada servicio o proveedor en el conector.

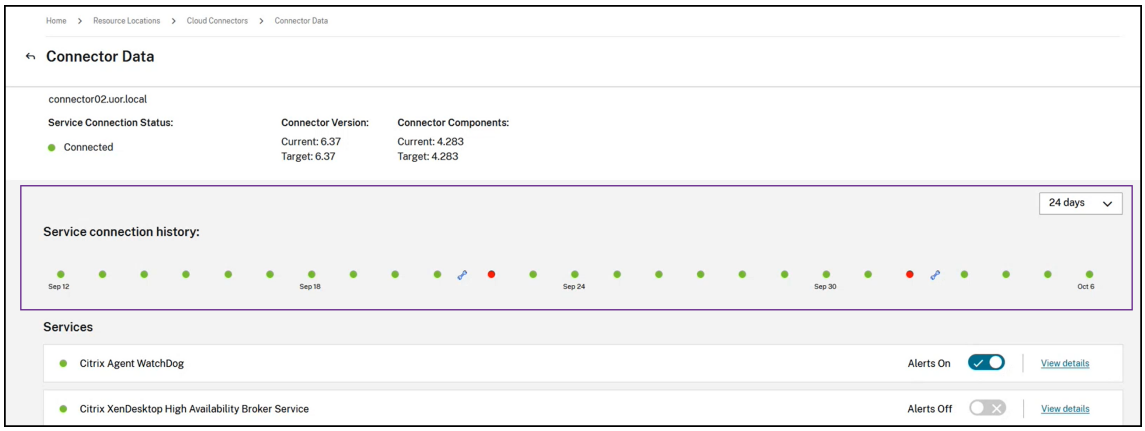
Ver datos de comprobación de estado de los conectores

1. En el menú de Citrix Cloud, seleccione **Ubicaciones de recursos**.
2. Seleccione el conector del que quiere ver datos de comprobación de estado.
3. En la página Conectores, vaya al menú de puntos suspensivos que hay junto al conector y seleccione **Ver datos del conector**.

Aparece la página Datos del conector, que muestra esta información.

- **Estado de la conexión del servicio**. Esta zona de la página Datos del conector muestra:
  - Si su conector está conectado a la nube
  - Para el conector y sus componentes, la versión instalada actualmente y la versión de destino que se instalarán en la próxima actualización

- **Historial de conexiones del servicio** 24 indicadores de estado muestran el estado del conector a lo largo del tiempo. De forma predeterminada, el historial de conexiones del servicio muestra el estado de las últimas 24 horas, en intervalos de una hora. Para ver más datos del historial, seleccione **24 días** en el menú desplegable. La vista muestra el estado de los 24 últimos días, en intervalos de un día.
  - Un punto verde indica un buen estado durante este intervalo de tiempo.
  - Un punto rojo indica un estado con errores o excepciones durante este intervalo de tiempo. Pase el mouse sobre el punto para obtener más información.
  - Un icono de llave inglesa indica que hubo una actualización durante ese intervalo de tiempo. Pase el mouse sobre el icono de la llave inglesa para obtener más información.
  - Un punto gris indica que no se recibió información sobre el estado durante ese intervalo de tiempo.



- **Servicios**. En esta zona se enumeran todos los servicios que se ejecutan en el conector.
  - El punto situado junto a cada servicio indica el estado actual del servicio.
  - Utilice **Alertas activadas** y **Alertas desactivadas** para controlar si se le notifican las alertas del servicio. Si las alertas están activadas, los fallos en el servicio provocan un fallo en el estado general de la conexión del conector.
  - Seleccione **Ver detalles** para ver los detalles del estado del servicio a lo largo del tiempo.
- **Métricas de conector**. Esta zona muestra el uso que el conector hace de la memoria, la CPU, los datos de red y el espacio en disco durante las últimas 24 horas o los últimos 24 días. Utilice el menú desplegable de la zona **Historial de conexiones del servicio** para controlar el período de tiempo que se muestra.

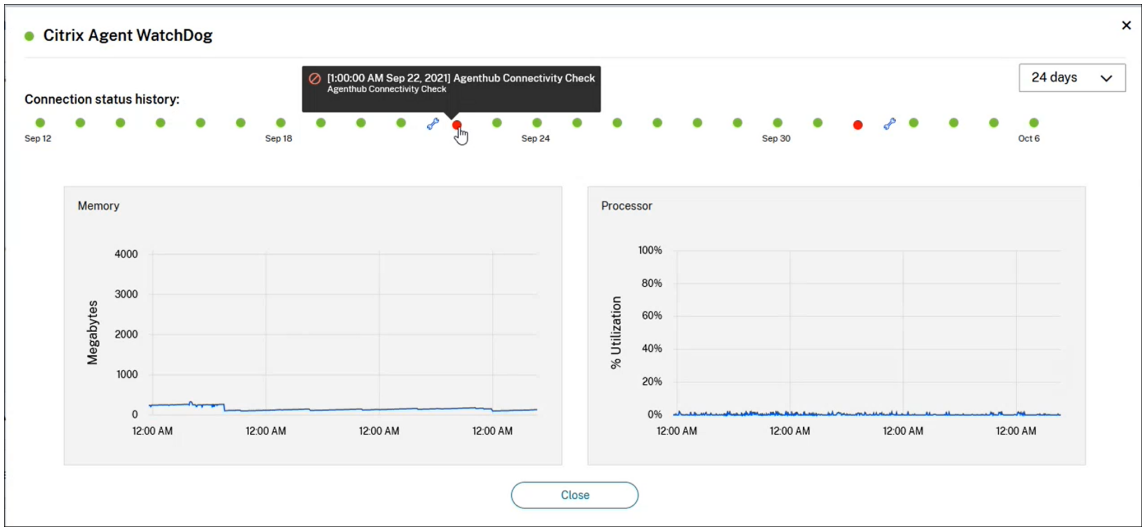
Ver detalles del servicio

Para ver las métricas y el historial del estado de las conexiones de cada servicio:

1. Utilice el menú desplegable de la sección **Historial de conexiones del servicio** para seleccionar el período de tiempo. Puede ver las últimas 24 horas, en intervalos de una hora, o los 24 últimos días, en intervalos de un día.
2. En la página Datos del conector, seleccione **Ver detalles** junto al servicio.

La página que aparece muestra:

- 24 indicadores de estado que muestran el estado del servicio a lo largo del tiempo.
  - Un punto verde indica un buen estado durante este intervalo de tiempo.
  - Un punto rojo indica un estado con errores o excepciones durante este intervalo de tiempo. Pase el mouse sobre el punto para obtener más información.
  - Un icono de llave inglesa indica que hubo una actualización durante ese intervalo de tiempo. Pase el mouse sobre el icono de la llave inglesa para obtener más información.
  - Un punto gris indica que no se recibió información sobre el estado durante ese intervalo de tiempo.
- Gráficos que muestran el uso de la memoria y del procesador por parte del servicio durante el período de tiempo especificado.



Notificaciones de los conectores

November 2, 2022

Los conectores generan notificaciones hasta 2 horas después de la aparición de una advertencia o error. Puede ver las notificaciones nuevas en el icono de la campana del encabezado de Citrix Cloud.

Haga clic en este icono para ver las notificaciones o seleccione **Notificaciones** en el menú de la consola.

Para obtener más información, consulte Notificaciones.

Cloud Connector

En esta tabla se indican las notificaciones que Cloud Connector puede generar:

Mensaje de alerta	Tipo de alerta	Detalles	La resolución
El conector *CONNECTOR_NAME* está fuera de conexión y obsoleto al no haber realizado tareas de mantenimiento con regularidad. Los conectores obsoletos afectarán a la disponibilidad del servicio e impedirán su mantenimiento.	Error	Si un conector ha estado fuera de conexión durante mucho tiempo y luego recupera la conexión, es posible que se trate de una versión antigua que no se pueda actualizar a la versión más reciente. Los conectores obsoletos no pueden realizar su mantenimiento y pueden afectar al proceso de mantenimiento de otros conectores en el entorno.	Cómo actualizar un Cloud Connector obsoleto
El conector *CONNECTOR_NAME* no está sincronizado con la hora UTC. Los conectores en este estado pueden afectar a la disponibilidad, la funcionalidad y al rendimiento del servicio.	Error		Cómo sincronizar la hora del Cloud Connector

Mensaje de alerta	Tipo de alerta	Detalles	La resolución
No se pudo realizar el mantenimiento del conector *CONNECTOR_NAME*. Si no se realiza ningún mantenimiento en este conector, no se podrá realizar mantenimiento de otros conectores del entorno. Los conectores con problemas de mantenimiento pueden afectar a la disponibilidad, la funcionalidad y al rendimiento del servicio.	Error	Se ha producido un error en la actualización de la versión del conector o en otra operación de mantenimiento en este conector.	Cómo resolver un mantenimiento fallido de Cloud Connector
El conector *CONNECTOR_NAME* ha estado fuera de conexión durante *NUMBER* h o más. Los conectores sin conexión afectarán a la disponibilidad del servicio e impedirán su mantenimiento.	Advertencia	Si el conector ha estado inaccesible durante una cantidad determinada de horas, se considera que está fuera de conexión.	Cómo restaurar la conexión de un Cloud Connector fuera de conexión

Mensaje de alerta	Tipo de alerta	Detalles	La resolución
El conector *CONNECTOR_NAME* no pudo realizar una comprobación de conectividad reciente. Un fallo en la verificación de la conectividad puede afectar a la disponibilidad o la funcionalidad del servicio.	Advertencia	Ha fallado una comprobación de conectividad con el código de error *HEALTH_CHECK_CODE*. Este conector no pudo contactar con determinadas direcciones web o IP que figuran en el mensaje de la notificación.	Error en la comprobación de conectividad de Cloud Connector
El conector *CONNECTOR_NAME* experimenta un uso elevado de la CPU. Los conectores que funcionan con recursos limitados pueden afectar a la disponibilidad, la funcionalidad y al rendimiento del servicio.	Advertencia	Este conector ha superado el 80 % del uso de la CPU durante un período de muestra de una hora.	Cómo resolver una alerta de disponibilidad de recursos de Cloud Connectors
El conector *CONNECTOR_NAME* tiene poco espacio libre en el disco. Los conectores que funcionan con espacio limitado en el disco afectarán al mantenimiento y al rendimiento del servicio.	Advertencia	Este conector tiene menos de 2 GB de espacio libre en el disco.	Cómo resolver una alerta de disponibilidad de recursos de Cloud Connectors

Mensaje de alerta	Tipo de alerta	Detalles	La resolución
El conector *CONNECTOR_NAME* ha detectado que un proceso o servicio crítico ya no se está ejecutando. Este estado puede afectar a la disponibilidad, la funcionalidad y al rendimiento del servicio.	Advertencia		

Recopilación de registros para Citrix Cloud Connector

October 2, 2023

Los registros de CDF se utilizan para solucionar problemas en los productos Citrix. Citrix Support utiliza seguimientos CDF para identificar problemas en la intermediación de aplicaciones y escritorios, la autenticación de usuarios y el registro de Virtual Delivery Agent (VDA). En este artículo, se describe cómo capturar datos de Cloud Connector que se pueden utilizar para resolver problemas que se pueden presentar en su entorno.

> **Notas importantes:**
>
> - Habilite el inicio de sesión en todas las máquinas con Cloud Connector de sus ubicaciones de recursos.
> - Para asegurarse de que está capturando todo el espectro de datos, Citrix recomienda utilizar la herramienta de captura CDFControl que reside en el VDA. Para obtener más información, consulte CTX111961 en Knowledge Center de Citrix Support. Para obtener más información acerca de la recopilación de registros para la aplicación Citrix Workspace, CTX141751.
> - Para enviar seguimientos CDF a Citrix, debe tener un caso abierto con Citrix Support. Los técnicos de Citrix Support no pueden revisar los seguimientos CDF que no están conectados a un caso de asistencia existente.

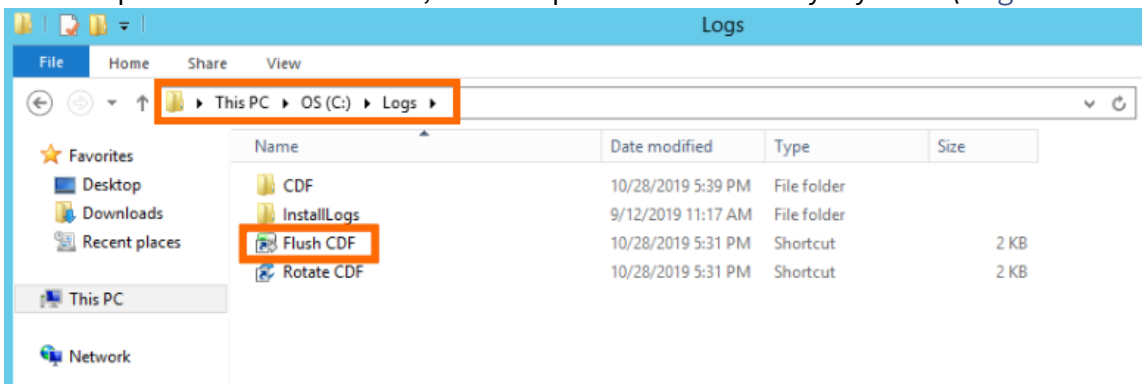
Paso 1: Reproducir el problema

En este paso, se reproduce el problema ocurrido en su entorno. Si el problema está relacionado con el inicio de aplicaciones o la intermediación, reproduzca el error de inicio. Si el problema está relacionado con el registro de VDA, reproduzca el intento de registro de VDA reiniciando manualmente Citrix Desktop Service en la máquina VDA.

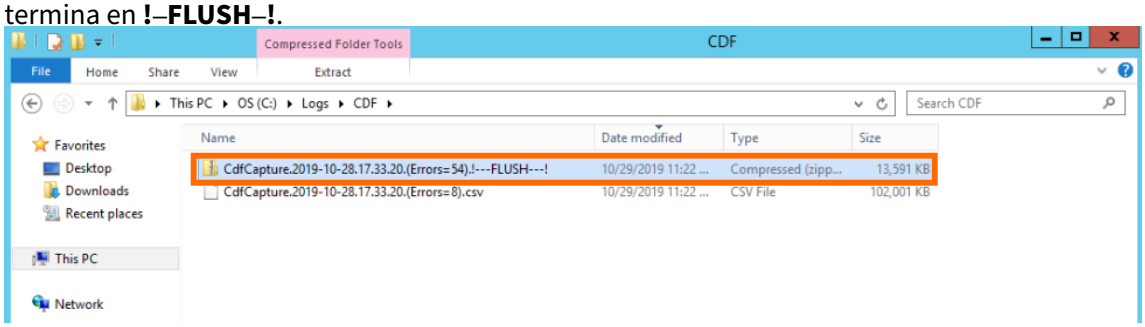
Paso 2: Obtener seguimientos CDF

En este paso, recopilará seguimientos de vaciado de CDF de cada Cloud Connector presente en su ubicación de recursos.

1. Acceda a la máquina de Cloud Connector iniciando una conexión RDP con una cuenta de administrador de dominio o administrador local.
2. En la máquina de Cloud Connector, abra el Explorador de archivos y vaya a `C:\logs`.



3. Ejecute **Flush CDF**. Aparecerá un icono brevemente en la barra de tareas de la máquina de Cloud Connector y, a continuación, desaparecerá.
4. En el Explorador de archivos, vaya a C:\logs\CDF e identifique la carpeta más reciente que termina en **!–FLUSH–!**.

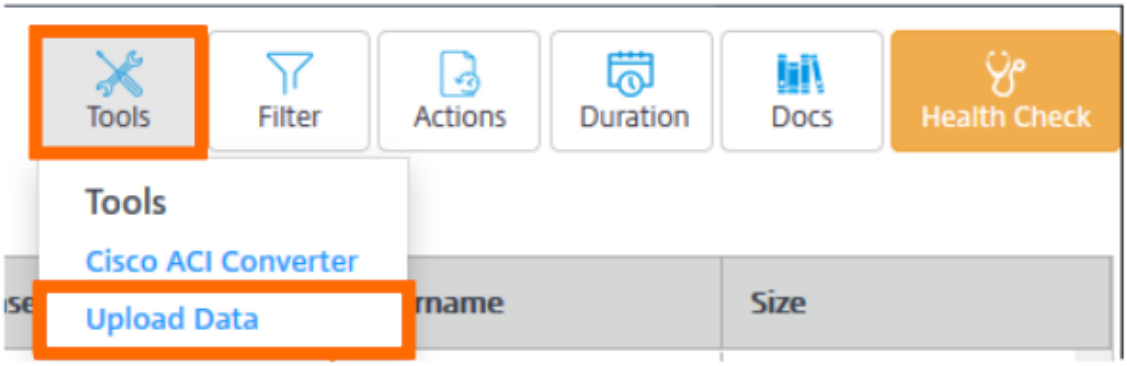


5. Realice los pasos 1 a 5 en cada máquina de Cloud Connector de su ubicación de recursos y combine todos los seguimientos de vaciado de Cloud Connector en un único archivo ZIP. Si no crea un archivo ZIP de los seguimientos de vaciado de todas las máquinas de Cloud Connector, deberá enviarlos uno a uno a Citrix.

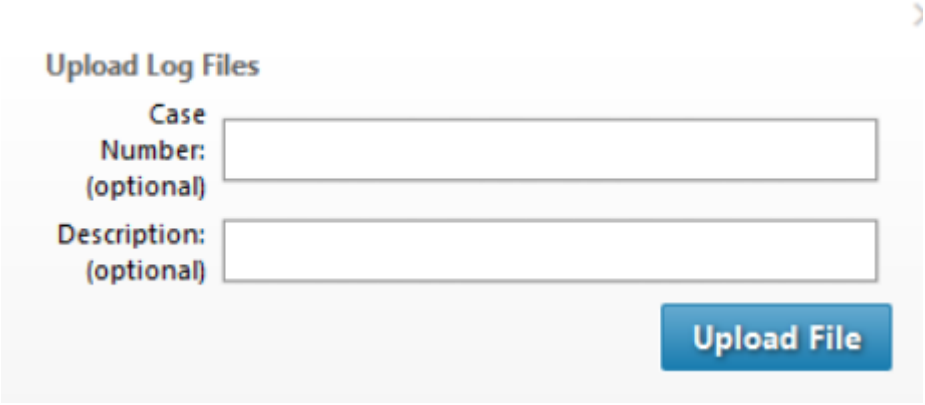
Paso 3: Enviar datos a Citrix

En este paso, adjuntará los seguimientos a su caso de Citrix Support y los enviará para análisis

1. Visite https://cis.citrix.com/ e inicie sesión con sus credenciales de Citrix.com.
2. Seleccione **Diagnóstico**.
3. Seleccione **Herramientas** y, a continuación, seleccione **Cargar datos**.



4. En **Número de caso**, introduzca el número de caso de Citrix Support. Los técnicos Citrix Support no pueden revisar correctamente los seguimientos CDF sin un número de caso adjunto a la carga de datos.



5. En **Descripción** (opcional), puede introducir una breve descripción o dejar este campo en blanco.
6. Seleccione **Cargar archivo** y seleccione el archivo ZIP que creó anteriormente. Si no ha creado un archivo ZIP con los seguimientos de vaciado de todas las máquinas de Cloud Connector, repita los pasos 3 a 6 para adjuntar cada seguimiento de vaciado que desee enviar.

Después de enviar los seguimientos de vaciado, Citrix Insight Services los procesa y los adjunta al caso de soporte especificado. Este proceso puede tardar hasta 24 horas, dependiendo del tamaño de los archivos.

Seleccionar una ubicación de recursos principal

October 2, 2023

Si tiene varias ubicaciones de recursos en su dominio, puede elegir una para que sea la ubicación "principal"o "preferida"para Citrix Cloud. La ubicación de recursos principal proporciona una conectividad entre Citrix Cloud y el dominio y un rendimiento óptimos, lo que permite a los usuarios iniciar sesión rápidamente.

Cuando se selecciona una ubicación de recursos principal, los Cloud Connectors de esa ubicación de recursos se utilizan para los inicios de sesión de usuario y las operaciones de aprovisionamiento si es posible. Si los Cloud Connectors de la ubicación de recursos principal no están disponibles, estas operaciones se realizan mediante otro Cloud Connector del dominio. Es posible que los inicios de sesión que utilicen un nombre principal de usuario (UPN) no contengan el nombre de dominio y que no usen la ubicación de recursos principal.

> **Nota:**
>
> Para garantizar que los Cloud Connectors estén siempre disponibles en cualquier ubicación de recursos, instale al menos dos Cloud Connectors en cada ubicación de recursos.

Para decidir qué ubicación de recursos quiere usar como ubicación de recursos principal, tenga en cuenta lo siguiente:

- ¿La ubicación de recursos tiene la mejor conectividad con el dominio?
- ¿Está la ubicación de recursos lo más cerca posible de la región geográfica en la que utiliza la consola de administración de Citrix Cloud? Por ejemplo, si su consola de Citrix Cloud está en https://us.cloud.com, la ubicación de recursos que elija sería la más cercana a la región de EE. UU.

Para seleccionar una ubicación de recursos principal

1. Desde la consola de administración de Citrix Cloud, haga clic en el botón de menú y seleccione **Administración de acceso e identidad**.
2. Haga clic en **Dominios** y luego expanda el dominio que contiene la ubicación de recursos que quiere usar.
3. Haga clic en **Establecer ubicación de recursos principal** y luego seleccione la ubicación de recursos que quiere designar como principal.
4. Haga clic en **Guardar**. Citrix Cloud muestra "Principal"junto a la ubicación de recursos seleccionada.

> **Nota:**
>
> Asegúrese de guardar sus selecciones en un dominio antes de expandir un dominio diferente. Cuando se expande un dominio y luego se expande otro, el dominio expandido anteriormente se contrae y se descarta cualquier selección no que no se hubiera guardado.

Seleccionar una ubicación de recursos principal diferente

1. Desde la consola de administración de Citrix Cloud, haga clic en el botón de menú y seleccione **Administración de acceso e identidad**.
2. Haga clic en **Dominios** y luego expanda el dominio que contiene la ubicación de recursos principal que quiere cambiar.
3. Haga clic en **Cambiar ubicación de recursos principal** y luego seleccione la ubicación de recursos que quiera usar.
4. Haga clic en **Guardar**.

Restablecer una ubicación de recursos principal

Al restablecer la ubicación de recursos principal se puede eliminar la designación de "Principal"de esa ubicación de recursos sin tener que seleccionar otra como principal. Cuando se elimina la designación de "Principal", cualquiera de los Cloud Connectors del dominio puede gestionar las operaciones de inicio de sesión de los usuarios. Como consecuencia, algunos usuarios pueden experimentar inicios de sesión más lentos.

1. Desde la consola de administración de Citrix Cloud, haga clic en el botón de menú y seleccione **Administración de acceso e identidad**.
2. Elija **Dominios** y luego expanda el dominio que contiene la ubicación de recursos principal que quiere cambiar.
3. Elija **Cambiar ubicación de recursos principal** y luego elija **Restablecer**. Aparece una notificación que le advierte que el rendimiento de los inicios de sesión puede verse afectado.
4. Seleccione **Comprendo el impacto que esto puede tener para los suscriptores** y luego haga clic en **Confirmar restablecimiento**.

Connector Appliance para Cloud Services

April 5, 2024

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. Connector Appliance permite administrar y centrarse en los recursos que ofrecen más valor a los usuarios.

Connector Appliance ofrece las siguientes funciones:

- **Conectar Active Directory (AD) con Citrix Cloud** habilita la administración de AD, lo que permite el uso de bosques y dominios de AD dentro de las ubicaciones de recursos. Elimina la necesidad de agregar más relaciones de confianza de AD. Para obtener más información, consulte Active Directory con el Connector Appliance.
- **Image Portability Service** simplifica la administración de imágenes en distintas plataformas. Esta funcionalidad es útil para administrar imágenes entre una ubicación de recursos local y otra en una nube pública. Las API de REST de Citrix Virtual Apps and Desktops sirven para automatizar la administración de recursos en un sitio de Citrix Virtual Apps and Desktops.

  El flujo de trabajo de Image Portability comienza cuando usa Citrix Cloud para iniciar la migración de una imagen desde su ubicación local a su suscripción de nube pública. Después de preparar la imagen, Image Portability Service le ayuda a transferir la imagen a su suscripción en la nube pública y a prepararla para su ejecución. Por último, Citrix Provisioning o Machine Creation Services aprovisionan la imagen en su suscripción a la nube pública.

  Para obtener más información, consulte Image Portability Service.
- **Citrix Secure Private Access** permite a los administradores proporcionar una experiencia coherente que integre el inicio de sesión único (SSO), el acceso remoto y la inspección de contenido en una única solución para el control de acceso de extremo a extremo. Para obtener más información, consulte Secure Private Access con Connector Appliance.

Es posible que haya otros servicios en Tech Preview que también dependan de Connector Appliance.

La plataforma de Connector Appliance forma parte de Citrix Cloud Platform y Citrix Identity Platform y puede procesar datos, incluida la información siguiente:

- Direcciones IP o nombres de dominio completo (FQDN)
- Identificadores de dispositivos, usuarios y ubicaciones de recursos
- Marcas de hora
- Datos de eventos
- Detalles de usuarios y grupos de Active Directory (por ejemplo, utilizados para autenticar y buscar usuarios y grupos)

Los detalles de la información específica que procesa el Connector Appliance están disponibles en la tabla de *datos recopilados por Citrix Cloud Platform* en Citrix Cloud Services Data Protection Overview.

Disponibilidad y administración de carga de Connector Appliances

Para administrar la carga de los conectores y conseguir una disponibilidad continuada de estos, instale varios Connector Appliances en cada una de las ubicaciones de recursos. Citrix recomienda contar con al menos dos Connector Appliances en cada ubicación de recursos. Si un Connector Appliance no está disponible en algún momento, los demás Connector Appliances pueden mantener la conexión. Dado que ninguno de los Connector Appliances guarda información sobre el estado, la carga se puede distribuir entre todos los dispositivos disponibles. No es necesario configurar la función de equilibrio de carga. Es automática. Si hay, al menos, un Connector Appliance disponible, no se pierde la comunicación con Citrix Cloud.

Si solo tiene un conector configurado para una ubicación de recursos, Citrix Cloud muestra una advertencia en las **ubicaciones de recursos** y en la página **Conectores**.

Novedades de los Connector Appliances

Connector Appliance se actualiza automáticamente. No es necesario que haga nada para actualizar el conector.

Puede configurar la ubicación de recursos para aplicar actualizaciones inmediatamente a medida que estén disponibles o durante un período de mantenimiento específico.

Para obtener más información sobre la configuración de actualizaciones, consulte Actualizaciones de los Connectors.

Como parte de la actualización, el Connector Appliance deja de estar disponible temporalmente. Las actualizaciones solo se aplican a un Connector Appliance en una ubicación de recursos a la vez. Por ese motivo, registre al menos dos Connector Appliances en cada ubicación de recursos, para garantizar que al menos un dispositivo esté siempre disponible.

Comunicación de Connector Appliance

Connector Appliance autentica y cifra toda la comunicación entre Citrix Cloud y las ubicaciones de recursos. Una vez instalado, el Connector Appliance inicia la comunicación con Citrix Cloud a través de una conexión saliente. Todas las conexiones se establecen desde el Connector Appliance hacia la nube mediante el puerto HTTPS estándar (443) y el protocolo TCP. No se permiten conexiones entrantes.

En esta tabla se enumeran los puertos a los que el Connector Appliance requiere acceso:

Servicio	Puerto	Protocolo de dominio compatible	Detalles de configuración
DNS	53	TCP/UDP	Este puerto debe estar abierto a la configuración local
NTP	123	UDP	Este puerto debe estar abierto a la configuración local
HTTPS	443	TCP	El Connector Appliance necesita un acceso saliente a este puerto

Para configurar el Connector Appliance, los administradores de TI deben poder acceder a la interfaz de administración en el puerto 443 (HTTPS) del Connector Appliance.

> **Nota:**
>
> Debe incluir `https://` al principio de la dirección IP.

Connector Appliance puede comunicarse tanto con sistemas locales de la ubicación de recursos como con sistemas externos. Si define uno o varios servidores web proxy durante el registro de Connector Appliances, solo se redirige el tráfico desde el Connector a sistemas externos a través de este proxy web. Si el sistema local se encuentra en un espacio de direcciones privado, el tráfico desde el Connector a este sistema no se redirige a través del proxy web.

Connector Appliance define los espacios de direcciones privadas como los siguientes intervalos de direcciones IPv4:

- 10.0.0.0 –10.255.255.255
- 172.16.0.0 –172.31.255.255
- 192.168.0.0 –192.168.255.255

Requisitos de la conectividad a Internet

La conexión a Internet desde los centros de datos requiere que el puerto 443 esté abierto para las conexiones salientes. Sin embargo, para poder funcionar en entornos que contienen restricciones de firewall o un servidor proxy de Internet, se necesitan más parámetros.

Para operar y utilizar correctamente los servicios de Citrix Cloud, debe poder establecerse contacto con las siguientes direcciones mediante conexiones HTTPS sin modificar:

- https://*.cloud.com
- https://*.citrixworkspacesapi.net
- https://*.citrixnetworkapi.net
- https://*.nssvc.net
  - Los clientes que no pueden habilitar todos los subdominios pueden utilizar las siguientes direcciones:
    * https://*.g.nssvc.net
    * https://*.c.nssvc.net
- https://*.servicebus.windows.net
- https://iwsprodeastusuniconacr.azurecr.io
- https://iwsprodeastusuniconacr.eastus.data.azurecr.io

Requisitos de la red

Compruebe que su entorno tenga la siguiente configuración:

- La red permite que el Connector Appliance utilice DHCP para obtener servidores DNS y NTP, una dirección IP, un nombre de host y un nombre de dominio, o bien puede configurar manualmente los parámetros de red en la consola de Connector Appliance.
- La red no está configurada para utilizar los rangos IP locales de enlace 169.254.0.1/24, 169.254.64.0/18 o 169.254.192.0/18, que el Connector Appliance utiliza internamente.
- El reloj del hipervisor se establece en la hora universal coordinada (UTC) y se sincroniza con un servidor horario o DHCP proporciona información del servidor NTP a Connector Appliance.
- Si utiliza un proxy con un Connector Appliance, el proxy debe estar sin autenticar o usar autenticación básica.

Requisitos del sistema

Connector Appliance está disponible en los siguientes hipervisores:

- Citrix Hypervisor 8.2 LTSR CU1
- Actualización 2 de la versión 7 de VMware ESXi
- Hyper-V en Windows Server 2016, Windows Server 2019 o Windows Server 2022.
- Nutanix AHV
- Microsoft Azure
- AWS
- Google Cloud Platform

El hipervisor debe tener las siguientes capacidades mínimas:

- Disco raíz de 20 GB
- 2 CPU virtuales
- 4 GB de memoria
- Una red IPv4

Puede alojar varios Connector Appliances en el host del mismo hipervisor. La cantidad de Connector Appliances en el mismo host solo está limitada por las limitaciones del hipervisor y del hardware.

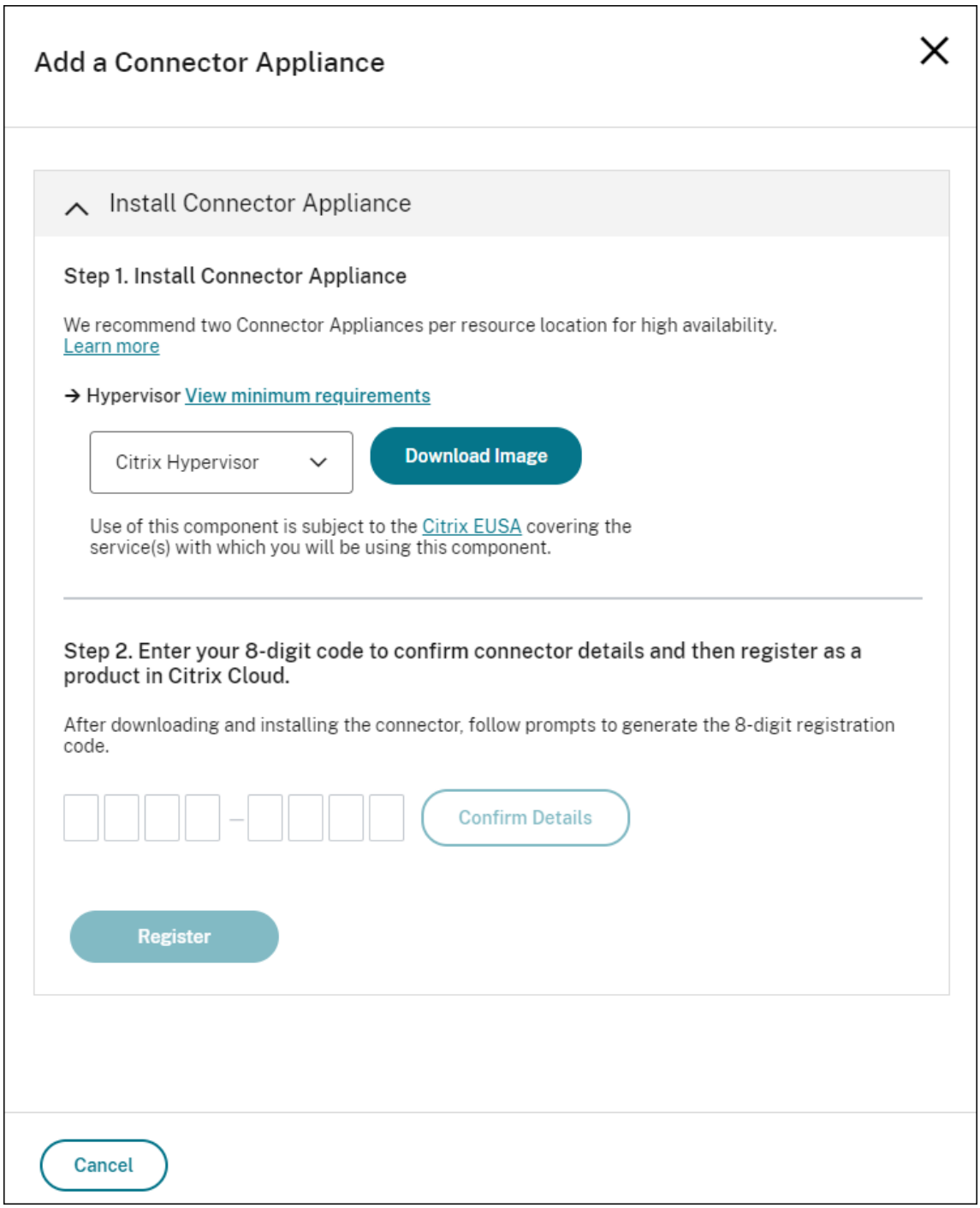
> **Nota:**
>
> No se admite la clonación, la suspensión y la toma de instantáneas de la VM de Connector Appliance.

Obtener el Connector Appliance

Descargue el software de Connector Appliance desde Citrix Cloud.

1. Inicie sesión en Citrix Cloud.
2. En el menú de la esquina superior izquierda, seleccione **Ubicaciones de recursos**.
3. Si aún no tiene una ubicación de recursos, haga clic en el icono más (+) o seleccione **Agregar una ubicación de recursos**.
4. En la ubicación de recursos en la que quiere registrar el Connector Appliance, haga clic en el icono del signo más (+) de **Connector Appliances**.

   Se abrirá la tarea **Agregar un Connector Appliance**.



5. En la lista **Hipervisor** del **paso 1**, elija el tipo de hipervisor o proveedor de la nube que utilizará para alojar el Connector Appliance.

   - Para hipervisores locales y entornos de nube, puede descargar el Connector Appliance dentro de Citrix Cloud:

     a) Haga clic en **Descargar imagen**.

b) Revise el Contrato de servicio del usuario final de Citrix y, si está de acuerdo, seleccione **Aceptar y continuar**.

c) Cuando se le solicite, guarde el archivo de Connector Appliance proporcionado.

La extensión del nombre del archivo de Connector Appliance depende del hipervisor que elija.

- Para algunos entornos de nube, puede obtener el Connector Appliance en la tienda:
  - AWS
  - Microsoft Azure
  - Google Cloud

6. Mantenga la tarea **Instalar Connector Appliance** abierta. Después de instalar el Connector Appliance, introduzca el código de registro en el **paso 2**.

También puede acceder a la tarea **Instalar Connector Appliance** desde la página **Conectores**. Seleccione el icono del signo más (+) para agregar un conector y elija agregar un Connector Appliance.

Instalar el Connector Appliance en el hipervisor

- Citrix Hypervisor
- VMware ESXi
- Hyper-V
- Nutanix AHV
- Microsoft Azure
- Google Cloud Platform
- AWS

Citrix Hypervisor

En esta sección, se describe cómo importar el Connector Appliance a un servidor de Citrix Hypervisor mediante XenCenter.

1. Conéctese al servidor o agregación de servidores de Citrix Hypervisor mediante XenCenter en un sistema que tenga acceso al archivo XVA descargado de Connector Appliance.
2. Seleccione **File** > **Import**.
3. Especifique o vaya a la ubicación en la que se encuentra el archivo XVA de Connector Appliance. Haga clic en **Siguiente**.
4. Seleccione el servidor de Citrix Hypervisor en el que alojar el Connector Appliance. Si no, también puede seleccionar la agregación de servidores en la que alojar el Connector Appliance y Citrix Hypervisor será quien elegirá un servidor disponible adecuado. Haga clic en **Siguiente**.

5. Especifique el repositorio de almacenamiento que se va a utilizar para el Connector Appliance. Haga clic en **Importar**.
6. Haga clic en **Add** para agregar una interfaz de red virtual. En la lista **Network**, seleccione la red que deberá utilizar el Connector Appliance. Haga clic en **Siguiente**.
7. Revise las opciones que se van a utilizar para implementar el Connector Appliance. Si alguna opción es incorrecta, utilice **Previous** para cambiarla.
8. Compruebe que **Start the new VM(s) automatically as soon as the import is complete** está marcado. Haga clic en **Finalizar**.

Una vez implementado e iniciado correctamente el Connector Appliance, la consola muestra una página de destino que contiene la dirección IP de Connector Appliance. Utilice esta dirección IP para conectarse a la página de administración de Connector Appliance y completar el proceso de registro.

De forma predeterminada, el Connector Appliance utiliza DHCP para establecer su configuración de red. Si DHCP no está disponible en su entorno, debe establecer la configuración de red en la consola del Connector Appliance para poder acceder a la consola de administración del Connector Appliance. Para obtener más información, consulte Establecer la configuración de red mediante la consola de Connector Appliance.

Paso siguiente: Registrar el Connector Appliance en Citrix Cloud.

VMware ESXi

En esta sección, se describe cómo implementar Connector Appliances en un host VMware ESXi mediante el cliente de VMware vSphere.

1. Conéctese al host ESXi mediante el cliente de vSphere en un sistema que tenga acceso al archivo OVA descargado de Connector Appliance.
2. Seleccione **File** > **Deploy OVF Template…**
3. Especifique o vaya a la ubicación en la que se encuentra el archivo OVA de Connector Appliance. Haga clic en **Siguiente**.
4. Revise los detalles de la plantilla. Haga clic en **Siguiente**.
5. Puede especificar un nombre único para la instancia de Connector Appliance. De forma predeterminada, el nombre se establece en **Connector Appliance**. Debe elegir un nombre que distinga esta instancia de Connector Appliance de otras instancias alojadas en el mismo host ESXi. Haga clic en **Siguiente**.
6. Especifique el almacenamiento de destino para el Connector Appliance. Haga clic en **Siguiente**.
7. Elija el formato en el que almacenar los discos virtuales. Haga clic en **Siguiente**.
8. Revise las opciones que se van a utilizar para implementar el Connector Appliance. Si alguna opción es incorrecta, utilice **Back** para cambiarla.
9. Seleccione **Power on after deployment**. Haga clic en **Finalizar**.

Una vez implementado e iniciado correctamente el Connector Appliance, la consola muestra una página de destino que contiene la dirección IP de Connector Appliance. Utilice esta dirección IP para conectarse a la página de administración de Connector Appliance y completar el proceso de registro.

De forma predeterminada, el Connector Appliance utiliza DHCP para establecer su configuración de red. Si DHCP no está disponible en su entorno, debe establecer la configuración de red en la consola de Connector Appliance para poder acceder a la interfaz de usuario de Connector Appliance. Para obtener más información, consulte Establecer la configuración de red mediante la consola de Connector Appliance.

Paso siguiente: Registrar el Connector Appliance en Citrix Cloud.

Hyper-V

En esta sección se describe cómo implementar un Connector Appliance en un host Hyper-V. Puede implementar la VM mediante el Administrador de Hyper-V o mediante el script de PowerShell incluido.

Implementar el Connector Appliance mediante el Administrador de Hyper-V

1. Conéctese a su host Hyper-V.
2. Copie o descargue el archivo ZIP de Connector Appliance en el host Hyper-V.
3. Extraiga el contenido del archivo ZIP. El archivo ZIP contiene un script de PowerShell y el archivo connector-appliance.vhdx.
4. Copie el archivo VHDX allí donde quiera guardar los discos de la VM. Por ejemplo: `C:\ConnectorApplianceVMs`.
5. Abra el Administrador de Hyper-V.
6. Haga clic con el botón secundario en el nombre del servidor y seleccione **Nuevo > Máquina virtual**.
7. En el **Asistente para crear máquinas virtuales**, en el panel **Especificar el nombre y la ubicación**, escriba un nombre único para identificar el Connector Appliance. Haga clic en **Siguiente**.
8. En el panel **Especificar generación**, seleccione **Generación 1**. Haga clic en **Siguiente**.
9. En el panel **Asignar memoria**, configure estos parámetros y, a continuación, haga clic en **Siguiente**:

    a) Asigne 4 GB de RAM.

b) Inhabilite la memoria dinámica.

10. En el panel **Configurar redes**, seleccione un botón de la lista (por ejemplo, el botón predeterminado). Haga clic en **Siguiente**.
11. En el panel **Conectar disco duro virtual** , seleccione **Usar un disco duro virtual existente**.
12. Busque la ubicación del archivo connector-appliance.vhdx y selecciónelo. Haga clic en **Siguiente**.
13. En el panel **Resumen**, revise los valores que ha elegido y haga clic en **Finalizar** para crear la VM.
14. En el panel **Máquinas virtuales**, haga clic con el botón secundario en la VM de Connector Appliance y seleccione **Configuración**.
15. En la ventana **Configuración**, seleccione **Hardware > Procesadores** y realice las siguientes acciones:

    a) En **Número de procesadores virtuales**, cambie el valor a **2**.
    b) Haga clic en **Aplicar**.
    c) Haga clic en **Aceptar**.

16. En el panel **Máquinas virtuales**, haga clic con el botón secundario en la VM de Connector Appliance y seleccione **Iniciar**.
17. Haga clic con el botón secundario en la VM de Connector Appliance y seleccione **Conectar** para abrir la consola.

Una vez implementado e iniciado correctamente el Connector Appliance, conéctese a la consola mediante el Administrador de Hyper-V. La consola muestra una página de inicio que contiene la dirección IP de Connector Appliance. Utilice esta dirección IP para conectarse a la página de administración de Connector Appliance y completar el proceso de registro.

De forma predeterminada, el Connector Appliance utiliza DHCP para establecer su configuración de red. Si DHCP no está disponible en su entorno, debe establecer la configuración de red en la consola de Connector Appliance para poder acceder a la interfaz de usuario de Connector Appliance. Para obtener más información, consulte Establecer la configuración de red mediante la consola de Connector Appliance.

Paso siguiente: Registrar el Connector Appliance en Citrix Cloud.

Implementar el Connector Appliance mediante un script de PowerShell El archivo connector-appliance.zip contiene un script de PowerShell que crea e inicia una nueva VM.

> **Nota:**
>
> Para ejecutar este script de PowerShell sin firmar, es posible que tenga que cambiar las directivas

> de ejecución en el sistema de Hyper-V. Para obtener más información, consulte https://go.microsoft.com/fwlink/?LinkID=135170. Si no, también puede utilizar el script proporcionado como base para crear o modificar su propio script local.

1. Conéctese a su host Hyper-V.
2. Copie o descargue el archivo ZIP de Connector Appliance en el host Hyper-V.
3. Extraiga el contenido del archivo ZIP: un script de PowerShell y un archivo VHDX.
4. En una consola de PowerShell, cambie el directorio actual a la ubicación donde se encuentra el contenido del archivo ZIP y ejecute este comando:

```
.\connector-appliance-install.ps1
<!--NeedCopy-->
```

5. Cuando se le solicite, escriba un nombre para la máquina virtual o seleccione **Introducir** para aceptar el valor predeterminado de **Connector Appliance**.
6. Cuando se le solicite, escriba un destino para el disco raíz o presione Entrar para usar el directorio predeterminado del sistema para los discos duros virtuales.
7. Cuando se le solicite, escriba un nombre de archivo para el disco raíz o seleccione **Introducir** para aceptar el valor predeterminado de connector-appliance.vhdx.
8. Cuando se le solicite, seleccione el modificador que quiere usar. Seleccione **Introducir**.
9. Revise el resumen de la información de importación de la VM. Si la información es correcta, seleccione **Introducir** para continuar. El script crea e inicia la VM de Connector Appliance.

Una vez implementado e iniciado correctamente el Connector Appliance, la consola muestra una página de destino que contiene la dirección IP de Connector Appliance. Utilice esta dirección IP para conectarse al Connector Appliance y complete el proceso de registro.

Paso siguiente: Registrar el Connector Appliance en Citrix Cloud.

Nutanix AHV

En esta sección se describe cómo implementar Connector Appliance desde el archivo `connector-appliance.vhdx` en un host de Nutanix AHV mediante la consola web de Nutanix Prism.

1. En el menú principal de la consola web de Nutanix Prism, seleccione la vista **Storage**.
2. Haga clic en **+ Storage Container** para crear un contenedor de almacenamiento con el archivo de imagen del Connector Appliance. Como alternativa, puede utilizar un contenedor de almacenamiento existente.
3. Cargue el archivo `connector-appliance.vhdx` a su contenedor de almacenamiento.

a) En el menú principal de la consola web, seleccione **Settings**.
b) Seleccione la ficha **Image Configuration** y haga clic en **+ Upload Image**.
c) En **Create Image**, especifique un nombre para la imagen en **Name**.
d) En la lista **Image Type**, seleccione **DISK**.
e) En la lista **Storage Container**, seleccione el contenedor de almacenamiento que creó.
f) Seleccione **Upload a file**.
g) Haga clic en **Choose file** y vaya al archivo `connector-appliance.vhdx` en su sistema local.
h) Haga clic en **Guardar**.

4. Espere hasta que se haya creado la imagen y su estado aparezca como **ACTIVE** en la página **Image Configuration**.
5. Seleccione la ficha **Network Configuration**.
6. Haga clic en **+ Create Network** para crear una red que pueda usar el Connector Appliance.
7. En la página **Create Network**, especifique la siguiente información:

   - El nombre de la red.
   - El ID de VLAN de la red.

8. En el menú principal de la consola web, seleccione la vista **VM**.
9. Haga clic en **+ Create VM** para crear una instancia del Connector Appliance.
10. En **Create VM**, especifique la siguiente información:

    - Nombre de la máquina virtual
    - La cantidad de vCPU
    - La cantidad de memoria en GiB

11. Seleccione esta opción para usar **Legacy BIOS**.
12. Haga clic en **+ Add New Disk** para agregar un disco a la máquina virtual.
13. En **Add Disk**, complete la siguiente información:

    a) En **Type**, seleccione **DISK**.
    b) En **Operation**, seleccione **Clone from Image Service**.
    c) Para **Bus Type**, seleccione **SCSI**.
    d) En **Image**, seleccione la imagen que creó al cargar el archivo del Connector Appliance.

14. Haga clic en **Add** para terminar de agregar el disco.
15. En **Create VM**, haga clic en **+ Add New NIC**.
16. En **Create NIC**, seleccione la red a la que quiere agregar la máquina virtual.

17. En **Network Connection State**, seleccione **Connected**.
18. Haga clic en **Add** para terminar de agregar la NIC.
19. Haga clic en **Save** para crear la máquina virtual.

    De forma predeterminada, la nueva máquina virtual está apagada.
20. En la vista **VM**, seleccione la máquina virtual y haga clic en **Power on**.
21. Espere a que se inicie la máquina virtual. Este proceso puede tardar unos minutos.

Una vez que el Connector Appliance se haya implementado y se haya iniciado correctamente, puede encontrar la dirección IP del Connector Appliance en uno de los siguientes lugares:

- En la vista **VM** de la consola web de Nutanix Prism.
- En la consola del Connector Appliance.

Utilice esta dirección IP para conectarse a la página de administración de Connector Appliance y completar el proceso de registro.

Paso siguiente: Registrar el Connector Appliance en Citrix Cloud.

Microsoft Azure

En esta sección se describe cómo implementar el Connector Appliance en Microsoft Azure. Puede implementar el Connector Appliance desde Azure Marketplace o desde la imagen de disco descargada mediante el script de PowerShell incluido.

Implementar el Connector Appliance desde Azure Marketplace Para implementar el Connector Appliance desde Azure Marketplace, siga estos pasos:

1. Vaya al Connector Appliance en Azure Marketplace (Azure Marketplace).

   También puede buscar "Connector Appliance for Cloud Services"en el buscador de la tienda.
2. Haga clic en **Get It Now** y, luego, en **Create**.
3. En la página **Create Citrix Connector Appliance for Cloud Services**, complete esta información:

   - Seleccione la **suscripción** (Subscription) que quiera usar.
   - Seleccione el **grupo de recursos** (Resource group) que quiera usar.
   - Seleccione la **región** (Region) en la que quiere ubicar el Connector Appliance.
   - Especifique un **nombre de máquina virtual** (VM name).
   - Seleccione una **red virtual** (Virtual network) a la que agregar el Connector Appliance. Esta red se usa para acceder a Citrix Cloud, a los recursos locales y a la página de administración de Connector Appliance. Esta red no se puede cambiar más adelante.

- Especifique un valor para **Subred** (Subnet).

Haga clic en **Next: Tags >**.

4. En la ficha **Tags**, agregue las etiquetas que necesite.

   Haga clic en **Next: Review + create >**.

5. Una vez revisados los detalles de la implementación, haga clic en **Create**.

Una vez implementado e iniciado correctamente el Connector Appliance, la consola muestra una página de destino que contiene la dirección IP de Connector Appliance. Utilice esta dirección IP para conectarse a la página de administración de Connector Appliance y completar el proceso de registro.

Paso siguiente: Registrar el Connector Appliance en Citrix Cloud.

Implementar la VM de Connector Appliance mediante un script de PowerShell El archivo `connector-appliance-azure.zip` contiene un script de PowerShell que crea e inicia una nueva VM. Puede utilizar el script proporcionado como base para crear o modificar su propio script local.

Antes de ejecutar el script, compruebe que tiene estos requisitos previos:

- Instale el módulo Az PowerShell en su entorno local de PowerShell.
- Ejecute el script de PowerShell en el directorio donde se encuentra el archivo VHD.

Siga estos pasos:

1. Copie o descargue el archivo ZIP de Connector Appliance en su sistema Windows.
2. Extraiga el contenido del archivo ZIP: un script de PowerShell y un archivo VHD.
3. Abra una consola de PowerShell como administrador.
4. Cambie el directorio actual a la ubicación donde se halla el contenido del archivo ZIP y ejecute este comando:

   ```
   .\connector-appliance-upload-Azure.ps1
   ```

5. Aparece un cuadro de diálogo en el que se le solicita que inicie sesión en Microsoft Azure. Introduzca sus credenciales.
6. Cuando aparezca la solicitud del script de PowerShell, seleccione la suscripción que quiere utilizar. Presione Entrar.
7. Siga las instrucciones del script, que le guiarán a través de la carga de la imagen y la creación de una máquina virtual.

8. Una vez creada la primera máquina virtual, el script le preguntará si quiere crear otra máquina virtual a partir de la imagen cargada.

    - Escriba y para crear otra máquina virtual.
    - Escriba n para salir del script.

Una vez implementado e iniciado correctamente el Connector Appliance, la consola muestra una página de destino que contiene la dirección IP de Connector Appliance. Utilice esta dirección IP para conectarse a la página de administración de Connector Appliance y completar el proceso de registro.

Paso siguiente: Registrar el Connector Appliance en Citrix Cloud.

AWS

En esta sección se describe cómo implementar el Connector Appliance en AWS. Connector Appliance está disponible como imagen AMI en AWS Marketplace, y le recomendamos que instale el Connector Appliance desde la imagen AMI. También puede implementar una imagen de disco descargada mediante la interfaz de usuario de AWS o el script de PowerShell incluido.

Requisitos previos de red Para implementar el Connector Appliance en AWS, asegúrese de que tiene acceso a Citrix Cloud desde la subred en la que se creó el Connector Appliance.

Recomendamos usar una dirección IP privada para el dispositivo, que requiere una configuración específica para proporcionar acceso a Citrix Cloud. Para conseguir esta configuración, realice los siguientes pasos en la **consola de administración de AWS**:

1. Cree la puerta de enlace NAT.

    a) En la barra de navegación superior, seleccione **Services > VPC > NAT Gateways**.

    b) En la sección superior derecha, haga clic en **Create NAT Gateway**. Introduzca la siguiente información:

        - Introduzca un nombre (**Name**).
        - Seleccione una subred (**subnet**) de la lista.
        - Establezca **Connectivity type** en **Public**.
        - Seleccione un **ID de asignación de IP elástica** de la lista. Si no hay una IP elástica disponible, haga clic en **Allocate Elastic IP** y siga las instrucciones para crear una.

    c) Haga clic en **Create NAT Gateway**.

2. Cree una entrada de tabla de redirección que incluya la puerta de enlace NAT.

    a) En la barra de navegación superior, seleccione **Services > VPC > Route Tables**.

b) En la parte superior derecha, haga clic en **Create route table**. Introduzca la siguiente información:

- Introduzca un nombre (**Name**).
- En la lista, seleccione la VPC que contiene la subred que seleccionó al crear la puerta de enlace NAT.

c) Haga clic en **Create route table**.

d) En la ficha **Routes** de la tabla de redirección que creó, haga clic en **Edit routes > Add route**.

e) Complete los campos **Destination** (destino) y **Target** (objetivo) para la nueva entrada de ruta.

- Establezca el destino en 0.0.0.0/0.
- Para el objetivo, seleccione la **puerta de enlace NAT** que creó en la lista.

f) Haga clic en **Save change**.

3. Conecte la subred que se va a utilizar para el Connector Appliance a esta tabla de redirección.

a) En la barra de navegación superior, seleccione **Services > VPC > Route Tables**.
b) Seleccione la tabla de redirección que contiene la puerta de enlace NAT.
c) En la página de presentación, vaya a la ficha **Subnet Associations**.
d) Haga clic en **Edit subnet associations**.
e) Seleccione la subred o subredes que conectar a la tabla de redirección.
f) Haga clic en **Save Associations**.

Implementar el Connector Appliance desde AWS Marketplace Antes de empezar, compruebe que cumple los siguientes requisitos previos:

- Tiene permisos para operar los recursos de EC2.
- Ha completado la configuración en Networking prerequisites.
- (Opcional) Puede crear un grupo de seguridad que restrinja qué direcciones IP tienen permiso para acceder a su Connector Appliance.

Siga estos pasos:

1. Inicie sesión en la **consola de administración de AWS**.
2. Busque la imagen AMI de Connector Appliance en AWS Marketplace. Puede hacerlo de estas maneras:

- Siga el enlace de la tienda que se proporciona en Citrix Cloud (AWS Marketplace).
- Busque la imagen AMI en AWS Management Console:

a) Vaya a **Services > Compute > EC2 > AMIs**.
b) Asegúrese de que se halla en la región US East (Ohio).
c) En **Public images**, busque "Citrix Connector Appliance"o el ID de AMI "ami-026eaf9b3b232577f".

3. Para verificar que tiene la AMI correcta, compruebe el ID de la AMI (ami-026eaf9b3b232577f) y el ID del propietario (414337923189).
4. Copie la AMI en su suscripción:

   a) Vaya a **Actions > Copy AMI**.
   b) En el cuadro de diálogo **Copy AMI**, puede seleccionar la **región de destino** (Destination Region) que necesite.
   c) Haga clic en **Copy AMI**.

5. En la página de resumen de la AMI copiada, haga clic en **Launch instance from AMI**.
6. En el cuadro de diálogo **Launch an instance**, complete estos pasos:

   a) Seleccione la cantidad de instancias que quiera crear. Para disponer de una mayor resistencia, le recomendamos que tenga dos o más Connector Appliances en cada ubicación de recursos.
   b) Especifique el nombre de la instancia.
   c) Para **Instance type**, seleccione **t2.medium**. El tipo de instancia debe tener al menos 4 GB y 2 CPU.
   d) Para **Key pair (login)**, seleccione **Proceed without a key pair**. No se permite el inicio de sesión SSH en el Connector Appliance, por lo que no se necesita ningún par de claves.
   e) Para **Network settings**, en la sección **Firewall (security group)**, configure estos parámetros:
      i. Elija si quiere **crear un grupo de seguridad** (Create security group) o **seleccionar un grupo de seguridad existente** (Select existing security group).
      ii. Desmarque **Allow SSH traffic from the internet**
      iii. Seleccione **Allow HTTPs traffic from the internet**.
      iv. Seleccione **Allow HTTP traffic from the internet**.

   Haga clic en **Launch instance**.

7. Una vez creada la instancia, en la sección **Success**, haga clic en el enlace del ID de la instancia para ver la instancia de Connector Appliance.

   También puede hacer clic en el botón **View all instances** de esta página o ir a **Services > EC2 > Instances**, en AWS Management Console, para ver una lista de sus instancias.

8. Cuando **Instance state** haya cambiado a **Running**, vaya a los detalles de la instancia y utilice la **dirección IPv4 privada** (Private IPv4 address) para conectarse al Connector Appliance y completar el proceso de registro.

Es posible que necesite usar un host bastión para ir a la página de administración de Connector Appliance en la dirección IP interna desde el explorador web y completar el proceso de registro.

De forma predeterminada, el Connector Appliance utiliza DHCP para establecer su configuración de red. Puede modificar esta configuración de red a través de la interfaz web de Connector Appliance. Para obtener más información, consulte Configurar los parámetros de red en la página de administración de Connector Appliances.

Paso siguiente: Registrar el Connector Appliance en Citrix Cloud.

Implementar el Connector Appliance mediante la interfaz de usuario de AWS Antes de empezar, compruebe que cumple los siguientes requisitos previos:

- Tiene permisos para operar los recursos de S3 y EC2.
- Ha creado una directiva y un rol de servicio que tienen acceso de importación de VM. Para obtener más información, consulte https://docs.aws.amazon.com/vm-import/latest/userguide/required-permissions.html#vmimport-role.

  > **Nota:**
  >
  > Para crear un rol de servicio, debe crear un bucket (depósito) de S3. Al crear la directiva, establezca el depósito de S3 que ha creado con acceso de importación de VM.

- Tiene acceso a AWS CloudShell. Solo está disponible en ciertas regiones. Para obtener la lista de regiones en las que se admite AWS CloudShell, consulte https://docs.aws.amazon.com/cloudshell/latest/userguide/supported-aws-regions.html.
- Ha completado la configuración en Networking prerequisites.

Siga estos pasos:

1. En su sistema local, extraiga el contenido de `connector-appliance-aws.zip`.
2. Inicie sesión en la **consola de administración de AWS**.
3. Para crear un depósito de almacenamiento, siga estos pasos. (Como alternativa, puede saltarse estos pasos y usar un depósito de almacenamiento existente).

   a) En la barra de navegación superior, seleccione **Services** > **S3** > **Create bucket**.
   b) Introduzca un nombre único para el depósito. Para obtener información sobre las convenciones de nomenclatura de depósitos en Amazon S3, consulte https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucketnamingrules.html.
   c) Seleccione la región para su depósito. Elija la misma región que su región de AWS, ya que no podrá usar los archivos del depósito si estas regiones son diferentes.
   d) Mantenga la configuración restante en los valores predeterminados y, a continuación, haga clic en **Create bucket**.

4. Haga clic en el nombre del depósito que ha creado. Haga clic en **Upload** > **Add files** y seleccione el archivo `connector-appliance.vhd`. Mantenga los parámetros restantes configurados en los valores predeterminados y haga clic en **Upload**.
5. Haga clic en el archivo cargado. Haga clic en **Copy URI S3**.
6. Haga clic en el **icono de AWS CloudShell** en la barra de navegación superior y ejecute los siguientes comandos:

   a) Cree una tarea para convertir el archivo VHD en una instantánea:

   ```
   aws ec2 import-snapshot --disk-container Format=VHD,Url="<
       S3_URI>"
   ```

   Sustituya el valor del marcador de posición por el URI de S3 que copió en el paso anterior. Por ejemplo: `aws ec2 import-snapshot --disk-container Format=VHD, Url="s3://my-aws-bucket/connector-appliance.vhd"`.

   Este comando se completa cuando el siguiente comando devuelve una cadena JSON que contiene `"Status": "completed"`. Anote el valor `ImportTaskId` de la salida de JSON.

   b) Ejecute este comando:

   ```
   aws ec2 describe-import-snapshot-tasks --import-task-ids <
       ImportTaskId>
   ```

   Reemplace el valor del marcador de posición por el valor `ImportTaskId` copiado en el paso anterior. Por ejemplo: `aws ec2 describe-import-snapshot-tasks --import-task-ids import-snap-0273h2836153itg5`.

7. En la **consola de administración de AWS**, en la barra de navegación superior, seleccione **Services** > **EC2**.
8. En el menú de la izquierda de la pantalla, haga clic en **Snapshots**.
9. Haga clic con el botón secundario en la instantánea que ha creado y, a continuación, en **Create Image**.
10. En el panel que se abre, complete estos pasos:

    a) Introduzca un nombre para su AMI.
    b) Seleccione **Hardware-assisted virtualization**.

    Haga clic en **Crear**.

11. En el menú de la izquierda de la pantalla, haga clic en **AMI**.
12. Haga clic con el botón secundario en la AMI que creó y haga clic en **Launch**.
13. En el panel que se abre, complete estos pasos:

a) Elija el tipo de instancia.
b) (Opcional) Personalice la red en la ficha **Configure Instance**.
c) (Opcional) Adjunte otro volumen en la ficha **Add Storage**.
d) En la ficha **Configure Security Group**, defina las reglas del grupo de seguridad.

Cuando haya revisado el inicio de la instancia, haga clic en **Review and Launch**.

Una vez que el Connector Appliance se haya implementado y se haya iniciado correctamente, vaya a **Services** > **EC2** > **Instances** y seleccione la instancia que ha creado. Utilice la **dirección IPv4 privada** para conectarse a la página de administración de Connector Appliance y complete el proceso de registro. Puede usar un host bastión para ir a la página de administración de Connector Appliance en la dirección IP interna desde el explorador web para continuar el proceso de instalación.

De forma predeterminada, el Connector Appliance utiliza DHCP para establecer su configuración de red. Puede modificar esta configuración de red a través de la interfaz web de Connector Appliance. Para obtener más información, consulte Configurar los parámetros de red en la página de administración de Connector Appliances.

Paso siguiente: Registrar el Connector Appliance en Citrix Cloud.

Implementar el Connector Appliance mediante un script de PowerShell El archivo `connector-appliance-aws.zip` contiene un script de PowerShell que crea e inicia una nueva VM. Antes de ejecutar el script, compruebe que tiene estos requisitos previos:

- Tiene instalado AWS.Tools, AWSPowerShell.NetCore o AWSPowerShell en el sistema. Para obtener más información, consulte https://docs.aws.amazon.com/powershell/latest/userguide/pstools-getting-set-up.html.
- Ha creado una directiva y un rol de servicio que tienen acceso de importación de VM. Tanto el rol de servicio como la directiva deben tener un nombre `vmimport` para que este script de PowerShell funcione. Para obtener más información, consulte https://docs.aws.amazon.com/vm-import/latest/userguide/required-permissions.html#vmimport-role.

  > **Nota:**
  >
  > Para crear un rol de servicio, debe crear un bucket (depósito) de S3. Al crear la directiva, establezca el depósito de S3 que ha creado con acceso de importación de VM.

- Ha creado un grupo de seguridad de Amazon EC2.
- Tiene permisos de S3 y acceso a la API.
- Ha completado la configuración en Networking prerequisites.

Siga estos pasos:

1. En el sistema local, extraiga el contenido de `connector-appliance-aws.zip` en una carpeta.
2. En PowerShell, ejecute los siguientes comandos:

   a) Para poder ejecutar un cmdlet de AWS en su entorno local, ejecute el siguiente comando para agregar un nuevo perfil al almacén de SDK de AWS:

   ```
   Set-AWSCredential -AccessKey <access_key_ID> -SecretKey <
       secret_key> -StoreAs MyProfile
   ```

   Sustituya los valores del marcador de posición por la clave de acceso y la clave secreta. Proporcione un nombre de perfil único. En el ejemplo que hemos ofrecido, es `MyProfile`.

   b) Establezca el perfil en el valor predeterminado:

   ```
   Initialize-AWSDefaultConfiguration -ProfileName MyProfile
   ```

   c) Cambie el directorio actual a la carpeta donde se encuentran los archivos extraídos y ejecute este comando:

   ```
   .\connector-appliance-upload-aws.ps1
   ```

3. Siga las instrucciones del script, que le guiarán en la selección de la región para su implementación de Connector Appliance, la carga de la imagen en el depósito elegido y la introducción de un nombre para su VM.

   - Debe usar el depósito con acceso de importación de VM creado anteriormente.
   - Cuando se le pida que seleccione la nube privada virtual (VPC) que va a usar, seleccione la VPC en la que están configuradas la puerta de enlace NAT y las tablas de redirección.
   - Cuando se le pida que seleccione la subred que va a usar, seleccione la subred conectada a la tabla de redirección que contiene la puerta de enlace NAT.

   Para obtener más información, consulte Requisitos previos de red.

Una vez implementado e iniciado correctamente el Connector Appliance, el script muestra la dirección IP privada de Connector Appliance. Es posible que necesite usar un host bastión para ir a la página de administración de Connector Appliance en la dirección IP interna desde el explorador web y completar el proceso de registro.

De forma predeterminada, el Connector Appliance utiliza DHCP para establecer su configuración de red. Puede modificar esta configuración de red a través de la interfaz web de Connector Appliance. Para obtener más información, consulte Configurar los parámetros de red en la página de administración de Connector Appliances.

Paso siguiente: Registrar el Connector Appliance en Citrix Cloud.

Google Cloud Platform

En esta sección se describe cómo implementar un Connector Appliance en Google Cloud Platform. Puede instalar el Connector Appliance desde Google Cloud Marketplace. También puede implementar una imagen de disco descargada mediante la consola de Google Cloud Platform o con el script de PowerShell incluido.

El archivo `connector-appliance-gcp.zip` contiene:

- `connector-appliance.tar.gz`, que es una imagen de disco del Connector Appliance
- `connector-appliance-upload-gcp.ps1`, que es un script de PowerShell que se puede usar para implementar automáticamente el Connector Appliance

Implementar el Connector Appliance desde Google Cloud Marketplace

1. Inicie sesión en su cuenta de Google.
2. Siga el enlace de la tienda que se proporciona en Citrix Cloud (Google Cloud Marketplace).

   También puede buscar "Connector Appliance for Cloud Services"en el buscador de la tienda.
3. Haga clic en **Launch**.
4. En la página **New Citrix Connector Appliance for Cloud Services deployment**, complete esta información:

   - Especifique un nombre en **Deployment name** para el trabajo de implementación.
   - Seleccione la zona o **Zone** en la que quiere ubicar el Connector Appliance.
   - Seleccione la familia de máquinas (**Machine family**), la serie (**Series**) y el tipo de máquina (**Machine type**) que quiera utilizar.
   - Seleccione el tipo de disco de arranque (**Boot disk type**) y el tamaño del disco de arranque en GB (**Boot disk size in GB**) que quiere utilizar.
   - En la sección **Networking**, especifique la interfaz de red que utilizará el Connector Appliance. Si quiere poder conectarse a la página de administración desde una red pública, especifique una IP externa (**External IP**).

   Haga clic en **Deploy**. Se le dirigirá a la página **Deployment Manager**.

   > **Nota:**
   >
   > Una vez que el Connector Appliance se haya implementado y se haya iniciado correctamente, recibirá un correo electrónico para confirmar que el Connector Appliance está implementado en Google Cloud Platform.

5. En la página **Deployment Manager**, haga clic en el nombre de la instancia. También puede buscar la instancia de Connector Appliance que creó en **Compute Engine**.

6. Si especificó anteriormente una IP externa (**External IP**) al configurar la interfaz de red de su Connector Appliance, copie **External IP address** en la sección **Network interfaces** de la ficha **Details**. Utilice esta dirección IP para conectarse a la página de administración de Connector Appliance y completar el proceso de registro. También puede usar **Primary internal IP address** para visitar la página de administración del Connector Appliance desde otra máquina quipo que se encuentre en la misma subred que su Connector Appliance.

Paso siguiente: Registrar el Connector Appliance en Citrix Cloud.

Implementar el Connector Appliance mediante la consola de Google Cloud Platform

1. En su sistema local, extraiga el contenido de `connector-appliance-gcp.zip`.
2. En su proyecto de Google Cloud Platform, cree un segmento de almacenamiento (también puede utilizar un segmento de almacenamiento existente).
   a) En el menú principal, seleccione **Cloud Storage**.
   b) En el panel principal, seleccione **Crear segmento**.
   c) Especifique el nombre del segmento.
   d) Configure los parámetros de acceso y almacenamiento de datos que necesite. Puede dejar estos parámetros como valores predeterminados.
   e) Haga clic en **Crear**.
3. Dentro del segmento de almacenamiento, seleccione **Subir archivos** y elija el archivo `connector-appliance.tar.gz`. Espere mientras se carga el archivo.
4. Seleccione el archivo cargado para ver sus detalles. Copie el valor del **URI de gsutil** en el portapapeles.
5. Para abrir Cloud Shell, haga clic en el icono **Activar Cloud Shell** de la barra del encabezado.
6. En Cloud Shell, ejecute este comando para crear una imagen:

```
gcloud compute images create "Image name" --guest-os-features=
    MULTI_IP_SUBNET --source-uri="gsutil URI of uploaded connector-
    appliance.tar.gz file"
```

7. En el menú principal, seleccione **Compute Engine** > **Instancias de VM**.
8. Seleccione **Crear instancia**. En el panel que se abre, especifique esta información:
   a) En el campo **Nombre**, especifique el nombre de la instancia de Connector Appliance.
   b) Elija una región en la que ubicar el Connector Appliance.
   c) Elija la configuración de la máquina.
   d) En la sección **Disco de arranque**, haga clic en **Cambiar**.
   e) En la sección que se abre, vaya a la ficha **Imágenes personalizadas**.
   f) En la lista **Imagen**, seleccione la imagen que acaba de crear.

g) Haga clic en **Seleccionar**.
h) En la sección **Firewall**, habilite el tráfico HTTPS para permitir el acceso a la página de administración de Connector Appliance.
i) Especifique las configuraciones adicionales que necesite. Por ejemplo, es posible que no quiera usar la configuración de red predeterminada.

Haga clic en **Crear**.

9. En la sección **Instancias de VM**, seleccione la máquina virtual recién creada para ver información detallada sobre ella.

Una vez implementado e iniciado correctamente el Connector Appliance, la sección **Instancias de VM** muestra las direcciones IP de Connector Appliance.

Si el Connector Appliance tiene una dirección IP externa, puede usar esta dirección IP para ir a la página de administración de Connector Appliance desde el explorador web y complete el proceso de registro.

Si el Connector Appliance solo tiene una dirección IP interna, utilice un host bastión para ir a la página de administración de Connector Appliance desde el explorador web y complete el proceso de registro. Para obtener más información, consulte https://cloud.google.com/compute/docs/connect/ssh-using-bastion-host.

Paso siguiente: Registrar el Connector Appliance en Citrix Cloud.

Implementar el Connector Appliance mediante un script de PowerShell Para usar el script de PowerShell proporcionado para implementar el Connector Appliance, debe tener el SDK de Google Cloud instalado en el sistema.

1. En el sistema local, extraiga el contenido de `connector-appliance-gcp.zip` en una carpeta.
2. En PowerShell, cambie el directorio a la carpeta donde se encuentran los archivos extraídos.
3. Ejecute el comando `.\connector-appliance-upload-GCP.ps1`.
4. En la ventana del explorador web que se abre, autentíquese en el SDK de Google Cloud con una cuenta que tenga acceso al proyecto en el que quiere implementar el Connector Appliance.
5. En Google Cloud Tools for PowerShell, cuando el script de PowerShell lo solicite, seleccione el proyecto que quiere usar. Presione Entrar.
6. Siga las instrucciones del script, que le guiarán a través de la carga del disco, la creación de una imagen y la creación de una máquina virtual.
7. Una vez creada la primera máquina virtual, el script le preguntará si quiere crear otra máquina virtual a partir de la imagen cargada.

- Escriba y para crear otra máquina virtual.
- Escriba n para salir del script.

Una vez implementado e iniciado correctamente el Connector Appliance, el script muestra la dirección IP interna de Connector Appliance. Si quiere, también puede ir a la consola de Google Cloud Platform para buscar la dirección IP interna de Connector Appliance. La sección **Compute Engine** > **Instancias de VM** muestra la dirección IP de Connector Appliance.

Utilice un host bastión para ir a la página de administración de Connector Appliance en la dirección IP interna desde el explorador web y completar el proceso de registro. Para obtener más información, consulte https://cloud.google.com/compute/docs/connect/ssh-using-bastion-host.

Paso siguiente: Registrar el Connector Appliance en Citrix Cloud.

Registrar el Connector Appliance en Citrix Cloud

Debe registrar un Connector Appliance en Citrix Cloud para ofrecer un canal de comunicación entre Citrix Cloud y las ubicaciones de recursos.

Después de instalar el Connector Appliance en el hipervisor e iniciarlo, la consola muestra la dirección IP de Connector Appliance. La consola también muestra una huella digital SSL que sirve para validar la conexión a la interfaz de usuario de Connector Appliance.

1. Copie la dirección IP de Connector Appliance en la barra de direcciones del explorador web.

> **Nota:**
>
> Es posible que tenga que incluir `https://` al principio de la dirección IP.

La interfaz de usuario de Connector Appliance utiliza un certificado autofirmado que tiene validez durante cinco años. Como resultado, es posible que aparezca un mensaje que informa de que la conexión no es segura. Para verificar la conexión con el Connector Appliance, puede comparar la huella digital SSL de la consola con la huella digital que el explorador recibe de la página web.

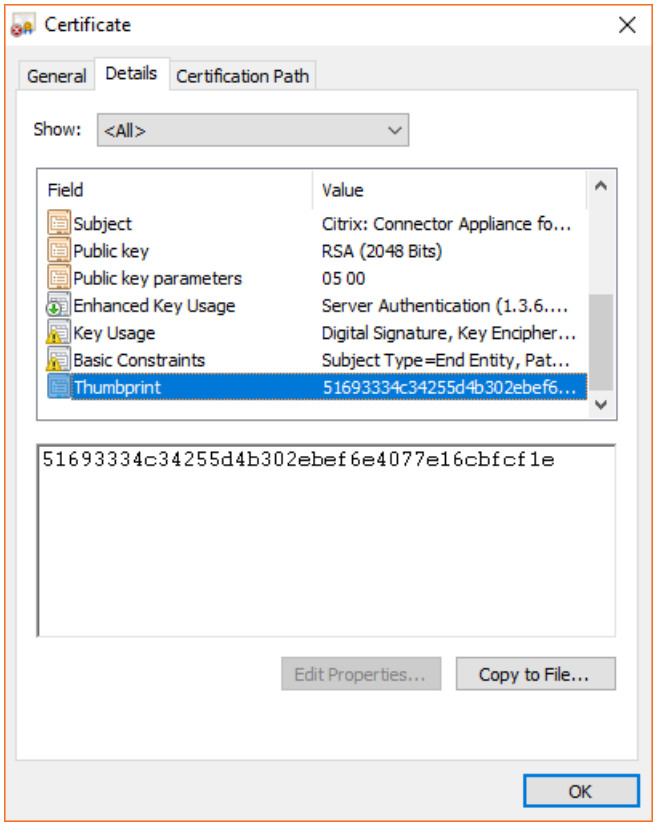
Por ejemplo, en el explorador Google Chrome, complete los siguientes pasos:

a) Haga clic en el marcador **No seguro** situado junto a la barra de direcciones.

b) Seleccione **Certificado**. Se abrirá la ventana **Certificado**.

c) Vaya a la ficha **Detalles** y busque el campo **Huella digital**.

   Si el valor del campo **Huella digital** y la huella digital SSL proporcionada en la consola coinciden, puede confirmar que el explorador se está conectando directamente a la interfaz de usuario de Connector Appliance.

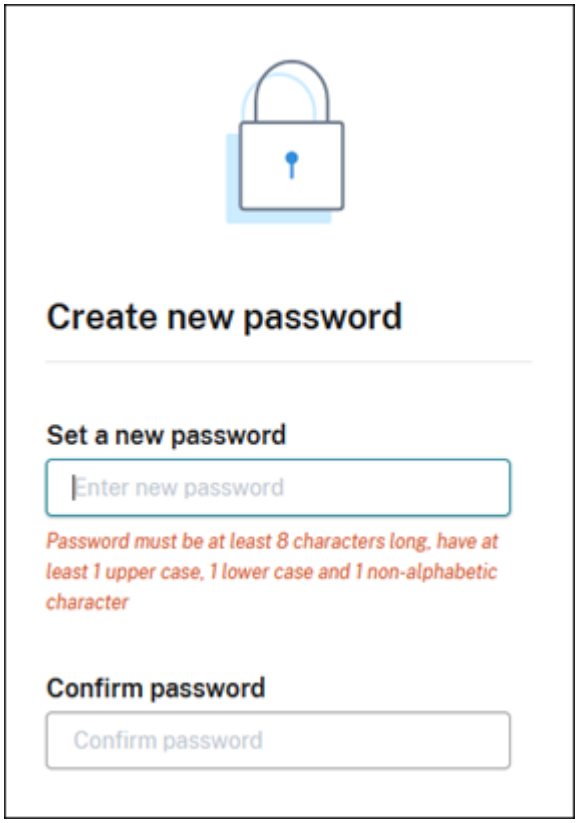


Puede reemplazar este certificado autofirmado por uno propio firmado por su organización o generado mediante la cadena de confianza de su organización. Para obtener más información, consulte Administrar certificados.

2. Si su explorador requiere un paso adicional para confirmar que quiere continuar hacia el sitio, complete este paso ahora.

   Se abrirá la página web **Crear contraseña**.

3. Cree una contraseña para la interfaz de usuario de Connector Appliance y haga clic en **Establecer contraseña**.

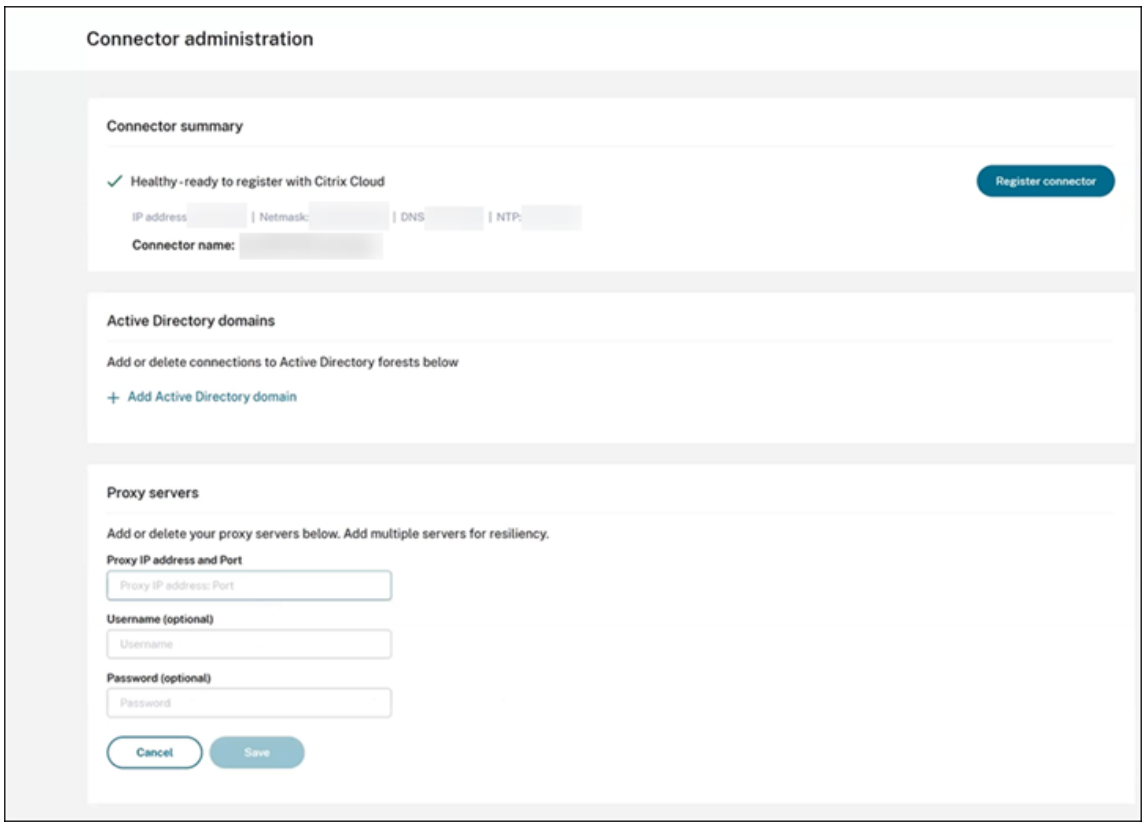


   La contraseña que establezca deberá cumplir los siguientes requisitos:

   - 8 o más caracteres de longitud
   - Contiene letras mayúsculas y minúsculas
   - Contiene al menos un carácter no alfabético

   Guarde esta contraseña en un lugar seguro para uso en el futuro.

4. Inicie sesión con la contraseña que acaba de establecer. Se abrirá la página de **administración de Connectors**.



5. (Opcional) Si utiliza uno o más servidores proxy web, puede agregar las direcciones proxy en la sección **Servidores proxy**. Se admiten proxys autenticados y no autenticados. Para agregar un proxy no autenticado, proporcione una **dirección IP y un puerto de proxy** válidos. Para agregar un proxy autenticado, proporcione también un nombre de **usuario** y una **contraseña** válidos.

   > **Nota:**
   >
   > Solo se admite la autenticación de proxy básica. No se admiten otras formas de autenticación.

   Solo el tráfico a sistemas externos se redirige a través del proxy web. Para obtener más información, consulte Comunicación de Connector Appliance.

6. (Opcional) Si su red usa proxies web que interceptan TLS para acceder a Internet, es posible que necesite que su Connector confíe en su entidad de certificación raíz para comunicarse correctamente con la nube.

   a) En **Entidades de certificación raíz**, seleccione **Agregar certificado**.

   b) Copie el contenido del certificado en formato PEM:

   ```
   -----BEGIN CERTIFICATE-----
   <certificate-base64-bytes>
   -----END CERTIFICATE-----
   ```



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

c) En **Detalles completos de certificado**, pegue el contenido del certificado.

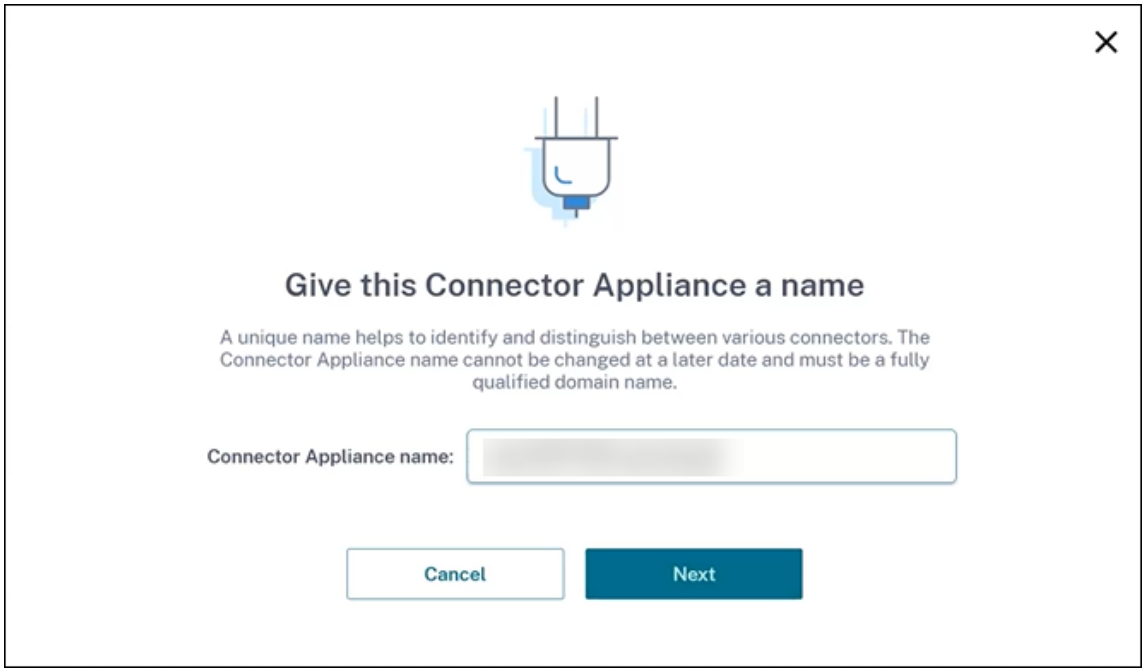
d) Seleccione **Agregar certificado**.

Para agregar una RootCA mediante las API de Connector Appliance, consulte Managing root certificate authorities en la documentación para desarrolladores de Citrix.

> **Nota:**
>
> Los certificados que hayan caducado o que caduquen en los próximos 30 días mostrarán una advertencia.

7. Haga clic en **Registrar Connector** para abrir la tarea de registro.
8. Elija un nombre para el Connector Appliance. Este nombre puede servirle para distinguir entre los diversos Connector Appliances que existen en la ubicación de recursos. Después de registrar el Connector Appliance, el nombre no se puede cambiar.

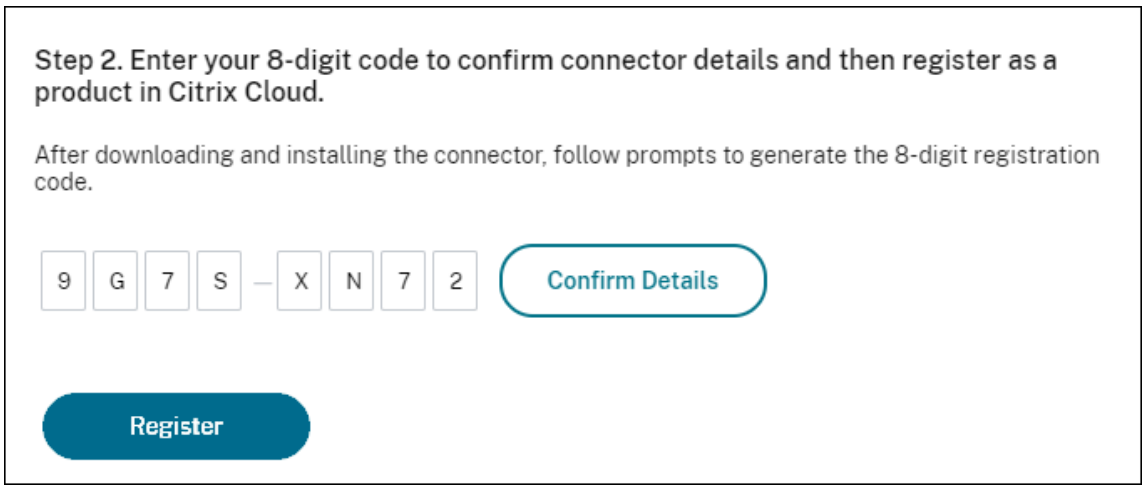
   Introduzca el nombre en el campo **Nombre de Connector Appliance** y haga clic en **Siguiente**.



   La página web proporciona un código para registrarse en Citrix Cloud. Este código caduca a los 15 minutos.

9. Utilice el botón **Copiar** para copiar el código en el portapapeles.
10. Vuelva a la página web **Ubicaciones de recursos**.
11. Pegue el código en el **paso 2** de la tarea **Instalar Connector Appliance**. Haga clic en **Confirmar detalles**.

    Citrix Cloud comprueba que el Connector Appliance esté presente y se puede contactar con él. Si el código de registro ha caducado, se le pedirá que genere un código nuevo.



12. Haga clic en **Registrar**.

    La página muestra si el registro se realizó correctamente. Si se produjo un error en el registro, se le pedirá que vuelva a intentarlo.

13. Haga clic en **Cerrar**.

La **página de administración de Connector Appliances** también le permite descargar un informe de diagnóstico de Connector Appliance. Para obtener más información, consulte Generar un informe de diagnóstico.

Después de registrar el Connector Appliance

Para cada ubicación de recursos, le recomendamos que instale y registre dos o varios Connector Appliances. Esta configuración garantiza una disponibilidad continua y permite a los conectores equilibrar la carga.

No puede administrar directamente el Connector Appliance.

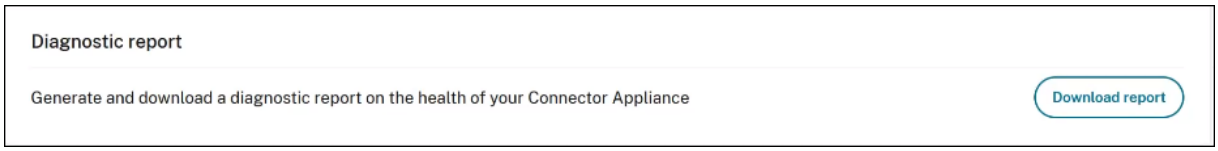
Connector Appliance se actualiza automáticamente. No es necesario que haga nada para actualizar el conector. Puede especificar la hora y el día en que quiera aplicar las actualizaciones de Connector Appliance en la ubicación de recursos. Para obtener más información, consulte Actualizaciones de los Connectors.

No clone, suspenda ni realice una instantánea de las máquinas virtuales de Connector Appliance. Estas acciones no están disponibles.

Solo se mostrará la página **Crear contraseña** la primera vez que se conecte a la interfaz de usuario de Connector Appliance. Guarde esta contraseña en un lugar seguro para uso en el futuro. No se puede restablecer esta contraseña. Si olvida la contraseña, debe instalar de nuevo el Connector Appliance. En conexiones posteriores a la interfaz de usuario, se le pedirá que introduzca la contraseña establecida al registrar el Connector Appliance.

Generar un informe de diagnóstico

Puede generar y descargar un informe de diagnóstico desde la **página de administración de Connector Appliances**.



1. Desde la consola de Connector Appliance del hipervisor, copie la dirección IP en la barra de direcciones del explorador web.
2. Introduzca la contraseña que estableció al registrar su Connector Appliance.
3. En la sección **Informe de diagnóstico** de la página, haga clic en **Descargar informe**.

Los informes de diagnóstico se proporcionan en un archivo `.zip`.

Comprobar la conexión de red

Puede comprobar la conexión de red desde la **página de administración de Connector Appliance** mediante la comprobación de diagnóstico **Captura de TCP**.

1. En la **página de administración de Connector Appliance**, haga clic en el nombre de su cuenta en la barra de encabezado y seleccione **Diagnóstico de red**.
2. (Opcional) En la sección **Captura de TCP**, introduzca la dirección IP, el nombre de host o el puerto de destino para restringir la captura de TCP.
3. En el menú **Duración del rastreo**, seleccione la duración correspondiente.
4. (Opcional) Habilite el **Rastreo de paquetes** para capturar el contenido de los paquetes.

   Cuando el rastreo de paquetes está inhabilitado, la funcionalidad de captura de TCP utiliza la premisa de "en la medida de lo posible"para capturar los encabezados para el diagnóstico. Este enfoque de "en la medida de lo posible"captura los primeros 94 bytes de cada paquete. Sin embargo, dado que los encabezados no tienen un tamaño fijo, es posible que no se capture todo el encabezado.
5. Haga clic en **Iniciar rastreo**.
6. Espere hasta que el rastreo se complete. Una vez finalizado, puede descargar un informe o iniciar un nuevo rastreo.

   - Haga clic en **Descargar** para descargar el informe de seguimiento. El informe de seguimiento se proporciona en un archivo `.pcap`.
   - Haga clic en **Iniciar rastreo** para comenzar otro rastreo.

Conectar Active Directory con Citrix Cloud

Puede usar un Connector Appliance para conectar una ubicación de recursos a bosques que no contienen recursos de Citrix Virtual Apps and Desktops. Por ejemplo, en el caso de los clientes de Citrix Secure Private Access o los clientes de Citrix Virtual Apps and Desktops con algunos bosques que solo se utilizan para la autenticación de usuarios.

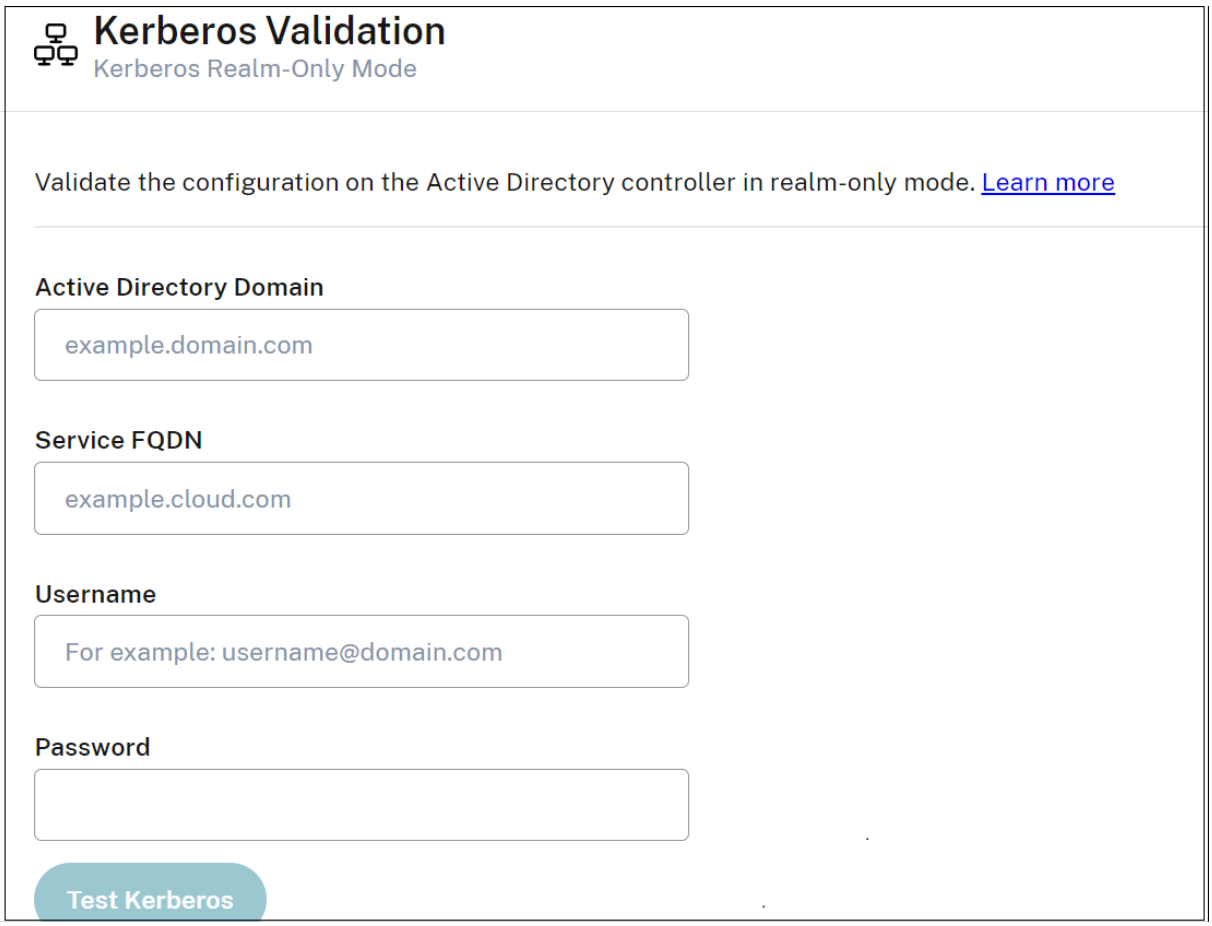
Para obtener más información, consulte Active Directory con el Connector Appliance.

Validar la configuración de Kerberos

Si usa Kerberos para Single Sign-On, puede comprobar que la configuración de su controlador de Active Directory sea correcta en la página **Administración de Connector Appliances**. La función **Validación de Kerberos** le permite validar una configuración del modo de solo dominio de Kerberos o una configuración del modo de delegación limitada de Kerberos (KCD).

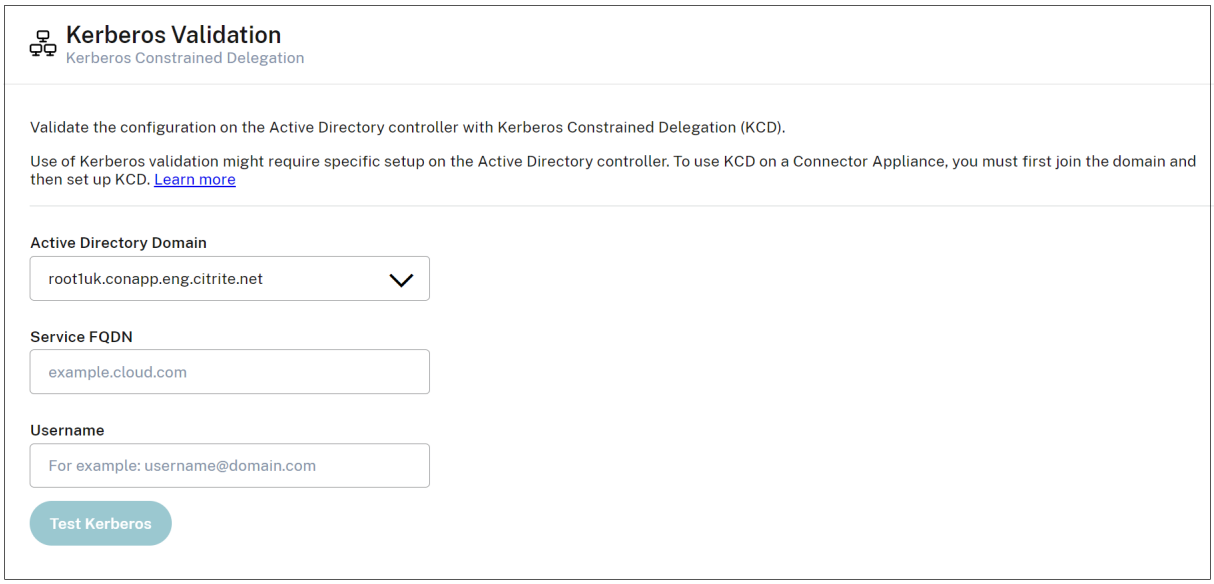
Valide la configuración de solo dominio de Kerberos:

1. Vaya a la página **Administración de Connector Appliances**.
2. Desde la consola de Connector Appliance del hipervisor, copie la dirección IP en la barra de direcciones del explorador web.
3. Introduzca la contraseña que estableció al registrar su Connector Appliance.
4. Para validar la configuración de solo dominio de Kerberos, seleccione la opción **Validación de Kerberos de solo dominio** en la sección **Dominios de Active Directory**.
5. Especifique el **dominio de Active Directory**.
    - Si piensa validar una configuración del modo de solo dominio de Kerberos, puede especificar cualquier dominio de Active Directory. Este modo no depende de la unión al dominio.
6. Especifique el **FQDN del servicio**. Se asume que el nombre de servicio predeterminado es "http". Si especifica "computer.example.com", este valor se considera igual que "https://computer.example.com".
7. Especifique el **nombre de usuario**.
8. Especifique la **Contraseña**.
9. Haga clic en **Probar Kerberos**.



Valide la configuración de la delegación limitada de Kerberos (KCD):

1. Vaya a la página **Administración de Connector Appliances**.
2. Para validar el modo **Delegación limitada de Kerberos (KCD)** de dominios a los que se haya unido el Connector Appliance, seleccione **Validación de Kerberos** en el menú de tres puntos suspensivos (…) del dominio correspondiente.
3. Especifique el **dominio de Active Directory**.
    - Si piensa validar una configuración de delegación limitada de Kerberos, debe seleccionar una opción de una lista de dominios unidos.
4. Especifique el **FQDN del servicio**. Se asume que el nombre de servicio predeterminado es "https". Por ejemplo, especificar "computer.example.com", este valor se considera igual que "https://computer.example.com%E2%80%9D".
5. Especifique el **nombre de usuario**.
    - Para el modo Delegación limitada de Kerberos, también puede validar la configuración de Kerberos mediante cuentas de servicio mediante la selección de la ficha **Cuentas de servicio**.
6. Haga clic en **Probar Kerberos**.



Si la configuración de Kerberos es correcta, verá el mensaje "Configuración de Kerberos validada correctamente". Si la configuración de Kerberos no es correcta, verá un mensaje de error que proporciona información sobre cómo falló la validación.

Para obtener más información sobre Kerberos, consulte la documentación de Microsoft.

Parámetros de red de Connector Appliance

De forma predeterminada, la dirección IP y los parámetros de red de Connector Appliance se asignan automáticamente mediante DHCP.

Una vez registrado el Connector Appliance mediante DHCP, puede modificar sus parámetros de red en la **página de administración de Connector Appliances**.

Sin embargo, si DHCP no está disponible en su entorno o si no tiene acceso a la **página de administración de Connector Appliances**, puede establecer la configuración de red directamente en la consola de Connector Appliance.

Configurar los parámetros de red en la página de administración de Connector Appliances

Una vez registrado el Connector Appliance mediante DHCP, puede modificar sus parámetros de red en la **página de administración de Connector Appliances**.

Para configurar manualmente los parámetros de red:

1. En la sección **Resumen del Connector**, seleccione **Modificar parámetros de red**.
2. En el cuadro de diálogo **Parámetros de red**, elija **Configurar sus propios parámetros de red**.
3. Introduzca la **dirección IP**, la **máscara de subred** y la **puerta de enlace predeterminada**.

4. Agregue al menos un **servidor DNS**.
5. Agregue al menos un **servidor NTP**.
6. Haga clic en **Guardar**.

Al guardar los cambios en los parámetros de red, se reinicia el Connector Appliance. Durante el reinicio, el Connector Appliance no estará disponible temporalmente. Se cerrará la sesión en la **página de administración de Connector Appliance** y la dirección URL de esta página cambia. Puede ver la nueva URL en la consola de Connector Appliance o en la información de red del hipervisor.

Para cambiar la configuración de red de modo que se utilicen valores asignados automáticamente:

1. En la sección **Resumen del Connector**, seleccione **Modificar parámetros de red**.
2. En el cuadro de diálogo **Parámetros de red**, elija **Obtener la dirección IP automáticamente**.
3. Haga clic en **Guardar**.

Al guardar los cambios en los parámetros de red, se reinicia el Connector Appliance. Durante el reinicio, el Connector Appliance no estará disponible temporalmente. Se cerrará la sesión en la **página de administración de Connector Appliance** y la dirección URL de esta página cambia. Puede ver la nueva URL en la consola de Connector Appliance o en la información de red del hipervisor.

Establecer la configuración de red mediante la consola de Connector Appliance

De forma predeterminada, la dirección IP y los parámetros de red de Connector Appliance se asignan automáticamente mediante DHCP. Sin embargo, si DHCP no está disponible en su entorno o si no tiene acceso a la **página de administración de Connector Appliances**, puede establecer la configuración de red directamente en la consola de Connector Appliance.

Para definir la configuración de red:

1. En el hipervisor, reinicie el Connector Appliance.
2. Mientras se inicia el Connector Appliance, observe la consola para ver el mensaje `Welcome to GRUB!`.
3. Cuando lo vea, presione **Esc** para entrar en el menú GRUB.
4. Para modificar los parámetros de arranque, presione **e**.

   Obtendrá una vista similar a esta imagen:

5. Modifique la línea que comienza por `linux` para incluir la configuración de red requerida.

   - Para especificar la red DHCP, agregue `network=dhcp` al final de la línea.
   - Para especificar redes estáticas, agregue los siguientes parámetros al final de la línea:

     ```
     network=static:ip=<static_ip_address>:netmask=<netmask>:route
        =<default_gateway>:dns=<dns_server_1>,<dns_server_2>:ntp=<
        ntp_server_1>,<ntp_server_2>
     <!--NeedCopy-->
     ```

     Reemplace los valores del marcador de posición por los valores de su configuración.

6. Presione **Ctrl+X** para iniciar el Connector Appliance con la nueva configuración.

Cambiar la contraseña de usuario de administrador del Connector Appliance

1. En el menú de usuario de la esquina superior derecha de la consola, seleccione **Cambiar contraseña**.

   Seleccione ![Cambiar contraseña] en el menú.(/en-us/citrix-cloud/media/connector-appliance-change-pw-menu.png)

   Aparece la página Cambiar contraseña.

   Llegará a la página ![Cambiar contraseña].(/en-us/citrix-cloud/media/connector-appliance-change-pw-page.png)

2. Introduzca su contraseña actual y, a continuación, introduzca y confirme la nueva contraseña. La nueva contraseña que establezca deberá cumplir los siguientes requisitos:

- 8 o más caracteres de longitud
- Contiene letras mayúsculas y minúsculas
- Contiene al menos un carácter no alfabético
- No puede ser igual que la contraseña actual

3. Seleccione **Cambiar contraseña** para guardar los cambios.

Citrix Cloud cierra sesión automáticamente y le redirige a la página de inicio de sesión.

Active Directory con el Connector Appliance

April 5, 2024

Puede usar un Connector Appliance para conectar una ubicación de recursos a bosques que no contienen recursos de Citrix Virtual Apps and Desktops. Por ejemplo, en el caso de los clientes de Citrix Secure Private Access o los clientes de Citrix Virtual Apps and Desktops con algunos bosques que solo se utilizan para la autenticación de usuarios.

Al usar Active Directory multidominio con Connector Appliance, se aplican estas restricciones:

- Connector Appliance no se puede usar en lugar de Cloud Connectors en bosques que contienen VDA.

Requisitos

Requisitos de Active Directory

- La máquina debe estar unida a un dominio de Active Directory que contenga los recursos y los usuarios que se usan para crear ofertas para los usuarios. Para obtener más información, consulte Casos de implementación para Connector Appliances en Active Directory en este artículo.
- Cada bosque de Active Directory que piense usar con Citrix Cloud debe ser siempre accesible desde dos Connector Appliances.
- Connector Appliance debe poder llegar a los controladores de dominio, tanto en el dominio raíz del bosque como en los dominios que piensa utilizar con Citrix Cloud. Para obtener más información, consulte los siguientes artículos de asistencia de Microsoft:
  - Cómo configurar dominios y relaciones de confianza
  - Sección "Puertos de servicios de sistemas"en Introducción a los servicios y requisitos de puerto de red para Windows

- Use grupos de seguridad universales, en lugar de grupos de seguridad globales. Esta configuración garantiza que la pertenencia a grupos de usuarios pueda obtenerse de cualquier controlador de dominio del bosque.

Requisitos de la red

- Debe estar conectada a una red que pueda contactar con los recursos que se usan en la ubicación de recursos.
- Debe estar conectada a Internet. Para obtener más información, consulte Requisitos del sistema y de conectividad.

Además de los puertos que aparecen en la comunicación del Connector Appliance, el Connector Appliance requiere una conexión saliente al dominio de Active Directory a través de estos puertos:

Servicio	Puerto	Protocolo de dominio compatible
Kerberos	88	TCP/UDP
End Point Mapper (servicio de localización DCE/RPC)	135	TCP
Servicio de nombres de NetBIOS	137	UDP
Datagrama de NetBIOS	138	UDP
Sesión de NetBIOS	139	TCP
LDAP	389	TCP/UDP
SMB por TCP	445	TCP
Contraseña de Kerberos	464	TCP/UDP
Catálogo global	3268	TCP
Puertos RPC dinámicos	49152–65535	TCP

El Connector Appliance utiliza la firma de LDAP para proteger las conexiones al controlador de dominio. Esto significa que no se requiere LDAP por SSL (LDAPS). Para obtener más información sobre la firma de LDAP, consulte How to enable LDAP signing in Windows Server y Microsoft Guidance for Enabling LDAP Channel Binding and LDAP Signing.

Niveles funcionales admitidos de Active Directory

Connector Appliance se ha probado y es compatible con estos niveles funcionales de bosque y dominio en Active Directory.

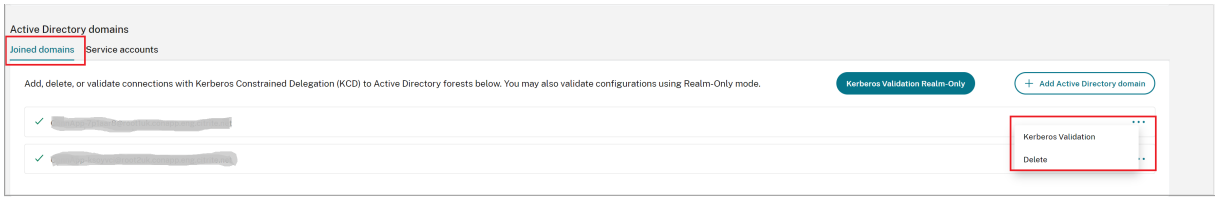
Nivel funcional de bosque	Nivel funcional de dominio	Controladores de dominio admitidos
Windows Server 2016	Windows Server 2016	Windows Server 2019

No se han probado otras combinaciones de controlador de dominio, nivel funcional de bosque ni nivel funcional de dominio con el Connector Appliance. Sin embargo, se espera que estas combinaciones funcionen y también se admitan.

Conectar un dominio de Active Directory a Citrix Cloud mediante Connector Appliance

Al conectarse a la página web de administración de Connector Appliances, la sección de dominios de Active Directory muestra dos fichas.

- **Dominios unidos**: Se utiliza para unir el Connector Appliance a dominios de AD mediante la creación de una cuenta de máquina para el dispositivo del dominio. Para validar Kerberos, haga clic en el menú de tres puntos de la parte derecha del dominio unido. Se requiere la presencia de una cuenta de máquina en el dominio.
- **Cuentas de servicio**: Se utilizan como parte de una solución de Secure Private Access (SPA) para poder usar SSO de Kerberos mediante una cuenta de servicio en lugar de una cuenta de máquina creada al unirse al dominio. Para validar Kerberos, haga clic en el menú de tres puntos de la parte derecha de la cuenta de servicio. Tener un dominio específico asociado a la máquina no es obligatorio. Sin embargo, aunque el Connector Appliance no esté conectado al dominio, puede conectarse al controlador de dominio.



Para configurar Active Directory de modo que se conecte a Citrix Cloud a través de Connector Appliance, complete estos pasos.

1. Instale un Connector Appliance en la ubicación de recursos.

   Puede seguir la información indicada en la documentación de producto de Connector Appliance.

2. 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.
3. En la sección **Dominios de Active Directory**, vaya a la ficha **Dominios unidos**.
4. Haga clic en **+ Agregar dominio de Active Directory**, y aparecerá una nueva ventana emergente para introducir el nombre de dominio.

   Connector Appliance comprueba el dominio. Si la comprobación se realiza correctamente, se abre el cuadro de diálogo **Unirse a Active Directory**. Esta nueva ventana le permite introducir el nombre de usuario y la contraseña para unirse al dominio.

5. Haga clic en **Agregar**.
6. Proporcione el nombre de usuario y la contraseña de un usuario de Active Directory con permiso de unión para el dominio.
7. 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).

   El nombre de esta máquina se crea en el dominio de Active Directory cuando el Connector Appliance se une a él.

8. Haga clic en **Unirse**.

   Ahora el dominio aparece en la sección **Dominios de Active Directory** de la interfaz de usuario de Connector Appliance.

9. Para agregar más **dominios de Active Directory**, seleccione **+ Agregar dominio de Active Directory** y repita los pasos anteriores.
10. Vaya a la página de dominios de la **consola de Citrix Cloud** y seleccione **Connector Appliance** para conectarse a sus dominios.
11. Si aún no ha registrado su Connector Appliance, continúe con los pasos que se describen en Registrar el Connector Appliance en Citrix Cloud.

Si recibe un error al unirse al dominio, compruebe que su entorno cumpla con los requisitos de Active Directory y los requisitos de red.

A continuación

- Puede agregar más dominios a este Connector Appliance.

  > **Nota:**
  >
  > Connector Appliance se prueba con hasta 10 bosques.

- Para mejorar la resiliencia, agregue cada dominio a más de un Connector Appliance en cada ubicación de recursos.

Ver la configuración de Active Directory

Puede ver la configuración de los dominios de Active Directory y los Connector Appliances en sus ubicaciones de recursos en estos lugares:

- En Citrix Cloud:
  1. En el menú, vaya a la página **Administración de acceso e identidad**.
  2. Vaya a la ficha **Dominios**.

     Los dominios de Active Directory se enumeran con las ubicaciones de recursos de las que forman parte.
- En la página web de Connector Appliance:
  1. Conéctese a la página web de Connector Appliance mediante la dirección IP proporcionada en la consola de Connector Appliance.
  2. Inicie sesión con la contraseña que creó al registrarse.
  3. En la sección **Dominios de Active Directory** de la página, puede ver la lista de dominios de Active Directory a los que se ha unido este Connector Appliance.

Quitar un dominio de Active Directory de un Connector Appliance

Para dejar un dominio de Active Directory, siga estos pasos:

1. Conéctese a la página web de Connector Appliance mediante la dirección IP proporcionada en la consola de Connector Appliance.
2. Inicie sesión con la contraseña que creó al registrarse.
3. En la sección **Dominios de Active Directory** de la página, busque el dominio que quiere dejar en la lista de dominios de Active Directory a los que se ha unido.
4. Anote el nombre de la cuenta de máquina creada por su Connector Appliance.

5. Haga clic en el icono de eliminación (papelera) que hay junto al dominio. Se muestra un cuadro de diálogo de confirmación.
6. Haga clic en **Continuar** para confirmar la acción.
7. Vaya a su controlador de Active Directory.
8. Elimine la cuenta de máquina creada por el Connector Appliance del controlador.

Casos de implementación para usar el Connector Appliance con Active Directory

Puede usar Cloud Connectors y Connector Appliances para conectarse a los controladores de Active Directory. El tipo de conector que se va a utilizar depende de la implementación.

Para obtener más información sobre el uso de Cloud Connectors con Active Directory, consulte Casos de implementación para Cloud Connectors en Active Directory.

Use el Connector Appliance para conectar su ubicación de recursos al bosque de Active Directory en estas situaciones:

- Quiere instalar Secure Private Access. Para obtener más información, consulte Secure Private Access con Connector Appliance.
- Tiene al menos un bosque que solo se usa para la autenticación de usuarios
- Quiere reducir la cantidad de conectores necesarios para admitir varios bosques
- Necesita un Connector Appliance para otros casos de uso

Solo los usuarios de al menos un bosque con un único conjunto de Connector Appliances para todos los bosques

Este caso se aplica a los clientes de Workspace Standard o a los clientes que utilizan un Connector Appliance para Secure Private Access.

En este caso, hay varios bosques que contienen solamente objetos de usuario (`forest1.local`, `forest2.local`). Estos bosques no contienen recursos. Un conjunto de Connector Appliances se implementa en una ubicación de recursos y se une a los dominios de cada uno de estos bosques.

- Relación de confianza: Ninguna
- Dominios enumerados en **Administración de acceso e identidad**: `forest1.local`, `forest2.local`
- Inicios de sesión de usuario en Citrix Workspace: Se admiten todos los usuarios
- Inicios de sesión de usuario en una implementación local de StoreFront: Se admiten todos los usuarios

Usuarios y recursos en bosques separados (con confianza) con un único conjunto de Connector Appliances para todos los bosques

Este caso se aplica a los clientes de Citrix Virtual Apps and Desktops con varios bosques.

En este caso, algunos bosques (`resourceforest1.local`, `resourceforest2.local`) contienen sus recursos (por ejemplo, VDA) y algunos bosques (`userforest1.local`, `userforest2.local`) contienen solo sus usuarios. Existe una relación de confianza entre estos bosques, lo que permite a los usuarios iniciar sesión en los recursos.

Se implementa un conjunto de Cloud Connectors en el bosque `resourceforest1.local`. Se implementa un conjunto separado de Cloud Connectors en el bosque `resourceforest2.local`.

Se implementa un conjunto de Connector Appliances en el bosque `userforest1.local`, y el mismo conjunto se implementa en el bosque `userforest2.local`.

- Relación de confianza: Confianza bidireccional de bosques o confianza unidireccional de los bosques de recursos a los bosques de usuarios
- Dominios enumerados en **Administración de acceso e identidad**: `resourceforest1.local`, `resourceforest2.local`, `userforest1.local`, `userforest2.local`
- Inicios de sesión de usuario en Citrix Workspace: Se admiten todos los usuarios
- Inicios de sesión de usuario en una implementación local de StoreFront: Se admiten todos los usuarios

Actualizaciones de los Connectors

August 3, 2023

Periódicamente, Citrix publica actualizaciones para aumentar el rendimiento, la seguridad y la fiabilidad de Cloud Connector o del Connector Appliance. De forma predeterminada, Citrix Cloud instala actualizaciones en cada conector, de una en una, tan pronto como estas actualizaciones estén disponibles. Para garantizar que las actualizaciones se instalen a tiempo sin afectar indebidamente a la experiencia de los usuarios con Citrix Cloud, puede controlar las actualizaciones de los conectores de la siguiente manera:

- Programe las actualizaciones para la hora del día y el día de la semana que prefiera.
- Agregue demoras únicas para que los conectores que especifique se actualicen dos semanas más tarde de lo programado.
- Si se produce un error en la actualización debido a un problema en la máquina host, reinicie la actualización una vez que se haya solucionado el problema.

También puede verificar que sus conectores están actualizados comparando la versión actual del conector en su ubicación de recursos con la versión de destino en Citrix Cloud.

> **Nota:**
>
> En este artículo se describe cómo programar las actualizaciones de los conectores mediante la consola de administración de Citrix Cloud. Para obtener información sobre cómo programar las actualizaciones de los conectores mediante las API de Citrix Cloud, consulte Citrix Cloud - Maintenance Schedules en la documentación de Citrix Developer.

Hora preferida del día

Cuando se especifica una hora preferida del día, Citrix Cloud instala las actualizaciones 24 horas después de que estén disponibles, a la hora preferida. Por ejemplo, si su hora preferida es las 2:00 a.m., hora del Pacífico de EE. UU., y una actualización está disponible el martes, Citrix Cloud espera 24 horas y, a continuación, la instala a las 2:00 a.m. del día siguiente.

Día preferido de la semana

Cuando se especifica un día preferido de la semana, Citrix Cloud espera siete días antes de instalar las actualizaciones en el día preferido. Este período de espera de siete días le da tiempo suficiente para elegir si quiere instalar la actualización a petición o esperar a que Citrix Cloud la instale el día que prefiera. Dependiendo del día de la semana que seleccione y el día en que estén disponibles las actualizaciones, Citrix Cloud podría esperar hasta 13 días para instalar las actualizaciones.

Ejemplo de un período de espera de 8 días

El lunes, configura los martes a las 6:00 p. m. como el día preferido para las actualizaciones. Más tarde ese día, Citrix Cloud le notifica que hay una actualización disponible y muestra el botón **Actualizar**. Si no inicia la actualización, Citrix Cloud espera siete días y, a continuación, la instala al día siguiente, el martes a las 6:00 p.m.

Ejemplo de un período de espera de 13 días

Ha configurado los lunes a las 6:00 p.m. como hora preferida para las actualizaciones. El martes, Citrix Cloud le notifica que hay una actualización disponible y muestra el botón **Actualizar**. Si no inicia la actualización, Citrix Cloud espera siete días y, a continuación, la instala seis días después, el lunes a las 6:00 p.m.

Notificaciones de actualización y actualizaciones a petición

Cuando hay actualizaciones disponibles, Citrix Cloud le informa con una alerta en sus Notificaciones. Además, cada conector muestra la fecha y hora en que se instalará la actualización.

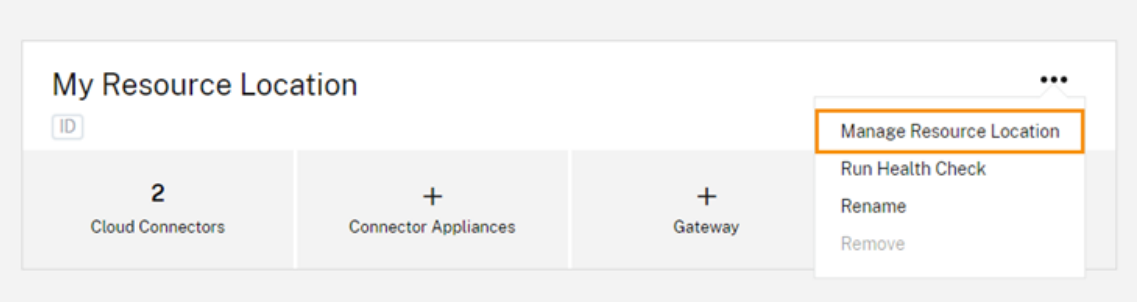
Después de que Citrix Cloud le notifique que hay una actualización disponible, cada conector muestra un botón **Actualizar** para que pueda instalar la actualización antes de su hora o día preferidos. Después de seleccionar **Actualizar** para cada conector, Citrix Cloud pone en cola las actualizaciones y las instala una a una. Una vez iniciadas las actualizaciones, no puede cancelarlas.

Una vez finalizada la actualización, Citrix Cloud muestra la fecha de la última actualización. Si no se puede completar alguna actualización, se enviará una notificación informándole.

Elegir una programación para las actualizaciones

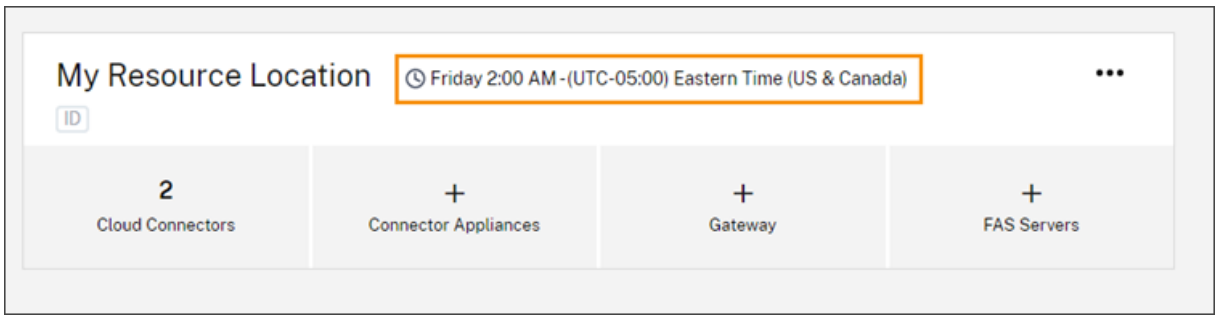
Siga los pasos que se indican en esta sección para programar las actualizaciones de los conectores a través de la consola de administración de Citrix Cloud. Para obtener información sobre cómo programar actualizaciones mediante las API de Citrix Cloud, consulte Citrix Cloud - Maintenance Schedules en la documentación de Citrix Developer.

1. En el menú de Citrix Cloud, seleccione **Ubicaciones de recursos**.
2. Busque la ubicación de recursos que quiere modificar y, en el menú de puntos suspensivos, seleccione **Administrar ubicación de recursos**.



3. En **Elija su método de actualización**, seleccione **Establezca una hora de inicio de mantenimiento** y elija el día, la hora y la zona horaria para instalar las actualizaciones.
    - Para especificar solo una hora preferida del día, seleccione la hora y la zona horaria en la que quiere que se instalen las actualizaciones. Citrix Cloud instala las actualizaciones 24 horas después de que estén disponibles, a la hora preferida.
    - Para especificar un día preferido de la semana, seleccione la hora, el día y la zona horaria. Citrix Cloud espera siete días después de que las actualizaciones estén disponibles antes de instalarlas en el día que prefiera.

Después de configurar la programación de actualización, Citrix Cloud la muestra junto al nombre de la ubicación del recurso.



La hora de inicio que seleccione se aplicará a todos los conectores, independientemente de la zona horaria en la que se encuentren. Si tiene conectores en distintas zonas horarias, Citrix Cloud instala las actualizaciones en la hora y la zona horaria seleccionados. Por ejemplo, si programa actualizaciones para las 2:00 de la madrugada en la zona horaria del Pacífico de Estados Unidos y tiene conectores en Londres, Citrix Cloud comenzará a instalar la actualización en esos conectores a las 2:00 de la madrugada, hora del Pacífico de los Estados Unidos.

Reiniciar actualizaciones

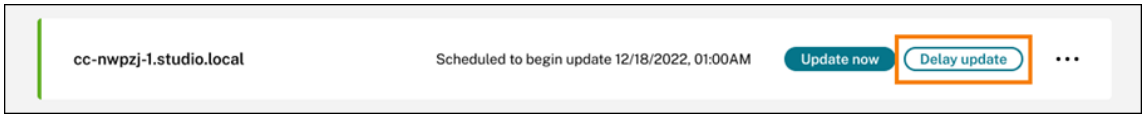
Si el conector experimenta un problema durante la instalación de la actualización, esta se detiene hasta que se resuelve el problema. Dado que las actualizaciones se instalan en cada conector, una a la vez, una actualización en pausa en un conector puede impedir que se actualicen todos los Cloud Connectors restantes de su cuenta de Citrix Cloud. Una vez resuelto el problema, puede reiniciar la actualización.

1. En el menú de Citrix Cloud, seleccione **Ubicaciones de recursos**.
2. Busque la ubicación de recursos que quiere administrar y seleccione el mosaico de **Cloud Connectors** o **Connector Appliances**.
3. Busque el conector que quiera administrar y seleccione **Reiniciar actualizaciones**.

Demorar actualizaciones

Puede demorar actualizaciones programadas para que se produzcan dos semanas más tarde en los conectores que especifique. Puede demorarlas solo una vez. Después de demorar la actualización una vez, no podrá demorarla de nuevo. Tampoco podrá cambiar el período predeterminado de dos semanas.

1. En el menú de Citrix Cloud, seleccione **Ubicaciones de recursos**.
2. Busque la ubicación de recursos que quiere administrar y seleccione el mosaico de **Cloud Connectors** o **Connector Appliances**.
3. Busque el conector que quiera administrar y seleccione **Demorar actualizaciones**.



La fecha programada pasa a ser dos semanas después de la fecha programada originalmente.

Actualizaciones no programadas

Aunque programe actualizaciones para una fecha y hora posteriores, es posible que Citrix Cloud instale igualmente una actualización lo antes posible en cuanto esta esté disponible. Las actualizaciones no programadas se producen cuando:

- La actualización no se puede instalar a la hora preferida, en las 48 horas siguientes a su disponibilidad. Por ejemplo: si la hora preferida es a las 2:00 de la madrugada y el conector está sin conexión durante tres días después de la publicación de la actualización, Citrix Cloud instala la actualización en cuanto el conector vuelve a conectarse.
- La actualización contiene una corrección para un problema vital de la seguridad o de la función.

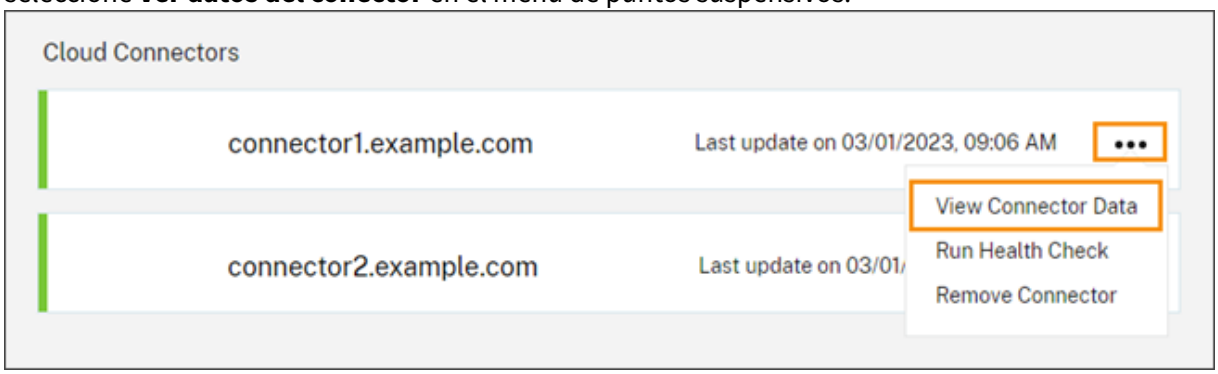
Comparar versiones de Cloud Connector

Puede comprobar la versión de Cloud Connector activa en su ubicación de recursos y si es la versión más reciente. Esta información le ayuda a comprobar que el Cloud Connector se esté actualizando correctamente.

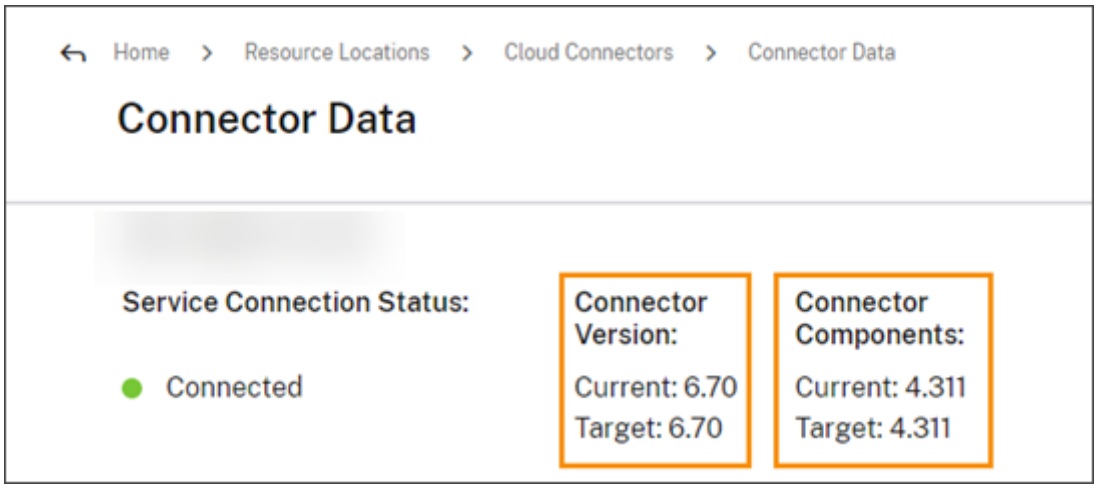
> **Nota:**
>
> Esta información no está disponible para Connector Appliances.

En la página **Ubicaciones de recursos**, seleccione el mosaico **Cloud Connectors** correspondiente a la ubicación de recursos que quiere administrar. Busque el Cloud Connector que quiere examinar y

seleccione **Ver datos del conector** en el menú de puntos suspensivos.



El número de versión **Actual** es la versión del software de Cloud Connector activa actualmente en la máquina de Cloud Connector. El número de versión **Objetivo** es la versión más reciente del software de Cloud Connector publicada por Citrix. Si la máquina se actualizó correctamente, los números de versión Actual y Objetivo coinciden.



Solución de errores de actualización

Software conflictivo instalado en la máquina con Cloud Connector o errores imprevistos durante el mantenimiento pueden provocar que el Cloud Connector no se actualice y se produzcan interrupciones del servicio. Para obtener información sobre cómo solucionar una actualización fallida tras el mantenimiento de Cloud Connector, consulte Resolver un mantenimiento fallido de Cloud Connector.

Si el Cloud Connector no se está actualizando correctamente, puede iniciar la solución de problemas al verificar estas condiciones:

- El Cloud Connector está encendido y conectado a Citrix Cloud mediante la utilidad de comprobación de la conectividad de Cloud Connector.
- Los proxies y los firewalls están configurados correctamente.

- Los servicios de Windows requeridos se hallan en estado Iniciado.
- El registro avanzado está habilitado en el Cloud Connector.

Para obtener instrucciones sobre cómo solucionar errores de actualización de Cloud Connector, consulte CTX270718 en Knowledge Center de Citrix Support.

Para obtener ayuda sobre la solución de problemas, puede enviar registros de Citrix Cloud Connector a Citrix. Para obtener más información, consulte Recopilación de registros para Citrix Cloud Connector.

Administración de acceso e identidad

July 2, 2024

En la sección Administración de acceso e identidad, se definen las cuentas y los proveedores de identidades utilizados para los administradores de Citrix Cloud y los suscriptores de espacios de trabajo.

Proveedores de identidades

Los proveedores de identidades admitidos para Citrix Cloud pueden utilizarse para autenticar a administradores de Citrix Cloud, suscriptores de espacios de trabajo o ambos.

Proveedor de identidades	Autenticación de administradores	Autenticación de suscriptores
Proveedor de identidades de Citrix	Sí	No
Active Directory local	No	Sí
Active Directory y token	No	Sí
Azure Active Directory	Sí	Sí
Citrix Gateway	No	Sí
Google Cloud Identity	Sí	Sí
Okta	No	Sí
SAML 2.0	Sí (solo grupos de AD)	Sí

De forma predeterminada, Citrix Cloud usa el proveedor de identidades de Citrix para administrar su cuenta de Citrix Cloud. El proveedor de identidades de Citrix solo autentica a administradores de Citrix Cloud.

Proveedor de identidades de Citrix

Citrix Cloud incluye el proveedor de identidades de Citrix integrado para autenticar a los administradores cuando inician sesión. En la consola de Citrix Cloud, el proveedor de identidades de Citrix se denomina Citrix Identity.
Si usa un proveedor de identidades diferente para la autenticación de administradores, Citrix recomienda tener al menos un administrador con acceso total en el **proveedor de identidades de Citrix**. Esta condición garantiza que:

- No se le bloqueará el acceso a su cuenta de Citrix Cloud si su proveedor de identidades principal deja de estar disponible.
- Puede acceder a su cuenta de Citrix Cloud para realizar determinadas operaciones que no se pueden completar al iniciar sesión con otro proveedor de identidades, como Azure AD. Por ejemplo, si Azure AD es el proveedor de identidades seleccionado y necesita reiniciar la conexión entre Azure AD y Citrix Cloud, puede realizar esta tarea después de iniciar sesión con el proveedor de identidades de Citrix.

Quitar el proveedor de identidades de Citrix

El proveedor de identidades de Citrix está conectado de forma predeterminada para todas las cuentas nuevas de Citrix Cloud. Si decide no usar el proveedor de identidades de Citrix, puede quitar la conexión, si fuera necesario. Por ejemplo, puede optar por quitar esta conexión para que sea conforme con las directivas de su organización en materia de seguridad y gestión de administradores.

Al quitar esta conexión, se inhabilita el proveedor de identidades de Citrix y por ello se puede usar para autenticar a los administradores de Citrix Cloud.

Para poder quitar la conexión con el proveedor de identidades de Citrix, debe tener otro proveedor de identidades configurado en Citrix Cloud. Citrix Cloud no permite quitar esta conexión sin que haya otro proveedor de identidades configurado.

> **Importante**
>
> Si pierde el acceso al proveedor de identidades elegido, debe contactar con Citrix Support para recuperar su cuenta de Citrix Cloud. Este proceso puede tardar varios días en completarse.

Para quitar la conexión con el proveedor de identidades de Citrix:

1. Desde la consola de administración de Citrix Cloud, haga clic en el botón de menú y seleccione **Administración de acceso e identidad**.
2. En la ficha **Autenticación**, busque el proveedor de identidades de Citrix.
3. Haga clic en el menú de tres puntos y seleccione **Eliminar proveedor de identidades**.

4. Cuando se le pida que confirme la eliminación, seleccione **Comprendo que al quitar este proveedor de identidades también se eliminarán los datos de configuración de este proveedor de identidades en Citrix Cloud**.
5. Haga clic en **Eliminar proveedor de identidades**.

Servicio de autenticación federada de Citrix

Citrix Cloud admite el uso del Servicio de autenticación federada de Citrix para ofrecer acceso con Single Sign-On a los suscriptores de espacios de trabajo. Para obtener más información, consulte los siguientes artículos:

- Conectar FAS con Citrix Cloud: Habilitar Single Sign-On para espacios de trabajo con Citrix Federated Authentication Service
- Citrix Tech Zone:
  - Reference Architecture: Federated Authentication Service
  - Tech Insight: Federated Authentication Service

Administradores

Los administradores usan su identidad para acceder a Citrix Cloud, llevar a cabo actividades de administración e instalar Citrix Cloud Connector.

Un mecanismo de identidad de Citrix ofrece la autenticación para los administradores mediante su dirección de correo electrónico y su contraseña. Los administradores también pueden usar sus credenciales de My Citrix para iniciar sesión en Citrix Cloud.

Autenticación de varios factores

Citrix Cloud proporciona métodos de autenticación de varios factores tanto para los administradores como para los suscriptores del espacio de trabajo.

En el caso de los administradores, la autenticación de varios factores es necesaria para iniciar sesión en Citrix Cloud. Los administradores pueden inscribir sus dispositivos cuando incorporan su cuenta de Citrix Cloud o después de aceptar una invitación de otro administrador. Para obtener información, consulte estos artículos:

- Configurar la autenticación de varios factores
- Administrar el método de autenticación MFA principal
- Administrar los métodos de recuperación de la autenticación MFA

En el caso de los suscriptores del espacio de trabajo, la autenticación de varios factores se habilita cuando los administradores configuran el método de autenticación con Active Directory y token. Active Directory y token es el proveedor de identidades predeterminado para Citrix Workspace. Tras la configuración, los suscriptores inscriben su dispositivo para la autenticación de varios factores. Para obtener información, consulte estos artículos:

- Para habilitar la autenticación con Active Directory y token
- Autenticación de dos factores (opcional)
- Reinscribir un dispositivo

Como alternativa, puede utilizar la autenticación de varios factores de Azure AD tanto para los administradores de Citrix Cloud como para los suscriptores del espacio de trabajo. Para obtener más información sobre los métodos de implementación, consulte Métodos de implementación de MFA de Microsoft Azure.

Agregar nuevos administradores

Durante el proceso de "onboarding"o incorporación de una cuenta, se crea un administrador inicial. Como el primer administrador, puede agregar otros administradores a su cuenta de Citrix Cloud. Esos administradores nuevos pueden utilizar sus credenciales de cuenta de Citrix o configurar una cuenta nueva, si fuera necesario. También puede perfilar los permisos de acceso de los administradores que agregue. La configuración de estos permisos le permite equiparar el nivel de acceso al rol del administrador de su organización.

Para obtener más información sobre cómo agregar administradores y configurar permisos de acceso, consulte Administrar el acceso del administrador.

Restablecer la contraseña

Si olvidó su contraseña o simplemente quiere restablecerla, haga clic en **¿Olvidó su nombre de usuario o su contraseña?** en la página de inicio de sesión de Citrix Cloud. Después de introducir su dirección de correo electrónico o nombre de usuario para encontrar su cuenta, Citrix le envía un mensaje con un enlace para restablecer la contraseña.

Bajo determinadas condiciones, Citrix requiere que restablezca la contraseña para ayudarle a mantener la contraseña de su cuenta segura. Para obtener más información sobre estas condiciones, consulte Cambiar la contraseña.

> **Nota:**
>
> Agregue **customerservice@citrix.com** a su lista de direcciones de correo electrónico permitidas para que los correos electrónicos de Citrix Cloud no terminen en sus carpetas de papelera o correo no deseado.

Quitar administradores

Se pueden quitar administradores de la cuenta de Citrix Cloud en la ficha **Administradores**. Al quitar un administrador, este ya no puede iniciar sesión en Citrix Cloud.

Si un administrador tiene una sesión abierta cuando se quita su cuenta, ese administrador permanecerá activo durante un minuto como máximo. Después, se le denegará el acceso a Citrix Cloud.

> **Nota:**
>
> - Si solo hay un administrador en la cuenta, no se puede quitar ese administrador. Citrix Cloud requiere al menos un administrador para cada cuenta de cliente.
> - Los Citrix Cloud Connectors no están vinculados a las cuentas de administrador. Los Cloud Connectors siguen funcionando, aunque se elimine la cuenta de administrador que los instaló.

Suscriptores

La identidad de un suscriptor define los servicios a los que tiene acceso en Citrix Cloud. Esta identidad proviene de las cuentas de dominio de Active Directory proporcionadas por los dominios dentro de la ubicación de recursos. Cuando se asigna un suscriptor a una oferta de una biblioteca se autoriza el acceso de ese suscriptor a la oferta.

Los administradores pueden controlar qué dominios se usan para proporcionar estas identidades en la ficha **Dominios**. Si va a usar dominios de varios bosques, instale al menos dos Citrix Cloud Connectors en cada bosque. Citrix recomienda contar con al menos dos Citrix Cloud Connectors para mantener un entorno de alta disponibilidad. Para obtener más información sobre la implementación de Cloud Connectors en Active Directory, consulte Casos de implementación para Cloud Connectors en Active Directory.

> **Nota:**
>
> - Al inhabilitar un dominio solo se impide la selección de nuevas identidades de ese dominio. No se impide que los suscriptores usen identidades que ya han sido asignadas.

> - Cada Citrix Cloud Connector puede enumerar y utilizar todos los dominios del único bosque en que esté instalado.

Administrar el uso de los suscriptores

Puede agregar suscriptores a las ofertas mediante cuentas individuales o grupos de Active Directory. El uso de grupos de Active Directory no requiere administración a través de Citrix Cloud, una vez asignado el grupo a una oferta.

Cuando un administrador quita un suscriptor o un grupo de suscriptores de una oferta, esos suscriptores ya no pueden acceder al servicio. Para obtener más información acerca de cómo quitar suscriptores de servicios específicos, consulte la documentación del servicio en cuestión en el sitio web de documentación de productos Citrix.

Ubicaciones de recursos principales

Una ubicación de recursos principal es una ubicación de recursos que se designa como "preferida" para las comunicaciones entre el dominio y Citrix Cloud. Para las ubicaciones de recursos principales, seleccione la ubicación de recursos con Citrix Cloud Connectors que tengan el mejor rendimiento y la mejor conectividad con el dominio. Convertir esta ubicación de recursos en su ubicación de recursos principal permite que los usuarios inicien sesión rápidamente en Citrix Cloud.

Para obtener más información, consulte Seleccionar una ubicación de recursos principal.

Más información

- Obtenga más información sobre los proveedores de identidades admitidos con el curso educativo Introduction to Citrix Identity and Authentication del sitio web de Citrix Training.
- Citrix Tech Zone:
  - Resumen técnico: Identidad del espacio de trabajo
  - Resumen técnico: Workspace Single Sign-On
  - Tech Insight: Mobile SSO

Administrar el acceso de administrador a Citrix Cloud

April 5, 2024

Los administradores se administran desde la consola de Citrix Cloud. Según el proveedor de identidades que utilice para autenticar a los administradores, puede agregar administradores de forma individual o con grupos.

Todos los administradores deben usar tokens como segundo factor de autenticación al iniciar sesión en Citrix Cloud. Después de agregar a un administrador, este puede inscribir su dispositivo en la autenticación de varios factores y generar tokens mediante cualquier aplicación que siga el estándar de contraseña temporal de un solo uso, como Citrix SSO.

Agregar nuevos administradores

Citrix Cloud admite estos proveedores de identidades para autenticar a los administradores:

- Proveedor de identidades de Citrix: El proveedor de identidades predeterminado en Citrix Cloud. Solo permite la incorporación de administradores individuales.
- Azure AD: Permite la incorporación de administradores de forma individual y con grupos de AAD. Los administradores de los grupos de AAD están limitados únicamente a roles de acceso personalizado. Para obtener más información, consulte Administrar grupos de administradores.
- SAML 2.0: Permite la incorporación de administradores únicamente a través de grupos de AD. Para obtener más información, consulte Conectar SAML como proveedor de identidades con Citrix Cloud.

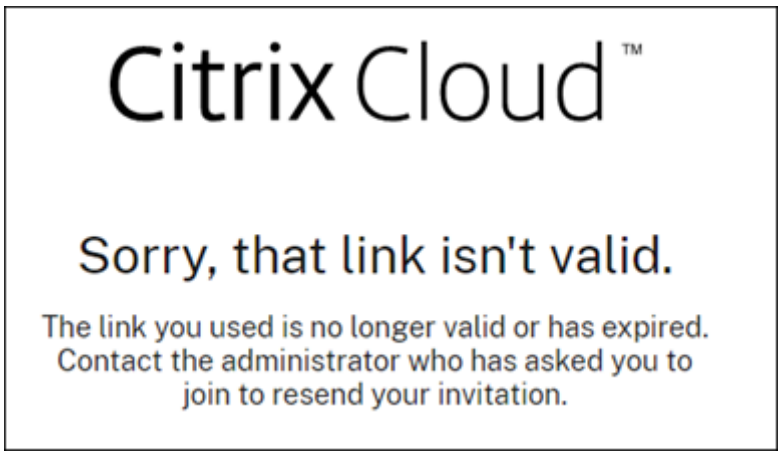
La incorporación de nuevos administradores emplea este flujo de trabajo:

1. Seleccione el proveedor de identidades que quiera usar para autenticar a los administradores.
2. Según el proveedor de identidades, invite a administradores individuales o seleccione los grupos a los que pertenecen los administradores.
3. Especifique los permisos de acceso que se parámetros a los roles de los administradores de su organización. Para obtener más información, consulte Modificar permisos de administrador en este artículo.

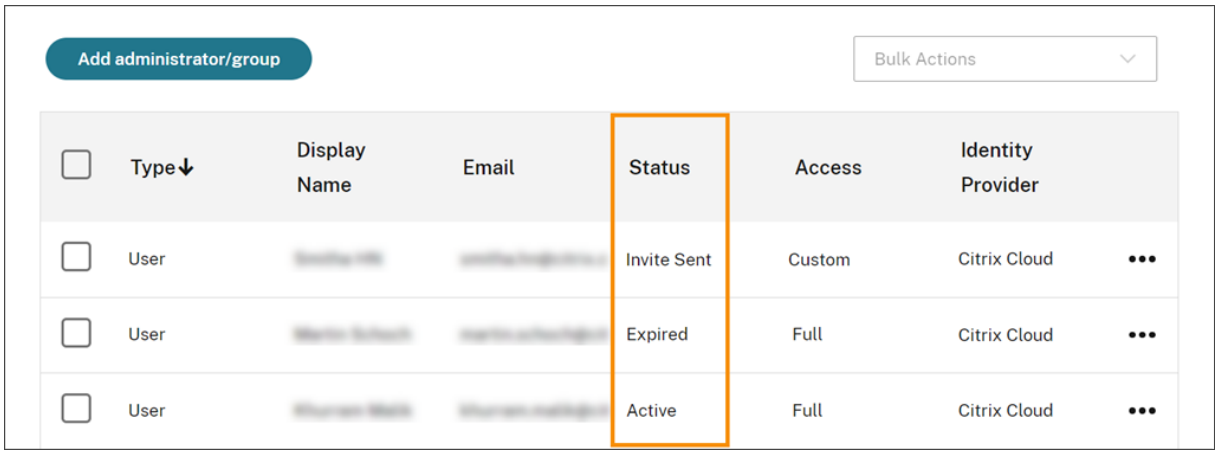
Invitar a administradores individuales

Agregar administradores individuales implica invitarlos a unirse a su cuenta de Citrix Cloud. Cuando agrega un administrador, Citrix le envía un correo electrónico de invitación. Antes de que el administrador pueda iniciar sesión, debe aceptar la invitación. Los administradores que agregue a través de grupos no reciben invitaciones y pueden iniciar sesión inmediatamente después de agregarlos.

Los correos de invitación se envían desde `cloud@citrix.com` y explican cómo acceder a la cuenta. La invitación es válida durante cinco días consecutivos a partir del día en que se envía. Transcurridos cinco días, el enlace de invitación caduca. Si el administrador invitado usa el enlace caducado, Citrix Cloud muestra un mensaje que indica que el enlace no es válido.



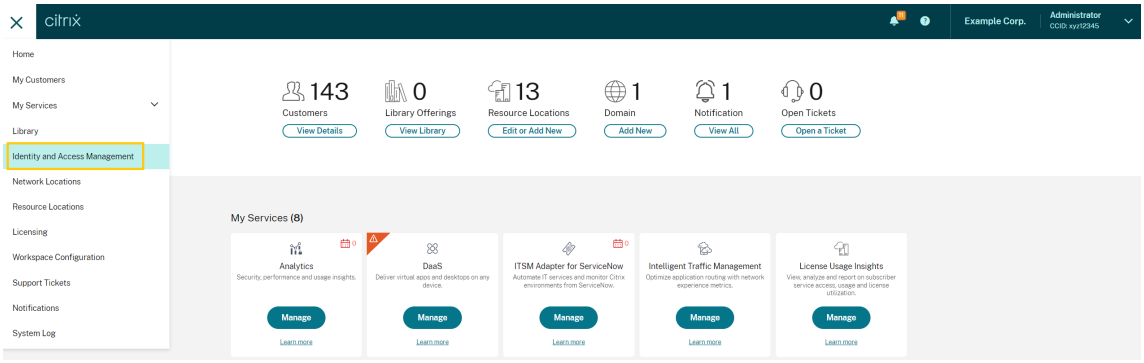
Citrix Cloud también muestra el estado de la invitación para que pueda ver si el administrador la aceptó e inició sesión en Citrix Cloud.



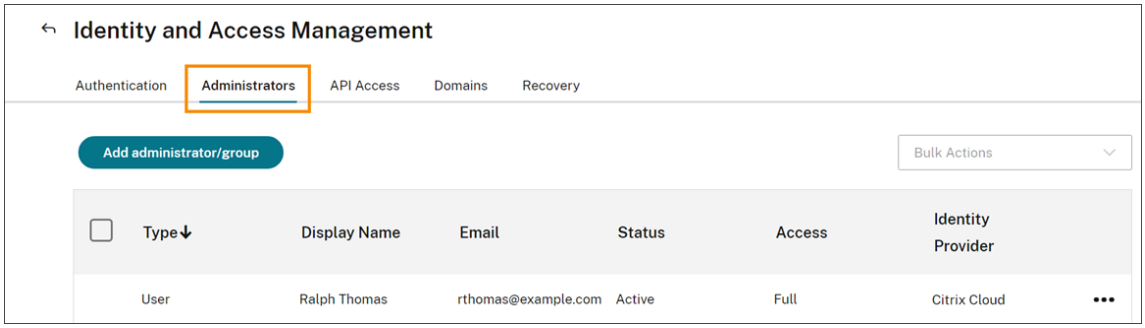
> **Nota**
>
> Las cuentas de administrador pueden estar asociadas a un máximo de 100 cuentas de clientes. Si un administrador necesita administrar más de 100 cuentas de clientes, debe crear una cuenta de administrador independiente con una dirección de correo electrónico diferente para administrar los clientes adicionales. También puede quitar ese administrador de las cuentas de clientes que ya no necesiten administrar.

Para invitar a un administrador

1. Inicie sesión en Citrix Cloud y, a continuación, seleccione **Administración de acceso e identidad** en el menú.



2. En la página **Administración de acceso e identidad**, seleccione **Administradores**. La consola muestra todos los administradores actuales de la cuenta.

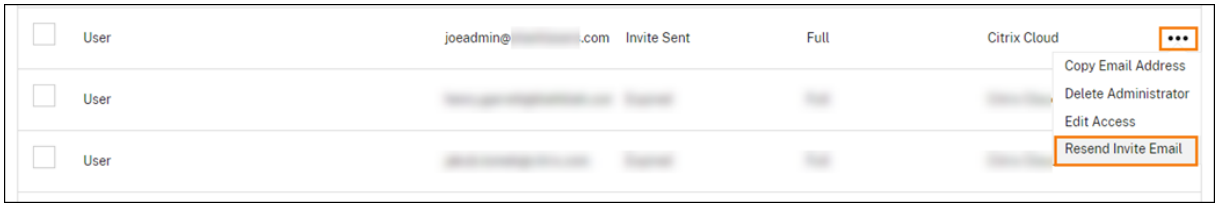


3. Seleccione **Agregar administrador/grupo**.
4. En **Detalles del administrador**, seleccione el proveedor de identidades que quiera usar. Si usa Azure AD, es posible que Citrix Cloud le pida que inicie sesión primero.
5. Si selecciona **Identidad de Citrix**, introduzca la dirección de correo electrónico del usuario y, a continuación, seleccione **Siguiente**.
6. Si **Azure Active Directory** está seleccionado, escriba el nombre del usuario que quiere agregar y, a continuación, haga clic en **Siguiente**. No se admite invitar a usuarios invitados de AAD.
7. En **Configurar acceso**, configure los permisos correspondientes para el administrador. El **acceso completo** (seleccionado de forma predeterminada) permite controlar todas las funciones y servicios suscritos de Citrix Cloud. El **acceso personalizado** permite controlar las funciones y servicios que seleccione.
8. Revise los detalles del administrador. Seleccione **Atrás** para realizar cambios.
9. Seleccione **Enviar invitación**. Citrix Cloud envía una invitación al usuario especificado y agrega el administrador a la lista.

Reenviar una invitación

Para volver a enviar la invitación, seleccione **Volver a enviar invitación** en el menú de puntos suspensivos, en el extremo derecho de la consola. El reenvío de una invitación no afecta al límite de cinco

días antes de que caduque la invitación.



Reenviar una invitación con un nuevo enlace de inicio de sesión

Si el correo electrónico de invitación original caduca, puede enviar otro al administrador. Siga estos pasos:

1. Eliminar el administrador de Citrix Cloud: En la página **Administradores**, busque el administrador en la lista y, a continuación, seleccione **Eliminar administrador** en el menú de tres puntos.
2. Espere unos instantes para asegurarse de que Citrix Cloud complete la eliminación. En algunos casos, invitar de nuevo al administrador inmediatamente después de la eliminación podría provocar el envío de una invitación con un enlace de inicio de sesión defectuoso.
3. Invite de nuevo al administrador como se describe en Para invitar a un administrador.

Aceptar una invitación de administrador

Si se le invita a una cuenta de Citrix Cloud, Citrix le envía un correo electrónico que incluye el ID de la organización y el nombre del cliente de la cuenta.

Para aceptar la invitación, haga clic en **Iniciar sesión**. A continuación, se abre una ventana de explorador. Si aún no tiene una cuenta de Citrix Cloud, el explorador muestra una página en la que puede crear su contraseña. Si ya tiene una cuenta, Citrix Cloud le pedirá que use su contraseña para iniciar sesión.

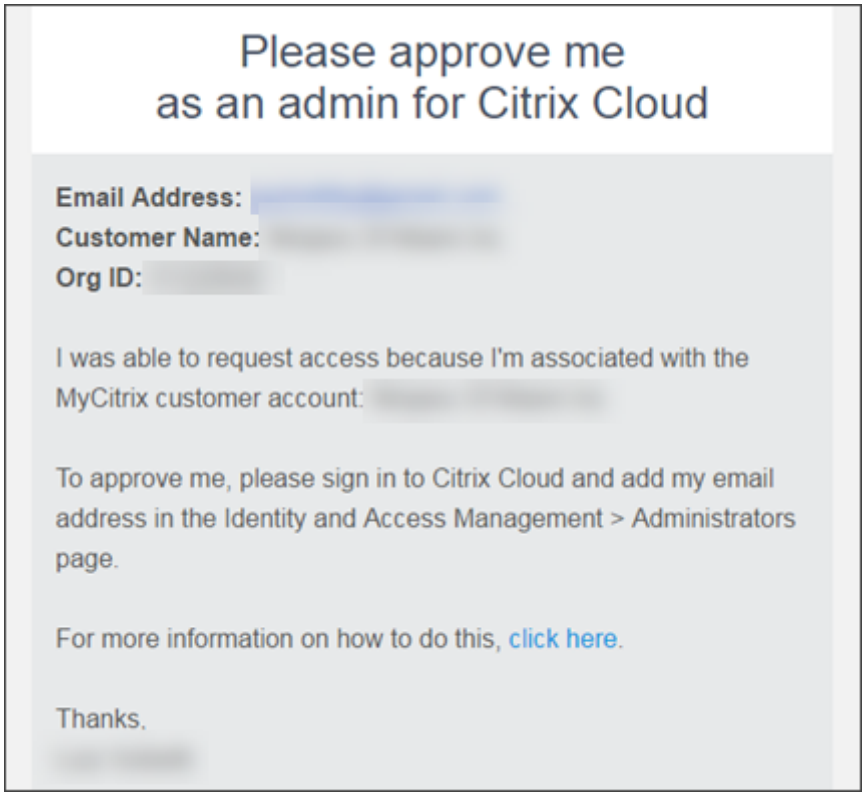
Durante el inicio de sesión, es posible que se le pida que se inscriba en la autenticación de varios factores. Para obtener instrucciones sobre cómo inscribirse, consulte Configurar la autenticación de varios factores.

Agregar grupos de administradores

Puede agregar administradores mediante grupos de AD (para la autenticación SAML) o grupos de Azure AD (para la autenticación de Azure AD). Para obtener más información, consulte Administrar grupos de administradores.

Aprobar las solicitudes para unirse a Citrix Cloud

De vez en cuando, es posible que reciba una solicitud de aprobación de Citrix Cloud en nombre de alguien de su organización que quiere unirse a su cuenta de Citrix Cloud como administrador.



Para aprobar estas solicitudes, invite a la persona que solicita unirse como administrador, tal como se describe en Invitar a administradores individuales de este artículo. Debe utilizar la misma dirección de correo electrónico que aparece en el correo electrónico de la solicitud de aprobación.

Tras recibir la invitación, la persona que solicita el acceso hace clic en el enlace **Iniciar sesión** para aceptar la invitación. A continuación, la persona puede crear una contraseña para Citrix Cloud e iniciar sesión en su cuenta.

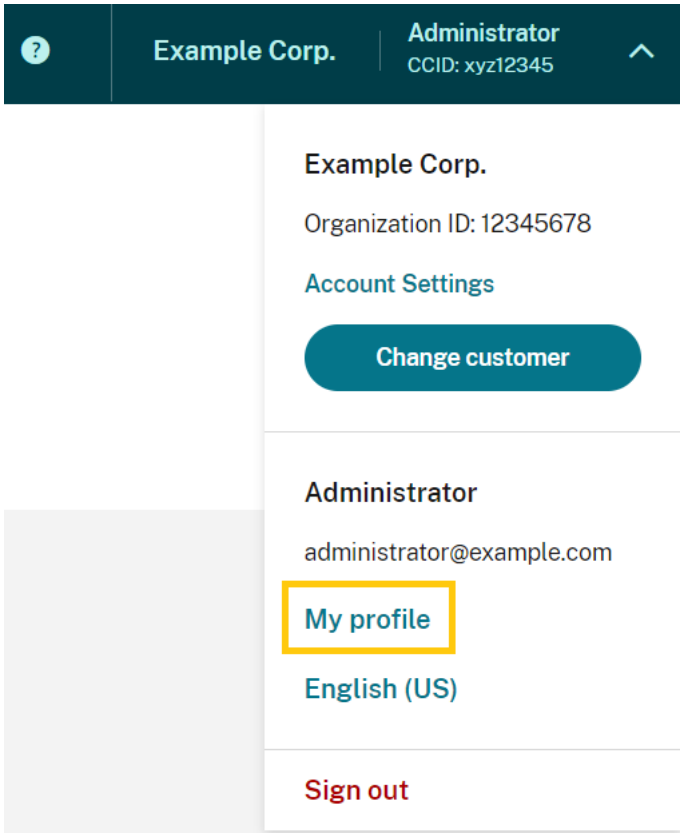
Para obtener más información sobre cómo se generan las solicitudes de aprobación, consulte ¿Qué sucede si la cuenta ya está en uso?.

Cambiar su dirección de correo electrónico

Puede cambiar su propia dirección de correo electrónico en Citrix Cloud. La nueva dirección debe ser diferente de la dirección de correo electrónico de recuperación para la autenticación de varios factores (MFA). Al cambiar su dirección de correo electrónico, Citrix Cloud le envía un correo electrónico de verificación a la nueva dirección. Tras la verificación, Citrix Cloud cierra la sesión para que se pueda

completar el cambio. Unos minutos después, podrá iniciar sesión de nuevo con su nueva dirección de correo electrónico.

1. En el menú superior derecho, seleccione **Mis parámetros**.



2. En **Dirección de correo electrónico**, seleccione **Cambiar correo**.
3. Introduzca la nueva dirección de correo electrónico que quiere usar y, a continuación, seleccione **Enviar correo de verificación**.
4. Introduzca el código de verificación de 6 dígitos del correo electrónico y, a continuación, seleccione **Verificar y completar**.
5. Seleccione **Sí, cambiar mi dirección de correo electrónico** para confirmar el cambio.

Tras confirmar los cambios, Citrix Cloud cierra la sesión. Unos minutos después, podrá iniciar sesión de nuevo con su nueva dirección de correo electrónico.

Modificar permisos de administrador

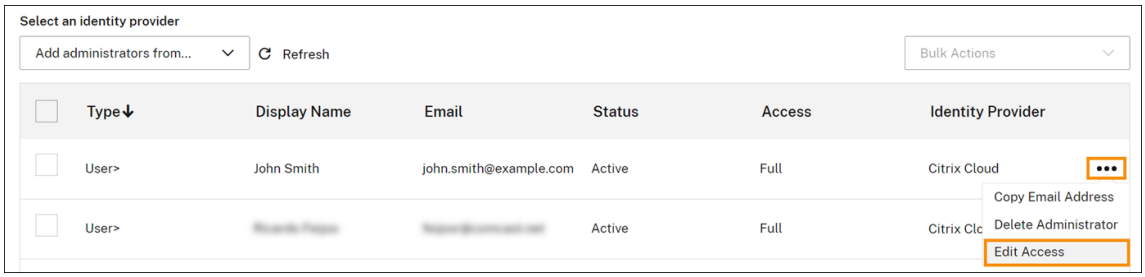
Al agregar administradores a su cuenta de Citrix Cloud, se definen los permisos de administrador adecuados para su rol en la organización. De forma predeterminada, a los nuevos administradores se les asignan *permisos de acceso total* a todas las funciones de la cuenta de Citrix Cloud y los servicios

disponibles Si quiere limitar el acceso a ciertas áreas de la consola de administración o a servicios específicos, puede definir *permisos de acceso personalizado*.

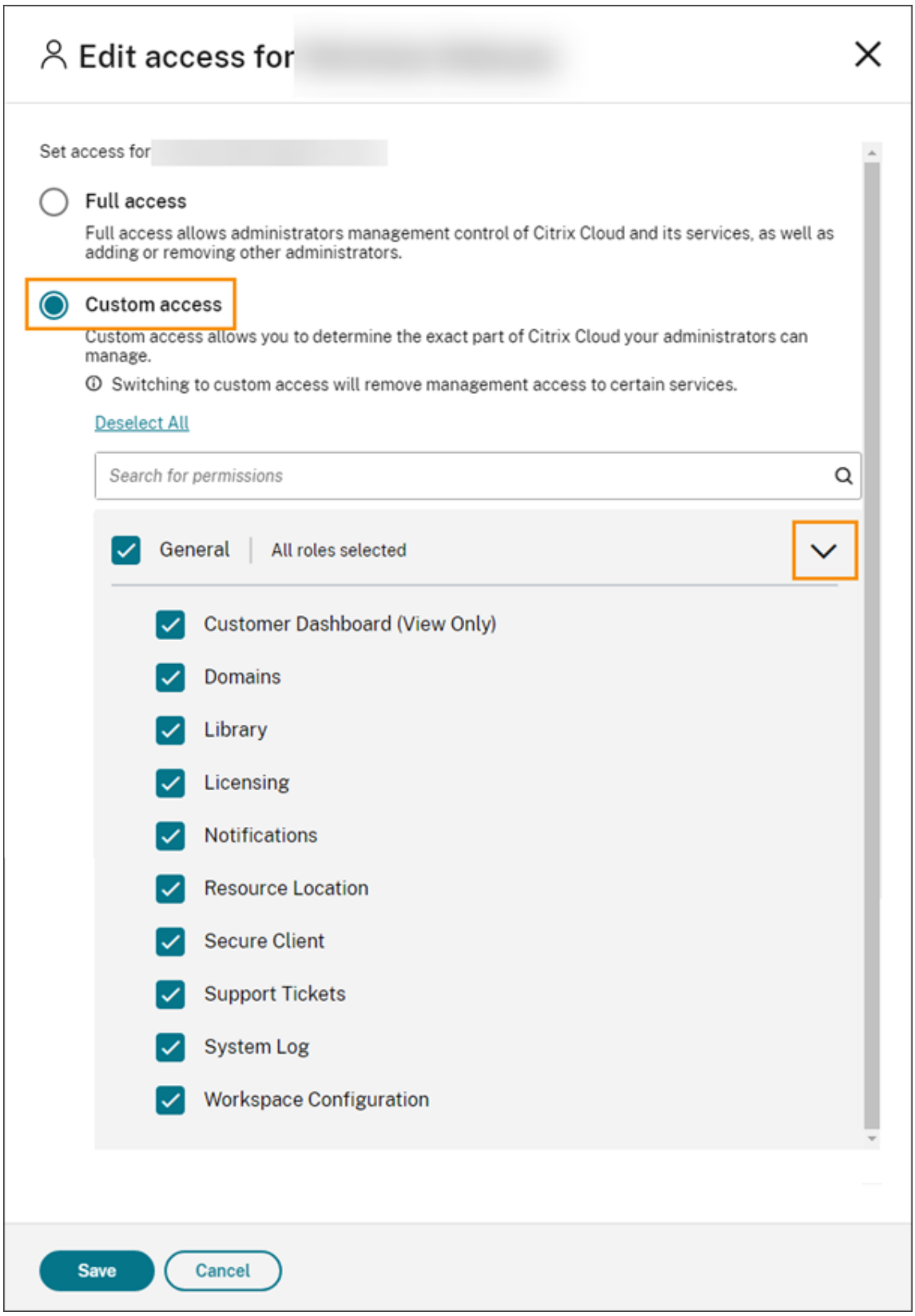
Solo los administradores de Citrix Cloud con acceso total pueden definir permisos para otros administradores.

Para cambiar los permisos de administradores existentes:

1. Inicie sesión en Citrix Cloud en https://citrix.cloud.com.
2. Desde el menú de Citrix Cloud, seleccione **Administración de acceso e identidad** y, luego, **Administradores**.
3. Seleccione el proveedor de identidades que quiere administrar: Identidad de Citrix (predeterminado), Active Directory (si usa SAML como proveedor de identidades) o Azure AD (si se conecta).
4. Busque al administrador o grupo que quiere gestionar, haga clic en el botón de puntos suspensivos y seleccione **Modificar acceso**.



5. Para permitir o prohibir permisos específicos, seleccione **Acceso personalizado**. Para permitir el acceso a todas las funciones de Citrix Cloud, seleccione **Acceso total**.
6. Para localizar los permisos de servicio rápidamente, empiece a escribir en el cuadro de búsqueda. Citrix Cloud muestra los permisos coincidentes a medida que escribe. Por ejemplo, si comienza a escribir "solo lectura", se mostrarán los permisos con "solo lectura"en el título. La búsqueda de permisos no distingue mayúsculas de minúsculas.
7. Para definir los permisos de acceso personalizado para la consola de administración de Citrix Cloud, expanda **General**.



8. Para definir permisos de acceso personalizado para un servicio específico, expanda el servicio.

9. Marque o deje sin marcar la casilla correspondiente a cada permiso según convenga.
10. Seleccione **Guardar**.

Permisos de la consola

En esta sección se describen los permisos de acceso personalizados que están disponibles para la consola de administración de Citrix Cloud. Para obtener más información sobre los permisos de acceso personalizados para un servicio específico, consulte la documentación del servicio.

- **Panel de mandos del cliente (solo lectura):** Solo para Citrix Service Providers (CSP). Otorga acceso de lectura al panel de mandos de los clientes.
- **Dominios:** Otorga acceso a la ficha **Administración de acceso e identidad > Dominios**. Los administradores pueden agregar un dominio de Active Directory al descargar el software de Citrix Cloud Connector desde esta ficha y al instalarlo en un servidor del dominio.
- **Biblioteca:** Otorga acceso a la página **Biblioteca** de la consola. Según los servicios a los que los administradores puedan acceder, los administradores pueden asignar usuarios a grupos de entrega para Citrix DaaS, agregar aplicaciones administradas de Intune desde Endpoint Management o permitir que los administradores con permisos de solo lectura vean detalles de las aplicaciones para Secure Private Access.
- **Licencias:** Otorga acceso a las fichas **Cloud Services** e **Implementaciones con licencia** de la página **Licencias** de la consola.
- **Notificaciones:** Otorga acceso a la página **Notificaciones** de la consola. Los administradores pueden ver y descartar notificaciones de Citrix Cloud.
- **Ubicaciones de recursos:** Otorga acceso a la página **Ubicaciones de recursos** de la consola. Los administradores pueden agregar nuevas ubicaciones de recursos y agregar servidores de FAS para Single Sign-On de Citrix Workspace. También pueden administrar las actualizaciones de los conectores.
- **Cliente seguro:** Otorga acceso a la ficha **Administración de acceso e identidad > Acceso a API > Clientes seguros**. Los administradores pueden crear y administrar sus propios clientes seguros para usarlos con las API de Citrix Cloud. Este permiso no incluye el acceso a la ficha **Administración de acceso e identidad > Acceso a API > Registros de productos**. Solo los administradores con acceso total pueden acceder a la ficha **Registros de productos**.
- **Tíquets de asistencia:** Otorga acceso a la opción del menú de la consola **Tíquets de asistencia** y a la opción del menú de ayuda **Abrir un tíquet**. Al seleccionar cualquiera de estas opciones, el administrador se dirige al portal My Support. Para obtener más información, consulte Asistencia técnica.
- **Registro del sistema:** Otorga acceso a la página **Registro del sistema** de la consola. Los administradores pueden ver los eventos del registro del sistema y exportar los eventos en un archivo CSV.

- **Configuración de Workspace:** Otorga acceso a la página **Configuración de Workspace** de la consola. Los administradores pueden cambiar los métodos de autenticación, personalizar la apariencia y el comportamiento de los espacios de trabajo, habilitar e inhabilitar servicios y configurar la agregación de sitios. Para obtener más información, consulte la documentación de producto de Citrix Workspace.
- **Clientes OAuth de Workspace (Tech Preview):** Otorga acceso a la ficha **Administración de acceso e identidad > Acceso a API > API de Workspace**. Los administradores pueden crear y administrar su propio cliente de OAuth para interactuar con las API de la plataforma Citrix Workspace. Los clientes de OAuth se usan exclusivamente para las API de Workspace e incluyen la opción de crear clientes privados que caducan automáticamente.

> **Nota:**
>
> Se recomienda asignar con precaución el rol personalizado de **clientes de OAuth de Workspace**. Es posible que los privilegios de acceso asociados a este rol permitan a los administradores acceder a recursos de los usuarios finales (VDA o aplicaciones) en la plataforma Workspace. También es importante tener en cuenta que los administradores con **acceso total** tendrán automáticamente permisos de acceso equivalentes a los de un administrador con el permiso de **clientes de OAuth de Workspace**.

Administrar el método de autenticación MFA principal

Para iniciar sesión en Citrix Cloud con autenticación de varios factores (MFA), puede utilizar una aplicación de autenticación o su dirección de correo electrónico. En esta sección se describe cómo cambiar la inscripción de un dispositivo para la autenticación MFA o cómo cambiar a un método de MFA diferente.

Cambiar un dispositivo para la autenticación MFA

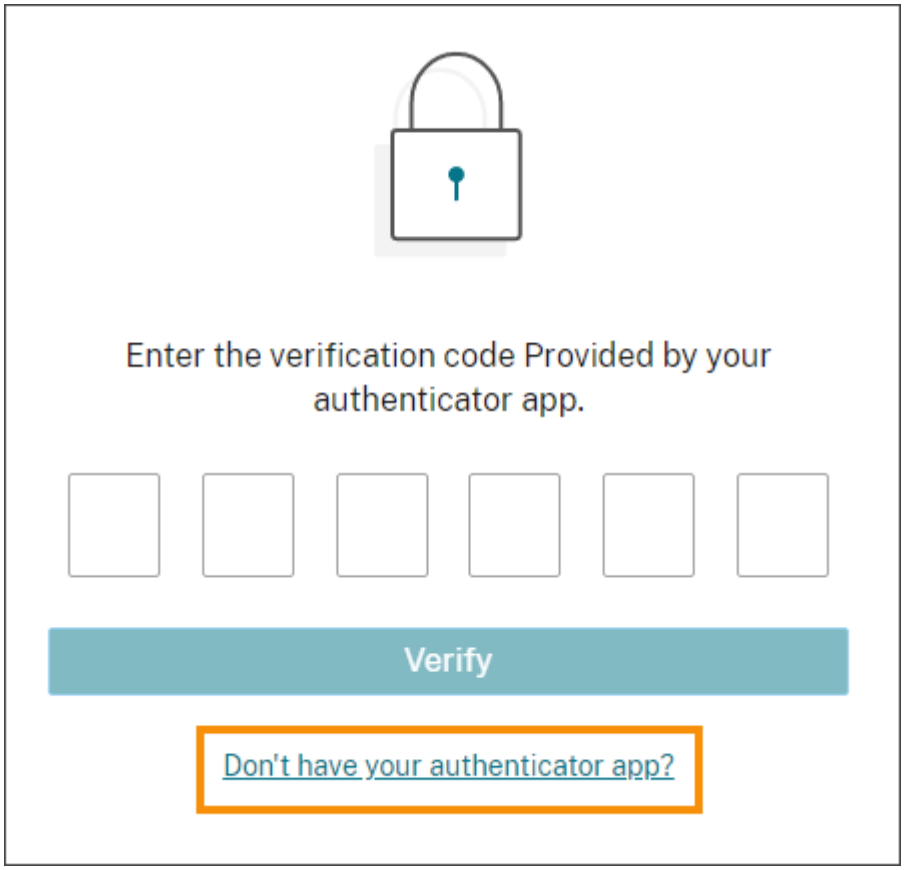
Si pierde el dispositivo inscrito, quiere utilizar otro dispositivo con Citrix Cloud o restablecer la aplicación de autenticación, puede reinscribirse en la autenticación MFA de Citrix Cloud.

> **Notas**
>
> - Al cambiar el dispositivo, se elimina la inscripción del dispositivo actual y se genera una nueva clave de aplicación de autenticación.
> - Si va a reinscribirse con la misma aplicación de autenticación de la inscripción original, elimine la entrada de Citrix Cloud de la aplicación de autenticación antes de iniciar el proceso de reinscripción. Los códigos mostrados en esta entrada ya no funcionarán después de completar la reinscripción. Si no elimina esta entrada antes o después de reinscribirse, la aplicación de autenticación mostrará dos entradas de Citrix Cloud con códigos diferentes

que pueden provocar confusión al iniciar sesión en Citrix Cloud.

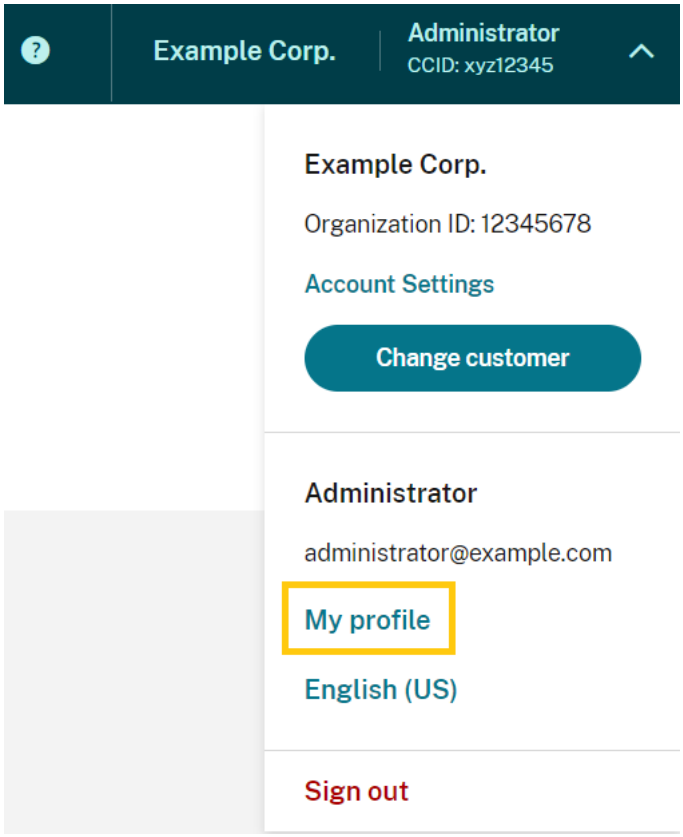
- Si va a reinscribirse con un nuevo dispositivo y no tiene una aplicación de autenticación, descargue una desde la tienda de aplicaciones de su dispositivo e instálela. Para que la experiencia sea más fluida, Citrix recomienda instalar una aplicación de autenticación antes de reinscribir el dispositivo.

1. Inicie sesión en Citrix Cloud e introduzca el código de su aplicación de autenticación.

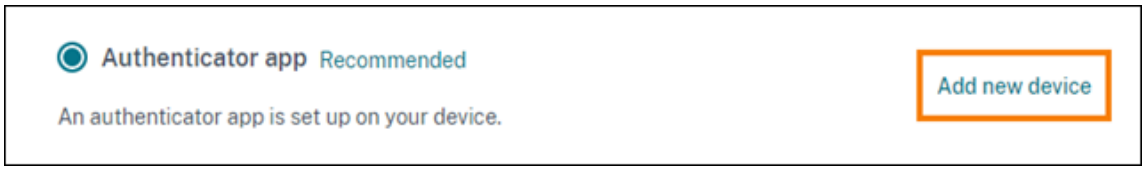


   Si no tiene una aplicación de autenticación, haga clic en **¿No tiene ninguna aplicación de autenticación?** y seleccione un método de recuperación para poder iniciar sesión. Dependiendo del método de recuperación seleccionado, introduzca el código de recuperación que recibió o un código de reserva no utilizado y seleccione **Verificar**.

2. Si es administrador de varias organizaciones de clientes, seleccione una.
3. En el menú superior derecho, seleccione **Mis parámetros**.



4. En la **aplicación de autenticación**, seleccione **Agregar nuevo dispositivo**.



5. Cuando se le pida que confirme el cambio de dispositivo, seleccione **Sí, quiero cambiarlo**.
6. Verifique su identidad introduciendo un código de verificación de la aplicación de autenticación. Si no tiene una aplicación de autenticación, seleccione **Usar un método de recuperación** para verificar su identidad con el método de recuperación que elija. Dependiendo del método de recuperación que seleccione, deberá introducir el código de verificación o el código de recuperación que recibió, o bien un código de reserva no utilizado. Seleccione **Verificar y continuar**.
7. Si está utilizando el dispositivo que inscribió originalmente y la aplicación de autenticación original, elimine la entrada de la aplicación de autenticación presente en Citrix Cloud.
8. Si está registrando un nuevo dispositivo y no tiene una aplicación de autenticación, descargue una de la tienda de aplicaciones de su dispositivo.
9. Desde la aplicación de autenticación, escanee el código QR con su dispositivo o introduzca la clave manualmente.

10. Introduzca el código de verificación de 6 dígitos de la aplicación de autenticación y seleccione **Verificar código**.

Después de cambiar el dispositivo, Citrix recomienda encarecidamente comprobar que los métodos de verificación de la página Mi perfil estén actualizados.

Cambiar el método de autenticación MFA

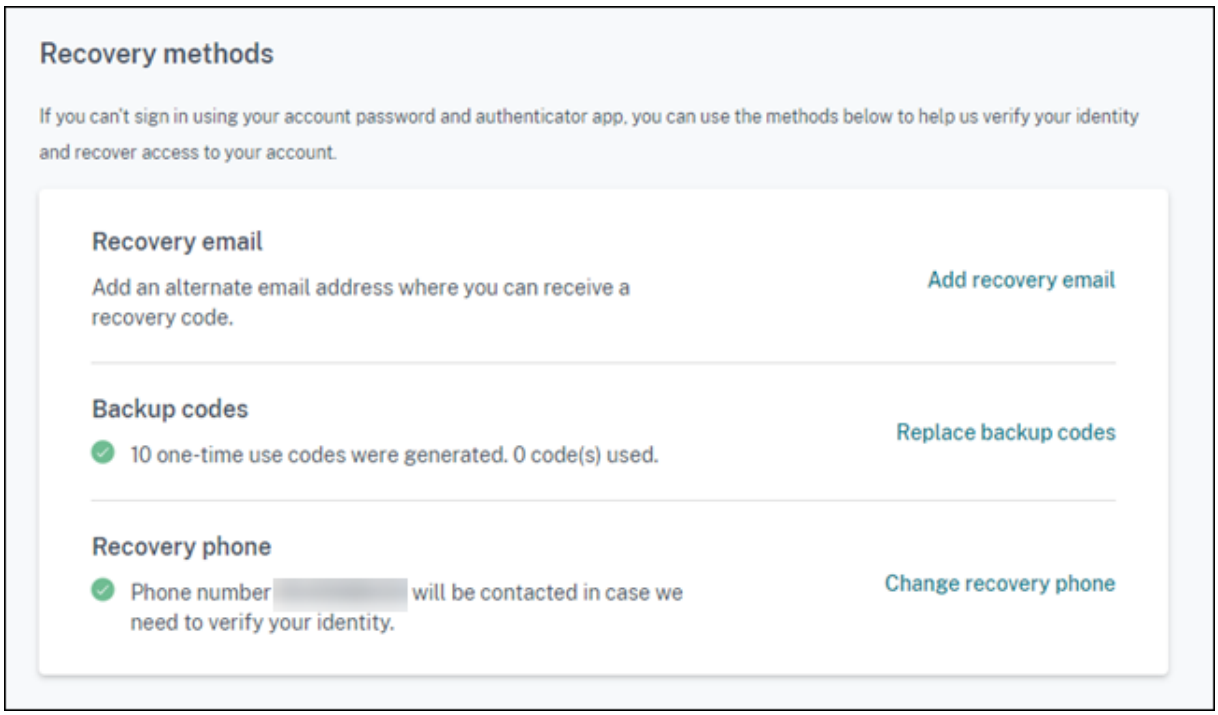
Si se inscribió en la autenticación MFA mediante una aplicación de autenticación y quiere cambiar de método para usar su dirección de correo electrónico, tenga en cuenta que, al cambiar el método de autenticación, se eliminará la inscripción del dispositivo. Si quiere volver a usar una aplicación de autenticación para la MFA, tendrá que volver a registrar su dispositivo.

1. En el menú superior derecho de la consola de Citrix Cloud, seleccione **Mis parámetros**.
2. En **Autenticación de varios factores (MFA)**, seleccione el método de autenticación al que quiera cambiar.
3. Si cambia a la autenticación MFA de correo electrónico:
    a) Seleccione **Sí, cambiar al correo** para confirmar que quiere cambiar el método de autenticación MFA.
    b) Introduzca el código de la aplicación de autenticación o utilice un método de recuperación para confirmar su identidad.
    c) Selecciona **Verificar y continuar** para completar el cambio.
4. Si cambia a una aplicación de autenticación:
    a) Cuando se le indique, introduzca el código de verificación que Citrix Cloud envía a su dirección de correo electrónico y seleccione **Verificar y continuar**. También puede utilizar un método de recuperación para confirmar su identidad.
    b) Con la aplicación de autenticación, escanee el código QR con la cámara del dispositivo o introduzca la clave alfanumérica.
    c) En **Compruebe su aplicación de autenticación**, introduzca el código de 6 dígitos de la aplicación de autenticación.
    d) Para completar la inscripción del dispositivo, haga clic en **Verificar código**.

Administrar los métodos de recuperación de la autenticación MFA

> **Importante:**
>
> Para asegurarse de que su cuenta de Citrix Cloud permanece segura, mantenga sus métodos de verificación al día con información precisa. Si pierde el acceso a la aplicación de autenticación o a la dirección de correo electrónico asociada a la autenticación MFA, estos métodos de verificación

> son la única forma de recuperar el acceso a su cuenta.



Agregar o cambiar el correo electrónico de recuperación

1. En el menú superior derecho, seleccione **Mis parámetros**.
2. En **Métodos de recuperación**, en **Correo de recuperación**, seleccione **Agregar correo de recuperación** si aún no ha agregado una dirección de correo electrónico de recuperación. Si ya agregó una dirección de correo electrónico de recuperación, seleccione **Cambiar el correo de recuperación**.
3. Cuando se le indique, introduzca el código de verificación de la aplicación de autenticación o el código enviado a su dirección de correo electrónico.
4. Introduzca la nueva dirección de correo electrónico que quiere usar y, a continuación, seleccione **Enviar correo de verificación**. Esta dirección de correo electrónico debe ser diferente de la dirección de correo electrónico que utiliza para su cuenta de Citrix Cloud. Citrix Cloud le envía un correo electrónico de verificación a la dirección de correo electrónico que ha introducido.
5. Introduzca el código del correo electrónico de verificación y, a continuación, haga clic en **Verificar código y completar**.

Generar nuevos códigos de reserva

Puede generar un nuevo conjunto de códigos de reserva cuando quiera. Al utilizar códigos de reserva, Citrix Cloud registra el número utilizado en la página Mi perfil.

Después de generar nuevos códigos de reserva, guárdelos en un lugar seguro.

1. En el menú superior derecho, seleccione **Mis parámetros**.
2. En **Métodos de recuperación**, en **Códigos de reserva**, seleccione **Generar nuevos códigos de reserva** si no generó códigos de reserva antes. Si ya generó códigos de reserva anteriormente, seleccione **Reemplazar códigos de reserva**.
3. Cuando se le pregunte si quiere reemplazar los códigos de reserva, seleccione **Sí, quiero reemplazarlos**.
4. Para verificar su identidad, introduzca un código de verificación de la aplicación de autenticación o el código enviado a su dirección de correo electrónico.
5. Seleccione **Verificar y continuar**. Citrix Cloud genera y muestra un nuevo conjunto de códigos de reserva.
6. Seleccione **Descargar códigos** para descargar los nuevos códigos en un archivo de texto. A continuación, seleccione **He guardado mis códigos de reserva**.
7. Seleccione **He guardado mis códigos de reserva** para terminar de reemplazarlos.

Cambiar el número de teléfono de recuperación

1. En el menú superior derecho, seleccione **Mis parámetros**.
2. En **Métodos de recuperación**, en **Teléfono de recuperación**, seleccione **Cambiar teléfono de recuperación**.
3. Introduzca el código de verificación de la aplicación de autenticación o el código enviado a su dirección de correo electrónico. Seleccione **Verificar y continuar**.
4. Introduzca el nuevo número de teléfono que quiere usar. A continuación, vuelva a introducir el número de teléfono para confirmar.
5. Seleccione **Guardar número de teléfono de recuperación**.

> **Nota:**
>
> Puede modificar los permisos de los administradores de Citrix Endpoint Management (CEM) solamente después de que el administrador haya aceptado una invitación de administrador y haya hecho clic en **Administrar** en el mosaico de CEM. Al igual que todos los administradores de Citrix Cloud, los administradores de CEM tienen acceso total de forma predeterminada.

Administrar grupos de administradores

February 15, 2024

Puede agregar administradores a su cuenta de Citrix Cloud mediante grupos en Active Directory, Azure Active Directory (AD) o Google Cloud Identity. A continuación, puede administrar los permisos de acceso a servicios para todos los administradores del grupo.

Requisitos previos de AD

Citrix Cloud permite la autenticación de grupos de AD a través de SAML 2.0. Antes de agregar miembros de sus grupos de administradores de AD a Citrix Cloud, debe configurar una conexión entre Citrix Cloud y su proveedor de SAML. Para obtener más información, consulte Conectar SAML como proveedor de identidades con Citrix Cloud.

Si ya tiene una conexión SAML en Citrix Cloud, debe conectar de nuevo su proveedor de SAML con Citrix Cloud antes de poder agregar grupos de administradores de AD. Si no conecta de nuevo SAML, es posible que no se puedan agregar grupos de administradores de AD. Para obtener más información, consulte Usar una conexión SAML existente para la autenticación del administrador.

Requisitos previos de Azure AD

El uso de la autenticación de grupos de Azure AD requiere la versión más reciente de la aplicación Azure AD para conectar su Azure AD a Citrix Cloud. Citrix Cloud adquirió esta aplicación cuando conectó su Azure AD por primera vez. Si conectó Azure AD a Citrix Cloud antes de mayo de 2019, es posible que Citrix Cloud no esté utilizando la aplicación más reciente para conectarse a Azure AD. Citrix Cloud no puede mostrar sus grupos de Azure AD si su cuenta no utiliza la aplicación más reciente.

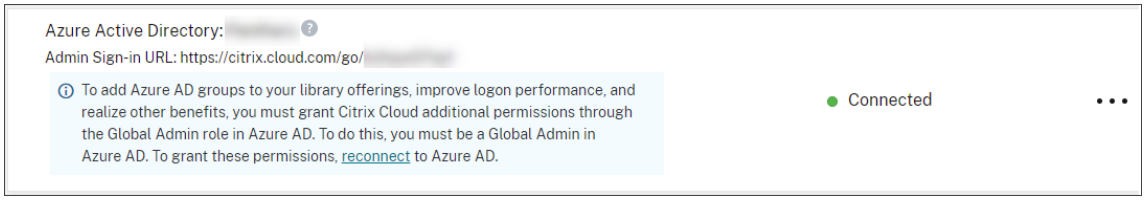
Antes de usar los grupos de Azure AD en Citrix Cloud, lleve a cabo las siguientes tareas:

1. Compruebe que está utilizando la aplicación más reciente para la conexión con Azure AD. Citrix Cloud muestra una notificación si no utiliza la aplicación más reciente.
2. Si la aplicación debe actualizarse, vuelva a conectar su Azure AD a Citrix Cloud. Por el hecho de reconectarse a su Azure AD, usted concede permisos de solo lectura a nivel de aplicación a Citrix Cloud y permite a Citrix Cloud volver a conectarse a su Azure AD en su nombre. Durante la reconexión, se muestra una lista de estos permisos para que los revise. Para obtener más información sobre los permisos que Citrix Cloud solicita, consulte Permisos de Azure Active Directory para Citrix Cloud.

> **Importante:**
>
> Debe ser un administrador global en Azure AD para completar esta tarea. Además, debe haber iniciado sesión en Citrix Cloud con una cuenta de administrador con acceso total en el proveedor de identidades de Citrix. Si inicia sesión con sus credenciales de Azure AD, se produce un error en la reconexión. Si no tiene ningún administrador que utilice el proveedor de identidades de Citrix, puede agregar uno temporalmente para realizar esta tarea y, a continuación, eliminarlo.

Para verificar la conexión a Azure AD

1. Inicie sesión en Citrix Cloud con una cuenta de administrador con acceso total en el proveedor de identidades de Citrix.
2. Desde el menú de Citrix Cloud, seleccione **Administración de acceso e identidad** y, luego, **Autenticación**.
3. Busque **Azure Active Directory**. Aparece una notificación si Citrix Cloud debe actualizar la aplicación para su conexión con Azure AD.



   Si Citrix Cloud ya utiliza la aplicación más reciente, no aparece ninguna notificación.

Para conectarse de nuevo a Azure AD

1. En la notificación de Azure AD de la consola de Citrix Cloud, haga clic en el enlace de **reconexión**. Aparecerá una lista de los permisos de Azure solicitados.
2. Revise los permisos y, a continuación, seleccione **Aceptar**.

Google Cloud Identity

Citrix Cloud admite la autenticación de grupos de administradores a través de Google Cloud Identity. Antes de agregar sus grupos de administradores a Citrix Cloud, debe configurar una conexión entre Citrix Cloud y Google Cloud Identity. Para obtener más información, consulte Conectar Google Cloud Identity como proveedor de identidades con Citrix Cloud.

Servicios compatibles

Estos servicios admiten permisos de acceso personalizados para grupos de administradores:

- Citrix Analytics
- NetScaler Console
- Citrix DaaS
- Workspace Environment Management Service
- License Usage Insights

Permisos admitidos

Puede asignar permisos de acceso personalizados solo a servicios admitidos y a determinadas funciones de la plataforma Citrix Cloud. Los permisos de acceso total no están disponibles.

Para las funciones de la plataforma Citrix Cloud, se admiten estos permisos de acceso personalizados:

- Dominios
- Licencias
- Ubicaciones de recursos
- Tíquets de asistencia
- Registro del sistema
- Configuración de Workspace

Para obtener más información sobre estos permisos, consulte Permisos de la consola.

Los grupos de administradores no tienen acceso a ningún otro servicio. Solo pueden administrar los servicios disponibles para los que tienen permiso de acceso.

Los cambios de permisos para un miembro del grupo de administradores que ya haya iniciado sesión surtirán efecto solo después de cerrar la sesión e iniciarla de nuevo.

Permisos resultantes para administradores con identidades de Citrix, AD, Azure AD y Google Cloud Identity

Cuando un administrador inicia sesión en Citrix Cloud, es posible que solo estén disponibles ciertos permisos si el administrador tiene tanto una identidad de Citrix (el proveedor de identidades predeterminado en Citrix Cloud) como una identidad de AD, Azure AD o Google Cloud Identity de un solo usuario o por grupo. En la tabla de esta sección se describen los permisos que están disponibles para cada combinación de estas identidades.

La *Identidad de un solo usuario* se refiere a los permisos de AD, Azure AD o Google Cloud Identity que se conceden al administrador a través de una cuenta individual. La *Identidad por grupo* se refiere a los permisos de AD, Azure AD o Google Cloud Identity que se conceden como miembro de un grupo.

Identidad de Citrix	Identidad de AD o Azure AD de un solo usuario	Identidad de AD o Azure AD por grupo	Google Cloud Identity por usuario único o por grupo	Permisos disponibles tras la autenticación
X	X			El administrador tiene permisos acumulados de ambas identidades después de una autenticación correcta con la identidad de Citrix, la identidad de AD o la identidad de Azure AD.
X		X		Cada identidad se trata como una entidad independiente. Los permisos disponibles dependen de si el administrador se autentica con la identidad de Citrix o la identidad de Azure AD.

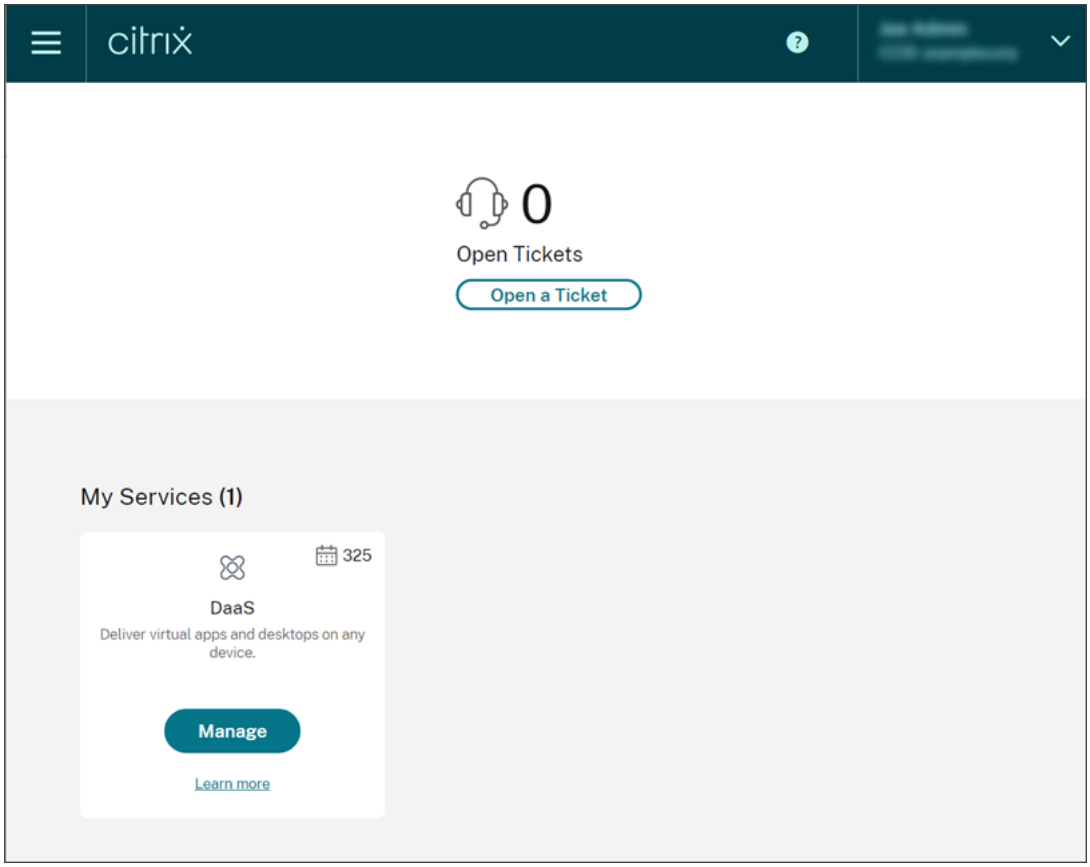
Identidad de Citrix	Identidad de AD o Azure AD de un solo usuario	Identidad de AD o Azure AD por grupo	Google Cloud Identity por usuario único o por grupo	Permisos disponibles tras la autenticación
X			X	Cada identidad se trata como una entidad independiente. Los permisos disponibles dependen de si el administrador se autentica con la identidad de Citrix o Google Cloud Identity.
	X	X		El administrador tiene permisos acumulados de ambas identidades al autenticarse en Citrix Cloud con AD o Azure AD.
	X		X	Cada identidad se trata como una entidad independiente. Los permisos disponibles dependen de si el administrador se autentica con la identidad de Citrix o Google Cloud Identity.

Identidad de Citrix	Identidad de AD o Azure AD de un solo usuario	Identidad de AD o Azure AD por grupo	Google Cloud Identity por usuario único o por grupo	Permisos disponibles tras la autenticación
		X	X	Cada identidad se trata como una entidad independiente. Los permisos disponibles dependen de si el administrador se autentica con la identidad de Citrix o Google Cloud Identity.
X	X	X		Al autenticarse con su identidad de Citrix, el administrador tiene permisos acumulados tanto de la identidad de Citrix como de la identidad de Azure AD de un solo usuario. Al autenticarse con Azure AD, el administrador tiene permisos acumulados de las tres identidades.

Experiencia en los inicios de sesión para administradores

Después de agregar un grupo a Citrix Cloud y definir los permisos del servicio, los administradores del grupo simplemente inician sesión al seleccionar **Iniciar sesión con mis credenciales de empresa** en la página de inicio de sesión de Citrix Cloud al introducir la URL de inicio de sesión correspondiente a la cuenta (por ejemplo, `https://citrix.cloud.com/go/mycompany`). A diferencia de agregar administradores individuales, los administradores del grupo no reciben ninguna invitación explícita, por lo que no recibirán ningún correo electrónico de invitación para ser administradores de Citrix Cloud.

Después de iniciar sesión, los administradores seleccionan **Administrar** en el mosaico de servicio para acceder a la consola de administración del servicio.



Los administradores a los que se conceden permisos solo como miembros de grupos pueden acceder a la cuenta de Citrix Cloud mediante la URL de inicio de sesión correspondiente a la cuenta de Citrix Cloud.

Los administradores a los que se conceden permisos a través de una cuenta individual y como miembros de un grupo pueden elegir la cuenta de Citrix Cloud a la que quieren acceder. Si el administrador es miembro de varias cuentas de Citrix Cloud, puede seleccionar una cuenta de Citrix Cloud en el selector de clientes después de autenticarse correctamente.

Limitaciones

Acceso a funciones de plataforma y servicio

Los permisos de acceso personalizados para estas funciones de la plataforma Citrix Cloud no están disponibles para miembros de grupos de administradores:

- Biblioteca
- Notificaciones
- Clientes seguros

Para obtener más información sobre los permisos disponibles, consulte Permisos admitidos en este artículo.

Las funciones de Citrix DaaS que se basan en las prestaciones de la plataforma de Citrix Cloud, como la asignación de usuarios de la Distribución rápida, no están disponibles.

Impacto de varios grupos en el rendimiento de las aplicaciones

Citrix recomienda que un solo administrador no pertenezca a más de 20 grupos que se hayan agregado a Citrix Cloud. Es posible que, si pertenece a más grupos, degrade el rendimiento de las aplicaciones.

Impacto de varios grupos en la autenticación

Si se asigna un administrador por grupos a varios grupos de AD o Azure AD, es posible que la autenticación falle porque hay demasiados grupos. Este problema se produce debido a una limitación en la integración de Citrix Cloud en AD y Azure AD. Cuando el administrador intenta iniciar sesión, Citrix Cloud intenta comprimir la cantidad de grupos que se obtienen. Si Citrix Cloud no puede aplicar la compresión correctamente, no se pueden obtener todos los grupos y se produce un error en la autenticación.

Es posible que este problema también afecte a los usuarios que se autentican en Citrix Workspace a través de AD o Azure AD. Si un usuario pertenece a varios grupos, es posible que la autenticación falle porque hay demasiados grupos.

Para resolver este problema, revise la cuenta de administrador o de usuario y verifique que solo pertenezcan a los grupos que son necesarios para su rol en la organización.

No se pueden agregar grupos porque hay demasiados pares de roles y ámbitos asignados

Al agregar un grupo con varios pares de roles y ámbitos, es posible que se produzca un error que indica que el grupo no se puede crear. Este error se produce porque hay demasiados pares de roles y

ámbitos asignados al grupo. Para resolver este error, divida los pares de roles y ámbitos en dos o más grupos y asigne los administradores a esos grupos.

Agregar un grupo de administradores a Citrix Cloud

1. Desde el menú de Citrix Cloud, seleccione **Administración de acceso e identidad** y, luego, **Administradores**.
2. Seleccione **Agregar administrador/grupo**.
3. En **Detalles del administrador**, seleccione el proveedor de identidades que quiera usar. Si se selecciona Azure AD, inicie sesión en Azure, si es necesario. Seleccione **Siguiente**.
4. Si es necesario, seleccione el dominio que quiere usar.
5. Busque el grupo que quiere agregar y seleccione el grupo.
6. En **Establecer acceso**, seleccione los roles que quiera asignar al grupo. Debe seleccionar al menos un rol.
7. Cuando haya terminado, seleccione **Guardar**.

Modificar los permisos de servicio de un grupo de administradores

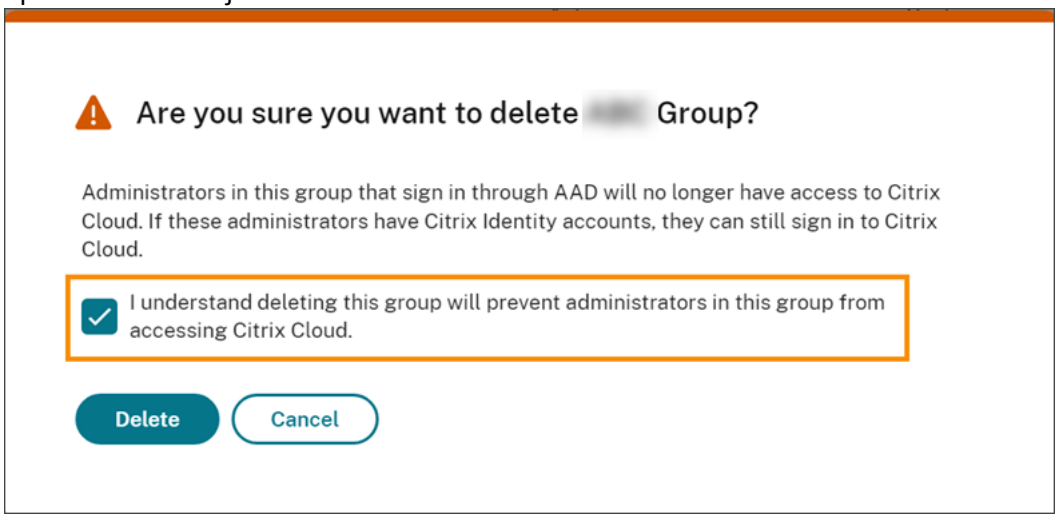
1. Desde el menú de Citrix Cloud, seleccione **Administración de acceso e identidad** y, luego, **Administradores**.
2. Busque el grupo de administradores que quiere administrar y, en el menú de puntos suspensivos, seleccione **Modificar acceso**.

3. Seleccione o desmarque los pares de roles y ámbitos que necesite.
4. Cuando haya terminado, seleccione **Guardar**.

Eliminar un grupo de administradores

1. Desde el menú de Citrix Cloud, seleccione **Administración de acceso e identidad** y, luego, **Administradores**.
2. Busque el grupo de administradores que quiere administrar y, en el menú de puntos suspensivos, seleccione **Eliminar grupo**.

Aparece un mensaje de confirmación.

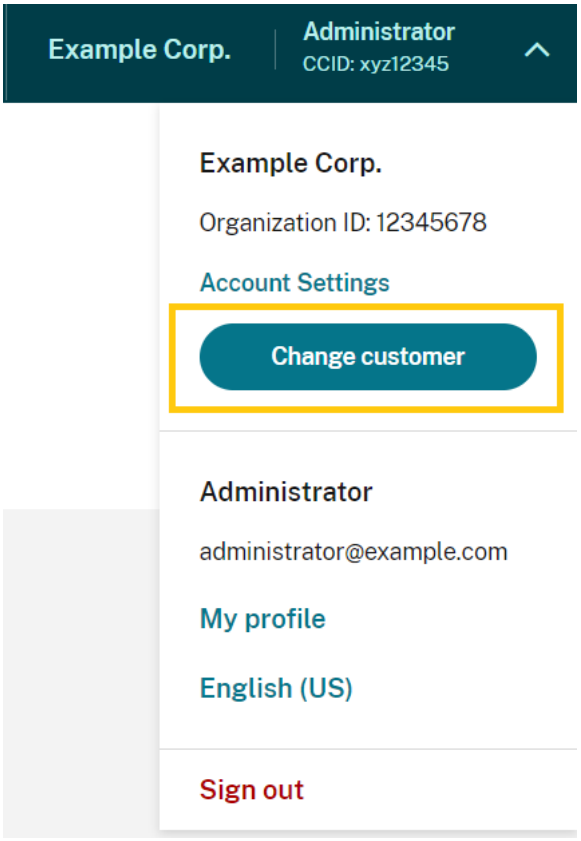


3. Elija **Entiendo que, al eliminar este grupo, los administradores de este grupo no podrán acceder a Citrix Cloud** para confirmar que conoce las consecuencias de eliminar el grupo.
4. Seleccione **Eliminar**.

Cambiar de cuenta de Citrix Cloud

> **Nota:**
>
> En esta sección se describe un caso que afecta únicamente a miembros de grupos de administradores de Azure AD.

De forma predeterminada, los miembros de grupos de administradores de Azure AD no pueden pasar de una cuenta de Citrix Cloud a otra a la que puedan acceder. Para estos administradores, la opción **Cambiar cliente**, que se muestra en la imagen siguiente, no aparece en el menú de usuario de Citrix Cloud.

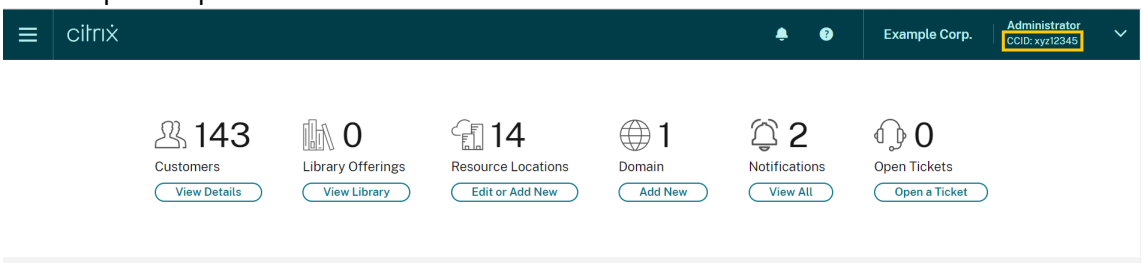


Para habilitar esta opción de menú y permitir que los miembros de grupos de Azure AD pasen a otras cuentas de Citrix Cloud, debe vincular las cuentas entre las que quiere que se muevan.

La vinculación de cuentas de Citrix Cloud implica un enfoque radial. Antes de vincular cuentas, decida qué cuenta de Citrix Cloud actuará como la cuenta desde la que se acceda a las otras cuentas (el "centro") y qué cuentas quiere que aparezcan en el selector de clientes (el "radio").

Antes de vincular cuentas, asegúrese de cumplir con los siguientes requisitos:

- Tiene permisos de acceso total en Citrix Cloud.
- Tiene acceso al Entorno de scripting integrado (ISE) de Windows PowerShell.
- Tiene los ID de cliente de las cuentas de Citrix Cloud que quiere vincular. El ID de cliente aparece en la esquina superior derecha de la consola de administración de cada cuenta.



- Tiene el token de portador de Citrix CWSAuth para la cuenta de Citrix Cloud que quiere vincular como cuenta central. Para obtener este token de portador, siga las instrucciones de CTX330675.

Debe proporcionar esta información al vincular sus cuentas de Citrix Cloud.

Para vincular cuentas de Citrix Cloud

1. Abra el ISE de PowerShell y pegue este script en el panel de trabajo:

```
1  $headers = @{
2    }
3
4  $headers.Add("Accept","application/json")
5  $headers.Add("Content-Type","application/json")
6  $headers.Add("Authorization","CWSAuth bearer=XXXXXXX")
7
8  $uri = "https://trust.citrixworkspacesapi.net/HubCustomerID/links"
9
10 $resp = Invoke-RestMethod -Method Get -Uri $uri -Headers $headers
11 $allLinks = $resp.linkedCustomers + @("SpokeCustomerID")
12
13 $body = @{
14  "customers"=$allLinks }
15
16 $bodyjson = $body | ConvertTo-Json
17
18 $resp = Invoke-WebRequest -Method Post -Uri $uri -Headers $headers
       -Body $bodyjson -ContentType 'application/json'
19 Write-Host "Citrix Cloud Status Code: $($resp.RawContent)"
20 <!--NeedCopy-->
```

2. En la línea 4, sustituya `CWSAuth bearer=XXXXXXX` por su valor de CWSAuth (por ejemplo, `CWSAuth bearer=AbCdef123Ghik...`). Este valor es un hash largo que se parece a una clave de certificado.
3. En la línea 6, sustituya `HubCustomerID` por el ID de cliente de la cuenta del centro.
4. En la línea 9, sustituya `SpokeCustomerID` por el ID de cliente de la cuenta del centro.
5. Ejecute el script.
6. Repita los pasos del 3 al 5 para vincular cuentas adicionales como radios.

Para desvincular cuentas de Citrix Cloud

1. Abra el ISE de PowerShell. Si el ISE de PowerShell ya está abierto, borre el contenido del panel de trabajo.
2. Pegue este script en el panel de trabajo:

```
1  $headers = @{
2    }
3
```



```
4  $headers.Add("Accept","application/json")
5  $headers.Add("Content-Type","application/json")
6  $headers.Add("Authorization","CWSAuth bearer=XXXXXXX")
7
8  $uri = "https://trust.citrixworkspacesapi.net/HubCustomerID/links/
       SpokeCustomerID"
9
10 $resp = Invoke-WebRequest -Method Delete -Uri $uri -Headers
       $headers
11 Write-Host "Response: $($resp.RawContent)"
12 <!--NeedCopy-->
```

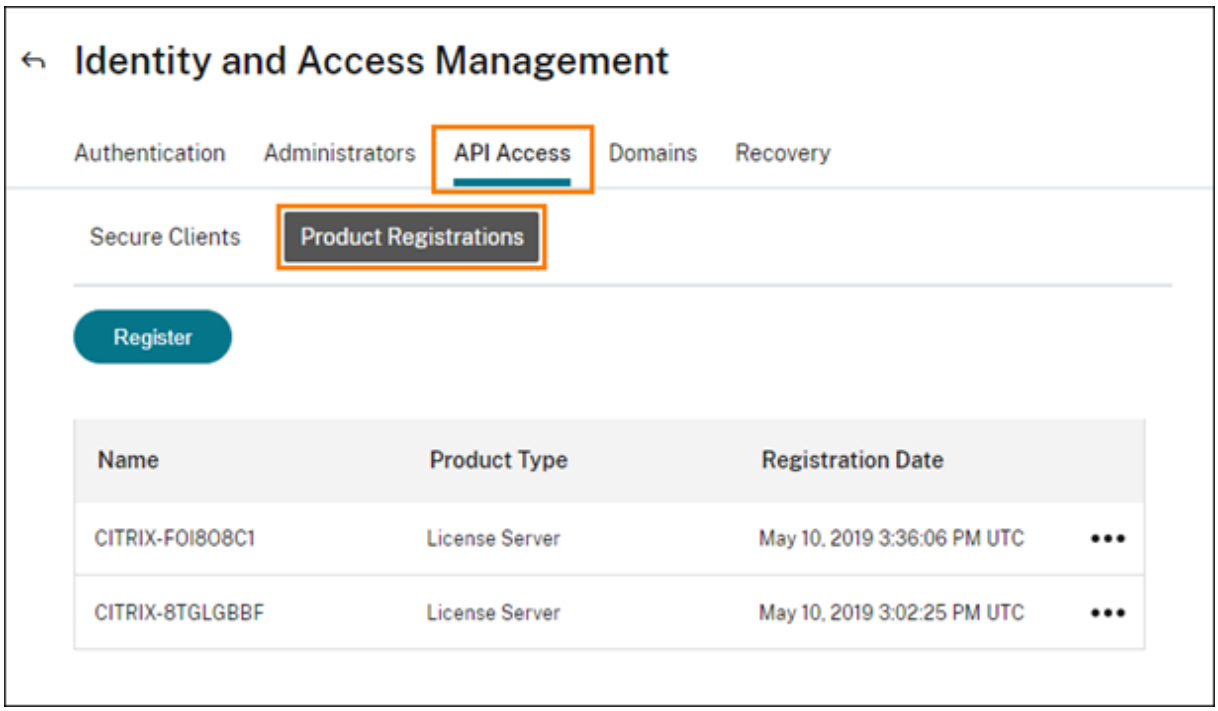
3. En la línea 4, sustituya `CWSAuth bearer=xxxxxxx1` por su valor de CWSAuth (por ejemplo, `CWSAuth bearer=AbCdef123Ghik...`). Este valor es un hash largo que se parece a una clave de certificado.
4. En la línea 6, sustituya `HubCustomerID` por el ID de cliente de la cuenta del centro.
5. En la línea 6, sustituya `SpokeCustomerID` por el ID de cliente de la cuenta del centro.
6. Ejecute el script.
7. Repita los pasos del 4 al 6 para desvincular cuentas adicionales.

Registrar productos locales en Citrix Cloud

October 2, 2023

Puede registrar fácilmente su producto Citrix local con la activación de código corto a través de Citrix Cloud. Según el producto, este código de 8 dígitos podría generarse durante el proceso de instalación del producto o al ejecutar la consola de administración del producto. Cuando el producto le pide que se registre, solicita el código de Citrix Cloud y lo muestra. A continuación, puede copiar y pegar este código o introducirlo manualmente en Citrix Cloud.

Tras el registro, la página Registros de productos (**Administración de acceso e identidad > Acceso a API > Registros de productos**) muestra los servidores en los que residen los productos registrados.



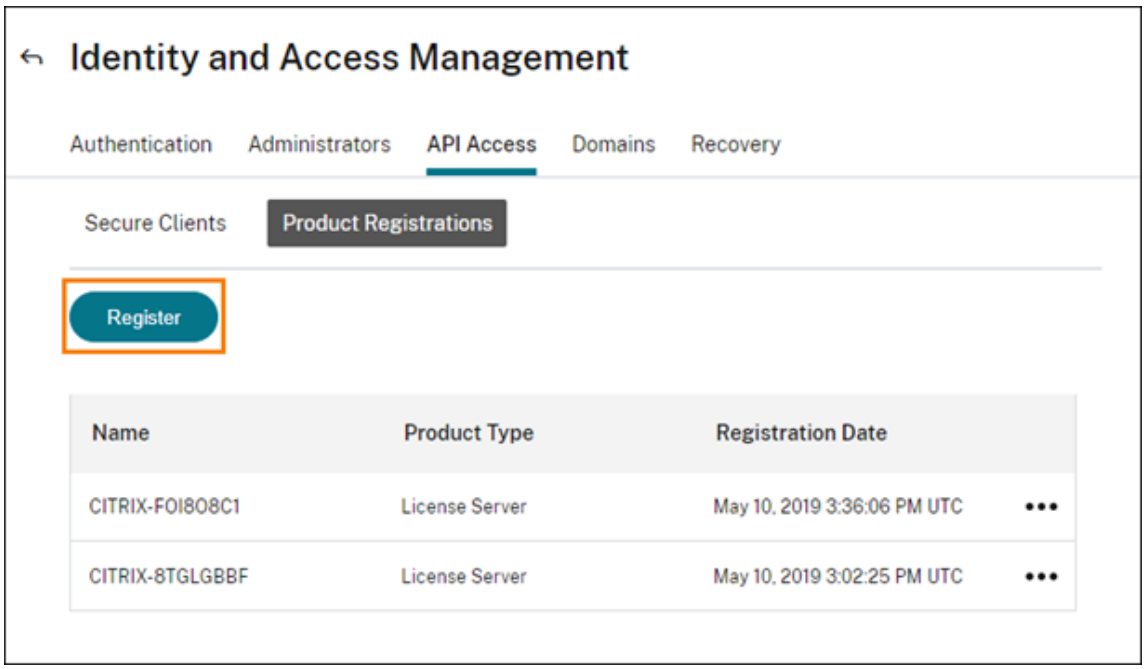
Los productos locales que puede registrar en Citrix Cloud incluyen:

- Dispositivo Citrix Connector para Cloud Services
- Servicio de autenticación federada de Citrix
- Citrix License Server
- Citrix Virtual Apps and Desktops, al registrar un sitio en Citrix Analytics for Performance

> **Nota:**
>
> En este artículo se describen los pasos para registrar un producto local en Citrix Cloud. Para conocer los requisitos específicos de un producto, consulte la documentación de ese producto.

Registrar un producto

1. Desde la consola de administración de Citrix Cloud, haga clic en el botón de menú y seleccione **Administración de acceso e identidad**.
2. Seleccione **Acceso a API > Registros de productos** y, a continuación, seleccione **Registrar**.

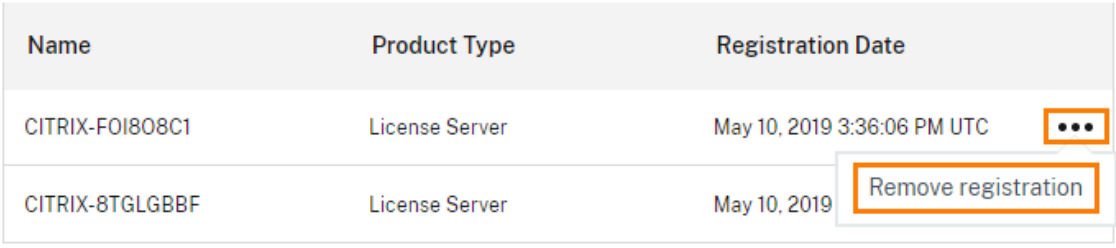


3. Introduzca el código alfanumérico de 8 caracteres de su producto Citrix y haga clic en **Continuar**.
4. Revise los detalles de registro y, a continuación, haga clic en **Registrar**.

Eliminar un registro de producto

Si quita de su entorno servidores que ejecutan un producto Citrix registrado, la página Registros de productos seguirá mostrando los servidores. Siga los pasos siguientes para quitar los servidores que hubiera en Citrix Cloud. Si es necesario, puede registrar el producto de nuevo más tarde para ver los servidores en la página Registros de productos.

1. En la página Registros de productos, busque el servidor a eliminar.
2. Haga clic en el botón de puntos suspensivos y seleccione **Quitar registro**.



3. Cuando se le solicite, seleccione **Quitar**.

Conectar Active Directory con Citrix Cloud

July 2, 2024

Citrix Cloud le permite usar su directorio de Active Directory (AD) local para autenticar a los suscriptores de espacios de trabajo. Además, algunos métodos de autenticación de Workspace necesitan una conexión entre AD y Citrix Cloud. Para obtener más información, consulte Elegir o cambiar los métodos de autenticación.

Citrix Cloud también admite el uso de tokens como segundo factor de autenticación para los suscriptores que inicien sesión en Workspace a través de Active Directory. Los suscriptores de espacios de trabajo pueden generar tokens mediante cualquier aplicación que siga el estándar TOTP (contraseña temporal de un solo uso), como Citrix SSO.

Para obtener más información sobre cómo autenticar suscriptores de espacios de trabajo con Active Directory y tokens, consulte Active Directory y token.

> **Sugerencia:**
>
> Puede obtener más información sobre los proveedores de identidades admitidos con el curso Introduction to Citrix Identity and Authentication. El módulo "Planning Citrix Identity and Access Management"incluye vídeos breves que le guían para conectar este proveedor de identidades a Citrix Cloud y habilitar la autenticación para Citrix Workspace.

Conectar Active Directory

La conexión de su Active Directory a Citrix Cloud implica instalar conectores en el dominio. Puede optar por utilizar Cloud Connectors o Connector Appliances como conectores para Active Directory. Para elegir el tipo de conector que utilizar en su entorno, consulte estos artículos:

- Casos de implementación de Cloud Connectors en Active Directory
- Casos de implementación para Connector Appliances en Active Directory

Conectar Active Directory a través de Connector Appliances

Puede usar un Connector Appliance para conectar una ubicación de recursos a bosques que no contienen recursos de Citrix Virtual Apps and Desktops. Por ejemplo, en el caso de los clientes de Citrix Secure Private Access o los clientes de Citrix Virtual Apps and Desktops con algunos bosques que solo se utilizan para la autenticación de usuarios.

Para obtener más información, consulte Active Directory con el Connector Appliance.

Conectar Active Directory mediante Cloud Connectors

Se requieren al menos dos Cloud Connectors para garantizar una conexión de alta disponibilidad a Citrix Cloud. Para obtener más información, consulte estos artículos:

- Detalles técnicos de Cloud Connector: Para requisitos del sistema y recomendaciones de implementación.
- Instalación de Cloud Connector: Para obtener instrucciones de instalación mediante la interfaz gráfica o la línea de comandos.

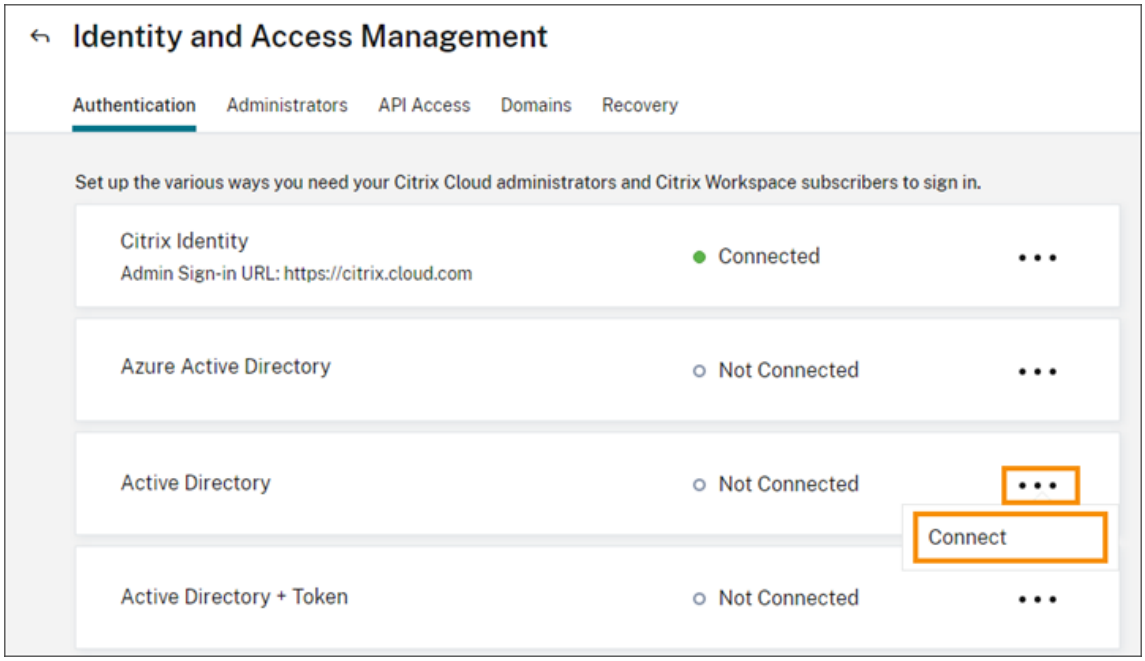
La conexión de Active Directory con Citrix Cloud implica las siguientes tareas:

1. Instale Cloud Connectors en su dominio. Citrix recomienda instalar dos Cloud Connectors para tener alta disponibilidad.
2. Si corresponde, habilite tokens para los dispositivos de usuario. Los suscriptores solo pueden inscribir dispositivos de uno en uno.

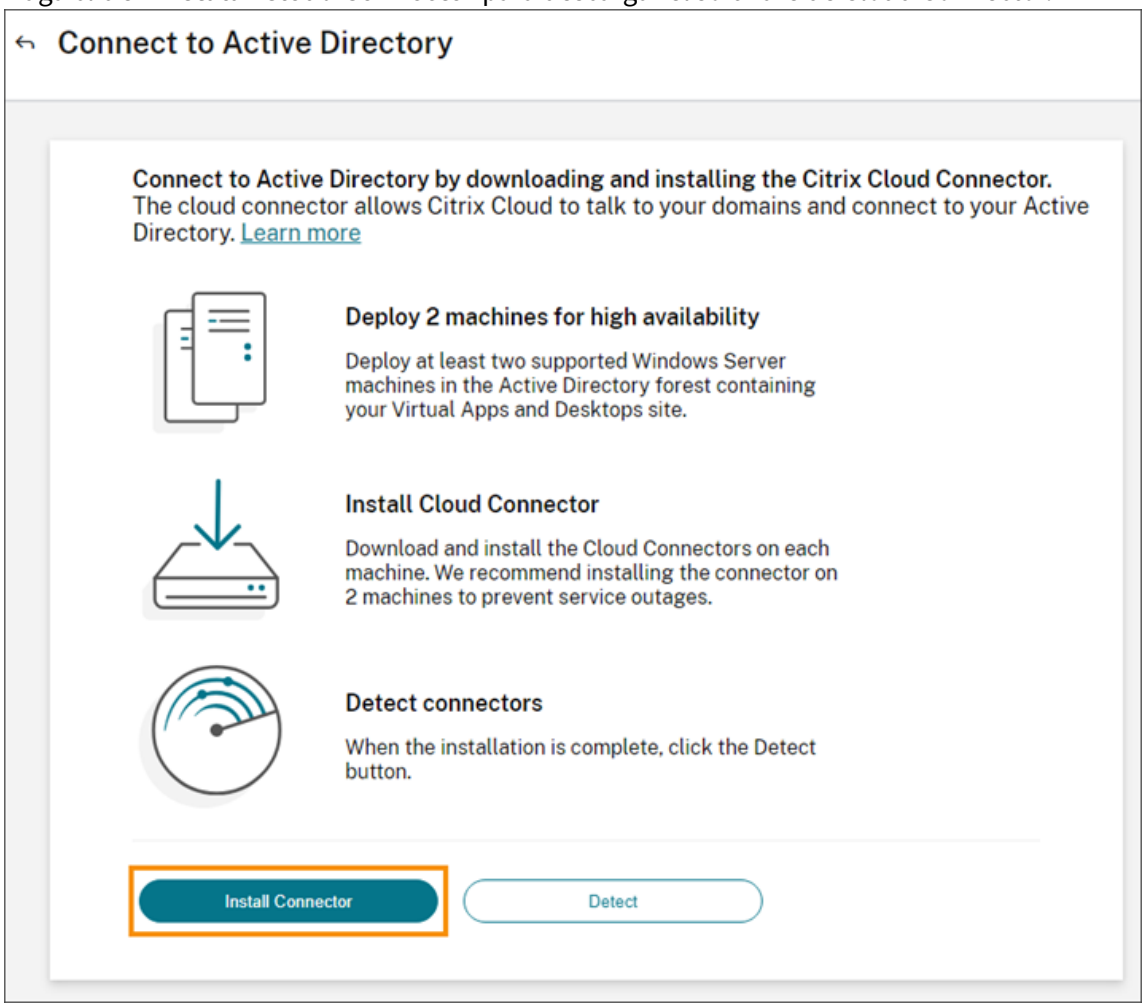
> **Importante:**
>
> Si piensa implementar Cloud Connectors para usarlos con Citrix DaaS, es posible que se necesiten pasos adicionales para garantizar que sus dominios de AD estén registrados y activos después de la implementación de los Cloud Connectors. Al verificar que los dominios de AD están activos en Citrix Cloud, se garantiza que la configuración del catálogo de máquinas se realice sin problemas. Para obtener más información sobre los pasos posteriores a la implementación de Citrix DaaS, consulte Agregar un tipo de recurso o activar un dominio no utilizado en Citrix Cloud en la documentación de producto de Citrix DaaS.

Para conectar su Active Directory a Citrix Cloud

1. Desde la consola de administración de Citrix Cloud, haga clic en el botón de menú y seleccione **Administración de acceso e identidad**.
2. En la ficha **Autenticación**, en **Active Directory**, haga clic en el menú de puntos suspensivos y seleccione **Conectar**.



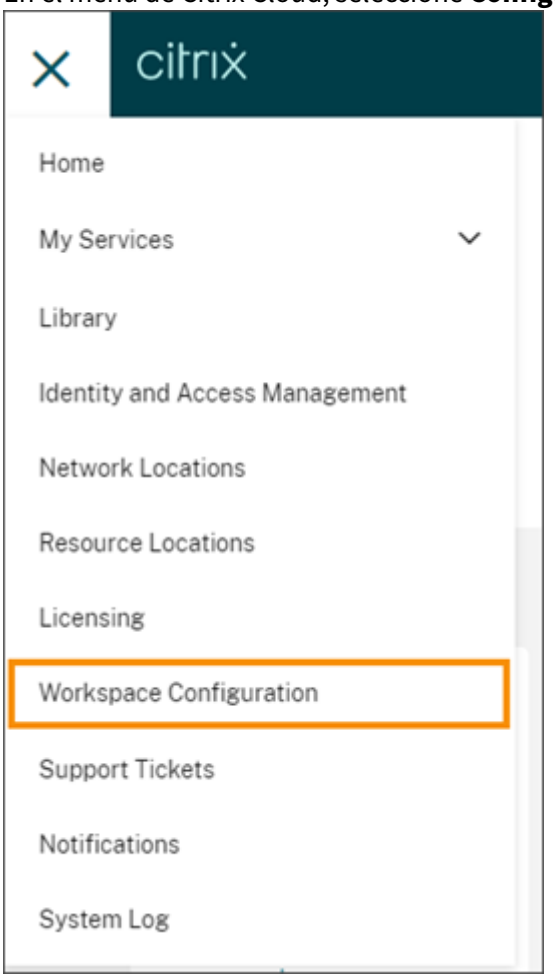
3. Haga clic en **Instalar Cloud Connector** para descargar el software de Cloud Connector.



4. Inicie el instalador de Cloud Connector y siga los pasos indicados en el asistente de instalación.
5. Desde la página **Conectar a Active Directory**, haga clic en **Detectar**. Después de la verificación, Citrix Cloud muestra un mensaje de que su Active Directory está conectado.
6. Haga clic en **Volver a Autenticación**. La entrada de **Active Directory** está marcada como **Habilitada** en la ficha **Autenticación**.

Para habilitar la autenticación con Active Directory y token

1. Conecte Active Directory con Citrix Cloud mediante Connector Appliances o Cloud Connectors.
2. En la sección **Administración de acceso e identidad** de Citrix Cloud, en la ficha **Autenticación**, compruebe que la entrada **Active Directory** esté marcada como **Habilitada**.
3. Haga clic en **Siguiente**. Aparece la página **Configurar token**, y la opción **Dispositivo único** está seleccionada de forma predeterminada.
4. Haga clic en **Guardar y finalizar** para completar la configuración. En la ficha **Autenticación**, la entrada **Active Directory + Token** está **habilitada**.
5. Habilite la autenticación con tokens para los espacios de trabajo:
   a) En el menú de Citrix Cloud, seleccione **Configuración de Workspace**.



b) En la ficha **Autenticación**, seleccione **Active Directory + Token**.

Después de habilitar la autenticación con Active Directory y token, los suscriptores de Workspace pueden registrar su dispositivo y usar una aplicación de autenticación para generar tokens. Los suscriptores solo pueden registrar dispositivos de uno en uno. Para obtener instrucciones sobre cómo registrar los dispositivos de los suscriptores, consulte Autenticación de dos factores (opcional).

Para obtener información sobre las opciones para reinscribir dispositivos de los suscriptores, consulte Reinscribir un dispositivo.

Más información

Citrix Tech Zone:

- Tech Insight: Authentication - TOTP
- Tech Insight: Authentication - Push

Conectar Azure Active Directory a Citrix Cloud

May 30, 2024

Citrix Cloud le permite usar Azure Active Directory (AD) para autenticar a administradores de Citrix Cloud y suscriptores de espacios de trabajo.

Al usar Azure AD con Citrix Cloud, puede:

- Utilizar su propio Active Directory y así controlar la auditoría y las directivas de contraseña, así como inhabilitar cuentas fácilmente cuando sea necesario.
- Configurar la autenticación de varios factores para conseguir un mayor nivel de seguridad frente a la posibilidad de robo de credenciales de inicio de sesión.
- Usar una página de inicio de sesión personalizada con su propia marca, de forma que los usuarios sepan que están entrando en el sitio correcto.
- Usar la federación con el proveedor de identidades que usted prefiera, incluidos ADFS, Okta y Ping, entre otros.

Permisos y aplicaciones de Azure AD

Citrix Cloud incluye una aplicación de Azure AD que permite a Citrix Cloud conectarse con Azure AD sin necesidad de iniciar sesión en una sesión activa de Azure AD. Desde la presentación de esta aplicación, Citrix ha publicado actualizaciones para mejorar el rendimiento y ofrecer nuevas funciones y permisos.

Si ya tiene una conexión de Azure AD a Citrix Cloud y quiere usar la aplicación actualizada más reciente, debe actualizar la conexión de Azure AD en Citrix Cloud. Para obtener más información, consulte Conectarse de nuevo a Azure AD para la aplicación actualizada en este artículo. Si decide no actualizar la aplicación, la conexión existente seguirá funcionando con normalidad.

Para obtener más información sobre las aplicaciones y los permisos de Azure AD que Citrix Cloud usa para conectarse a su directorio de Azure AD, consulte Permisos de Azure Active Directory para Citrix Cloud.

> **Sugerencia:**
>
> Puede obtener más información sobre los proveedores de identidades admitidos con el curso Introduction to Citrix Identity and Authentication. El módulo "Planning Citrix Identity and Access Management"incluye vídeos breves que le guían para conectar este proveedor de identidades a Citrix Cloud y habilitar la autenticación para Citrix Workspace.

Autenticación con varias cuentas de Citrix Cloud

En este artículo se describe cómo conectar Azure AD como un proveedor de identidades con una sola cuenta de Citrix Cloud. Si tiene varias cuentas de Citrix Cloud, puede conectar cada una de ellas al mismo arrendatario de Azure AD. Realice las siguientes tareas:

1. Inicie sesión en su cuenta de Citrix Cloud y seleccione el ID de cliente correspondiente en el selector de clientes.
2. Si el cliente seleccionado es el primero al que va a conectar a Azure AD, siga todos los pasos que se indican en este artículo para sincronizar su AD y Azure AD, conectar el cliente a Citrix Cloud y agregar administradores.
3. Para conectar a otro cliente, haga clic en el menú de usuarios en la esquina superior derecha de la consola de Citrix Cloud, seleccione **Cambiar cliente**y seleccione el siguiente ID de cliente al que desee conectarse.
4. Para conectar el cliente a su Azure AD, siga el procedimiento que se describe en la sección Conectar Citrix Cloud a Azure AD de este artículo.
5. Repita los pasos 3 y 4 para cada ID de cliente.

Preparar Active Directory y Azure AD

Para poder utilizar Azure AD, debe cumplir estos requisitos:

- Dispone de una cuenta de Microsoft Azure. Todas las cuentas de Azure se incluyen gratis con Azure AD. Si no dispone de una cuenta de Azure, regístrese en https://azure.microsoft.com/en-us/free/?v=17.36.

- Tiene el rol de administrador global en Azure AD. Este rol es necesario para dar a Citrix Cloud su consentimiento para conectarse a Azure AD.
- Las cuentas de administrador tienen su propiedad de correo ("mail") configurada en Azure AD. Para ello, puede sincronizar las cuentas de su sistema local de Active Directory con Azure AD mediante la herramienta de Microsoft Azure AD Connect. También puede configurar las cuentas no sincronizadas de Azure AD con correo electrónico de Office 365.

Sincronizar las cuentas con Azure AD Connect

1. Compruebe que las cuentas de Active Directory tienen la propiedad de usuario "Correo electrónico"configurada:
   a) Abra "Usuarios y equipos"de Active Directory.
   b) En la carpeta **Usuarios**, busque la cuenta que quiera verificar, haga clic en ella con el botón secundario y seleccione **Propiedades**. En la ficha **General**, verifique que el campo **Correo electrónico** contiene una entrada válida. Citrix Cloud requiere que los administradores que se agregan desde Azure AD tengan direcciones de correo electrónico diferentes a las de los administradores que inician sesión con una identidad alojada por Citrix.
2. Instale y configure Azure AD Connect. Para obtener instrucciones completas, consulte Introducción a Azure AD Connect mediante la configuración rápida en el sitio web de Microsoft Azure.

Conectar Citrix Cloud a Azure AD

Para conectar su cuenta de Citrix Cloud a su Azure AD, Citrix Cloud necesita permiso para acceder a su perfil de usuario (o el perfil del usuario que inició la sesión), así como a los perfiles básicos de los usuarios en Azure AD. Citrix le solicita este permiso para poder obtener su nombre y su dirección de correo electrónico (como administrador) y permitirle buscar otros usuarios para agregarlos como administradores más adelante. Para obtener más información sobre los permisos de aplicación que Citrix Cloud solicita, consulte Permisos de Azure Active Directory para Citrix Cloud.

> **Importante:**
>
> Debe ser un administrador global en Azure AD para completar esta tarea o pedirle a un administrador global que se ocupe de los requisitos previos antes de iniciar sesión en Citrix Cloud.

1. Haga clic en el botón de **menú** en la esquina superior izquierda de la página y seleccione **Administración de acceso e identidad**.
2. Busque Azure Active Directory y seleccione **Conectar** en el menú de puntos suspensivos.
3. Cuando se le solicite, introduzca un identificador para su empresa, que sea corto y pueda usarse en una URL, y haga clic en **Conectar**. El identificador que elija debe ser único a nivel global dentro de Citrix Cloud.

4. Cuando se le solicite, inicie sesión en la cuenta de Azure con la que quiere conectarse. Azure muestra los permisos que Citrix Cloud necesita para acceder a la cuenta y obtener la información necesaria para la conexión. La mayoría de estos permisos son de solo lectura y permiten a Citrix Cloud recopilar información básica de Microsoft Graph, como grupos y perfiles de usuario. Si integró Citrix Endpoint Management o XenMobile Server con Microsoft Intune, debe conceder permisos de lectura y escritura relacionados con Microsoft Intune. Para obtener más información, consulte Permisos de Azure Active Directory para Citrix Cloud.
5. Haga clic en **Aceptar** para aceptar la solicitud de permisos.

Método de conexión alternativo

Puede separar el flujo de conexión en las dos fases siguientes:

1. Creación de la aplicación Azure AD (Entra ID) en Azure.
2. Conexión de Citrix Cloud a la aplicación Azure AD (Entra ID) en Citrix Cloud.

En primer lugar, debe crear una URL que el administrador global pueda usar para agregar las aplicaciones empresariales al arrendatario. Para obtener más información, consulte Construct the URL for granting tenant-wide admin consent.

Esta es la explicación de la URL creada.
`https://login.microsoftonline.com/<tenant url>/adminconsent?client_id=f9c0e999-22e7-409f-bb5e-956986abdf02&redirect_uri=https://portal.azure.com`

dónde:
`tenant url` es la URL o ID del arrendatario.
`f9c0e999-22e7-409f-bb5e-956986abdf02` es el ID de cliente de Citrix Cloud.

Agregar administradores a Citrix Cloud desde Azure AD

Citrix Cloud permite agregar administradores de forma individual o como grupos de Azure AD.

Para agregar administradores individuales desde Azure AD, consulte Administrar el acceso del administrador.

Para agregar grupos de administradores de Azure AD a Citrix Cloud, consulte Administrar grupos de administradores.

Iniciar sesión en Citrix Cloud mediante Azure AD

Una vez conectadas las cuentas de usuario de Azure AD, los usuarios pueden iniciar sesiones en Citrix Cloud mediante los siguientes métodos:

- Vaya a la URL de inicio de sesión de administradores que configuró cuando conectó inicialmente el proveedor de identidades de Azure AD de su empresa. Ejemplo:`https://citrix.cloud.com/go/mycompany`
- En la página de inicio de sesión de Citrix Cloud, haga clic en **Iniciar sesión con mis credenciales de empresa**, introduzca el identificador que creó cuando conectó inicialmente Azure AD (por ejemplo, "miempresa") y haga clic en **Continuar**.

Habilitar la autenticación de Azure AD para espacios de trabajo

Después de conectar Azure AD a Citrix Cloud, puede permitir que los suscriptores se autentiquen en sus espacios de trabajo a través de Azure AD.

> **Importante:**
>
> Antes de habilitar la autenticación del espacio de trabajo de Azure AD, revise la sección Azure Active Directory para conocer los aspectos a tener en cuenta sobre el uso de Azure AD con los espacios de trabajo.

1. En Citrix Cloud, haga clic en el menú situado en la esquina superior izquierda y seleccione **Configuración de Workspace**.
2. En la ficha **Autenticación**, seleccione **Azure Active Directory**.
3. Haga clic en **Confirmar** para aceptar los cambios en la experiencia del espacio de trabajo; se producirán cuando la autenticación de Azure AD esté habilitada.

Habilitar las funciones avanzadas de Azure AD

Azure AD ofrece autenticación de varios factores, funciones de seguridad de primera clase, federación con 20 proveedores de identidades diferentes y autoservicio de restablecimiento y cambio de contraseñas, entre otras muchas funciones. Si activa estas funciones para los usuarios de Azure AD, Citrix Cloud podrá aprovechar estas capacidades automáticamente.

Para comparar las capacidades de nivel de servicio de Azure AD y los precios correspondientes, consulte https://azure.microsoft.com/en-us/pricing/details/active-directory/.

Conectarse de nuevo a Azure AD para la aplicación actualizada

Citrix Cloud incluye una aplicación de Azure AD que permite a Citrix Cloud conectarse con Azure AD sin necesidad de iniciar sesión en una sesión activa de Azure AD. Desde la presentación de esta aplicación, Citrix la ha actualizado de esta manera:

- En agosto de 2018, esta aplicación se actualizó para mejorar su rendimiento y prepararle mejor para futuras versiones.

- En mayo de 2019, la aplicación se actualizó para agregar grupos de administradores de Azure AD a Citrix Cloud.
- En abril de 2022, la aplicación se actualizó para usar el permiso GroupMember.Read.All, que reemplaza al permiso Group.Read.All.

Si conectó Azure AD a Citrix Cloud antes de que se publicaran estas actualizaciones y quiere usar la aplicación actualizada más reciente, debe desconectar Azure AD de Citrix Cloud y conectarlo de nuevo. El uso de la aplicación más reciente es opcional. Si decide no actualizar la aplicación, la conexión existente seguirá funcionando con normalidad.

Requisitos

Antes de conectar Azure AD de nuevo, verifique que cumple estos requisitos:

- Debe ser un administrador con permisos de acceso total en el proveedor de identidades de Citrix predeterminado. Si ha iniciado sesión en Citrix Cloud con las credenciales de Azure AD, se produce un error en la reconexión. Si no tiene ningún administrador que utilice el proveedor de identidades de Citrix en su cuenta, puede agregar uno temporalmente y eliminarlo después de conectar Azure AD de nuevo. Para obtener instrucciones, consulte Invitar a administradores individuales.
- Si usa Azure AD para autenticar a suscriptores de espacios de trabajo, seleccione otro proveedor de identidades de manera temporal. Citrix Cloud no le permite desconectar Azure AD si también se usa como método de autenticación para Citrix Workspace. Para obtener más información, consulte Elegir o cambiar los métodos de autenticación en la documentación de Citrix Workspace.

Para conectar Azure AD de nuevo

1. Inicie sesión en Citrix Cloud como administrador con permisos de acceso total en el proveedor de identidades de Citrix.
2. Desde el menú de Citrix Cloud, seleccione **Administración de acceso e identidad** y, luego, **Autenticación**.
3. Busque **Azure Active Directory** y seleccione **Desconectar** en el menú de puntos suspensivos que hay en el extremo derecho de la página.
4. En el menú de puntos suspensivos, seleccione **Conectar**.

> **Nota:**
>
> Si va a desconectar Azure Active Directory como se menciona en el paso 3, Citrix Cloud solicita al administrador que elimine todos los perfiles de administrador de este proveedor de identidades. Para evitar esta operación, el administrador puede seguir los pasos que se indican a continuación

> para reconectar el proveedor de identidades de Azure AD.
>
> 1. Como administrador global, vaya a Azure y elimine la aplicación.
> 2. Inicie sesión en Citrix Cloud, vaya a **Administración de acceso e identidad** y haga clic en **Autenticación**. En la ficha **Autenticación**, puede observar que Azure AD sigue conectado.
> 3. Agregue un nuevo administrador en Citrix Cloud para Azure AD.
>
> Esto hará que se cree de nuevo la aplicación y tenga lugar la reconexión sin eliminar a los administradores.

Permisos de Azure Active Directory para Citrix Cloud

December 12, 2023

En este artículo se describen los permisos que Citrix Cloud solicita al conectar y usar Azure Active Directory (AD). Según cómo se use Azure AD con la cuenta de Citrix Cloud, es posible que se creen una o varias aplicaciones de empresa en el arrendatario de destino de Azure AD. Puede conectar varias cuentas de Citrix Cloud a un arrendatario de Azure AD y usar las mismas aplicaciones de empresa sin crear un conjunto de aplicaciones para cada cuenta.

> **Nota:**
>
> A partir de abril de 2022, la aplicación de Azure AD que Citrix Cloud usa para conectar su Azure AD se actualizó para usar el permiso GroupMember.Read.All en lugar del permiso Group.Read.All. Si ya tiene una conexión de Azure AD (de antes de abril de 2022) y quiere que la aplicación utilice el nuevo permiso, debe desconectar y reconectar Azure AD a Citrix Cloud. Esta acción garantiza que su cuenta utilice la aplicación de Azure AD más reciente en Citrix Cloud. Para obtener más información, consulte Conectarse de nuevo a Azure AD para la aplicación actualizada.
>
> Si decide no actualizar la aplicación, la conexión existente seguirá funcionando con normalidad.

Aplicaciones de empresa

En la siguiente tabla, se enumeran las aplicaciones de empresa de Azure AD que Citrix Cloud usa al conectarse y usar Azure AD y el propósito para el que se usa cada aplicación.

Nombre	ID de aplicación	Uso
Citrix Cloud	e95c4605-aeab-48d9-9c36-1a262ef8048e	Inicio de sesión de suscriptores de espacios de trabajo

Nombre	ID de aplicación	Uso
Citrix Cloud	f9c0e999-22e7-409f-bb5e-956986abdf02	Conexión predeterminada entre Azure AD y Citrix Cloud
Citrix Cloud	1b32f261-b20c-4399-8368-c8f0092b4470	Invitaciones e inicios de sesión de administrador
Citrix Cloud	5c913119-2257-4316-9994-5e8f3832265b	Conexión predeterminada entre Azure AD y Citrix Cloud con Citrix Endpoint Management
Citrix Cloud	e067934c-b52d-4e92-b1ca-70700bd1124e	Conexión antigua entre Azure AD y Citrix Cloud con Citrix Endpoint Management

Permisos

Los permisos en las aplicaciones de empresa de Citrix Cloud permiten que Citrix Cloud acceda a ciertos datos en su arrendatario de Azure AD. Citrix Cloud utiliza estos datos para realizar funciones específicas, como conectarse a su arrendatario de Azure AD, permitir que los administradores inicien sesión en Citrix Cloud mediante una URL de inicio de sesión dedicada y conectar su arrendatario de Azure AD a Endpoint Management. Citrix Cloud solo puede acceder a estos datos con su consentimiento. Estos permisos representan la cantidad mínima de privilegios que Citrix Cloud necesita para funcionar con Azure AD. Para obtener más información sobre los permisos y el consentimiento en Azure AD, consulte Permissions and consent in the Microsoft identity platform en el sitio web de documentación de Microsoft Azure.

En este artículo, cada conjunto de permisos de aplicación de Azure AD incluye la siguiente información:

- **Nombre de la API:** Las aplicaciones de recursos desde las que Citrix Cloud solicita los permisos. Estas aplicaciones son Microsoft Graph y Windows Azure Active Directory. Citrix Cloud solicita los mismos permisos desde estas dos aplicaciones de recursos.
- **Tipo:** Los niveles de acceso que Citrix Cloud solicita para un permiso determinado. Los permisos en una aplicación de empresa pueden tener uno de los siguientes niveles de acceso:
  - Los **permisos delegados** se utilizan para actuar en nombre de un usuario que ha iniciado sesión, como cuando se consulta el perfil del usuario.
  - Los **permisos de aplicación** se utilizan cuando la aplicación realiza una acción sin la presencia del usuario, como consultas a usuarios de un grupo en particular. Este tipo de permiso requiere el consentimiento de un administrador global en Azure AD.

- **Valor de notificación:** La cadena de información que Azure AD asigna a un permiso determinado. Los permisos en una aplicación de empresa pueden tener uno de los siguientes valores de notificación:
  - **User.Read:** Permite a los administradores de Citrix Cloud agregar usuarios desde el directorio de Azure AD conectado como administradores de la cuenta de Citrix Cloud.
  - **User.ReadBasic.All:** Recopila información básica del perfil del usuario. Es un subconjunto de User.Read.All, pero el permiso en sí sigue destinado para la compatibilidad con versiones anteriores.
  - **User.Read.All:** Citrix Cloud llama a List users en Microsoft Graph para habilitar la navegación y la selección de usuarios desde el directorio de Azure AD del cliente conectado. Por ejemplo, los usuarios de Azure AD pueden obtener acceso a un recurso de Citrix DaaS con el espacio de trabajo. Citrix Cloud no se puede usar `User.ReadBasic.All`, ya que necesita acceder a propiedades que están fuera del perfil básico, como `onPremisesSecurityIdentifier`.
  - **GroupMember.Read.All:** Citrix Cloud llama a List groups en Microsoft Graph para habilitar la navegación y la selección de grupos desde el directorio de Azure AD del cliente conectado. Por ejemplo, los grupos de Azure AD también pueden obtener acceso a aplicaciones de Citrix DaaS.
  - **Directory.Read.All:** Citrix Cloud llama a List memberOf en Microsoft Graph para obtener la pertenencia a grupos del usuario, ya que `Groups.Read.All` no es suficiente.
  - **DeviceManagementApps.ReadWrite.All:** Permite a Citrix Cloud leer y escribir en las propiedades, las asignaciones de grupo, el estado de las aplicaciones, las configuraciones de aplicaciones y las directivas de protección de aplicaciones administradas por Microsoft Intune.
  - **Directory.AccessAsUser.All:** Permite a Citrix Cloud tener el mismo acceso a la información del directorio que el usuario que ha iniciado sesión.

> **Nota:**
>
> **Directory.Read.All** solo se aplica a **Conexión predeterminada entre Azure AD y Citrix Cloud con Endpoint Management**.

Inicio de sesión de suscriptores de espacios de trabajo

Esta aplicación de Citrix Cloud (ID: e95c4605-aeab-48d9-9c36-1a262ef8048e) usa estos permisos:

Nombre de la API	Valor de notificación	Nombre del permiso	Tipo
Microsoft Graph	User.Read	Iniciar sesión y leer el perfil del usuario	Delegado

Conexión predeterminada entre Azure AD y Citrix Cloud

Esta aplicación Citrix Cloud (ID: f9c0e999-22e7-409f-bb5e-956986abdf02) utiliza estos permisos:

Nombre de la API	Valor de notificación	Permiso	Tipo
Microsoft Graph	GroupMember.Read.All	Leer todos los grupos	Delegado
Microsoft Graph	User.ReadBasic.All	Leer los perfiles básicos de todos los usuarios	Delegado
Microsoft Graph	User.Read.All	Leer los perfiles completos de todos los usuarios	Delegado
Microsoft Graph	User.Read	Iniciar sesión y leer el perfil del usuario	Delegado
Microsoft Graph	GroupMember.Read.All	Leer todos los grupos	Aplicación
Microsoft Graph	User.Read.All	Leer el perfil completo de todos los usuarios	Aplicación
Microsoft Graph	User.Read	Iniciar sesión y leer el perfil del usuario	Aplicación

Invitaciones e inicios de sesión de administrador

Esta aplicación Citrix Cloud (ID: 1b32f261-b20c-4399-8368-c8f0092b4470) usa estos permisos:

Nombre de la API	Valor de notificación	Nombre del permiso	Tipo
Microsoft Graph	User.Read	Iniciar sesión y leer el perfil del usuario	Delegado
Microsoft Graph	User.ReadBasic.All	Leer los perfiles básicos de todos los usuarios	Delegado

Conexión predeterminada entre Azure AD y Citrix Cloud con Endpoint Management

Esta aplicación Citrix Cloud (ID: 5c913119-2257-4316-9994-5e8f3832265b) utiliza estos permisos:

Nombre de la API	Valor de notificación	Nombre del permiso	Tipo
Microsoft Graph	GroupMember.Read.All	Leer todos los grupos	Delegado
Microsoft Graph	User.ReadBasic.All	Leer los perfiles básicos de todos los usuarios	Delegado
Microsoft Graph	User.Read	Iniciar sesión y leer el perfil del usuario	Delegado
Microsoft Graph	Directory.Read.All	Leer datos de directorio	Aplicación
Microsoft Graph	Directory.Read.All	Leer datos de directorio	Delegado
Microsoft Graph	DeviceManagementApps.ReadWrite.All	Leer y escribir en aplicaciones de Microsoft Intune	Delegado
Microsoft Graph	Directory.AccessAsUser.All	Acceder al directorio en nombre del usuario con la sesión iniciada	Delegado

Conexión antigua entre Azure AD y Citrix Cloud con Endpoint Management

Esta aplicación Citrix Cloud (ID: e067934c-b52d-4e92-b1ca-70700bd1124e) usa estos permisos:

Nombre de la API	Valor de notificación	Nombre del permiso	Tipo
Microsoft Graph	GroupMember.Read.All	Leer todos los grupos	Delegado
Microsoft Graph	User.ReadBasic.All	Leer los perfiles básicos de todos los usuarios	Delegado
Microsoft Graph	User.Read	Iniciar sesión y leer el perfil del usuario	Delegado
Microsoft Graph	DeviceManagementApps.ReadWrite.All	Leer y escribir en aplicaciones de Microsoft Intune	Delegado
Microsoft Graph	Directory.AccessAsUser.All	Acceder al directorio en nombre del usuario con la sesión iniciada	Delegado

Conectar un dispositivo Citrix Gateway local como proveedor de identidades con Citrix Cloud

July 2, 2024

Citrix Cloud admite el uso de dispositivos Citrix Gateway locales como proveedores de identidades para autenticar a los suscriptores que inician sesión en sus espacios de trabajo.

Con la autenticación de Citrix Gateway, puede:

- Siga autenticando a los usuarios a través de su dispositivo Citrix Gateway existente para que puedan acceder a los recursos de la implementación local de Virtual Apps and Desktops a través de Citrix Workspace.
- Utilice las funciones de autenticación, autorización y auditoría (AAA) de Citrix Gateway con Citrix Workspace.
- Utilice funciones como la autenticación PassThrough, las tarjetas inteligentes, los tokens seguros, las directivas de acceso condicional, la federación y muchas otras para proporcionar a los usuarios acceso a los recursos que necesitan a través de Citrix Workspace.

> **Sugerencia:**
>
> Puede obtener más información sobre los proveedores de identidades admitidos con el curso Introduction to Citrix Identity and Authentication. El módulo "Planning Citrix Identity and Access Management"incluye vídeos breves que le guían para conectar este proveedor de identidades a Citrix Cloud y habilitar la autenticación para Citrix Workspace.

Versiones compatibles

La autenticación de Citrix Gateway se puede utilizar con las siguientes versiones locales de producto:

- Citrix Gateway 12.1 54.13 Advanced Edition o posterior
- Citrix Gateway 13.0 41.20 Advanced Edition o posterior

Requisitos previos

Cloud Connectors

Necesita al menos dos (2) servidores donde instalar el software Citrix Cloud Connector. Estos servidores deben cumplir los siguientes requisitos:

- Cumplir los requisitos del sistema descritos en los Detalles técnicos de Cloud Connector.

- No tener ningún otro componente de Citrix instalado, no ser un controlador de dominio de Active Directory ni ser cualquier otra máquina de importancia crítica para la infraestructura de la ubicación de recursos.
- Estar unido al dominio donde reside el sitio. Si los usuarios acceden a las aplicaciones del sitio en varios dominios, debe instalar al menos dos Cloud Connectors en cada dominio.
- Estar conectado a una red que puede contactar con el sitio.
- Debe estar conectada a Internet. Para obtener más información, consulte Requisitos del sistema y de conectividad.
- Se requieren al menos dos Cloud Connectors para garantizar una conexión de alta disponibilidad con Citrix Cloud. Después de la instalación, los Cloud Connectors permiten a Citrix Cloud localizar y comunicarse con su sitio.

Para obtener más información sobre la instalación de Cloud Connector, consulte Instalar Cloud Connector.

Active Directory

Antes de habilitar la autenticación de Citrix Gateway, realice las siguientes tareas:

- Compruebe que los suscriptores de Workspace tengan cuentas de usuario en Active Directory (AD). Los suscriptores sin cuentas de AD no pueden iniciar sesión en Workspace correctamente.
- Compruebe que las propiedades de usuario de las cuentas de AD de los suscriptores estén rellenadas. Citrix Cloud requiere estas propiedades para establecer el contexto de usuario cuando los suscriptores inicien sesión. Si estas propiedades no se rellenan, los suscriptores no pueden iniciar sesión en Workspace. Estas propiedades incluyen lo siguiente:
  - Dirección de correo electrónico
  - Nombre simplificado
  - Nombre común
  - Nombre de cuenta SAM
  - Nombre principal del usuario
  - OID
  - SID
- Conecte Active Directory (AD) con su cuenta de Citrix Cloud. En esta tarea, instala el software de Cloud Connector en los servidores que ha preparado, tal y como se describe en la sección Cloud Connectors. Los Cloud Connectors permiten a Citrix Cloud comunicarse con su entorno local. Para obtener instrucciones, consulte Conectar Active Directory con Citrix Cloud.
- Si lleva a cabo la federación con la autenticación de Citrix Gateway, sincronice los usuarios de AD con el proveedor de la federación. Citrix Cloud necesita los atributos de usuario de AD para los suscriptores de espacios de trabajo para que puedan iniciar sesión correctamente.

Requisitos

Directivas avanzadas de Citrix Gateway

Para la autenticación de Citrix Gateway, se necesitan directivas avanzadas en el Gateway local porque las directivas clásicas han dejado de utilizarse. Con las directivas avanzadas, está disponible la autenticación de varios factores (MFA) para Citrix Cloud, incluidas opciones como el encadenamiento del proveedor de identidades. Si utiliza ahora directivas clásicas, debe crear directivas avanzadas para utilizar la autenticación de Citrix Gateway en Citrix Cloud. Puede volver a utilizar la parte Acciones de la directiva clásica cuando cree la directiva avanzada.

Certificados para firma

Cuando configure el Gateway para autenticar suscriptores en Citrix Workspace, el Gateway actúa como un proveedor de OpenID Connect. Los mensajes entre Citrix Cloud y Gateway se ajustan al protocolo OIDC, que implica la firma digital de tokens. Por lo tanto, debe configurar un certificado para firmar estos tokens. Este certificado debe ser emitido por una entidad de certificación (CA) pública. No se admite el uso de un certificado emitido por una CA privada, ya que no hay forma de proporcionar a Citrix Cloud el certificado raíz de la CA privada. Por lo tanto, la cadena de certificados de confianza no se puede establecer. Si configura varios certificados para la firma, estas claves se rotan para cada mensaje.

Las claves deben estar enlazadas a la **VPN global**. Sin esas claves, los suscriptores no pueden acceder a su espacio de trabajo después de iniciar sesión.

Sincronización de relojes

Dado que los mensajes firmados digitalmente en OIDC llevan una marca de hora, el Gateway debe estar sincronizado con la hora NTP. Si el reloj no está sincronizado, Citrix Cloud asume que los tokens están obsoletos cuando comprueba su validez.

Descripción general de tareas

Para configurar la autenticación de Citrix Gateway, realice las siguientes tareas:

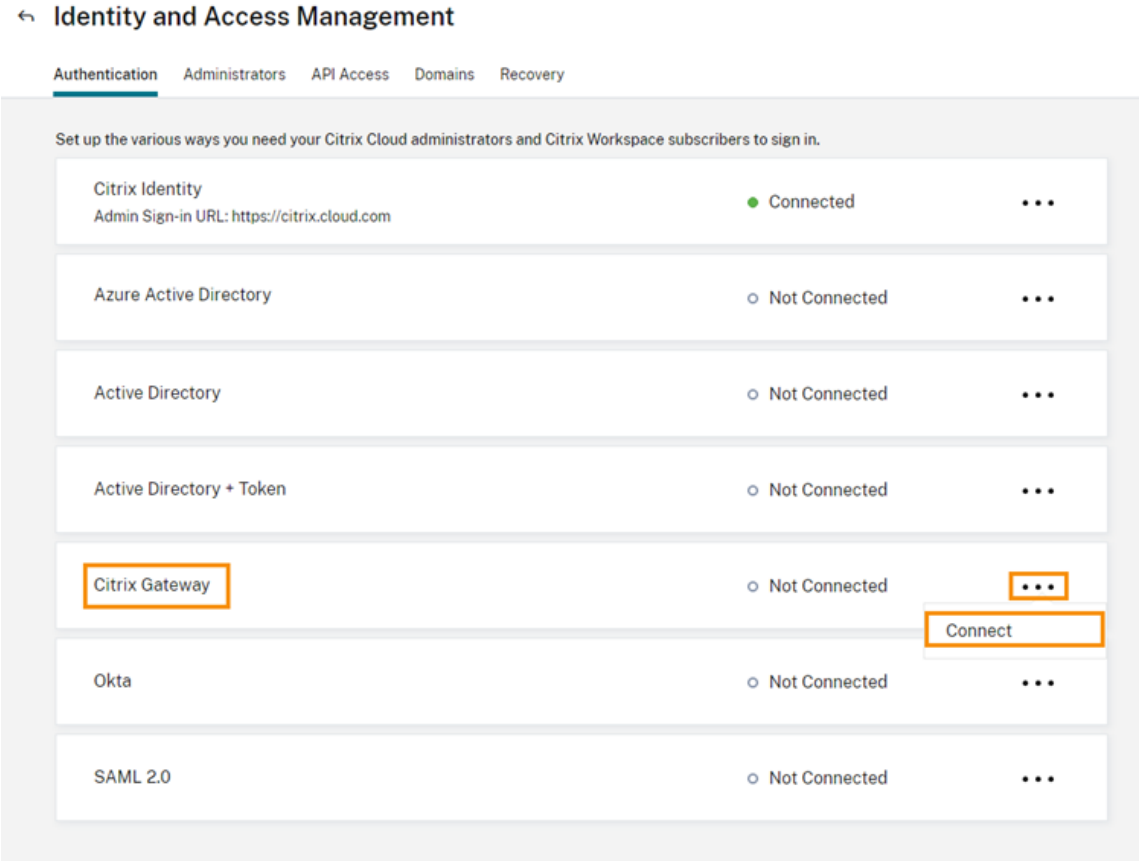
1. En **Administración de acceso e identidad**, comience a configurar la conexión con su dispositivo Gateway. En este paso, generará el ID de cliente, el secreto y la URL de redirección para el dispositivo Gateway.
2. En el dispositivo Gateway, cree una directiva avanzada de IdP de OAuth con la información generada desde Citrix Cloud. Esto permite que Citrix Cloud se conecte con el dispositivo Gateway local. Para obtener más instrucciones, consulte los siguientes artículos:

- Citrix Gateway 12.1: Usar un dispositivo Citrix Gateway local como el proveedor de identidades para Citrix Cloud
- Citrix Gateway 13.0: Usar un dispositivo Citrix Gateway local como el proveedor de identidades para Citrix Cloud

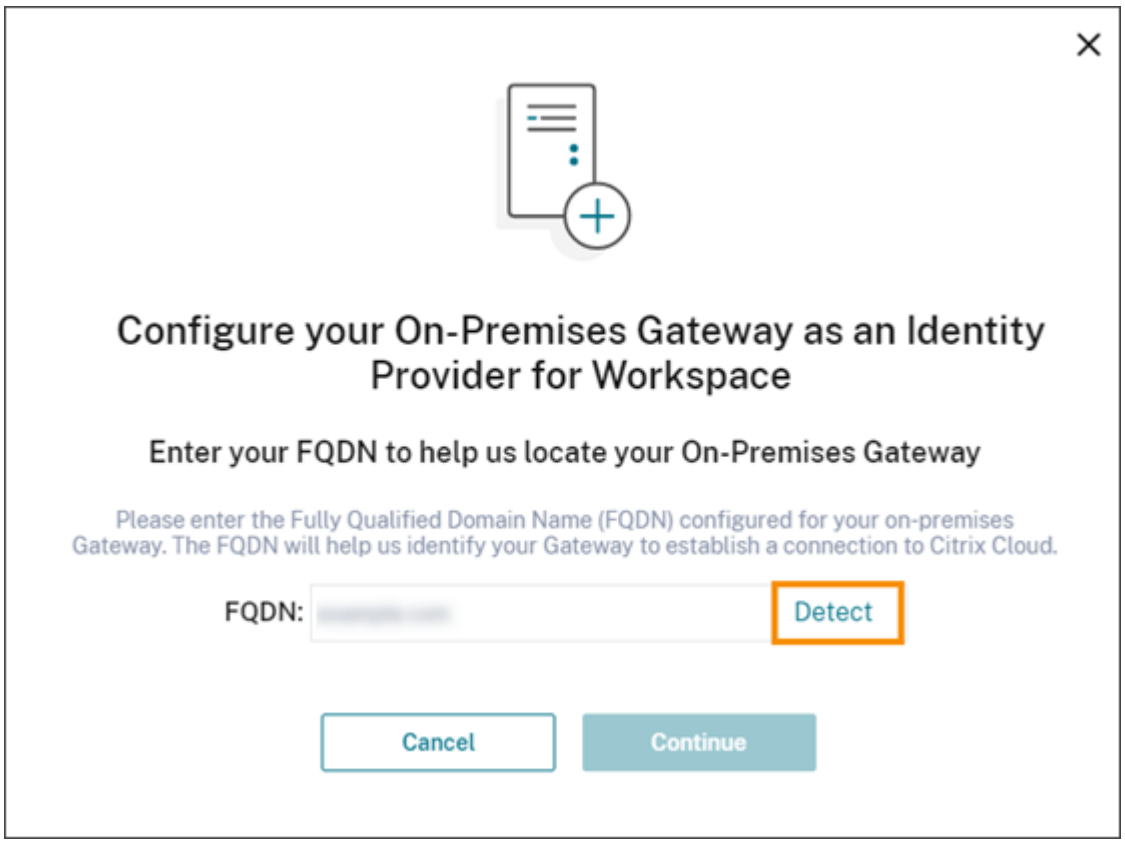
3. En **Configuración de Workspace**, habilite la autenticación de Citrix Gateway para los suscriptores.

Para habilitar la autenticación de Citrix Gateway para suscriptores de espacios de trabajo

1. Desde la consola de administración de Citrix Cloud, haga clic en el botón de menú y seleccione **Administración de acceso e identidad**.
2. En la ficha **Autenticación**, en **Citrix Gateway**, haga clic en el menú de puntos suspensivos y seleccione **Conectar**.



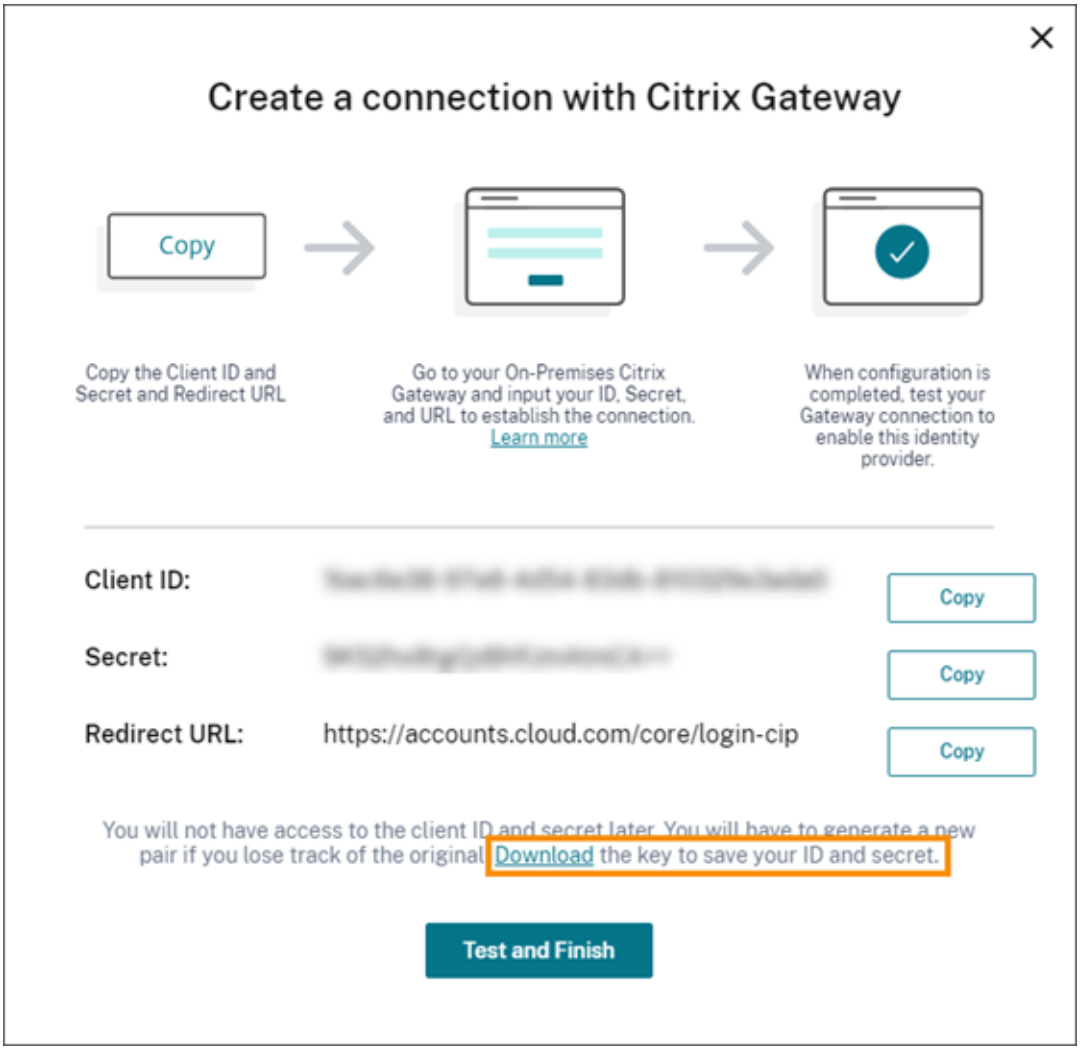
3. Introduzca el FQDN del dispositivo Gateway local y haga clic en **Detectar**.



Una vez que Citrix Cloud lo haya detectado correctamente, haga clic en **Continuar**.

4. Cree una conexión con el dispositivo Gateway local:

   a) Copie el ID de cliente, el secreto y la URL de redirección que muestra Citrix Cloud.



Igualmente, descargue una copia de esta información y guárdela de forma local y segura como referencia. Esta información no está disponible en Citrix Cloud una vez generada.

b) En el dispositivo Gateway, cree una directiva avanzada de IdP de OAuth. Utilice para ello el ID de cliente, el secreto y la URL de redirección provenientes de Citrix Cloud. Para obtener más instrucciones, consulte los siguientes artículos:

- Para Citrix Gateway 12.1: Usar un dispositivo Citrix Gateway local como el proveedor de identidades para Citrix Cloud
- Para Citrix Gateway 13.0: Usar un dispositivo Citrix Gateway local como el proveedor de identidades para Citrix Cloud

c) Haga clic en **Probar y finalizar**. Citrix Cloud verifica que el dispositivo Gateway sea accesible y esté configurado correctamente.

5. Habilite la autenticación de Citrix Gateway para los espacios de trabajo:

a) En el menú de Citrix Cloud, seleccione **Configuración de Workspace**.
b) En la ficha **Autenticación**, seleccione **Citrix Gateway**.

c) Seleccione **Comprendo los efectos en la experiencia de uso de los suscriptores** y, a continuación, haga clic en **Guardar**.

Solución de problemas

Como primer paso, revise las secciones Requisitos previos y Requisitos de este artículo. Compruebe que tiene todos los componentes necesarios en su entorno local y que ha realizado todas las configuraciones necesarias. Si falta alguno de estos elementos o no está configurado correctamente, no funcionará la autenticación del espacio de trabajo con Citrix Gateway.

Si sufre problemas al establecer una conexión entre Citrix Cloud y el dispositivo Gateway local, compruebe los siguientes puntos:

- El FQDN de Gateway es accesible desde Internet.
- Ha escrito correctamente el FQDN de Gateway en Citrix Cloud.
- Ha introducido correctamente la URL de Gateway en el parámetro `-issuer` de la directiva de IdP de OAuth. Ejemplo: `-issuer https://GatewayFQDN.com`. El parámetro `issuer` distingue entre mayúsculas y minúsculas.
- Los valores del ID de cliente, el secreto y la URL de redirección de Citrix Cloud se han escrito correctamente en los campos ID de cliente, Secreto de cliente, URL de redirección y Audiencia de la directiva de IdP de OAuth. Compruebe que se ha introducido el ID de cliente correcto en el campo Audiencia de la directiva.
- La directiva de autenticación de IdP de OAuth está configurada correctamente. Para obtener más instrucciones, consulte los siguientes artículos:
  - Citrix Gateway 12.1: Usar un dispositivo Citrix Gateway local como el proveedor de identidades para Citrix Cloud
  - Citrix Gateway 13.0: Usar un dispositivo Citrix Gateway local como el proveedor de identidades para Citrix Cloud
- Compruebe que la directiva está vinculada correctamente al servidor de autenticación AAA tal y como se describe en Binding Authentication Policies.

Servidores del catálogo global

Además de recuperar los detalles de la cuenta de usuario, Gateway recupera el nombre de dominio de los usuarios, el nombre NETBIOS de AD y el nombre de dominio raíz de AD. Para recuperar el nombre NETBIOS de AD, Gateway busca en el AD donde residen las cuentas de usuario. Los nombres NETBIOS no se replican en servidores del catálogo global.

Si utiliza servidores del catálogo global en su entorno de AD, las acciones LDAP configuradas en estos servidores no funcionan con Citrix Cloud. En su lugar, debe configurar los AD individuales en la acción

LDAP. Si tiene varios dominios o bosques, puede configurar varias directivas LDAP.

Búsqueda de AD para SSO con Kerberos o encadenamiento de IdP

Si utiliza Kerberos o un proveedor de identidades externo que utiliza protocolos SAML u OIDC para el inicio de sesión de los suscriptores, compruebe que la búsqueda de AD esté configurada. Gateway requiere búsquedas de AD para recuperar las propiedades de usuario de AD de los suscriptores y las propiedades de configuración de AD.

Compruebe que tiene directivas LDAP configuradas, incluso aunque la autenticación la lleven a cabo servidores de terceros. Para configurar estas directivas, agregue un segundo factor de autenticación al perfil del esquema de inicio de sesión existente mediante las siguientes tareas:

1. Cree un servidor de autenticación LDAP que solo extraiga atributos y grupos desde Active Directory.
2. Cree una directiva LDAP de autenticación avanzada.
3. Cree una etiqueta de directiva de autenticación.
4. Defina la etiqueta de directiva de autenticación como el factor siguiente, después del proveedor de identidades principal.

Para agregar LDAP como segundo factor de autenticación

1. Cree el servidor de autenticación LDAP:
    a) Seleccione **System > Authentication > Basic Policies > LDAP > Servers > Add**.
    b) En la página **Create Authentication LDAP Server**, introduzca la información siguiente:
        - En **Choose Server Type**, seleccione **LDAP**.
        - En **Name**, escriba un nombre descriptivo del servidor.
        - Seleccione **Server IP** y, a continuación, escriba la dirección IP del servidor LDAP.
        - En **Security Type**, seleccione el tipo de seguridad de LDAP requerido.
        - En **Server Type**, seleccione **AD**.
        - En **Autenticación**, no marque la casilla de verificación. Esta casilla de verificación debe desmarcarse porque este servidor de autenticación solo sirve para extraer grupos y atributos de usuarios de Active Directory, no para la autenticación.
    c) En **Other Settings**, introduzca la siguiente información:
        - En **Server Logon Name Attribute**, escriba **UserPrincipalName**.
        - En **Group Attribute**, seleccione **memberOf**.
        - En **Sub Attribute Name**, seleccione **cn**.
2. Cree la directiva LDAP de autenticación avanzada:

a) Seleccione **Security > AAA-Application Traffic > Policies > Authentication > Advanced Policies > Policy > Add**.
b) En la página **Create Authentication Policy**, introduzca la información siguiente:
   - En **Name**, escriba un nombre descriptivo de la directiva.
   - En **Action Type**, seleccione **LDAP**.
   - En **Action**, seleccione el servidor de autenticación LDAP que creó antes.
   - En **Expression**, escriba **TRUE**.
c) Haga clic en **Create** para guardar la configuración.

3. Cree la etiqueta de directiva de autenticación:

a) Seleccione **Security > AAA-Application Traffic > Policies > Authentication > Advanced Policies > Policy Label > Add**.
b) En **Name**, escriba un nombre descriptivo de la etiqueta de directiva de autenticación.
c) En Login Schema, seleccione **LSCHEMA_INT**.
d) En **Policy Binding**, en **Select Policy**, seleccione la directiva LDAP de autenticación avanzada que creó antes.
e) En **GoTo Expression**, seleccione **END**.
f) Haga clic en **Bind** para finalizar la configuración.

4. Defina la etiqueta de directiva de autenticación LDAP como el factor siguiente, después del proveedor de identidades principal.

a) Seleccione **System > Security > AAA-Application Traffic > Virtual Servers**.
b) Seleccione el servidor virtual que contiene el vínculo para su proveedor de identidades principal y seleccione **Edit**.
c) En **Advanced Authentication Policies**, seleccione los vínculos existentes en **Authentication Policy**.
d) Seleccione el vínculo para su proveedor de identidades principal y, a continuación, seleccione **Edit Binding**.
e) En la página **Policy Binding**, en **Select Next Factor**, seleccione la etiqueta de directiva de autenticación LDAP que creó antes.
f) Haga clic en **Bind** para guardar la configuración.

Contraseña predeterminada para la autenticación de varios factores

Si utiliza la autenticación de varios factores (MFA) para los suscriptores de espacios de trabajo, Gateway utiliza la contraseña del último factor como contraseña predeterminada para el inicio de sesión único. Esta contraseña se envía a Citrix Cloud cuando los suscriptores inician sesión en su espacio de trabajo. Si la autenticación LDAP va seguida de otro factor en el entorno, debe configurar la contraseña de LDAP como la contraseña predeterminada que se envía a Citrix Cloud. Habilite **SSOCredentials** en el esquema de inicio de sesión correspondiente al factor de LDAP.

Más información

Citrix Tech Zone: Tech Insight: Authentication - Gateway

Conectar Google Cloud Identity como proveedor de identidades con Citrix Cloud

October 2, 2023

Citrix Cloud admite el uso de Google Cloud Identity como proveedor de identidades para autenticar a los suscriptores que inician sesión en sus espacios de trabajo. Tras conectar la cuenta de Google de su organización a Citrix Cloud, puede ofrecer una experiencia de inicio de sesión unificada para acceder a recursos de Citrix Workspace y Google.

Requisitos para la configuración con unión a un dominio y sin unión a ningún dominio

Puede configurar Google Cloud Identity como proveedor de identidades en Citrix Cloud mediante una máquina que esté unida a un dominio o no.

- Unidas a un dominio significa que las máquinas están unidas a un dominio en su instancia de Active Directory (AD) local y la autenticación utiliza los perfiles de usuario que están almacenados allí.
- No unidas a ningún dominio significa que las máquinas no están unidas a un dominio de AD y la autenticación usa los perfiles de usuario que están almacenados en su directorio de Google Workspace (también conocidos como usuarios nativos de Google).

En la tabla siguiente se enumeran los requisitos de cada tipo de configuración.

Requisito	Unido a un dominio	No unida a ningún dominio	Más información
AD local	Sí	No	Consulte Preparar Active Directory y Citrix Cloud Connectors en este artículo.

Requisito	Unido a un dominio	No unida a ningún dominio	Más información
Citrix Cloud Connectors implementados en su ubicación de recursos	Sí	No; los Cloud Connectors no son necesarios para acceder a las máquinas que no están unidas a ningún dominio.	Preparar Active Directory y Citrix Cloud Connectors en este artículo.
Sincronización de AD con Google Cloud	Opcional solo si se usa Gateway Service y no otros servicios. De lo contrario, esta tarea es obligatoria.	No	Consulte Sincronizar Active Directory con Google Cloud Identity en este artículo.
Cuenta de desarrollador con acceso a la consola de Google Cloud Platform. Se utiliza para crear una cuenta de servicio y una clave, y para habilitar la API del SDK de administración.	Sí	Sí	Consulte Crear una cuenta de servicio, Crear una clave de cuenta de servicio y Configurar la delegación en todo el dominio en este artículo.
Una cuenta de administrador con acceso a la consola de administración de Google Workspace. Se utiliza para configurar la delegación en todo el dominio y una cuenta de usuario de API de solo lectura.	Sí	Sí	Consulte Configurar la delegación en todo el dominio y Agregar una cuenta de usuario de API de solo lectura en este artículo.

Autenticación con varias cuentas de Citrix Cloud

En este artículo se describe cómo conectar Google Cloud Identity como un proveedor de identidades con una sola cuenta de Citrix Cloud. Si tiene varias cuentas de Citrix Cloud, puede conectar cada

una a la misma cuenta de Google Cloud mediante la misma cuenta de servicio y la misma cuenta de usuario de API de solo lectura. Simplemente inicie sesión en Citrix Cloud y seleccione el ID de cliente correspondiente en el selector de clientes.

Preparar Active Directory y Citrix Cloud Connectors

Si utiliza una máquina **unida a un dominio** con Google Cloud Identity, use esta sección para preparar la instancia de AD local. Si usa una máquina que no está unida a un dominio, omita esta tarea y continúe con Crear una cuenta de servicio en este artículo.

Necesita al menos dos (2) servidores en su dominio de Active Directory en los que instalar el software de Citrix Cloud Connector. Los Cloud Connectors son necesarios para permitir la comunicación entre Citrix Cloud y su ubicación de recursos. Se requieren al menos dos Cloud Connectors para garantizar una conexión de alta disponibilidad con Citrix Cloud. Estos servidores deben cumplir los siguientes requisitos:

- Cumplir los requisitos descritos en los Detalles técnicos de Cloud Connector.
- No tener ningún otro componente de Citrix instalado, no ser un controlador de dominio de Active Directory ni ser cualquier otra máquina de importancia crítica para la infraestructura de la ubicación de recursos.
- Está unido al dominio de Active Directory (AD). Si los recursos y los usuarios del espacio de trabajo residen en varios dominios, debe instalar al menos dos Cloud Connectors en cada dominio. Para obtener más información, consulte Casos de implementación para Cloud Connectors en Active Directory.
- Conectado a una red que puede establecer contacto con los recursos a los que acceden los usuarios a través de Citrix Workspace.
- Debe estar conectada a Internet. Para obtener más información, consulte Requisitos del sistema y de conectividad.

Para obtener más información sobre la instalación de Cloud Connectors, consulte Instalar Cloud Connector.

Sincronizar Active Directory con Google Cloud Identity

Si utiliza una máquina **unida a un dominio** con Google Cloud Identity, use esta sección para preparar la instancia de AD local. Si usa una máquina que no está unida a un dominio, omita esta tarea y continúe con Crear una cuenta de servicio en este artículo.

La sincronización de su AD con Google Cloud Identity es opcional si solo usa Citrix Gateway Service sin ningún otro servicio habilitado. Solo para estos servicios, puede usar usuarios nativos de Google sin necesidad de sincronizarlos con su AD.

Si utiliza otros servicios de Citrix Cloud, es necesario sincronizar su AD con Google Cloud Identity. Google Cloud debe pasar estos atributos de usuario de AD a Citrix Cloud:

- SecurityIDentifier (SID)
- objectGUID
- userPrincipalName (UPN)

Para sincronizar AD con Google Cloud

1. Descargue e instale la utilidad Google Cloud Directory Sync del sitio web de Google. Para obtener más información sobre esta utilidad, consulte la documentación de Google Cloud Directory Sync en el sitio web de Google.
2. Después de instalar la utilidad, inicie Configuration Manager (**Inicio > Configuration Manager**).
3. Especifique los parámetros del dominio de Google y los parámetros de LDAP tal y como se describe en Definir la sincronización con el gestor de configuración de la documentación de la utilidad.
4. En **General Settings**, seleccione **Custom Schemas**. No cambie las selecciones predeterminadas.
5. Configure un esquema personalizado para aplicarlo a todas las cuentas de usuario. Introduzca la información necesaria con el formato y la ortografía exactos que se especifican en esta sección.

    a) Seleccione la ficha **Custom Schemas** y, a continuación, seleccione **Add Schema**.
    b) Seleccione **Use rules defined in "User Accounts"**.
    c) En **Schema Name**, escriba **citrix-schema**.
    d) Seleccione **Add Field** y, a continuación, introduzca esta información:
        - Dentro de **Schema field template**, en **Schema Field**, seleccione **userPrincipalName**.
        - Dentro de **Google field details**, en **Field Name**, introduzca **UPN**.
    e) Repita el paso 4 para crear estos campos:
        - objectGUID: En **Schema field template**, seleccione **objectGUID**. En **Google field details**, introduzca **objectGUID**.
        - SID: En **Schema field template**, seleccione **Custom**. En **Google field details**, introduzca **SID**.
        - objectSID: En **Schema field template**, seleccione **Custom**. En **Google field details**, introduzca **objectSID**.
    f) Seleccione **OK** para guardar las entradas.

6. Termine de configurar los parámetros restantes de su organización y verifique los parámetros de sincronización tal y como se describe en Definir la sincronización con el gestor de configuración de la documentación de la utilidad.

7. Seleccione **Sync & apply changes** para sincronizar su Active Directory con su cuenta de Google.

Una vez finalizada la sincronización, la sección User Information de Google Cloud muestra la información de Active Directory de los usuarios.

Crear una cuenta de servicio

Para completar esta tarea, necesita una cuenta de desarrollador de Google Cloud Platform.

1. Inicie sesión en https://console.cloud.google.com.
2. En la barra lateral del panel, seleccione **IAM & Admin** y, a continuación, seleccione **Service Accounts**.
3. Seleccione **Create service account**.
4. En **Service account details**, introduzca el nombre y el ID de la cuenta de servicio.
5. Seleccione **Listo**.

Crear una clave de cuenta de servicio

1. En la página **Service Accounts**, seleccione la cuenta de servicio que acaba de crear.
2. Seleccione la ficha **Keys** y, a continuación, seleccione **Add key > Create new key**.
3. Deje seleccionada la opción predeterminada de tipo de clave JSON.
4. Seleccione **Crear**. Guarde la clave en una ubicación segura a la que pueda acceder más adelante. La clave privada se introduce en la consola de Citrix Cloud cuando se conecta a Google Cloud Identity como proveedor de identidades.

Configurar la delegación en todo el dominio

1. Habilite la API del SDK de administración:
    a) En el menú de Google Cloud Platform, seleccione **APIs & Services > Enabled APIs & services**.
    b) Seleccione **Enable APIs and services** cerca de la parte superior de la consola. Aparecerá la página de inicio de la biblioteca de API.
    c) Busque **Admin SDK API** y selecciónela en la lista de resultados.
    d) Seleccione **Enable**.
2. Cree un cliente de API para la cuenta de servicio:
    a) En el menú de Google Cloud Platform, seleccione **IAM & Admin > Service Accounts** y, a continuación, seleccione la cuenta de servicio que creó antes.
    b) En la ficha **Details** de la cuenta de servicio, expanda **Advanced settings**.

c) En **Domain-wide Delegation**, copie el ID de cliente y seleccione **View Google Workspace Admin Console**.

d) Si hace falta, seleccione la cuenta de administrador de Google Workspace que quiera usar. Aparecerá la consola de administración de Google.

e) En la barra lateral de la administración de Google, seleccione **Security > Access and data control > API controls**.

f) En **Domain wide delegation**, haga clic en **Manage Domain Wide Delegation**.

g) Seleccione **Add new**.

h) En **Client ID**, pegue el ID de cliente de la cuenta de servicio que copió en el paso C.

i) En **OAuth scopes**, introduzca estos ámbitos en una línea delimitada por comas:

```
https://www.googleapis.com/auth/admin.directory.user.readonly,
    https://www.googleapis.com/auth/admin.directory.group.
    readonly,https://www.googleapis.com/auth/admin.directory.
    domain.readonly
<!--NeedCopy-->
```

j) Seleccione **Authorize**.

Agregar una cuenta de usuario de API de solo lectura

En esta tarea, creará una cuenta de usuario de Google Workspace con acceso a API de solo lectura para Citrix Cloud. Esta cuenta no se usa para ningún otro propósito y no tiene otros privilegios.

1. En el menú de la administración de Google, seleccione **Directory > Users**.
2. Seleccione **Add new user** e introduzca la información de usuario correspondiente.
3. Seleccione **Add new user** para guardar la información de la cuenta.
4. Cree un rol personalizado para la cuenta de usuario de solo lectura:

   a) En el menú de la administración de Google, seleccione **Account > Admin roles**.

   b) Seleccione **Create new role**.

   c) Introduzca un nombre para el nuevo rol. Ejemplo: API-ReadOnly

   d) Seleccione **Continue**.

   e) En **Admin API privileges**, seleccione estos privilegios:

   - Users > Read
   - Groups > Read
   - Domain Management

   f) Seleccione **Continue** y, a continuación, seleccione **Create role**.

5. Asigne el rol personalizado a la cuenta de usuario de solo lectura que creó antes:

   a) En la página de detalles del rol personalizado, en el panel **Admins**, seleccione **Assign users**.

b) Comience a escribir el nombre de la cuenta de usuario de solo lectura y selecciónelo en la lista de usuarios.
c) Seleccione **Assign role**.
d) Para comprobar la asignación de roles, regrese a la página Users (**Directory > Users**) y seleccione la cuenta de usuario de solo lectura. La asignación de roles personalizados se muestra en **Admin roles and privileges**.

Conectar Google Cloud Identity con Citrix Cloud

1. Inicie sesión en Citrix Cloud en https://citrix.cloud.com.
2. Desde la consola de administración de Citrix Cloud, haga clic en el botón de menú y seleccione **Administración de acceso e identidad**.
3. Busque **Google Cloud Identity** y seleccione **Conectar** en el menú de puntos suspensivos.
4. Cuando se le solicite, introduzca un identificador breve y fácil de usar para la URL de su empresa y seleccione **Guardar y continuar**. El identificador que elija debe ser único a nivel global dentro de Citrix Cloud.
5. Seleccione **Importar archivo** y, a continuación, seleccione el archivo JSON que guardó al crear la clave de la cuenta de servicio. Esta acción importa su clave privada y la dirección de correo electrónico de la cuenta de servicio de Google Cloud que creó.
6. En **Usuario suplantado**, introduzca el nombre de la cuenta de usuario de API de solo lectura.
7. Seleccione **Next**. Citrix Cloud verifica los detalles de su cuenta de Google y prueba la conexión.
8. Revise los dominios asociados que aparecen en la lista. Si son correctos, seleccione **Confirmar** para guardar la configuración.

Agregar administradores a Citrix Cloud

Puede agregar administradores y grupos de administradores individuales de Citrix Cloud a través de Google Cloud. Para obtener más información, consulte estos artículos:

- Para administradores individuales: Administrar el acceso de administrador a Citrix Cloud
- Para grupos de administradores: Administrar grupos de administradores

Después de agregar administradores a Citrix Cloud, pueden iniciar sesión mediante uno de estos métodos:

- Vaya a la URL de inicio de sesión de administradores que configuró cuando definió inicialmente Google Cloud como un proveedor de identidades. Ejemplo:`https://citrix.cloud.com/go/mycompany`
- En la página de inicio de sesión de Citrix Cloud, seleccione **Iniciar sesión con mis credenciales de empresa**, introduzca el identificador único de su empresa (por ejemplo, “miempresa”) y haga clic en **Continuar**.

Habilitar la autenticación con Google Cloud Identity para espacios de trabajo

1. En el menú de Citrix Cloud, seleccione **Configuración de Workspace > Autenticación**.
2. Seleccione **Google Cloud Identity**. Cuando se le solicite, seleccione **Comprendo los efectos en la experiencia de uso de los suscriptores** y haga clic en **Guardar**.

Conectar Okta como proveedor de identidades con Citrix Cloud

July 2, 2024

Citrix Cloud admite el uso de Okta como proveedor de identidades para autenticar a los suscriptores que inician sesión en sus espacios de trabajo. Tras conectar su organización de Okta a Citrix Cloud, puede ofrecer una experiencia de inicio de sesión común para que sus suscriptores accedan a los recursos de Citrix Workspace.

Después de habilitar la autenticación con Okta en Configuración de Workspace, los suscriptores tienen una experiencia de inicio de sesión diferente. La selección de la autenticación de Okta ofrece un inicio de sesión federado, no Single Sign-On. Los suscriptores inician sesión en el espacio de trabajo desde una página de inicio de sesión de Okta, pero es posible que deban autenticarse una segunda vez al abrir una aplicación o escritorio desde Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops). Para habilitar Single Sign-On y evitar un segundo mensaje de inicio de sesión, debe usar el Servicio de autenticación federada de Citrix con Citrix Cloud. Para obtener más información, consulte Conectar el Servicio de autenticación federada de Citrix con Citrix Cloud.

Requisitos previos

Cloud Connectors o Connector Appliances

Los Cloud Connectors o los Connector Appliances son necesarios para permitir la comunicación entre Citrix Cloud y su ubicación de recursos. Se requieren al menos dos Cloud Connectors o Connector Appliances para garantizar una conexión de alta disponibilidad con Citrix Cloud. Necesita al menos dos Connectors unidos a su dominio de Active Directory. Pueden ser Cloud Connectorso Connector Appliances.

Los conectores deben cumplir estos requisitos:

- Cumplir con los requisitos descritos en su documentación respectiva
- Está unido al dominio de Active Directory (AD). Si los usuarios de su espacio de trabajo residen en varios dominios, la función de varios dominios de los Connector Appliances se puede usar para unir varios dominios.

- Conectado a una red que puede establecer contacto con los recursos a los que acceden los usuarios a través de Citrix Workspace.
- Debe estar conectada a Internet. Para obtener más información, consulte Requisitos del sistema y de conectividad.

Para obtener más información sobre la instalación de Cloud Connectors, consulte Instalar Cloud Connector.
Para obtener más información sobre la instalación de Connector Appliances, consulte Instalación de Connector Appliances.

Dominio Okta

Al conectar Okta a Citrix Cloud, debe proporcionar el dominio Okta de la organización. Citrix admite los siguientes dominios Okta:

- okta.com
- okta-eu.com
- oktapreview.com

También puede usar dominios personalizados de Okta con Citrix Cloud. Revise las consideraciones importantes para el uso de dominios personalizados en Customize the Okta URL domain, en el sitio web de Okta.

Para obtener más información acerca de cómo localizar el dominio personalizado de la organización, consulte Finding Your Okta Domain en el sitio web de Okta.

Aplicación web OIDC de Okta

Para usar Okta como proveedor de identidades, debe crear una aplicación web OIDC de Okta con credenciales de cliente que pueda usar con Citrix Cloud. Después de crear y configurar la aplicación, anote el ID de cliente y el secreto de cliente. Proporcione estos valores a Citrix Cloud cuando conecte su organización de Okta.

Para crear y configurar esta aplicación, consulte las siguientes secciones de este artículo:

- Crear una integración de aplicación web OIDC de Okta
- Configurar la aplicación web OIDC de Okta

URL del espacio de trabajo

Al crear la aplicación Okta, debe proporcionar la URL del espacio de trabajo desde Citrix Cloud. Para localizar la URL del espacio de trabajo, seleccione **Configuración de Workspace** en el menú Citrix Cloud. La dirección URL del espacio de trabajo se muestra en la ficha **Acceso**.

> **Importante:**
>
> Si modifica la URL del espacio de trabajo más adelante, deberá actualizar la configuración de la aplicación Okta con la nueva URL. De lo contrario, los suscriptores podrían tener problemas al cerrar sesión en sus espacios de trabajo.

Token de API de Okta

El uso de Okta como proveedor de identidades con Citrix Cloud requiere un token de API para su organización de Okta. Cree este token mediante una cuenta de administrador de solo lectura en su organización de Okta. Este token debe poder leer los usuarios y grupos de su organización de Okta.

Para crear el token de API, consulte Crear un token de API de Okta en este artículo. Para obtener más información acerca de los tokens de API, consulte Create an API token en el sitio web de Okta.

> **Importante:**
>
> Al crear el token de API, tome nota del valor del token (por ejemplo, copie el valor temporalmente en un documento de texto sin formato). Okta muestra este valor solo una vez, por lo que puede crear el token justo antes de realizar los pasos descritos en Conectar Citrix Cloud con su organización de Okta.

Sincronizar cuentas con el agente de AD de Okta

Para usar Okta como proveedor de identidades, primero debe integrar su AD local con Okta. Para ello, instale el agente de AD para Okta en su dominio y agregue su AD a su organización de Okta. Para obtener instrucciones sobre la implementación del agente de AD para Okta, consulte Get started with Active Directory integration en el sitio web de Okta.

Después, importe los usuarios y grupos de AD a Okta. Al importar, incluya estos valores asociados a sus cuentas de AD:

- Correo electrónico
- SID
- UPN
- OID

> Nota:
>
> Si utiliza el servicio Citrix Gateway con Workspace, no necesita sincronizar sus cuentas de AD con su organización de Okta.

Para sincronizar los usuarios y grupos de AD con la organización de Okta:

1. Instale y configure el agente de AD para Okta. Para obtener instrucciones completas, consulte los siguientes artículos en el sitio web de Okta:
   - Instalar el agente de Active Directory para Okta
   - Configurar la importación y los parámetros de la cuenta de Active Directory
   - Configurar las opciones de aprovisionamiento de Active Directory
2. Agregue sus usuarios y grupos de AD a Okta realizando una importación manual o una importación automatizada. Para obtener más información sobre los métodos e instrucciones de importación de Okta, consulte Manage Active Directory users and groups en el sitio web de Okta.

Crear una integración de aplicación web OIDC de Okta

1. En la consola de administración de Okta, en **Applications**, seleccione **Applications**.
2. Seleccione **Create App Integration**.
3. En **Sign in method**, seleccione **OIDC - OpenID Connect**.
4. En **Application type**, seleccione **Web Application**. Seleccione **Siguiente**.
5. En **App Integration Name**, introduzca un nombre descriptivo para la integración de aplicaciones.
6. En **Tipo de concesión**, seleccione **Código de autorización** (seleccionado de forma predeterminada).
7. En **Sign-in redirect URIs**, introduzca `https://accounts.cloud.com/core/login-okta`.
8. En **Sign-out redirect URIs**, introduzca la URL de Workspace de Citrix Cloud.
9. En **Assignments**, en **Controlled access**, seleccione si quiere asignar la integración de aplicaciones a todos los miembros de su organización, solo a los grupos que especifique, o si prefiere asignar el acceso más adelante.
10. Seleccione **Guardar**. Tras guardar la integración de la aplicación, la consola muestra la página de configuración de la aplicación.
11. En la sección **Client Credentials**, copie los valores de **Client ID** y **Client Secret**. Proporcione estos valores cuando conecte Citrix Cloud con su organización de Okta.

Configurar la aplicación web OIDC de Okta

En este paso, configurará su aplicación web OIDC de Okta con los parámetros necesarios para Citrix Cloud. Citrix Cloud requiere estos parámetros para autenticar a sus suscriptores a través de Okta cuando inician sesión en sus espacios de trabajo.

1. (Opcional) Actualice los permisos del cliente para el tipo de concesión implícita. Puede optar por realizar este paso si prefiere conceder la cantidad mínima de privilegios para este tipo de

concesión.

a) En la página de configuración de la aplicación Okta, en la ficha **General**, vaya a la sección **General Settings** y seleccione **Edit**.
b) En la sección **Application**, en **Grant type**, en **Client acting on behalf of a user**, borre el parámetro **Allow Access Token with implicit grant type**.
c) Seleccione **Guardar**.

2. Agregue atributos de aplicación. Los atributos distinguen mayúsculas y minúsculas.

a) En el menú de la consola de Okta, seleccione **Directory > Profile Editor**.
b) Seleccione el perfil **User (default)** de Okta. Okta muestra la página del perfil **User**.
c) En **Attributes**, seleccione **Add attribute**.
d) Introduzca la siguiente información:
   - Display Name: cip_email
   - Variable Name: cip_email
   - Description: Dirección de correo electrónico del usuario de AD
   - Longitud del atributo: Seleccione **Mayor que** y, a continuación, introduzca **1**.
   - Attribute Required: Yes
e) Seleccione **Save and Add Another**.
f) Introduzca la siguiente información:
   - Display Name: cip_sid
   - Variable Name: cip_sid
   - Description: Identificador de seguridad de usuario de AD
   - Longitud del atributo: Seleccione **Mayor que** y, a continuación, introduzca **1**.
   - Attribute Required: Yes
g) Seleccione **Save and Add Another**.
h) Introduzca la siguiente información:
   - Display Name: cip_upn
   - Variable Name: cip_upn
   - Description: Nombre principal de usuario de AD
   - Longitud del atributo: Seleccione **Mayor que** y, a continuación, introduzca **1**.
   - Attribute Required: Yes
i) Seleccione **Save and Add Another**.
j) Introduzca la siguiente información:
   - Display Name: cip_oid
   - Variable Name: cip_oid
   - Description: GUID de usuario de AD
   - Longitud del atributo: Seleccione **Mayor que** y, a continuación, introduzca **1**.
   - Attribute Required: Yes

k) Seleccione **Guardar**.

3. Modifique las asignaciones de atributos de la aplicación:

   a) En la consola de Okta, seleccione **Directory > Profile Editor**.
   b) Busque el perfil **active_directory** de su AD. Es posible que este perfil se etiquete con el formato `myDomain User`, donde `myDomain` es el nombre de su dominio de AD integrado.
   c) Seleccione **Mappings**. Aparece la página User Profile Mappings de su dominio de AD, y se selecciona la ficha para asignar su AD al usuario de Okta.
   d) En la columna **Okta User Profile**, busque los atributos que creó en el paso 2 y asígnelos de esta manera:
      - Para `cip_email`, seleccione `email` en la columna Perfil de usuario de su dominio. Al seleccionarse, la asignación aparece como `appuser.email`.
      - Para `cip_sid`, seleccione `objectSid` en la columna Perfil de usuario de su dominio. Al seleccionarse, la asignación aparece como `appuser.objectSid`.
      - Para `cip_upn`, seleccione `userName` en la columna Perfil de usuario de su dominio. Al seleccionarse, la asignación aparece como `appuser.userName`.
      - Para `cip_oid`, seleccione `externalId` en la columna Perfil de usuario de su dominio. Al seleccionarse, la asignación aparece como `appuser.externalId`.
   e) Seleccione **Save Mappings**.
   f) Seleccione **Apply updates now**. Okta inicia una tarea para aplicar las asignaciones.
   g) Sincronice Okta con su AD.
      i. En la consola de Okta, seleccione **Directory > Directory Integrations**.
      ii. Seleccione tu AD integrado.
      iii. Seleccione la ficha **Provisioning** .
      iv. En **Settings**, seleccione **To Okta**.
      v. Vaya a la sección **Okta Attribute Mappings** y, a continuación, seleccione **Force Sync**.

Crear un token de API de Okta

1. Inicie sesión en la consola de Okta con una cuenta de administrador de solo lectura.
2. En el menú de la consola de Okta, seleccione **Security > API**.
3. Seleccione la ficha **Tokens** y, a continuación, seleccione **Create Token**.
4. Introduzca un nombre para el token.
5. Seleccione **Create Token**.
6. Copie el valor del token. Este valor se proporciona al conectar su organización de Okta con Citrix Cloud.

Conectar Citrix Cloud con su organización de Okta

1. Inicie sesión en Citrix Cloud en https://citrix.cloud.com.
2. Desde la consola de administración de Citrix Cloud, haga clic en el botón de menú y seleccione **Administración de acceso e identidad**.
3. Ubique **Okta** y seleccione **Conectar** en el menú de tres puntos.
4. En **URL de Okta**, introduzca su dominio de Okta.
5. En **Token de API de Okta**, introduzca el token de API de su organización de Okta.
6. En **ID de cliente** y **Secreto del cliente**, introduzca el ID y el secreto del cliente de la integración de la aplicación web OIDC que creó antes. Para copiar estos valores de la consola de Okta, seleccione **Aplicaciones** y busque su aplicación de Okta. En **Credenciales del cliente**, utilice el botón **Copiar al portapapeles** para cada valor.
7. Haga clic en **Probar y finalizar**. Citrix Cloud verifica los detalles de Okta y prueba la conexión.

Una vez que la conexión se haya verificado correctamente, puede habilitar la autenticación de Okta para los suscriptores de espacios de trabajo.

Habilitar la autenticación con Okta para espacios de trabajo

1. En el menú de Citrix Cloud, seleccione **Configuración de Workspace > Autenticación**.
2. Seleccione **Okta**.
3. Cuando se le solicite, seleccione **Comprendo los efectos en la experiencia de uso de los suscriptores**.
4. Seleccione **Guardar**.

Tras cambiar a la autenticación de Okta, Citrix Cloud inhabilita temporalmente los espacios de trabajo durante unos minutos. Cuando se habilitan de nuevo los espacios de trabajo, sus suscriptores podrán iniciar sesión con Okta.

Más información

- Citrix Tech Zone:
  - Tech Insight: Authentication - Okta
  - Resumen técnico: Identidad del espacio de trabajo
  - Tech Brief: Workspace SSO

Conectar SAML como proveedor de identidades con Citrix Cloud

July 2, 2024

Citrix Cloud admite el uso de SAML (Lenguaje de marcado de aserción de seguridad) como proveedor de identidades para autenticar a los administradores de Citrix Cloud y a los suscriptores que inician sesión en sus espacios de trabajo. Con su instancia de Active Directory (AD) local, puede usar el proveedor SAML 2.0 que prefiera.

Acerca de este artículo

En este artículo se describen los pasos necesarios para configurar una conexión entre Citrix Cloud y su proveedor SAML. En algunos de estos pasos, se describen las acciones que debe realizar en la consola de administración del proveedor SAML. Los comandos específicos que utilice para realizar estas acciones pueden ser distintos de los descritos en este artículo, dependiendo del proveedor SAML elegido. Estos comandos de proveedor SAML se proporcionan únicamente a efectos de ejemplo. Consulte la documentación de su proveedor SAML para obtener más información sobre los comandos correspondientes.

Configuraciones de proveedor SAML

Citrix proporciona las siguientes guías de configuración para garantizar que su proveedor SAML interactúe sin problemas con Citrix Cloud:

- SAML con Active Directory Federated Services (ADFS): Consulte Configurar la autenticación SAML en Citrix Cloud mediante ADFS.
- SAML con identidades de Azure Active Directory: Consulte Iniciar sesión en espacios de trabajo con SAML mediante identidades de Azure Active Directory.
- Aplicación Citrix Cloud SAML SSO para Azure AD: Consulte Tutorial: Azure Active Directory single sign-on (SSO) integration with Citrix Cloud SAML SSO en el sitio web de documentación de la aplicación de Microsoft Azure AD.
- SAML con dominios personalizados de Citrix Workspace: Consulte Iniciar sesión en espacios de trabajo con SAML mediante dominios personalizados
- SAML con Okta: Consulte Configurar Okta como proveedor SAML para la autenticación de espacios de trabajo

Proveedores de SAML compatibles

Los proveedores de SAML que admiten la especificación oficial de SAML 2.0 son compatibles con Citrix Cloud.

Citrix ha probado estos proveedores de SAML para autenticar a administradores de Citrix Cloud y a suscriptores de Citrix Workspace mediante Single Sign-On (SSO) y Single Logout (SLO). También se admiten proveedores de SAML que no aparecen en esta lista.

- Microsoft ADFS
- Microsoft Azure AD
- Duo
- Okta
- OneLogin
- PingOne SSO
- PingFederate

Al probar estos proveedores, Citrix utilizó estos parámetros para configurar la conexión SAML en la consola de Citrix Cloud:

- Mecanismo de enlace: HTTP Post
- Respuesta SAML: Firmar respuesta o aserción
- Contexto de autenticación: Sin especificar, Exacto

Los valores de estos parámetros se configuran de forma predeterminada al configurar la conexión SAML en Citrix Cloud. Citrix recomienda usar estos parámetros al configurar la conexión con el proveedor de SAML que elija.

Para obtener más información sobre estos parámetros, consulte Agregar metadatos de proveedores de SAML a Citrix Cloud en este artículo.

Compatibilidad con identificadores de entidad con ámbito

En este artículo se describe cómo configurar la autenticación SAML mediante una única aplicación SAML y el ID de entidad genérico predeterminado de Citrix Cloud.

Si sus requisitos de autenticación SAML incluyen la necesidad de varias aplicaciones SAML en un único proveedor de SAML, consulte Configurar una aplicación SAML mediante un ID de entidad con ámbito en Citrix Cloud.

Requisitos previos

El uso de la autenticación SAML con Citrix Cloud presenta los siguientes requisitos:

- Proveedor SAML compatible con SAML 2.0.
- Dominio de AD local.
- Dos Cloud Connectors implementados en una ubicación de recursos y unidos al dominio de AD local. Los Cloud Connectors se utilizan para garantizar que Citrix Cloud pueda comunicarse con su ubicación de recursos.
- Integración de AD con su proveedor SAML.

Cloud Connectors

Necesita al menos dos (2) servidores donde instalar el software Citrix Cloud Connector. Citrix recomienda al menos dos servidores para la alta disponibilidad de Cloud Connector. Estos servidores deben cumplir los siguientes requisitos:

- Cumplir los requisitos del sistema descritos en los Detalles técnicos de Cloud Connector.
- No tener ningún otro componente de Citrix instalado, no ser un controlador de dominio de AD ni ser cualquier otra máquina de importancia crítica para la infraestructura de la ubicación de recursos.
- Estar unidos al dominio donde residen los recursos. Si los usuarios acceden a los recursos en varios dominios, debe instalar al menos dos Cloud Connectors en cada dominio.
- Estar conectados a una red que puede establecer contacto con los recursos a los que acceden los usuarios a través de Citrix Workspace.
- Debe estar conectada a Internet. Para obtener más información, consulte Requisitos del sistema y de conectividad.

Para obtener más información sobre la instalación de Cloud Connector, consulte Instalar Cloud Connector.

Active Directory

Antes de configurar la autenticación SAML, realice las siguientes tareas:

- Verifique que sus suscriptores de Workspace tengan cuentas de usuario en su AD. Los suscriptores sin cuentas de AD no pueden iniciar sesión en sus espacios de trabajo correctamente cuando se configura la autenticación SAML.
- Implemente Cloud Connectors en su instancia de AD local para conectar AD a su cuenta de Citrix Cloud.
- Sincronice los usuarios de AD con el proveedor SAML. Citrix Cloud necesita los atributos de usuario de AD para los suscriptores de espacios de trabajo para que puedan iniciar sesión correctamente.

Atributos de usuario de AD Estos atributos son obligatorios para todos los objetos de usuario de Active Directory, y deben rellenarse:

- Nombre común
- Nombre de cuenta SAM
- Nombre principal de usuario (UPN)
- GUID de objeto
- SID

Citrix Cloud usa los atributos Object GUID y SID de su AD para establecer el contexto de usuario cuando los suscriptores inician sesión en Citrix Workspace. Si algunas de estas propiedades no está rellenada, los suscriptores no pueden iniciar sesión.

Estos atributos no son necesarios para usar la autenticación SAML con Citrix Cloud, pero Citrix recomienda rellenarlos para garantizar una experiencia de usuario óptima:

- Dirección de correo electrónico
- Display Name

Citrix Cloud usa el atributo Display Name para mostrar correctamente los nombres de los suscriptores en Citrix Workspace. Si este atributo no está rellenado, los suscriptores pueden iniciar sesión igualmente, pero es posible que sus nombres no se muestren como es debido.

Integración de SAML con Active Directory

Antes de habilitar la autenticación SAML, debe integrar su AD local con su proveedor SAML. Esta integración permite al proveedor SAML pasar los siguientes atributos de usuario de AD requeridos a Citrix Cloud en la aserción SAML:

- objectSID (SID)
- objectGUID (OID)
- userPrincipalName (UPN)
- Mail (email)
- Nombre simplificado (displayName)

Puede configurar un subconjunto de estos atributos siempre que los atributos SID o UPN estén incluidos en la aserción SAML. Citrix Cloud obtiene los demás atributos de su AD según sea necesario.

> **Nota:**
>
> Para garantizar un rendimiento óptimo, Citrix recomienda configurar todos los atributos que se mencionan en esta sección.

Aunque los pasos de integración precisos varían entre los distintos proveedores SAML, el proceso de integración suele incluir las siguientes tareas:

1. Instalar un agente de sincronización en su dominio de AD para establecer una conexión entre su dominio y su proveedor SAML. Si utiliza ADFS como proveedor SAML, este paso no es obligatorio.
2. Cree atributos personalizados y asígnelos a los atributos de usuario de AD requeridos que se mencionan anteriormente en esta sección. Como referencia, los pasos generales de esta tarea se describen en la sección Crear y asignar atributos SAML personalizados de este artículo.
3. Sincronizar los usuarios de AD con su proveedor SAML.

Para obtener más información sobre cómo integrar su AD con su proveedor SAML, consulte la documentación del producto de su proveedor SAML.

Autentificación de administrador con SAML 2.0

Citrix Cloud admite el uso de SAML 2.0 para autenticar a miembros de grupos de administradores en AD. Para obtener más información sobre cómo agregar grupos de administradores a Citrix Cloud, consulte Administrar grupos de administradores.

Usar una conexión SAML existente para la autenticación del administrador

Si ya tiene una conexión SAML 2.0 en Citrix Cloud y quiere usarla para autenticar a administradores, primero debe desconectar SAML 2.0 en **Administración de acceso e identidad** y, a continuación, configurar de nuevo la conexión. Si usa la conexión SAML para autenticar a suscriptores de Citrix Workspace, también debe inhabilitar el método de autenticación SAML en **Configuración de Workspace**. Tras configurar de nuevo la conexión SAML, puede agregar grupos de administradores a Citrix Cloud.

Si intenta agregar grupos de administradores sin antes desconectar y conectar de nuevo SAML 2.0, la opción de identidad **Active Directory** descrita en Agregar un grupo de administradores a Citrix Cloud no aparece.

Descripción general de las tareas para configurar una nueva conexión SAML

Para configurar una nueva conexión SAML 2.0 en Citrix Cloud, debe realizar estas tareas:

1. En **Administración de acceso e identidad**, conecte su AD local a Citrix Cloud como se describe en Conectar Active Directory a Citrix Cloud.
2. Integre su proveedor de SAML con su AD local como se describe en Integración de SAML con Active Directory en este artículo.
3. Configure la URL de inicio de sesión que los administradores pueden usar para iniciar sesión en Citrix Cloud.

4. En **Administración de acceso e identidad**, configure la autenticación SAML en Citrix Cloud. Esta tarea implica configurar su proveedor SAML con los metadatos de SAML de Citrix Cloud y, a continuación, configurar Citrix Cloud con los metadatos de su proveedor SAML para crear la conexión SAML.

Descripción general de las tareas para utilizar una conexión SAML existente para los administradores de Citrix Cloud

Si ya tiene una conexión SAML 2.0 en Citrix Cloud y quiere usarla para la autenticación de administradores, realice estas tareas:

1. Si corresponde, inhabilite la autenticación SAML 2.0 de espacios de trabajo: En **Configuración de Workspace > Autenticación**, seleccione un método de autenticación diferente y, a continuación, seleccione **Confirmar**.
2. Desconecte la conexión SAML 2.0 existente: En **Administración de acceso e identidad > Autenticación**, busque la conexión SAML. En el menú de puntos suspensivos del extremo derecho, seleccione **Desconectar**. Seleccione **Sí, desconectar** para confirmar la acción.
3. Conecte de nuevo SAML 2.0 y configure la conexión: En el menú de puntos suspensivos de **SAML 2.0**, seleccione **Conectar**.
4. Cuando se le solicite, introduzca un identificador único para la URL de inicio de sesión que los administradores utilizarán para iniciar sesión.
5. Configure la conexión SAML como se describe en Configurar los metadatos del proveedor SAML en este artículo.

Después de configurar la conexión SAML, puede agregar grupos de administradores de AD a Citrix Cloud como se describe en Administrar grupos de administradores. También puede habilitar SAML de nuevo para los suscriptores de espacios de trabajo como se describe en este artículo.

Crear y asignar atributos SAML personalizados

Si ya tiene configurados atributos personalizados para SID, UPN, OID, email y displayName en su proveedor SAML, no tiene que realizar esta tarea. Vaya a Crear una aplicación de conector SAML y utilice los atributos SAML personalizados existentes en el paso 5.

> **Nota:**
>
> En los pasos de esta sección, se describen las acciones que debe realizar en la consola de administración del proveedor SAML. Los comandos específicos que utilice para realizar estas acciones pueden ser distintos de los descritos en esta sección, dependiendo del proveedor SAML elegido. Los comandos de proveedor SAML de esta sección se ofrecen únicamente a efectos de ejemplo. Consulte la documentación de su proveedor SAML para obtener más información sobre los co-

> mandos correspondientes.

1. Inicie sesión en la consola de administración de su proveedor SAML y seleccione la opción para crear atributos de usuario personalizados. Por ejemplo, dependiendo de la consola del proveedor SAML, podría seleccionar **Users > Custom User Fields > New User Field**.
2. Agregue atributos para estas propiedades de AD. Asigne un nombre a los atributos con los valores predeterminados que se muestran.

Propiedad de AD	Obligatorio u opcional	Valor predeterminado
userPrincipalName	Obligatorio si no se agrega un atributo para el SID (recomendado).	`cip_upn`
objectSID	Obligatorio si no se agrega un atributo para el UPN.	`cip_sid`
objectGUID	Opcional para autenticación	`cip_oid`
mail	Opcional para autenticación	`cip_email`
displayName	Requerido por la interfaz de usuario de Workspace	`displayName`
givenName	Requerido por la interfaz de usuario de Workspace	`firstName`
sn	Requerido por la interfaz de usuario de Workspace	`lastName`
AD Forest	Opcional para autenticación	`cip_forest`
AD Domain	Opcional para autenticación	`cip_domain`

3. Seleccione el AD que conectó con Citrix Cloud. Por ejemplo, dependiendo de la consola del proveedor SAML, podría seleccionar **Users > Directories**.
4. Seleccione la opción para agregar atributos de directorio. Por ejemplo, dependiendo de la consola del proveedor SAML, podría seleccionar **Directory Attributes**.
5. Seleccione la opción para agregar atributos y asigne los siguientes atributos de AD a los atributos de usuario personalizados que creó en el paso 2:
   - Si agregó el atributo para SID en el paso 2 (por ejemplo, `cip_sid`), seleccione **objectSid** y asígnelo al atributo que creó.
   - Si agregó el atributo para UPN en el paso 2 (por ejemplo, `cip_upn`), seleccione **userPrincipalName** y asígnelo al atributo que creó.
   - Si agregó el atributo para ObjectGUID en el paso 2 (por ejemplo, `cip_oid`), seleccione **ObjectGUID** y asígnelo al atributo que creó.

- Si agregó el atributo para Mail en el paso 2 (por ejemplo, `cip_email`), seleccione **mail** y asígnelo al atributo que creó.
- Si agregó el atributo para Display Name en el paso 2 (por ejemplo, `displayName`), seleccione **displayName** y asígnelo al atributo que creó.

Configurar la URL de inicio de sesión de los administradores

1. Inicie sesión en Citrix Cloud en https://citrix.cloud.com.
2. Desde la consola de administración de Citrix Cloud, haga clic en el botón de menú y seleccione **Administración de acceso e identidad**.
3. Busque **SAML 2.0** y seleccione **Conectar** en el menú de puntos suspensivos.
4. Cuando se le solicite, introduzca un identificador breve y fácil de usar para la URL de su empresa y seleccione **Guardar y continuar**. Aparecerá la página **Configurar SAML**.
5. Vaya a la siguiente sección para configurar la conexión SAML con Citrix Cloud.

Configurar los metadatos del proveedor SAML

En esta tarea, se crea una aplicación de conector con metadatos de SAML de Citrix Cloud. Después de configurar la aplicación SAML, utilice los metadatos de SAML de la aplicación de conector para configurar la conexión SAML con Citrix Cloud.

> **Nota:**
>
> En algunos pasos de esta sección, se describen las acciones que debe realizar en la consola de administración del proveedor SAML. Los comandos específicos que utilice para realizar estas acciones pueden ser distintos de los descritos en esta sección, dependiendo del proveedor SAML elegido. Los comandos de proveedor SAML de esta sección se ofrecen únicamente a efectos de ejemplo. Consulte la documentación de su proveedor SAML para obtener más información sobre los comandos correspondientes.

Crear una aplicación de conector SAML

1. Desde la consola de administración del proveedor SAML, agregue una aplicación para un proveedor de identidades con atributos y respuesta de firma. Por ejemplo, dependiendo de la consola del proveedor, podría seleccionar **Applications > Applications > Add App** y, a continuación, **SAML Test Connector (IdP w/ attr w/ sign response)**.
2. Si procede, introduzca un nombre simplificado y guarde la aplicación.
3. En la pantalla **Configurar SAML** de Citrix Cloud, en **Metadatos SAML**, seleccione **Descargar**. El archivo XML de metadatos aparece en otra ficha del explorador.

> **Nota:**
>
> Si es necesario, también puede descargar este archivo desde `https://saml.cloud.com/saml/metadata.xml`. Es posible que este dispositivo de punto final funcione mejor con algunos proveedores de identidades al importar y supervisar los metadatos del proveedor SAML.

4. Introduzca los siguientes detalles para la aplicación de conector:
   - En el campo **Audiencia**, escriba `https://saml.cloud.com`.
   - En el campo **Destinatario**, escriba `https://saml.cloud.com/saml/acs`.
   - En el campo del validador de URL de ACS, escriba `https://saml.cloud.com/saml/acs`.
   - En el campo de URL de ACS, escriba `https://saml.cloud.com/saml/acs`.
5. Agregue sus atributos SAML personalizados como valores de parámetro en la aplicación:

Cree este campo	Asigne este atributo personalizado
cip_sid	El atributo personalizado que creó para SID. Ejemplo: cip_sid
cip_upn	El atributo personalizado que creó para UPN. Ejemplo: cip_upn
cip_oid	El atributo personalizado que creó para ObjectGUID. Ejemplo: cip_oid
cip_email	El atributo personalizado que creó para Mail. Ejemplo: cip_email
displayName	El atributo personalizado que creó para Display Name. Ejemplo: displayName

6. Agregue los suscriptores de su espacio de trabajo como usuarios para permitirles acceder a la aplicación.

Agregar metadatos de proveedor SAML a Citrix Cloud

1. Adquiera los metadatos SAML de su proveedor SAML. La siguiente imagen es un ejemplo del posible aspecto de este archivo:

2. En la pantalla **Configurar SAML** de Citrix Cloud, introduzca los siguientes valores del archivo de metadatos del proveedor SAML:

   - En **ID de entidad del proveedor de identidades**, introduzca el valor **entityID** del elemento **EntityDescriptor** en los metadatos.

     ```
     <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="
     https://app. .com/saml/metadata/8c733cbd-c579-41d4-b4e1-4ff034893d19">
     ```

   - En **Firmar solicitud de autenticación**, seleccione **Sí** para permitir que Citrix Cloud firme solicitudes de autenticación, certificando que provienen de Citrix Cloud y no de un actor malintencionado. Seleccione **No** si prefiere agregar la URL de ACS de Citrix a una lista de permitidos que su proveedor SAML utilice para publicar respuestas SAML de forma segura.
   - En **URL del servicio SSO**, introduzca la URL del mecanismo de vínculo que quiere utilizar. Puede usar un vínculo HTTP-POST o HTTP-Redirect. En el archivo de metadatos, busque los elementos **SingleSignOnService** con valores de vínculo **HTTP-POST** o **HTTP-Redirect**.

- En **Mecanismo vinculante**, seleccione el mecanismo que coincida con el vínculo de la URL del servicio SSO que eligió en el archivo de metadatos. De forma predeterminada, está seleccionada **HTTP Post**.
- En **Respuesta SAML**, seleccione el método de firma que el proveedor SAML utiliza para la respuesta SAML y la aserción SAML. De forma predeterminada, está seleccionada la opción **Firmar respuesta o aserción**. Citrix Cloud rechaza cualquier respuesta que no esté firmada como se especifica en este campo.

3. En la consola de administración del proveedor SAML, realice las siguientes acciones:
   - Seleccione **SHA-256** como algoritmo de firma SAML.
   - Descargue el certificado X.509 como archivo PEM, CRT o CER codificado en Base64.
4. En la página **Configurar SAML** de Citrix Cloud, en **Certificado X.509**, seleccione **Cargar archivo** y seleccione el archivo de certificado que descargó en el paso anterior.
5. Seleccione **Continuar** para completar la carga.
6. En **Contexto de autenticación**, seleccione el contexto que quiere utilizar y el nivel de rigurosidad con que quiere que Citrix Cloud aplique este contexto. Seleccione **Mínimo** para solicitar la autenticación en el contexto seleccionado sin exigir la autenticación en ese contexto. Seleccione **Exacto** para solicitar la autenticación en el contexto seleccionado y exigir la autenticación solo en ese contexto. Si su proveedor SAML no admite contextos de autenticación o usted prefiere no usarlos, seleccione **No especificado** y **Mínimo**. De forma predeterminada, se selecciona **Sin especificar** y **Exacto**.
7. Para la **URL de cierre de sesión** (opcional), decida si quiere o no que los usuarios que cierran sesión en Citrix Workspace o en Citrix Cloud también cierren sesión en todas las aplicaciones web en las que iniciaron sesión anteriormente a través del proveedor SAML.
   - Si quiere que los usuarios permanezcan conectados a sus aplicaciones web después de cerrar sesión en Citrix Workspace o Citrix Cloud, deje en blanco el campo **URL de cierre de sesión**.
   - Si quiere que los usuarios cierren sesión en todas las aplicaciones web después de cerrar sesión en Citrix Workspace o Citrix Cloud, introduzca el dispositivo de punto final SingleLogout (SLO) de su proveedor SAML. Si utiliza Microsoft ADFS o Azure Active Directory como proveedor SAML, el dispositivo de punto final SLO es el mismo que el dispositivo de punto final Single Sign-on (SSO).

8. Verifique que estos valores de atributos predeterminados en Citrix Cloud coincidan con los valores de atributos correspondientes configurados en su proveedor SAML. Para que Citrix Cloud encuentre estos atributos en la aserción SAML, los valores que introduzca aquí deben coincidir con los de su proveedor SAML. Si no configuró algún atributo en su proveedor SAML, puede usar el valor predeterminado en Citrix Cloud o dejar el campo vacío a menos que se indique lo contrario.

   - **Nombre de atributo para User Display Name**: El valor predeterminado es `displayName` .
   - **Nombre de atributo para User Given Name**: El valor predeterminado es `firstName`.
   - **Nombre de atributo para User Family Name**: El valor predeterminado es `lastName`.
   - **Nombre de atributo para Security Identifier (SID)**: Debe introducir este nombre de atributo de su proveedor SAML si no creó ningún atributo para UPN. El valor predeterminado es `cip_sid`.
   - **Nombre de atributo para User Principal Name (UPN)**: Debe introducir este nombre de atributo de su proveedor SAML si no creó ningún atributo para SID. El valor predeterminado es `cip_upn`.
   - **Nombre de atributo para Email**: El valor predeterminado es `cip_email`.
   - **Nombre de atributo para AD Object Identifier (OID)**: El valor predeterminado es `cip_oid`.
   - **Nombre de atributo para AD Forest**: El valor predeterminado es `cip_forest`.
   - **Nombre de atributo para AD Domain**: El valor predeterminado es `cip_domain`.

9. Seleccione **Probar y finalizar** para comprobar que ha configurado correctamente la conexión.

Agregar administradores a Citrix Cloud desde AD

Para obtener instrucciones sobre cómo agregar y administrar grupos de AD en Citrix Cloud, consulte Administrar grupos de administradores.

Habilitar la autenticación con SAML para espacios de trabajo

1. En el menú de Citrix Cloud, seleccione **Configuración de Workspace**.

2. Seleccione la ficha **Autenticación**
3. Seleccione **SAML 2.0**.

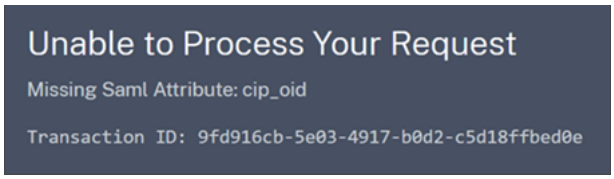
Solución de problemas

Errores de atributos

Es posible que se produzcan errores de atributos en cualquiera de estas condiciones:

- Los atributos obligatorios de su configuración de SAML no están codificados correctamente.
- Faltan los atributos `cip_sid` y `cip_upn` en la aserción SAML.
- Los atributos `cip_sid` o `cip_oid` faltan en la aserción SAML y Citrix Cloud no puede obtenerlos de Active Directory debido a un problema de conectividad.

Cuando se produce un error de atributo, Citrix Cloud muestra un mensaje de error que incluye los atributos correspondiente.



Para resolver este tipo de error:

1. Asegúrese de que su proveedor SAML envía los atributos necesarios con la codificación correcta, tal y como se muestra en la tabla siguiente. Como mínimo, se debe incluir el atributo SID o UPN.

Atributo	Codificación	Si son necesarias
cip_email	Debe estar en formato String (`user@domain`)	
cip_oid	Debe estar en formato Base64 o String	
cip_sid	Debe estar en formato Base64 o String	Sí, si no se usa `cip_upn`
cip_upn	Debe estar en formato String (`user@domain`)	Sí, si no se usa `cip_sid`

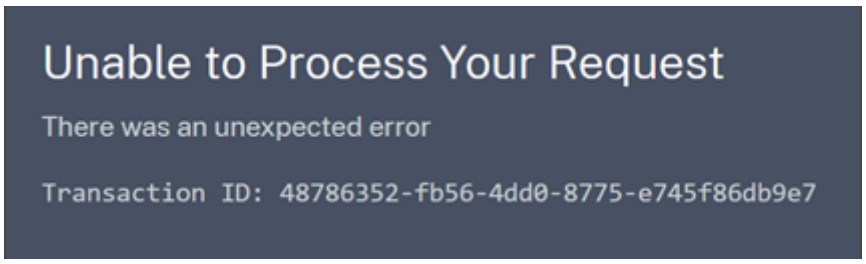
2. Verifique que los Cloud Connectors estén conectados y en buen estado para que Citrix Cloud pueda obtener los atributos faltantes que necesite. Para obtener más información, consulte Comprobaciones avanzadas de estado de Cloud Connector.

Errores inesperados

Es posible que Citrix Cloud experimente un error inesperado cuando:

- Un usuario inicia una solicitud SAML mediante un flujo iniciado por IdP. Por ejemplo, la solicitud se realiza seleccionando un mosaico a través del portal de aplicaciones del proveedor de identidades, en lugar de ir directamente a la URL del espacio de trabajo (`customer.cloud.com`).
- El certificado SAML no es válido o ha caducado.
- El contexto de autenticación no es válido.
- La aserción SAML y la firma de respuesta no coinciden.

Cuando se produce este error, Citrix Cloud muestra un mensaje de error genérico.

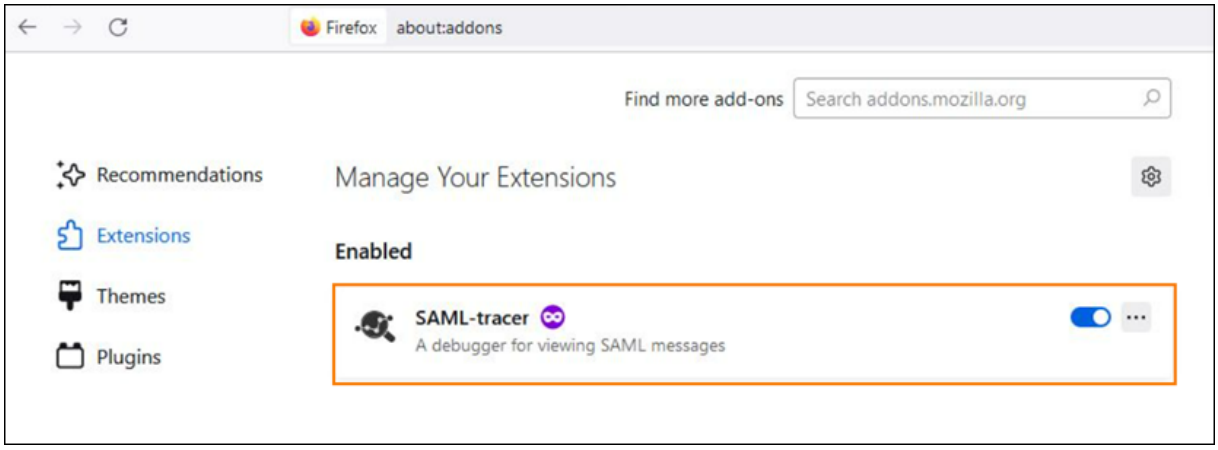


Si este error se produce al ir a Citrix Cloud a través del portal de aplicaciones de un proveedor de identidades, puede usar la siguiente solución temporal:

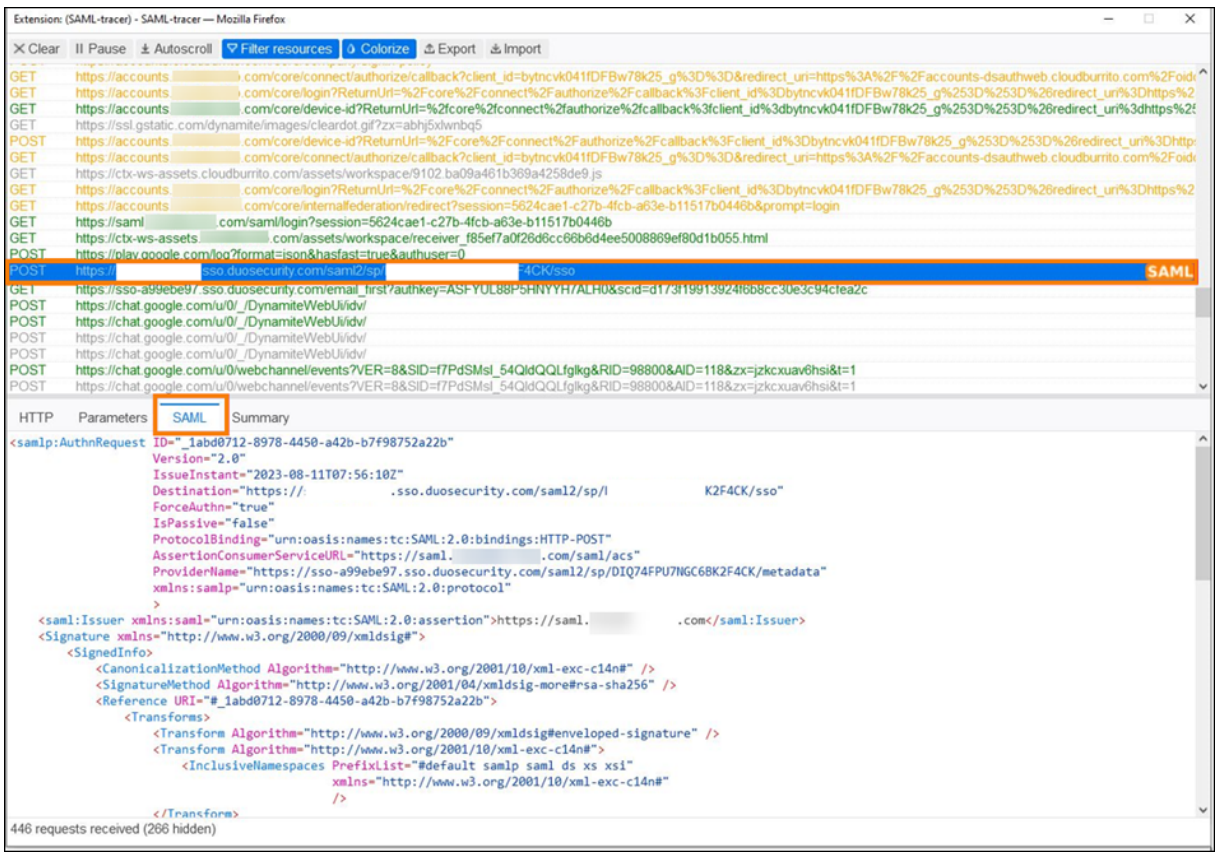
1. Cree una aplicación de marcador en el portal de aplicaciones del proveedor de identidades que haga referencia a la URL del espacio de trabajo (por ejemplo, `https://customer.cloud.com`).
2. Asigne usuarios tanto a la aplicación SAML como a la aplicación de marcador.
3. Cambie la configuración de visibilidad de la aplicación SAML y la aplicación de marcador, de manera que la aplicación de marcador sea visible y la aplicación SAML esté oculta en el portal de aplicaciones.
4. Inhabilite el parámetro **Sesiones de proveedores de identidad federada** en Configuración de Workspace para quitar solicitudes de contraseña adicionales. Para obtener instrucciones, consulte Sesiones de proveedores de identidad federada en la documentación del producto Citrix Workspace.

Recomendaciones para la depuración de errores

Citrix recomienda usar la extensión de explorador web SAML-tracer para todas las depuraciones de SAML. Esta extensión está disponible para los exploradores web más comunes. La extensión decodifica solicitudes y respuestas codificadas en Base64 en XML SAML, lo que las hace legibles para las personas.



Esta herramienta le permite, como administrador, comprobar el valor de los atributos SAML que se envían al usuario y buscar la presencia de firmas en solicitudes y respuestas de SAML. En caso de que necesite ayuda con un problema relacionado con SAML, Citrix Support solicita el archivo SAML-tracer para comprender el problema y resolver su caso de asistencia.



Más información

- Documentos de Microsoft: Tutorial: Integración del inicio de sesión único (SSO) de Azure Active Directory con Citrix Cloud SAML SSO

- SAML con Active Directory Federated Services (ADFS): Configurar la autenticación SAML en Citrix Cloud mediante ADFS.
- Citrix Tech Zone: Tech Insight: Authentication - SAML

Configurar una aplicación SAML mediante un ID de entidad con ámbito en Citrix Cloud

December 12, 2023

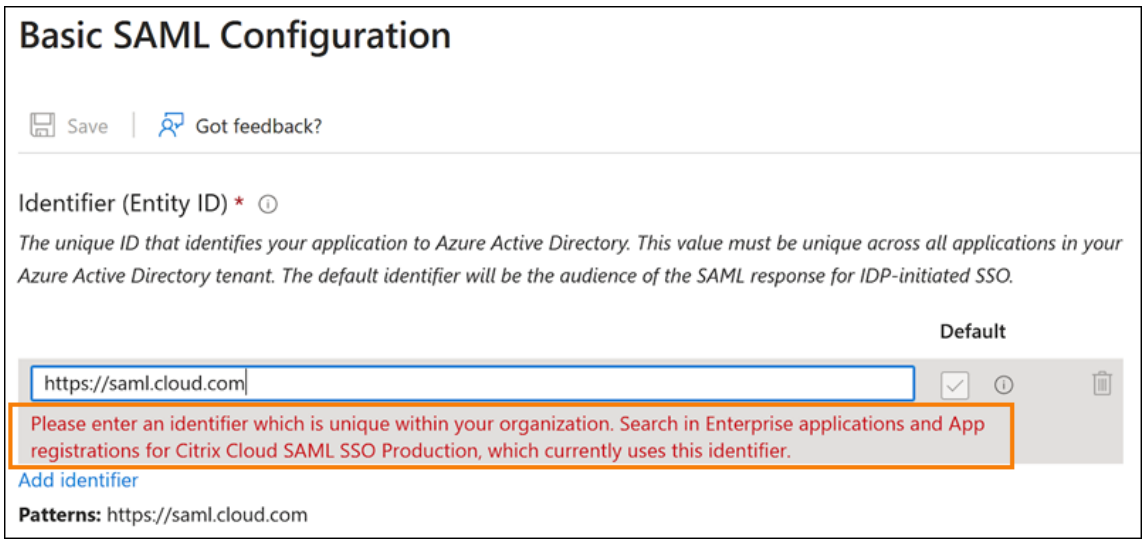
Author:
Mark Dear

En este artículo se describe cómo aprovisionar varias aplicaciones SAML en el mismo proveedor de SAML.

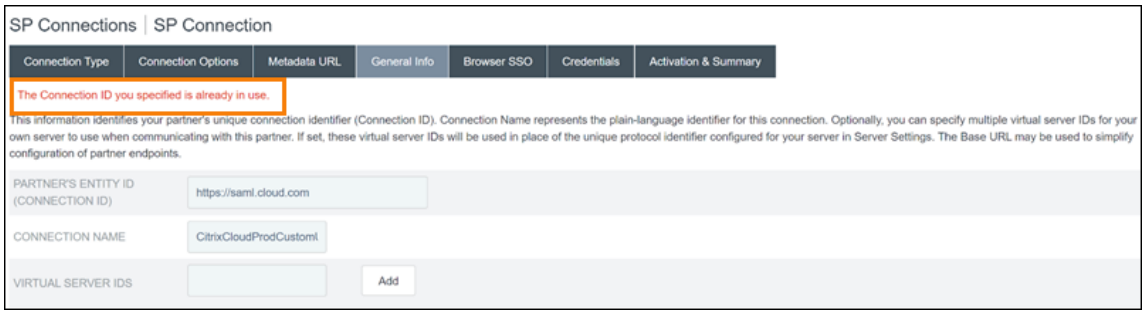
Algunos proveedores de SAML, como Azure Active Directory (AD), Active Directory Federation Services (ADFS), PingFederate y PingSSO, prohíben volver a utilizar el ID de entidad del mismo proveedor de servicios (SP) en varias aplicaciones de SAML. Como resultado, los administradores que crean dos o más aplicaciones SAML diferentes dentro del mismo proveedor de SAML no pueden vincularlas a los mismos arrendatarios de Citrix Cloud o a otros diferentes. Al intentar crear una segunda aplicación SAML con el ID de entidad del mismo SP, como `https:\\saml.cloud.com`, cuando una aplicación SAML existente ya lo está utilizando, se desencadena un error en el proveedor de SAML que indica que el ID de entidad ya se está usando.

Estas imágenes ilustran el error:

- En Azure Active Directory:



- En PingFederate:



La función de ID de entidad con ámbito de Citrix Cloud aborda esta limitación para que pueda crear más de una aplicación SAML dentro del proveedor de SAML (por ejemplo, un arrendatario de Azure AD) y vincularla a un único arrendatario de Citrix Cloud.

¿Qué es un ID de entidad?

Un ID de entidad SAML es un identificador único que se usa para identificar una entidad específica en el protocolo de autorización y autenticación SAML. Normalmente, el ID de entidad es una URL o URI que se asigna a la entidad y se utiliza en metadatos y mensajes SAML. Cada aplicación SAML que cree en su proveedor de SAML se considera una entidad única.

En una conexión SAML entre Citrix Cloud y Azure AD, por ejemplo, Citrix Cloud es el proveedor de servicios (SP) y Azure AD es el proveedor de SAML. Ambos tienen un ID de entidad que debe configurarse en el lado opuesto de la conexión SAML. Esto significa que el ID de entidad de Citrix Cloud debe configurarse dentro de Azure AD, y el ID de entidad de Azure AD debe configurarse en Citrix Cloud.

Estos ID de entidad son ejemplos de un ID de entidad genérico y un ID de entidad con ámbito en Citrix Cloud:

- Genérico: `https://saml.cloud.com`
- Con ámbito: `https://saml.cloud.com/67338f11-4996-4980-8339-535f76d0c8fb`

ID de entidad de SP genéricos y con ámbito por región

Las conexiones SAML existentes en Citrix Cloud (creadas antes de noviembre de 2023) utilizan el mismo ID de entidad genérico para cada conexión SAML y cada arrendatario de Citrix Cloud. Solo las conexiones SAML nuevas de Citrix Cloud ofrecen la opción de usar un ID de entidad con ámbito.

Si opta por utilizar ID de entidad con ámbito para las nuevas conexiones, cualquier conexión SAML existente seguirá funcionando con sus ID de entidad genéricos originales.

En esta tabla se enumeran los ID de entidad de SP genéricos y con ámbito para cada región de Citrix Cloud:

Región de Citrix Cloud	ID de entidad de SP genérico	ID de entidad con ámbito
Estados Unidos, Unión Europea, Asia Pacífico-Sur	`https://saml.cloud.com`	`https://saml.cloud.com/67338f11-4996-4980-8339-535f76d0c8fb`
Japón	`https://saml.citrixcloud.jp`	`https://saml.citrixcloud.jp/db642d4c-ad2c-4304-adcf-f96b6aa16c29`
Gobierno	`https://saml.cloud.us`	`https://saml.cloud.us/20f1cf66-cfe9-4dd3-865c-9c59a6710820`

Generación de ID de entidad de SP únicos para conexiones SAML nuevas y existentes

Al crear una conexión SAML, Citrix Cloud genera un ID único (GUID). Para generar un ID de entidad con ámbito, habilite la opción **Configurar ID de entidad de SAML con ámbito** al crear la conexión.

Si quiere actualizar una conexión SAML existente para usar ID de entidad con ámbito, debe desconectar y conectar de nuevo su proveedor de SAML desde la página **Administración de acceso e identidad > Autenticación** de Citrix Cloud. Citrix Cloud no permite modificar directamente las conexiones SAML existentes. Sin embargo, puede clonar la configuración y modificar el clon.

> **Importante:**
>
> Al cerrar el proceso de conexión SAML antes de completarlo, se descarta el ID de entidad que Citrix Cloud genera automáticamente. Al reiniciar el proceso de conexión SAML, Citrix Cloud genera un nuevo GUID de ID de entidad con ámbito. Use este nuevo ID de entidad con ámbito al configurar el proveedor de SAML. Si piensa actualizar una conexión SAML existente para usar ID de entidad con ámbito, debe actualizar la aplicación SAML para esa conexión mediante el ID de entidad con ámbito que genera Citrix Cloud.

Preguntas frecuentes sobre los ID de entidad con ámbito

¿Puedo crear más de una aplicación SAML de Azure AD dentro del mismo arrendatario de Azure AD y vincularla a uno o más arrendatarios de Citrix Cloud?

La función de ID de entidad con ámbito de Citrix Cloud aborda la limitación de evitar la duplicación de ID de entidad que imponen algunos proveedores de SAML. Con esta función, puede aprovisionar más de una aplicación SAML en su arrendatario de Azure AD y configurar cada una con un ID de entidad con ámbito de un único arrendatario de Citrix Cloud.

¿Puedo seguir vinculando la misma aplicación SAML de Azure AD a varios arrendatarios de Citrix Cloud?

Este caso es habitual entre clientes de Citrix Cloud, y Citrix sigue ofreciendo asistencia al respecto. Para implementar este caso, debe cumplir estos requisitos:

- Use un ID de entidad genérico, como `https://saml.cloud.com`.
- No habilite ID de entidad con ámbito para su conexión SAML.

¿Cómo decido si usar o no un ID de entidad con ámbito en mi proveedor de SAML?

Los ID de entidad con ámbito de Citrix Cloud ofrecen la flexibilidad de utilizar un ID de entidad genérico o con ámbito, según sus requisitos. Tenga en cuenta la cantidad de aplicaciones SAML que necesita y la cantidad de arrendatarios de Citrix Cloud que tiene. Además, tenga en cuenta si cada arrendatario podría compartir una aplicación SAML existente o necesitar su propia aplicación SAML con ámbito.

> **Importante:**
>
> Si su proveedor de SAML ya le permite crear varias aplicaciones SAML con el mismo ID de entidad (como `https://saml.cloud.com`), no necesita habilitar ID de entidad con ámbito ni realizar ningún cambio en su configuración de SAML actual. No necesita actualizar parámetros ni en Citrix Cloud ni en su aplicación SAML.

Proveedores de SAML afectados

En esta tabla se enumeran los proveedores de SAML que permiten o limitan el uso de ID de entidad duplicados.

Proveedor de SAML	Admite ID de entidad duplicados
Azure AD (nube)	No
ADFS (local)	No
PingFederate (local)	No
PingOneSSO (nube)	No
Okta (nube)	Sí
Duo (nube)	Sí
OneLogin (nube)	Sí

Casos de uso afectados

En esta tabla se indica si se admite un ID de entidad genérico o con ámbito en función de las aplicaciones SAML que requiera su caso de uso, y si su proveedor de SAML admite ID de entidad duplicados.

Requisito de los casos de uso	¿El proveedor de SAML admite ID de entidad duplicados?	Configuración compatible
Solo una aplicación SAML	Sí	ID de entidad genérico o con ámbito
Solo una aplicación SAML	No	ID de entidad genérico o con ámbito
Dos o más aplicaciones SAML	Sí	ID de entidad genérico o con ámbito
Dos o más aplicaciones SAML	No	ID de entidad con ámbito
Pares de aplicación SAML y URL personalizada de Workspace	Sí	ID de entidad genérico o con ámbito
Pares de aplicación SAML y URL personalizada de Workspace	No	ID de entidad con ámbito
Vincular la misma aplicación SAML a varios arrendatarios de Citrix Cloud	Sí	ID de entidad genérico
Vincular la misma aplicación SAML a varios arrendatarios de Citrix Cloud	No	ID de entidad genérico

Configurar la conexión SAML principal con un ID de entidad con ámbito

En esta tarea, creará una conexión SAML en Citrix Cloud mediante un ID de entidad con ámbito para la aplicación SAML principal (aplicación SAML 1).

1. Desde la consola de administración de Citrix Cloud, haga clic en el botón de menú y seleccione **Administración de acceso e identidad**.
2. En la ficha **Autenticación**, busque **SAML 2.0** y seleccione **Conectar** en el menú de tres puntos.
3. Cuando se le solicite crear su URL de inicio de sesión única, introduzca un identificador breve y fácil de usar para la URL de su empresa (por ejemplo, `https://citrix.cloud.com/go/mycompany`) y seleccione **Guardar y continuar**. Este identificador debe ser único en Citrix Cloud.
4. En **Configurar proveedor de identidades SAML**, seleccione **Configurar ID de entidad SAML con ámbito**. Citrix Cloud genera automáticamente ID de entidad con ámbito y rellena los campos de ID de entidad, Assertion Consumer Service y URL de cierre de sesión.
5. En **Configurar una conexión SAML a Citrix Cloud**, introduzca los detalles de conexión de su proveedor de SAML.
6. Acepte las asignaciones de atributos SAML predeterminados.
7. Seleccione **Probar y finalizar**.

Configurar la conexión SAML principal con un ID de entidad genérico

En esta tarea, creará una conexión SAML en Citrix Cloud con el ID de entidad genérico predeterminado para la aplicación SAML principal (aplicación SAML 1).

1. Desde la consola de administración de Citrix Cloud, haga clic en el botón de menú y seleccione **Administración de acceso e identidad**.
2. En la ficha **Autenticación**, busque **SAML 2.0** y seleccione **Conectar** en el menú de tres puntos.
3. Cuando se le solicite crear su URL de inicio de sesión única, introduzca un identificador breve y fácil de usar para la URL de su empresa (por ejemplo, `https://citrix.cloud.com/go/mycompany`) y seleccione **Guardar y continuar**. Este identificador debe ser único en Citrix Cloud.
4. En **Configurar proveedor de identidades SAML**, compruebe que la opción **Configurar ID de entidad SAML con ámbito** esté inhabilitada.
5. En **Configurar una conexión SAML a Citrix Cloud**, introduzca los detalles de conexión de su proveedor de SAML.
6. En **Metadatos SAML del proveedor de servicios**, haga clic en **Descargar** para obtener una copia de los metadatos SAML genéricos, si es necesario.
7. Acepte las asignaciones de atributos SAML predeterminados.
8. Seleccione **Probar y finalizar**.

Configurar una conexión SAML mediante dominios personalizados de Citrix Workspace

En esta sección se detalla cómo configurar una conexión SAML mediante una URL de Workspace personalizada con un ID de entidad genérico o con ámbito.

Las tareas de esta sección solo se aplican si tiene una URL de Workspace personalizada existente que use con SAML. Si no usa una URL de Workspace personalizada con autenticación SAML, puede omitir las tareas de esta sección.

Para obtener más información, consulte los siguientes artículos:

- Configurar un dominio personalizado
- Iniciar sesión en espacios de trabajo con SAML mediante dominios personalizados

Configurar una conexión SAML con una URL personalizada de Workspace y un ID de entidad genérico

En esta tarea, la opción **Configurar ID de entidad con ámbito** está inhabilitada.

1. En el menú de Citrix Cloud, seleccione **Autenticación de Workspace**.
2. En **URL de Workspace personalizada**, seleccione **Modificar** en el menú de tres puntos.
3. Seleccione **Usar la URL de [nombreDeCliente].cloud.com y la URL de dominio personalizado**.
4. Introduzca el ID de entidad genérico, la URL de SSO y la URL de SLO opcional para la aplicación SAML 2, y cargue el certificado de firma que descargó anteriormente de su proveedor de SAML.
5. Si es necesario, en **Metadatos SAML del proveedor de servicios del dominio personalizado**, haga clic en **Descargar** para obtener una copia de los metadatos SAML genéricos para la aplicación SAML de la URL personalizada de Workspace.
6. Haga clic en **Guardar**.

Configurar una conexión SAML con una URL personalizada de Workspace y un ID de entidad con ámbito

En esta tarea, la opción **Configurar ID de entidad con ámbito** está habilitada.

1. En el menú de Citrix Cloud, seleccione **Autenticación de Workspace**.
2. En **URL de Workspace personalizada**, seleccione **Modificar** en el menú de tres puntos.
3. Seleccione **Usar la URL de [nombreDeCliente].cloud.com y la URL de dominio personalizado**.
4. Introduzca el ID de entidad con ámbito, la URL de SSO y la URL de SLO opcional para la aplicación SAML 2, y cargue el certificado de firma SAML que descargó anteriormente de su proveedor de SAML.

5. Haga clic en **Guardar**.

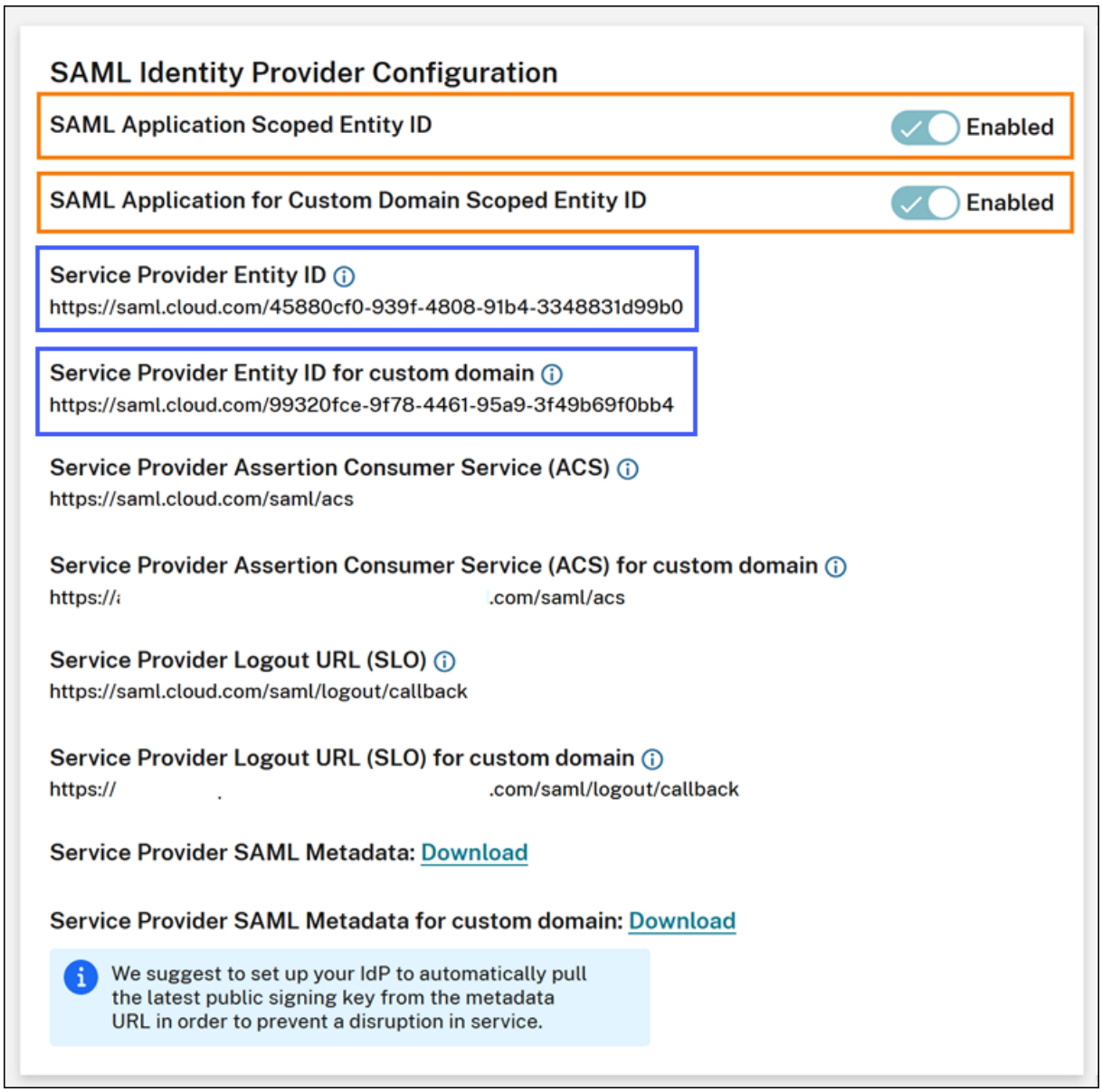
Tras guardar la configuración, Citrix Cloud genera los metadatos SAML con ámbito que contienen el GUID correcto. Si es necesario, puede obtener una copia de los metadatos con ámbito de la aplicación SAML de la URL personalizada de Workspace.

1. En la página **Administración de acceso e identidad**, busque la conexión SAML y seleccione **Ver** en el menú de tres puntos.
2. En **Metadatos SAML del proveedor de servicios del dominio personalizado**, haga clic en **Descargar**.

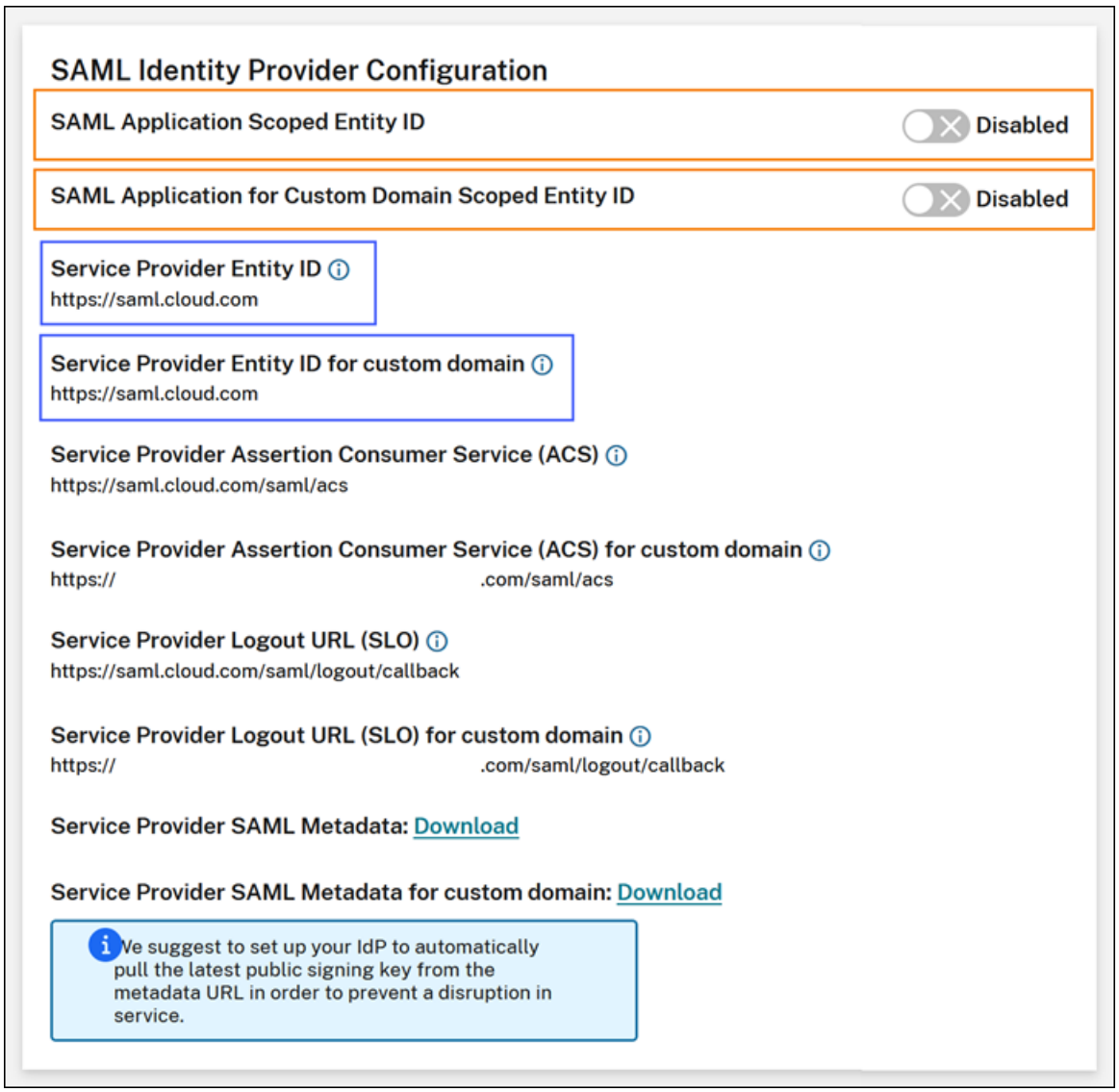
Ver la configuración SAML de aplicaciones SAML principales y de URL de Workspace personalizadas

Al ver los detalles de configuración de la conexión SAML con ámbito, Citrix Cloud muestra los parámetros de ID de entidad con ámbito tanto para la aplicación SAML principal como para la aplicación SAML de dominio personalizado de Workspace.

Por ejemplo, al habilitar los ID de entidad con ámbito, los campos **ID de entidad del proveedor de servicios** e **ID de entidad del proveedor de servicios del dominio personalizado** contienen los ID de entidad con ámbito que genera Citrix Cloud.



Cuando los ID de entidad con ámbito están inhabilitados, los campos **ID de entidad del proveedor de servicios** e **ID de entidad del proveedor de servicios del dominio personalizado** contienen los ID de entidad genéricos.



Para actualizar aplicaciones SAML existentes en su proveedor de SAML, agregue el ID de entidad con ámbito al valor del ID de entidad existente.

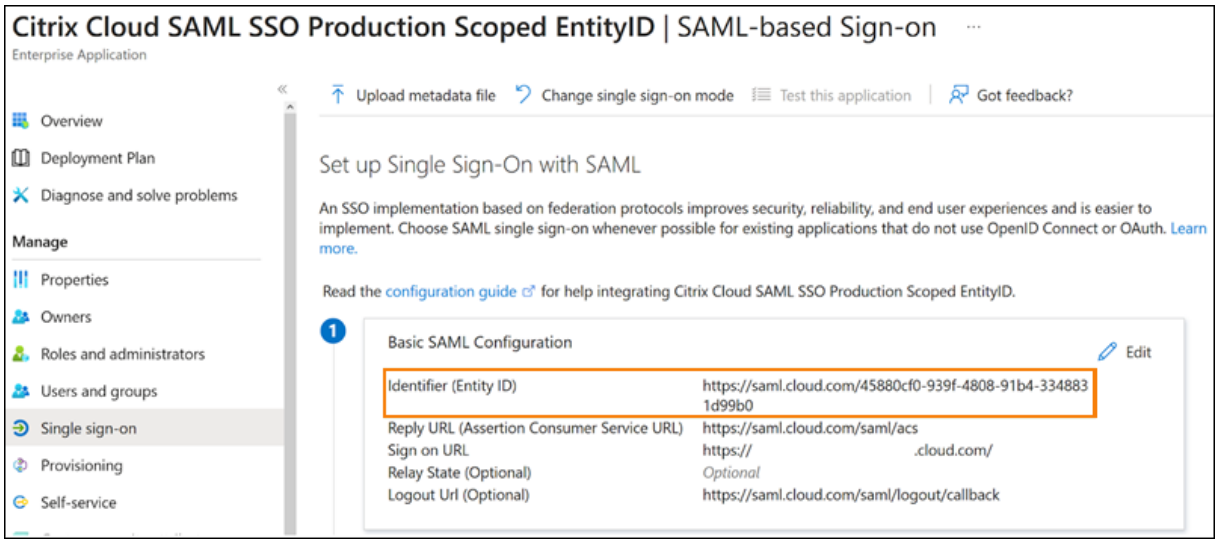
Configuración del proveedor de SAML mediante ID de entidad con ámbito

Tras configurar la conexión SAML en Citrix Cloud con ID de entidad con ámbito, puede agregar el ID de entidad con ámbito a su proveedor de SAML.

En esta sección se incluyen ejemplos de configuración de Azure AD y PingFederate.

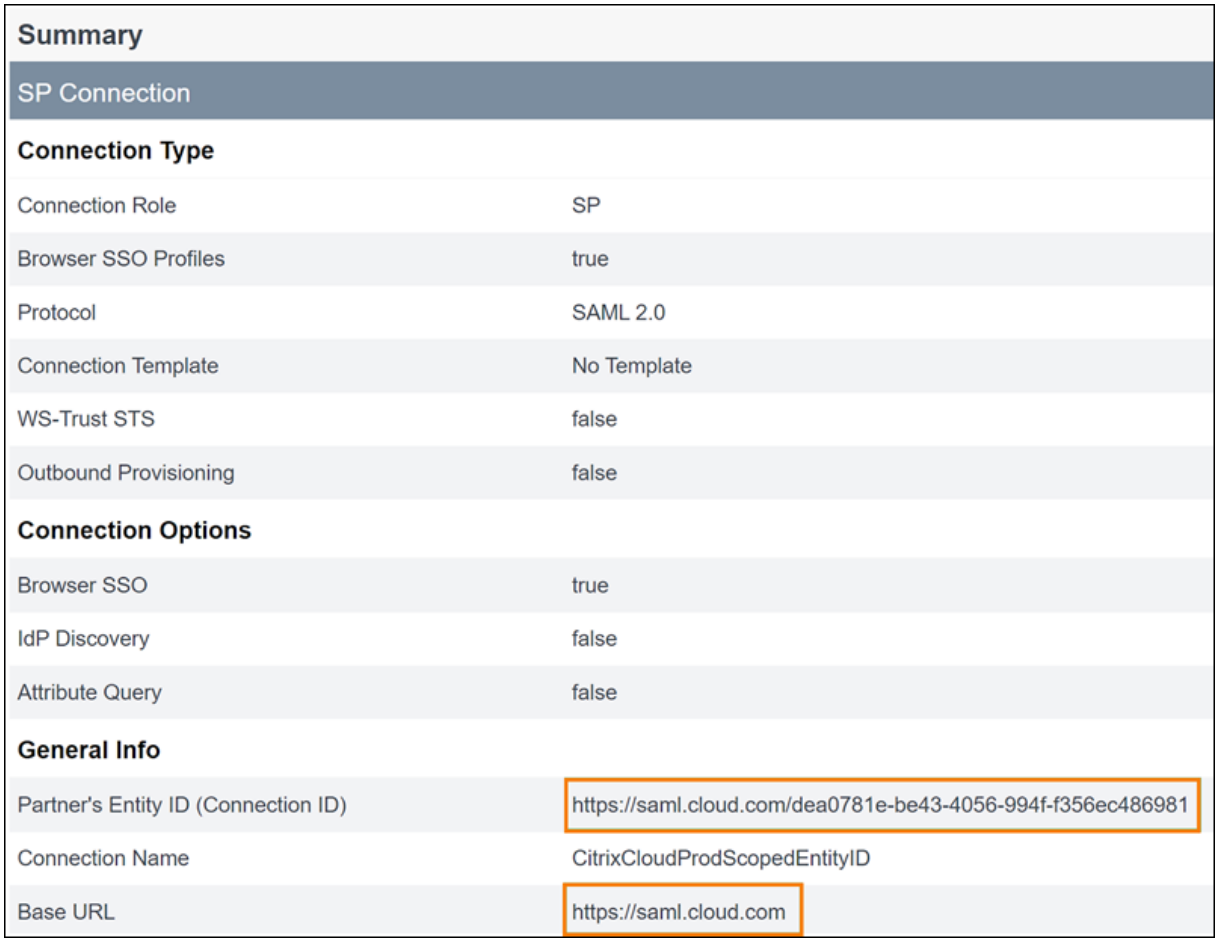
Configuración de SAML de Azure AD mediante ID de entidad con ámbito

En este ejemplo, el ID de entidad con ámbito de Citrix Cloud se introduce en el campo **Identificador** de Azure AD.



Configuración de SAML de PingFederate mediante ID de entidad con ámbito

En este ejemplo, el ID de entidad con ámbito y el ID de entidad genérico de Citrix Cloud se rellenan en los campos **Partner's Entity ID** y **Base URL**, respectivamente.



Summary	
SP Connection	
Connection Type	
Connection Role	SP
Browser SSO Profiles	true
Protocol	SAML 2.0
Connection Template	No Template
WS-Trust STS	false
Outbound Provisioning	false
Connection Options	
Browser SSO	true
IdP Discovery	false
Attribute Query	false
General Info	
Partner's Entity ID (Connection ID)	https://saml.cloud.com/dea0781e-be43-4056-994f-f356ec486981
Connection Name	CitrixCloudProdScopedEntityID
Base URL	https://saml.cloud.com

Solución de problemas

Citrix recomienda utilizar la extensión para exploradores web SAML-tracer para solucionar posibles problemas con la configuración de SAML. Esta extensión decodifica solicitudes y respuestas codificadas en Base64 y las transforma en XML SAML de modo que la información sea legible para humanos. Puede usar la extensión SAML-tracer para examinar las solicitudes SAML de SSO y SLO que Citrix Cloud (el proveedor de servicios) genera y envía a su proveedor de SAML (el proveedor de identidades). La extensión puede mostrar si el ámbito del ID de entidad (GUID) está incluido en ambas solicitudes.

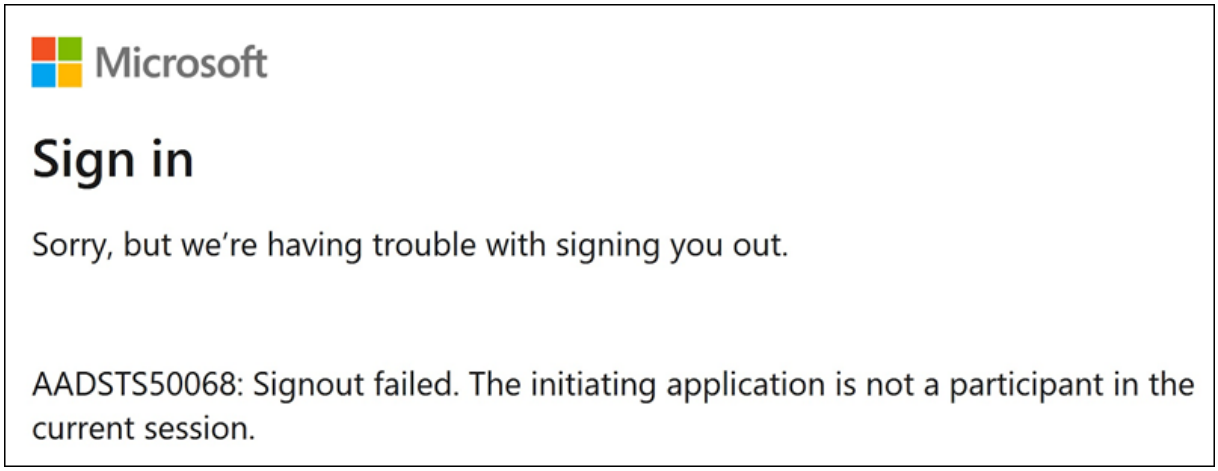
1. Desde el panel Extensiones de su explorador web, instale y habilite la extensión SAML-tracer.
2. Realice una operación de inicio y cierre de sesión de SAML, y capture todo el flujo con la extensión SAML-tracer.
3. Busque esta línea en la solicitud de SSO de SAML o en la solicitud de SLO.

```
1 <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
     https://saml.cloud.com/cfee4a86-97a8-49cf-9bb6-fd15ab075b92</
     saml:Issuer>
2 <!--NeedCopy-->
```


4. Compruebe que el ID de entidad coincida con el ID de entidad configurado en la aplicación de su proveedor de SAML.
5. Compruebe que el ID de entidad con ámbito esté presente en el campo **Emisor** y asegúrese de que esté configurado correctamente en su proveedor de SAML.
6. Exporte y guarde el resultado JSON de SAML-tracer. Si trabaja con Citrix Support para resolver un problema, cargue el resultado en su caso de asistencia de Citrix.

Solución de problemas de Azure AD

Problema: No se puede cerrar sesión en Azure AD cuando SLO está configurado. Azure AD muestra este error al usuario:



Si los ID de entidad con ámbito están habilitados para la conexión SAML en Citrix Cloud, el ID de entidad con ámbito se debe enviar en las solicitudes de SSO y SLO.

Causa: La entidad con ámbito está configurada, pero falta el ID de entidad en la solicitud de SLO. Compruebe que el ID de entidad con ámbito esté presente en la solicitud de SLO del resultado de SAML-tracer.

Solución de problemas de PingFederate en instancias locales

Problema: No se puede iniciar o cerrar sesión en PingFederate después de habilitar el parámetro ID de entidad con ámbito.

Causa: El administrador de PingFederate agregó el ID de entidad con ámbito a la URL base de la conexión del SP.

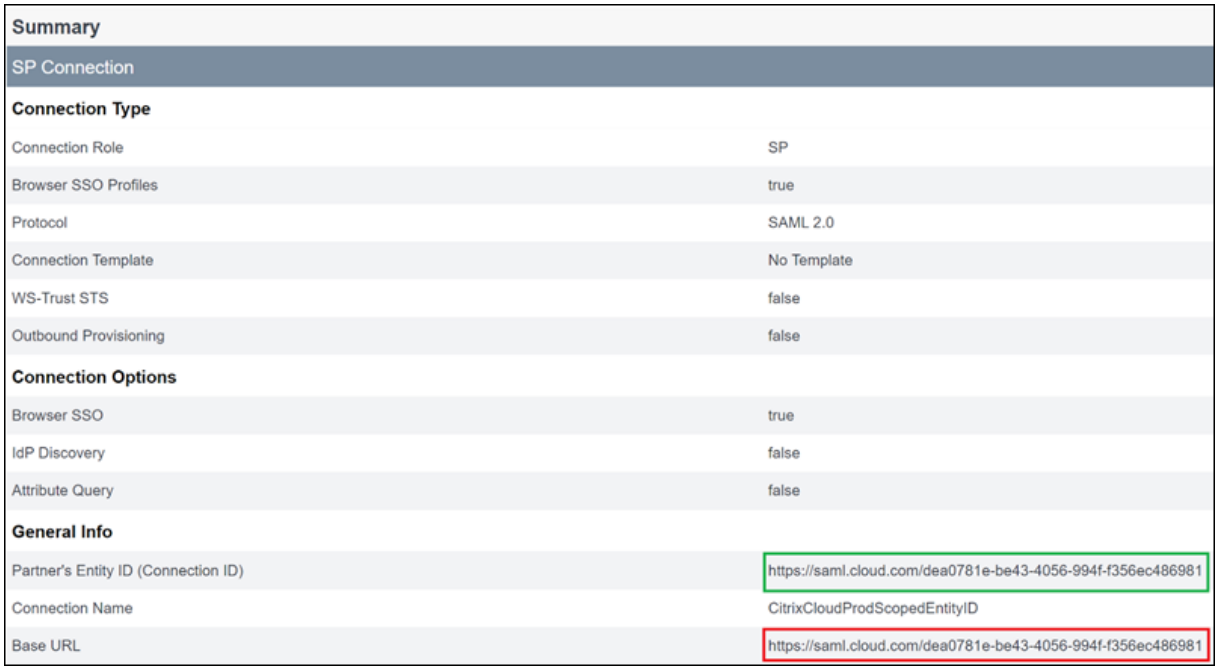
Para corregir este problema, agregue el ID de entidad con ámbito únicamente al campo **Partner's Entity ID**. Al agregar el ID de entidad con ámbito a la URL base, se produce un dispositivo de punto final SAML con formato incorrecto. Si la URL base de Citrix Cloud no se actualiza correctamente, todas

las demás URL relativas a dispositivos de punto final SAML que se deriven de la URL base producen errores de inicio de sesión.

Estos dispositivos de punto final son ejemplos de dispositivos de punto final SAML de Citrix Cloud con formato incorrecto que podrían aparecer en el resultado de SAML-tracer:

- `https://saml.cloud.com/<GUID>/saml/acs`
- `https://saml.cloud.com/<GUID>/saml/logout/callback`

Esta imagen muestra una aplicación SAML de PingFederate mal configurada. El campo correctamente configurado se muestra en verde. El campo configurado incorrectamente se muestra en rojo.



Summary	
SP Connection	
Connection Type	
Connection Role	SP
Browser SSO Profiles	true
Protocol	SAML 2.0
Connection Template	No Template
WS-Trust STS	false
Outbound Provisioning	false
Connection Options	
Browser SSO	true
IdP Discovery	false
Attribute Query	false
General Info	
Partner's Entity ID (Connection ID)	https://saml.cloud.com/dea0781e-be43-4056-994f-f356ec486981
Connection Name	CitrixCloudProdScopedEntityID
Base URL	https://saml.cloud.com/dea0781e-be43-4056-994f-f356ec486981

SAML con Azure AD e identidades de AAD para la autenticación de espacios de trabajo

March 12, 2024

Author:
Mark Dear

En este artículo, se describe cómo configurar SAML para la autenticación de espacios de trabajo mediante identidades de Azure Active Directory (AD) en lugar de identidades de AD. Use esta configuración si los usuarios de Azure AD no pueden enumerar los PC en la nube Windows 365 o los VDA unidos a un dominio de Azure AD después de iniciar sesión en Citrix Workspace con el comportamiento de SAML

predeterminado. Tras completar la configuración, los usuarios pueden iniciar sesión en Citrix Workspace mediante la autenticación SAML para acceder tanto a aplicaciones como a escritorios HDX a través de Citrix DaaS y a PC en la nube Windows 365 a través de Azure.

El comportamiento predeterminado de la autenticación de Citrix Cloud y SAML en Citrix Workspace es confirmar la identidad de usuarios de AD. Para la configuración descrita en este artículo, es necesario usar Azure AD Connect para importar identidades de AD a Azure AD. Las identidades de AD contienen el SID del usuario, que Citrix Workspace puede enviar a Citrix DaaS y permite enumerar e iniciar recursos HDX. Como se utiliza la versión Azure AD de las identidades de los usuarios, los usuarios también pueden enumerar e iniciar recursos de Azure, como los PC en la nube Windows 365, desde Citrix Workspace.

> **Importante:**
>
> La enumeración hace referencia a la lista de recursos que ven los usuarios después de iniciar sesión en Citrix Workspace. Los recursos a los que puede acceder un usuario determinado dependen de su identidad de usuario y de los recursos que estén asociados a esa identidad en Citrix DaaS. Hay un artículo asociado que proporciona instrucciones sobre cómo usar Azure AD e identidades de AD como proveedor de SAML para autenticarse en Workspace. Encontrará instrucciones detalladas en SAML con Azure AD e identidades de AD para la autenticación de espacios de trabajo

Ámbito de las funciones

Este artículo se aplica a los usuarios que usan esta combinación de funciones de Citrix Cloud y Azure:

- SAML para la autenticación de espacios de trabajo
- Enumeración de recursos de Citrix DaaS y HDX publicados mediante VDA unidos a un dominio de AD
- Enumeración de recursos de VDA unidos a un dominio de Azure AD
- Enumeración de recursos de VDA unidos a un dominio híbrido de Azure
- Enumeración e inicio de W365 Cloud PC

> **Importante:**
>
> No utilice este flujo SAML de AAD para iniciar sesión con SAML en Citrix Cloud, ya que esto requiere que el usuario administrador de Citrix Cloud sea miembro de un grupo de AD y, por lo tanto, se debe usar una identidad de usuario de AD. Encontrará instrucciones detalladas en SAML con Azure AD e identidades de AD para la autenticación de espacios de trabajo

¿Qué es mejor: identidades de AD o identidades de Azure AD?

Para determinar si los usuarios de su espacio de trabajo deben autenticarse mediante identidades SAML de AD o SAML de Azure AD:

1. Decida qué combinación de recursos quiere poner a disposición de sus usuarios en Citrix Workspace.
2. Use esta tabla para determinar qué tipo de identidad de usuario es adecuado para cada tipo de recurso.

Tipo de recurso (VDA)	Identidad del usuario al iniciar sesión en Citrix Workspace	¿Necesita una identidad SAML con Azure AD?	¿FAS proporciona Single Sign-On (SSO) a VDA?
Unida a AD	AD, Azure AD importado de AD (contiene SID)	No. Use el SAML predeterminado.	Sí
Híbrido unido	AD, Azure AD importado de AD (contiene SID)	No. Use el SAML predeterminado.	Sí, para AD como proveedor de identidades. FAS no es obligatorio si se selecciona Azure AD para VDA.
Unida a Azure AD	Usuario nativo de Azure AD, Azure AD importado de AD (contiene SID)	Sí, use SAML a través de Azure AD.	SSO funciona con la autenticación moderna de Azure AD. No se requiere FAS.
PC en la nube Windows 365	Usuario nativo de Azure AD, Azure AD importado de AD (contiene SID)	Sí, use SAML a través de Azure AD.	SSO funciona con la autenticación moderna de Azure AD. No se requiere FAS.
Unido a AD, unido a Azure AD, PC en la nube Windows 365	Azure AD importado de AD (contiene SID)	Sí, use SAML a través de Azure AD.	Sí, para los unidos a AD. No, para PC en la nube Windows 365 y unidos a Azure AD.

Más información

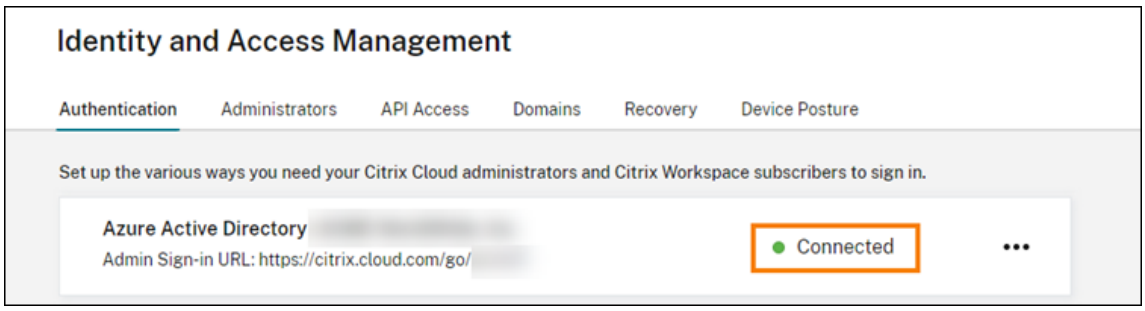
- Documentación de Citrix DaaS:
  - Identidades de las máquinas

  - Citrix HDX Plus para Windows 365

- Documentación de Citrix FAS: Instalación y configuración
- Documentación de Microsoft Azure: ¿Qué es Azure AD Connect?

Requisitos

- Su arrendatario de Azure AD debe estar conectado a su arrendatario de Citrix Cloud. En la consola de Citrix Cloud, para ver su conexión a Azure AD, seleccione **Administración de acceso e identidad > Autenticación**.



- El método de autenticación de espacios de trabajo debe estar configurado en **SAML 2.0**. No utilice Azure AD como método de autenticación. Para cambiar el método de autenticación de espacios de trabajo, vaya a **Configuración de Workspace > Autenticación** en la consola de Citrix Cloud.
- El sufijo UPN `@yourdomain.com` debe importarse y verificarse en Azure AD como nombre de dominio personalizado. En Azure Portal, se encuentra en **Azure Active Directory > Nombres de dominio personalizados**.
- Las identidades de usuario de Azure AD se deben importar de AD mediante Microsoft Azure AD Connect. Esto garantiza que las identidades de los usuarios se importen correctamente y tengan el sufijo UPN correcto. No se admiten usuarios de Azure AD con sufijos UPN `@yourtenant.onmicrosoft.com`.
- Citrix FAS debe implementarse y conectarse a la ubicación de recursos y arrendatarios de Citrix Cloud. FAS proporciona Single Sign-On en aplicaciones y escritorios HDX que se inician desde Citrix Workspace. No es necesario configurar cuentas sombra de AD porque el UPN `user@customerdomain` de las identidades de usuario de AD y Azure AD debe coincidir. FAS genera los certificados de usuario necesarios con el UPN correcto y realiza un inicio de sesión con tarjeta inteligente cuando se inician recursos HDX.

Configurar la aplicación SAML personalizada de Azure AD Enterprise

De forma predeterminada, el comportamiento del inicio de sesión SAML en espacios de trabajo es confirmar la identidad de un usuario de AD. El atributo SAML **cip_directory** es un valor de cadena codificado que es el mismo para todos los suscriptores y actúa como un conmutador. Citrix Cloud y Citrix Workspace detectan este atributo durante el inicio de sesión y activan SAML para confirmarlo con la versión Azure AD de la identidad del usuario. El uso del parámetro **azuread** con este atributo supedita el comportamiento predeterminado de SAML y, en su lugar, activa el uso de SAML en Azure AD.

Aunque los pasos de esta sección son para Azure AD, puede crear una aplicación SAML similar con otro proveedor de SAML 2.0 (por ejemplo, ADFS, Duo, Okta, OneLogin, PingOneSSO, etc.), siempre que realice las mismas tareas. Tu proveedor de SAML debe permitirte configurar un atributo SAML codificado (cip_directory = azuread) en la aplicación SAML. Simplemente cree las mismas asignaciones de atributos SAML que se describen en esta sección.

1. Inicie sesión en Azure Portal.
2. En el menú del portal, seleccione **Azure Active Directory**.
3. En el panel de la izquierda, en **Manage**, seleccione **Enterprise Applications**.
4. En la barra de comandos del panel de trabajo, seleccione **New Application**.
5. En la barra de comandos, seleccione **Create your own application**. No utilice la plantilla de aplicaciones de empresa de SSO SAML de Citrix Cloud. La plantilla no le permite modificar la lista de notificaciones ni los atributos SAML.
6. Introduzca un nombre para la aplicación y, a continuación, seleccione **Integrate any other application you don't find in the gallery (Non-gallery)**. Haga clic en **Crear**. Aparecerá la página de información general de la aplicación.
7. En el panel de la izquierda, seleccione **Single sign-on**. En el panel de trabajo, selecciona **SAML**.
8. En la sección **Basic SAML Configuration**, seleccione **Edit** y configure estos parámetros:

    a) En la sección **Identifier (Entity ID)**, seleccione **Add identifier** y, a continuación, introduzca el valor asociado a la región en la que se encuentra el arrendatario de Citrix Cloud:

    - Para las regiones de la Unión Europea, Estados Unidos y Asia-Pacífico Sur, introduzca `https://saml.cloud.com`.
    - Para la región de Japón, introduzca `https://saml.citrixcloud.jp`.
    - Para la región de Citrix Cloud Government, introduzca `https://saml.cloud.us`.

    b) En la sección **Reply URL (Assertion Consumer Service URL)**, seleccione **Add reply URL** y, a continuación, introduzca el valor asociado a la región en la que se encuentra su arrendatario de Citrix Cloud:

- Para las regiones de la Unión Europea, Estados Unidos y Asia-Pacífico Sur, introduzca `https://saml.cloud.com/saml/acs`.
- Para la región de Japón, introduzca `https://saml.citrixcloud.jp/saml/acs`.
- Para la región de Citrix Cloud Government, introduzca `https://saml.cloud.us/saml/acs`.

c) En la sección **Logout URL (Optional)**, introduzca el valor asociado a la región en la que se encuentra el arrendatario de Citrix Cloud:

- Para las regiones de la Unión Europea, Estados Unidos y Asia-Pacífico Sur, introduzca `https://saml.cloud.com/saml/logout/callback`.
- Para la región de Japón, introduzca `https://saml.citrixcloud.jp/saml/logout/callback`.
- Para la región de Citrix Cloud Government, introduzca `https://saml.cloud.us/saml/logout/callback`.

d) En la barra de comandos, seleccione **Save**.

9. En la sección **Attributes & Claims**, seleccione **Edit** para configurar estas notificaciones. Estas notificaciones aparecen en la aserción SAML incluida en la respuesta SAML.

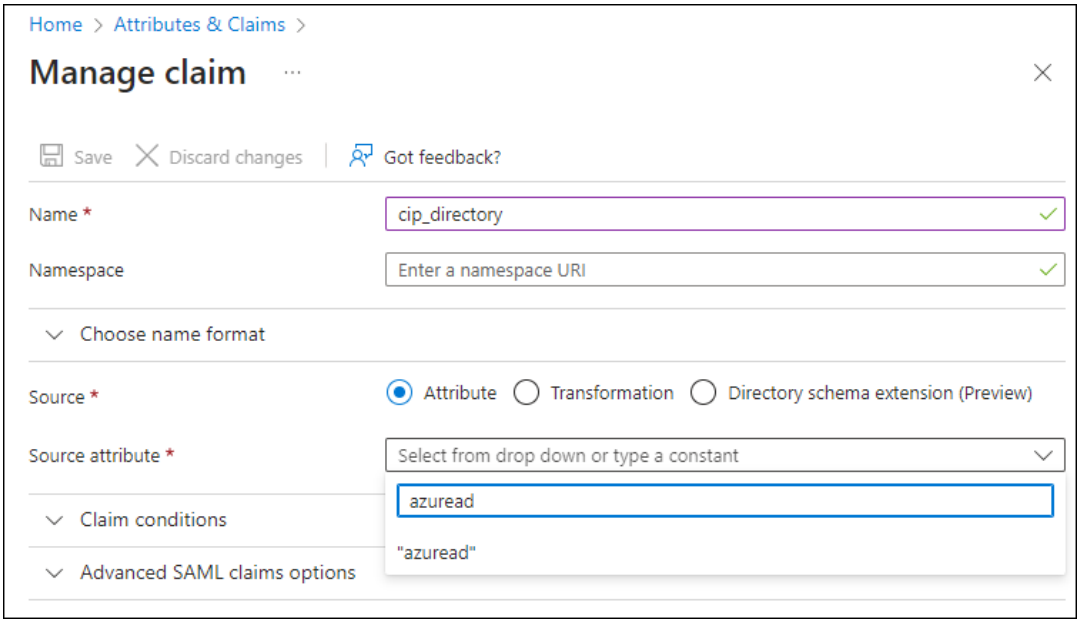
a) Para **Unique User Identifier (Name ID)**, deje el valor predeterminado de `user.userprincipalname`.

b) En la barra de comandos, seleccione **Add new claim**.

c) En **Name**, escriba **cip_directory**.

d) En **Source**, deje la opción **Attribute** seleccionada.

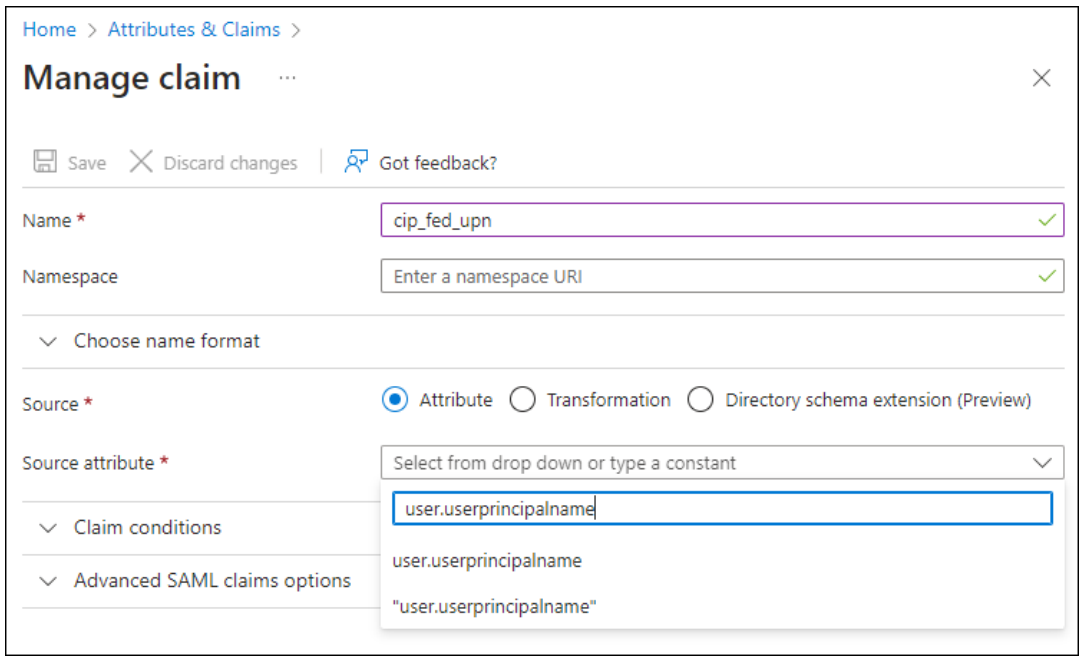
e) En **Source attribute**, introduzca **azuread**. Este valor aparece entre comillas después de introducirlo.



f) En la barra de comandos, seleccione **Save**.

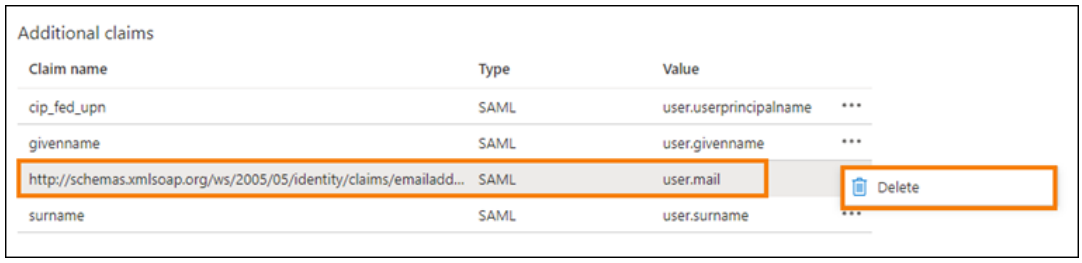
g) Cree notificaciones adicionales con estos valores en los campos **Name** y **Source attribute**:

Nombre	Atributo de origen
cip_fed_upn	user.userprincipalname
displayName	user.displayname
firstName	user.givenname
lastName	user.surname

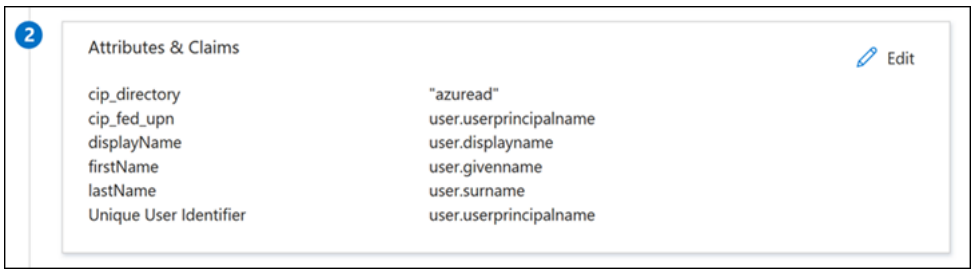


> **Importante:**
>
> Para crear estas notificaciones adicionales, repita los pasos b-f para cada notificación o modifique las notificaciones predeterminadas en la sección **Additional claims** que ya tienen los atributos de origen enumerados en la tabla anterior. Las notificaciones predeterminadas incluyen el espacio de nombres `http://schemas.xmlsoap.org/ws/2005/05/identity/claims`.
>
> Si modifica las notificaciones predeterminadas, debe quitar el espacio de nombres de cada notificación. Si crea notificaciones, debe eliminar las notificaciones que incluyen el espacio de nombres. Si las notificaciones con este espacio de nombres se incluyen en la aserción SAML resultante, dicha aserción no será válida e incluirá nombres de atributos SAML incorrectos.

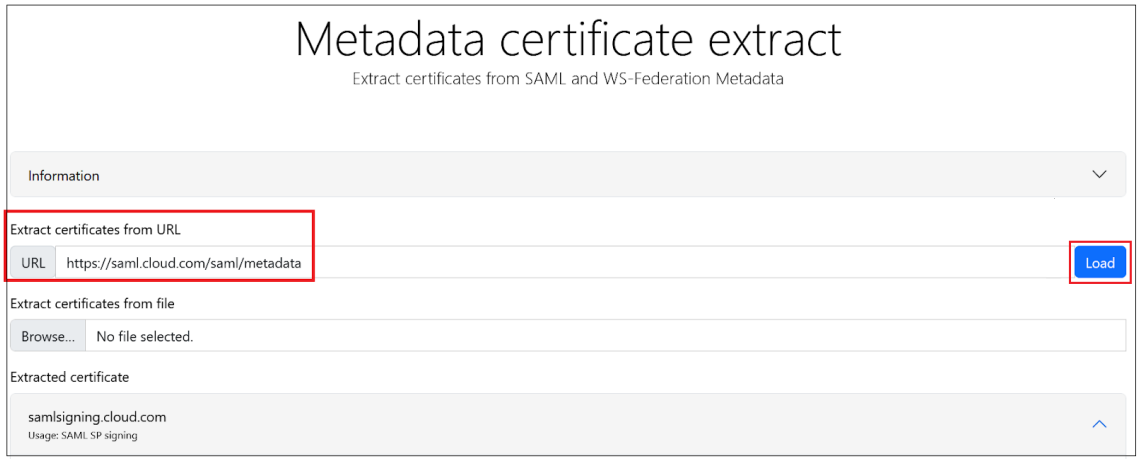
h) En la sección **Additional claims**, para las notificaciones restantes con el espacio de nombres `http://schemas.xmlsoap.org/ws/2005/05/identity/claims`, haga clic en el botón de puntos suspensivos (…) y, a continuación, haga clic en **Delete**.



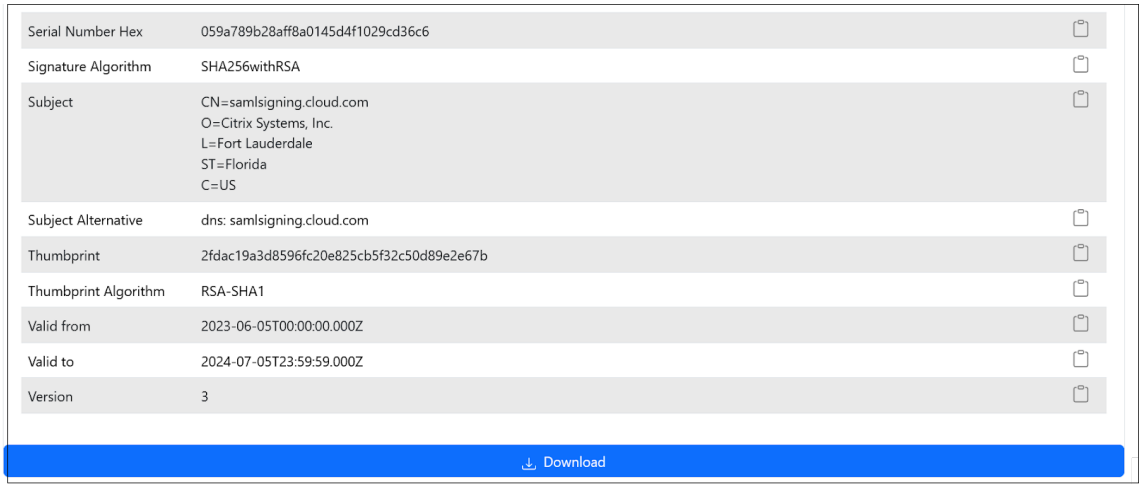
Al terminar, la sección **Attributes & Claims** aparece como se ilustra a continuación:

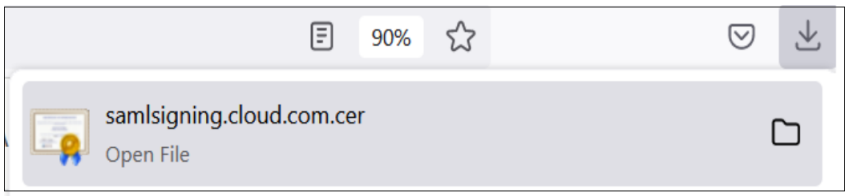


10. Obtenga una copia del certificado de firma SAML de Citrix Cloud con esta herramienta en línea de terceros.
11. Introduzca https://saml.cloud.com/saml/metadata en el campo URL y haga clic en **Cargar**.



12. Desplácese al final de la página y haga clic en **Descargar**.

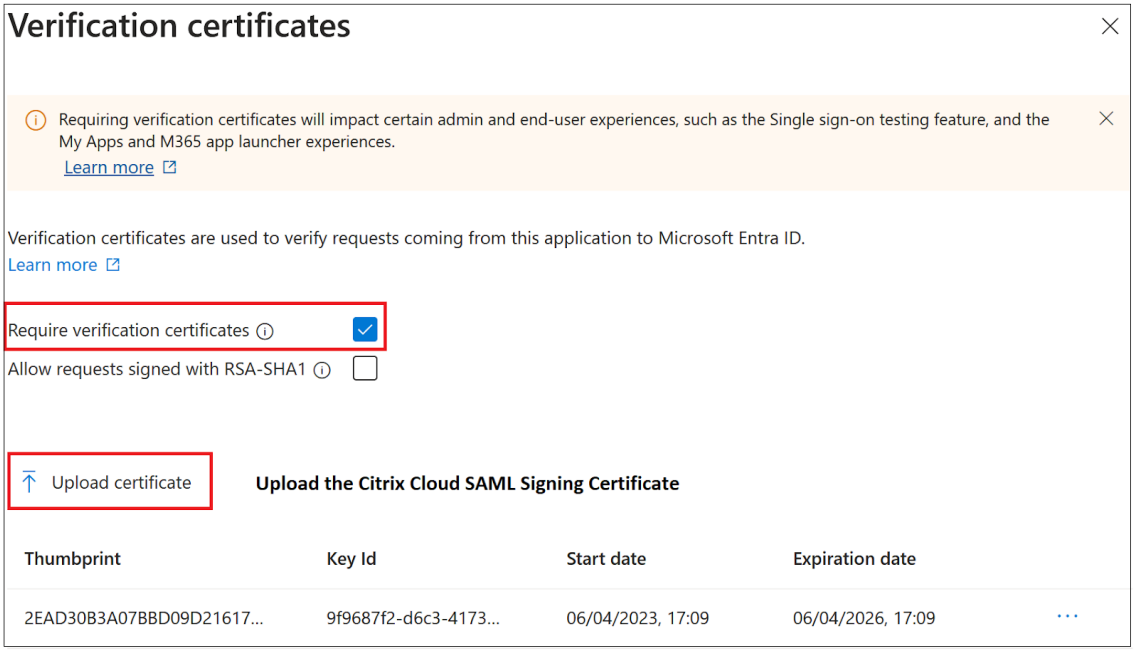


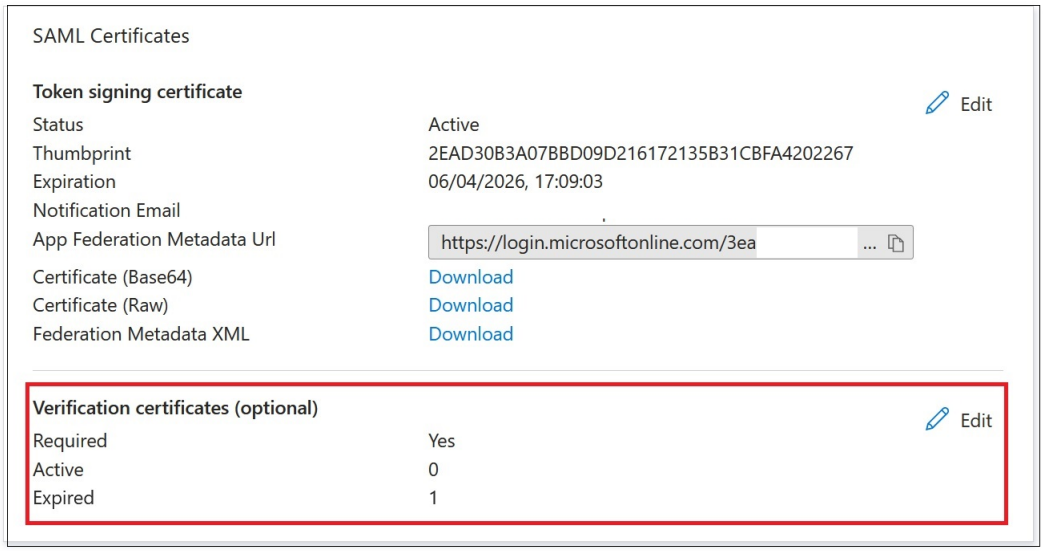


13. Configure los parámetros de firma de la aplicación SAML de Azure Active Directory.

14. Cargue el certificado de firma SAML de producción obtenido en el paso 10 en la aplicación SAML de Azure Active Directory.

    - Habilite **Exigir certificados de verificación**.





Solución de problemas

1. Compruebe que sus aserciones SAML contienen los atributos de usuario correctos mediante una herramienta de red SAML, como la extensión para exploradores web SAML-tracer.
2. Busque la respuesta SAML que se muestra en amarillo y compárela con este ejemplo:

3. Haga clic en la ficha **SAML** del panel inferior para decodificar la respuesta SAML y verla como XML.
4. Desplácese hasta el final de la respuesta y compruebe que la aserción SAML contenga los atributos SAML y los valores de usuario correctos.

Si los suscriptores siguen sin poder iniciar sesión en sus espacios de trabajo, contacte con Citrix Support y proporcione esta información:

- Captura de SAML-tracer
- Fecha y hora en que no se pudo iniciar sesión en Citrix Workspace
- El nombre de usuario afectado
- La dirección IP de la persona que llama del equipo cliente que utilizó para iniciar sesión en Citrix Workspace. Puede usar una herramienta como https://whatismyip.com para obtener esta dirección IP.

SAML con Azure AD e identidades de AD para la autenticación de espacios de trabajo

May 30, 2024

Author:
Mark Dear

En este artículo se describe cómo configurar SAML para la autenticación de espacios de trabajo mediante identidades de Active Directory (AD). El comportamiento predeterminado de la autenticación de Citrix Cloud y SAML en Citrix Workspace o Citrix Cloud, independientemente del proveedor de SAML utilizado, es confirmar la identidad de usuarios de AD. Para la configuración descrita en este artículo, es necesario usar Azure AD Connect para importar identidades de AD a Azure AD.

> **Importante:**
>
> Es fundamental determinar el flujo de SAML adecuado para los usuarios finales de Workspace, ya que afecta directamente a su proceso de inicio de sesión y a la visibilidad de los recursos. La identidad elegida influye en los tipos de recursos a los que puede acceder un usuario final de Workspace.
> Hay un artículo asociado que proporciona instrucciones sobre cómo usar Azure AD como proveedor de SAML para autenticarse en Workspace mediante identidades de AAD. Encontrará instrucciones detalladas en SAML con Azure AD e identidades de AAD para la autenticación de espacios de trabajo.
> Normalmente, los usuarios finales de Workspace suelen necesitar abrir aplicaciones y escritorios proporcionados por los VDA unidos a un dominio de AD. Es fundamental revisar detenidamente los casos de uso descritos en ambos artículos antes de decidir cuál es el flujo de SAML más adecuado para su organización. En caso de duda, Citrix recomienda usar el **flujo SAML de AD** y seguir las instrucciones de este artículo, ya que se ajusta al caso de DaaS más común.

Ámbito de las funciones

Este artículo se aplica a los usuarios que usan esta combinación de funciones de Citrix Cloud y Azure:

- SAML para la autenticación de espacios de trabajo mediante identidades de AD
- Inicio de sesión de administrador de SAML para Citrix Cloud mediante identidades de AD
- Enumeración de recursos de Citrix DaaS y HDX publicados mediante VDA unidos a un dominio de AD
- Enumeración de recursos de VDA unidos a un dominio de AD

¿Qué es mejor: identidades de AD o identidades de Azure AD?

Para determinar si los usuarios de su espacio de trabajo deben autenticarse mediante identidades SAML de AD o SAML de Azure AD:

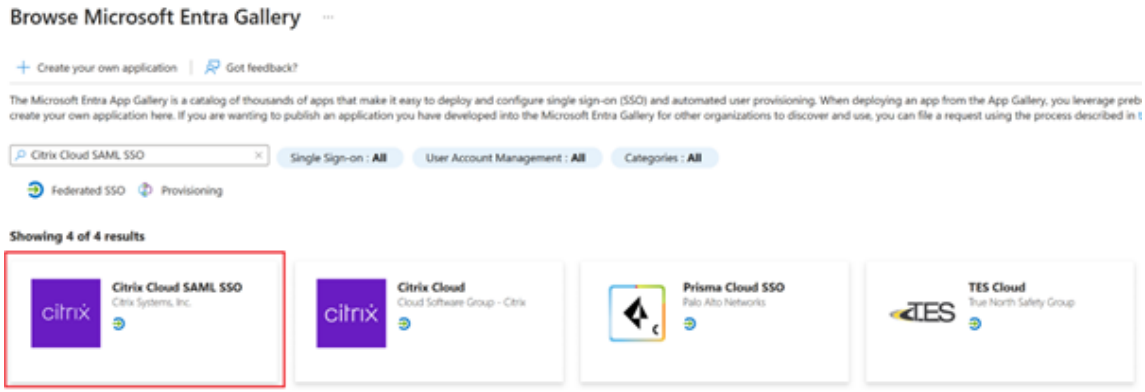
1. Decida qué combinación de recursos quiere poner a disposición de sus usuarios en Citrix Workspace.
2. Use esta tabla para determinar qué tipo de identidad de usuario es adecuado para cada tipo de recurso.

Tipo de recurso (VDA)	Identidad del usuario al iniciar sesión en Citrix Workspace	¿Necesita una identidad SAML con Azure AD?	¿FAS proporciona Single Sign-On (SSO) a VDA?
Unida a AD	AD, Azure AD importado de AD (contiene SID)	No. Use el SAML predeterminado.	Sí

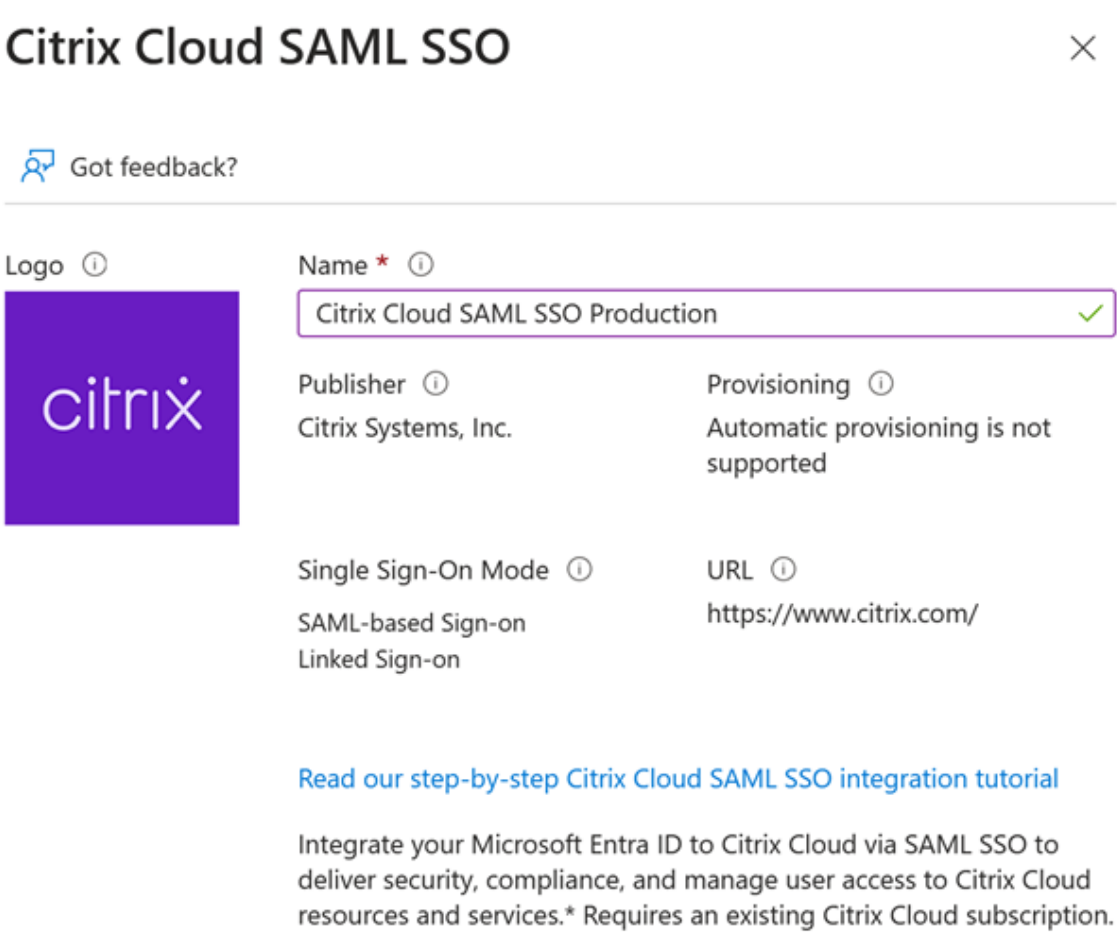
Configurar la aplicación SAML personalizada de Azure AD Enterprise

De forma predeterminada, el comportamiento del inicio de sesión SAML en espacios de trabajo es confirmar la identidad de un usuario de AD.

1. Inicie sesión en Azure Portal.
2. En el menú del portal, seleccione **Azure Active Directory**.
3. En el panel de la izquierda, en **Manage**, seleccione **Enterprise Applications**.
4. En el cuadro de búsqueda, introduzca `Citrix Cloud SAML SSO` para buscar la plantilla de aplicación SAML para Citrix.



5. Introduzca un nombre adecuado para la aplicación SAML, como `Citrix Cloud SAML SSO Production`



6. En el panel de navegación izquierdo, seleccione **Inicio de sesión único** y, en el panel de trabajo, haga clic en **SAML**.
7. En la sección **Basic SAML Configuration**, haga clic en **Edit** y configure estos parámetros:

   a) En la sección **Identifier (Entity ID)**, seleccione **Add identifier** y, a continuación, introduzca el valor asociado a la región en la que se encuentra el arrendatario de Citrix Cloud:
   - Para las regiones de Europa, Estados Unidos y Asia-Pacífico Sur, introduzca `https://saml.cloud.com`.
   - Para la región de Japón, introduzca `https://saml.citrixcloud.jp`.
   - Para la región de Citrix Cloud Government, introduzca `https://saml.cloud.us`.

   b) En la sección **Reply URL (Assertion Consumer Service URL)**, seleccione **Add reply URL** y, a continuación, introduzca el valor asociado a la región en la que se encuentra su arrendatario de Citrix Cloud:
   - Para las regiones de Europa, Estados Unidos y Asia-Pacífico Sur, introduzca `https://saml.cloud.com/saml/acs`.
   - Para la región de Japón, introduzca `https://saml.citrixcloud.jp/saml/acs`.

- Para la región de Citrix Cloud Government, introduzca `https://saml.cloud.us/saml/acs`.

c) En la sección **URL de inicio de sesión**, introduzca la URL de su espacio de trabajo.

d) En la sección **Logout URL (Optional)**, introduzca el valor asociado a la región en la que se encuentra el arrendatario de Citrix Cloud:

- Para las regiones de Europa, Estados Unidos y Asia-Pacífico Sur, introduzca `https://saml.cloud.com/saml/logout/callback`.
- Para la región de Japón, introduzca `https://saml.citrixcloud.jp/saml/logout/callback`.
- Para la región de Citrix Cloud Government, introduzca `https://saml.cloud.us/saml/logout/callback`.

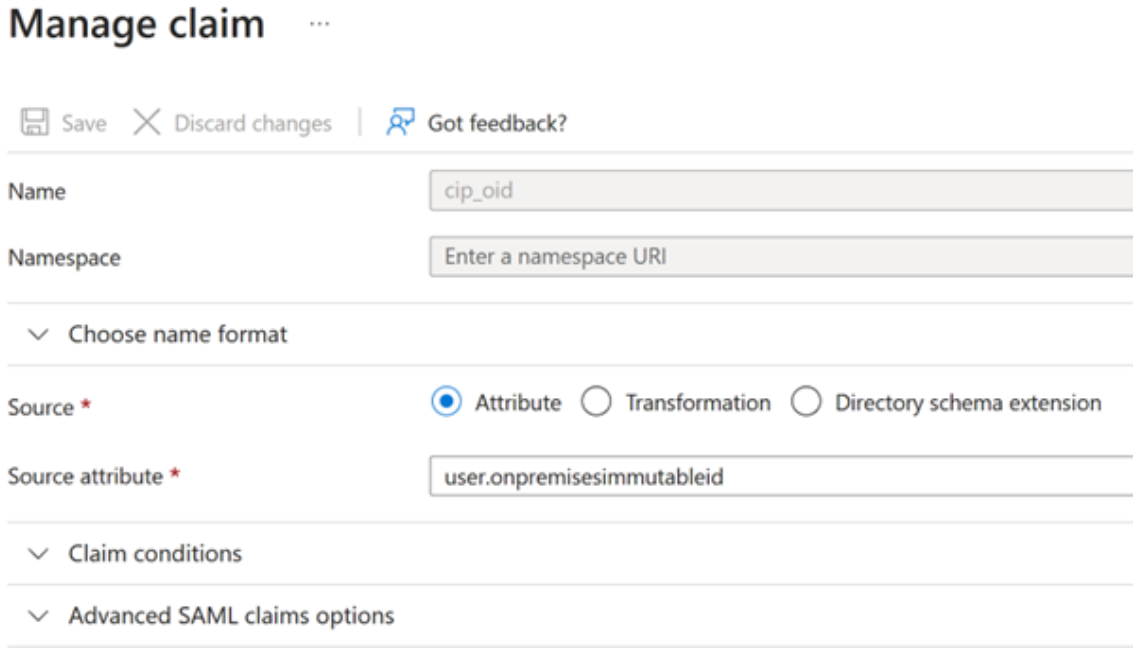
e) En la barra de comandos, haga clic en **Guardar**. La sección **Configuración básica de SAML** se muestra de esta manera:

8. En la sección **Attributes & Claims**, haga clic en **Edit** para configurar estas notificaciones. Estas notificaciones aparecen en la aserción SAML incluida en la respuesta SAML. Tras crear la aplicación SAML, configure estos atributos.

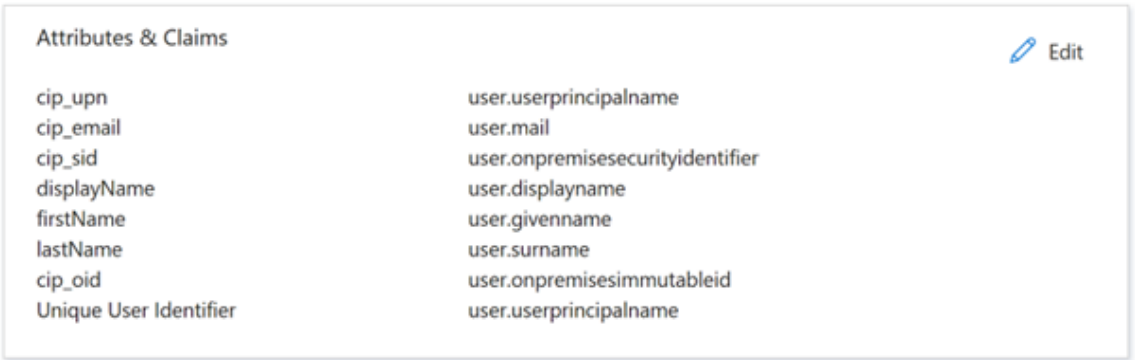
a) Para la notificación **Unique User Identifier (Name ID)**, deje el valor predeterminado de `user.userprincipalname`.

b) Para la notificación **cip_upn**, deje el valor predeterminado de `user.userprincipalname`.

c) Para la notificación **cip_email**, deje el valor predeterminado de `user.mail`.
d) Para la notificación **cip_sid**, deje el valor predeterminado de `user.onpremisesecurityidentit` .
e) Para la notificación **cip_oid**, modifique la notificación existente y seleccione **Atributo de origen**. Busque la cadena `object` y seleccione `user.onpremisesimmutableid`.



a) Para **displayName**, deje el valor predeterminado de `user.displayname`.
b) En la sección **Additional claims**, para las notificaciones restantes con el espacio de nombres `http://schemas.xmlsoap.org/ws/2005/05/identity/claims`, haga clic en el botón de puntos suspensivos (…) y, a continuación, haga clic en **Delete**. No es necesario incluir estas notificaciones, ya que son duplicados de los atributos de usuario anteriores.

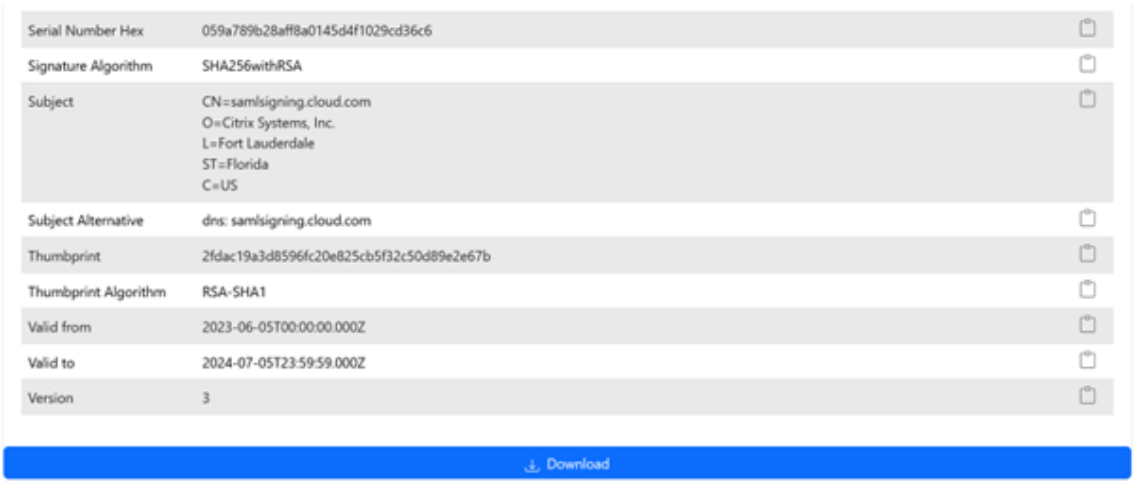


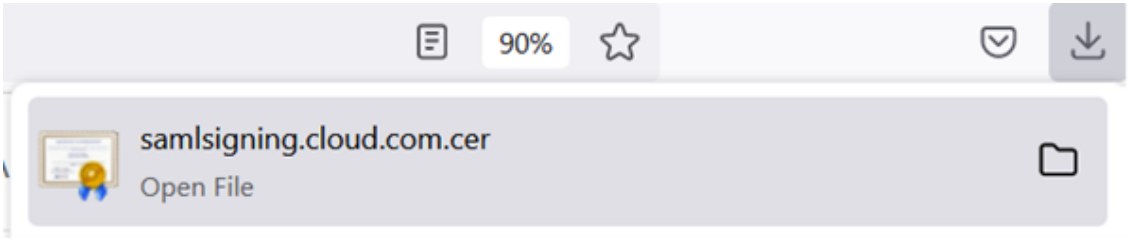
Al terminar, la sección **Attributes & Claims** aparece como se ilustra a continuación:

a) Obtenga una copia del certificado de firma SAML de Citrix Cloud con esta herramienta en línea de terceros.

b) Introduzca `https://saml.cloud.com/saml/metadata` en el campo URL y haga clic en **Cargar**.

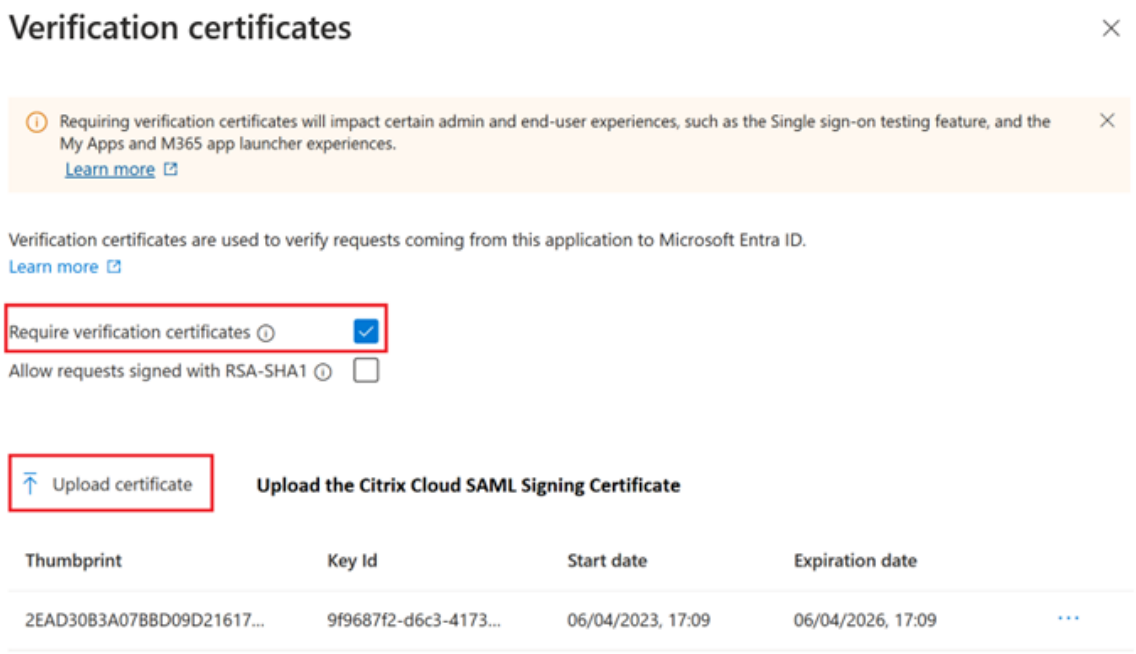
9. Desplácese al final de la página y haga clic en **Descargar**.

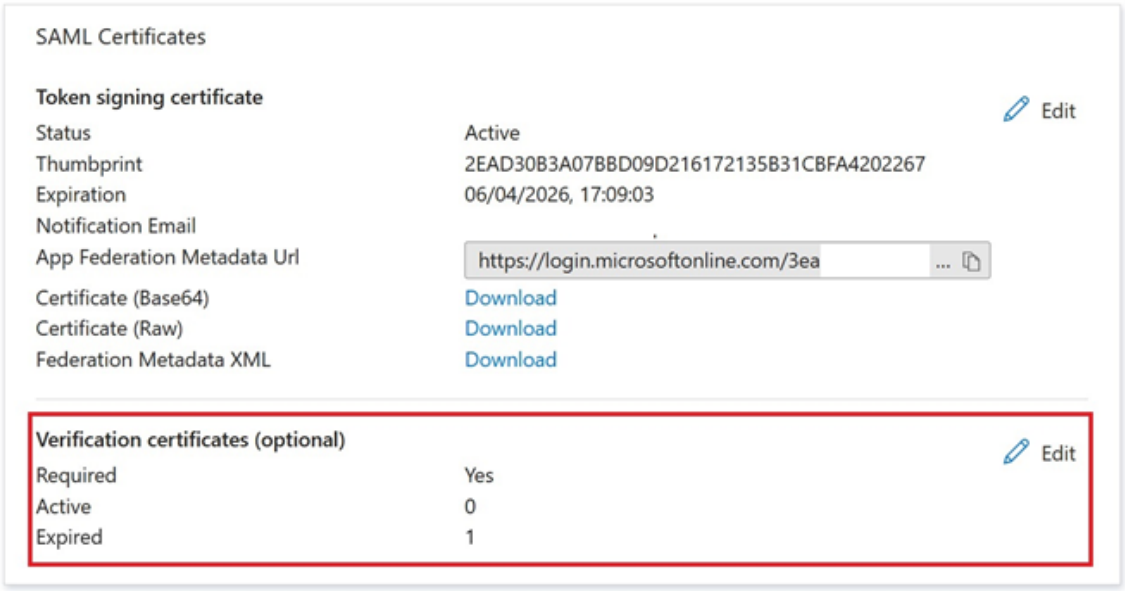




10. Configure los parámetros de firma de la aplicación SAML de Azure Active Directory.
11. Cargue el certificado de firma SAML de producción obtenido en el paso 10 en la aplicación SAML de Azure Active Directory

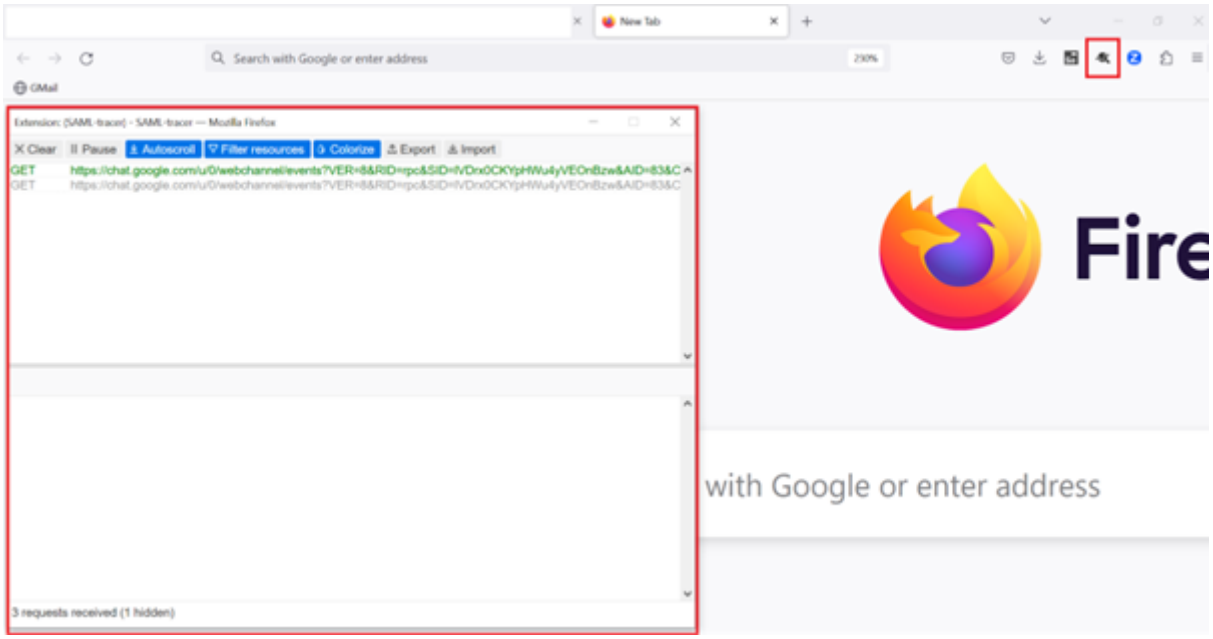
    a) Habilite **Exigir certificados de verificación**.





Solución de problemas

1. Compruebe que sus aserciones SAML contienen los atributos de usuario correctos mediante una herramienta de red SAML, como la extensión para exploradores web SAML-tracer.



1. Busque la respuesta SAML que se muestra en amarillo y compárela con este ejemplo:

2. Haga clic en la ficha **SAML** del panel inferior para decodificar la respuesta SAML y verla como XML.
3. Desplácese hasta el final de la respuesta y compruebe que la aserción SAML contenga los atributos SAML y los valores de usuario correctos.

Si sus suscriptores siguen sin poder iniciar sesión en su espacio de trabajo o no pueden ver sus escritorios de Citrix HDX Plus para Windows 365, contacte con Citrix Support y proporcione esta información:

- Captura de SAML-tracer
- Fecha y hora en que no se pudo iniciar sesión en Citrix Workspace
- El nombre de usuario afectado
- La dirección IP de la persona que llama del equipo cliente que utilizó para iniciar sesión en Citrix Workspace. Puede usar una herramienta como https://whatismyip.com para obtener esta dirección IP.

Configurar SAML simplificado para uso con usuarios de SAML nativos e invitados

July 2, 2024

Author:
Mark Dear, Javier Lopez Santacruz

Antes de seguir con este artículo, es esencial que comprenda si "SAML simplificado"es apropiado para su caso de uso de autenticación. Lea detenidamente las descripciones de los casos de uso y las preguntas frecuentes antes de decidir si implementar esta solución SAML para casos de uso en particular. Antes de continuar, asegúrese de que entiende perfectamente los casos en los que SAML simplificado es apropiado y los tipos de identidades que debe usar. La mayoría de los casos de uso de SAML se pueden completar siguiendo otros artículos sobre SAML y enviando los cuatro atributos cip_* para la autenticación.

> **Nota:**
>
> El uso de "SAML simplificado"aumenta la carga que soportan los Citrix Cloud Connectors, ya que tienen que buscar, el SID, el OID y el correo electrónico de los usuarios para cada inicio de sesión de usuario final en Workspace, en lugar de buscar estos valores en la aserción SAML. Desde el punto de vista del rendimiento del Citrix Cloud Connector, es preferible enviar los cuatro atributos cip_* en la aserción SAML si realmente no se requiere SAML simplificado.

Requisitos previos

- Una aplicación SAML configurada específicamente para usarse con SAML simplificado que solo envía **cip_upn** para la autenticación dentro de la aserción SAML.
- Usuarios de front-end de su proveedor de SAML.
- Una ubicación de recursos que contenga un par de Citrix Cloud Connectors unidos al bosque y al dominio de AD donde se crean las cuentas sombra de AD.
- Sufijos de UPN alternativos agregados al bosque de AD del back-end donde se crean las cuentas sombra de AD.
- Cuentas sombra de AD del back-end con UPN coincidentes.
- Recursos de DaaS o CVAD asignados a los usuarios de las cuentas sombra de AD.
- Uno o más servidores FAS vinculados a la misma ubicación de recursos.

Preguntas frecuentes

¿Por qué debo usar SAML simplificado?

Es muy común que las grandes organizaciones inviten a contratistas y empleados temporales a su plataforma de identidades. El objetivo es conceder al contratista acceso temporal a Citrix Workspace usando la identidad existente del usuario, como la dirección de correo electrónico del contratista o una dirección de correo electrónico ajena a la organización. SAML simplificado permite el uso de iden-

tidades de front-end nativas o de invitado que no existen en el dominio de AD donde se publican los recursos de DaaS.

¿Qué es SAML simplificado?

Normalmente, al iniciar sesión en Citrix Workspace, se usan cuatro atributos cip_* de SAML y sus correspondientes atributos de usuario de AD para autenticar al usuario final. Se espera que estos cuatro atributos SAML estén presentes en la aserción SAML y se rellenen con atributos de usuario de AD. SAML simplificado hace referencia al hecho de que solo se requiere el atributo cip_upn de SAML para que la autenticación funcione correctamente.

Atributo de AD	Nombre de atributo predeterminado en la aserción SAML
userPrincipalName	cip_upn
Mail	cip_email
objectSID	cip_sid
objectGUID	cip_oid

Los otros tres atributos de usuario de AD, ObjectSID, ObjectGUID y Mail, necesarios para la autenticación, se obtienen mediante los Citrix Cloud Connectors unidos al dominio de AD donde reside la cuenta sombra de AD. Ya no es necesario incluirlos en la aserción SAML durante un flujo de inicio de sesión de SAML para Workspace o Citrix Cloud.

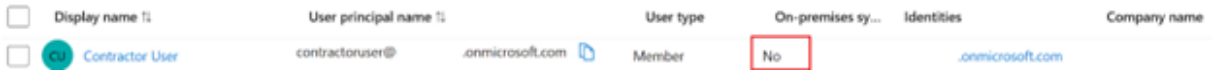
Atributo de AD	Nombre de atributo predeterminado en la aserción SAML
userPrincipalName	cip_upn

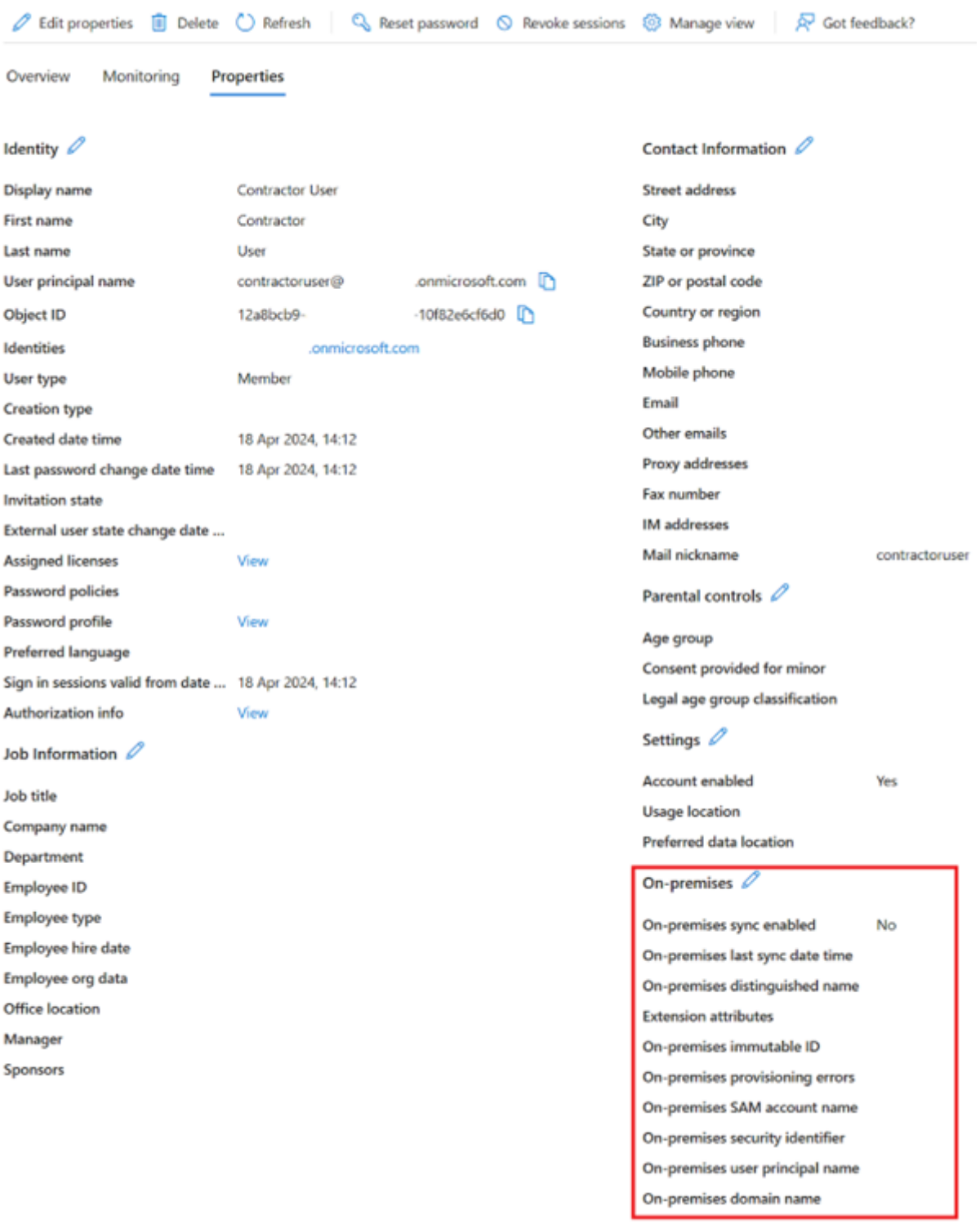
> **Importante:**
>
> Sigue siendo necesario enviar el nombre simplificado, **displayName**, para todos los flujos de SAML, incluido SAML simplificado. La interfaz de usuario de Workspace requiere **displayName** para mostrar correctamente el nombre completo del usuario de Workspace.

¿Qué es una identidad de usuario de SAML nativa?

Un usuario de SAML nativo es una identidad de usuario que solo existe en el directorio de su proveedor de SAML, por ejemplo, Entra ID u Okta. Estas identidades no contienen atributos de usuario locales,

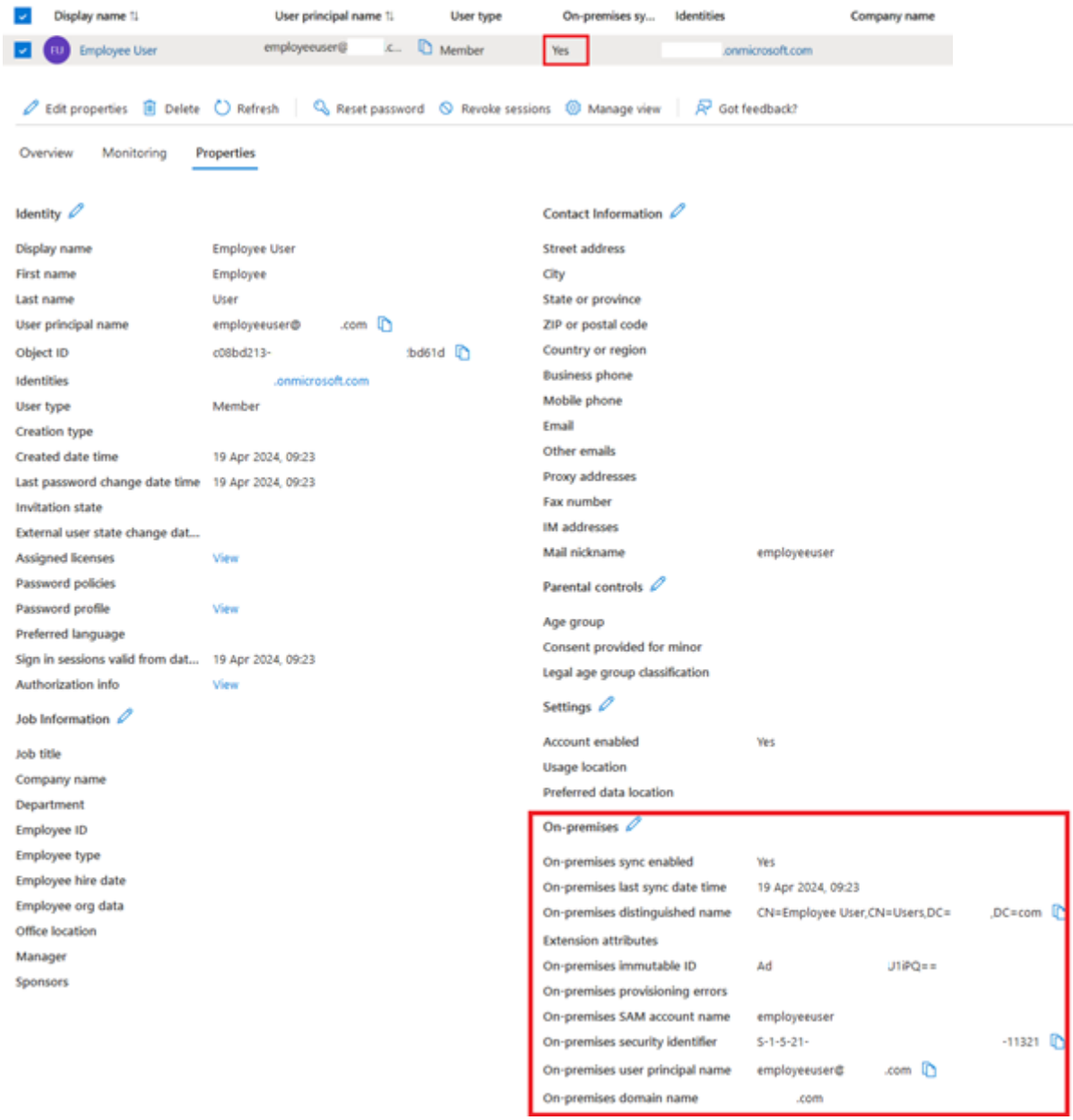
ya que no se crean mediante herramientas de sincronización de AD como Entra ID Connect. Requieren cuentas sombra de back-end de AD coincidentes para poder enumerar e iniciar los recursos de DaaS. El usuario de SAML nativo debe estar asignado a la cuenta correspondiente dentro de Active Directory.





¿Qué es una identidad de usuario de SAML respaldada por AD?

Un usuario de SAML respaldado por AD es una identidad de usuario que existe en el directorio de su proveedor de SAML, como Entra ID u Okta, y también en su bosque de AD local. Estas identidades contienen atributos de usuario locales, ya que se crean mediante herramientas de sincronización de AD como Entra ID Connect. No se requieren cuentas sombra de back-end de AD para estos usuarios, ya que contienen SID y OID locales y, por lo tanto, pueden enumerar e iniciar recursos de DaaS.

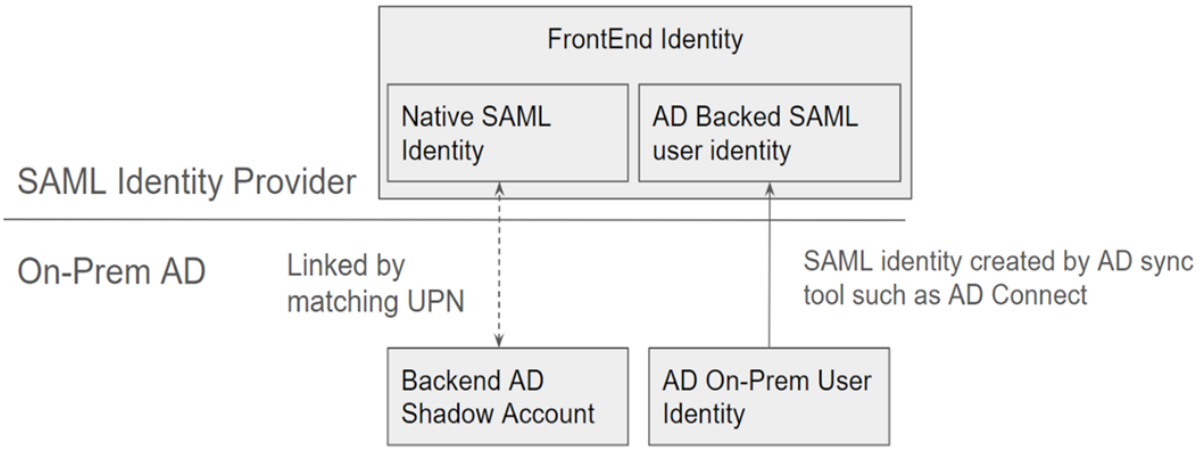


¿Qué es una identidad de front-end?

Una identidad de front-end es la identidad que se usa para iniciar sesión tanto en el proveedor de SAML como en Workspace. Las identidades de front-end tienen diferentes atributos de usuario en función de cómo se crearon en el proveedor de SAML.

1. Identidad de usuario de SAML nativa
2. Identidad de usuario de SAML respaldada por AD

Su proveedor de SAML puede tener una combinación de estos dos tipos de identidades. Por ejemplo, si tiene contratistas y empleados permanentes en su plataforma de identidades, SAML simplificado funcionará para ambos tipos de identidades de front-end, pero solo es obligatorio si tiene algunas cuentas que son de tipo identidad de usuario de SAML nativa.



¿Qué es una cuenta sombra de AD de back-end?

Una cuenta sombra de AD de back-end es una cuenta de AD que DaaS usa, la cual se asigna a la identidad de front-end correspondiente dentro de su proveedor de SAML.

¿Por qué son necesarias las cuentas sombra de AD de back-end?

Para enumerar los recursos de DaaS o CVAD publicados mediante los VDA unidos a un dominio de AD, se requieren las cuentas de AD del bosque de Active Directory a las que están unidos los VDA. Asigne los recursos de su grupo de entrega de DaaS a los usuarios de cuentas sombra y a los grupos de AD que contengan cuentas sombra en el dominio de AD al que unió sus VDA.

> **Importante:**
>
> Solo los usuarios nativos de SAML sin atributos de dominio de AD necesitan cuentas sombra de AD coincidentes. Si sus identidades de front-end se importan de Active Directory, no necesita

> usar SAML simplificado ni crear cuentas sombra de AD de back-end.

¿Cómo vinculamos la identidad de front-end a la cuenta sombra de AD de back-end correspondiente?

Para vincular la identidad del front-end a la identidad del back-end se usan UPN coincidentes. Las dos identidades vinculadas deben tener UPN idénticos para que Workspace pueda saber que representan al mismo usuario final que necesita iniciar sesión en Workspace y enumerar e iniciar los recursos de DaaS.

¿Se necesita Citrix FAS para SAML simplificado?

Sí. Se requiere Servicio de autenticación federada (FAS) para el inicio único de sesión en el VDA cuando se usa cualquier método de autenticación federada para iniciar sesión en Workspace.

¿Qué es el "problema de discordancia de SID"y cuándo puede ocurrir?

El "problema de discordancia de SID"se produce cuando la aserción SAML contiene un SID para un usuario de front-end que no coincide con el SID del usuario de la cuenta sombra de AD. Esto puede ocurrir cuando la cuenta que inicia sesión en su proveedor de SAML tiene un SID local distinto del SID de usuario de la cuenta sombra. Esto solo puede ocurrir cuando la identidad de front-end se aprovisiona mediante herramientas de sincronización de AD, como Entra ID Connect, y desde un bosque de AD diferente de aquel en el que se creó la cuenta sombra.

SAML simplificado impide que se produzca el "problema de discordancia de SID". Se obtiene siempre el SID correcto para el usuario de la cuenta sombra a través de los Citrix Cloud Connectors unidos al dominio de AD de back-end. La búsqueda de usuarios de cuentas sombra se realiza mediante el UPN de usuario del front-end, que se empareja con su usuario de la cuenta sombra del back-end correspondiente.

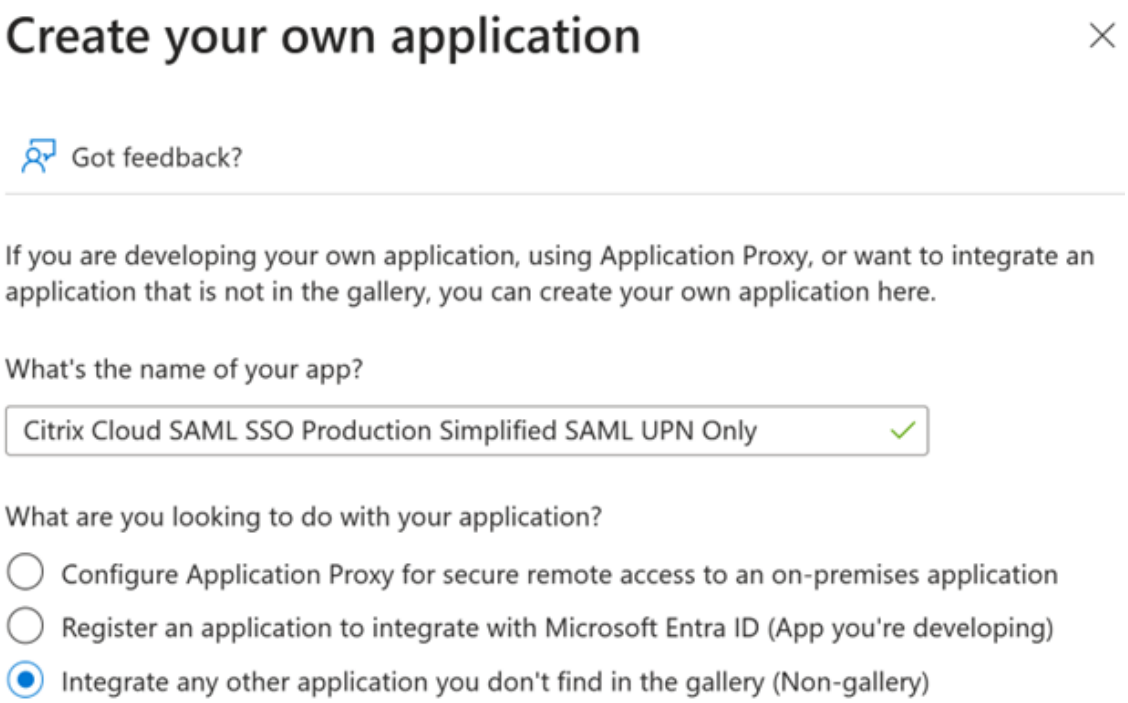
Ejemplo del problema de discordancia del SID:
El usuario del front-end lo creó Entra ID Connect y se sincroniza con el **bosque 1 de AD**.
`S-1-5-21-000000000-0000000000-0000000001-0001`

El usuario de la cuenta sombra del back-end se creó en el **bosque 2 de AD** y se asignó a recursos de DaaS
`S-1-5-21-000000000-0000000000-0000000002-0002`

La aserción SAML contiene los cuatro atributos cip_* y **cip_sid** contiene el valor `S-1-5-21-000000000-00000`
, que no coincide con el SID de la cuenta sombra y desencadena un error.

Configurar SAML simplificado con Entra ID para cuentas de invitados externos

1. Inicie sesión en Azure Portal.
2. En el menú del portal, seleccione **Entra ID**.
3. En el panel de la izquierda, en **Manage**, seleccione **Enterprise Applications**.
4. Seleccione **Create your own application**.
5. Introduzca un nombre adecuado para la aplicación SAML, como `Citrix Cloud SAML SSO Production Simplified SAML`.



6. En el panel de navegación izquierdo, seleccione **Single sign-on** y, en el panel de trabajo, haga clic en **SAML**.
7. En la sección **Basic SAML Configuration**, haga clic en **Edit** y configure estos parámetros:
   a) En la sección **Identifier (Entity ID)**, seleccione **Add identifier** y, a continuación, introduzca el valor asociado a la región en la que se encuentra el arrendatario de Citrix Cloud:
      - Para las regiones de Europa, Estados Unidos y Asia-Pacífico Sur, introduzca `https://saml.cloud.com`.
      - Para la región de Japón, introduzca `https://saml.citrixcloud.jp`.
      - Para la región de Citrix Cloud Government, introduzca `https://saml.cloud.us`.
   b) En la sección **Reply URL (Assertion Consumer Service URL)**, seleccione **Add reply URL** y, a continuación, introduzca el valor asociado a la región en la que se encuentra su arrendatario de Citrix Cloud:

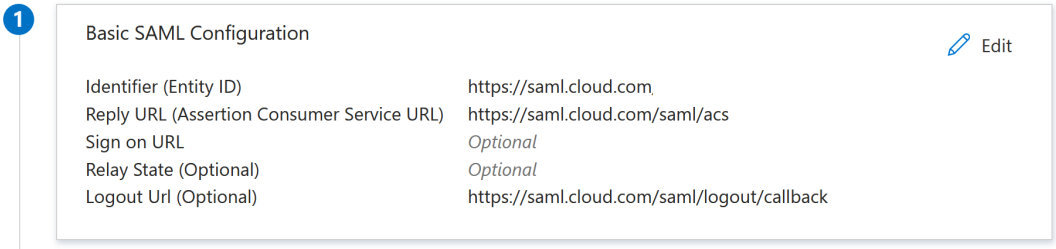
- Para las regiones de Europa, Estados Unidos y Asia-Pacífico Sur, introduzca `https://saml.cloud.com/saml/acs`.
- Para la región de Japón, introduzca `https://saml.citrixcloud.jp/saml/acs`.
- Para la región de Citrix Cloud Government, introduzca `https://saml.cloud.us/saml/acs`.

c) En la sección **URL de inicio de sesión**, introduzca la URL de su espacio de trabajo.

d) En la sección **Logout URL (Optional)**, introduzca el valor asociado a la región en la que se encuentra el arrendatario de Citrix Cloud:

- Para las regiones de Europa, Estados Unidos y Asia-Pacífico Sur, introduzca `https://saml.cloud.com/saml/logout/callback`.
- Para la región de Japón, introduzca `https://saml.citrixcloud.jp/saml/logout/callback`.
- Para la región de Citrix Cloud Government, introduzca `https://saml.cloud.us/saml/logout/callback`.

e) En la barra de comandos, haga clic en **Guardar**. La sección **Configuración básica de SAML** se muestra de esta manera:



8. En la sección **Attributes & Claims**, haga clic en **Edit** para configurar estas notificaciones. Estas notificaciones aparecen en la aserción SAML incluida en la respuesta SAML. Tras crear la aplicación SAML, configure estos atributos.

a) Para la notificación **Unique User Identifier (Name ID)**, deje el valor predeterminado de `user.userprincipalname`.

b) Para la notificación **cip_upn**, deje el valor predeterminado de `user.userprincipalname`.

c) Para **displayName**, deje el valor predeterminado de `user.displayname`.

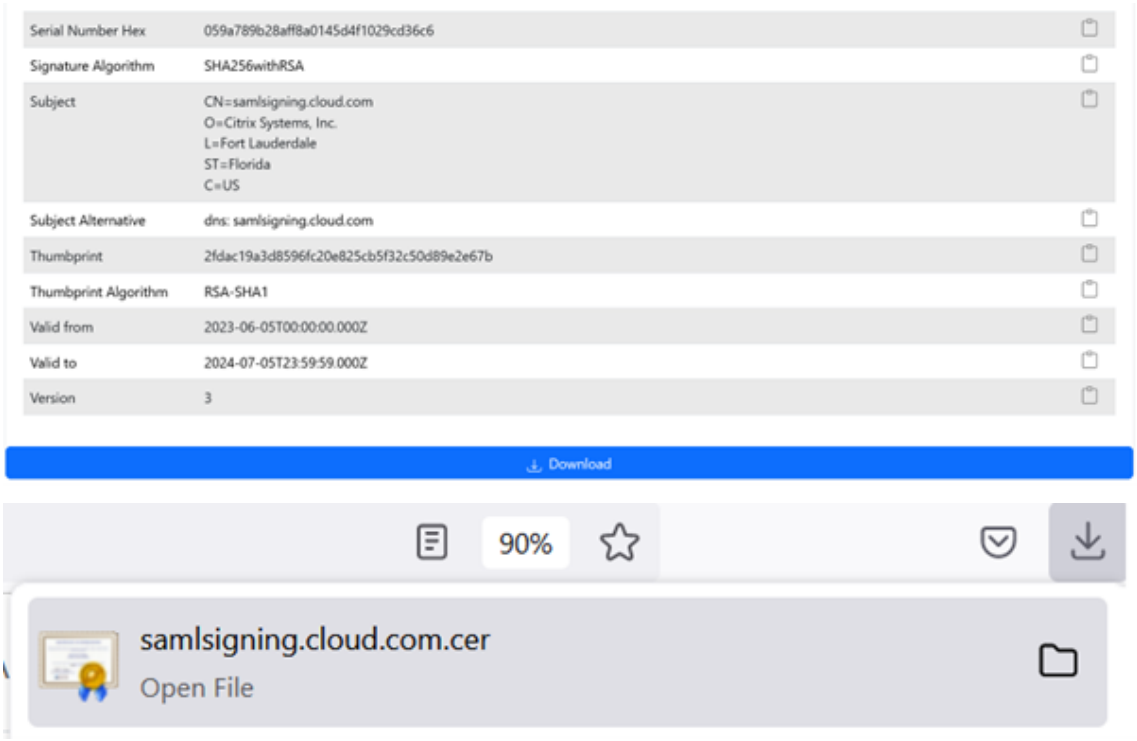
d) En la sección **Additional claims**, para las notificaciones restantes con el espacio de nombres `http://schemas.xmlsoap.org/ws/2005/05/identity/claims`, haga clic en el botón de puntos suspensivos (…) y, a continuación, haga clic en **Delete**. No es necesario incluir estas notificaciones, ya que son duplicados de los atributos de usuario anteriores.

Al terminar, la sección **Attributes & Claims** aparece como se ilustra a continuación:

e) Obtenga una copia del certificado de firma SAML de Citrix Cloud con esta herramienta en línea de terceros.

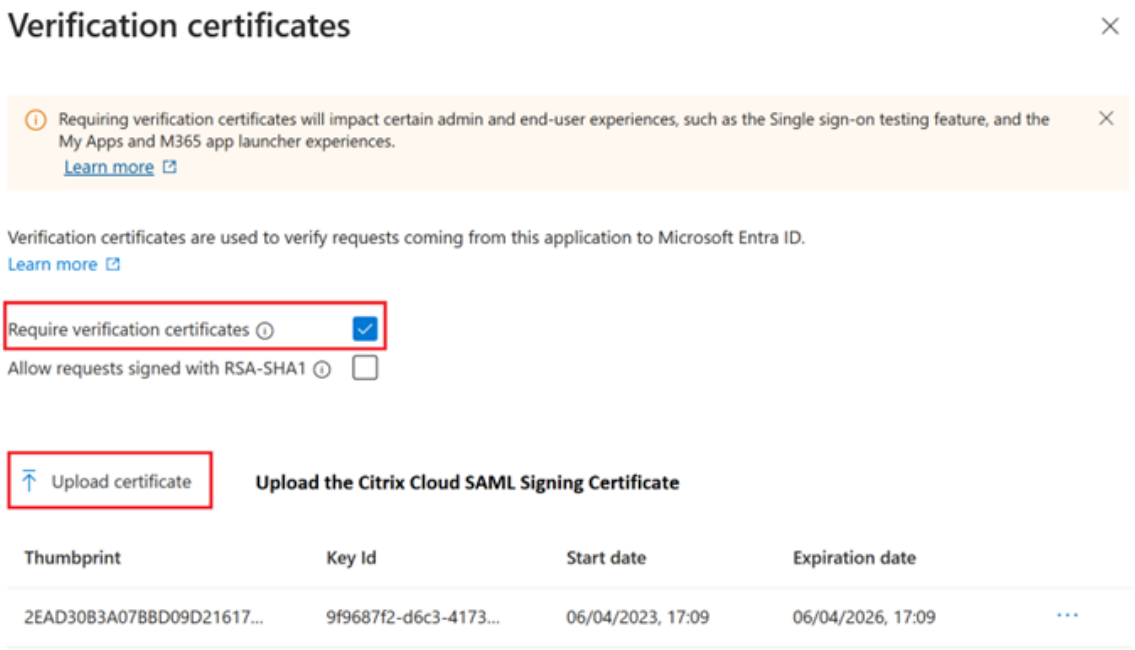
f) Introduzca `https://saml.cloud.com/saml/metadata` en el campo URL y haga clic en **Cargar**.

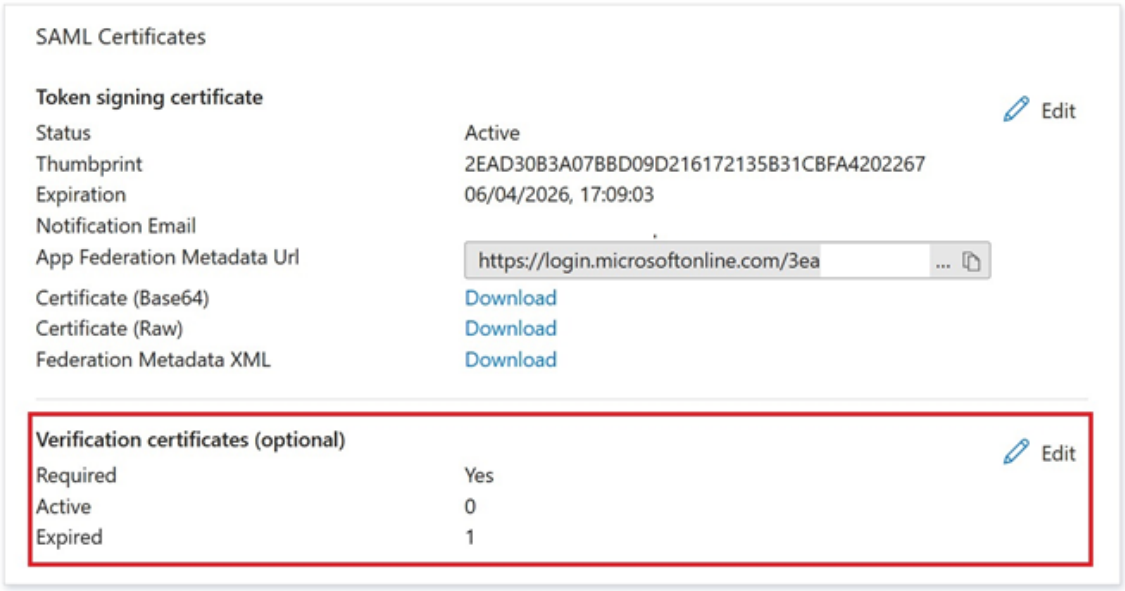
9. Desplácese al final de la página y haga clic en **Descargar**.



10. Configure los parámetros de firma de la aplicación SAML de Azure Active Directory.
11. Cargue el certificado de firma SAML de producción obtenido en el paso 10 en la aplicación SAML de Azure Active Directory

    a) Habilite **Exigir certificados de verificación**.

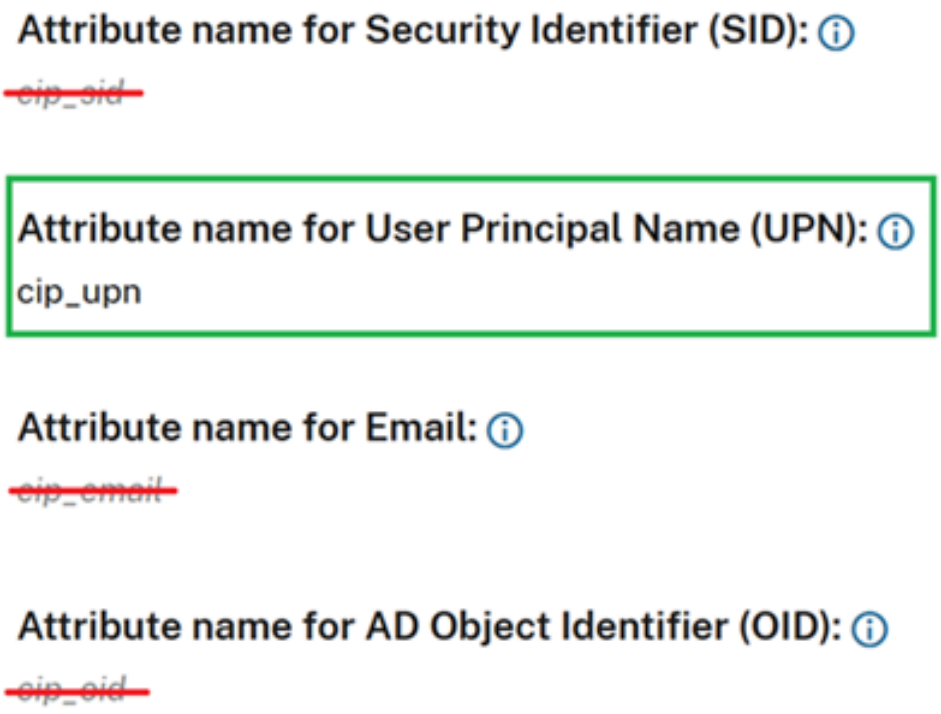




Configurar la conexión de SAML simplificado de Citrix Cloud

De forma predeterminada, Citrix Cloud espera que cip_upn, cip_email, cip_sid y cip_oid estén presentes en la aserción SAML y no podrá iniciar sesión en SAML si no se envían estos atributos. Para evitarlo, quite las comprobaciones de estos atributos cuando cree la nueva conexión SAML.

1. Cree una nueva conexión SAML con los parámetros predeterminados.
2. Vaya a la sección **SAML Attribute Mappings Configuration** en la parte inferior y haga los cambios necesarios antes de guardar la nueva configuración de SAML.
3. Quite el nombre del atributo SAML de cada uno de los campos **cip_email**, **cip_sid** y **cip_oid**.
4. No quite **cip_upn** de su campo.
5. No quite ningún otro atributo de sus campos respectivos. La interfaz de usuario de Workspace sigue necesitando **displayName** y no debe cambiarse.



Configure la ubicación de recursos y los conectores de su cuenta sombra de AD

Se requiere una ubicación de recursos y un par de conectores dentro del bosque de AD de la cuenta oculta del back-end. Citrix Cloud requiere conectores de este bosque de AD para buscar las identidades y los atributos de los usuarios de las cuentas sombra, como cip_email, cip_sid y cip_oid, cuando solo se proporciona cip_upn directamente en la aserción SAML.

1. Cree una nueva **ubicación de recursos** que contenga Citrix Cloud Connectors unidos al bosque de AD de la cuenta sombra del back-end.

2. Asigne un nombre a la ubicación de recursos, de manera que coincida con el bosque de AD que contiene las cuentas sombras de AD del back-end que quiere usar.
3. Configure un par de Citrix Cloud Connectors en la ubicación de recursos recién creada.

Por ejemplo
ccconnector1.shadowaccountforest.com
ccconnector2.shadowaccountforest.com

Configurar FAS en el bosque de AD del back-end

Los usuarios contratistas del front-end definitivamente necesitarán FAS. Durante los inicios de DaaS, los usuarios contratistas no podrán introducir manualmente las credenciales de Windows para completar el inicio, ya que es probable que no conozcan la contraseña de la cuenta sombra de AD.

1. Configure uno o más servidores de FAS en el bosque de AD del back-end donde se crearon las cuentas sombra.
2. Vincule los servidores de FAS a la misma ubicación de recursos que contiene un par de Citrix Cloud Connectors unidos al bosque de AD del back-end donde se crearon las cuentas sombra.

Configurar sufijos de UPN alternativos en su dominio de AD

> **Importante:**
>
> Un UPN no es lo mismo que la dirección de correo electrónico del usuario. En muchos casos, tienen el mismo valor para facilitar su uso, pero UPN y correo electrónico tienen diferentes usos internos y se definen en diferentes atributos de Active Directory.

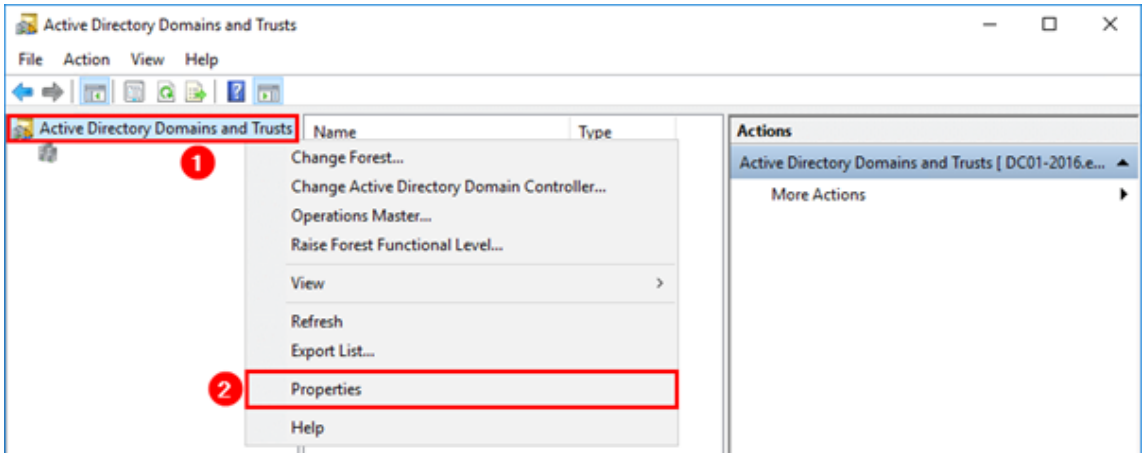
El sufijo del nombre principal de usuario (UPN) forma parte del nombre de inicio de sesión en AD. Cuando se cree una cuenta, usará el sufijo de UPN implícito de su bosque de AD de forma predeterminada, como yourforest.com. Tendrá que agregar un sufijo de UPN alternativo coincidente para cada usuario externo del front-end que quiera invitar a sus arrendatarios de Okta o Azure AD.

Por ejemplo, si invita a un usuario externo `contractoruser@hotmail.co.uk` y quiere asociarlo a una cuenta sombra de AD del back-end `contractoruser@yourforest.com`, agregue `yourforest.com` como sufijo ALT de UPN en su bosque de AD.

Agregar sufijos de UPN alternativos en Active Directory mediante la interfaz de usuario de Active Directory Domains and Trusts

1. Inicie sesión en un controlador de dominio dentro de su bosque de AD de back-end.
2. Abra el **cuadro de diálogo Run**, escriba `domain.msc` y, a continuación, haga clic en **OK**.
3. En la ventana Active Directory Domains and Trusts, haga clic con el botón secundario en **Active Directory Domains and Trusts** y, a continuación, seleccione **Properties**.

4. En la ficha **UPN Suffixes**, en el cuadro Alternative UPN Suffixes, agregue un sufijo de UPN alternativo y, a continuación, seleccione **Add**.



5. Haga clic en **OK**.

Administrar sufijos de UPN de un bosque de AD de back-end con PowerShell

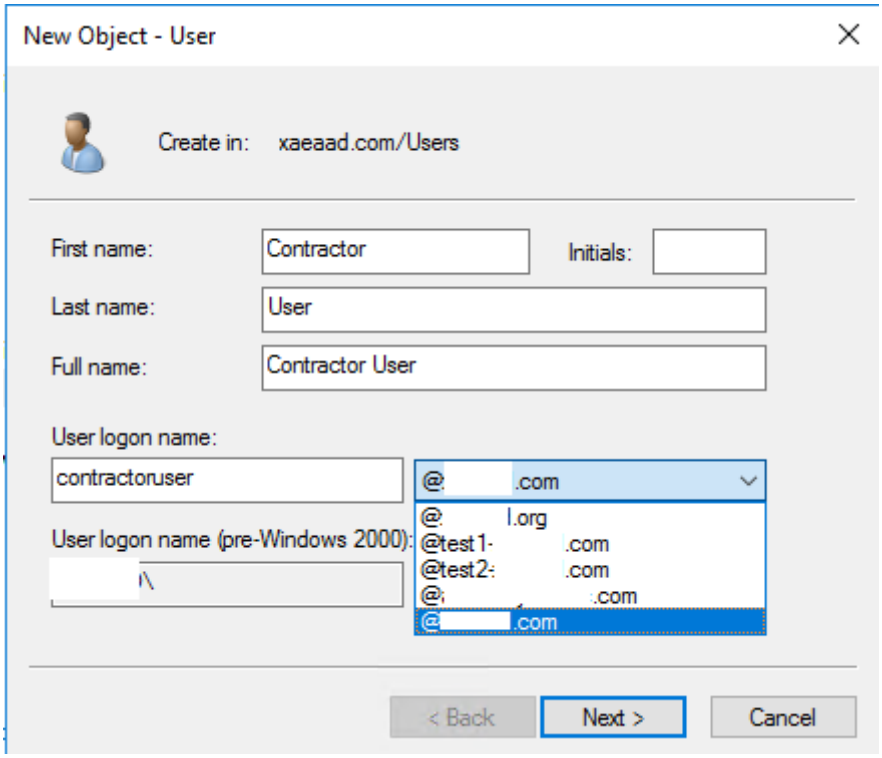
Es posible que tenga que agregar una gran cantidad de sufijos UPN nuevos a su bosque de AD de back-end para crear los UPN de cuenta sombra necesarios. La cantidad de sufijos de UPN alternativos que tendrá que agregar a su bosque de AD de back-end dependerá de la cantidad de usuarios externos diferentes que decida invitar a su arrendatario de proveedores de SAML.

Aquí se incluye el código de PowerShell para hacerlo si es necesario crear una gran cantidad de nuevos sufijos de UPN alternativos.

```
# Get the list of existing ALT UPN suffixes within your AD Forest
(Get-ADForest).UPNSuffixes

# Add or remove ALT UPN Suffixes
$NewUPNSuffixes = @("yourforest.com","externalusers.com")

# Set action to "add" or "remove" depending on the operation you wish
   to perform.
$Action = "add"
foreach($NewUPNSuffix in $NewUPNSuffixes)
{

    Get-ADForest | Set-ADForest -UPNSuffixes @{
 $Action=$NewUPNSuffix }

 }

<!--NeedCopy-->
```


Configurar una cuenta sombra de AD en su bosque de AD de back-end

1. Crea un nuevo usuario de cuenta sombra de AD.
2. El UPN implícito del bosque de AD, por ejemplo, `yourforest.local`, aparece seleccionado de forma predeterminada para los nuevos usuarios de AD. Seleccione el sufijo de UPN alternativo correspondiente que creó anteriormente. Por ejemplo, seleccione `yourforest.com` como sufijo de UPN del usuario de la cuenta sombra.



El UPN de usuario de la cuenta sombra también se puede actualizar a través de PowerShell.

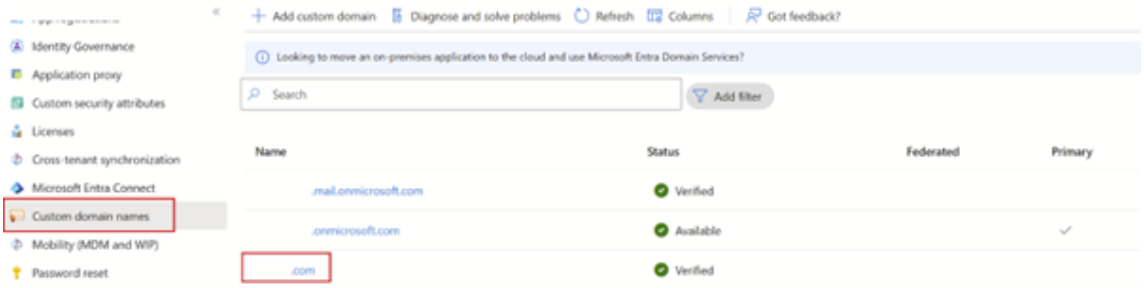
```
Set-ADUser "contractoruser" -UserPrincipalName "
    contractoruser@yourforest.com"
<!--NeedCopy-->
```

3. El UPN de usuario de la cuenta sombra debe coincidir exactamente con el UPN de usuario externo de la identidad de front-end.
4. Pruebe el inicio de sesión del usuario de front-end en Workspace.
5. Verifique que todos los recursos previstos aparecen enumerados en Workspace una vez que se haya realizado correctamente el inicio de sesión. Deberían aparecer los recursos asignados a la cuenta sombra de AD.

Configurar el UPN de usuario invitado de Entra ID para que coincida con el UPN de la cuenta sombra de AD

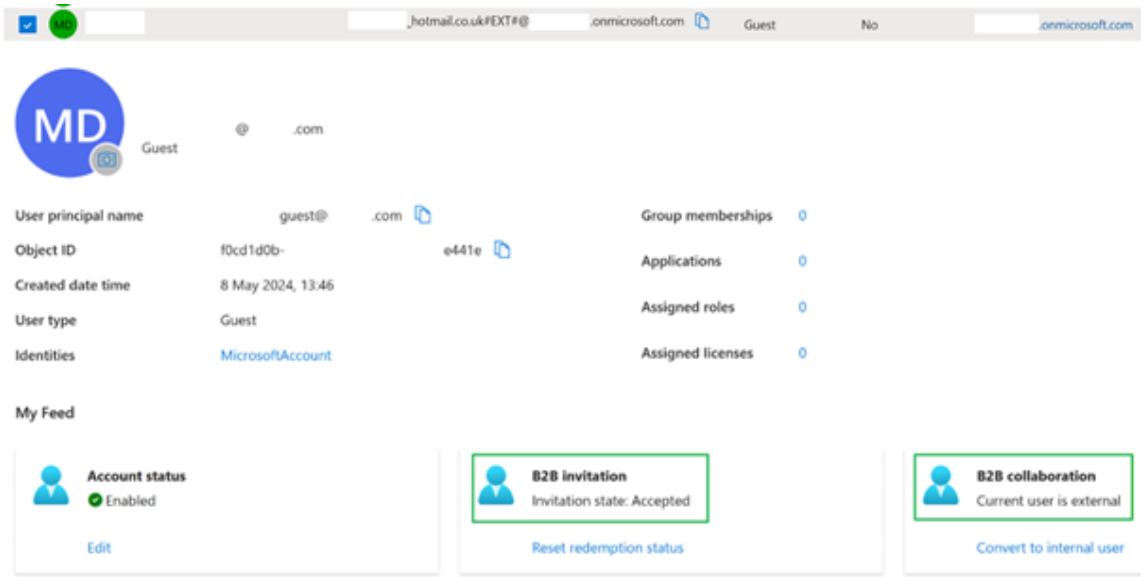
Cuando se invita a usuarios externos a un arrendatario de Entra ID, se genera automáticamente un UPN que indica que el usuario es externo. Al usuario externo de Entra ID se le asignará automáticamente el sufijo de UPN @Entra IDTenant.OnMicrosoft.com, que no es adecuado para su uso con SAML simplificado y no coincidirá con su cuenta sombra de AD. Deberá actualizarse para que coincida con un dominio de DNS importado en Entra ID y con el sufijo de UPN alternativo que creó en su bosque de AD.

1. Importe un dominio personalizado en Entra ID que coincida con el sufijo de UPN alternativo que agregó a su bosque de AD.



2. Invite a un usuario, por ejemplo, `contractoruser@hotmail.co.uk`, y asegúrese de que el usuario invitado acepta la invitación de Microsoft al arrendatario de Entra ID.

   Ejemplo de formato de UPN de usuario invitado externo generado por Microsoft. `contractoruser_hotmail.co.uk#EXT#@yourEntra IDtenant.onmicrosoft.com`



> **Importante:**
>
> Citrix Cloud y Workspace no pueden usar UPN que contengan el carácter # para la autenticación SAML.

3. Instale los módulos de Azure PowerShell Graph necesarios para poder administrar usuarios de Entra ID.

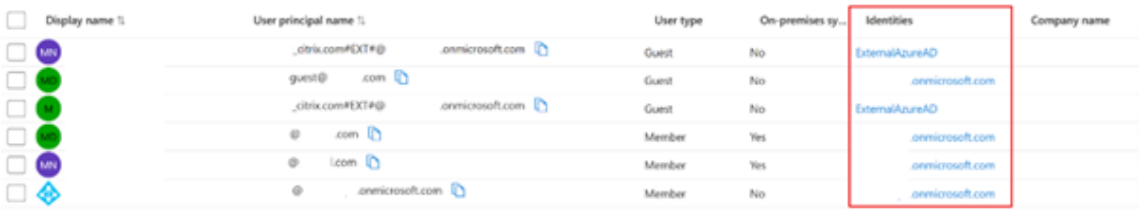
```
Install-Module -Name "Microsoft.Graph" -Force
Get-InstalledModule -Name  "Microsoft.Graph"
<!--NeedCopy-->
```

4. Inicie sesión en su arrendatario de Entra ID con una cuenta de administrador global y con el ámbito `Directory.AccessAsUser.All`.

> **Importante:**
>
> Si usa una cuenta con menos privilegios o no especifica el ámbito `Directory.AccessAsUser.All`, no podrá completar el paso 4 ni actualizar el UPN del usuario invitado.

```
$EntraTenantID = "<yourEntraTenantID>"
Connect-MgGraph -Tenant $EntraTenantID -Scopes "Directory.
    AccessAsUser.All"
<!--NeedCopy-->
```

5. Obtenga la lista completa de usuarios invitados externos de su arrendatario de Entra ID (opcional).




```
Get-MgUser -filter "userType eq 'Guest'" | Select Id,DisplayName,
    UserPrincipalName,Mail
<!--NeedCopy-->
```

6. Obtenga la identidad de usuario invitado cuyo UPN necesita actualizar y, a continuación, actualice su sufijo de UPN.

```
$GuestUserId = (Get-MgUser -UserId "contractoruser_hotmail.co.uk#
    EXT#@yourEntra IDtenant.onmicrosoft.com").Id

Update-MgUser -UserId $GuestUserId -UserPrincipalName "
    contractoruser@yourforest.com"
<!--NeedCopy-->
```

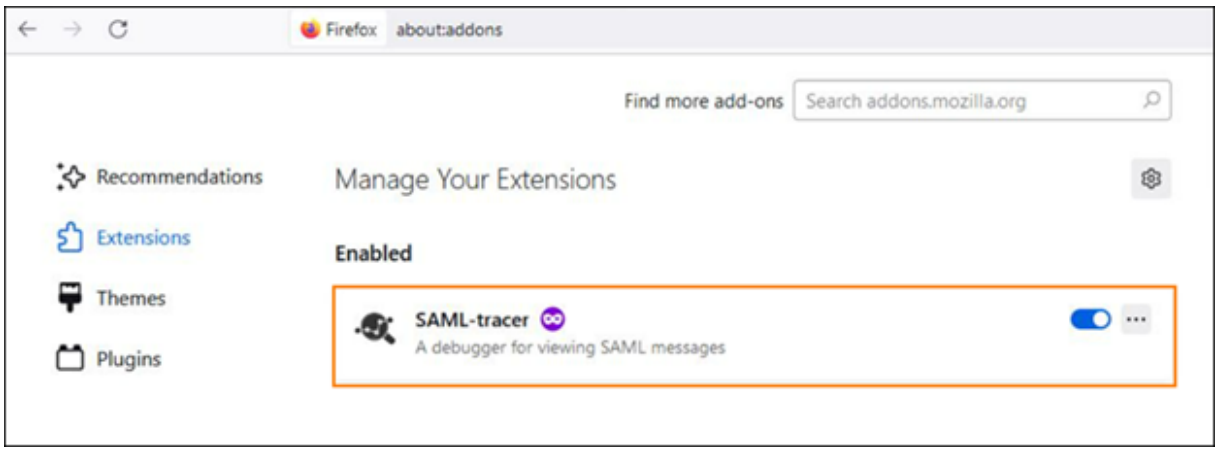

7. Compruebe que se puede encontrar la identidad del usuario invitado utilizando su UPN recién actualizado.

```
Get-MgUser -UserId "contractoruser@yourforest.com"
<!--NeedCopy-->
```

Probar la solución de SAML simplificado

Una vez que se hayan completado todos los pasos documentados en AD, Citrix Cloud y su proveedor de SAML, debe probar el inicio de sesión y verificar que se muestra la lista correcta de recursos para el usuario invitado en Workspace.

Citrix recomienda usar la extensión de explorador web SAML-tracer para todas las depuraciones de SAML. Esta extensión está disponible para los exploradores web más comunes. La extensión decodifica solicitudes y respuestas codificadas en Base64 en XML SAML, lo que las hace legibles para las personas.



Ejemplo de una aserción SAML simplificado que usa solo cip_upn para la autenticación capturada con SAML-tracer.


```
<AttributeStatement>
    <Attribute Name="http://schemas.microsoft.com/identity/claims/tenantid">
        <AttributeValue>                                    </AttributeValue>
    </Attribute>
    <Attribute Name="http://schemas.microsoft.com/identity/claims/objectidentifier">
        <AttributeValue>                                    </AttributeValue>
    </Attribute>
    <Attribute Name="http://schemas.microsoft.com/identity/claims/identityprovider">
        <AttributeValue>https://sts.windows.net/                                    /</AttributeValue>
    </Attribute>
    <Attribute Name="http://schemas.microsoft.com/claims/authnmethodsreferences">
        <AttributeValue>http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/        </AttributeValue>
    </Attribute>
    <Attribute Name="cip_upn">
        <AttributeValue>                    </AttributeValue>
    </Attribute>
    <Attribute Name="lastName">
        <AttributeValue>    </AttributeValue>
    </Attribute>
    <Attribute Name="firstName">
        <AttributeValue>    </AttributeValue>
    </Attribute>
    <Attribute Name="displayName">
        <AttributeValue>          </AttributeValue>
    </Attribute>
</AttributeStatement>
```

FrontEnd Identity Type	Synched from AD	Has Connectors in AD	Needs AD Shadow Account	Login using Attribute
Internal AD Backed User in Shadow Account Forest	Yes	Yes	No	UPN
Internal AD Backed User in Different Forest	Yes	No	Yes	UPN
Internal Native User	No	Not applicable	Yes	UPN
External Guest User	No	Not applicable	Yes	Email

1. Asigne los recursos de DaaS correctos a los usuarios o grupos de cuentas sombra y respaldados por AD que los contienen.
2. Inicie la extensión de explorador SAML-tracer y capture todo el flujo de inicio y cierre de sesión.
3. Inicie sesión en Workspace con el atributo especificado en la tabla para el tipo de usuario de front-end que quiere probar.

   Inicio de sesión de usuario invitado de Entra ID: El usuario contratista al que invitó a su arrendatario de Entra ID como usuario invitado tiene la dirección de correo electrónico `contractoruser@hotmail.co.uk`.

   Introduzca la **dirección de correo electrónico** del usuario invitado cuando Entra ID se lo pida.

   O BIEN:

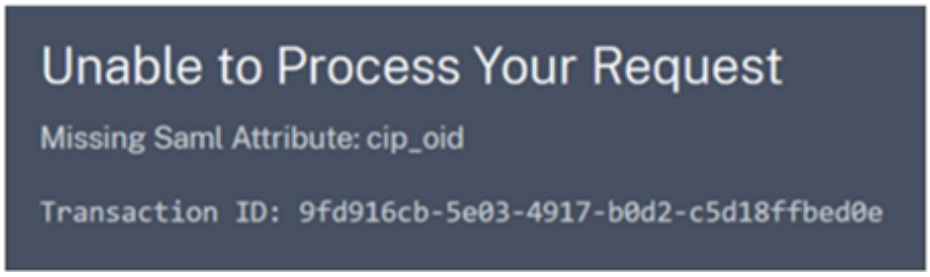
   Inicio de sesión de usuario de Entra ID respaldado por AD o usuario nativo de Entra ID: Estos usuarios de Entra ID tendrán un UPN con el formato `adbackeduser@yourforest.com` o `nativeuser@yourforest.com`.

   Introduzca el **UPN** del usuario cuando Entra ID se lo pida.
4. Compruebe que la aserción solo contenga el atributo **cip_upn** para la autenticación y que también contenga el atributo **displayName** que requiere la interfaz de usuario de Workspace.

5. Compruebe que el usuario puede ver los recursos de DaaS necesarios en la interfaz de usuario.

Solución de problemas de la solución de SAML simplificado

Errores de falta de atributos cip_*



Causa 1: El atributo SAML no está presente en la aserción SAML, pero Citrix Cloud está configurado para esperar recibirlo. No ha quitado los atributos cip_* innecesarios de la conexión SAML de Citrix Cloud en la sección de atributos de SAML. Desconecte SAML y vuelva a conectarlo para quitar las referencias a los atributos cip_* innecesarios.

Causa 2: Este error también puede producirse si no hay una cuenta sombra de AD correspondiente para que los Citrix Cloud Connectors la busquen en su bosque de AD de back-end. Es posible que haya configurado correctamente la identidad del front-end, pero la identidad de la cuenta sombra de AD del back-end con un UPN coincidente no existe o no se puede encontrar.

El inicio de sesión se realiza correctamente, pero no se muestra ningún recurso de DaaS después de que el usuario haya iniciado sesión en Workspace

Causa: Lo más probable es que se deba a una asignación de UPN de identidad de front-end a back-end incorrecta.

Asegúrese de que los 2 UPN de las identidades de front-end y back-end coincidan exactamente y representen al mismo usuario final que inicia sesión en Workspace. Compruebe que el grupo de entrega de DaaS contenga asignaciones a los usuarios correctos de la cuenta sombra de AD o a los grupos de AD que los contienen.

Durante el inicio de los recursos de DaaS, se produce un error en el SSON de FAS en los VDA unidos al dominio de AD

Al intentar iniciar recursos de DaaS, se solicita al usuario final de Workspace que introduzca sus credenciales de Windows en GINA. Además, el ID de evento 103 aparece en los registros de eventos de Windows de sus servidores FAS.

[S103] El servidor [CC:FASServer] solicitó el UPN [frontenduser@yourforest.com] `SID S-1-5-21-000000000-`, pero la búsqueda devolvió `SID S-1-5-21-000000000-0000000000-0000000001-0002`. [correlación: cc#967472c8-4342-489b-9589-044a24ca57d1]

Causa: Su implementación de SAML simplificado tiene un "problema de discordancia de SID". Tiene identidades de front-end que contienen SID de un bosque de AD que es distinto del bosque de AD de la cuenta sombra de back-end.
No envíe **cip_sid** en la aserción SAML.

El inicio de sesión falla para los usuarios respaldados por AD cuando existe el mismo sufijo UPN en varios bosques de AD conectados

Citrix Cloud tiene varias ubicaciones de recursos y conectores unidos a diferentes bosques de AD. El inicio de sesión falla cuando se usan usuarios respaldados por AD importados en Entra ID desde un bosque de AD diferente del bosque de AD de la cuenta sombra.

El bosque de AD 1 se sincroniza con Entra ID para crear usuarios de front-end con UPN como `frontenduser@yourforest.com`.

El bosque de AD 2 contiene las cuentas sombra de back-end con UPN como `frontenduser@yourforest.com`.

Causa: Su implementación de SAML simplificado tiene un "problema de ambigüedad de UPN". Citrix Cloud no puede determinar qué conectores usar para buscar la identidad de back-end del usuario.

No envíe **cip_sid** en la aserción SAML.
El UPN de su usuario existe en más de un bosque de AD conectado a Citrix Cloud.

Configurar un servidor de PingFederate local como proveedor de SAML para Workspaces y Citrix Cloud

April 26, 2024

Author:
Mark Dear

Este artículo ha sido redactado en colaboración entre los ingenieros de Citrix y Ping y ha sido revisado por ambas partes para garantizar la precisión técnica en el momento de la redacción. Consulte la documentación de Ping para obtener instrucciones sobre cómo aprovisionar, configurar y obtener licencia para un servidor de PingFederate local para usarlo como proveedor de SAML, ya que esos detalles van más allá del alcance de este artículo.

Este documento se redactó usando las versiones 11.3 y 12 de PingFederate.

Requisitos previos

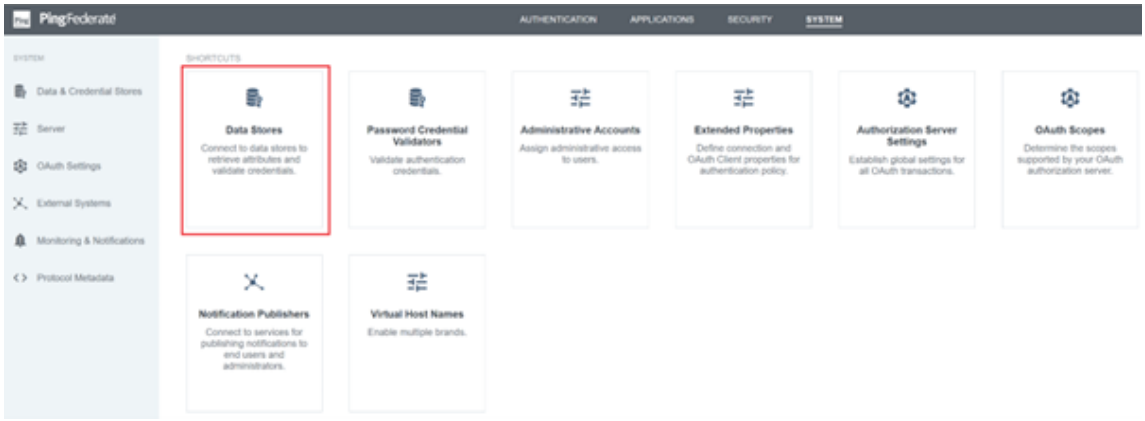
Este artículo aborda específicamente la configuración de SAML y garantiza que se cumplan estas condiciones.

- Ya ha aprovisionado un servidor de PingFederate local en su organización y ha obtenido la licencia necesaria. Para obtener más información, consulte Instalación de PingFederate.
- Debe haber instalado una versión compatible de Java en el servidor de PingFederate. Consulte la documentación de Ping Identity para conocer las versiones de Java compatibles. Para obtener más información, consulte Requisito de Java PingFederate.
- Ha configurado las reglas de red y firewall necesarias para permitir que Citrix Cloud y Workspace se redirijan al servidor de PingFederate local durante el proceso de inicio de sesión SAML de la consola de administración de Workspace o Citrix Cloud. Para obtener más información, consulte Requisitos de red de PingFederate.
- Ha importado un certificado x509 firmado públicamente a su servidor de PingFederate que puede actuar como certificado de servidor para el servidor de PingFederate.
- Ha importado un certificado x509 firmado públicamente a su servidor de PingFederate que puede actuar como certificado de firma SAML para el IdP. Este certificado debe cargarse en Citrix Cloud durante el proceso de conexión SAML.
- Ha conectado su Active Directory local a PingFederate. Para obtener más información, consulte Almacén de datos LDAP de PingFederate

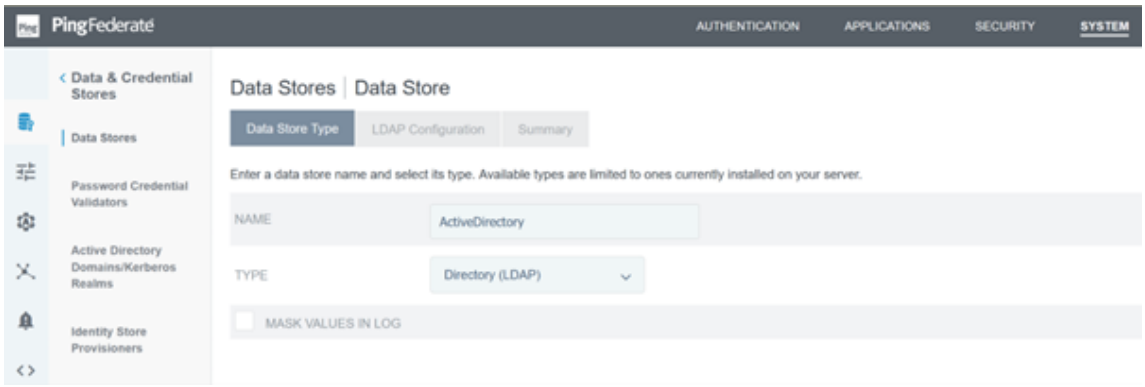
> **Nota:**
>
> Mientras configura PingFederate para su uso con Citrix Cloud y Workspace, consulte la documentación de PingFederate para comprender el efecto de cada uno de los parámetros de SAML y para ayudar a completar las instrucciones que se ofrecen aquí.

Configurar una conexión de Active Directory para su dominio de AD mediante un almacén de datos dentro de PingFederate

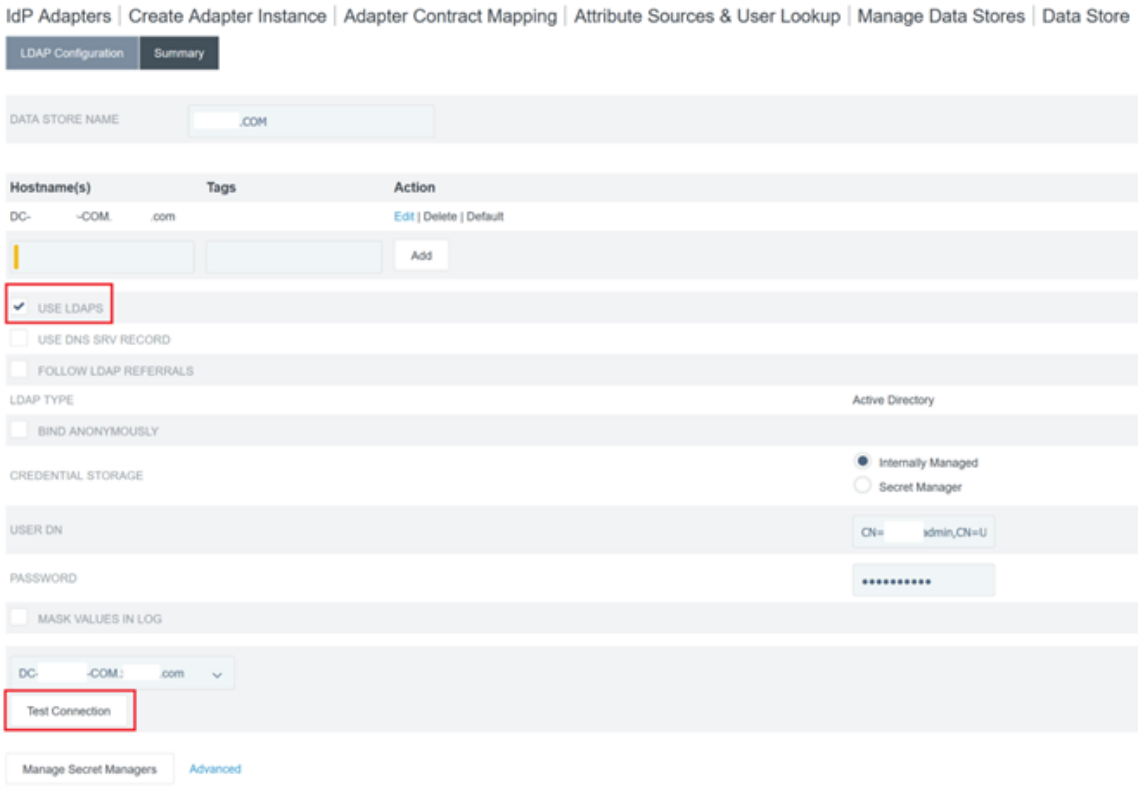
1. Configure una conexión de Active Directory dentro de los almacenes de datos.



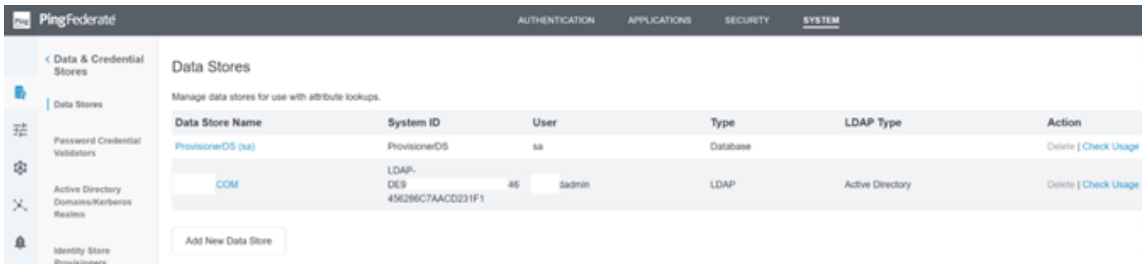
2. Seleccione Tipo como **Directorio (LDAP)**.



3. Configure sus controladores de dominio para las conexiones LDAPS y agregue su lista de FQDN de los controladores de dominio en el campo de nombres de host. A continuación, haga clic en **Probar conexión**.

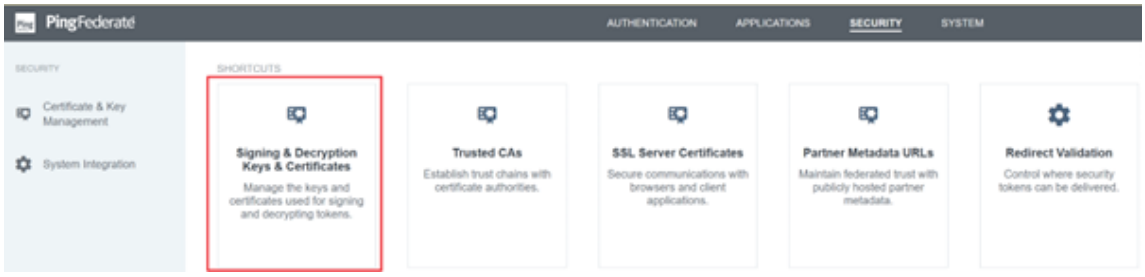


4. Una vez configurada, la conexión de Active Directory debe parecerse a este ejemplo:



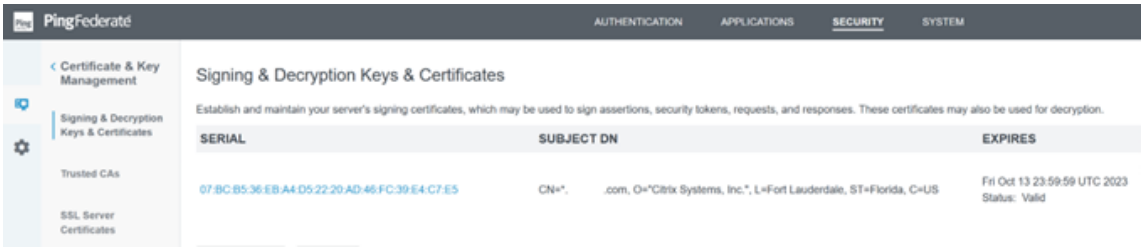
Cargar el certificado de firma SAML de Citrix Cloud

1. Haga clic en la ficha **Seguridad**
2. Cargue el certificado de firma SAML que quiere que utilice PingFederate en las **claves y certificados de firma y descifrado**.

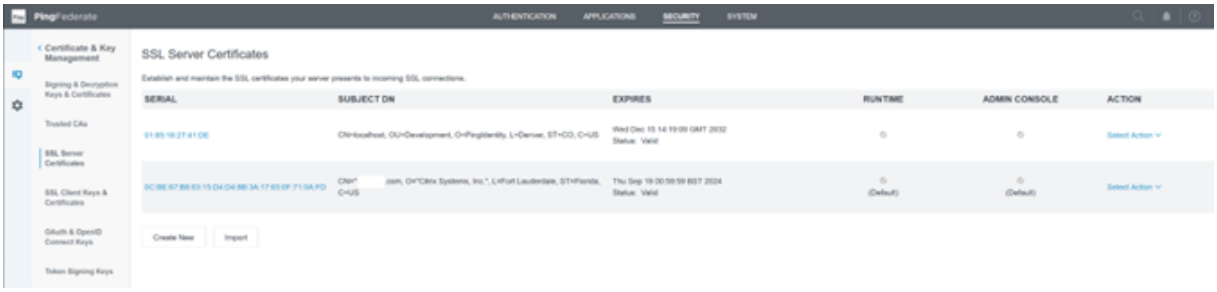


> **Nota:**
>
> En este ejemplo, el certificado usado es un certificado de Digicert `pingfederateserver.domain.com` firmado públicamente.

3. Cargue todos los certificados de CA utilizados para firmar su certificado de firma SAML del servidor de PingFederate.



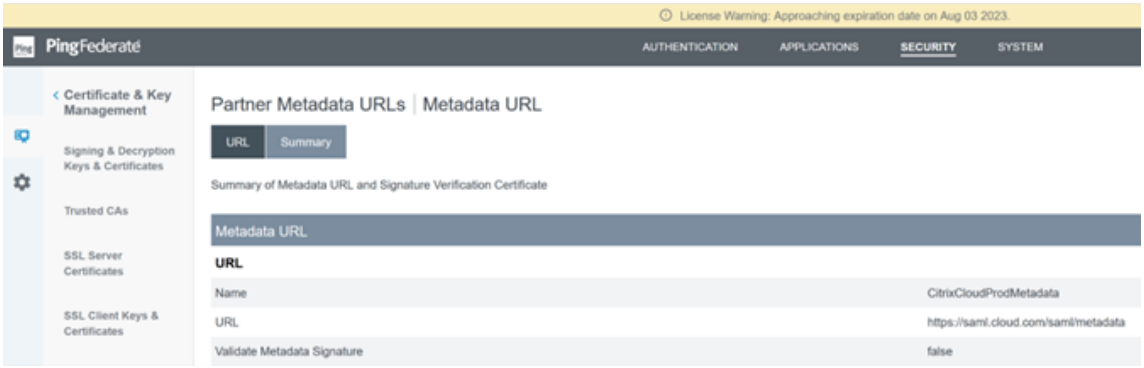
> **Nota:**
>
> El certificado del servidor de PingFederate y el certificado de firma SAML pueden ser el mismo certificado SSL o puede usar certificados SSL diferentes. Al configurar la conexión SAML, debe proporcionar una copia del certificado de firma SAML a Citrix Cloud.



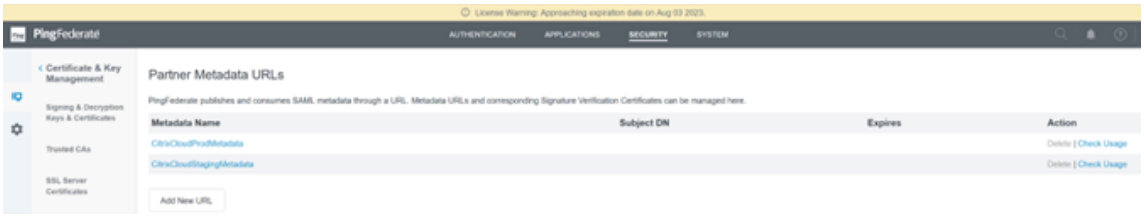
Cargar los metadatos de Citrix Cloud

1. Proporcione un nombre para los metadatos de Citrix Cloud e introduzca la URL de metadatos correspondiente a la región de Citrix Cloud en la que se encuentra su arrendatario de Citrix Cloud.

   - https://saml.cloud.com/saml/metadata - Comercio en la UE, EE. UU. y APS
   - https://saml.citrixcloud.jp/saml/metadata - Japón
   - https://saml.cloud.us/saml/metadata - Gobierno



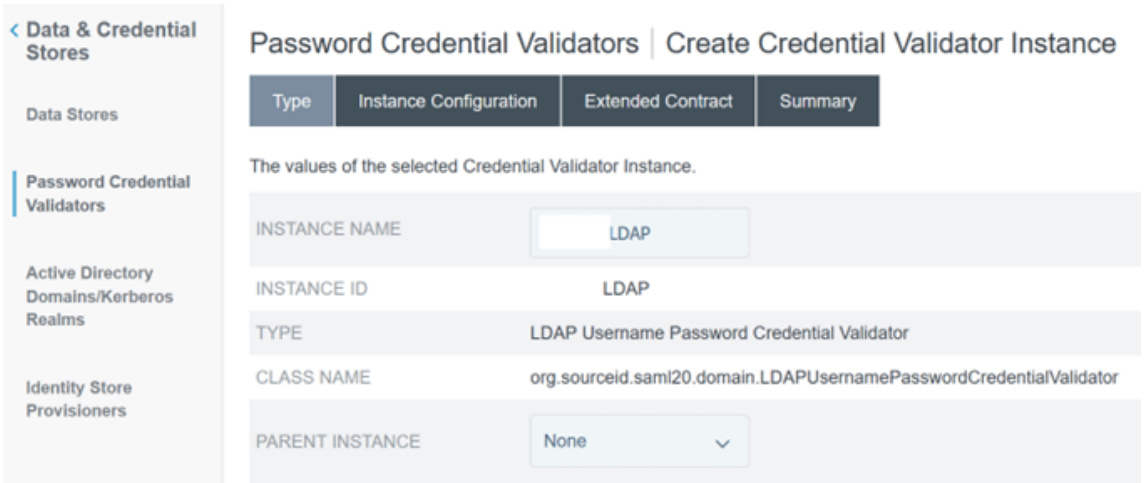
2. Una vez configurada, la configuración de metadatos de Citrix Cloud debe parecerse a este ejemplo.



Configurar un validador de credenciales de contraseñas dentro de PingFederate

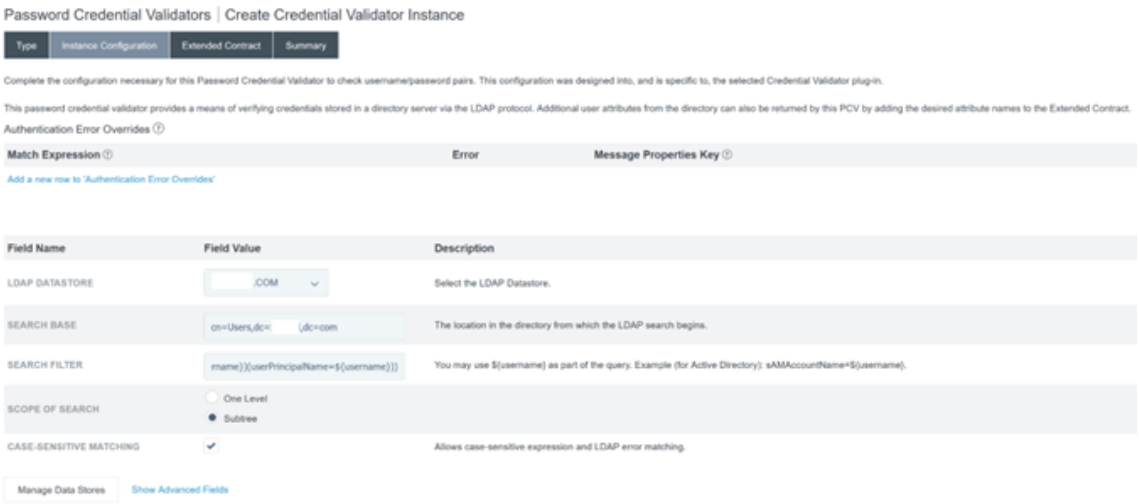
Para obtener más información, consulte Validador de credenciales de contraseña de PingFederate

1. Configure el tipo de validador de credenciales de contraseña como nombre de usuario y contraseña de LDAP.



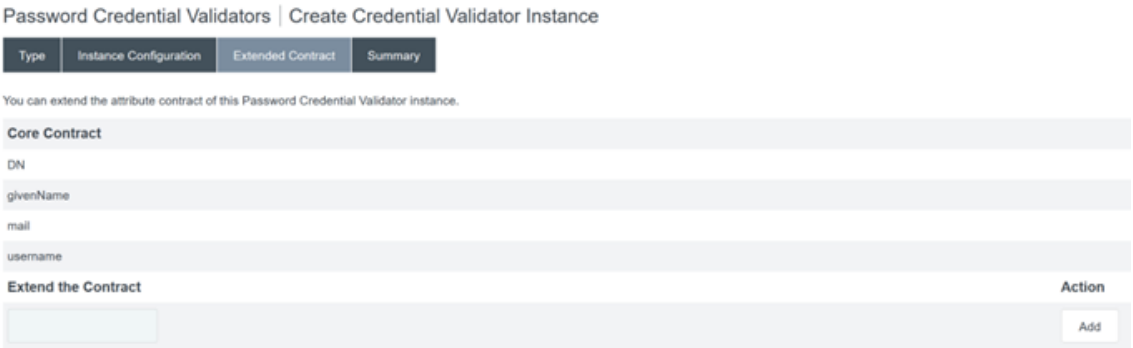
2. Configure la **configuración de instancias**. Seleccione la conexión de dominio de AD y el almacén de datos que configuró anteriormente en Configurar una conexión de Active Directory para su dominio de AD mediante un almacén de datos dentro de PingFederate. Introduzca un filtro LDAP adecuado como se muestra en el ejemplo.


```
(((sAMAccountName=${ username } )(userPrincipalName=${ username }
 ))
```

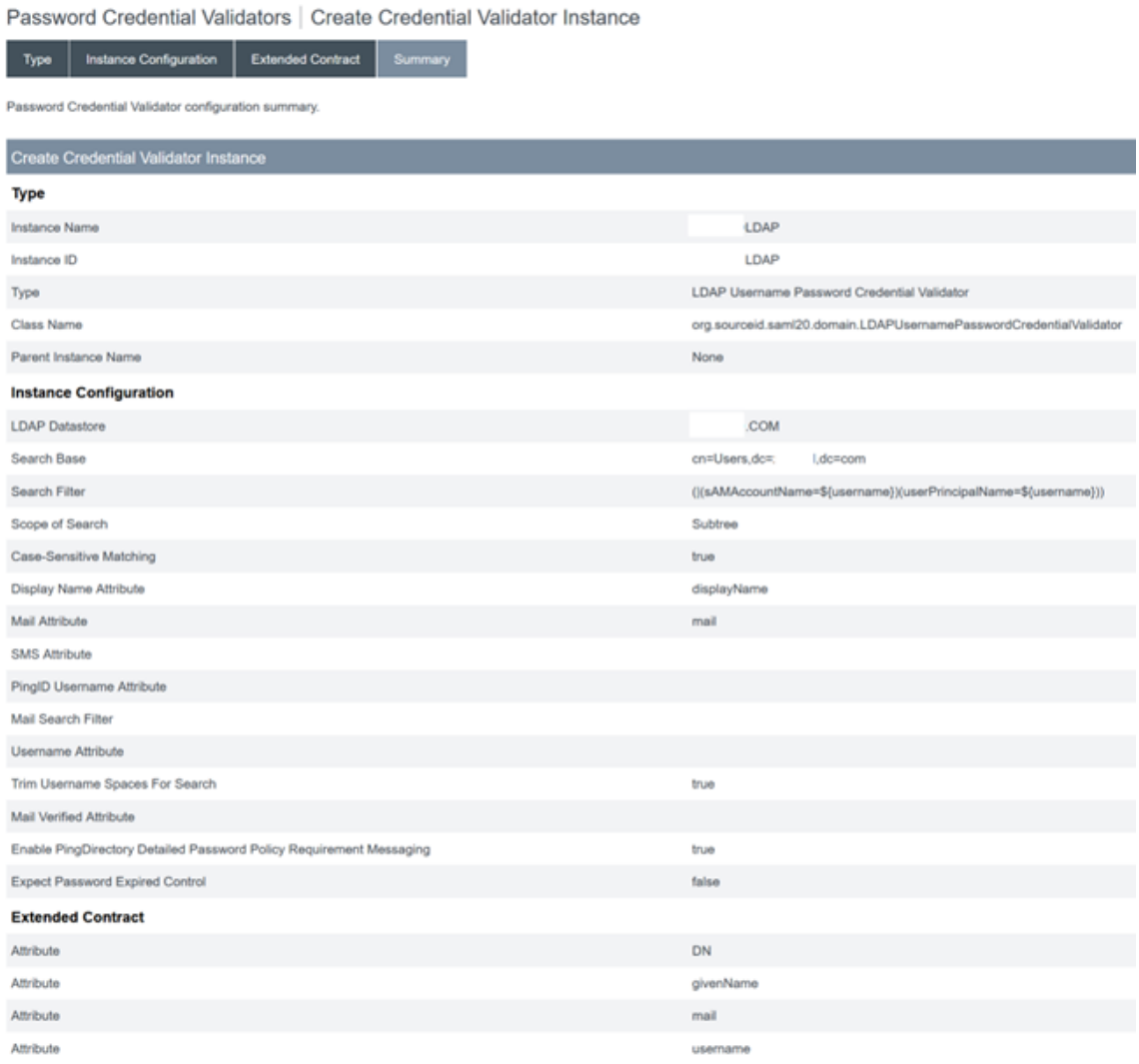


> **Nota:** El filtro de ejemplo incluye los formatos de nombre de usuario de AD sAMAccountName y userPrincipalName, lo que permite a los usuarios finales iniciar sesión en Workspace o Citrix Cloud con cualquiera de estos formatos. El filtro de ejemplo admite los formatos de nombre de usuario de AD sAMAccountName y userPrincipalName, lo que permite a los usuarios finales iniciar sesión en Workspace o Citrix Cloud con cualquiera de estos formatos.

3. Configure el **contrato extendido**.



4. El resumen del **validador de credenciales de contraseña** debe parecerse a este ejemplo.



Password Credential Validators | Create Credential Validator Instance

Type | Instance Configuration | Extended Contract | Summary

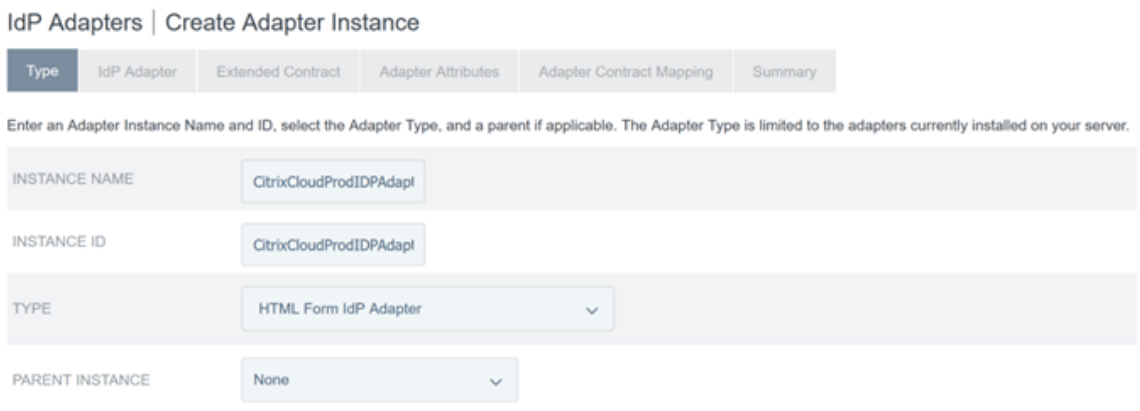
Password Credential Validator configuration summary.

Create Credential Validator Instance	
Type	
Instance Name	LDAP
Instance ID	LDAP
Type	LDAP Username Password Credential Validator
Class Name	org.sourceid.saml20.domain.LDAPUsernamePasswordCredentialValidator
Parent Instance Name	None
Instance Configuration	
LDAP Datastore	.COM
Search Base	cn=Users,dc= l,dc=com
Search Filter	(|(sAMAccountName=${username})(userPrincipalName=${username}))
Scope of Search	Subtree
Case-Sensitive Matching	true
Display Name Attribute	displayName
Mail Attribute	mail
SMS Attribute	
PingID Username Attribute	
Mail Search Filter	
Username Attribute	
Trim Username Spaces For Search	true
Mail Verified Attribute	
Enable PingDirectory Detailed Password Policy Requirement Messaging	true
Expect Password Expired Control	false
Extended Contract	
Attribute	DN
Attribute	givenName
Attribute	mail
Attribute	username

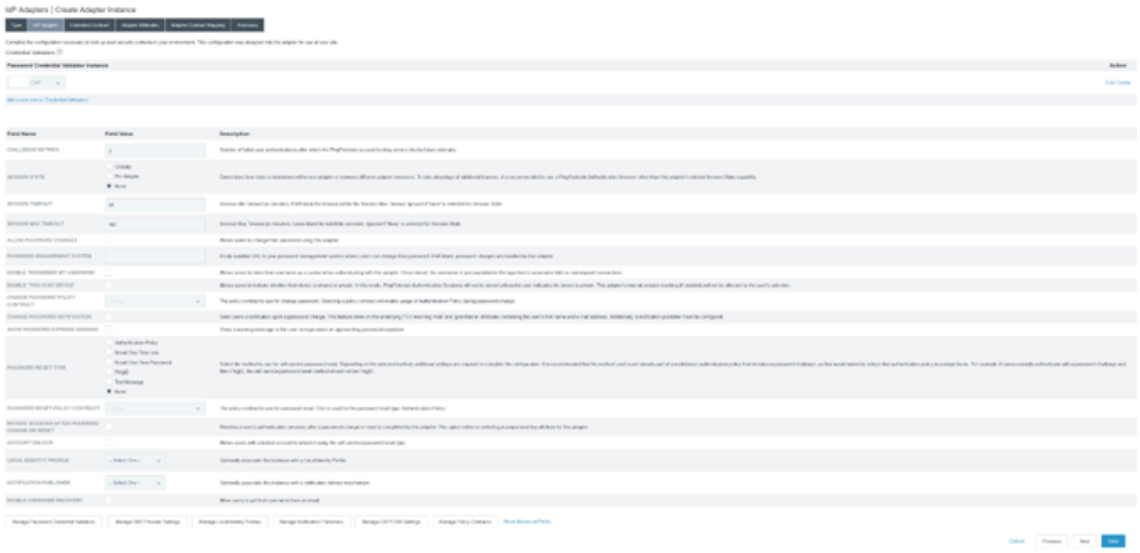
Configurar el adaptador IDP dentro de PingFederate

Para obtener más información, consulte Adaptador de formulario HTML de PingFederate

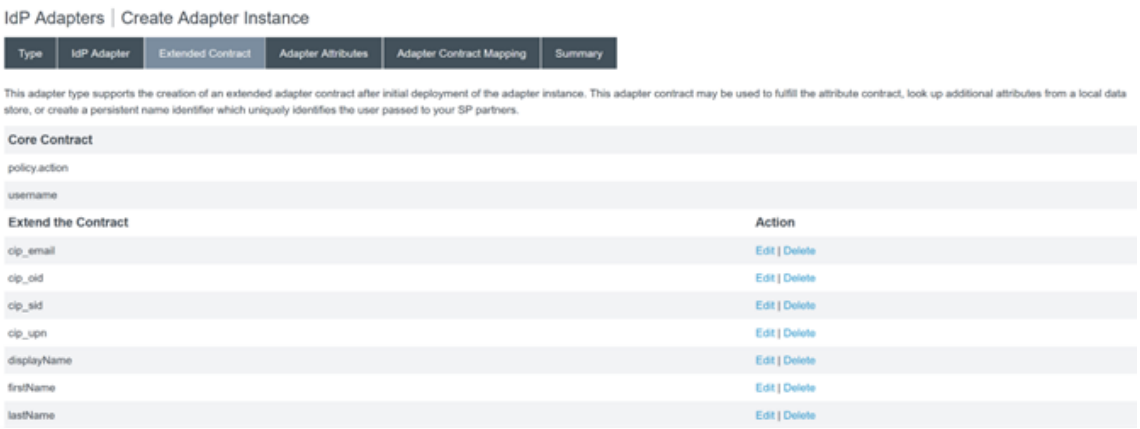
1. Cree un nuevo adaptador IDP de tipo adaptador IdP de formulario HTML.



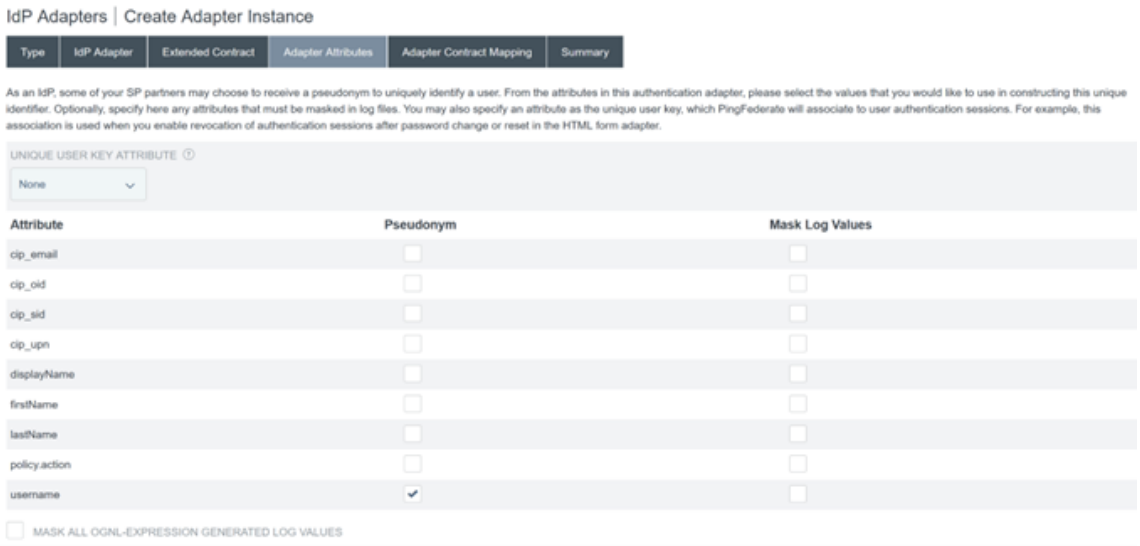
2. Seleccione el **validador de credenciales de contraseña** existente que configuró anteriormente y configure el adaptador IDP. Para obtener más información, consulte Configurar un validador de credenciales de contraseñas dentro de PingFederate.



3. Configure el **contrato extendido** con los atributos de SAML que se transfieren a Citrix Cloud o Workspaces durante el inicio de sesión de SAML.



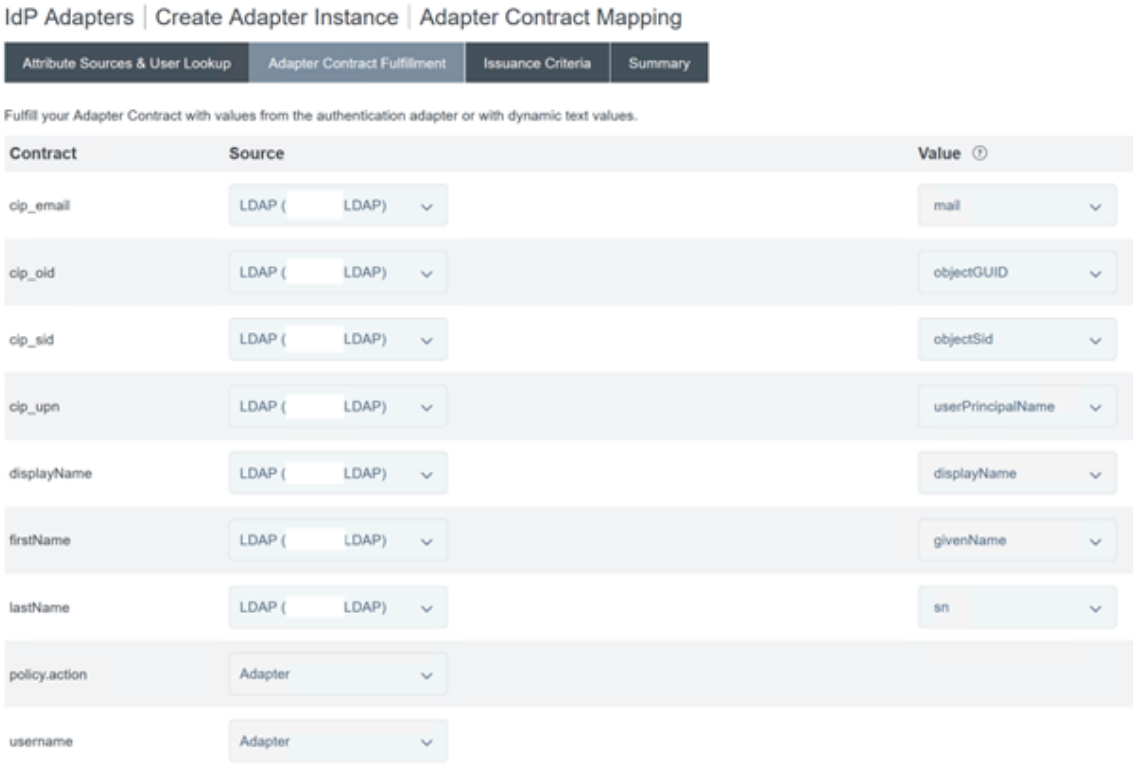
4. Configure los **atributos del adaptador**.



5. Configure la **asignación de contratos de adaptadores** por la cual los atributos de SAML se asignan a los atributos de usuario de LDAP desde las identidades de AD. Haga clic en **Configurar el contrato del adaptador**.

6. Configure las **fuentes de atributos y búsqueda de usuarios**.

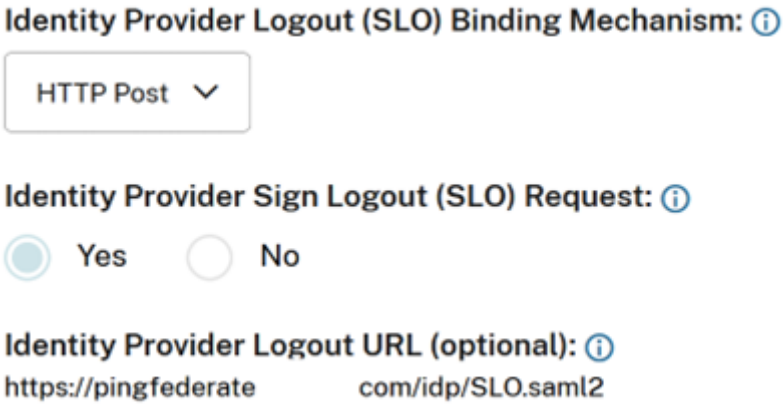
7. Configure el **cumplimiento del contrato del adaptador**. Seleccione **LDAP** y el nombre de su almacén de datos de Active Directory como fuente de los datos de atributos de usuario. El valor es el atributo de Active Directory para el usuario, como `objectGUID` o `objectSid`.



Configuración de la conexión del proveedor de servicios (aplicación SAML) para Citrix Cloud o Workspaces

La configuración de ejemplo de PingFederate que se proporciona a continuación asume los siguientes requisitos de autenticación de SAML dentro de su organización.

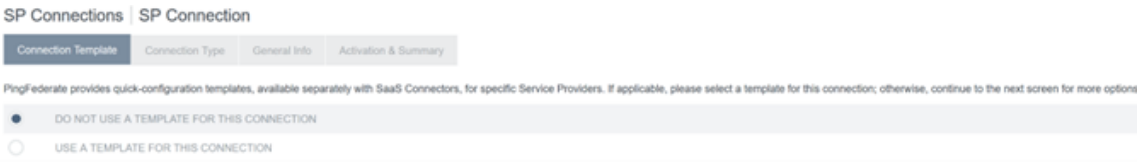
- Las solicitudes de autenticación SAML enviadas desde la consola de administración de Workspace o Citrix Cloud DEBEN estar firmadas.
- Los enlaces HTTP POST de SAML se utilizarán para las solicitudes de SSO y SLO.
- El cierre de sesión único (SLO) es un requisito en su organización. Cuando un usuario final cierra sesión en Workspace o en la consola de administración de Citrix Cloud, Citrix Cloud envía una solicitud de SLO de SAML al proveedor de SAML (IdP) para cerrar la sesión del usuario.
- PingFederate requiere solicitudes HTTP POST firmadas para iniciar el cierre de sesión. El proveedor de SAML requiere solicitudes de SLO firmadas.



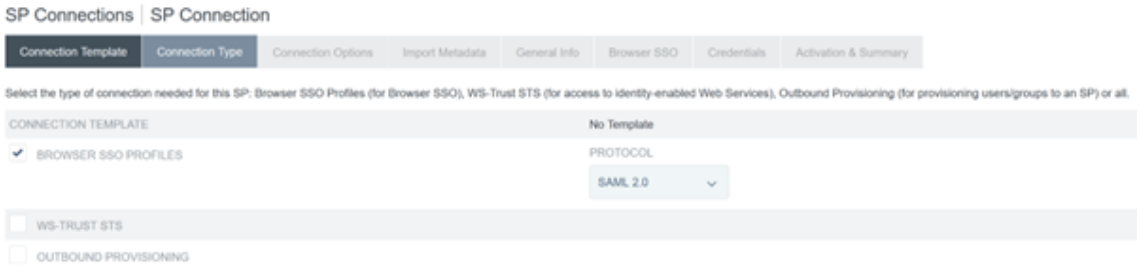
Para obtener más información, consulte PingFederate SP Management

Procedimiento

1. Configure la **plantilla de conexión**.

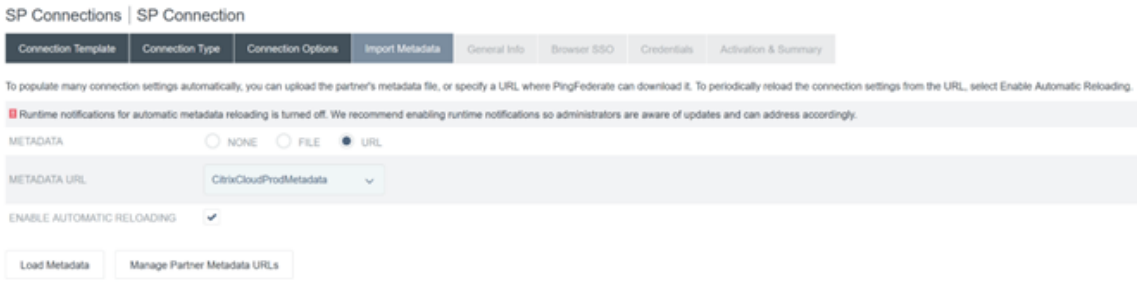


2. Configure el **tipo de conexión** y seleccione los **perfiles de SSO del explorador web y SAML 2.0**.



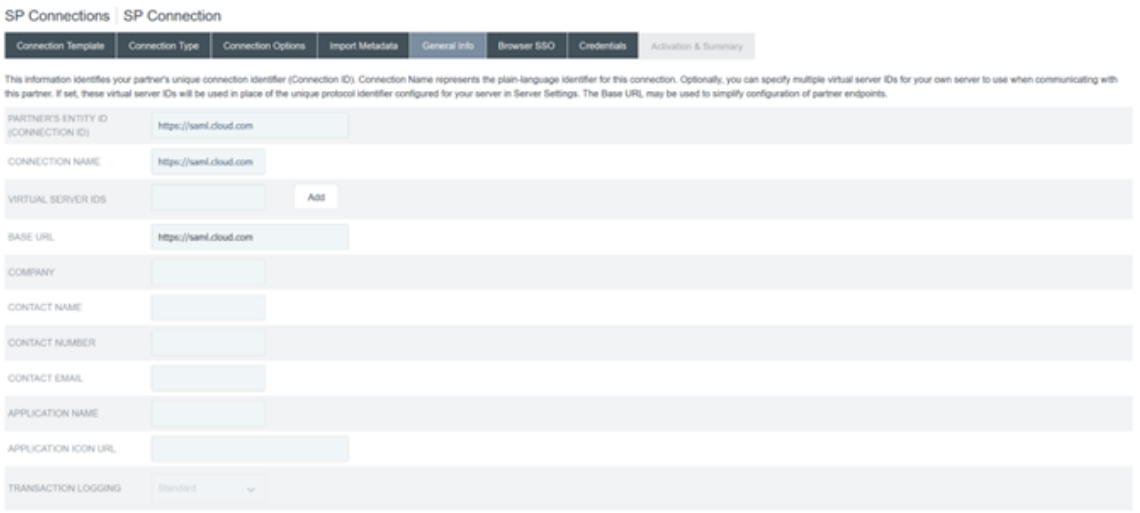
3. Configure las **opciones de conexión**.

4. Importe los metadatos de Citrix Cloud. Seleccione la URL y la URL de `CitrixCloudProdMetadata` que creó anteriormente y haga clic en **Cargar metadatos**

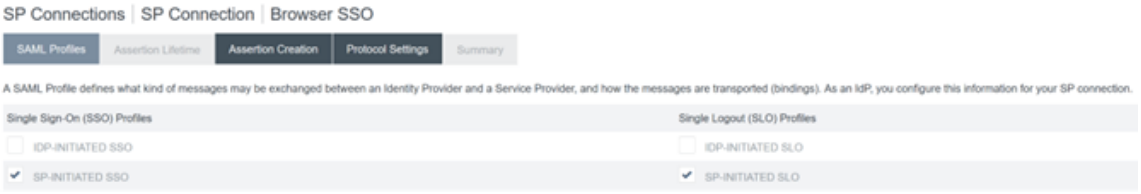


5. Configure la **información general**. Establezca el ID de la entidad de conexión del proveedor de servicios, la URL base y el nombre de conexión en el punto final SAML de Citrix Cloud de su región de clientes de Citrix Cloud.

   - https://saml.cloud.com - Comercio en la UE, EE. UU. y APS
   - https://saml.citrixcloud.jp - Japón
   - https://saml.cloud.us - Gov



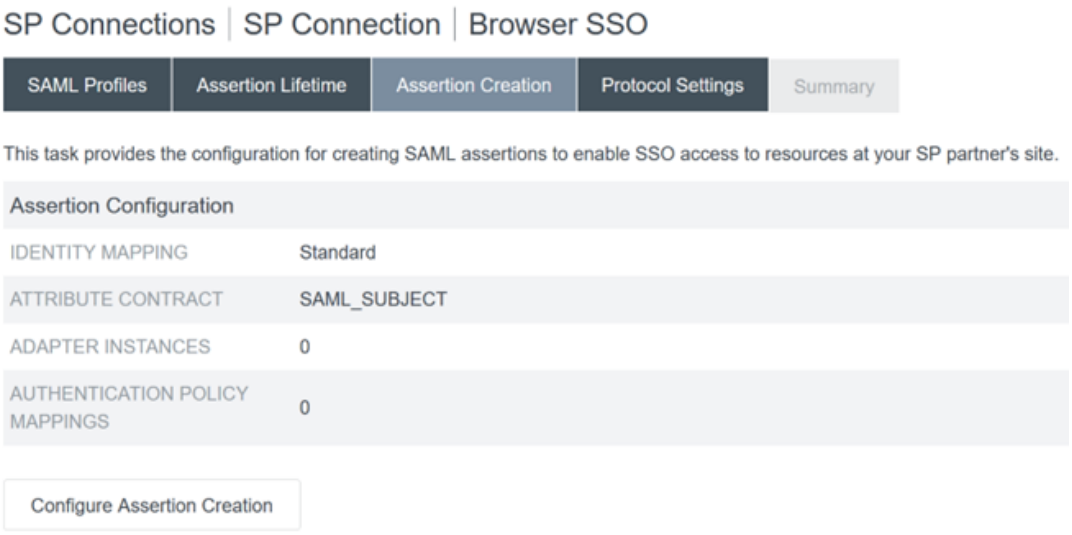
6. Configure los **parámetros del protocolo**.



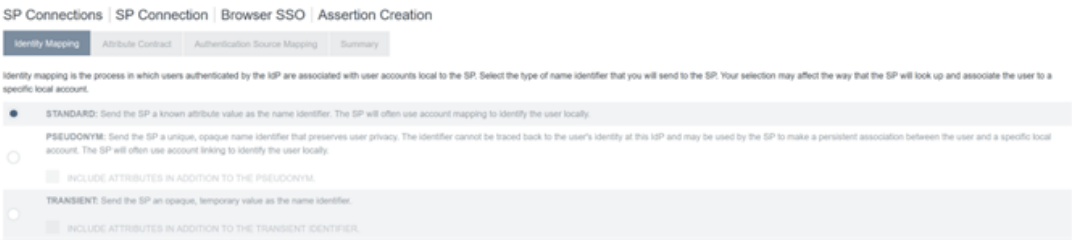
7. Use los parámetros predeterminados de **Vida útil de las aserciones**.

8. Configure la creación de aserciones SAML.

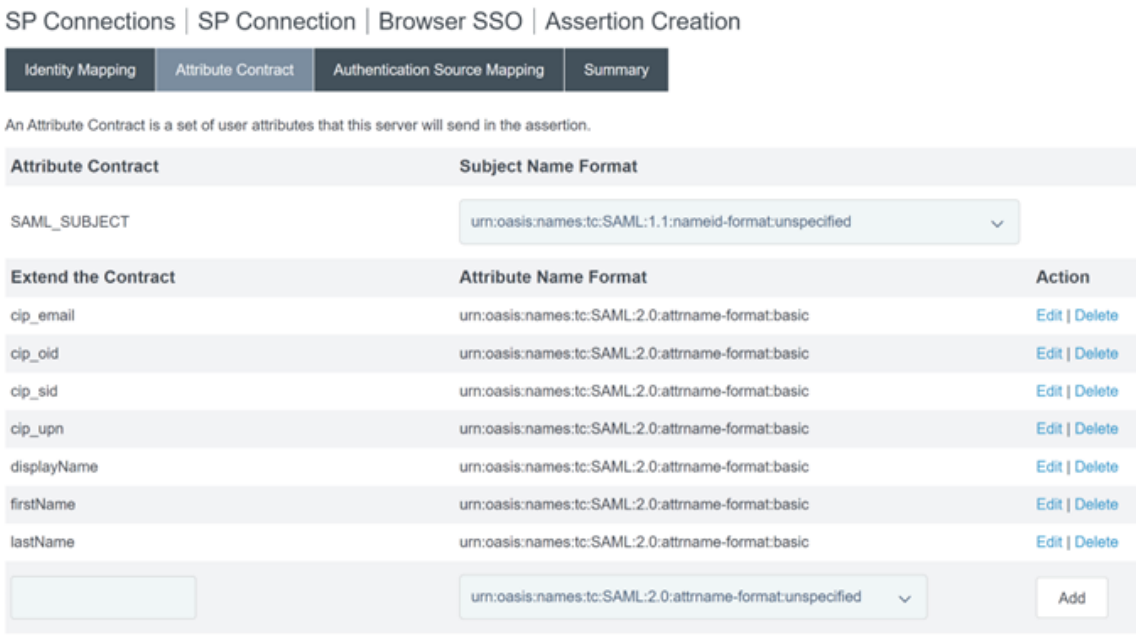
   a) Haga clic en **Configurar creación de aserciones**



   b) Seleccione **Standard**.

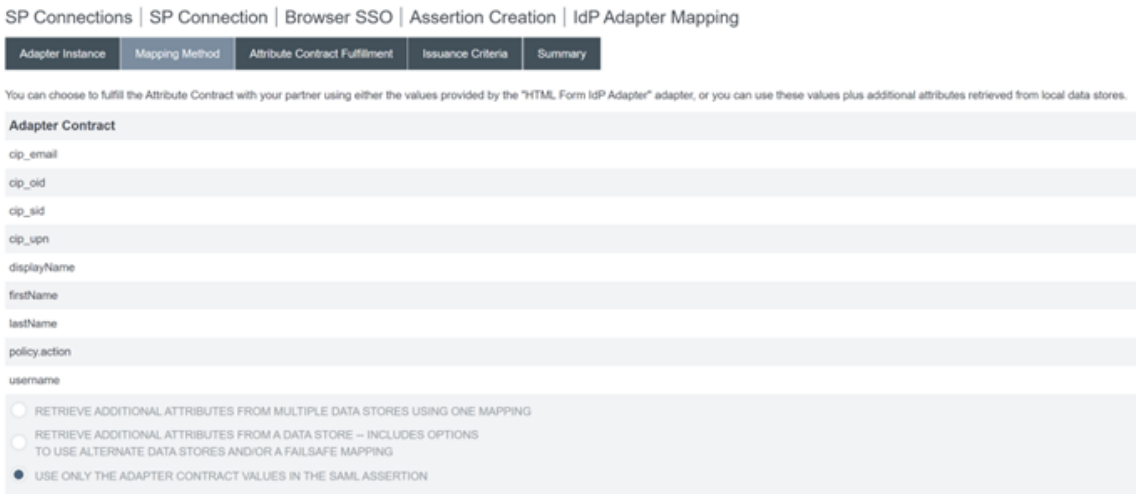


9. Configure el **contrato de atributos**.

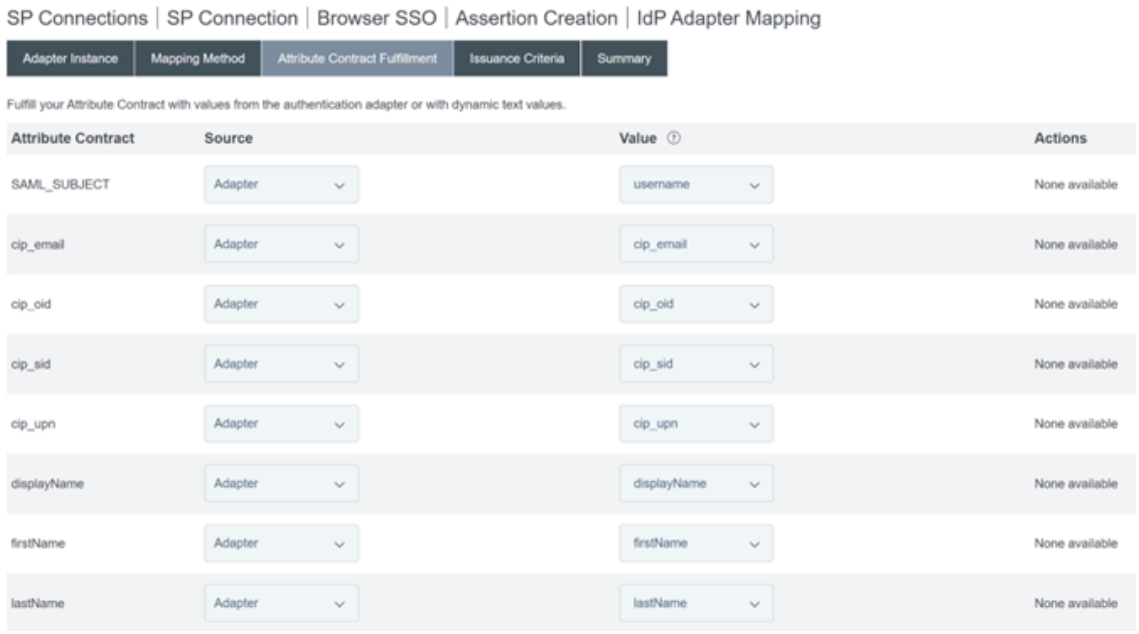


10. Configure la **instancia del adaptador**.

11. Configure el **método de mapeo**.



12. Configure el **cumplimiento del contrato de atributos**.

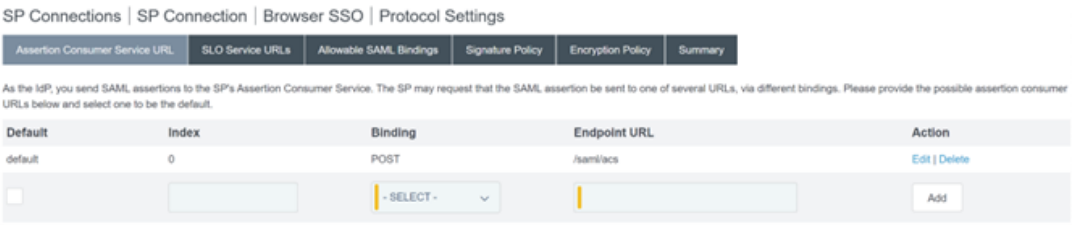


13. Configure los **criterios de emisión de certificados** como valores predeterminados sin condiciones.

14. La **asignación del adaptador IDP** completa se muestra de esta manera:
15. Configure los **parámetros del protocolo**. Las rutas SAML requeridas por Citrix Cloud se anexarán a la URL base de su servidor de PingFederate. Es posible anular la URL base intro-

duciendo una ruta completa en el campo URL del punto final, pero esto suele ser innecesario e indeseable.
URL base: https://youpingfederateserver.domain.com

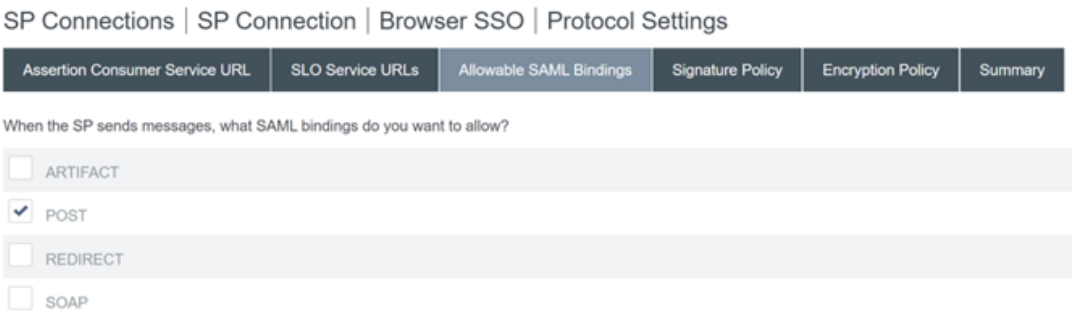
a) Configure la URL de ACS (Assertion Consumer Service) que anexa la ruta SAML a la URL base del servidor de PingFederate. URL del punto final - `/saml/acs`



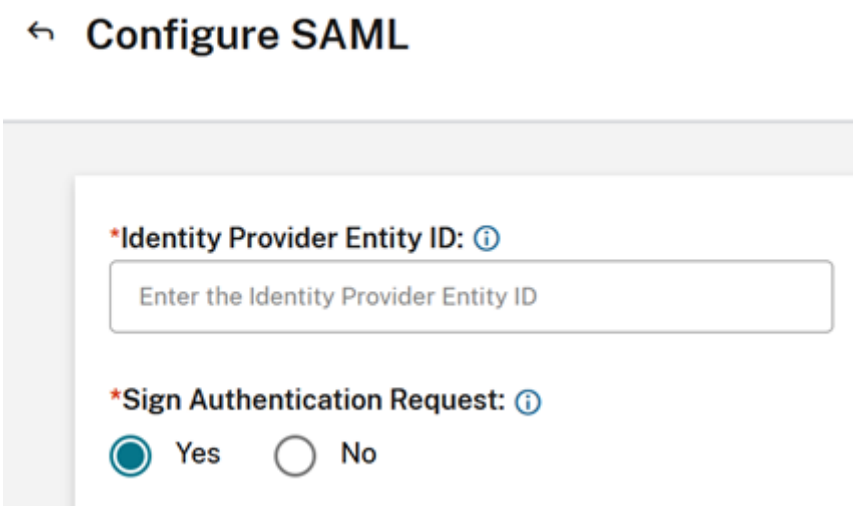
b) Configure la **URL del servicio SLO**. URL del punto final - `/saml/logout/callback`

> **Importante:**
>
> La conexión SAML de Citrix Cloud requiere que se configure una URL de cierre de sesión de PingFederate correspondiente si quiere ejecutar el servicio SLO al cerrar sesión en Workspace o Citrix Cloud. Si no configura la URL de cierre de sesión en su conexión SAML, los usuarios finales simplemente cerrarán sesión en Workspace, pero no en PingFederate.

a) Configure los **enlaces SAML permitidos**.

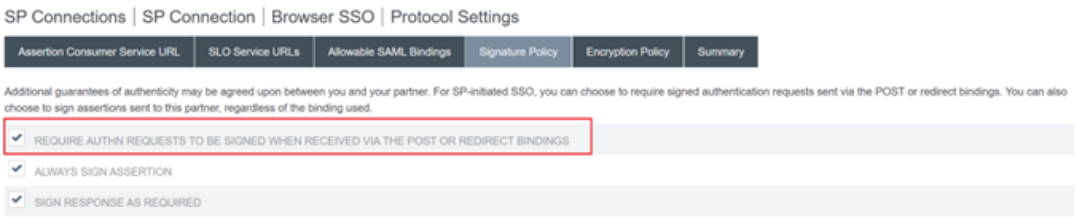


b) Configure la **directiva de firmas**.

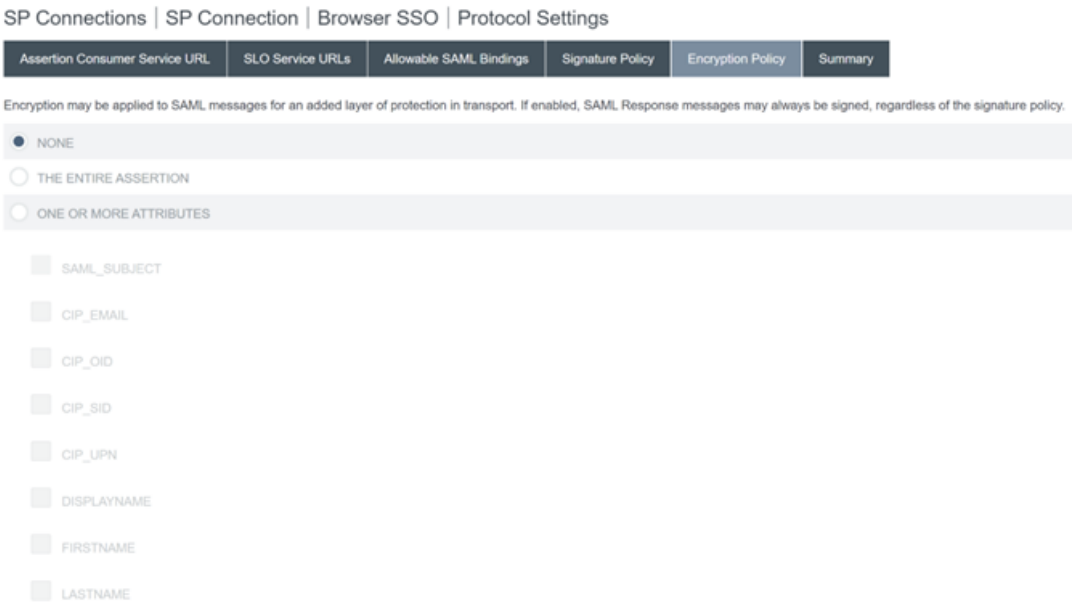


> **Importante:**
>
> Los parámetros de firma SAML deben configurarse de forma coherente en ambos lados de la conexión SAML. Workspace o Citrix Cloud (SP) deben configurarse para enviar solicitudes de SSO y SLO firmadas.

a) PingFederate (IDP) debe configurarse para ejecutar la aplicación de solicitudes firmadas mediante el certificado de verificación de firmas SAML de Citrix Cloud.

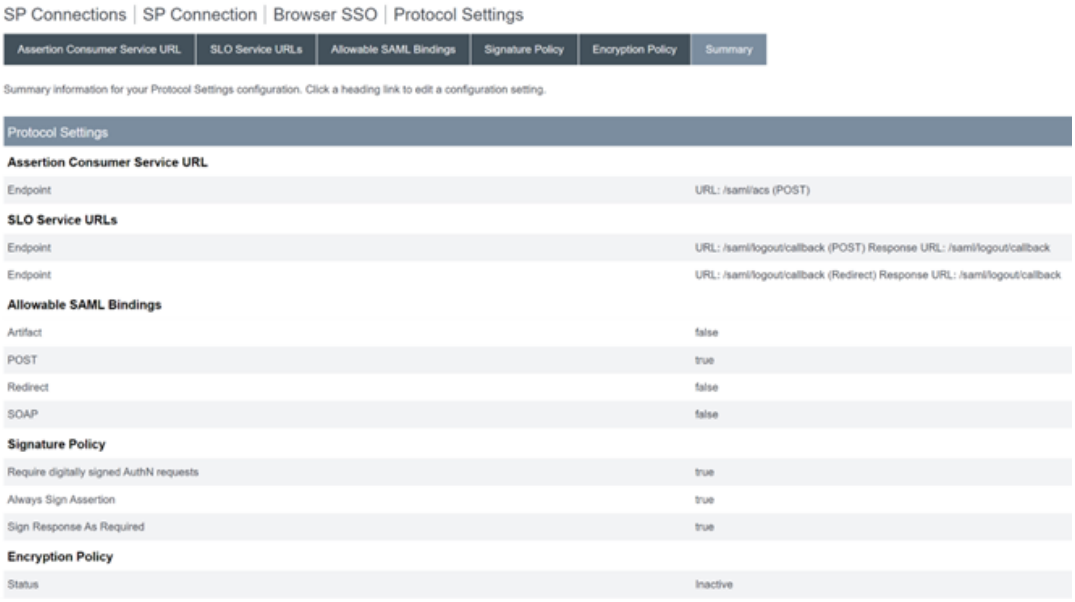


b) Configure la **directiva de cifrado**.

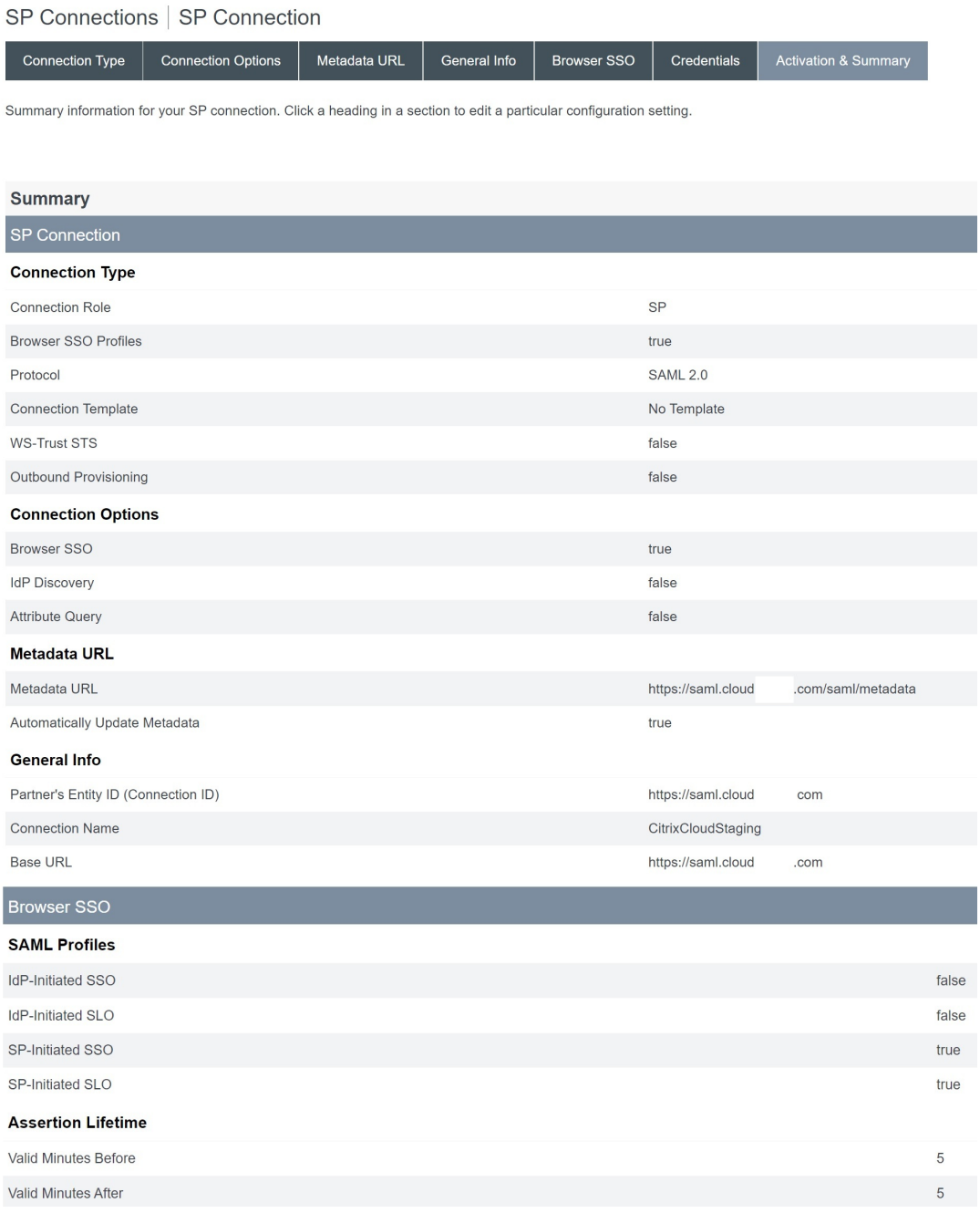


> **Nota:**
>
> Se recomienda establecer Cifrado en **NINGUNO** durante la configuración y las pruebas iniciales para poder depurar los problemas relacionados con atributos SAML faltantes o incorrectos en la aserción. Si necesita aserciones cifradas, se recomienda habilitar el cifrado después de comprobar que el inicio de sesión en Workspace o Citrix Cloud se ha realizado correctamente y que todos los recursos se han enumerado correctamente y se pueden iniciar. No será posible depurar los problemas relacionados con SAML mientras el cifrado esté habilitado si no puede ver como texto normal el contenido de la aserción SAML.

c) Revise la ficha **Resumen**.



d) Revise la **Conexión del proveedor de servicios (SP) de Citrix Cloud**. Una vez configurada la **conexión del SP de Citrix Cloud**, debería tener este aspecto:



SP Connections | SP Connection

Connection Type | Connection Options | Metadata URL | General Info | Browser SSO | Credentials | Activation & Summary

Summary information for your SP connection. Click a heading in a section to edit a particular configuration setting.

Summary

SP Connection	
Connection Type	
Connection Role	SP
Browser SSO Profiles	true
Protocol	SAML 2.0
Connection Template	No Template
WS-Trust STS	false
Outbound Provisioning	false
Connection Options	
Browser SSO	true
IdP Discovery	false
Attribute Query	false
Metadata URL	
Metadata URL	https://saml.cloud .com/saml/metadata
Automatically Update Metadata	true
General Info	
Partner's Entity ID (Connection ID)	https://saml.cloud com
Connection Name	CitrixCloudStaging
Base URL	https://saml.cloud .com

Browser SSO	
SAML Profiles	
IdP-Initiated SSO	false
IdP-Initiated SLO	false
SP-Initiated SSO	true
SP-Initiated SLO	true
Assertion Lifetime	
Valid Minutes Before	5
Valid Minutes After	5

Assertion Creation	
Identity Mapping	
Enable Standard Identifier	true
Attribute Contract	
Attribute	SAML_SUBJECT
Subject Name Format	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
Attribute	cip_email
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	cip_oid
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	cip_sid
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	cip_upn
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	displayName
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	firstName
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	lastName
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Authentication Source Mapping	
Adapter instance name	CitrixCloudStagingIDPAdaptor
Adapter Instance	
Selected adapter	CitrixCloudStagingIDPAdaptor
Mapping Method	
Adapter	HTML Form IdP Adapter
Mapping Method	Use only the Adapter Contract values in the mapping
Attribute Contract Fulfillment	
SAML_SUBJECT	username (Adapter)
cip_email	cip_email (Adapter)
cip_oid	cip_oid (Adapter)
cip_sid	cip_sid (Adapter)
cip_upn	cip_upn (Adapter)
displayName	displayName (Adapter)
firstName	firstName (Adapter)
lastName	lastName (Adapter)
Issuance Criteria	
Criterion	(None)

Protocol Settings	
Assertion Consumer Service URL	
Endpoint	URL: /saml/acs (POST)
SLO Service URLs	
Endpoint	URL: /saml/logout/callback (POST) Response URL: /saml/logout/callback
Endpoint	URL: /saml/logout/callback (Redirect) Response URL: /saml/logout/callback
Allowable SAML Bindings	
Artifact	false
POST	true
Redirect	false
SOAP	false
Signature Policy	
Require digitally signed AuthN requests	true
Always Sign Assertion	true
Sign Response As Required	true
Encryption Policy	
Status	Inactive

Credentials	
Digital Signature Settings	
Selected Certificate	CN=*. .com, O="Citrix Systems, Inc.", L=Fort Lauderdale, ST=Florida, C=US (0C:BE:67:B8:63:15:D4:D4:8B:3A:17:65:0F:71:0A:FD | Exp: Sep 19, 2024)
Include Certificate in KeyInfo	false
Selected Signing Algorithm	RSA SHA256

Signature Verification		
Trust Model		
Trust Model	Unanchored	
Signature Verification Certificate		
Active Certificate 1	CN=samlsigning.cloud	.com, O="Citrix Systems, Inc.", L=Fort Lauderdale, ST=Florida, C=US (03:48:4A:61:BF:59:EB:13:9C:20:FE:F1:5B:3A:83:29 | Exp: May 11, 2024)
Active Certificate 2	CN=samlsigning.cloud	.com, O="Citrix Systems, Inc.", L=Fort Lauderdale, ST=Florida, C=US (0B:5F:B5:43:89:16:B0:2F:98:45:58:D1:DA:D1:B1:1D | Exp: Mar 11, 2025)

> **Consejo práctico:**
>
> Use la página Resumen y Activación de la conexión del SP para revisar s aplicación SAML y con fines de depuración, ya que permite realizar cambios de configuración rápidos y sencillos. La página Resumen y Activación de la conexión del SP le permite acceder a cualquiera de las subsecciones de configuración de SAML haciendo clic en el título de esa sección. Haga clic en cualquiera de los títulos resaltados en rojo para actualizar estos parámetros.

Protocol Settings	
Assertion Consumer Service URL	
Endpoint	URL: /saml/acs (POST)
SLO Service URLs	
Endpoint	URL: /saml/logout/callback (POST)
Allowable SAML Bindings	
Artifact	false
POST	true
Redirect	true
SOAP	false
Signature Policy	
Require digitally signed AuthN requests	false
Always Sign Assertion	true
Sign Response As Required	true

16. La **conexión del SP de Citrix Cloud** completada debería mostrarse en la lista de esta manera.

17. Es posible exportar la conexión del SP en forma de archivo XML. Citrix recomienda realizar una copia de seguridad de la conexión del SP una vez que la haya probado con Citrix Cloud y Workspace.

Actualizar el certificado de firma SAML del proveedor de identidades

May 30, 2024

Author:
Mark Dear

Las conexiones SAML que usan solicitudes y respuestas firmadas dependen de dos certificados de firma SAML diferentes. Uno para cada lado de la conexión SAML.

Certificado de firma del proveedor de SAML

El proveedor de SAML proporciona este certificado y se carga en Citrix Cloud al configurar la conexión SAML.

Los certificados de firma de SAML deben rotarse antes de que caduquen para que los administradores de Citrix Cloud tengan tiempo de prepararse para la implementación. Tanto los proveedores de servicios como los proveedores de identidades requieren la rotación de certificados para garantizar la alineación y evitar cualquier tiempo de inactividad.

Preguntas frecuentes

¿Para qué se usa el certificado del proveedor de SAML?

El certificado del proveedor de SAML se usa para verificar la firma de las respuestas SAML enviadas desde el proveedor de SAML a Citrix Cloud durante el proceso de autenticación.

¿Dónde puedo obtener una copia del certificado de firma del proveedor de identidades (IdP) más reciente?

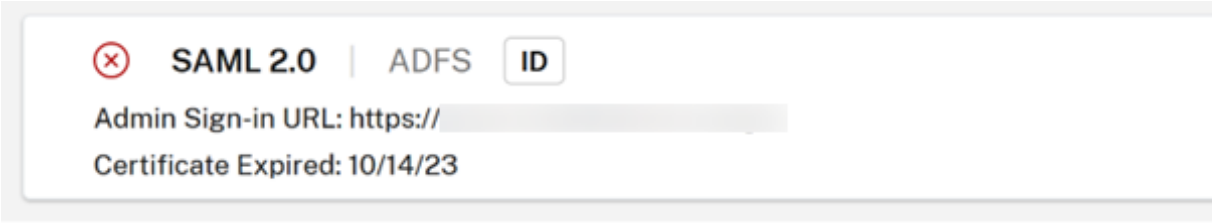
Este certificado lo proporciona su proveedor de SAML, como Azure AD, Okta, PingFederate o ADFS. Citrix no controla la rotación ni la actualización de este certificado. Este certificado se carga en Citrix Cloud cuando se crea inicialmente la conexión SAML. La fecha de caducidad de los **certificados de firma del proveedor de identidades** suele ser de larga duración. Es posible que sea necesario reemplazarlos cada pocos años y con una frecuencia inferior a la del **certificado de firma del proveedor de servicios**

¿Cómo puedo saber si el certificado de firma de mi proveedor de SAML está a punto de caducar y afectar a mi conexión SAML de Citrix Cloud?

Citrix Cloud mostrará advertencias 30 días antes de la fecha de caducidad del certificado de firma de su proveedor de SAML.

```
Certificate Expiring Soon: <certExpirationDate>
```

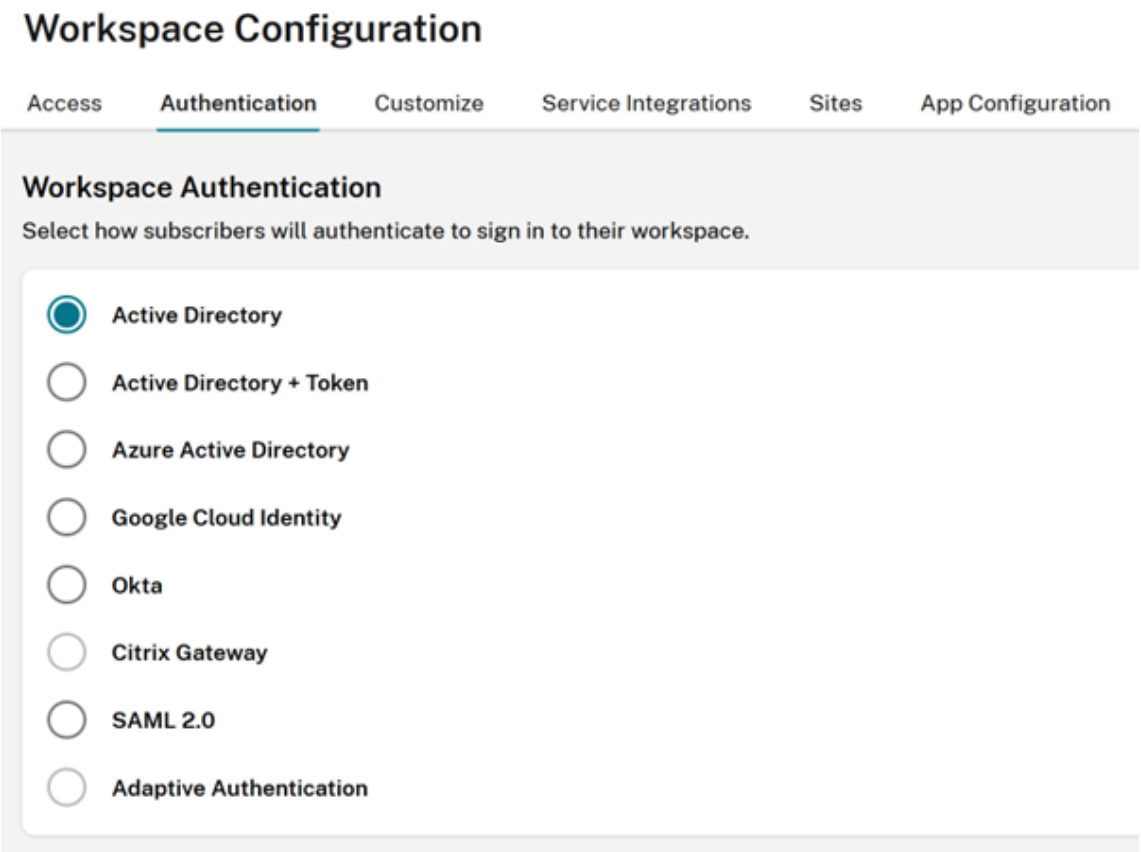
También mostrará un error una vez que el certificado haya caducado, como se muestra a continuación.



¿Puedo actualizar el certificado del proveedor de SAML y seguir usando la conexión SAML sin tiempo de inactividad?

No. Es necesario realizar una desconexión de SAML y volver a conectar durante un período de mantenimiento programado.
Actualizar el certificado de firma del proveedor de identidades (IdP)

1. Seleccione un IdP alternativo en **Configuración de Workspace** y seleccione **Autenticación** mientras realiza la operación de desconexión y reconexión de SAML, como Active Directory.



2. Haga una copia de reserva de la URL de GO existente, como `https://citrix.cloud.com/go/<yourgourl>`, usada para iniciar sesión con SAML en Citrix Cloud.
3. Haga una copia de reserva de sus dispositivos de punto final de SAML. Estos se pueden copiar

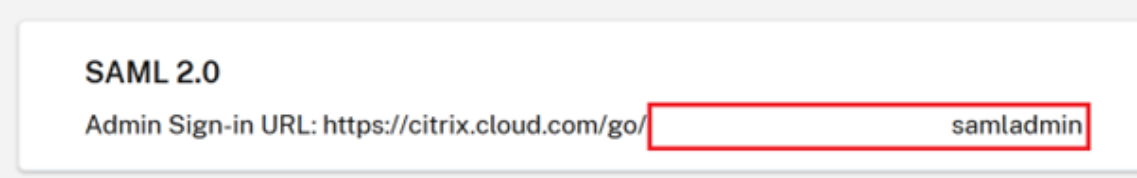
desde la consola de Citrix Cloud. Haga una copia de reserva de los dispositivos de punto final de SAML siguientes desde su conexión SAML.

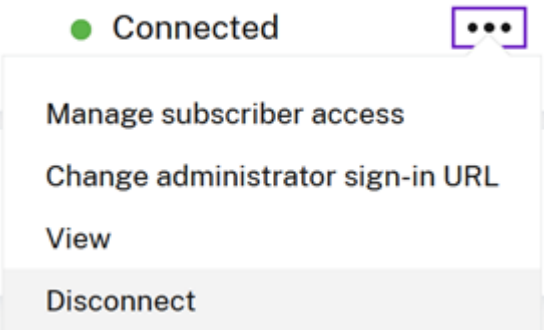
- ID de entidad del proveedor de identidades
- URL del servicio SSO del proveedor de identidades
- URL de cierre de sesión del proveedor de identidades

Haga una copia de reserva del ID de entidad, la URL de SSO y la URL de cierre de sesión.

> **Importante:**
>
> Asegúrese de que tiene una copia del certificado de firma del IdP existente y del de reemplazo antes de realizar la desconexión. De este modo, podrá revertir al certificado anterior si el nuevo certificado del proveedor de SAML no es válido y provoca problemas de inicio de sesión. No podrá obtener una copia del certificado antiguo desde la interfaz de usuario de Citrix Cloud antes de realizar la desconexión. Tendrá que obtenerlo de su aplicación SAML.

1. Desconecte SAML en **Administración de acceso e identidad**, vaya a **Autenticación**, seleccione la conexión SAML, haga clic en los puntos suspensivos y seleccione **Desconectar**
2. Reconecte SAML en **Administración de acceso e identidad** y haga clic en **Autenticación**





3. Acepte todos los parámetros de conexión SAML predeterminados.
4. Introduzca de nuevo todos los dispositivos de punto final de la aplicación SAML de los que haya realizado copia de reserva anteriormente o vuelva a obtenerlos para su aplicación SAML desde la interfaz de usuario de su proveedor de SAML.

- ID de entidad del proveedor de identidades
- URL del servicio SSO del proveedor de identidades
- URL de cierre de sesión del proveedor de identidades

> **Importante:**
>
> Si usa la función ID de entidad con ámbito, tendrá que actualizar su aplicación SAML con el nuevo ID de ámbito después de realizar la desconexión o reconexión de SAML. Para obtener más información sobre la función ID de entidad con ámbito, consulte Configurar una aplicación SAML mediante un ID de entidad con ámbito en Citrix Cloud. Copie el ID de ámbito recién generado de la interfaz de usuario de SAML de Citrix Cloud y actualice el ID de entidad de la aplicación SAML con el ID de ámbito de reemplazo.
> El ID de entidad debe actualizarse a `https://saml.cloud.com/<new scope ID after reconnect>`.

Actualizar el certificado de firma SAML del proveedor de servicios

May 30, 2024

Author:
Mark Dear

Las conexiones SAML que usan solicitudes y respuestas firmadas dependen de dos certificados de firma SAML diferentes. Uno para cada lado de la conexión SAML.

Certificado de firma del proveedor de servicios

Citrix proporciona este certificado de forma periódica y lo carga en su aplicación SAML o lo obtiene mediante los metadatos de SAML de Citrix Cloud.

Los certificados de firma de SAML deben rotarse antes de que caduquen para que los administradores de Citrix Cloud tengan tiempo de prepararse para la implementación. Tanto los proveedores de servicios como los proveedores de identidades exigen la rotación de certificados para garantizar la alineación y evitar cualquier tiempo de inactividad.

Si un proveedor de SAML seleccionado no admite la rotación automática del certificado de firma de SAML del proveedor de servicios, se debe realizar una rotación manual para reemplazar el certificado que vence.

> **Importante:**
>
> Todas las guías existentes en esta sección de documentos electrónicos de SAML incluyen detalles sobre cómo configurar la firma en ambos lados de la conexión SAML. Citrix solo recomienda con-

> figuraciones de SAML firmadas, ya que son más seguras y algunos proveedores de SAML las requieren para cerrar sesión (SLO) correctamente.

Preguntas frecuentes

¿Qué es la firma SAML?

Los certificados de firma SAML son certificados X.509 que sirven para verificar los datos enviados entre el proveedor de servicios (SP) y el proveedor de SAML (IdP). Su proveedor de SAML (IdP) usa el certificado de firma SAML de Citrix Cloud para verificar la firma enviada por Citrix Cloud en su solicitud de autenticación SAML. Citrix Cloud usa el certificado de firma del proveedor de SAML para verificar que la respuesta SAML proviene de un IdP conectado y de confianza.

¿Qué es la aplicación de solicitudes firmadas con SAML?

El hecho de que Citrix Cloud esté configurado para enviar solicitudes firmadas no garantiza que el proveedor de SAML imponga el uso de firmas ni rechace las solicitudes de SAML entrantes sin firmar. La mayoría de los proveedores de SAML tienen una opción para exigir solicitudes firmadas, lo que significa que, si se recibe una solicitud sin firmar para iniciar sesión en el proveedor de SAML, el inicio de sesión fallará. Es responsabilidad del administrador del proveedor de SAML comprobar el estado de la configuración del IdP. La asistencia técnica de Citrix no controla ni tiene ninguna visibilidad sobre si las solicitudes firmadas se exigen en la aplicación SAML.

¿Con qué frecuencia rota Citrix el certificado de firma SAML del proveedor de servicios?

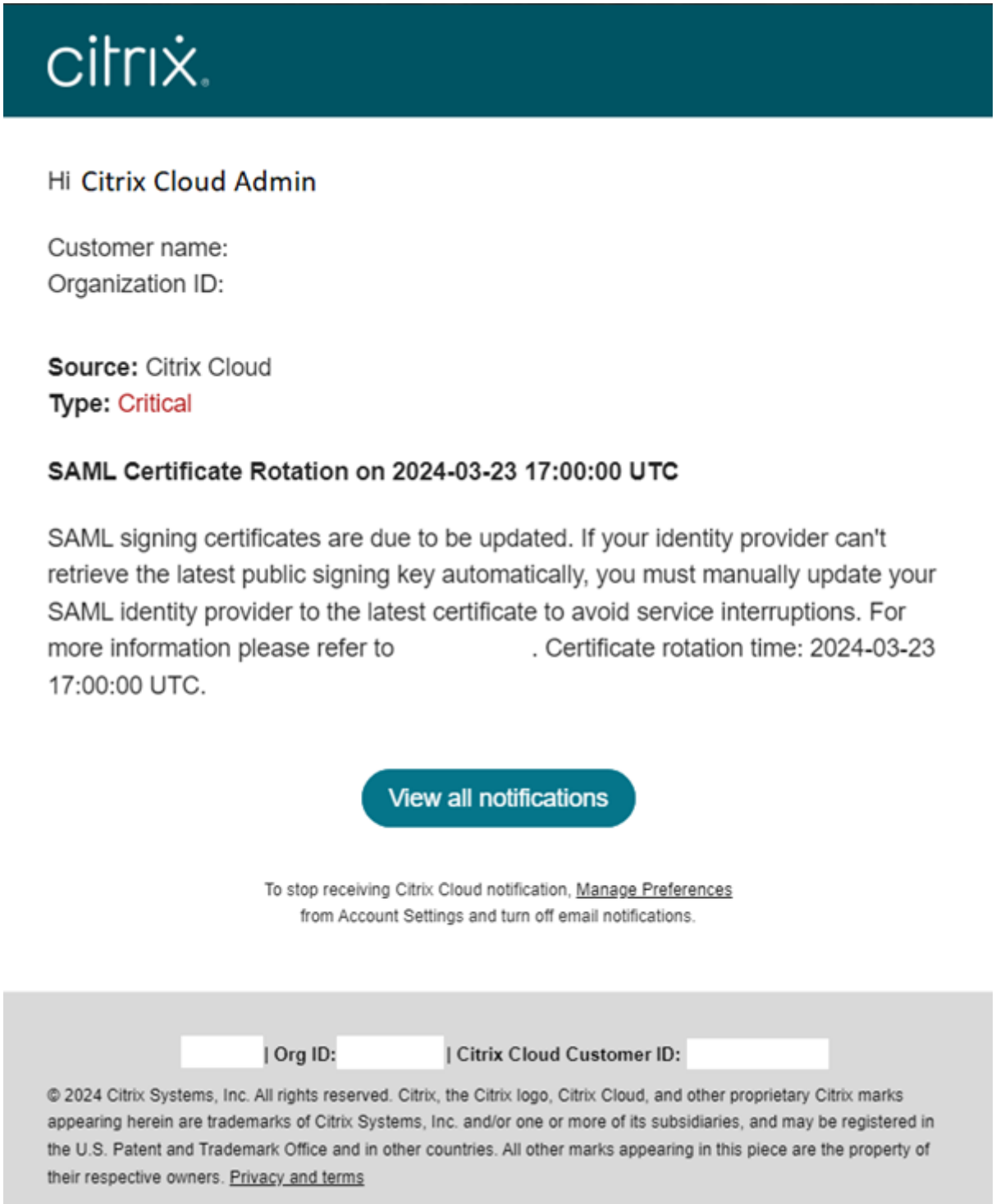
Para permitir una superposición suficiente entre el certificado de firma del proveedor de servicios activo y el recién emitido, Citrix rota el certificado de firma del proveedor de servicios aproximadamente cada 11 meses. Esto sirve para garantizar que haya un certificado válido disponible para los clientes de Citrix Cloud 30 días antes de que caduque el certificado existente.

¿Qué es la fase de anuncio del certificado de firma SAML del proveedor de servicios?

Durante la fase de anuncio, los certificados de firma SAML actual y de reemplazo estarán presentes en los metadatos de Citrix Cloud. Hasta la fecha y hora de rotación, solo se puede usar el certificado activo para la verificación de solicitudes SAML.

¿Por qué he recibido una notificación por correo electrónico y en la consola de administración de Citrix Cloud que indica que el certificado de firma SAML actual de Citrix Cloud está a punto de caducar y debe sustituirse?

Los proveedores de SAML (IdP) requieren un certificado válido y actualizado para verificar la firma de las solicitudes SAML entrantes de los proveedores de servicios, como Workspace y la consola de administrador de Citrix Cloud. Nos pondremos en contacto con los clientes de Citrix Cloud que usen SAML para iniciar sesión en Workspace o en la consola de administración de Citrix Cloud para informarles de una rotación inminente de los certificados de firma SAML.



citrix.

Hi **Citrix Cloud Admin**

Customer name:
Organization ID:

Source: Citrix Cloud
Type: Critical

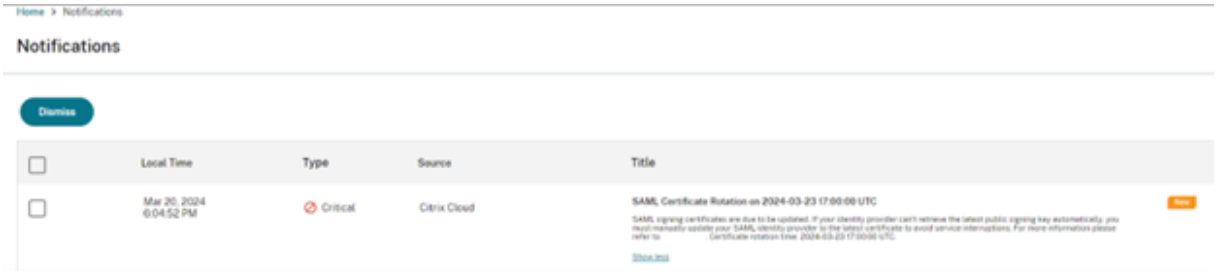
SAML Certificate Rotation on 2024-03-23 17:00:00 UTC

SAML signing certificates are due to be updated. If your identity provider can't retrieve the latest public signing key automatically, you must manually update your SAML identity provider to the latest certificate to avoid service interruptions. For more information please refer to . Certificate rotation time: 2024-03-23 17:00:00 UTC.

View all notifications

To stop receiving Citrix Cloud notification, Manage Preferences from Account Settings and turn off email notifications.

| Org ID: | Citrix Cloud Customer ID:



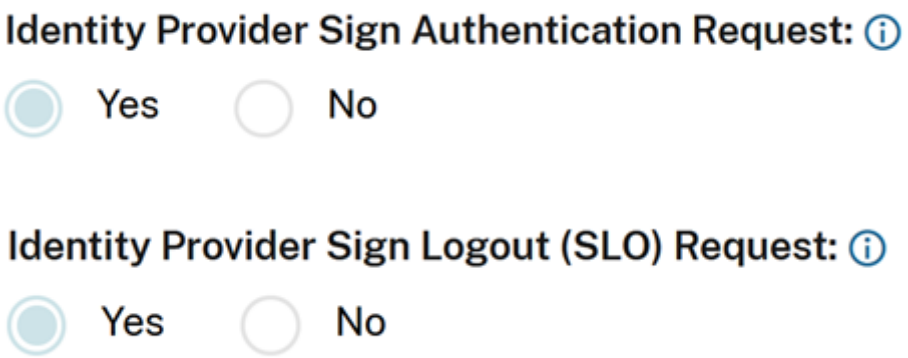
¿Cómo puedo saber si mi cliente de Citrix Cloud se ve afectado por la rotación de certificados de firma SAML de Citrix Cloud o no?

Esto afectará a los clientes de Citrix Cloud con la siguiente configuración de SAML.

- Su conexión SAML en Citrix Cloud está configurada con **Firmar solicitud de autenticación = Sí**
- Ha configurado su proveedor de SAML, como Azure Active Directory, ADFS u Okta, para rechazar las solicitudes SAML sin firmar (aplicación de solicitudes firmadas).
- Tiene el cierre de sesión único (SLO) configurado en su conexión SAML de Citrix Cloud y en su proveedor de SAML. Es posible que su proveedor de SAML requiera la firma de las solicitudes de SLO, como las de Okta y PingFederate.

¿Cómo compruebo la configuración de firma de mi conexión SAML de Citrix Cloud?

Vaya a **Administración de acceso e identidad** > **SAML 2.0** > **Ver** para comprobar si tiene habilitado **Firmar solicitud de autenticación** en su conexión SAML de Citrix Cloud. Todas las conexiones SAML nuevas en Citrix Cloud tendrán el valor predeterminado **Solicitud de cierre de sesión/autenticación de firma del proveedor de identidades = Sí**, tanto para el inicio de sesión (SSO) como para el cierre de sesión (SLO).



¿Cómo compruebo si el uso obligado de firma está configurado en mi aplicación SAML?

Esto varía en función del proveedor de SAML que use. Es posible que algunos ni siquiera ofrezcan esta opción. AzureAD, ADFS, Okta y PingFederate admiten el uso obligado de firmas. Es fundamental que el administrador de SAML conozca las capacidades de su proveedor de SAML y su configuración actual. La asistencia técnica de Citrix no tiene control ni visibilidad sobre esto.

¿Dónde puedo obtener una copia del certificado de firma del proveedor de servicios (SP) más reciente?

Citrix proporciona este certificado a través de los metadatos de SAML de Citrix Cloud y se actualiza periódicamente durante la fase de anuncio de la rotación de certificados de firma del SP. Esto ocurre al menos una vez por año natural.

EE. UU., UE y APS: https://saml.cloud.com/saml/metadata

JP: https://saml.citrixcloud.jp/saml/

GOV: https://saml.cloud.us/saml/metadata

¿Cuándo es seguro quitar el antiguo certificado de firma SAML de Citrix Cloud si mi aplicación SAML admite varios certificados de verificación?

No quite el antiguo certificado de firma de Citrix Cloud hasta la fecha y hora de rotación del certificado indicadas en el correo electrónico y en la notificación de la consola de administración de Citrix Cloud.

Usar el intercambio de metadatos para actualizar automáticamente el proveedor de SAML con el certificado de firma SAML más reciente del proveedor de servicios (SP) de Citrix Cloud

Mediante el intercambio de metadatos de SAML, el proveedor de SAML consume los metadatos de SAML de Citrix Cloud automáticamente al supervisar la URL de los metadatos, como https://saml.cloud.com/saml/metadata. Si su proveedor de SAML admite el intercambio de metadatos de SAML, es posible que el certificado de firma del SP ya se haya actualizado automáticamente.
Verifique que su proveedor de SAML admite el intercambio de metadatos. Después, puede verificar si la actualización ha tenido lugar antes de que caduque el certificado de firma SAML actual.

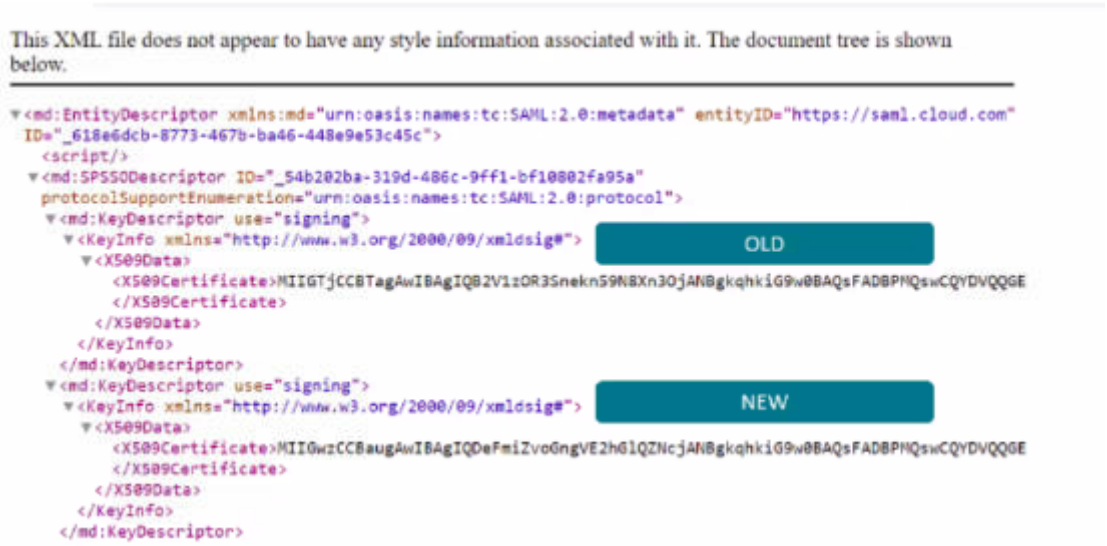
> **Importante**
>
> Hay una gran variación en términos de las funciones de SAML que admite cada proveedor de SAML externo. Es responsabilidad del administrador de Citrix Cloud conocer y comprender las capacidades y los requisitos del proveedor de SAML usado. Esto es necesario para garantizar que la configuración del proveedor de SAML (proveedor de identidades) y la configuración de conexión SAML (proveedor de servicios) de Citrix Cloud coincidan. Consulte la documentación de su proveedor de SAML para determinar si admite la verificación de firmas y si las solicitudes y respuestas de SAML deben firmarse.

Actualizar manualmente el proveedor de SAML con el certificado de firma SAML más reciente del proveedor de servicios de Citrix Cloud

> **Importante**
>
> La rotación del certificado del proveedor de servicios se debe realizar cada vez que se publique un nuevo certificado desde Citrix Cloud; de lo contrario, el inicio de sesión de SAML se verá afectado y se producirá un tiempo de inactividad.

1. Para adquirir los metadatos de SAML más recientes de Citrix Cloud, consulte su conexión SAML actual en **Administración de acceso e identidad**, haga clic en **Autenticación**, seleccione **Conexión SAML** y haga clic en **Ver**.
   La siguiente imagen es un ejemplo del aspecto que podría tener este archivo en regiones de Citrix Cloud como EE. UU., UE y APS:

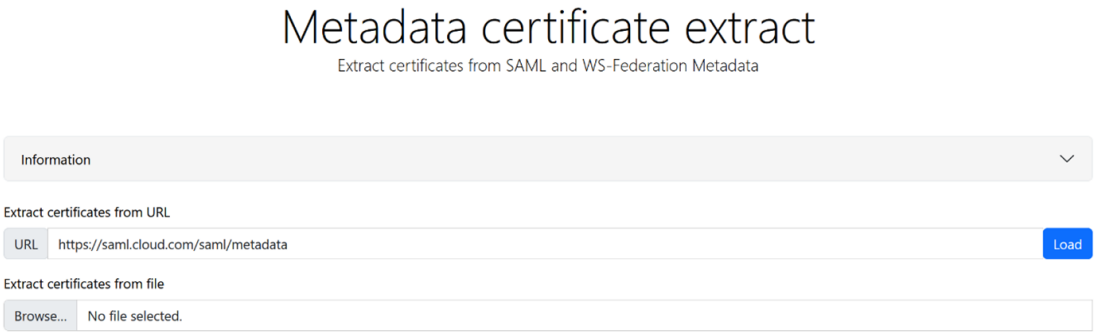
   https://saml.cloud.com/saml/metadata



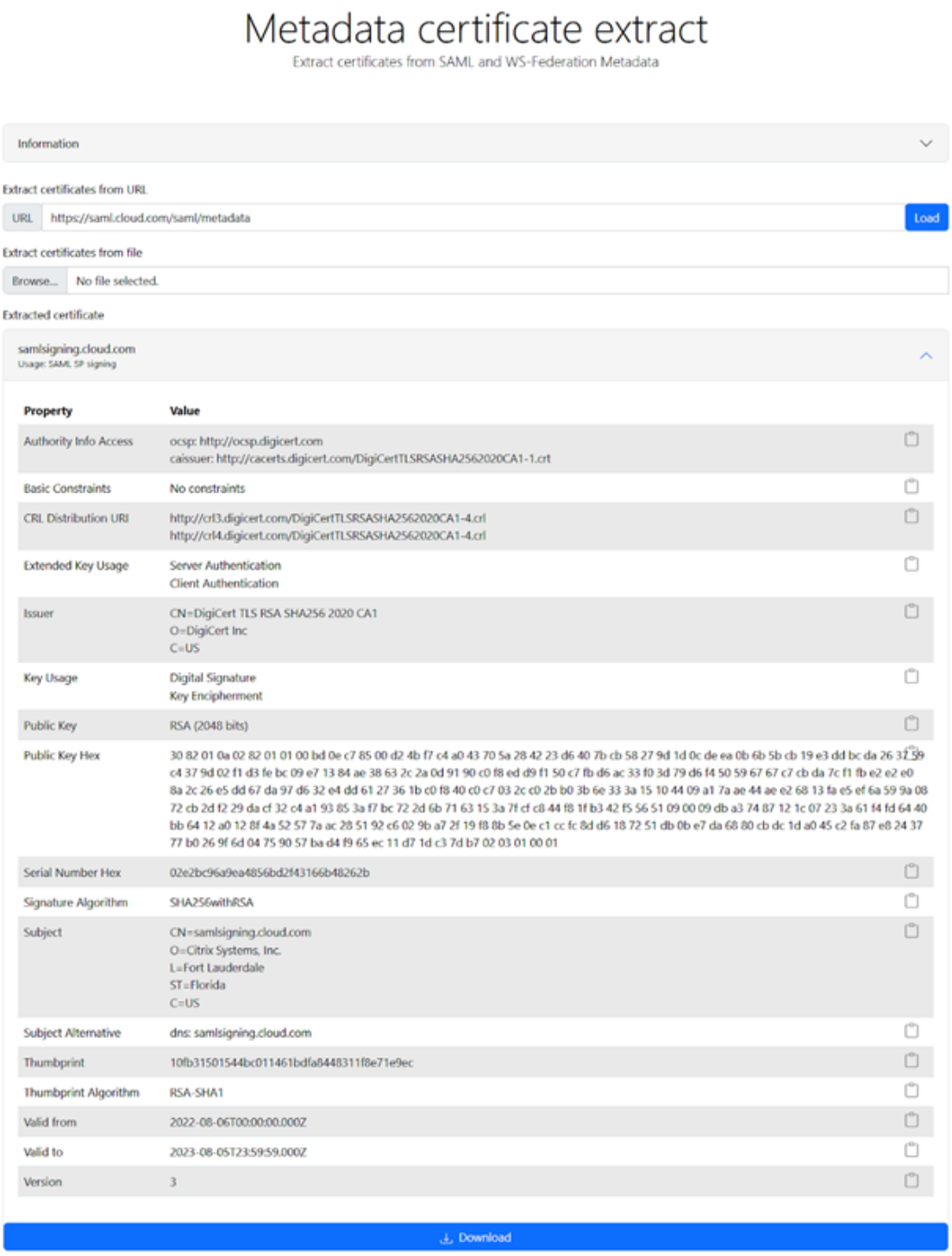
En este ejemplo de archivo XML de metadatos, hay dos certificados de firma SAML x509 de Citrix Cloud.

2. Es posible extraer el certificado x509 de los metadatos cargando el archivo XML en una herramienta de terceros o proporcionando la URL de los metadatos.
3. Vaya a https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract
4. Introduzca la URL de metadatos de SAML correspondiente a la región de su cliente de Citrix Cloud:

   - EE. UU., UE y APS: https://saml.cloud.com/saml/metadata
   - JP: https://saml.citrixcloud.jp/saml/metadata
   - GOV: https://saml.cloud.us/saml/metadata



Descargue el certificado de firma SAML desde https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract.



5. Cargue el certificado SAML del proveedor de servicios de Citrix Cloud recién extraído en su proveedor de SAML. Este proceso será diferente para cada proveedor de SAML. Verifique que el procedimiento de rotación de certificados de firma del proveedor de servicios es correcto. Para ello, consulte la documentación específica de su proveedor de SAML.

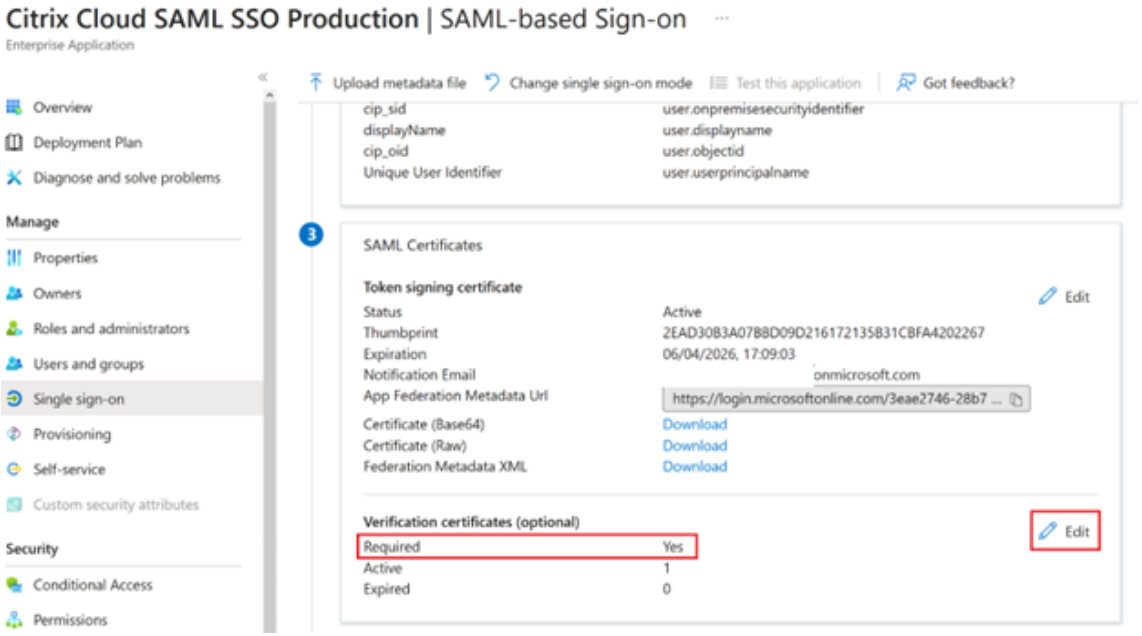
   En función del proveedor de SAML, es posible que sea necesario reemplazar el certificado de

firma de SAML existente por uno nuevo. En algunos casos, el proveedor de SAML puede admitir varios certificados de firma de SP al mismo tiempo, por lo que solo bastará con cargar el nuevo. Se recomienda quitar el certificado antiguo una vez que haya caducado.

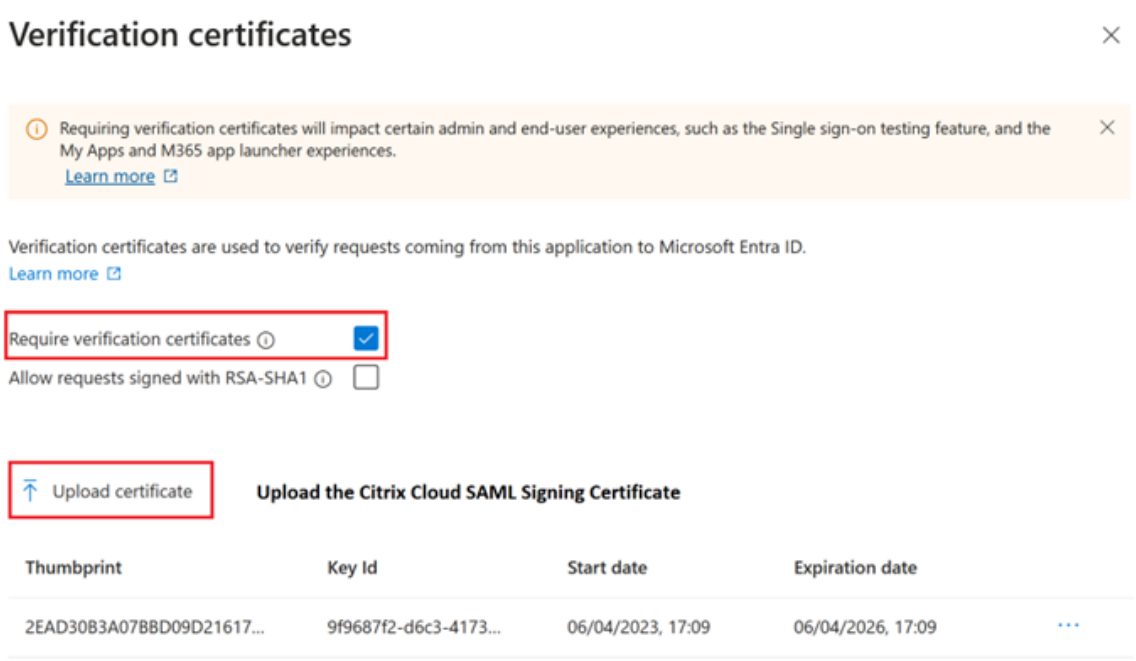
Cargar un certificado de firma SAML de Citrix Cloud de reemplazo en su aplicación SAML de Azure Active Directory

Antes de configurar la aplicación SAML de Azure Active Directory, consulte SAML Request Signature Verification para obtener más información.

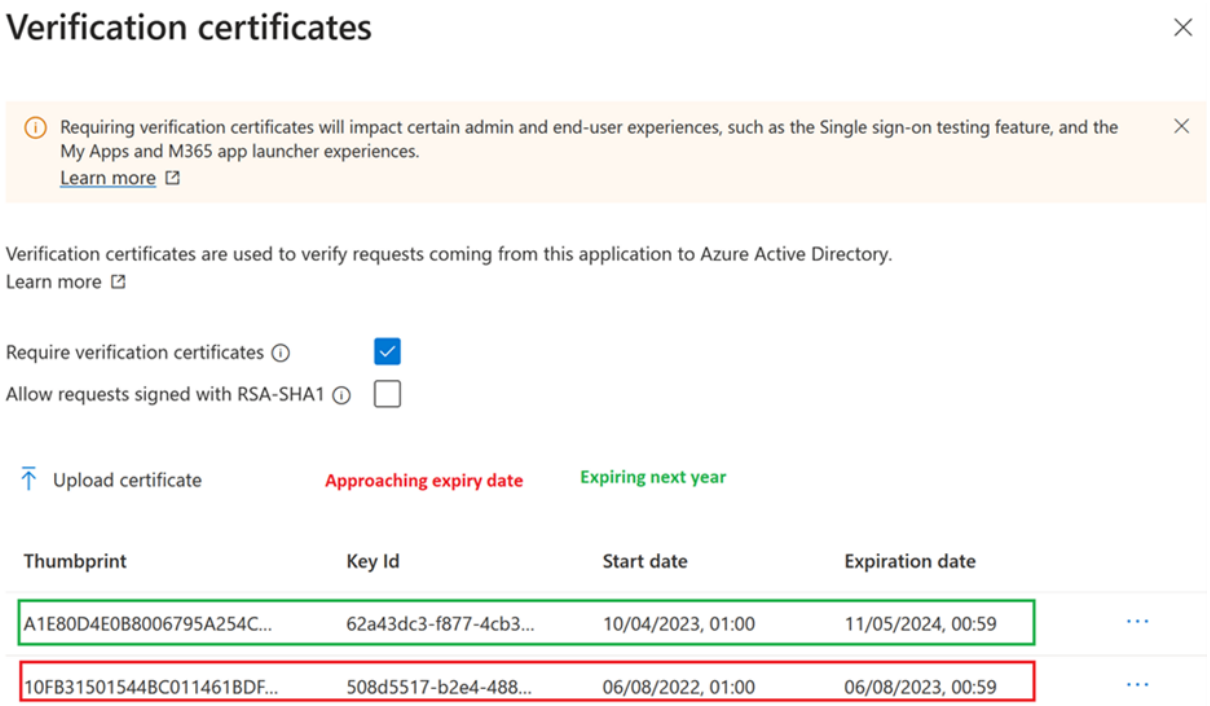
1. Vaya a **Azure Active Directory**, seleccione **Enterprise Applications** y haga clic en su aplicación SAML.
2. Busque la sección de certificados SAML dentro de la aplicación SAML.



3. Seleccione **Upload Certificate** y cargue el certificado de firma SAML de Citrix Cloud de reemplazo obtenido de los metadatos de SAML.



> **Nota:**
>
> Las aplicaciones SAML de Azure Active Directory pueden tener configurados varios certificados de verificación de firma para que sea posible cargar un certificado de reemplazo mucho antes de que caduque el certificado actual. La siguiente captura de pantalla muestra dos certificados válidos. Uno de los certificados caducará en un futuro próximo. Siempre que al menos uno de los certificados cargados sea válido y no haya caducado, el inicio de sesión con SAML en Citrix Workspace y Citrix Cloud seguirá funcionando correctamente y no se producirá ninguna interrupción.

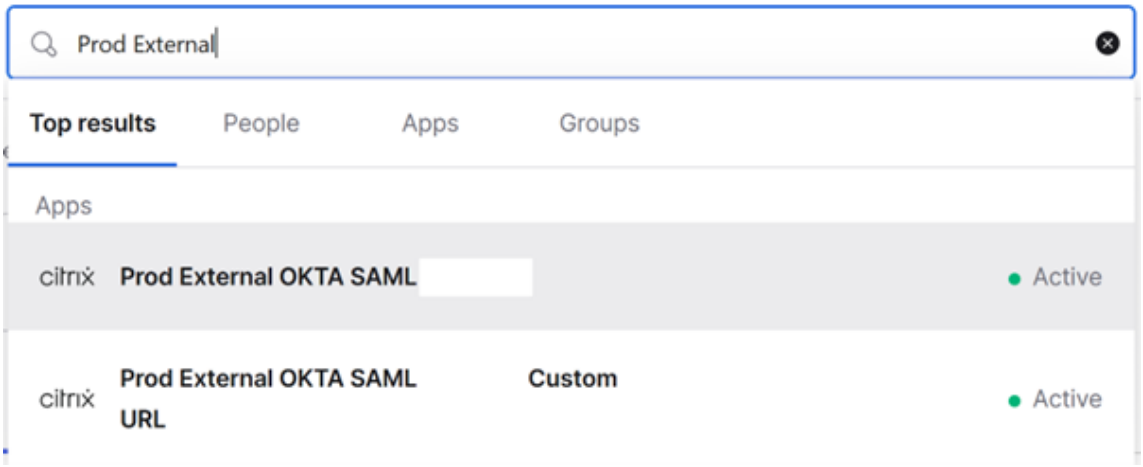


> **Importante:**
>
> No quite el certificado de verificación existente hasta que hayan pasado la fecha y la hora de rotación de SAML indicadas en el correo electrónico y en la notificación de la consola de administración de Citrix Cloud. El nuevo certificado de Citrix Cloud se activa solo en la fecha y la hora indicadas en esas dos notificaciones.

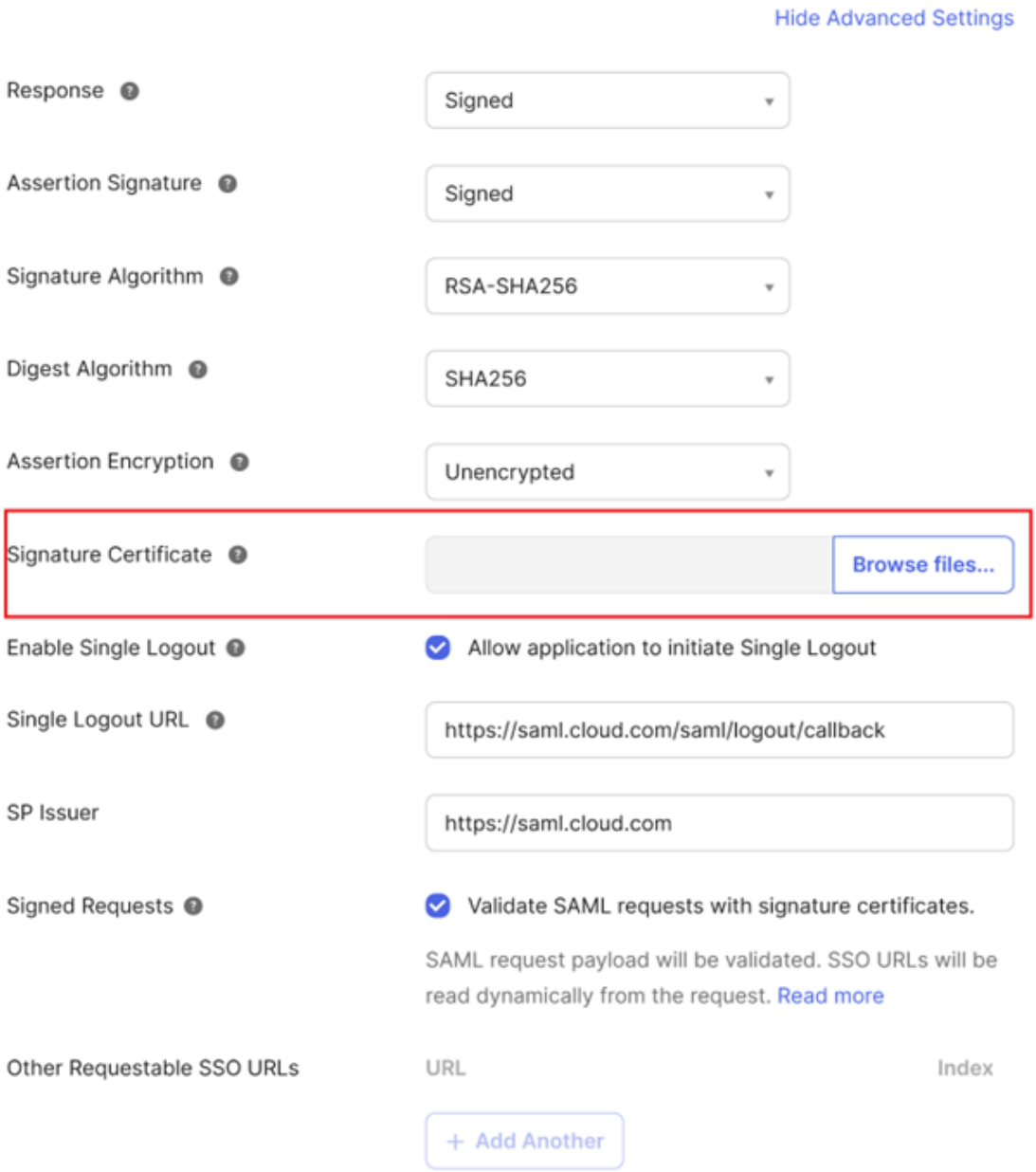
Cargar un certificado de firma SAML de Citrix Cloud de reemplazo en su aplicación SAML de Okta

Okta no admite varios certificados de firma SAML de proveedor de servicios (SP) al mismo tiempo. No tiene más opción que sobrescribir el certificado de firma de SP de Citrix Cloud que utiliza actualmente con el nuevo. Se recomienda hacerlo en un período de mantenimiento programado.

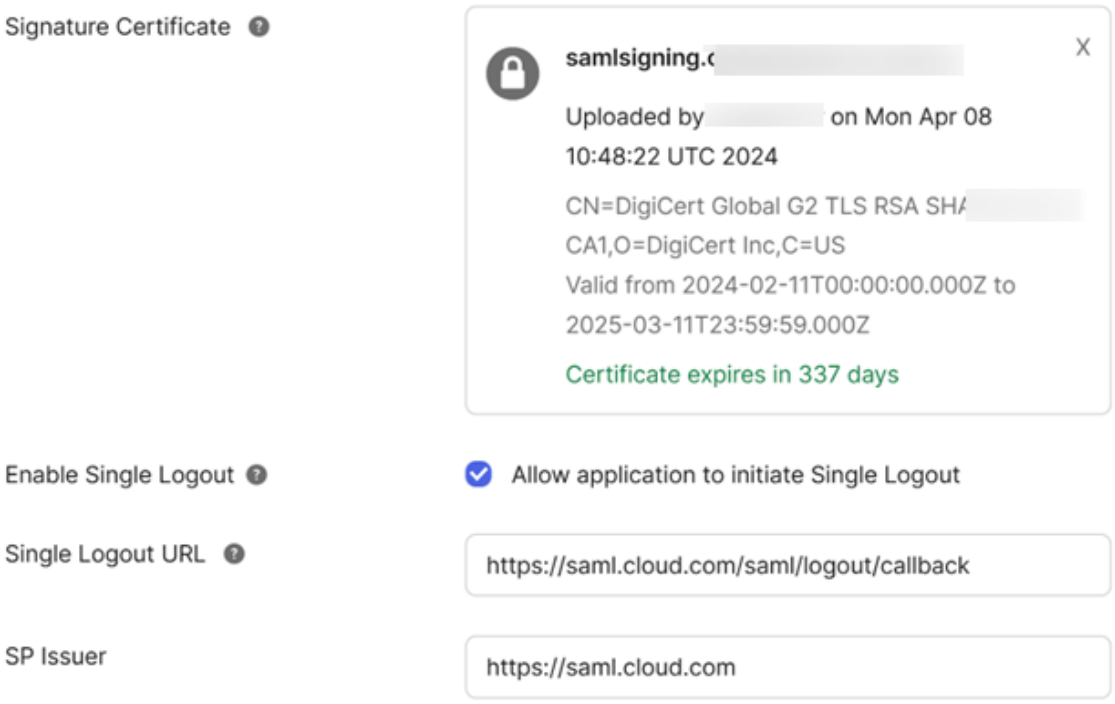
1. Vaya a **Applications**, seleccione **Applications** y busque su aplicación SAML de Okta



2. En **General**, vaya a **SAML Settings**, haga clic en **Edit**, seleccione **Configure SAML**, seleccione **Show Advanced Settings** y haga clic en **Signature Certificate** para cargar el certificado de reemplazo. Okta no muestra el certificado de firma SAML de Citrix Cloud actual en la interfaz de usuario de carga. Solo mostrará el certificado de reemplazo una vez que se haya cargado.



3. Seleccione **Signature Certificate**, haga clic en **Browse Files** y cargue el certificado de firma SAML de Citrix Cloud de reemplazo obtenido de los metadatos de SAML de Citrix Cloud.



> **Importante**
>
> No sobrescriba el certificado de verificación existente hasta la fecha y la hora de rotación de SAML indicadas en el correo electrónico y en la notificación de la consola de administración de Citrix Cloud. El nuevo certificado de Citrix Cloud solo se activa en la fecha y la hora indicadas en esas dos notificaciones.

Configurar ADFS como proveedor SAML para la autenticación de espacios de trabajo

July 2, 2024

Author:
Mark Dear

En este artículo se describe cómo configurar la confianza de usuario de confianza que Citrix Cloud requiere para iniciar sesión en Citrix Workspace o Citrix Cloud mediante SAML.

Tras completar los pasos que se indican en este artículo, puede configurar la conexión SAML entre el servidor ADFS y Citrix Cloud, tal y como se describe en Conectar SAML como proveedor de identidades con Citrix Cloud. Para obtener instrucciones para introducir los valores de ADFS correctos para la conexión SAML, consulte la sección Configuración de SAML en Citrix Cloud de este artículo.

Requisitos previos

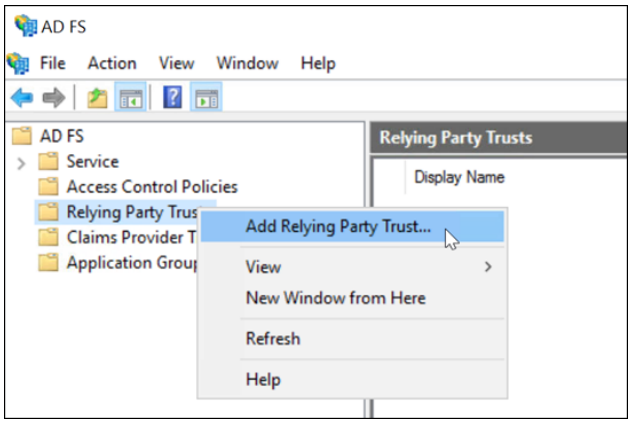
En las instrucciones de este artículo se supone que tiene una implementación de servidor ADFS operativa con Citrix FAS en su entorno. Citrix FAS debe proporcionar Single Sign-On a los VDA durante el inicio de las sesiones.

Para obtener más información, consulte los siguientes artículos:

- Documentación de Citrix FAS:
  - Instalar y configurar
  - Implementación ADFS
- Citrix Tech Zone: Arquitectura de referencia: Servicio de autenticación federada

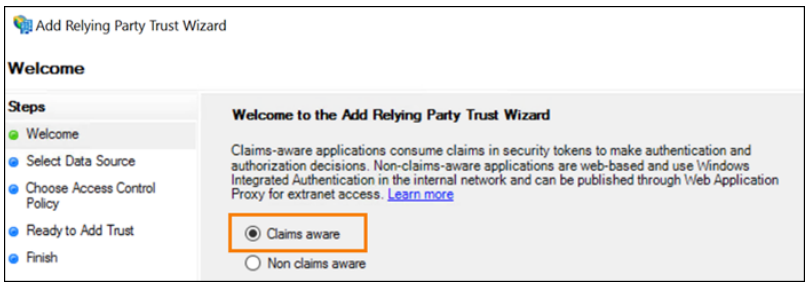
Configurar confianza de un usuario de confianza para Citrix Cloud

1. Desde la consola de administración de AD FS, expanda el nodo de **AD FS** en el panel izquierdo.
2. Haga clic con el botón secundario en **Relying Party Trust** y seleccione **Add Relying Party Trust**.

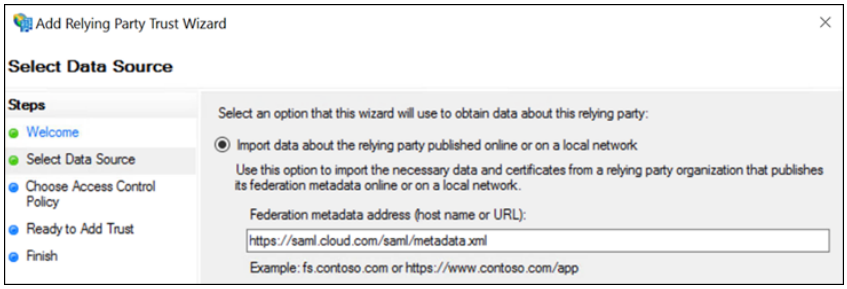


   Aparecerá el asistente Add Relying Party Trust.

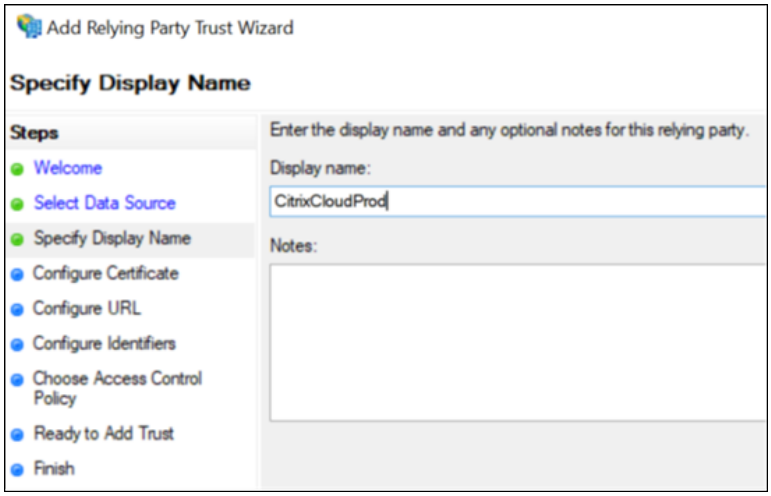
3. Seleccione **Claims aware** y, a continuación, seleccione **Next**.



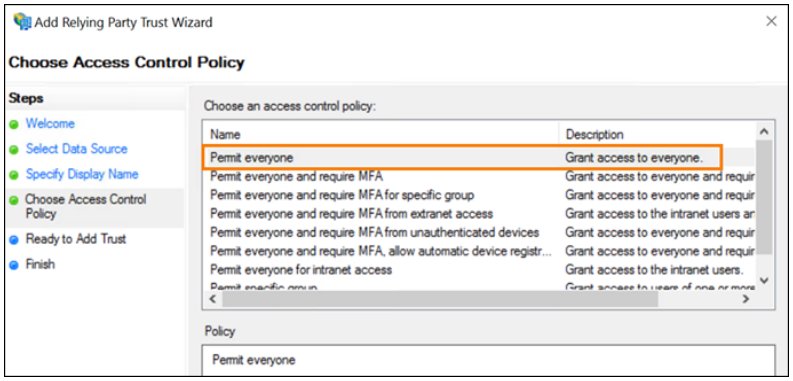
4. En **Federation metadata address**, introduzca `https://saml.cloud.com/saml/metadata.xml`. Seleccione **Siguiente**.



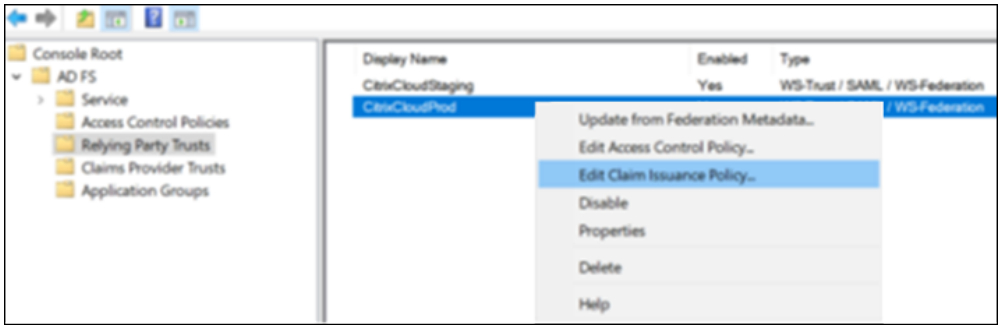
5. Para el nombre simplificado, introduzca `CitrixCloudProd`. Seleccione **Siguiente**.



6. Para la directiva de control de acceso, seleccione **Permit everyone**. Seleccione **Siguiente**.

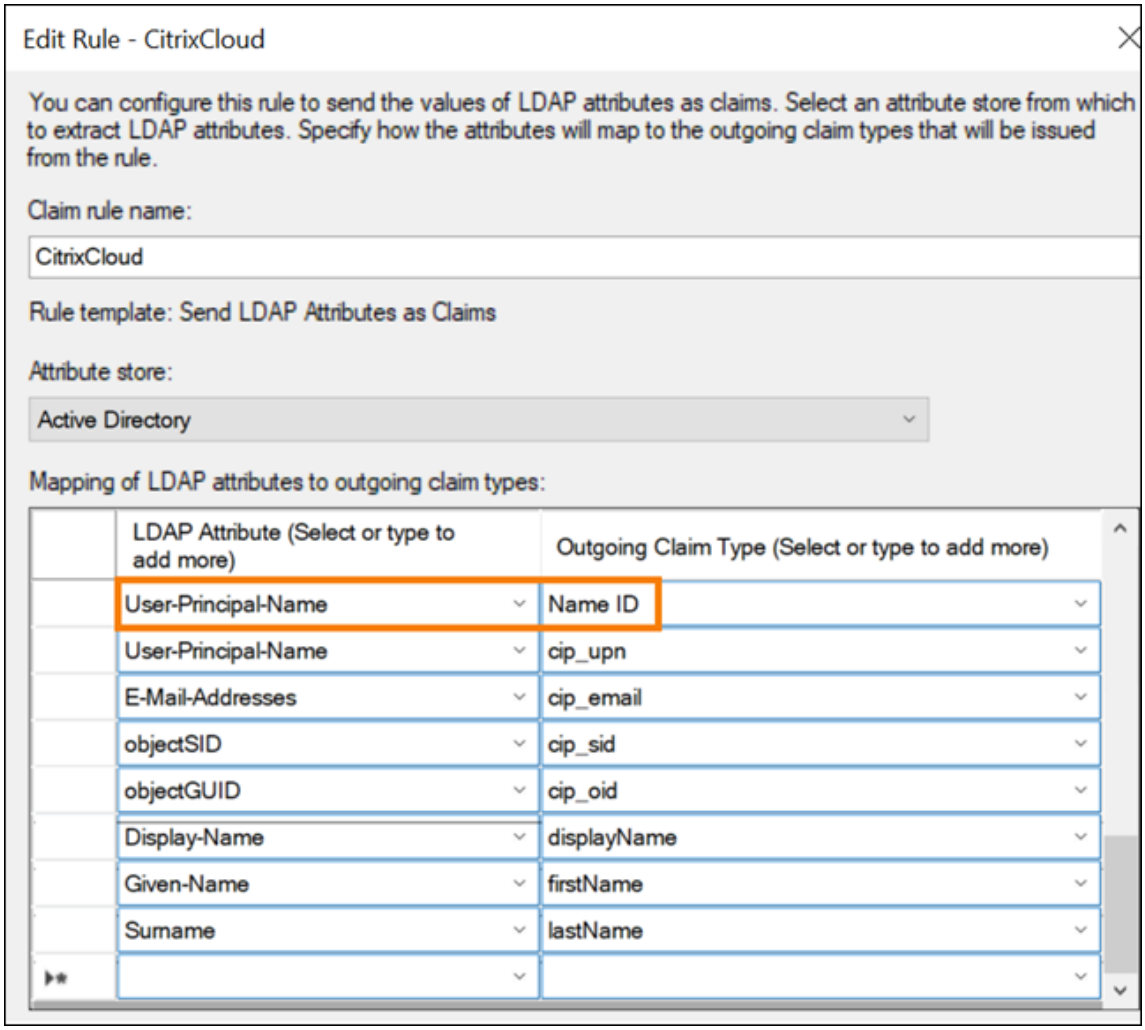


7. En la pantalla **Ready to Add Trust**, seleccione **Next**.
8. En la pantalla **Finish**, seleccione **Configure claims issuance policy for this application**. Seleccione **Siguiente**.



9. Haga clic con el botón secundario en la confianza de usuario de confianza recién creada y seleccione **Edit Claim Issuance Policy**.
10. Haga clic en **Add Rule** y, a continuación, seleccione **Send LDAP Attributes as Claims**. Seleccione **Siguiente**.
11. En **Claim rule name**, introduzca `CitrixCloud`.
12. En el **Attribute store**, seleccione **Active Directory**.
13. En **Mapping of LDAP attributes to outgoing claim types**, agregue los siguientes atributos LDAP, tal y como se muestra:

Atributo LDAP	Tipo de notificación de salida
userprincipalname	Name ID
userprincipalname	cip_upn
E-Mail-Addresses	cip_email
objectSID	cip_sid
objectGUID	cip_oid
Display-Name	displayName
Given-Name	firstName
Surname	lastName



14. Seleccione **Finish**.

Modificar la confianza de un usuario de confianza de Citrix Cloud mediante PowerShell

Si ha configurado el servidor ADFS con la configuración predeterminada "listo para usar", los pasos de esta sección le permiten actualizarlo para que cumpla con la configuración recomendada por Citrix. Esta tarea es necesaria para resolver un problema en el que se produce un error en el cierre de sesión único de SAML desde Citrix Cloud o Citrix Workspace si el atributo `nameidentifier` no está incluido en el conjunto de reglas de notificación o no es el primer atributo de SAML del conjunto de reglas de notificación.

> **Nota:**
>
> No es necesario que realice esta tarea si creó su conjunto de reglas de notificación siguiendo los pasos de la sección Configurar confianza de un usuario de confianza para Citrix Cloud de este artículo.

Para completar esta tarea, sustituya el conjunto de reglas existente por un nuevo conjunto de reglas de notificación mediante PowerShell. La consola de administración de ADFS no admite este tipo de operación.

1. En el servidor ADFS, busque el ISE de PowerShell. Haga clic con el botón secundario y seleccione **Run as administrator**.
2. Haga una copia de seguridad de sus reglas de notificación de ADFS existentes en un archivo de texto:

```
Get-ADFSRelyingPartyTrust -name "CitrixCloudStaging" | Select-
    Object -ExpandProperty IssuanceTransformRules | Out-File "$env:
    USERPROFILE\desktop\claimrulesbackup.txt"
<!--NeedCopy-->
```

3. Descargue el archivo claimrules.txt que Citrix proporciona en https://github.com/citrix/sample-scripts/tree/master/citrix-cloud.
4. Copie el archivo claimrules.txt en su escritorio.
5. Importe las reglas de notificación necesarias del archivo claimrules.txt:

```
Set-ADFSRelyingPartyTrust -Name "CitrixCloudProd" `
                      -MetadataUrl "https://saml.cloud.com/saml/
                         metadata" `
                      -AutoUpdateEnabled $True `
                      -IssuanceTransformRulesFile "$env:
                         USERPROFILE\desktop\claimrules.txt" `
                      -SignedSamlRequestsRequired $True `
                      -SamlResponseSignature "MessageAndAssertion"
                          `
                      -Enabled $True
<!--NeedCopy-->
```

Actualice la configuración de firma de SAML para la confianza de usuario de confianza mediante PowerShell

De forma predeterminada, las confianzas de usuario de confianza de ADFS tienen la configuración siguiente:

- EncryptClaims: True
- SignedSamlRequestsRequired: False
- SamlResponseSignature: AssertionOnly

Para mayor seguridad, Citrix recomienda utilizar solicitudes SAML firmadas tanto para Single Sign-On (SSO) como para el cierre de sesión único. En esta sección se describe cómo actualizar la configuración de firma de una confianza de usuario de confianza existente mediante PowerShell para que cumpla con la configuración recomendada por Citrix.

1. Obtenga la configuración actual de RelyingPartyTrust de su servidor ADFS.

```
Get-ADFSRelyingPartyTrust -TargetName "CitrixCloudProd"
<!--NeedCopy-->
```

2. Actualice la configuración de confianza de usuario de confianza de **CitrixCloudProd**.

```
Set-ADFSRelyingPartyTrust -Name "CitrixCloudProd" `
                          -SignedSamlRequestsRequired $True `
                          -SamlResponseSignature "MessageAndAssertion"
<!--NeedCopy-->
```

3. Póngase en contacto con Citrix Support y solicite activar la función de autenticación **EnableSamlLogoutSigningAndPost** en su cliente de Citrix Cloud. Esto hace que Citrix Cloud envíe las solicitudes de cierre de sesión único de SAML como solicitudes POST firmadas, en lugar de solicitudes de redireccionamiento sin firmar cuando los usuarios cierran sesión en Citrix Workspace o Citrix Cloud. El envío de solicitudes POST firmadas es obligatorio si el proveedor SAML requiere solicitudes firmadas para el cierre de sesión único y rechaza las redirecciones sin firmar.

Configuración de SAML en Citrix Cloud

Al configurar la conexión SAML en Citrix Cloud (como se describe en Agregar metadatos de proveedor SAML a Citrix Cloud), introduzca los valores de ADFS de la siguiente manera:

En este campo de Citrix Cloud	Introduzca este valor
ID de entidad	`https://adfs.YourDomain.com/adfs/services/trust`, donde `YourDomain.com` es el dominio del servidor ADFS.
Firmar solicitud de autenticación	Sí
URL del servicio SSO	`https://adfs.YourDomain.com/adfs/ls`, donde `YourDomain.com` es el dominio del servidor ADFS.
Mecanismo vinculante	HTTP Post
Respuesta SAML	Firmar respuesta o aserción
Contexto de autenticación	No especificado, exacto
URL de cierre de sesión	`https://adfs.YourDomain.com/adfs/ls`, donde `YourDomain.com` es el dominio del servidor ADFS.

Iniciar sesión en espacios de trabajo con SAML mediante dominios personalizados

November 27, 2023

Author:
Mark Dear

Si configuró un dominio personalizado en Citrix Workspace (por ejemplo, `https://workspaces.yourdomain.com`), es posible que necesite configuración adicional en Citrix Cloud y en su proveedor de SAML, según los casos de inicio de sesión de SAML que quiera permitir en Citrix Cloud.

Es posible que necesite un par de aplicaciones SAML para esta configuración. Citrix Cloud requiere dispositivos de punto final de proveedores de servicios (SP) de SAML diferentes, según si la aplicación SAML utiliza las URL de cloud.com o workspaces.sudominio.com para realizar la operación de inicio de sesión.

Para obtener más información sobre la configuración de dominios personalizados en Citrix Workspace, consulte Configurar un dominio personalizado en la documentación de producto de Citrix Workspace.

Consideraciones para implementar una o dos aplicaciones SAML

Para determinar si necesita implementar una solución con una o dos aplicaciones SAML, identifique qué combinación de casos de inicio de sesión SAML necesita permitir su proveedor de SAML.

Estos casos de inicio de sesión comparten la misma aplicación SAML (aplicación SAML 1) de forma predeterminada:

- Autenticación SAML para Citrix Workspace, en la que la URL de inicio de sesión de Workspace de su región (cloud.com, citrixcloud.jp, cloud.us) está configurada en su proveedor de SAML como ID de entidad del SP.
- Autenticación SAML para Citrix Cloud mediante su URL de inicio de sesión única (por ejemplo, `https://citrix.cloud.com/go/mycompany`). En este caso, los administradores se autentican en Citrix Cloud mediante SAML, según su pertenencia a grupos de Active Directory (AD).

Agregar la autenticación SAML para usuarios a través de un dominio personalizado (por ejemplo, `https://workspaces.mycompany.com`) que defina en Configuración de Workspace requiere una segunda aplicación SAML (aplicación SAML 2).

En esta tabla se enumeran las combinaciones permitidas de casos de inicio de sesión SAML y las aplicaciones SAML necesarias.

Iniciar sesión en Workspace con una URL de Workspace	Iniciar sesión en Workspace con la URL de un dominio personalizado	Iniciar sesión en Citrix Cloud mediante una URL de inicio de sesión SAML	¿Se necesita la aplicación SAML 1?	¿Se necesita la aplicación SAML 2?
Sí	No	No	Sí: usar dispositivos de punto final SAML de cloud.com	No
No	Sí	No	Sí: usar dispositivos de punto final SAML de dominios personalizados	No
No	No	Sí	Sí: usar dispositivos de punto final SAML de cloud.com	No
Sí	No	Sí	Sí: usar dispositivos de punto final SAML de cloud.com	No
No	No	Sí	Sí: usar los dispositivos de punto final SAML de cloud.com	Sí: usar dispositivos de punto final SAML de dominios personalizados
Sí	Sí	Sí	Sí: usar dispositivos de punto final SAML de cloud.com	Sí: usar dispositivos de punto final SAML de dominios personalizados

Configuración de una única aplicación SAML

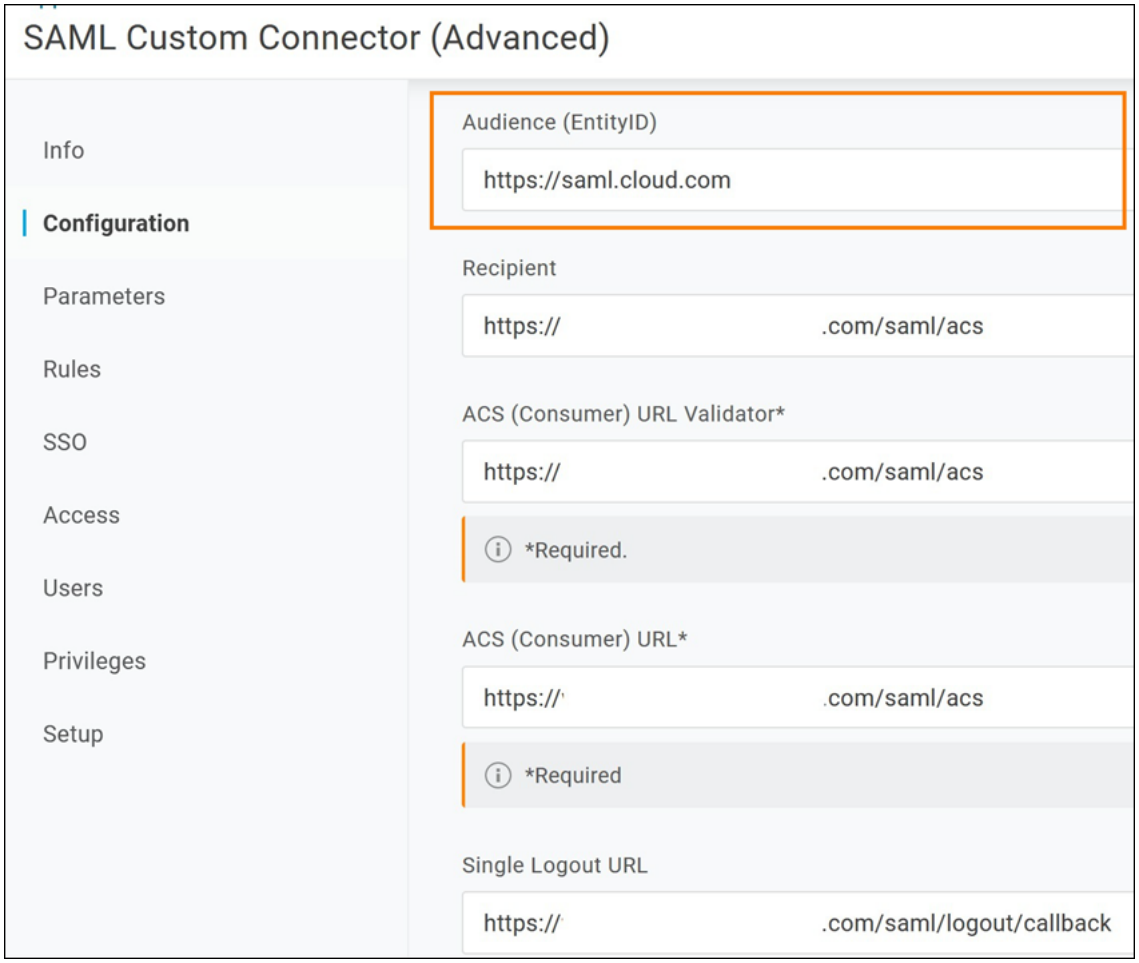
1. En Citrix Cloud, vaya a **Configuración de Workspace > Acceso** y configure un dominio personalizado. Para obtener más información, consulte Configurar un dominio personalizado.
2. En la consola de administración de su proveedor de SAML, configure una única aplicación SAML

mediante el dominio personalizado como dispositivos de punto final del SP.

3. Descargue el certificado de firma SAML para la aplicación SAML. En un paso posterior, cargue este certificado en Citrix Cloud.
4. Para el ID de entidad, asegúrese de que se haya introducido `https://saml.cloud.com`. En función del proveedor de SAML, es posible que este parámetro se denomine **Audience** (audiencia). Para todos los demás dispositivos de punto final, sustituya `https://saml.cloud.com` por el dominio personalizado de Workspace que configuró en el paso 1.

   Este ejemplo ilustra la configuración del dispositivo de punto final de Okta, donde **Audience Restriction** contiene el valor del ID de entidad:

   Este ejemplo ilustra la configuración del dispositivo de punto final de OneLogin, donde **Audience** contiene el valor del ID de entidad:



5. En Citrix Cloud, vaya a **Administración de acceso e identidad > Autenticación** y configure la conexión SAML.
6. Vaya a **Configuración de Workspace > Autenticación** y seleccione **SAML 2.0**.
7. Vaya a **Configuración de Workspace > URL de Workspace personalizada > Modificar** y seleccione **Usar solo el dominio personalizado**.
8. Seleccione **Guardar** para guardar los cambios.
9. Para probar la configuración, inicie sesión en Citrix Workspace con su URL de Workspace personalizada (`https://workspaces.mycompany.com`).

Configuración de dos aplicaciones SAML

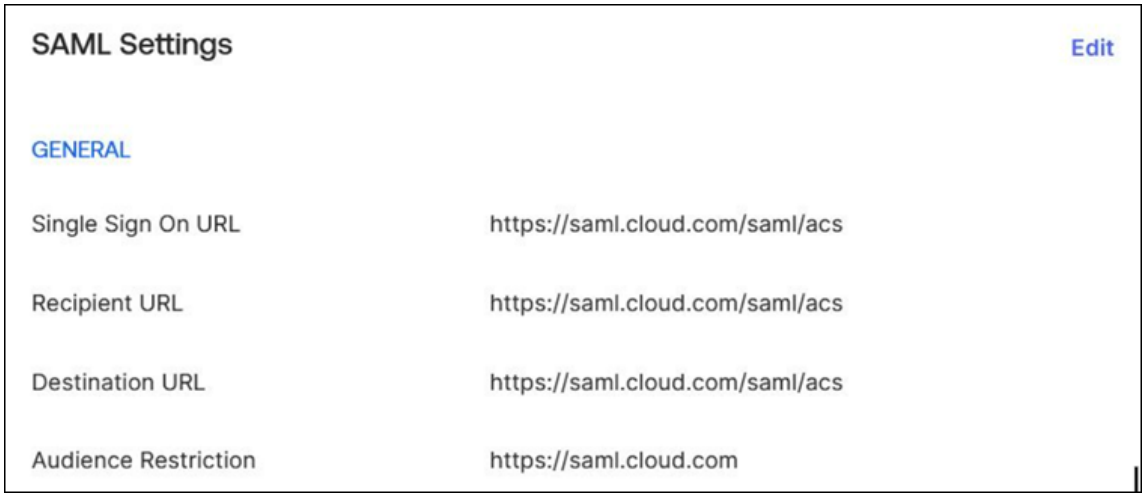
1. En Citrix Cloud, vaya a **Configuración de Workspace > Acceso** y configure un dominio personalizado. Para obtener más información, consulte Configurar un dominio personalizado.
2. En la consola de administración de su proveedor de SAML, configure dos aplicaciones SAML. Configure estas aplicaciones de forma idéntica, incluidos los parámetros de firma idéntica para

las solicitudes de SSO y SLO, el tipo de vínculo y los parámetros de cierre de sesión. Si las configuraciones de estas aplicaciones SAML no coinciden, es posible que note diferencias en el comportamiento de inicio y de cierre de sesión al cambiar entre la URL de Workspace y su dominio personalizado de Workspace.

3. En la primera aplicación SAML, configure estos dispositivos de punto final del SP:

   - ID de entidad: `https://saml.cloud.com`
   - Assertion Consumer Service: `https://saml.cloud.com/saml/acs`
   - Cierre de sesión: `https://saml.cloud.com/saml/logout/callback`

   Este ejemplo muestra esta configuración de dispositivos de punto final en la consola de administración de Okta:

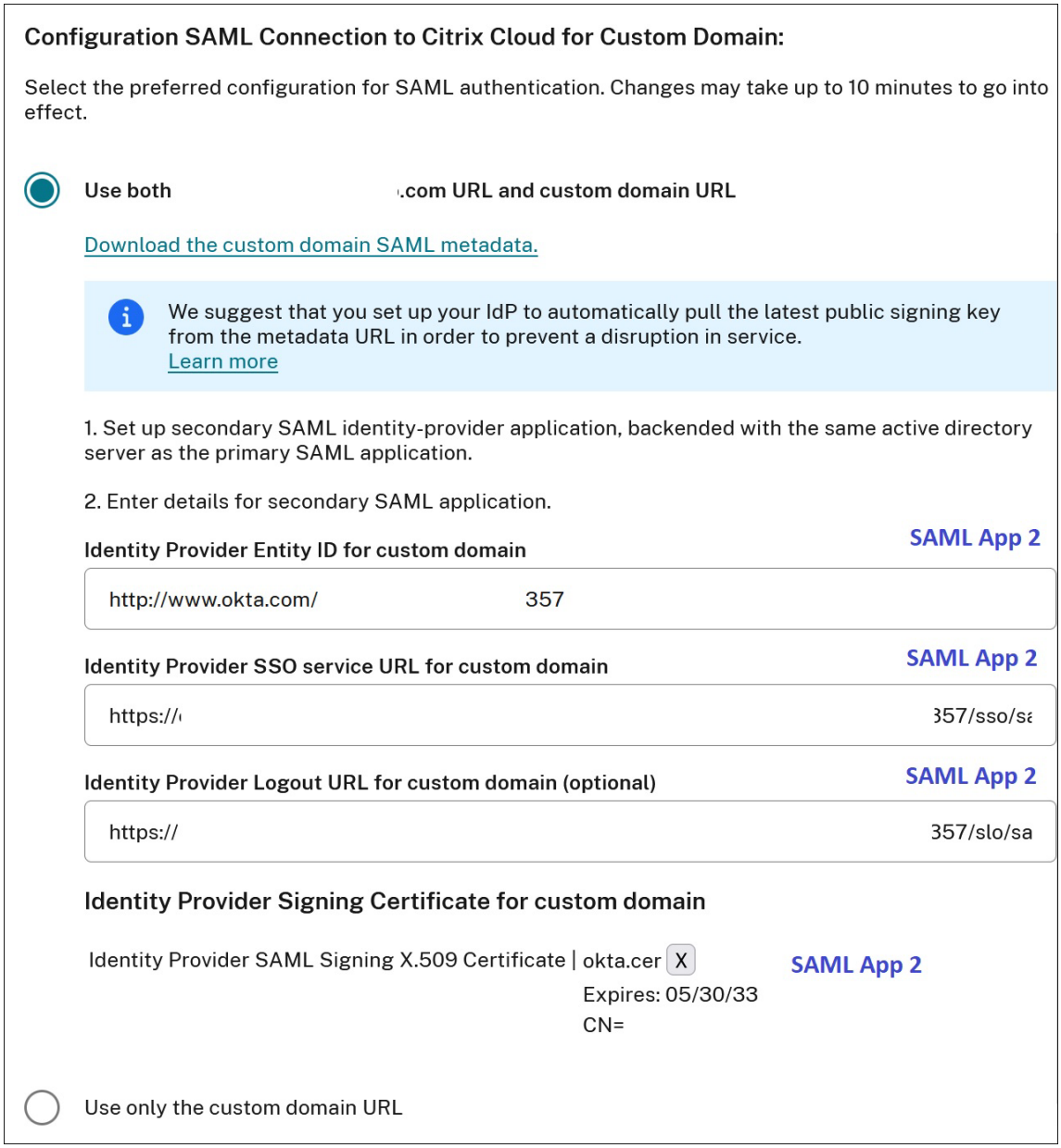
   

4. En la segunda aplicación SAML, configure estos dispositivos de punto final del SP. Use su dominio personalizado de Workspace solo para los dispositivos de punto final de Assertion Consumer Service y del cierre de sesión.

   - ID de entidad: `https://saml.cloud.com`
   - Assertion Consumer Service: `https://workspaces.mycompany.com/saml/acs`
   - Cierre de sesión: `https://workspaces.mycompany.com/saml/logout/callback`

   Este ejemplo muestra esta configuración de dispositivos de punto final en la consola de Okta. Tenga en cuenta que **Audience Restriction** contiene el valor del ID de entidad.

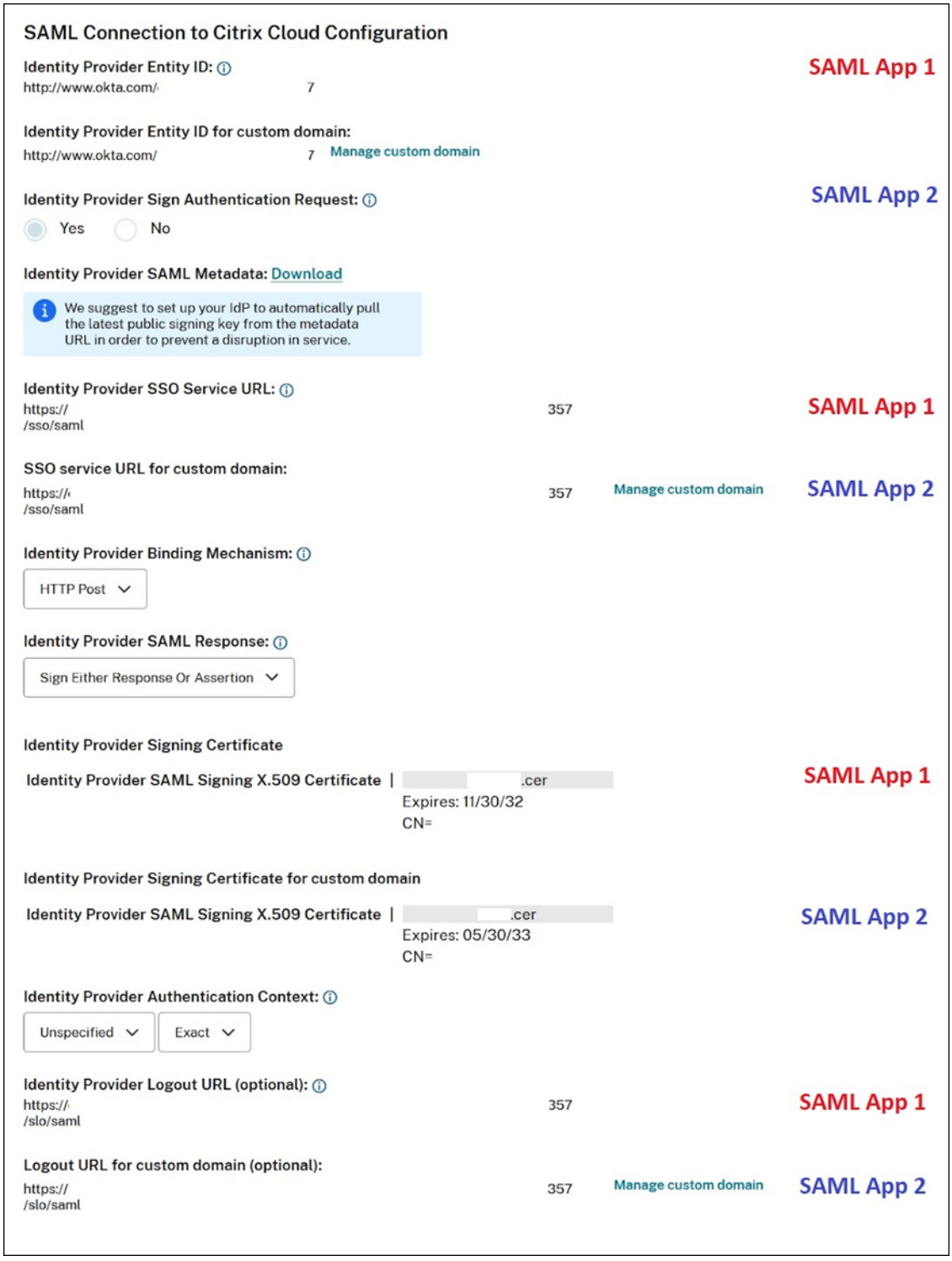
5. Descargue los certificados de firma SAML para ambas aplicaciones SAML. Los cargará en Citrix Cloud en un paso posterior.
6. En la consola de administración de Citrix Cloud, configure una conexión SAML:
    a) Desde la consola de administración de Citrix Cloud, haga clic en el botón de menú y seleccione **Administración de acceso e identidad**.
    b) En la ficha **Autenticación**, busque **SAML 2.0**, haga clic en el botón de tres puntos y seleccione **Conectar**.
    c) En la página **Configurar SAML**, introduzca los detalles de la primera aplicación SAML que creó en el paso 2.
7. Configure Citrix Workspace para usar la nueva conexión SAML:
    a) En el menú de Citrix Cloud, seleccione **Configuración de Workspace**.
    b) En la ficha **Autenticación**, seleccione **SAML 2.0**.
8. En la ficha **Acceso**, en **URL de Workspace**, seleccione **Modificar**.
9. En la página **Configurar para SAML**, seleccione **Usar la URL de cliente.cloud.com y la URL de dominio personalizado**.
10. Introduzca la siguiente información:
    - En **ID de entidad del proveedor de identidades del dominio personalizado**, introduzca el ID de entidad de la segunda aplicación SAML que creó en el paso 2.
    - En **URL del servicio SSO para el dominio personalizado**, introduzca la URL de SSO de la segunda aplicación SAML.
    - En **URL de cierre de sesión para el dominio personalizado**, introduzca la URL de SLO de la segunda aplicación SAML.
    - En **Certificado de firma del proveedor de identidades para dominio personalizado**, cargue el certificado de firma SAML desde la segunda aplicación SAML.



11. Seleccione **Guardar** para guardar los cambios.

Ver los detalles de la conexión SAML

Tras la configuración, vaya a **Administración de acceso e identidad > Autenticación**. En **SAML 2.0**, seleccione **Seleccionar proveedor de SAML > Ver** en el menú de tres puntos. La página Configuración de SAML muestra pares de dispositivos de punto final de SAML configurados para el ID de entidad, la URL de SSO y la URL de cierre de sesión.



Todos los demás parámetros de configuración de SAML se aplican tanto a la primera como a la segunda aplicación SAML que haya creado.

Verificar los inicios de sesión en Citrix Workspace

Para verificar el comportamiento de inicio y de cierre de sesión configurado, haga estas pruebas:

- Inicie sesión en Citrix Workspace con su URL de Workspace (`https://mycompany.cloud.com`) y su proveedor de SAML.
- Inicie sesión en Citrix Workspace con su dominio personalizado de Workspace (`https://workspace.mycompany.com`) y su proveedor de SAML.
- Inicie sesión en Citrix Cloud con su URL de inicio de sesión única (`https://citrix.cloud.com/go/mycompany`) y su proveedor de SAML.

Configurar Okta como proveedor SAML para la autenticación de espacios de trabajo

March 12, 2024

Author:
Mark Dear

En este artículo se describen los pasos necesarios para configurar una aplicación SAML de Okta y una conexión entre Citrix Cloud y su proveedor SAML. En algunos de estos pasos, se describen las acciones que debe realizar en la consola de administración del proveedor SAML.

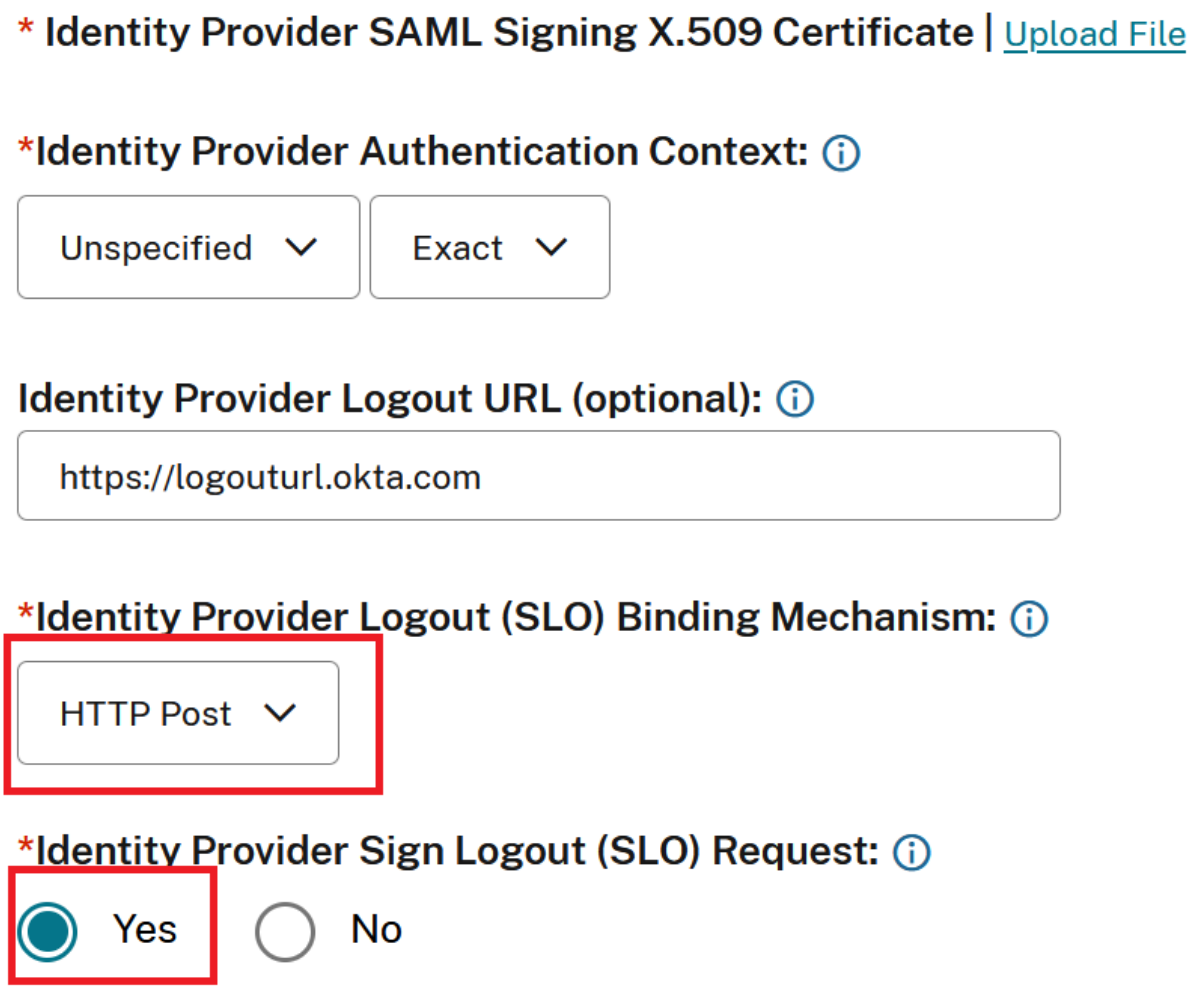
Requisitos previos

Antes de completar las tareas de este artículo, asegúrese de cumplir estos requisitos previos:

- Citrix Support ha habilitado la función **SendNameIDPolicyInSAMLRequest** en Citrix Cloud. Esta función se habilita por solicitud. Para obtener más información sobre estas funciones, consulte Funciones de la nube requeridas para SAML con Okta.
- Tiene una organización de Okta que usa uno de estos dominios de Okta:
  - okta.com
  - okta-eu.com
  - oktapreview.com
- Sincronizó su Active Directory (AD) con su organización de Okta.
- Las **solicitudes de autenticación de firmas** están habilitadas en su organización de Okta.
- **Cierre de sesión único o Single Logout (SLO) para proveedor de identidades** está configurado tanto en las aplicaciones SAML de Okta como en Citrix Cloud. Al configurar SLO y el

usuario final cierra sesión en Citrix Workspace, también cierra sesión en Okta y en todos los demás proveedores de servicios que comparten la aplicación SAML de Okta.

- **Solicitudes de cierre de sesión (SLO) de proveedores de identidad** está habilitado en Citrix Cloud.
- **Cierre de sesión vinculante (SLO) para proveedor de identidades** es HTTPPost en Citrix Cloud.



Funciones de la nube requeridas para SAML con Okta

Antes de completar las tareas de este artículo, debe contactar con Citrix Support para habilitar la función **SendNameIDPolicyInSAMLRequest**. Esta función permite a Citrix Cloud proporcionar la directiva **NameID** como **Unspecified** en la solicitud SAML a su proveedor SAML. Esta función solo está habilitada para usarse con Okta.

Para solicitar estas funciones, inicie sesión en su cuenta de Citrix y abra un tíquet a través del sitio web de Citrix Support.

Requisitos

Este artículo incluye una tarea en la que crear una aplicación SAML en la consola de administración de Okta. Esta aplicación requiere un certificado de firma SAML para su región de Citrix Cloud.

> **Importante:**
>
> El certificado de firma debe estar codificado en formato PEM. Citrix Cloud no acepta la firma de certificados en otros formatos de codificación.

Puede extraer este certificado de los metadatos SAML de Citrix Cloud de su región mediante una herramienta de extracción como la que se encuentra en https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract. Citrix recomienda adquirir previamente el certificado SAML de Citrix Cloud para poder proporcionarlo cuando sea necesario.

En los pasos de esta sección, se describe cómo obtener el certificado de firma mediante la herramienta de extracción de https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract.

Para adquirir los metadatos de Citrix Cloud para su región:

1. En la herramienta de extracción que prefiera, introduzca la URL de metadatos de su región de Citrix Cloud:
   - Para las regiones de la Unión Europea, Estados Unidos y Asia-Pacífico Sur, introduzca `https://saml.cloud.com/saml/metadata`.
   - Para la región de Japón, introduzca `https://saml.citrixcloud.jp/saml/metadata`.
   - Para la región de Citrix Cloud Government, introduzca `https://saml.cloud.us/saml/metadata`.
2. Haga clic en **Load**. El certificado extraído aparece debajo de la URL introducida.
3. Haga clic en **Download** para descargar el certificado en formato PEM.

Sincronizar cuentas con el agente de AD de Okta

Para usar Okta como proveedor SAML, primero debe integrar su AD local con Okta. Para ello, instale el agente de AD para Okta en su dominio y agregue su AD a su organización de Okta. Para obtener instrucciones sobre la implementación del agente de AD para Okta, consulte Get started with Active Directory integration en el sitio web de Okta.

Después, importe los usuarios y grupos de AD a Okta. Al importar, incluya estos valores asociados a sus cuentas de AD:

- Correo electrónico

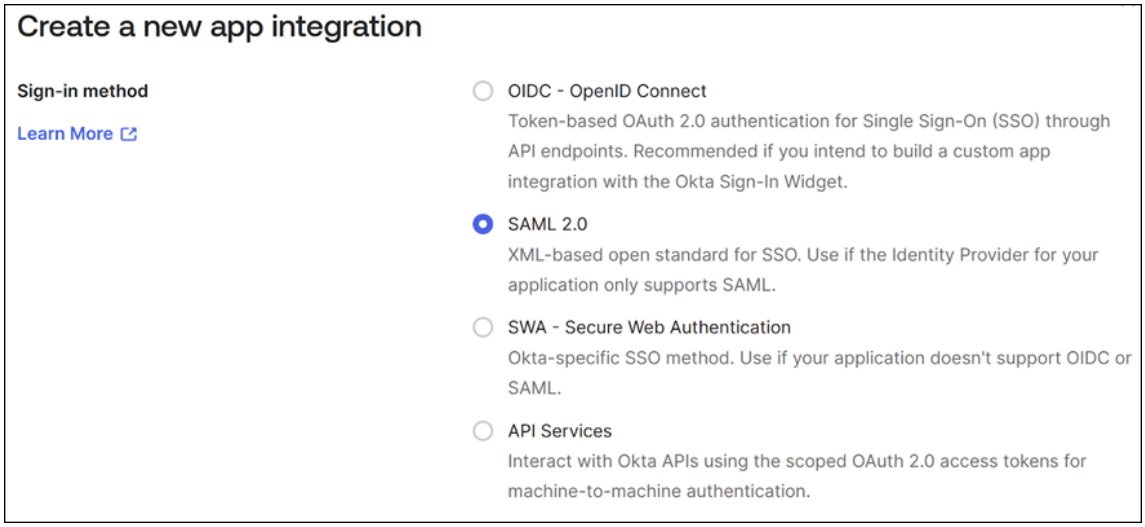
- SID
- UPN
- OID

Para sincronizar los usuarios y grupos de AD con la organización de Okta:

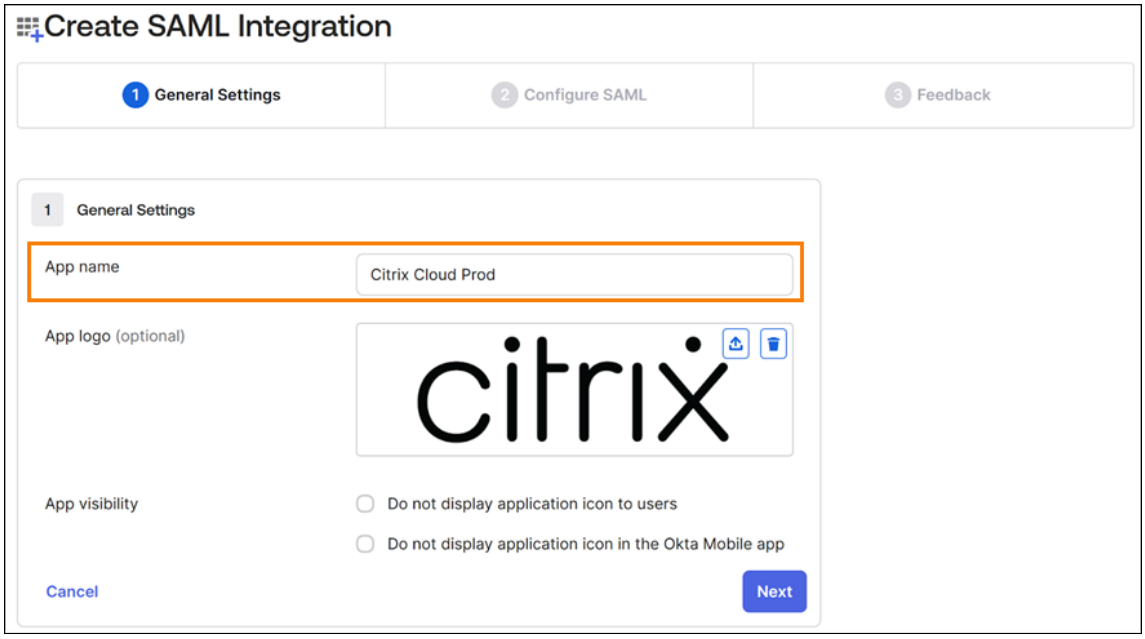
1. Instale y configure el agente de AD para Okta. Para obtener instrucciones completas, consulte los siguientes artículos en el sitio web de Okta:
   - Instalar el agente de Active Directory para Okta
   - Configurar la importación y los parámetros de la cuenta de Active Directory
   - Configurar las opciones de aprovisionamiento de Active Directory
2. Agregue sus usuarios y grupos de AD a Okta realizando una importación manual o una importación automatizada. Para obtener más información sobre los métodos e instrucciones de importación de Okta, consulte Manage Active Directory users and groups en el sitio web de Okta.

Configurar una aplicación SAML de Okta para la autenticación de espacios de trabajo

1. Inicie sesión en su organización de Okta con una cuenta de administrador con permisos para agregar y configurar aplicaciones SAML.
2. En la consola de administración, seleccione **Applications > Applications > Create App Integration** y, a continuación, seleccione **SAML 2.0**. Seleccione **Siguiente**.



3. En **App Name**, introduzca un nombre descriptivo de la aplicación. Seleccione **Siguiente**.



4. En la sección **SAML Settings**, configure la conexión del proveedor de servicios (SP) de Citrix Cloud:

   a) En **Single sign-on URL**, introduzca la URL que corresponde a la región de Citrix Cloud de su cliente de Citrix Cloud:

      - Si su ID de cliente se encuentra en las regiones de la Unión Europea, Estados Unidos o Asia-Pacífico Sur, introduzca `https://saml.cloud.com/saml/acs`.
      - Si su ID de cliente se encuentra en la región de Japón, introduzca `https://saml.citrixcloud.jp/saml/acs`.
      - Si su ID de cliente se encuentra en la región de Citrix Cloud Government, introduzca `https://saml.cloud.us/saml/acs`.

   b) Seleccione **Use this for Recipient and Destination URL**.

   c) En **Audience URI (SP Entity ID)**, introduzca la URL que corresponde a la región de Citrix Cloud de su cliente de Citrix Cloud:

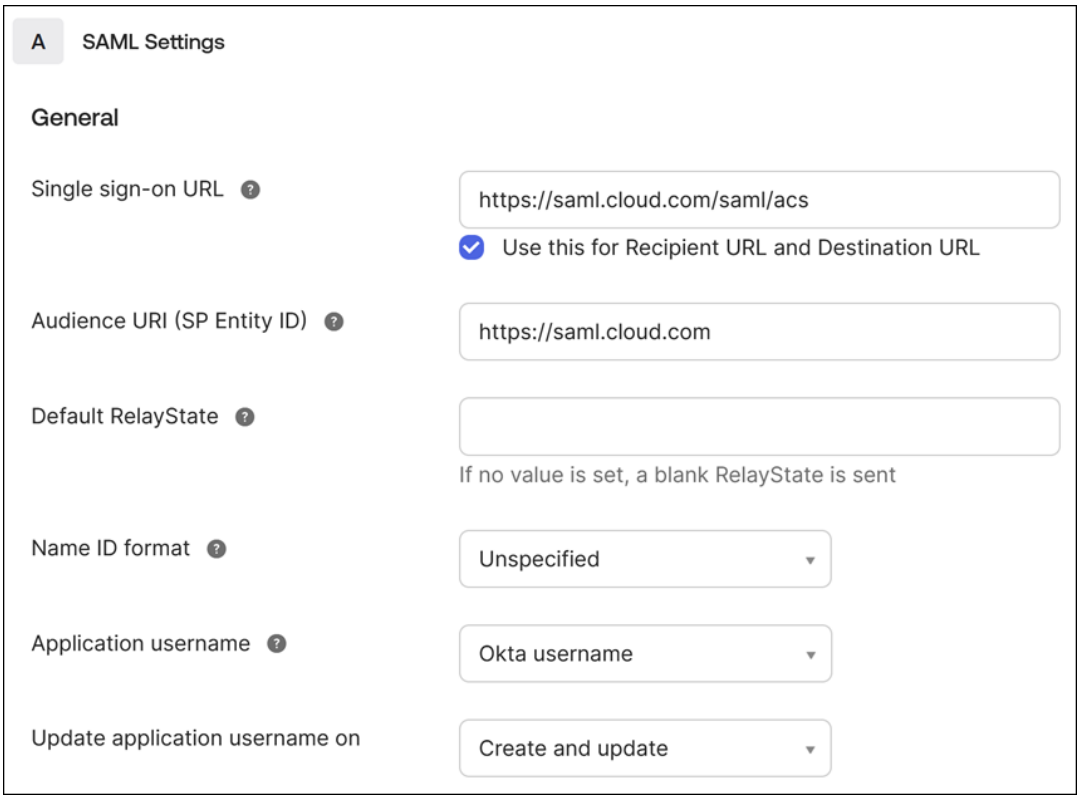
      - Si su ID de cliente se encuentra en las regiones de la Unión Europea, Estados Unidos o Asia-Pacífico Sur, introduzca `https://saml.cloud.com`.
      - Si su ID de cliente se encuentra en la región de Japón, introduzca `https://saml.citrixcloud.jp`.
      - Si su ID de cliente se encuentra en la región de Citrix Cloud Government, introduzca `https://saml.cloud.us`.

   d) En **Name ID Format**, seleccione **Unspecified**. La directiva de NameID que Citrix Cloud envía en la solicitud SAML debe coincidir con el formato de NameID especificado en la aplicación SAML de Okta. Si estos elementos no coinciden, al habilitar **Sign Authentication**

Request, se producirá un error en Okta.

e) En **Application username**, seleccione **Okta username**.

Como ejemplo de esta configuración, esta imagen ilustra la configuración correcta para las regiones de EE. UU., la UE y Asia-Pacífico Sur:



> **Importante:**
>
> La configuración de **Name ID** debe configurarse como **Unspecified**. Si se usa un valor diferente para este parámetro, se produce un error en el inicio de sesión de SAML.

f) Haga clic en **Show Advanced Settings** y configure estos parámetros:

- En **Response**, seleccione **Signed**.
- En **Assertion Signature**, seleccione **Signed**.
- En **Signature Algorithm**, seleccione **RSA-SHA256**.
- En **Assertion Encryption**, seleccione **Unencrypted**.

g) En **Signature Certificate**, cargue el certificado de firma SAML para su región de Citrix Cloud en formato PEM. Para obtener instrucciones sobre cómo adquirir el certificado de firma SAML, consulte Requisitos en este artículo.

h) En **Enable Single Logout**, seleccione **Allow application to initiate Single Logout**.

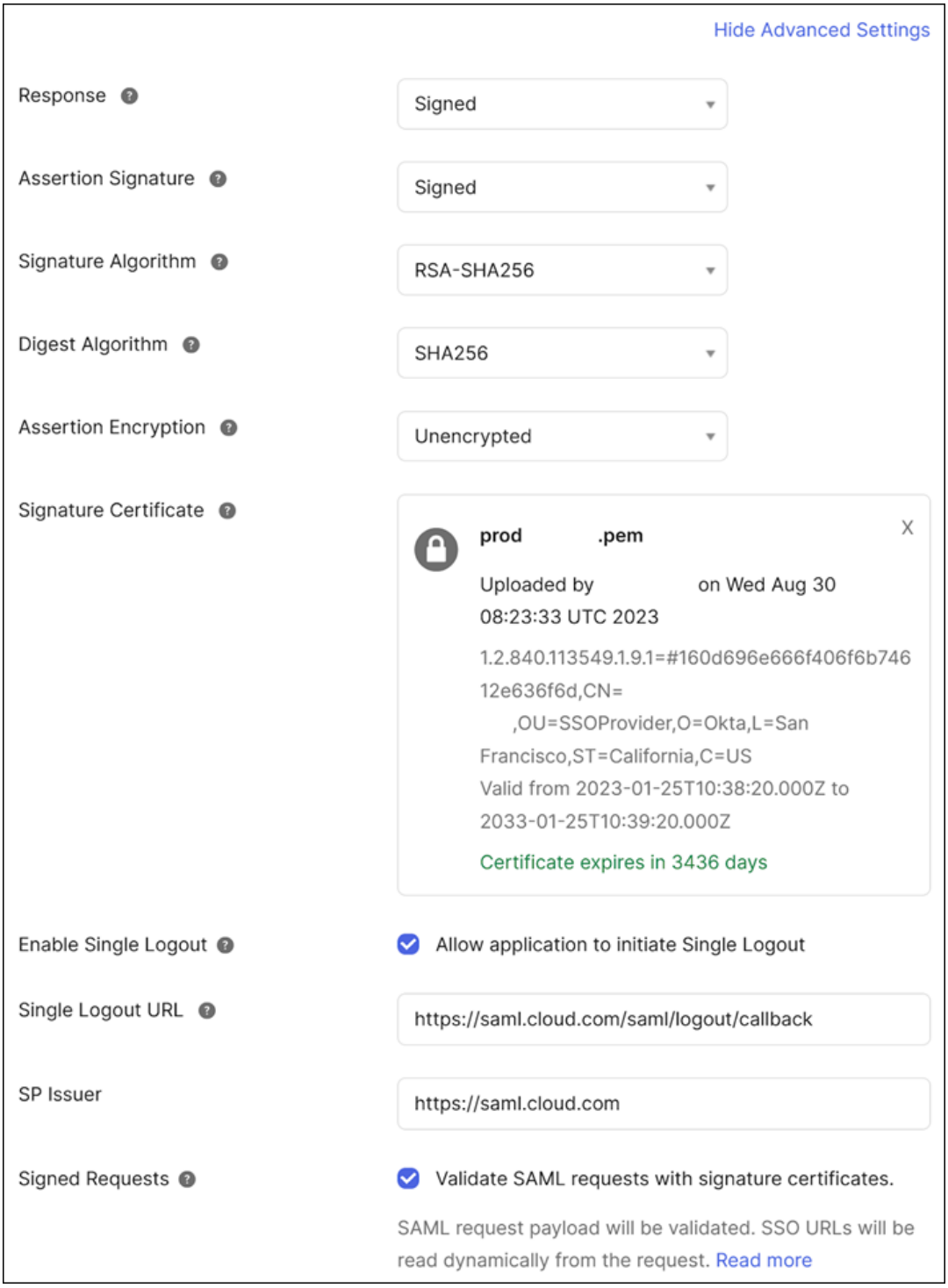
i) En **Single Logout URL**, introduzca la URL que corresponde a su región de Citrix Cloud:

- Para las regiones de la Unión Europea, Estados Unidos y Asia-Pacífico Sur, introduzca `https://saml.cloud.com/saml/logout/callback`.
- Para la región de Japón, introduzca `https://saml.citrixcloud.jp/saml/saml/logout/callback`.
- Para Citrix Cloud Government, introduzca `https://saml.cloud.us/saml/logout/callback`.

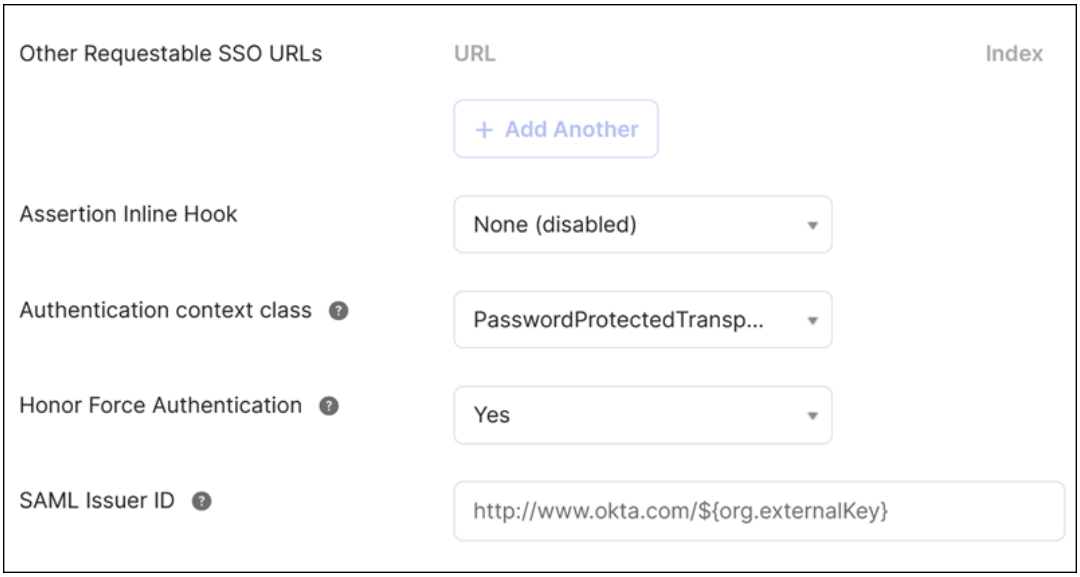
j) En **SP Issuer**, introduzca el valor que introdujo antes en **Audience URI (SP Entity ID)** (paso 4c de esta tarea).

k) En **Signed Requests**, seleccione **Validate SAML requests with signature certificates**.

Esta imagen ilustra la configuración correcta para las regiones de EE. UU., la UE y Asia-Pacífico Sur:

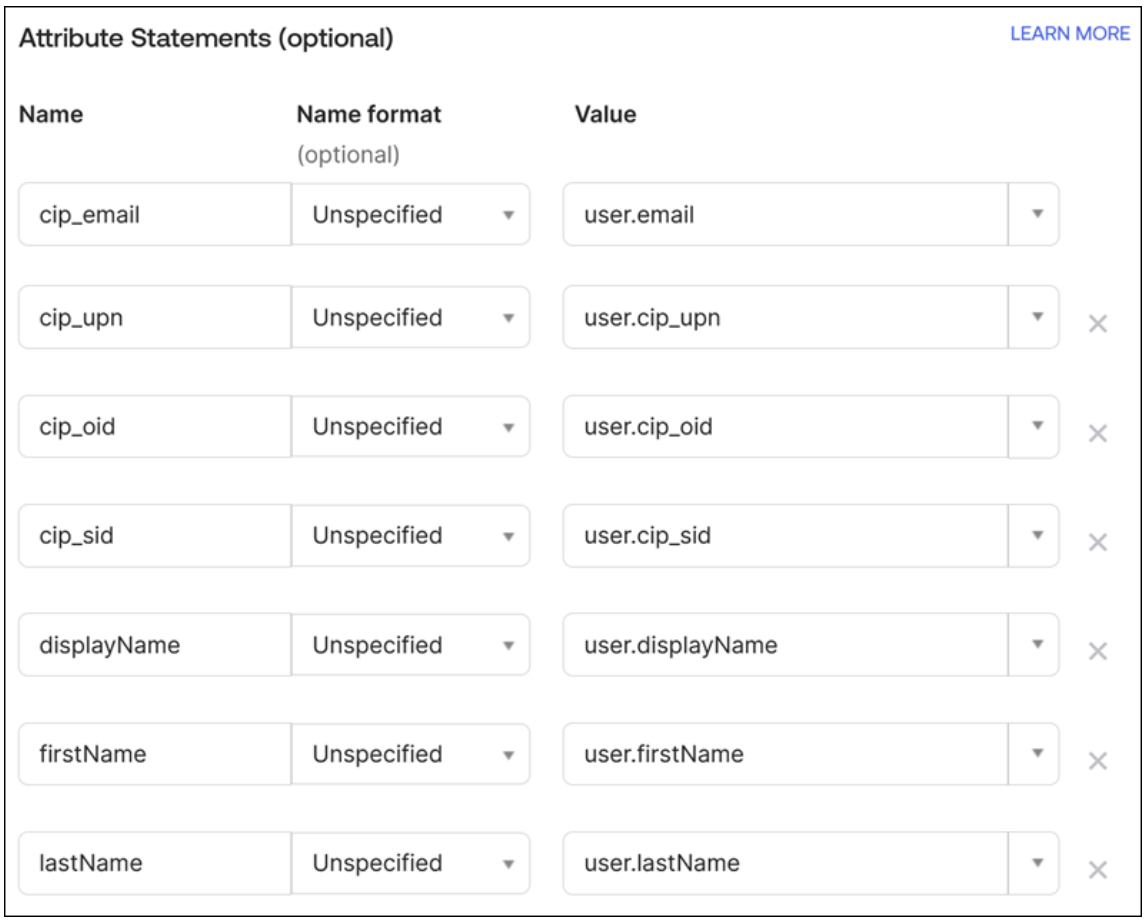


l) Para el resto de parámetros avanzados, acepte los valores predeterminados.

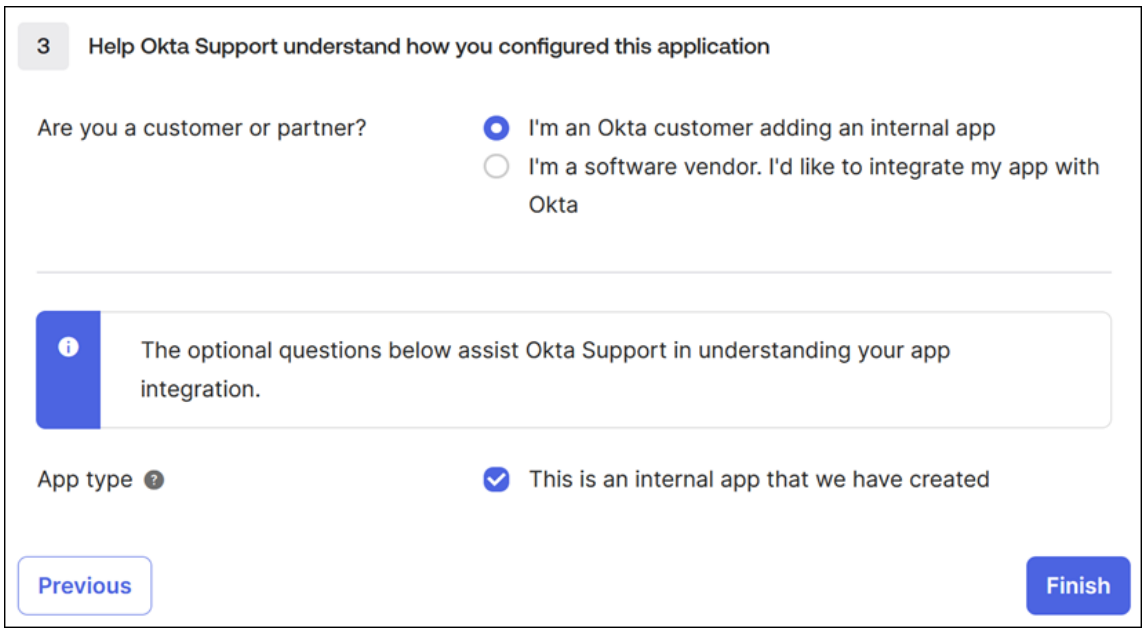


5. En **Attribute Statements (optional)**, introduzca valores para **Name**, **Name format** y **Value** tal y como se muestra en esta tabla:

Nombre	Formato del nombre	Valor
cip_email	Sin especificar	user.email
cip_upn	Sin especificar	user.cip_upn
cip_oid	Sin especificar	user.cip_oid
cip_sid	Sin especificar	user.cip_sid
displayName	Sin especificar	user.displayName
firstName	Sin especificar	user.firstName
lastName	Sin especificar	user.lastName



6. Seleccione **Siguiente**. Aparece la declaración de configuración de Okta.



7. En **Are you a customer or partner?**, seleccione **I'm an Okta customer adding an internal app**.

8. En **App type**, seleccione **This is an internal app that we have created**.
9. Seleccione **Finish** para guardar la configuración. Aparece la página de perfil de la aplicación SAML y muestra el contenido de la ficha **Sign On**.

Tras la configuración, seleccione la ficha **Assignments** y asigne usuarios y grupos a la aplicación SAML.

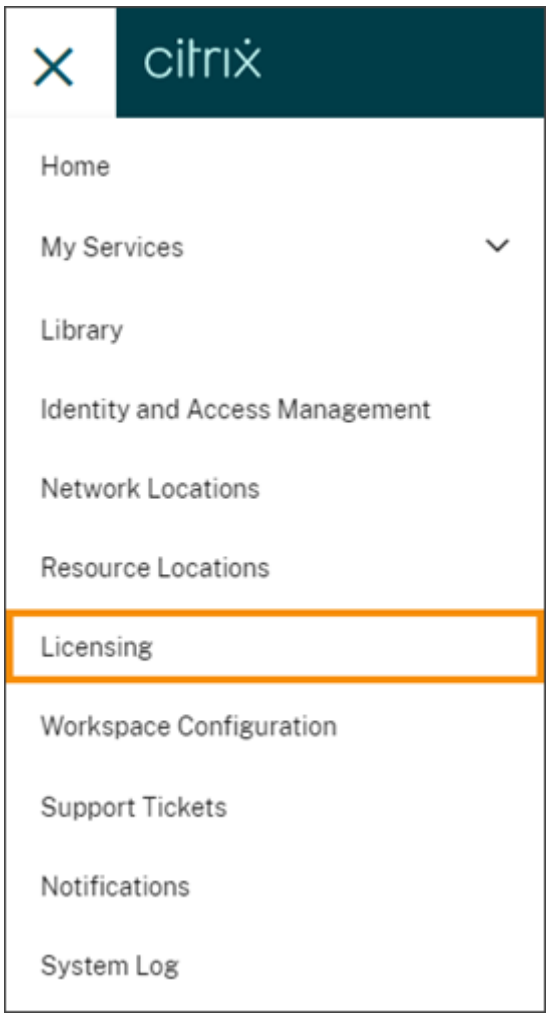
Licencias para Citrix Cloud

October 2, 2023

Citrix Cloud ofrece supervisión del uso y de las licencias para ciertos servicios de la nube. Además, la supervisión del uso y de las licencias está disponible para implementaciones locales donde Citrix License Server esté registrado con Citrix Cloud.

Licencias para clientes de empresa

Los clientes de empresa pueden supervisar las asignaciones y el uso de licencias de los servicios de la nube admitidos al seleccionar **Licencias** en el menú de Citrix Cloud.



Para obtener más información sobre la supervisión del uso y de las licencias de empresa para servicios de la nube, consulte Supervisar el uso activo y de licencias en los servicios de la nube.

Licencias para implementaciones locales

Los clientes de empresa con una implementación local de Citrix Virtual Apps and Desktops pueden usar Citrix Cloud para mantenerse al día de las licencias y del uso de los modelos de licencias simultáneas y de usuario/dispositivo. Al registrar Citrix License Server con Citrix Cloud, los clientes pueden utilizar la página **Implementaciones con licencia** de Citrix Cloud para las siguientes tareas:

- Supervisar el estado de informes de servidores de licencias registrados
- Ver asignaciones de licencias y tendencias de uso de implementaciones que utilizan el modelo de licencias de usuario/dispositivo.
- Ver tendencias de picos de uso máximo de licencias para implementaciones que utilizan el modelo de licencias simultáneas.

Para obtener más información sobre la supervisión de licencias y uso de implementaciones locales de Virtual Apps and Desktops, consulte Supervisar las licencias y el uso de las implementaciones locales.

Licencias para Citrix Service Providers (CSP)

Los Citrix Service Providers pueden usar estas herramientas para comprender y generar informes sobre las licencias y el uso de los productos:

- License Usage Insights es un servicio gratuito de Citrix Cloud que recopila y agrega información de uso de los productos en clientes arrendatarios únicos y multiarrendatario. Para obtener más información, consulte Licencias para Citrix Service Providers.
- La función de licencias de Citrix Cloud permite a los clientes de CSP supervisar sus licencias y el uso de los productos de Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service) admitidos. Los CSP pueden iniciar sesión en la cuenta de Citrix Cloud de su cliente para ver y exportar esta información. Para obtener más información, consulte estos artículos:
  - Supervisión del uso y las licencias de los clientes para Citrix DaaS
  - Supervisión del uso y las licencias de los clientes para Citrix DaaS Standard para Azure

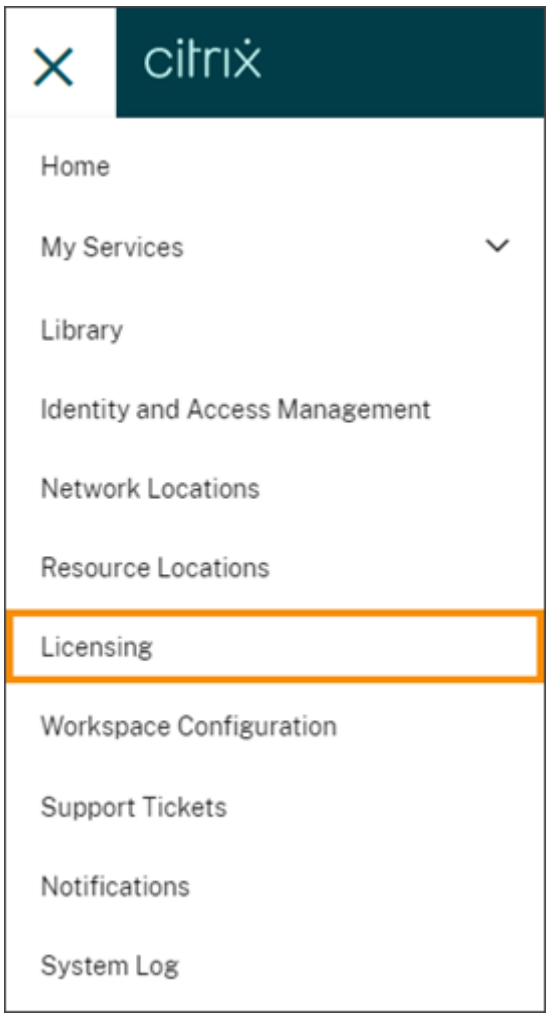
Supervisar el uso activo y de licencias en los servicios de la nube

October 2, 2023

Las licencias de Citrix Cloud le permiten mantenerse al tanto del consumo de licencias para los servicios de la nube adquiridos. Con los informes de resumen y de detalles, puede:

- Ver la disponibilidad de las licencias y las asignaciones
- Ver tendencias diarias y mensuales del uso activo de los servicios de la nube relevantes
- Ver en detalle la asignación de cada licencia individual y las tendencias de uso
- Exportar datos de uso de licencias a CSV

Para ver los datos de licencias de sus servicios de la nube, seleccione **Licencias** en el menú de la consola.



Nota:

En este artículo, se describen las funciones del menú Licencias que ofrecen todos los servicios de Citrix Cloud disponibles. Algunos aspectos del menú Licencias pueden ser diferentes, ya que dependen del servicio (por ejemplo, la asignación de licencias). Para obtener más información acerca de las licencias y el uso de cada servicio, consulte los siguientes artículos:

- Supervisar las licencias y el uso activo de Citrix DaaS (usuario/dispositivo)
- Supervisar las licencias y el pico de uso de Citrix DaaS y Citrix DaaS Standard para Azure (licencias simultáneas)
- Supervisar el uso activo y de licencias de Citrix DaaS Standard para Azure (usuario/dispositivo solo)
- Supervisar las licencias y el uso activo de Endpoint Management Service
- Supervisar el uso de ancho de banda de Gateway Service
- Supervisar licencias y el uso de Secure Private Access

Regiones y servicios de la nube disponibles

Licencias solo está disponible para los servicios compatibles en las regiones de EE. UU., la UE y Asia-Pacífico Sur.

Licencias está disponible para los siguientes servicios de la nube:

- Citrix DaaS (modelos de licencias de usuario/dispositivo y simultáneas): Antes denominado Citrix Virtual Apps and Desktops Service
- Citrix DaaS Standard para Azure (modelo de licencias de usuario/dispositivo): Antes denominado Citrix Virtual Apps and Desktops Standard para Azure
- Endpoint Management
- Gateway
- Secure Private Access (antes denominado Secure Workspace Access)

Licencias de varios tipos para Citrix DaaS

Las licencias en Citrix Cloud admiten licencias de varios tipos para Citrix DaaS. Si se introducen los modelos de licencia Usuario/dispositivo y Simultáneas en una misma cuenta de Citrix Cloud, Citrix Cloud muestra el uso de licencias de cada modo en la página Licencias de la consola.

Citrix recomienda configurar licencias de varios tipos en los niveles de sitio y grupo de entrega antes de revisar la página Licencias. De lo contrario, es posible que no aparezca la información correcta. Para obtener instrucciones, consulte Licencias de varios tipos en la documentación de Citrix DaaS.

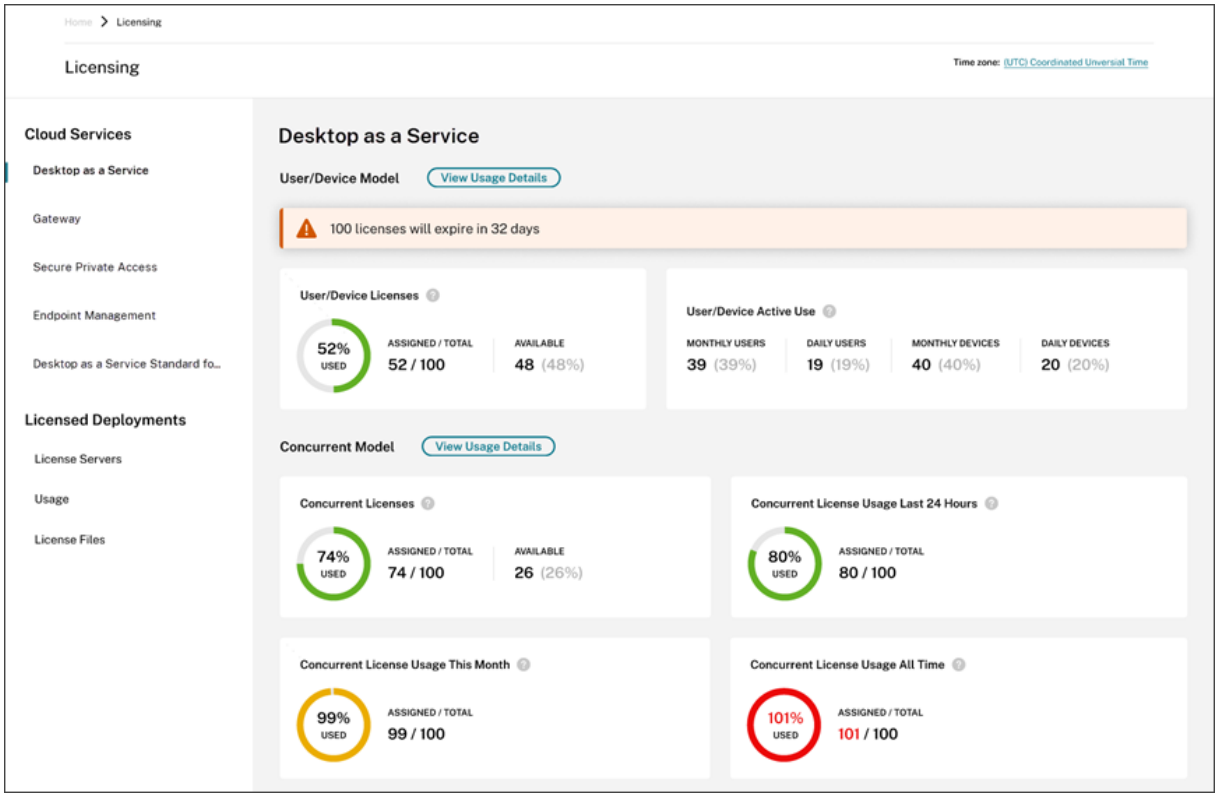
Si la página de la consola Licencias no muestra el uso correcto de licencias de varios tipos después de usar correctamente los métodos de configuración de Web Studio o PowerShell, tiene las siguientes opciones:

- Esperar 30 días y liberar las licencias que no utilice.
- Ponerse en contacto con el Servicio de atención al cliente de Citrix.

Asignación de licencias

En general, a los usuarios se les asigna una licencia al usar por primera vez un servicio de la nube. Algunos servicios pueden asignar licencias de manera diferente, según el modelo de licencias que utilicen. Para obtener más información sobre cómo se asignan las licencias a cada servicio, consulte los artículos de Licencias a los que se hace referencia en la parte superior de este artículo.

Resumen y detalles de la función Licencias



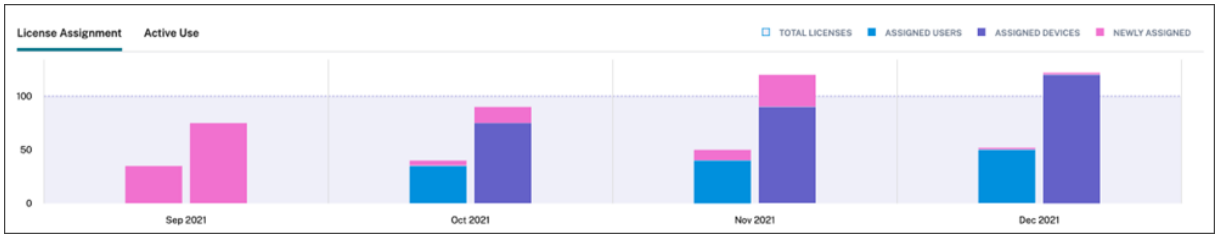
El resumen de Licencias ofrece una vista general de la siguiente información para cada servicio disponible:

- Porcentaje de licencias asignadas respecto al total de licencias adquiridas. El color del porcentaje cambia de verde a amarillo a medida que se aproxima al 100%. El color del porcentaje se vuelve rojo si se excede el 100%.
- La relación entre las licencias asignadas y las licencias adquiridas, y la cantidad restante de licencias disponibles.
- El tiempo que queda para que caduque la suscripción al servicio de la nube. Si la suscripción caduca en los próximos 90 días, aparece un mensaje de advertencia.

En el caso de algunos servicios, este resumen puede incluir información adicional, como el uso activo. Para obtener más información acerca de detalles específicos del servicio, consulte los artículos de Licencias a los que se hace referencia en la parte superior de este artículo.

Tendencias de uso y actividad de licencias

Para obtener una vista detallada de sus licencias de servicios de la nube, haga clic en **Ver detalles de uso**. Así, verá un desglose de las tendencias de uso y los usuarios que utilizan las licencias de los servicios de la nube.



La información que contiene este desglose puede variar, ya que depende del servicio de la nube. Para obtener más información sobre las tendencias de uso y la actividad de licencias específicas de cada servicio, consulte los artículos de Licencias a los que se hace referencia en la parte superior de este artículo.

Liberar licencias asignadas

En general, una licencia asignada es candidata para liberarse cuando el usuario no ha utilizado un servicio de la nube durante 30 días consecutivos. Cuando se libera una licencia, la cantidad de licencias restantes aumenta y el número de licencias asignadas disminuye en consecuencia.

En el caso de algunos servicios, la liberación de licencias puede ser diferente, ya que depende del modelo de licencias utilizado. Para obtener más información acerca de la liberación de licencias en un servicio específico, consulte los artículos de Licencias a los que se hace referencia en la parte superior de este artículo.

Preguntas frecuentes

- **¿Citrix impide el uso de servicios de la nube si la cantidad de licencias asignadas excede la cantidad de licencias adquiridas?** No, Citrix no impide el inicio de ningún servicio si usted usa un exceso de licencias de Cloud. La función Uso de licencias le da la información necesaria para comprender cómo se están usando las licencias. Citrix espera que usted supervise sus asignaciones de licencias y se mantenga dentro del límite de la cantidad de licencias adquiridas. Si, en algún momento, usted cree que va a exceder la cantidad de licencias que tiene para el servicio, Citrix recomienda que contacte con su representante de ventas para hablar de sus requisitos de licencias.
- **¿Qué información de licencias se recopila?** Actualmente, solo se recopila la información de licencia asociada con los nombres de inicio de sesión de los usuarios.
- **¿Se admiten licencias de varios tipos con Citrix DaaS (por ejemplo, mediante modelos de usuario/dispositivo y usuarios simultáneos)?** Sí. Consulte Licencias de varios tipos en este artículo para obtener más información.
- **¿Se admiten las licencias de varias ediciones para Citrix DaaS? Por ejemplo, ¿puedo usar las ediciones Premium y Advanced en la misma cuenta de Citrix Cloud?** No, este uso no es

posible. Un sitio de Citrix DaaS solo puede tener licencia de una edición. Si quiere usar varias instancias de Citrix DaaS en la misma cuenta de Citrix Cloud, deben tener la misma edición.

- **¿Cuál es la diferencia entre la información de los informes de Supervisar (en Director) y las licencias simultáneas?** El informe de Supervisar y la explicación de las sesiones simultáneas proporcionan una interpretación y unas métricas diferentes a las de una medida de las licencias simultáneas en uso. En la mayoría de los casos, el uso del número de sesiones simultáneas dentro de Director como representación o previsión de licencias simultáneas máximas en uso exagera considerablemente el número de licencias simultáneas necesarias. No utilice el informe de Supervisar en Director como sustituto de un informe sobre el uso simultáneo de licencias. Las dos principales diferencias entre las herramientas de presentación de informes son:
  - **Duración del tiempo de muestreo:** La licencia tiene un período de muestreo de cinco minutos. Cada cinco minutos, Citrix Cloud cuenta los dispositivos únicos actualmente conectados al servicio. Todos los períodos de muestreo de cinco minutos se agregan para determinar el pico de uso en un período de 24 horas, mensual y de la duración del contrato. El informe de Supervisar en Director puede mostrar intervalos de hasta dos horas en función de cómo se genere el informe.
  - **Singularidad:** las licencias buscan la singularidad entre los dispositivos cuando se inician las sesiones. El informe de Supervisar no tiene en cuenta los dispositivos únicos.

- **Después de migrar usuarios a una nueva instancia de un servicio en la nube (por ejemplo, cambié el nombre del dominio de mi organización), ¿por qué se cuentan dos veces mis licencias para los mismos usuarios?-* Citrix Cloud utiliza el nombre principal de usuario (UPN) para contar los usuarios únicos. Si un usuario accede al servicio de la nube antes y después de la migración, Citrix Cloud captura dos UPN únicos para el usuario, cada uno con un nombre de dominio diferente. Por lo tanto, Citrix Cloud cuenta el mismo usuario dos veces. Puede liberar la asignación de la antigua licencia 30 días después, siempre que el usuario no acceda al servicio con el nombre de dominio antiguo. Citrix no impide el inicio de ningún servicio si usted usa un exceso de licencias de Cloud.
- **¿Por qué veo licencias duplicadas para el mismo usuario o dispositivo? *- Esto se debe al diseño de la aplicación Workspace para HTML5 y la aplicación Workspace instalada localmente. El inicio mediante la aplicación Workspace para HTML5 consume una licencia de usuario/dispositivo. Asimismo, el inicio a través de la aplicación Workspace instalada localmente consume una licencia de usuario/dispositivo. Por lo tanto, si un usuario inicia aplicaciones a través de la aplicación Workspace para HTML5 y, a continuación, a través de una versión de la aplicación Workspace instalada localmente, Citrix Cloud muestra que el usuario consumió dos licencias. Esta forma de funcionar no afecta a la conectividad del usuario, pero puede hacer que los informes de uso de licencias de los dispositivos aparezcan "inflados"en la consola de Licencias. Citrix no impide el inicio de ningún servicio si usted usa un exceso de licencias de Cloud.

Supervisar las licencias y el uso activo de Citrix DaaS (usuario/dispositivo)

November 2, 2023

En este artículo se describe cómo puede administrar las asignaciones de licencias de servicios en la nube y supervisar el uso activo a través de la consola Licencias de Citrix Cloud.

Si adquirió Citrix Azure Consumption Fund para usarlo con la implementación de su servicio, consulte Supervisar el consumo de recursos de Azure administrado por Citrix para Citrix DaaS para obtener más información.

Asignación de licencias

Citrix Cloud asigna una licencia cuando un usuario o dispositivo único inicia una aplicación o escritorio por primera vez.

Truncamiento de nombres de dominio

Si aloja varios dominios y tiene usuarios con cuentas similares en esos dominios (por ejemplo, `johnsmith@company.com` y `johnsmith@mycompany.com`), puede permitir que Citrix Cloud ignore el dominio de la cuenta y considere únicamente el nombre de usuario de la cuenta (por ejemplo, antoniolopez). Este proceso se conoce como *truncamiento de nombres de dominio*. De forma predeterminada, el truncamiento de nombres de dominio está inhabilitado.

Cuando se habilita el truncamiento de nombres de dominio, el cálculo de usuarios únicos de Citrix Cloud cambia. En lugar de contar `johnsmith@company.com` y `johnsmith@mycompany.com` como dos usuarios únicos, Citrix Cloud solo cuenta a antoniolopez como usuario único. Este cambio de cálculo afecta a estos datos de Licensing:

- Asignación de licencias
- Uso activo
- Tendencias del uso de licencias a lo largo del tiempo
- Licencias aptas para su publicación

Estos cambios en los datos de licencias también se reflejan al exportar datos a un archivo CSV desde la consola de Licensing.

> **Nota:**
>
> Si aloja varios dominios con cuentas similares en las que el nombre de usuario sea ligeramente

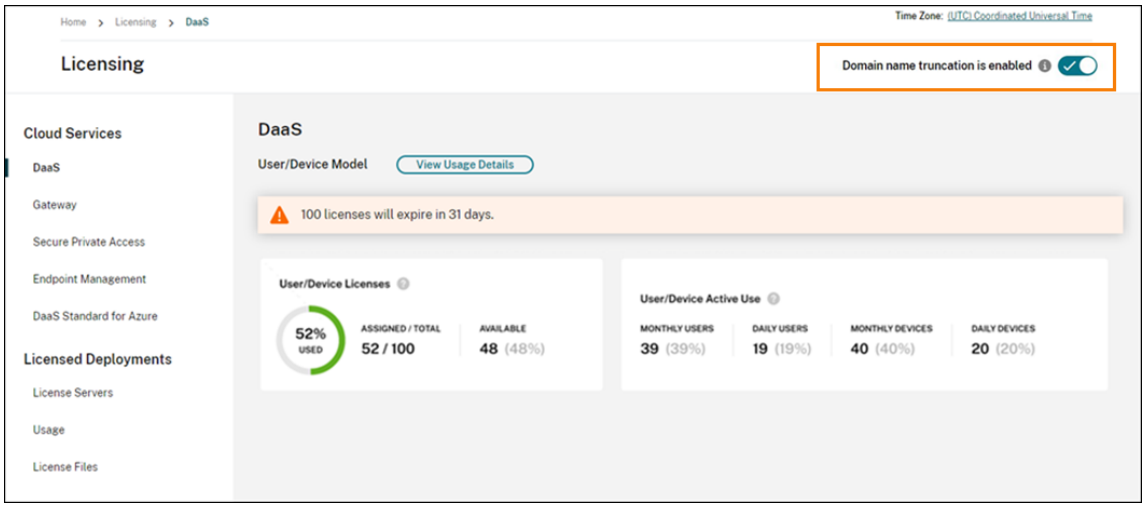
> diferente (por ejemplo, un usuario individual tiene las cuentas `johnsmith@company.com` y `jsmith@newcompany.com`), el truncamiento de nombres de dominio no afecta a los cálculos de Citrix Cloud. Citrix Cloud sigue considerando a antoniolopez y alopez como usuarios únicos aunque pertenezcan a la misma persona.

Habilitar o inhabilitar el truncamiento de nombres de dominio

De forma predeterminada, el truncamiento de nombres de dominio está inhabilitado. El truncamiento de nombres de dominio afecta a los datos de uso del usuario/dispositivo desde el momento en que habilita o inhabilita la función. Por ejemplo, si habilita el truncamiento de nombres de dominio en un mes determinado, los datos que Citrix Cloud registra en ese mes se ven afectados. Sin embargo, los datos históricos de los meses anteriores, cuando la función estaba inhabilitada, no se ven afectados. Del mismo modo, si inhabilita el truncamiento de nombres de dominio en un mes determinado, los datos que Citrix Cloud registra en ese mes se ven afectados. Sin embargo, los datos históricos de los meses en los que se habilitó la función permanecen intactos.

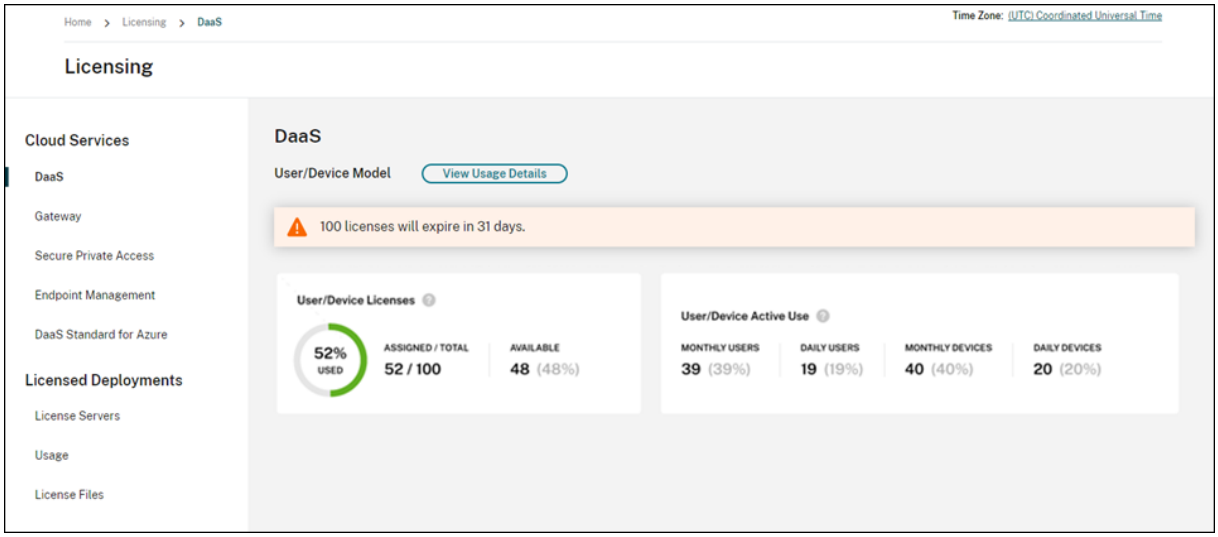
Para habilitar o inhabilitar el truncamiento de nombres de dominio:

1. Haga clic en el botón situado cerca de la esquina superior derecha de la consola de Licensing.



2. Cuando se le pida que confirma la acción, seleccione **Sí, lo entiendo**.

Resumen de las licencias



El resumen de las licencias proporciona una vista rápida de la siguiente información:

- Porcentaje de licencias asignadas respecto al total de licencias adquiridas. El color del porcentaje cambia de verde a amarillo a medida que se aproxima al 100%. El color del porcentaje se vuelve rojo si se excede el 100%.

  El total de licencias adquiridas es la suma de las licencias que se adquirieron para las ediciones de Citrix DaaS que utilizan el modelo de licencias de usuario/dispositivo.
- La relación entre las licencias asignadas y las licencias adquiridas, y la cantidad restante de licencias disponibles.
- Estadísticas del uso activo diario y mensual:
  - El uso activo mensual se refiere a la cantidad de dispositivos o usuarios únicos que han utilizado el servicio en los últimos 30 días.
  - El uso activo diario se refiere a la cantidad de dispositivos o usuarios únicos que han utilizado el servicio en las últimas 24 horas.
- El tiempo que queda para que caduque la suscripción al servicio de la nube. Si la suscripción caduca en los próximos 90 días, aparece un mensaje de advertencia.

Calcular licencias asignadas y uso activo

Para reflejar con precisión el modelo de licencias de usuario/dispositivo para Citrix DaaS, Citrix Cloud cuenta la cantidad de usuarios únicos y dispositivos únicos que han utilizado el servicio. Para medir las licencias asignadas, Citrix Cloud utiliza el menor de estos recuentos. Para medir el uso activo, Citrix Cloud usa cada recuento como la cantidad de usuarios activos y dispositivos activos en un período determinado.

Ejemplo de cálculo de licencias asignadas

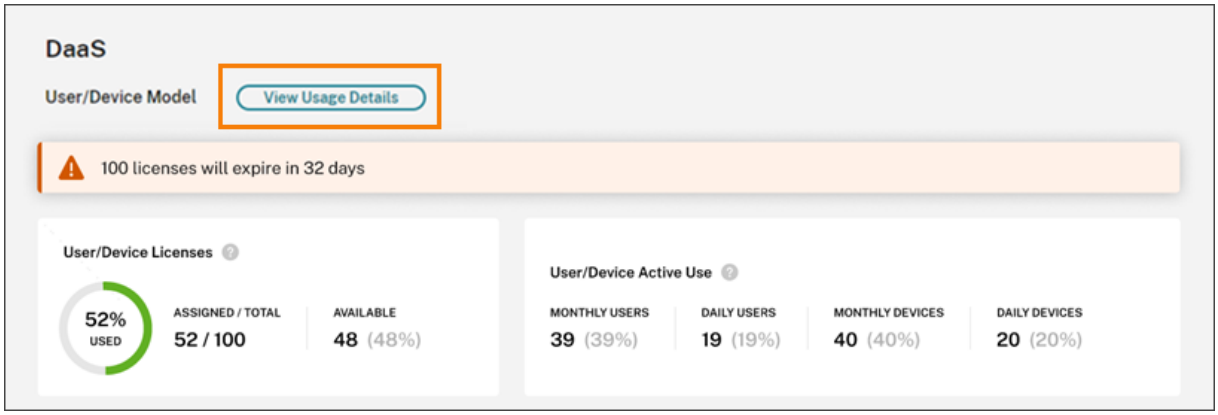
Si 100 usuarios únicos y 50 dispositivos únicos han utilizado el servicio, Citrix Cloud utiliza el número menor (50) para determinar la cantidad de licencias asignadas. El porcentaje de licencias utilizadas y la cantidad de licencias disponibles se basan en estas 50 licencias asignadas.

Ejemplo de cálculo del uso activo

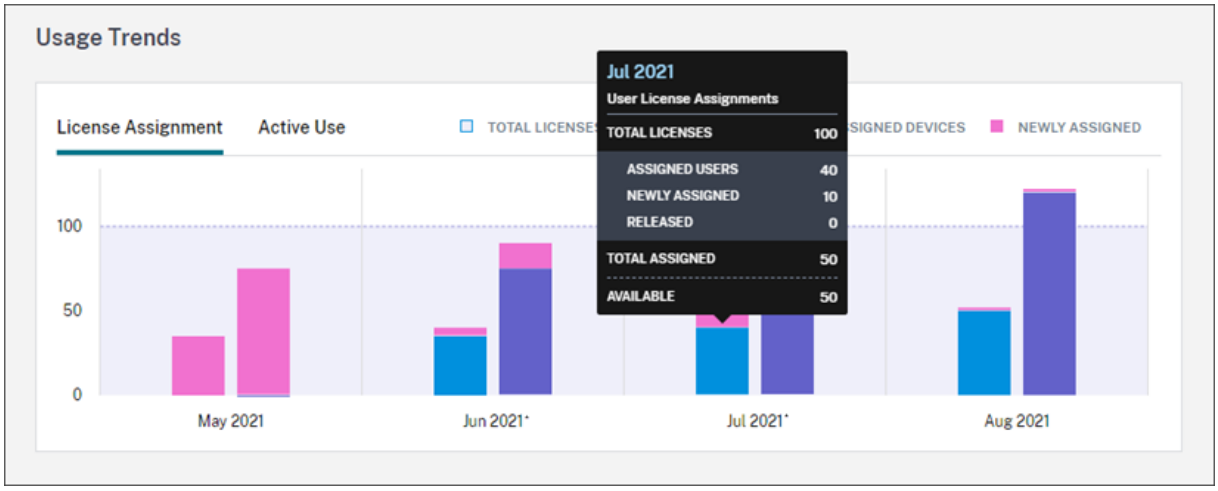
Si 10 usuarios únicos y 20 dispositivos únicos han utilizado el servicio en los últimos 30 días, Citrix Cloud determina que el uso activo mensual es de 10 usuarios activos y 20 dispositivos activos. Del mismo modo, si se contaron 30 usuarios únicos y 15 dispositivos únicos en las últimas 24 horas, Citrix Cloud determina que el uso activo diario es de 30 usuarios activos y 15 dispositivos activos.

Tendencias de uso

Para obtener una vista detallada de sus licencias, haga clic en **Ver detalles de uso** en el extremo derecho del resumen. A continuación, verá un desglose de las tendencias de uso y los dispositivos y usuarios individuales que utilizan licencias de servicios de la nube.



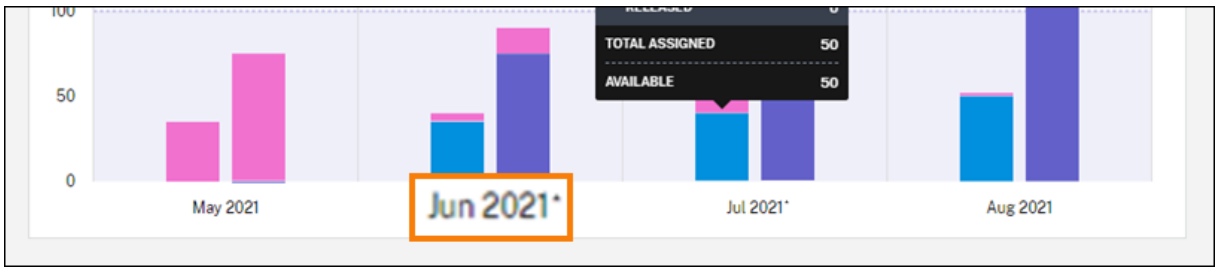
La sección **Tendencias de uso** muestra este desglose como un gráfico.



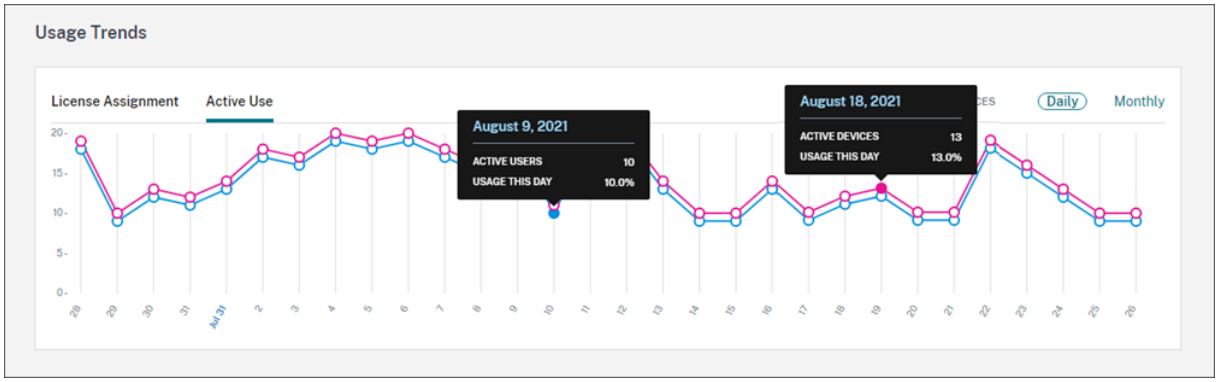
En el gráfico **Asignación de licencias**, cuando se apunta a una barra de un mes o un día específicos, se muestra la información siguiente:

- **Total de licencias:** La cantidad total de licencias que ha comprado del servicio de la nube para todos los derechos incluidos.
- **Usuarios asignados:** El cúmulo de licencias asignadas a los usuarios hasta el mes actual.
- **Dispositivos asignados:** El cúmulo de licencias asignadas a dispositivos hasta el mes actual. Si este número parece particularmente alto para un mes determinado, podría deberse a inicios de aplicaciones o escritorios que ocurren a través de un explorador web. Para reducir este número, Citrix recomienda usar una aplicación Workspace instalada localmente.
- **Asignadas recientemente:** La cantidad de licencias nuevas que se asignaron cada mes. Por ejemplo, un usuario accede al servicio de la nube por primera vez en julio y se le asigna una licencia. Esta licencia se cuenta como "Asignada recientemente"para el mes de julio.
- **Publicadas:** La cantidad de licencias aptas que se liberaron durante cada mes. Por ejemplo, si 20 licencias eran aptas para liberarse y usted liberó 10 de ellas en julio, la cantidad de licencias liberadas que aparece en julio es de 10.

Los intervalos de tiempo en los que está habilitado el truncamiento de dominios se marcan con un asterisco.



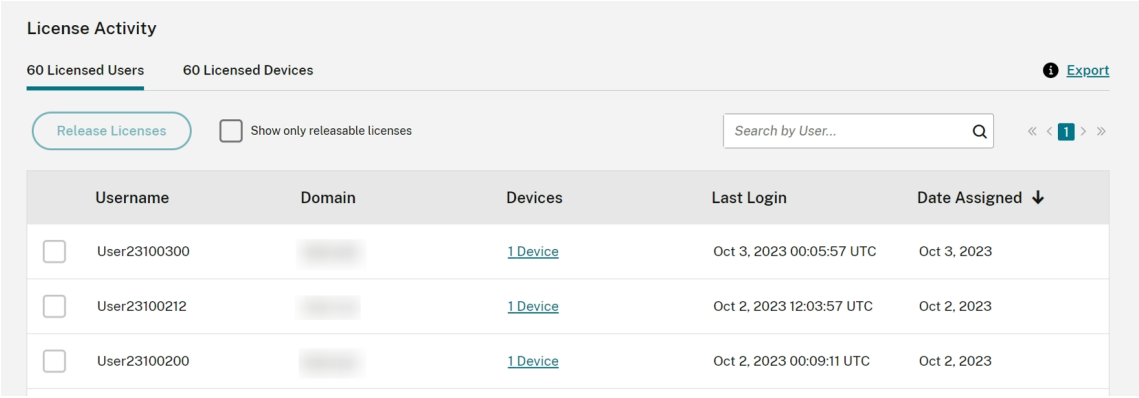
En el gráfico **Uso activo**, se pueden ver usuarios y dispositivos activos durante el mes y el año anteriores, respectivamente. Cuando se apunta a un punto concreto en el gráfico, se revela la cantidad de usuarios o dispositivos activos y el porcentaje de uso.



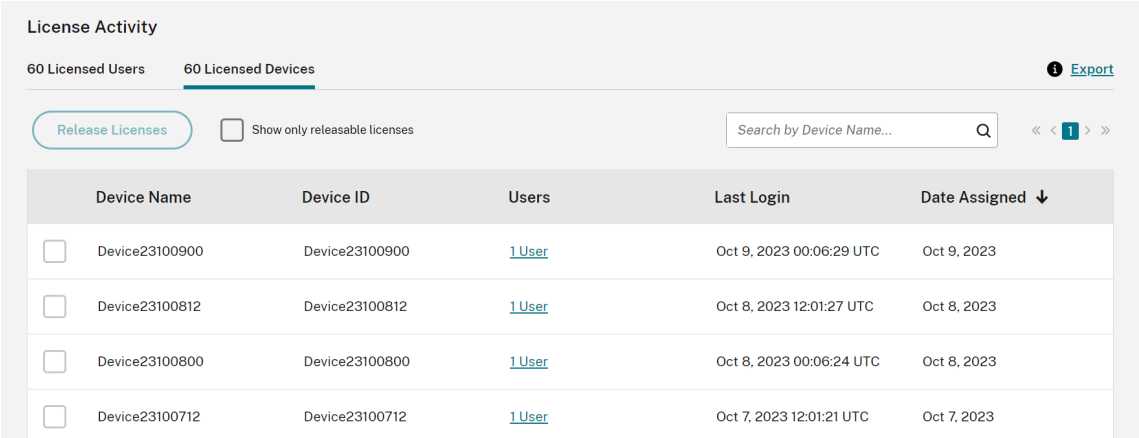
Actividad de licencias

La sección **Actividad de licencias** muestra esta información:

- Una lista de los usuarios individuales que tienen licencias asignadas, incluidos los dispositivos asociados.



- Una lista de los dispositivos que tienen licencias asignadas, incluidos los usuarios asociados.



- La fecha en que se asignó una licencia al usuario o dispositivo.

También puede filtrar la lista para mostrar solamente licencias que pueden liberarse. Consulte Para liberar licencias asignadas en este artículo.

Liberar licencias asignadas

Cuando se asigna una licencia, el período de asignación es de 90 días, y se establece la conexión con el servicio. Si un usuario o dispositivo no ha iniciado aplicaciones ni escritorios durante 90 días, estas licencias se consideran licencias no utilizadas, y Citrix Cloud las libera transcurridos 90 días. Este proceso está automatizado y el administrador necesita hacer nada.

Tras el período de asignación (90 días), el administrador solo puede liberar las licencias manualmente en estos casos:

- El usuario ya no está asociado a la empresa.
- El usuario tiene un permiso de ausencia prolongada.

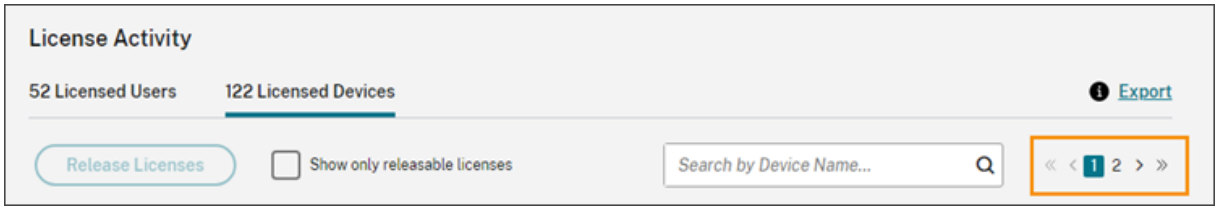
Los administradores pueden liberar las licencias de dispositivos solo cuando los dispositivos están fuera de servicio.

> **Nota:**
>
> - Se recomienda seguir el proceso automatizado de liberación de las licencias. Sin embargo, si el administrador tiene la intención de liberar las licencias antes del período de 90 días, aparte de los motivos mencionados anteriormente, es posible que infrinja el CLUF de Citrix. Antes de realizar esta acción, contacte con Citrix.
> - El administrador puede liberar manualmente una única licencia a través de la interfaz de usuario. Como alternativa, el administrador puede optar por liberar licencias mediante la API de licencias de la nube. Para obtener más información, consulte APIs to manage Citrix cloud licensing.

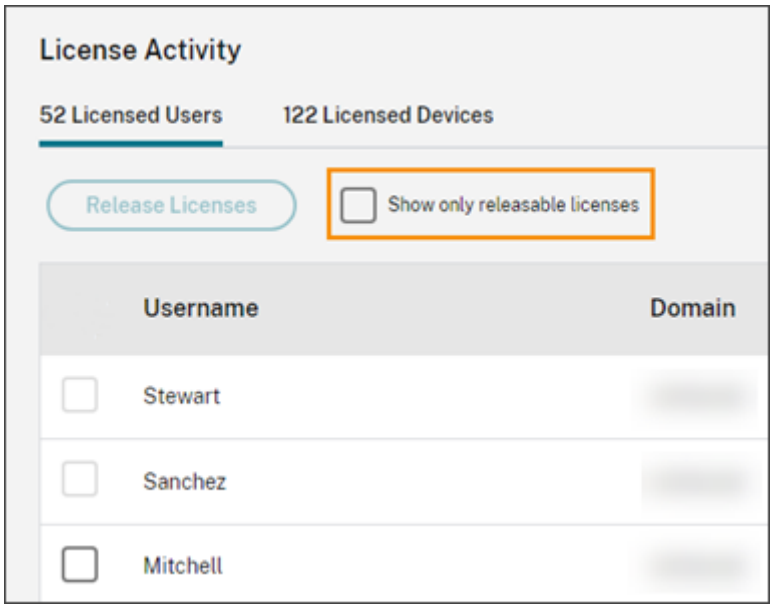
Buscar licencias que se pueden liberar

Si el usuario o el dispositivo no han iniciado aplicaciones ni escritorios durante 30 días, Citrix Cloud coloca la licencia en estado liberable. Las licencias liberables aparecen en la lista Usuarios con licencia o Dispositivos con licencia con una casilla de verificación de color gris oscuro que se puede seleccionar. Las licencias que no se pueden liberar muestran una casilla de verificación gris claro para indicar que la licencia no se puede seleccionar.

La lista que aparece en la sección **Actividad de licencias** muestra hasta 100 licencias asignadas a la vez. Si tiene más de 100 licencias, utilice los controles de página para desplazarse por la lista.



Para encontrar rápidamente las licencias liberables, haga clic en **Mostrar solo licencias que se pueden liberar**, junto al botón **Liberar licencias**. Esta acción oculta licencias asignadas que aún no se pueden liberar.



Seleccionar licencias que se pueden liberar

Marque la casilla gris oscuro situada junto a cada licencia para liberarla. Al seleccionar una licencia de la lista, se activa el botón **Liberar licencias**.

Puede seleccionar todas las licencias liberables una por una y hacer clic en **Liberar licencias**.

Para liberar licencias asignadas

1. En **Actividad de licencias**, haga clic en la ficha **Usuarios con licencias** o **Dispositivos con licencia**.
2. Si es necesario, haga clic en **Mostrar licencias que se pueden liberar** para mostrar solo los usuarios con licencias que pueden liberarse.
3. Seleccione los usuarios o dispositivos que quiera administrar y, a continuación, haga clic en **Liberar licencias**.
4. Revise los usuarios o dispositivos seleccionados y, a continuación, haga clic en **Liberar licencias**.

Supervisar las licencias y los picos de uso de Citrix DaaS (licencias de usuario simultáneas)

October 2, 2023

En este artículo se describe la experiencia de administrar licencias de usuario simultáneas únicamente para **Citrix DaaS**.

Para obtener información sobre las licencias de usuario/dispositivo para Citrix DaaS, consulte Supervisar las licencias y el uso activo de Citrix DaaS (usuario/dispositivo).

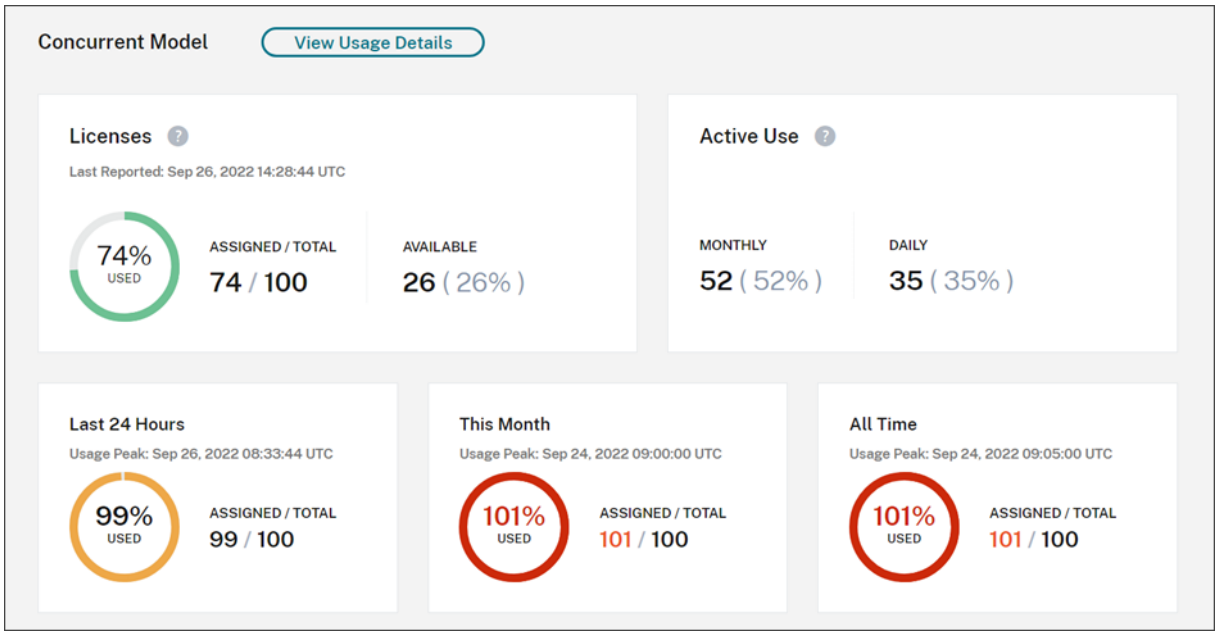
Para obtener información sobre las licencias de usuario/dispositivo y las licencias de usuario simultáneas para Citrix DaaS Standard para Azure, consulte Supervisar las licencias y el uso de Citrix DaaS Standard para Azure.

Asignación de licencias

Citrix Cloud asigna una licencia cuando un usuario inicia una aplicación o un escritorio en su dispositivo. Cuando el usuario cierra sesión o se desconecta de la sesión, la licencia ya no se asigna. Dado que la asignación de licencias puede cambiar en función del número de dispositivos que acceden a aplicaciones o escritorios en un momento dado, Citrix Cloud evalúa el número de licencias en uso cada cinco minutos.

Para obtener más información sobre el modelo de licencias de usuario simultáneas, consulte Licencia simultánea en la documentación de producto de Licensing.

Resumen de las licencias



El resumen de las licencias proporciona una vista rápida de la siguiente información:

- Porcentaje del total de licencias adquiridas actualmente en uso cuando Citrix Cloud evaluó por última vez las licencias en uso. Citrix Cloud calcula este porcentaje cada cinco minutos en función de los dispositivos únicos con conexiones activas al servicio. El total de licencias adquiridas es la suma de las licencias que se adquirieron para las ediciones de Citrix DaaS que utilizan el modelo de licencias de usuario simultáneas.
- La relación entre las licencias asignadas actualmente a las licencias adquiridas totales, y la cantidad restante de licencias disponibles. La cifra **Total** que se muestra en esta relación representa la cantidad total de licencias en propiedad actualmente (a partir de la fecha y la hora del último informe).
- Estadísticas de pico de uso. Al calcular el pico de licencias en uso, Citrix Cloud obtiene el máximo de licencias utilizadas en los siguientes períodos de tiempo:
  - **Últimas 24 horas:** El máximo de licencias utilizadas simultáneamente durante las últimas 24 horas.
  - **Este mes:** El máximo de licencias utilizadas simultáneamente en el mes del calendario actual.
  - **Siempre:** El máximo de licencias utilizadas simultáneamente desde el inicio de la suscripción.

  La cifra **Total** mostrada para estos períodos de pico de uso representa el total de licencias en propiedad en ese momento. Si el total de licencias en propiedad aumenta o disminuye y hay un aumento correspondiente en las licencias asignadas, la cifra **Total** cambia para reflejar la

nueva cantidad de licencias en propiedad en ese momento. Sin embargo, si no hay un pico de uso correspondiente, la cifra **Total** no cambia.

- Estadísticas de uso activo. Citrix Cloud muestra la cantidad total de conexiones únicas durante estos períodos:
  - **Mensual:** La cantidad total de conexiones del mes natural anterior.
  - **Diario:** La cantidad total de conexiones de las 24 horas anteriores.
    Estas cifras también se representan como porcentajes del total de licencias en su posesión durante estos períodos.

Calcular el pico de licencias en uso

Para reflejar con precisión el modelo de licencias de usuario simultáneas, Citrix Cloud cuenta la cantidad de dispositivos únicos que han accedido al servicio de forma simultánea cada cinco minutos. Si el recuento es mayor que el pico de uso actual que se muestra, Citrix Cloud muestra el nuevo pico de uso con la fecha y la hora en que se alcanzó. Si el recuento es menor que el pico de uso actual, el pico de uso actual no cambia.

> **Importante:**
>
> Si utiliza Supervisar en Director para obtener información acerca de las sesiones simultáneas, tenga en cuenta que el informe de Supervisar proporciona una interpretación diferente de las sesiones simultáneas y no refleja con precisión el número de licencias de usuario simultáneas en uso. Para obtener más información acerca de las diferencias entre los informes de Supervisar y los informes de Licencias, consulte las Preguntas frecuentes.

Calcular el uso activo mensual

Al principio de cada mes, Citrix Cloud toma una instantánea del mes natural anterior. Citrix Cloud muestra la cantidad total de conexiones únicas que hubo durante ese mes natural.

Calcular el uso activo diario

Todos los días, a la misma hora, Citrix Cloud toma una instantánea de las 24 horas anteriores. Citrix Cloud muestra la cantidad total de conexiones únicas que hubo durante ese período de 24 horas.

Tendencias de uso y actividad de licencias

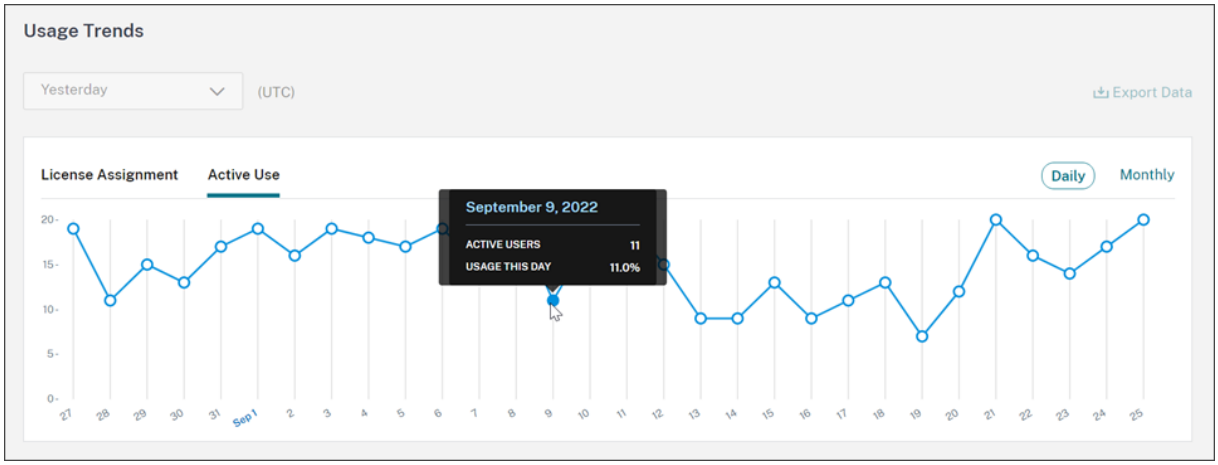
Para obtener una vista histórica de sus licencias, haga clic en **Ver detalles de uso**.

La sección **Tendencias de uso** muestra la siguiente información:

- **Asignación de licencias** muestra un gráfico con esta información:
  - **Total de licencias:** El total de licencias de usuario simultáneas adquiridas.
  - **Pico de licencias en uso:** El máximo de licencias asignadas para el intervalo de fechas seleccionado. De forma predeterminada, Citrix Cloud muestra el pico de uso para cada mes del año natural actual. Para ver un desglose del pico de uso mensual o por horas, seleccione el mes o día del calendario que quiere ver en el menú desplegable.

  Si el intervalo de fechas seleccionado aún no ha terminado, Citrix Cloud muestra el pico de uso actual del último intervalo de tiempo. Por ejemplo, si desglosa un día natural que aún está en curso, se muestra el máximo de licencias por cada hora hasta el momento actual. Si el máximo de licencias aumenta en el siguiente intervalo de cinco minutos, Citrix Cloud actualiza el pico de uso de la hora actual.
- **Uso activo** muestra un gráfico con esta información:
  - **Diario:** La cantidad total de conexiones de cada día durante los 30 días anteriores.
  - **Mensual:** La cantidad total de conexiones de cada mes durante año natural anterior.

Al señalar un intervalo en los gráficos **Asignación de licencias** o **Uso activo**, se muestran los detalles de ese intervalo.



Liberar licencias

Las licencias de usuario simultáneas se liberan automáticamente cuando los usuarios cierran sesión o se desconectan de su sesión. No necesita liberar estas licencias manualmente.

Supervisar el uso y las licencias de Citrix DaaS Standard para Azure

November 2, 2023

En este artículo se describe la experiencia de administrar asignaciones de licencias para los modelos de licencias de usuario/dispositivo y de licencias de usuario simultáneas.

Citrix Azure Consumption Fund (solo para licencias de usuario/dispositivo)

Si adquirió Citrix Azure Consumption Fund para usarlo con la implementación de su servicio, consulte Supervisar el consumo de recursos de Azure administrado por Citrix para Citrix DaaS para obtener más información sobre los informes de consumo de los recursos administrados por Citrix.

Asignación de licencias

Modelo de licencias de usuario/dispositivo: Citrix Cloud asigna una licencia cuando un usuario o un dispositivo únicos inician un escritorio por primera vez.

Modelo de licencias de usuario simultáneas: Citrix Cloud asigna una licencia cuando un usuario inicia una aplicación o un escritorio en su dispositivo. Cuando el usuario cierra sesión o se desconecta de la sesión, la licencia ya no se asigna. Dado que la asignación de licencias puede cambiar en función del número de dispositivos que acceden a escritorios en un momento dado, Citrix Cloud evalúa el número de licencias en uso cada cinco minutos.

Para obtener más información sobre el modelo de licencias simultáneas, consulte Licencias simultáneas en la documentación de producto de Licensing.

Calcular el pico de licencias en uso

Para reflejar con precisión el modelo de licencias simultáneas, Citrix Cloud cuenta la cantidad de dispositivos únicos que han accedido al servicio de forma simultánea cada cinco minutos. Si el recuento es mayor que el pico de uso actual que se muestra, Citrix Cloud muestra el nuevo pico de uso con la fecha y la hora en que se alcanzó. Si el recuento es menor que el pico de uso actual, el pico de uso actual no cambia.

Truncamiento de nombres de dominio

Esta función solo está disponible para el modelo de licencias de **usuario/dispositivo**.

Si aloja varios dominios y tiene usuarios con cuentas similares en esos dominios (por ejemplo, `johnsmith@company.com` y `johnsmith@mycompany.com`), puede permitir que Citrix Cloud ignore el dominio de la cuenta y considere únicamente el nombre de usuario de la cuenta (por ejemplo, antoniolopez). Este proceso se conoce como *truncamiento de nombres de dominio*. De forma predeterminada, el truncamiento de nombres de dominio está inhabilitado.

Cuando se habilita el truncamiento de nombres de dominio, el cálculo de usuarios únicos de Citrix Cloud cambia. En lugar de contar `johnsmith@company.com` y `johnsmith@mycompany.com` como dos usuarios únicos, Citrix Cloud solo cuenta a antoniolopez como usuario único. Este cambio de cálculo afecta a estos datos de Licensing:

- Asignación de licencias
- Uso activo
- Tendencias del uso de licencias a lo largo del tiempo
- Licencias aptas para su publicación

Estos cambios en los datos de licencias también se reflejan al exportar datos a un archivo CSV desde la consola de Licensing.

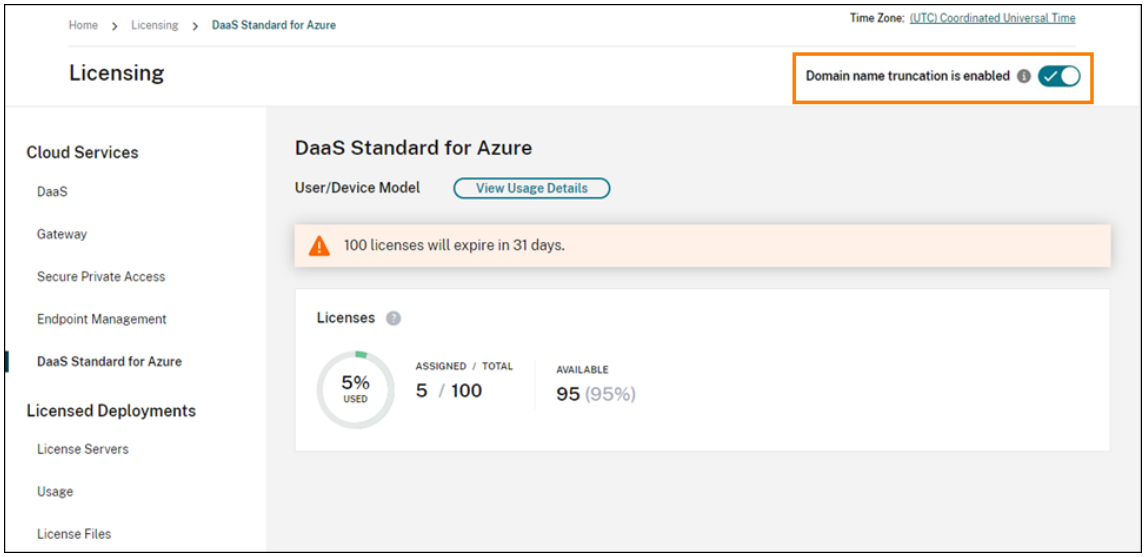
> **Nota:**
>
> Si aloja varios dominios con cuentas similares en las que el nombre de usuario sea ligeramente diferente (por ejemplo, un usuario individual tiene las cuentas `johnsmith@company.com` y `jsmith@newcompany.com`), el truncamiento de nombres de dominio no afecta a los cálculos de Citrix Cloud. Citrix Cloud sigue considerando a antoniolopez y alopez como usuarios únicos aunque pertenezcan a la misma persona.

Habilitar o inhabilitar el truncamiento de nombres de dominio

De forma predeterminada, el truncamiento de nombres de dominio está inhabilitado. El truncamiento de nombres de dominio afecta a los datos de uso del usuario/dispositivo desde el momento en que habilita o inhabilita la función. Por ejemplo, si habilita el truncamiento de nombres de dominio en un mes determinado, los datos que Citrix Cloud registra en ese mes se ven afectados. Sin embargo, los datos históricos de los meses anteriores, cuando la función estaba inhabilitada, no se ven afectados. Del mismo modo, si inhabilita el truncamiento de nombres de dominio en un mes determinado, los datos que Citrix Cloud registra en ese mes se ven afectados. Sin embargo, los datos históricos de los meses en los que se habilitó la función permanecen intactos.

Para habilitar o inhabilitar el truncamiento de nombres de dominio:

1. Haga clic en el botón situado cerca de la esquina superior derecha de la consola de Licensing.



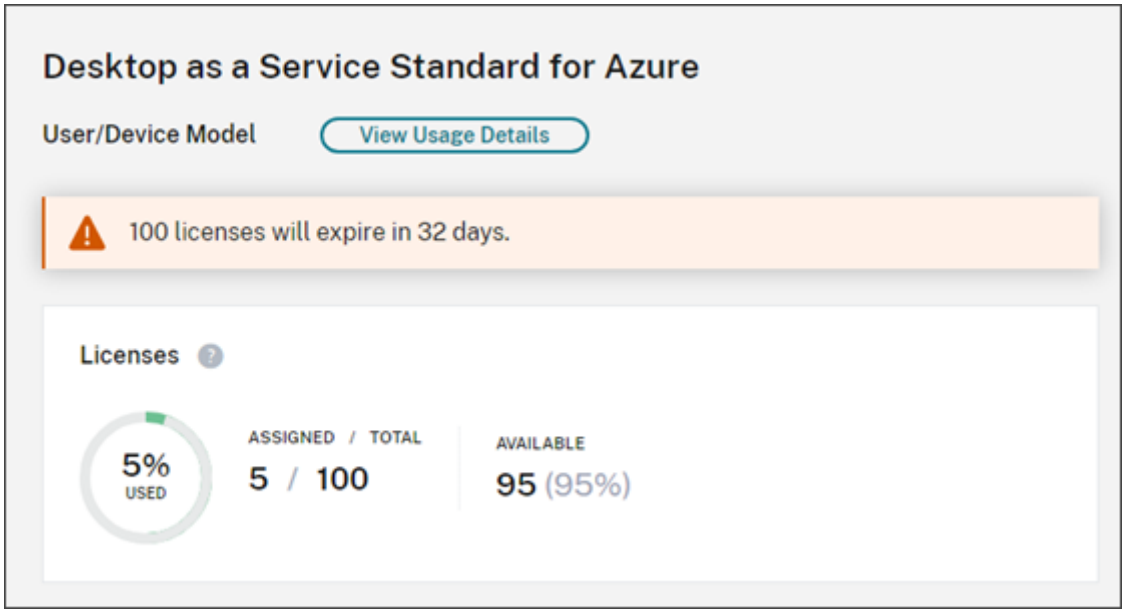
2. Cuando se le pida que confirma la acción, seleccione **Sí, lo entiendo**.

Resumen de las licencias

Citrix Cloud muestra vistas resumidas de las licencias que se están usando en los modelos de licencias de usuario/dispositivo y de licencias de usuario simultáneas.

Resumen para usuarios y dispositivos

Para el modelo de usuario/dispositivo, el resumen de las licencias muestra las licencias que se están usando en relación con la cantidad total de licencias que usted posea.

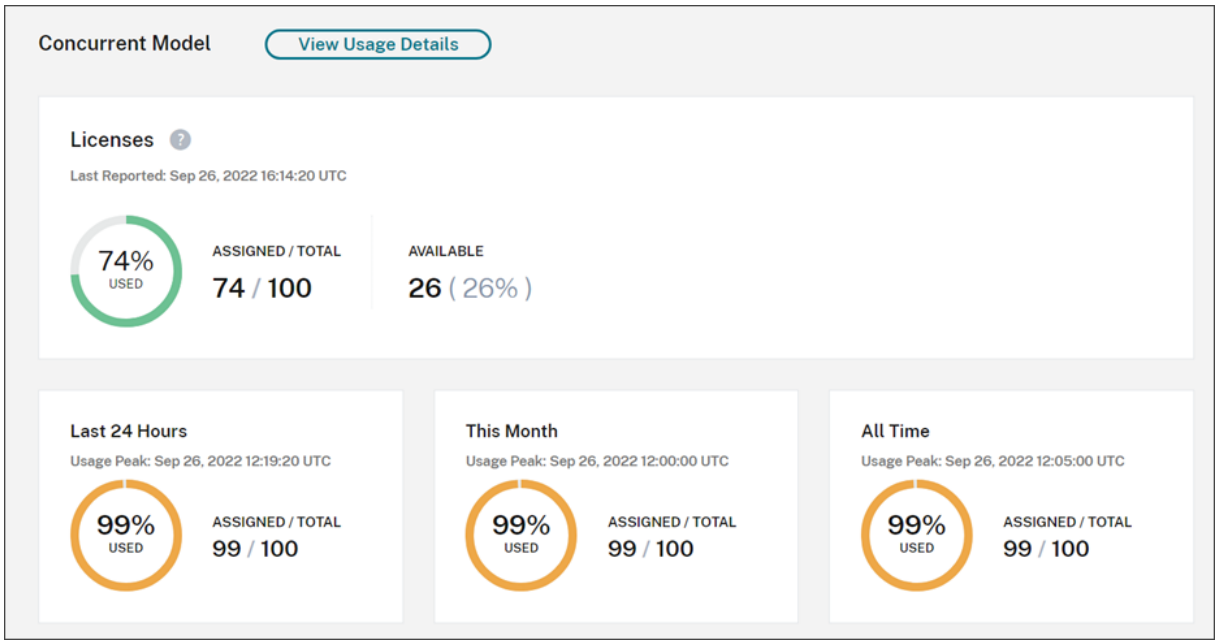


El color del porcentaje cambia de verde a amarillo a medida que se aproxima al 100%. El color del porcentaje se vuelve rojo si se excede el 100%.

Citrix Cloud también muestra la relación entre las licencias asignadas y las licencias adquiridas, y la cantidad restante de licencias disponibles.

Resumen para licencias de usuario simultáneas

Para el modelo de licencias simultáneas, el resumen de las licencias proporciona una visión general de esta información:



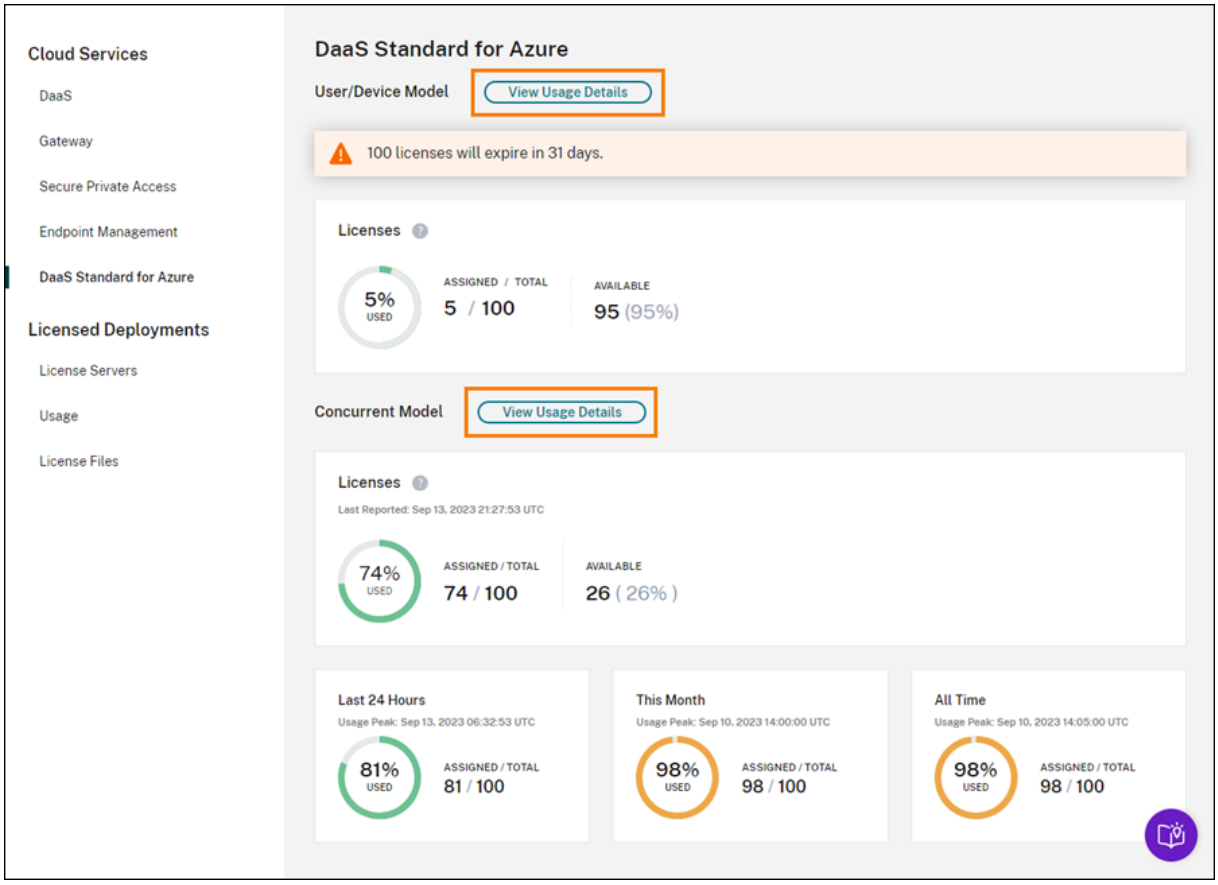
- Porcentaje del total de licencias adquiridas actualmente en uso cuando Citrix Cloud evaluó por última vez las licencias en uso. Citrix Cloud calcula este porcentaje cada cinco minutos en función de los dispositivos únicos con conexiones activas al servicio. El total de licencias adquiridas es la suma de las licencias que se adquirieron para Citrix DaaS Standard para Azure que utilizan el modelo de licencias simultáneas.
- La relación entre las licencias asignadas actualmente a las licencias adquiridas totales, y la cantidad restante de licencias disponibles. La cifra **Total** que se muestra en esta relación representa la cantidad total de licencias en propiedad actualmente (a partir de la fecha y la hora del último informe).
- Estadísticas de pico de uso. Al calcular el pico de licencias en uso, Citrix Cloud obtiene el máximo de licencias utilizadas en los siguientes períodos de tiempo:
  - **Últimas 24 horas:** El máximo de licencias utilizadas simultáneamente durante las últimas 24 horas.

- **Este mes:** El máximo de licencias utilizadas simultáneamente en el mes del calendario actual.
- **Siempre:** El máximo de licencias utilizadas simultáneamente desde el inicio de la suscripción.

La cifra **Total** mostrada para estos períodos de pico de uso representa el total de licencias en propiedad en ese momento. Si el total de licencias en propiedad aumenta o disminuye y hay un aumento correspondiente en las licencias asignadas, la cifra **Total** cambia para reflejar la nueva cantidad de licencias en propiedad en ese momento. Sin embargo, si no hay un pico de uso correspondiente, la cifra **Total** no cambia.

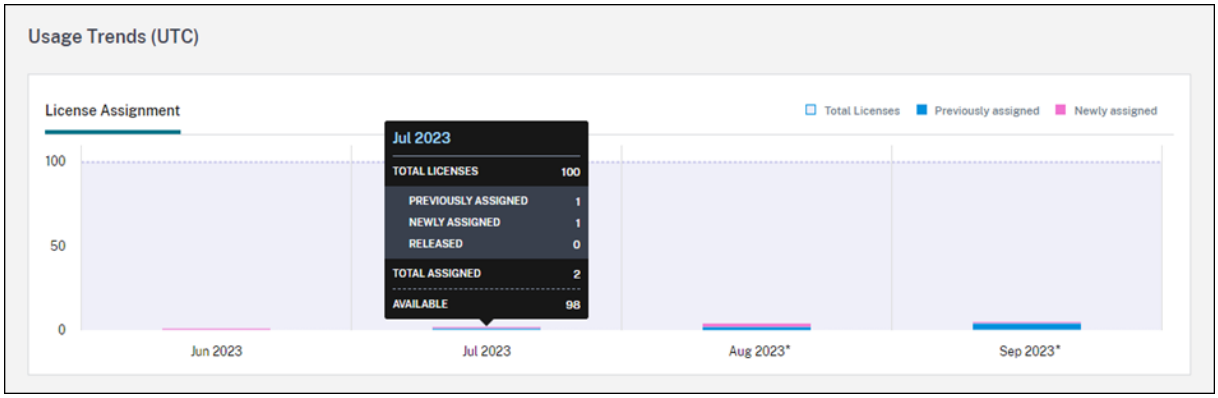
Tendencias de uso

Citrix Cloud muestra un desglose de las tendencias de uso de las licencias de usuario/dispositivo y de las licencias de usuario simultáneas. Para ver este desglose, seleccione **Ver detalles de uso** en la página de resumen de las licencias.



Tendencias para usuarios y dispositivos

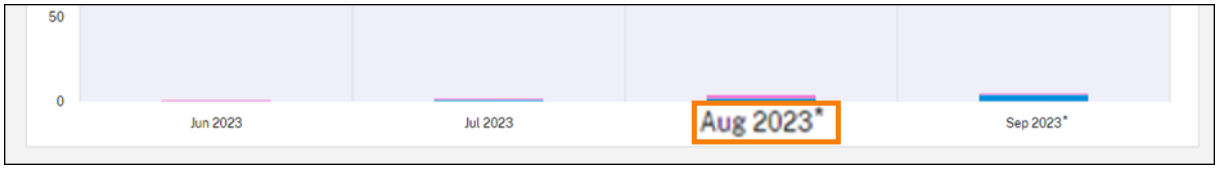
En el caso de las licencias de usuario/dispositivo, la sección **Tendencias de uso** muestra un desglose de las licencias asignadas en forma de gráfico.



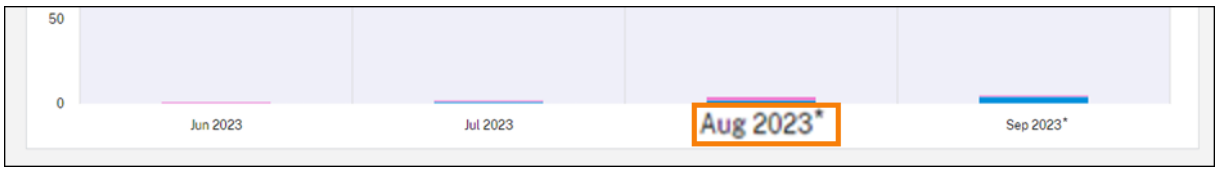
Al señalar un intervalo en el gráfico, se muestra esta información:

- **Total de licencias:** La cantidad total de licencias que ha comprado del servicio de la nube para todos los derechos incluidos.
- **Asignadas previamente:** La cantidad de licencias asignadas en el mes anterior. Por ejemplo, un usuario accede al servicio de la nube por primera vez en julio y se le asigna una licencia. Esta licencia se cuenta como "Asignada recientemente"para el mes de julio. Para el mes de agosto, esta licencia se cuenta como "Asignada previamente".
- **Asignadas recientemente:** La cantidad de licencias nuevas que se asignaron cada mes. Por ejemplo, un usuario accede al servicio de la nube por primera vez en julio y se le asigna una licencia. Esta licencia se cuenta como "Asignada recientemente"para el mes de julio.

Los intervalos de tiempo en los que está habilitado el truncamiento de dominios se marcan con un asterisco.



Los intervalos de tiempo en los que está habilitado el truncamiento de dominios se marcan con un asterisco.



Tendencias para licencias de usuario simultáneas

En el caso de las licencias de usuario simultáneas, la sección **Tendencias de uso** muestra esta información:

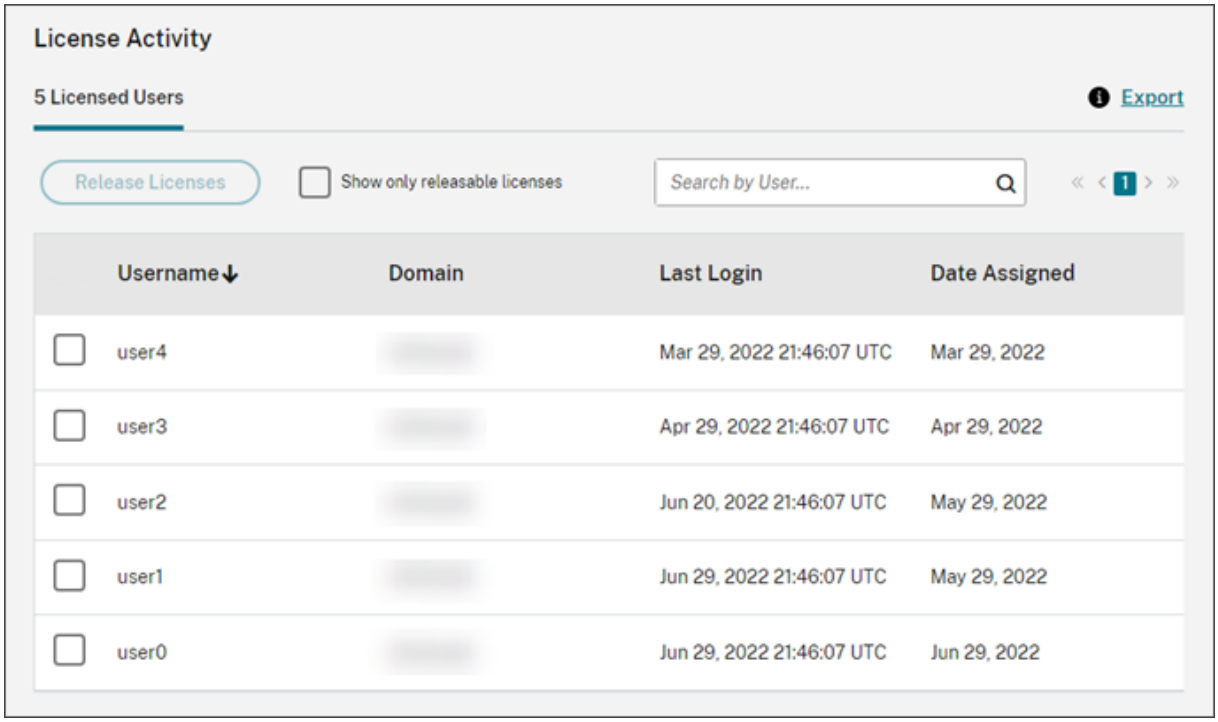
- **Total de licencias:** El total de licencias simultáneas adquiridas.
- **Pico de licencias en uso:** El máximo de licencias asignadas para el intervalo de fechas seleccionado. De forma predeterminada, Citrix Cloud muestra el pico de uso para cada mes del año natural actual. Para ver un desglose del pico de uso mensual o por horas, seleccione el mes o día del calendario que quiere ver en el menú desplegable.

  Si el intervalo de fechas seleccionado aún no ha terminado, Citrix Cloud muestra el pico de uso actual del último intervalo de tiempo. Por ejemplo, si desglosa un día natural que aún está en curso, se muestra el máximo de licencias por cada hora hasta el momento actual. Si el máximo de licencias aumenta en el siguiente intervalo de cinco minutos, Citrix Cloud actualiza el pico de uso de la hora actual.

Al señalar un intervalo en el gráfico, se muestran el total de licencias y los picos de licencias en uso durante ese intervalo.

Actividad de las licencias para usuarios y dispositivos

Para las licencias de usuario/dispositivo, la sección **Actividad de licencias** muestra una lista de usuarios individuales que tienen licencias asignadas licencias y la fecha en que se les asignaron. Esta sección no está disponible para las licencias simultáneas.



También puede filtrar la lista para mostrar solamente licencias que pueden liberarse. Consulte Liberar licencias asignadas en este artículo.

Liberar licencias de usuario/dispositivo

La capacidad para liberar licencias de usuario/dispositivo que cumplan los requisitos varía según el tipo de suscripción al servicio.

- **Suscripciones anuales al servicio:** Si tiene una suscripción anual, puede liberar licencias para usuarios que no hayan iniciado una aplicación o un escritorio en los últimos 30 días. Puede liberar varias licencias en bloque o una a una.
- **Suscripciones mensuales al servicio:** Si tiene una suscripción mensual, puede liberar licencias el primer día de cada mes, independientemente del período de inactividad.

Cuando se asigna una licencia, el período de asignación es de 90 días, y se establece la conexión con el servicio. Si un usuario o dispositivo no ha iniciado aplicaciones ni escritorios durante 90 días, estas licencias se consideran licencias no utilizadas, y Citrix Cloud las libera transcurridos 90 días. Este proceso está automatizado y el administrador necesita hacer nada.

Tras el período de asignación (90 días), el administrador solo puede liberar las licencias manualmente en estos casos:

- El usuario ya no está asociado a la empresa.
- El usuario tiene un permiso de ausencia prolongada.

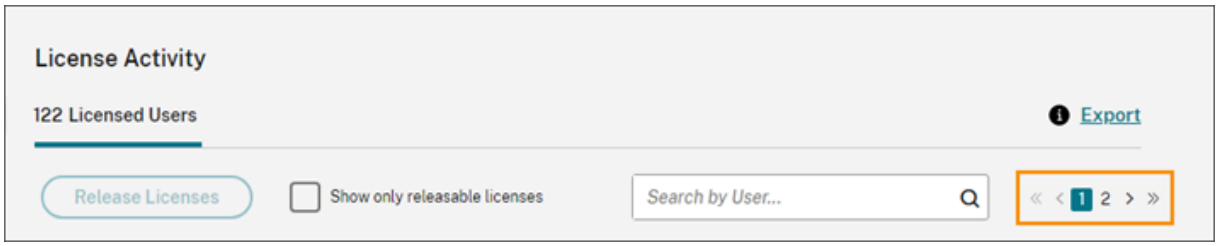
Los administradores pueden liberar las licencias de dispositivos solo cuando los dispositivos están fuera de servicio.

> **Nota:**
>
> - Se recomienda seguir el proceso automatizado de liberación de las licencias. Sin embargo, si el administrador tiene la intención de liberar las licencias antes del período de 90 días, aparte de los motivos mencionados anteriormente, es posible que infrinja el CLUF de Citrix. Antes de realizar esta acción, contacte con Citrix.
> - El administrador puede liberar manualmente una única licencia a través de la interfaz de usuario. Como alternativa, el administrador puede optar por liberar licencias mediante la API de licencias de la nube. Para obtener más información, consulte APIs to manage Citrix cloud licensing.

Buscar licencias aptas

Si el usuario o el dispositivo no han iniciado aplicaciones ni escritorios durante 30 días, Citrix Cloud coloca la licencia en estado liberable. Las licencias liberables aparecen en la lista Usuarios con licencia o Dispositivos con licencia con una casilla de verificación de color gris oscuro que se puede seleccionar. Las licencias que no se pueden liberar muestran una casilla de verificación gris claro para indicar que la licencia no se puede seleccionar.

La lista que aparece en la sección **Actividad de licencias** muestra hasta 100 licencias asignadas a la vez. Si tiene más de 100 licencias, utilice los controles de página para desplazarse por la lista.



Para encontrar rápidamente las licencias aptas, seleccione **Mostrar solo licencias que se pueden liberar**, junto al botón **Liberar licencias**. Esta acción oculta licencias asignadas que aún no se pueden liberar.

Seleccionar licencias aptas

Marque la casilla gris oscuro situada junto a cada licencia para liberarla. Al seleccionar una licencia, se activa el botón **Liberar licencias**.

Puede seleccionar todas las licencias liberables una por una y hacer clic en **Liberar licencias**.

Liberar licencias asignadas

1. Si es necesario, haga clic en **Mostrar licencias que se pueden liberar** para mostrar solo los usuarios con licencias que pueden liberarse.
2. Seleccione los usuarios que quiera administrar y, a continuación, haga clic en **Liberar licencias**.
3. Revise los usuarios seleccionados y, a continuación, haga clic en **Liberar licencias**.

Liberar licencias de usuario simultáneas

Las licencias de usuario simultáneas se liberan automáticamente cuando los usuarios cierran sesión o se desconectan de su sesión. No necesita liberar estas licencias manualmente.

Supervisar licencias y el uso activo en Endpoint Management

November 27, 2023

Asignación de licencias

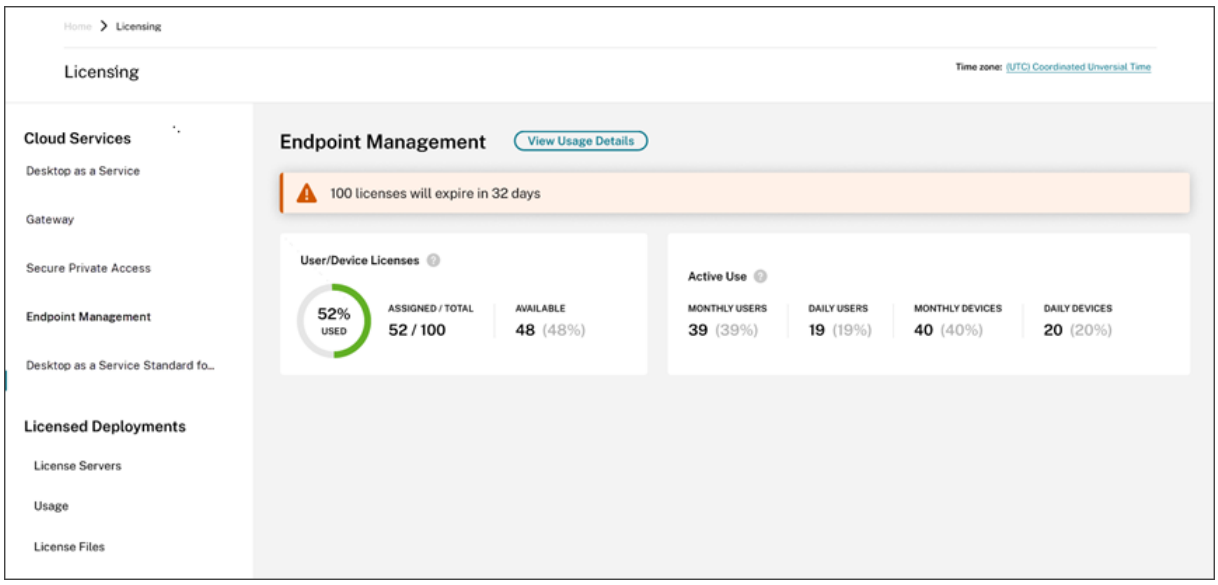
En general, a los usuarios se les asigna una licencia al usar por primera vez un servicio de la nube. Para Endpoint Management, se asigna una licencia cuando un usuario inscribe un dispositivo. Una

vez inscrito el dispositivo, se le realizan comprobaciones periódicas con Citrix Cloud. A continuación, Citrix Cloud utiliza este "pulso de comprobaciones"para calcular el uso mensual y ayuda a los administradores a estar al día del uso más reciente del servicio por parte de los usuarios.

El primer uso se produce la primera vez que un usuario inscribe un dispositivo o la primera vez que se genera un "pulso de comprobaciones"para el dispositivo.

Las licencias se asignan por usuario. Por lo tanto, si dos usuarios inscriben y usan el mismo dispositivo, se asignan dos licencias.

Resumen y detalles de la función Licencias

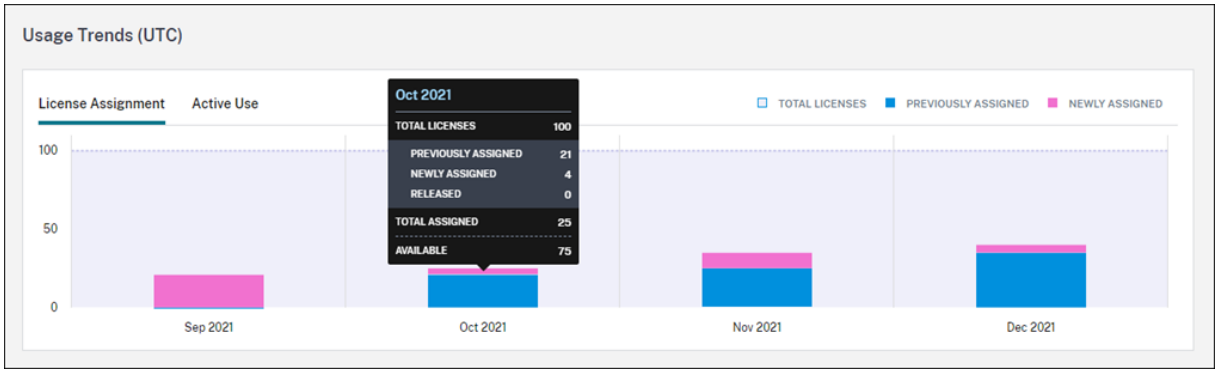


El resumen de Licencias ofrece una vista general de la siguiente información para cada servicio disponible:

- Porcentaje de licencias asignadas respecto al total de licencias adquiridas. El color del porcentaje cambia de verde a amarillo a medida que se aproxima al 100%. El color del porcentaje se vuelve rojo si se excede el 100%.
- La relación entre las licencias asignadas y las licencias adquiridas, y la cantidad restante de licencias disponibles.
- Estadísticas del uso activo diario y mensual:
  - El uso activo mensual se refiere a la cantidad de usuarios únicos que han utilizado el servicio en los últimos 30 días.
  - El uso activo diario se refiere a la cantidad de usuarios únicos que han utilizado el servicio en las últimas 24 horas.
- El tiempo que queda para que caduque la suscripción al servicio de la nube. Si la suscripción caduca en los próximos 90 días, aparece un mensaje de advertencia.

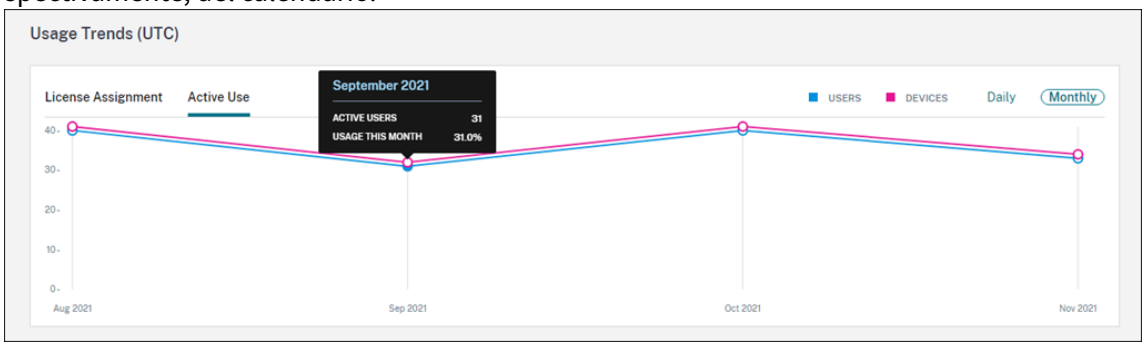
Tendencias de uso

Para obtener una vista detallada de sus licencias, haga clic en **Ver detalles de uso**. A continuación, verá un desglose de las tendencias de uso y los dispositivos y usuarios individuales que utilizan licencias de servicios de la nube.



Este desglose muestra la siguiente información:

- **Total de licencias:** La cantidad total de licencias que ha comprado del servicio de la nube para todos los derechos incluidos.
- **Asignadas previamente:** Las licencias del servicio Cloud que ya estaban asignadas al principio de cada mes. Por ejemplo, si a un usuario se le asigna una licencia en julio, esa asignación se cuenta en la cantidad de "Asignadas previamente"en el mes de agosto.
- **Asignadas recientemente:** La cantidad de licencias de servicios de nube que se asignaron ese mes. Por ejemplo, se asignará una licencia a un usuario que accede al servicio Cloud por primera vez en julio. Esta licencia se cuenta en la cantidad de "Asignadas recientemente"en el mes de julio.
- **Uso activo:** Tendencias del uso activo diario y mensual durante el mes y el año anteriores, respectivamente, del calendario.

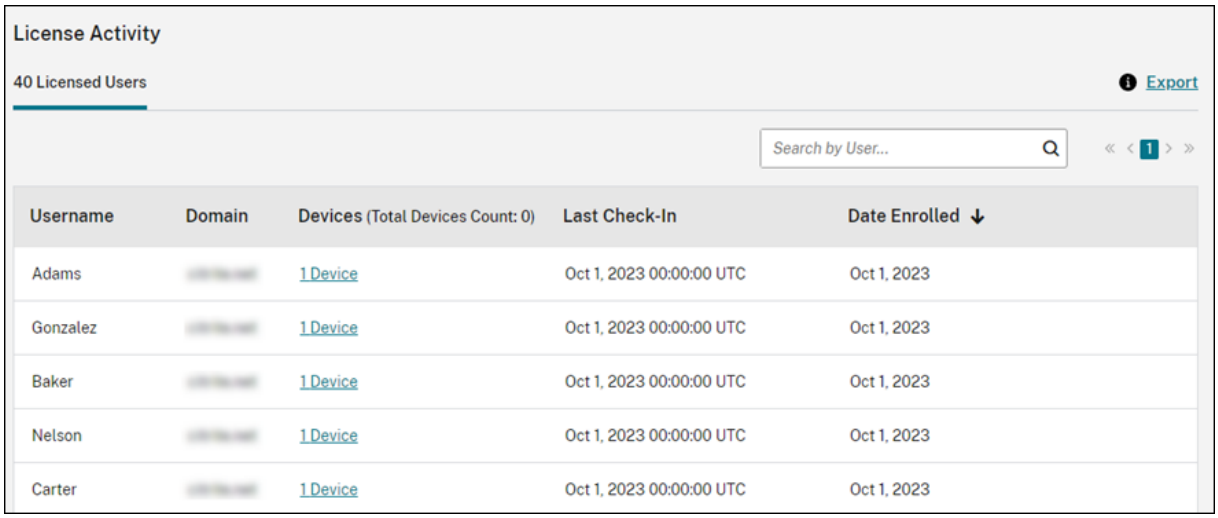


Actividad de licencias

La sección **Actividad de licencias** muestra una lista con esta información:

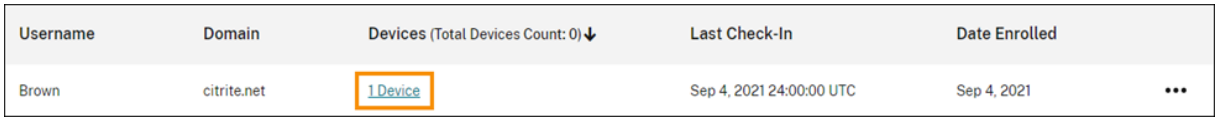
- Los usuarios con licencias asignadas

- La fecha en que se han asignado las licencias
- La cantidad de dispositivos inscritos y la fecha de la última comprobación de cada usuario

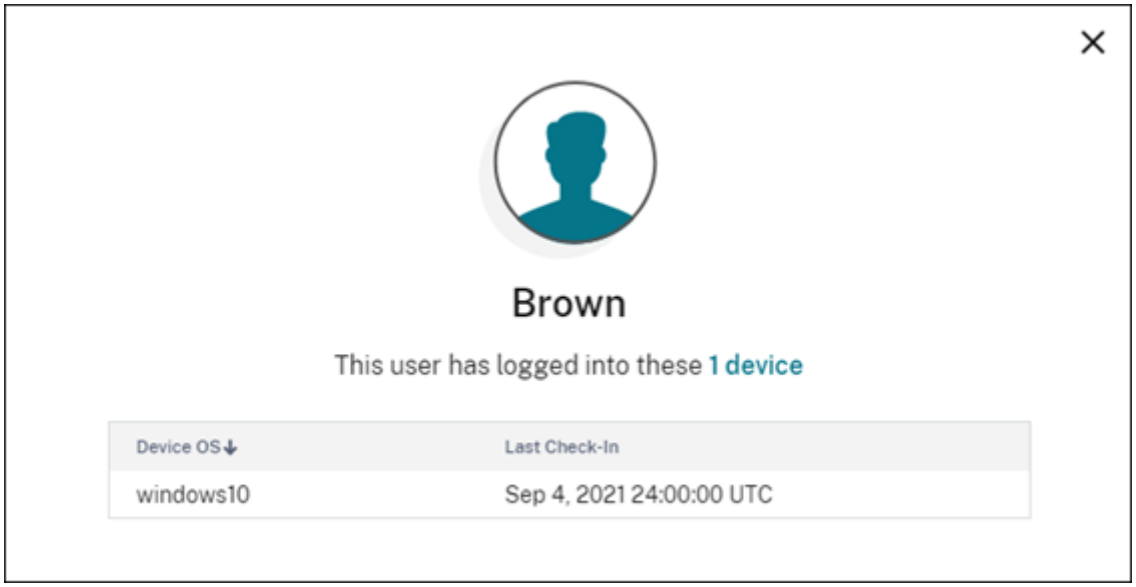


Ver los dispositivos inscritos

Para ver la cantidad de dispositivos inscritos para un usuario específico, haga clic en el enlace de la columna de **dispositivos** .



Citrix Cloud muestra una lista de los dispositivos inscritos del usuario y la fecha de la última comprobación de cada dispositivo.



Liberar automáticamente licencias asignadas

Citrix Cloud libera automáticamente licencias para los usuarios que cumplan **todas** estas condiciones durante los últimos 30 días:

- El usuario no ha inscrito ningún dispositivo nuevo.
- El usuario tiene un dispositivo existente que no se ha registrado en Citrix Cloud.

No se requiere ninguna otra acción para liberar las licencias aptas.

Una vez que se hayan publicado las licencias aptas, los usuarios pueden adquirir otra licencia mediante la inscripción de un dispositivo.

Supervisar el uso de ancho de banda de Gateway Service

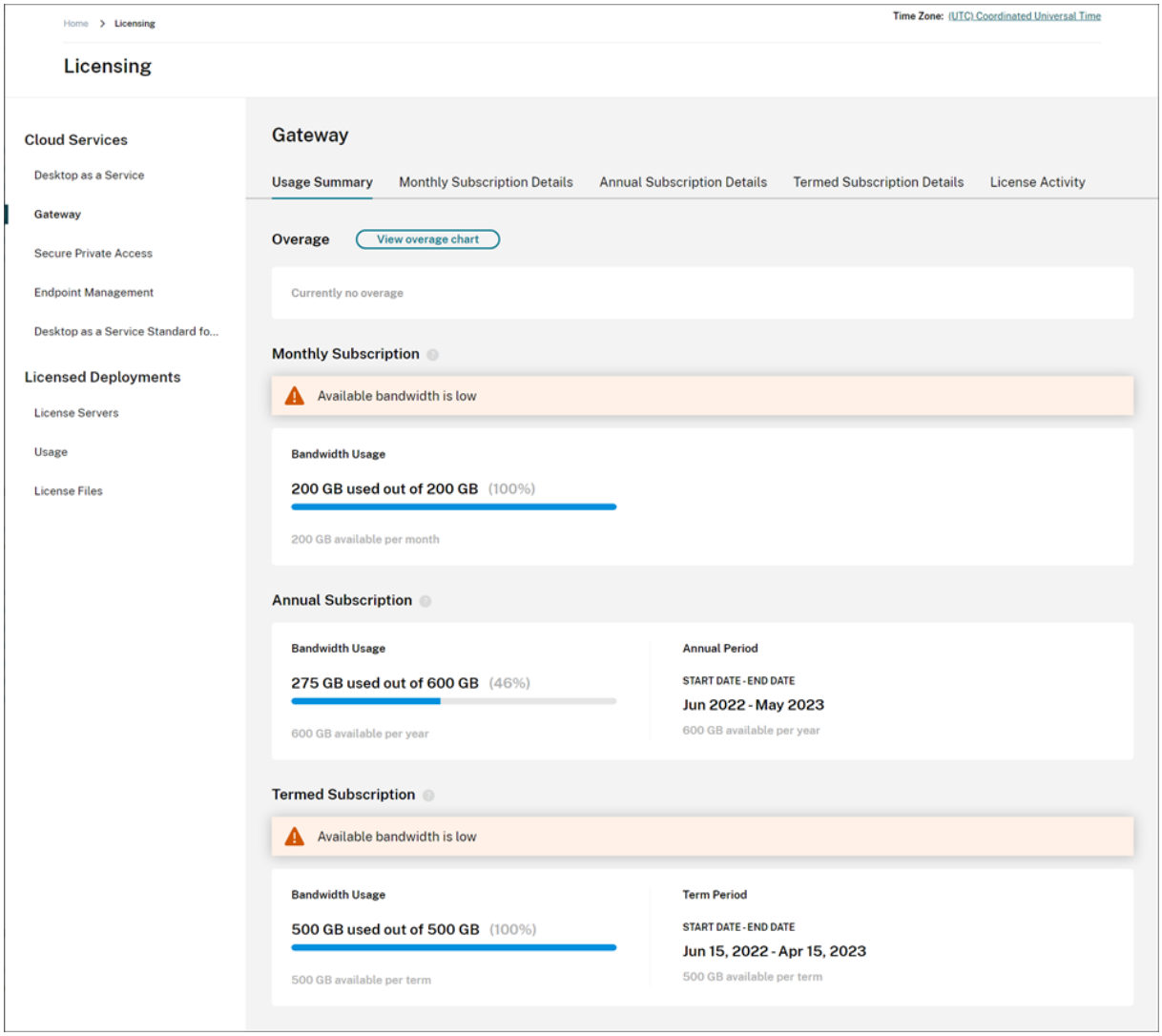
October 2, 2023

En este artículo se describe el uso del ancho de banda a través de Gateway Service cuando se usa con Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service) y Citrix Workspace. El consumo de ancho de banda de Gateway Service incluido con Virtual Apps Essentials Service no se muestra en la página **Licencias** de la consola de administración de Citrix Cloud.

> **Nota:**
>
> Las licencias para Gateway Service le ayudan a comprender el uso del ancho de banda en relación con el uso de aplicaciones y escritorios virtuales. Citrix no aplica asignaciones de uso de ancho de banda en su entorno. Si hay un exceso en la asignación de ancho de banda, Citrix no interfiere con cargas de trabajo de producción ni con el funcionamiento del servicio. Si Citrix cambia la forma en que se aplican las directivas para Gateway Service y el uso del ancho de banda, Citrix se lo notificará antes de que se apliquen estos cambios.

Resumen de uso

El resumen de uso proporciona un resumen visual del uso del ancho de banda para cada suscripción de Gateway Service y del excedente total de todas sus suscripciones (mensual, anual y de plazos estipulados).



Citrix Cloud muestra el ancho de banda total y el ancho de banda consumido para cada tipo de suscripción.

Según el tipo de suscripción, Citrix Cloud también muestra el período de facturación de la suscripción:

- Suscripciones mensuales: Citrix Cloud no muestra el período de facturación actual. Para estas suscripciones, el período de facturación comienza el primer día de cada mes y finaliza el último día de ese mes.
- Suscripciones anuales: Citrix Cloud muestra las fechas de inicio y finalización del período de facturación. Para estas suscripciones, el período de facturación es de un año.
- Suscripciones con plazos estipulados: Citrix Cloud muestra las fechas de inicio y finalización del período de facturación. Para estas suscripciones, el período de facturación es el período para el que se compró la suscripción. Por ejemplo, si se compra una suscripción con un plazo estipulado de tres años, las fechas de inicio y finalización del período de facturación corresponden

a ese intervalo de tres años.

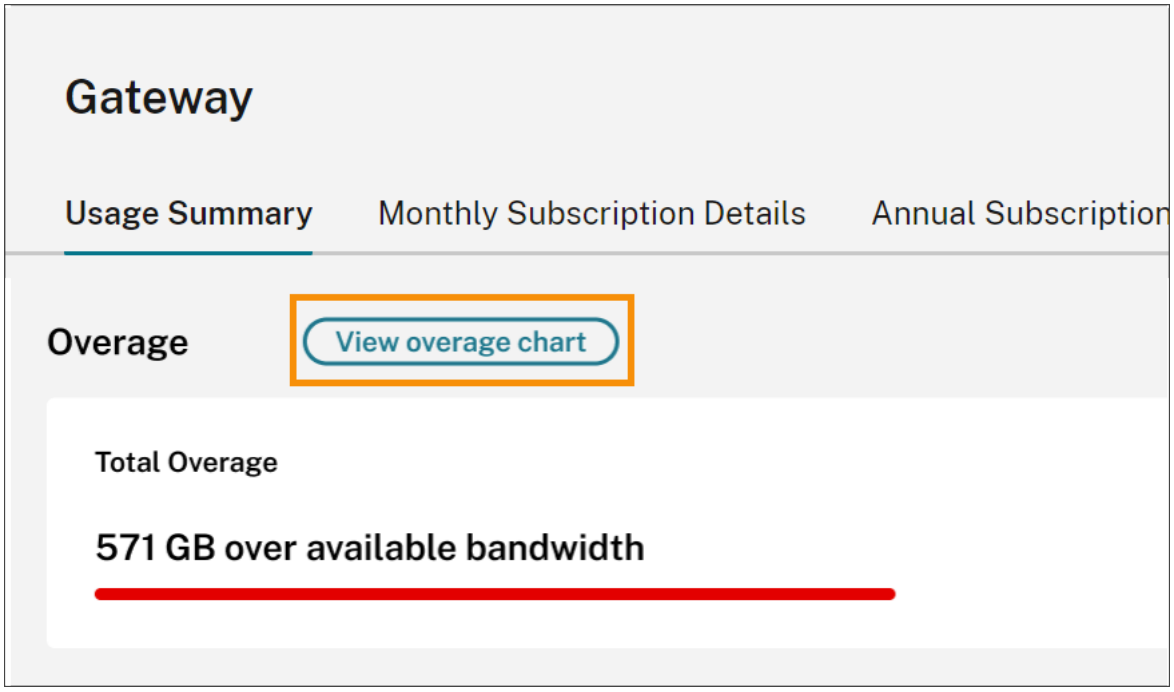
Si una suscripción caduca en 90 días, aparecerá un mensaje de advertencia para dicha suscripción.

Excedente

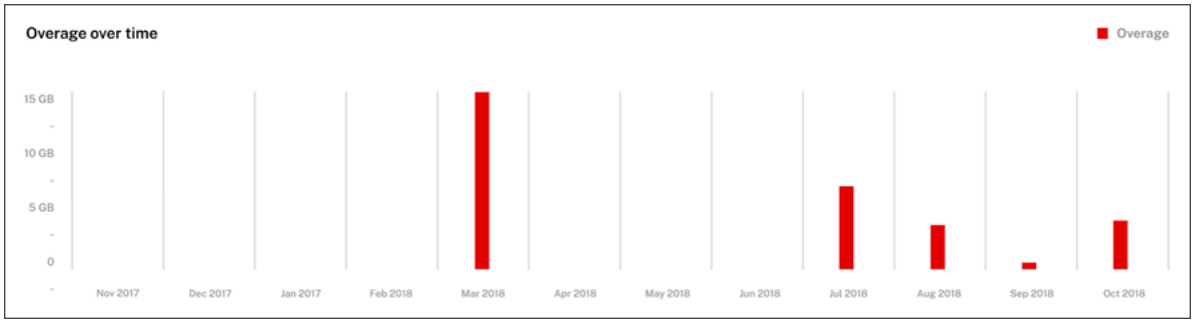
Citrix Cloud calcula el excedente mensual en todas sus suscripciones. Si consume más ancho de banda del que compró, Citrix Cloud muestra el exceso de ancho de banda como excedente.

Si tiene varias suscripciones, Citrix Cloud compara primero el uso del ancho de banda con la suscripción que tiene la fecha de finalización más temprana. Si agota la asignación de ancho de banda de esa suscripción, Citrix Cloud compara el uso del ancho de banda con la suscripción que tiene la fecha de finalización más temprana. Si agota la asignación de ancho de banda en todas sus suscripciones, Citrix Cloud muestra el exceso de uso como excedente.

La página Resumen de uso muestra el excedente total del mes actual. Para ver el excedente a lo largo del tiempo, seleccione **Ver gráfico de excedente**.



Citrix Cloud muestra un gráfico del excedente total de los últimos 12 meses.



El excedente del mes actual no se transfiere al mes siguiente. Cuando comience el mes siguiente, el excedente total se restablece.

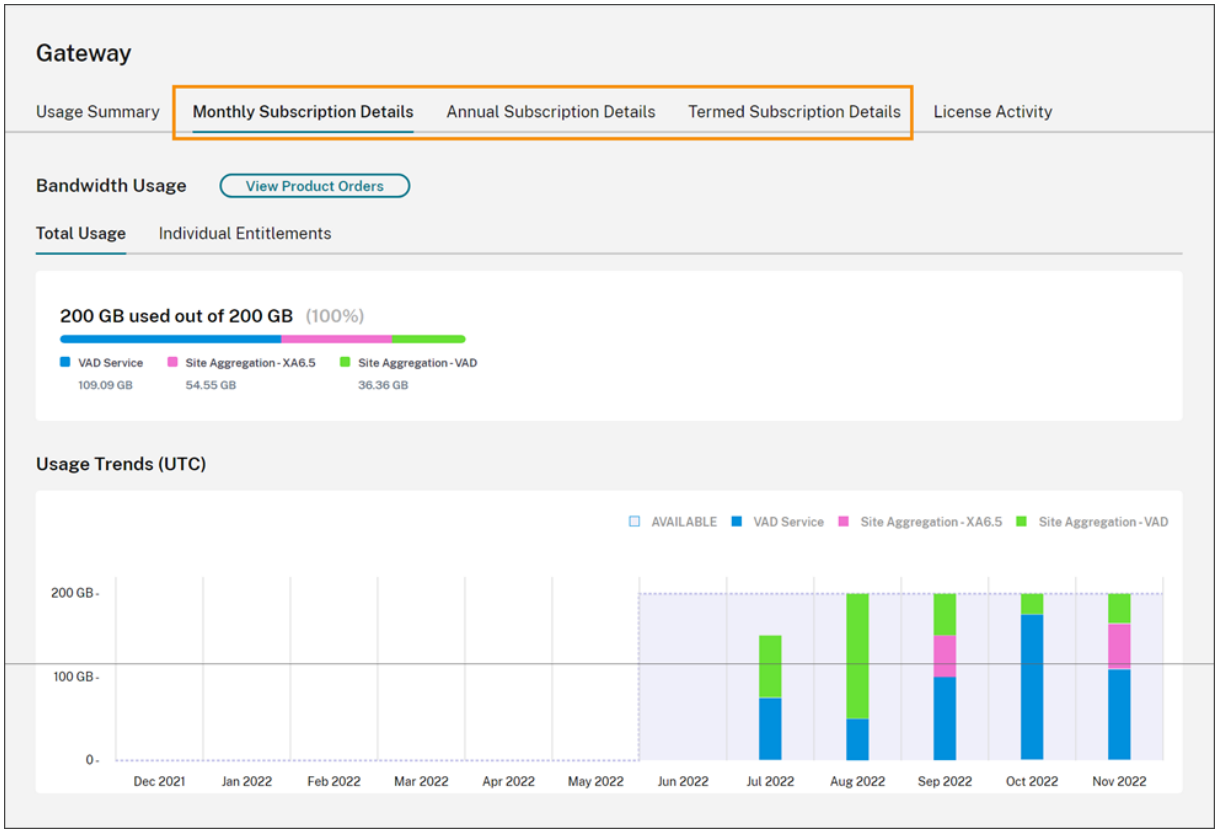
Ancho de banda no utilizado

Citrix Cloud restablece automáticamente el uso del ancho de banda de una suscripción en el siguiente período de facturación. Si no utiliza todo el ancho de banda durante un período de suscripción determinado, Citrix Cloud no transferirá el ancho de banda no utilizado al siguiente período de facturación.

Por ejemplo, si su suscripción mensual incluye 150 GB de ancho de banda total y utiliza 100 GB de ancho de banda en un mes determinado, Citrix Cloud restablece el uso y muestra 150 GB como el ancho de banda total al empezar el mes siguiente. El ancho de banda no utilizado no se agrega a su asignación total de ancho de banda.

Detalles de uso

Para ver en detalle sus suscripciones, seleccione las fichas con detalles mensuales, anuales o plazos estipulados de la suscripción que hay en la parte superior de la consola.



Para cada tipo de suscripción, la ficha Detalles muestra esta información:

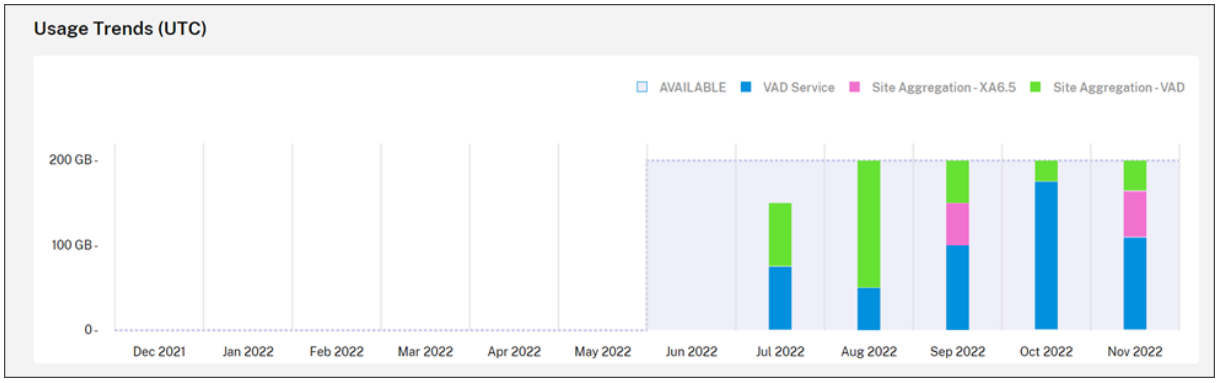
- **Uso total:** El ancho de banda consumido con respecto al ancho de banda total disponible en todas las suscripciones de un tipo determinado. Para las suscripciones mensuales, se muestra el uso total del mes actual. Para las suscripciones anuales y con plazos estipulados, el uso total se acumula de todas las suscripciones anuales o con plazos estipulados.
- **Derechos individuales:** El ancho de banda total consumido por cada suscripción de un tipo determinado. Por ejemplo, si tiene varias suscripciones anuales, esta ficha muestra un desglose del uso de cada suscripción anual por separado.

El ancho de banda consumido se desglosa en función del acceso a través de Citrix DaaS (**VAD Service**) o mediante la implementación de Virtual Apps and Desktops local mediante la agregación de sitios en Citrix Workspace.

Tendencias de uso

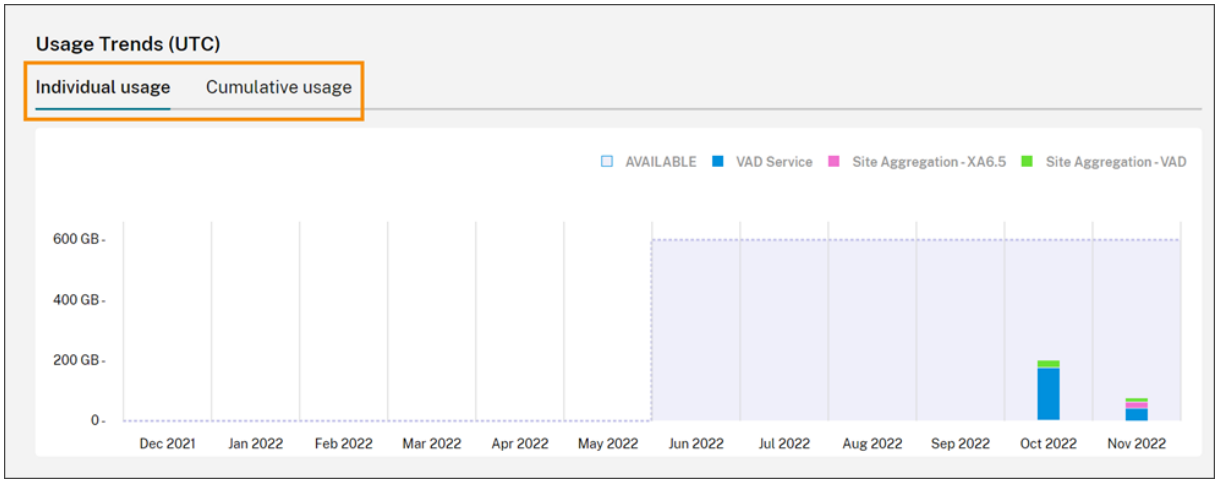
La sección **Tendencias de uso** muestra un desglose del uso de los últimos 12 meses.

Para las suscripciones mensuales, el uso se muestra para cada mes en que tuvo lugar.

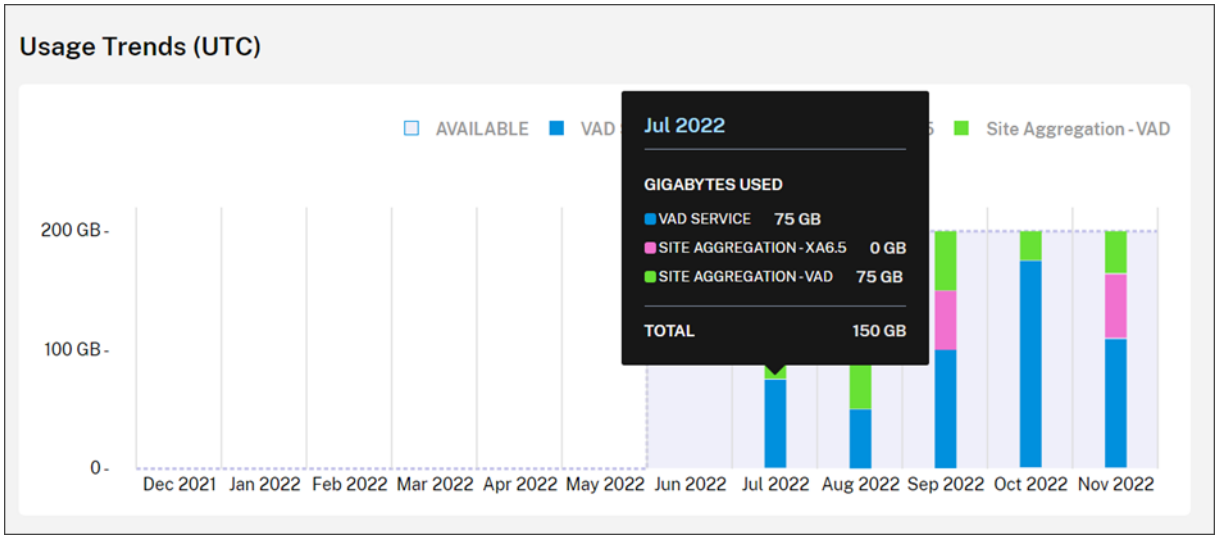


Para las suscripciones anuales y con plazos estipulados, esta sección incluye estas vistas:

- **Uso individual:** El uso del ancho de banda de cada mes del período de facturación actual.
- **Uso acumulado:** El uso del ancho de banda acumulado de cada mes del período de facturación actual.



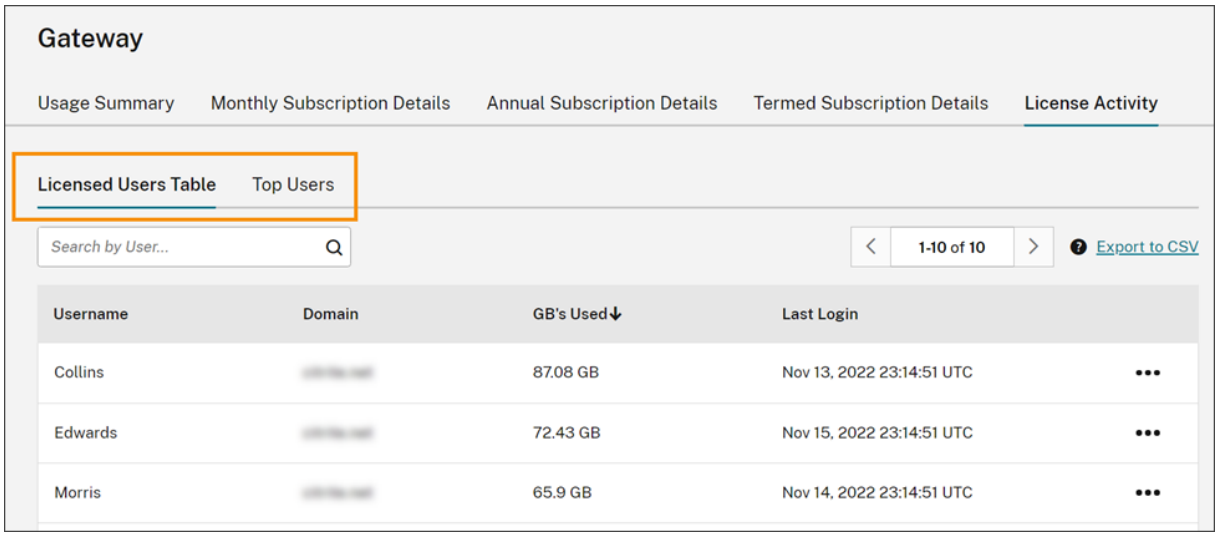
Para todos los tipos de suscripciones, al señalar las barras del gráfico de tendencias de uso, se muestra el uso del ancho de banda en ese momento, desglosado por acceso.



Actividad de licencias

La sección **Actividad de licencias** ofrece vistas con esta información:

- **Usuarios con licencia:** Muestra una lista de los usuarios individuales que tienen licencias asignadas. Esta lista incluye el dominio al que pertenece cada usuario, el ancho de banda utilizado durante los últimos 30 días y la fecha en que el usuario utilizó por última vez un servicio que requería un uso del ancho de banda.
- **Usuarios destacados**: Muestra una lista de los 10 usuarios que más ancho de banda han consumido. Esta lista incluye un desglose del uso de cada usuario durante los últimos 30 días según el tipo de acceso (Citrix DaaS o Virtual Apps and Desktops local mediante la agregación de sitios).

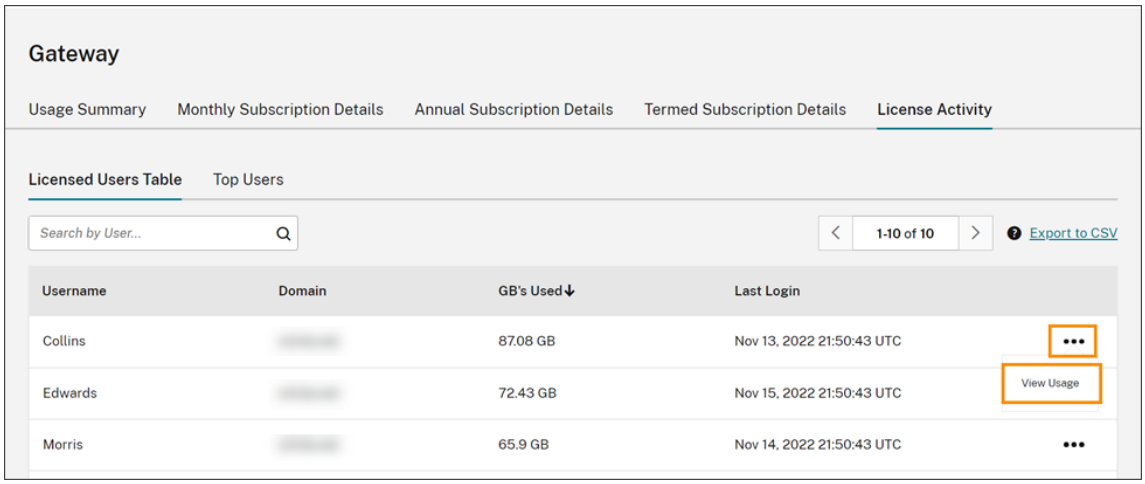


Citrix Cloud muestra el uso del ancho de banda de los últimos 30 días para un usuario determinado

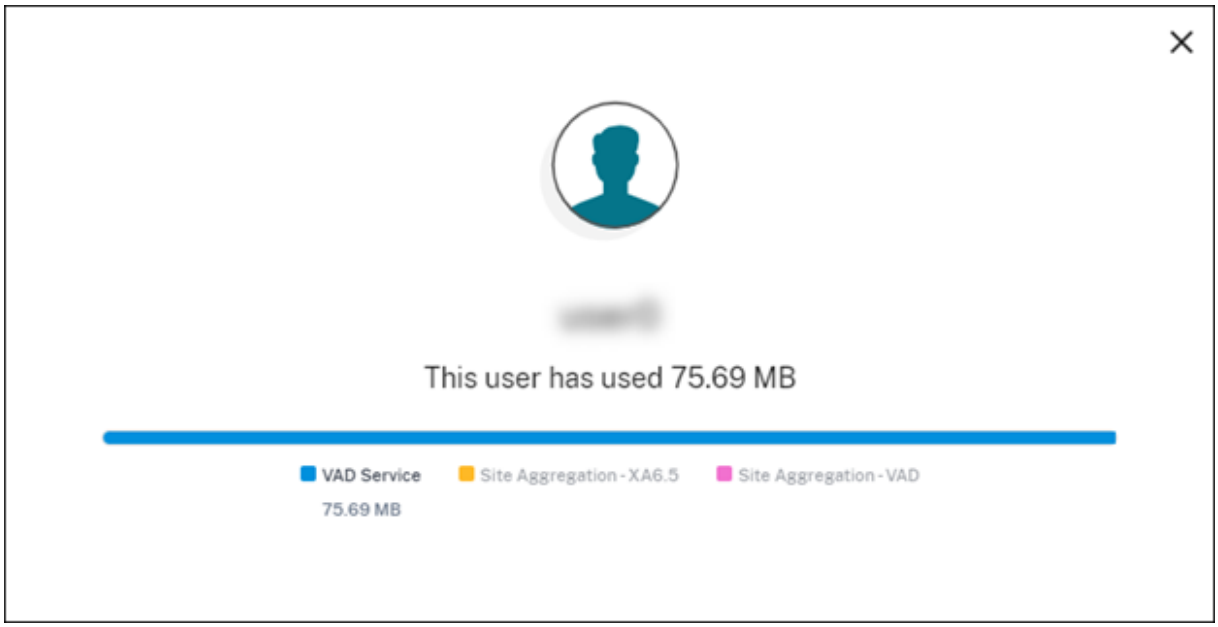
aunque ya no emplee licencias. Cuando caduca una suscripción a Gateway Service, Citrix Cloud sigue mostrando el ancho de banda que los usuarios individuales consumieron en el período de 30 días.

Consultar los detalles de uso de un usuario específico

1. Seleccione **Tabla de usuarios con licencia** y, en la lista, busque el usuario que quiere ver.
2. Seleccione **Ver uso** en el menú de puntos suspensivos del extremo derecho de la página.

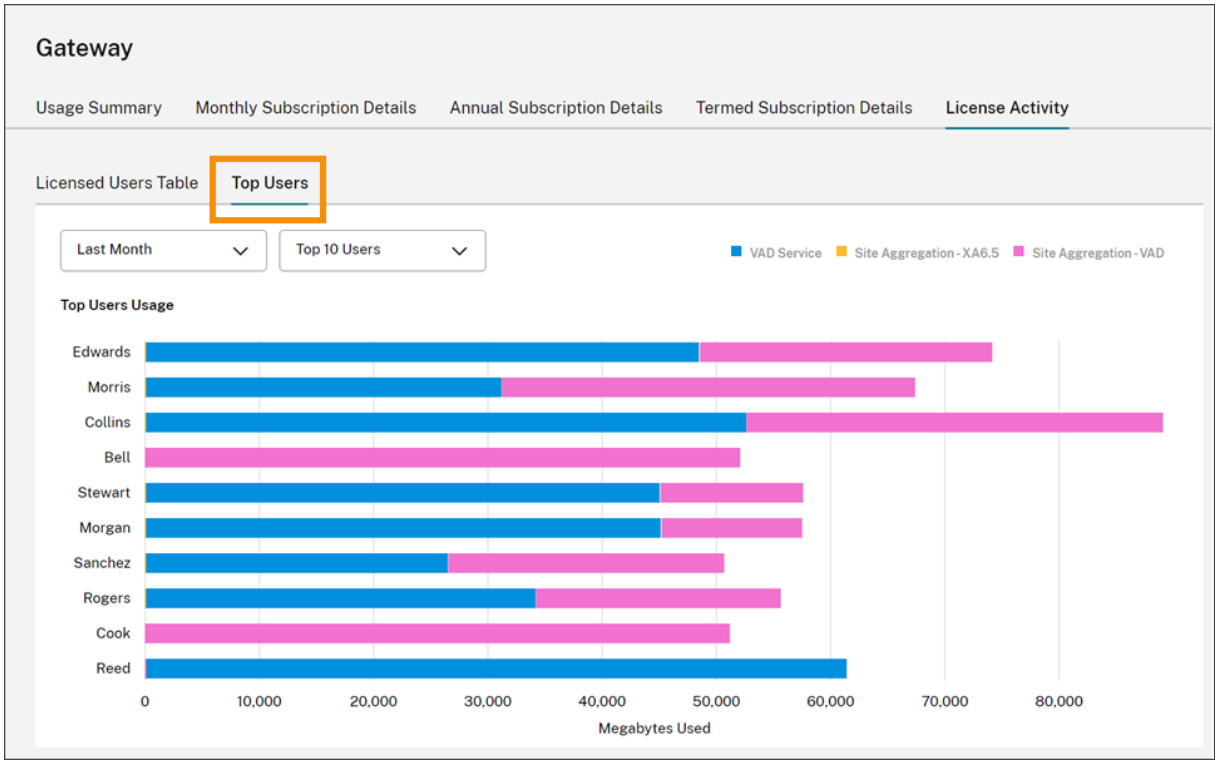


Citrix Cloud muestra el ancho de banda del usuario desglosado por acceso.



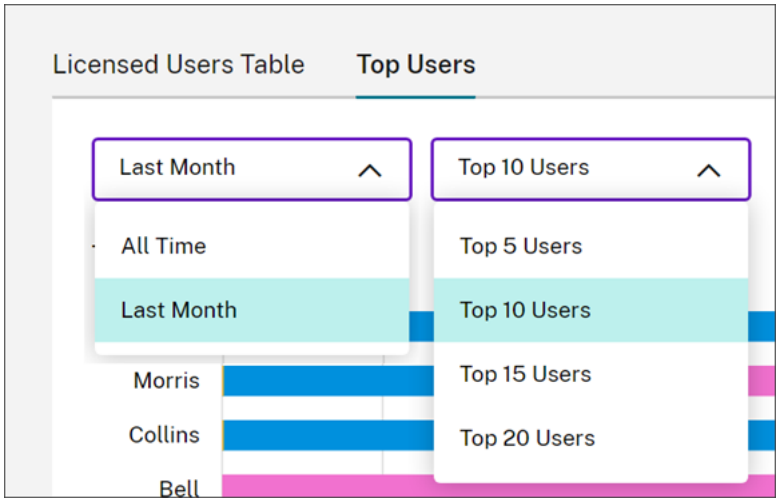
Consultar los detalles de uso de usuarios destacados

Seleccione **Usuarios destacados**.



Citrix Cloud muestra un gráfico del uso del ancho de banda de los usuarios destacados, desglosado por acceso.

De forma predeterminada, el gráfico de **Usuarios destacados** muestra los 10 usuarios que han utilizado más ancho de banda durante los últimos 30 días. Puede cambiar esta vista para mostrar los 5, los 15 o los 20 usuarios destacados. También puede cambiar la duración a **Todo el tiempo**, que muestra los usuarios destacados a lo largo de la vigencia de la suscripción. Para cambiar esta vista, seleccione una opción de cada menú.



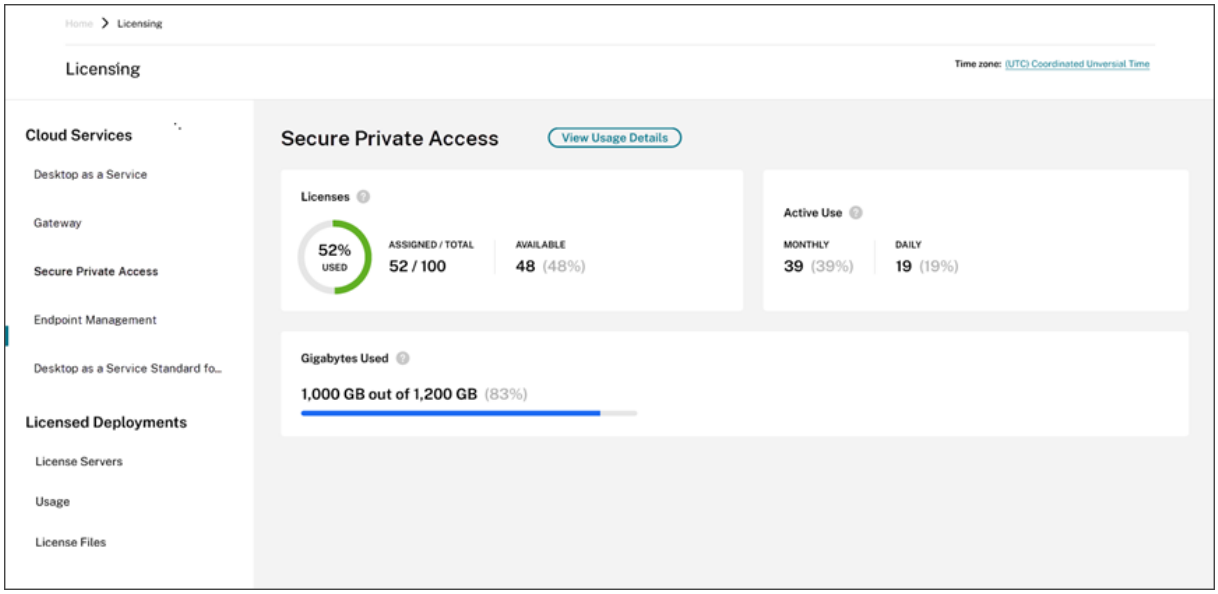
Supervisar licencias y el uso de Secure Private Access

November 27, 2023

Asignación de licencias

Se asigna una licencia cuando un usuario único inicia aplicaciones web y SaaS o aplicaciones TCP y UDP por primera vez.

Resumen de las licencias



El resumen de las licencias muestra esta información:

- Porcentaje de licencias asignadas respecto al total de licencias adquiridas.
  - El color del porcentaje cambia de verde a amarillo a medida que se aproxima al 100%. Si el porcentaje supera el 100 %, este se vuelve rojo.
- La relación entre las licencias asignadas y las licencias adquiridas, y la cantidad restante de licencias disponibles para su asignación.
- Estadísticas del uso activo diario y mensual:
  - El uso activo mensual se refiere a la cantidad de usuarios únicos que han utilizado el servicio en los últimos 30 días.
  - El uso activo diario se refiere a la cantidad de usuarios únicos que han utilizado el servicio en las últimas 24 horas.

- La cantidad de ancho de banda consumida con respecto a la cantidad total de ancho de banda de todas las suscripciones.
- El tiempo que queda para que caduque la suscripción al servicio de la nube. Si la suscripción está a punto de caducar en los próximos 90 días, aparece un mensaje de advertencia.

Licencias y ancho de banda utilizados

En las suscripciones de Secure Private Access Advanced, cada usuario tiene acceso a 5 GB de ancho de banda al mes (60 GB por usuario al año). En las suscripciones de Secure Private Access Standard, cada usuario tiene acceso a 1 GB de ancho de banda al mes (12 GB por usuario al año). Este ancho de banda se agrega para la cantidad total de licencias y durante el período de suscripción.

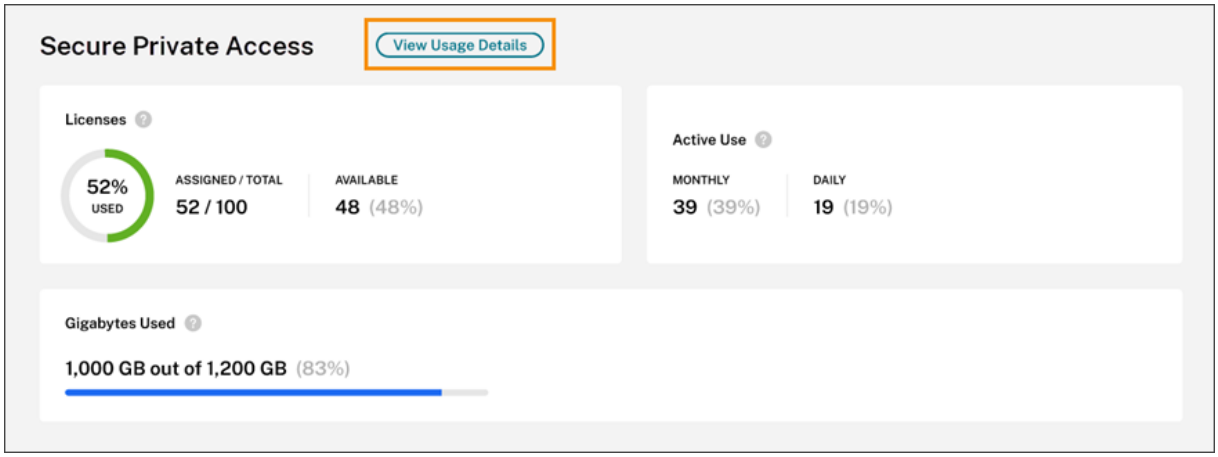
Por ejemplo, si adquiere 100 licencias durante tres años, tendrá 18 000 GB de ancho de banda en total (6000 GB al año durante tres años). Este ancho de banda se reparte entre todos los usuarios con licencia durante el período de 3 años. Si compra más suscripciones, Citrix Cloud muestra el número total de licencias y el ancho de banda para todas las suscripciones.

Si no utiliza la cantidad total de ancho de banda durante el período de suscripción, Citrix Cloud no transfiere el ancho de banda no utilizado al renovar. Cuando use más ancho de banda del que adquirió al caducar la suscripción, la cantidad de ancho de banda disponible permanece en cero cuando renueve la suscripción.

Para diferentes suscripciones con plazos superpuestos, la cantidad de ancho de banda asociada a cada suscripción se elimina de Licencias cuando caduca dicha suscripción. Por ejemplo, si adquirió dos suscripciones, Citrix Cloud muestra el total de licencias y el ancho de banda total de ambas suscripciones. Cuando la primera suscripción caduca, Citrix Cloud muestra solo el ancho de banda asociado a la suscripción no caducada.

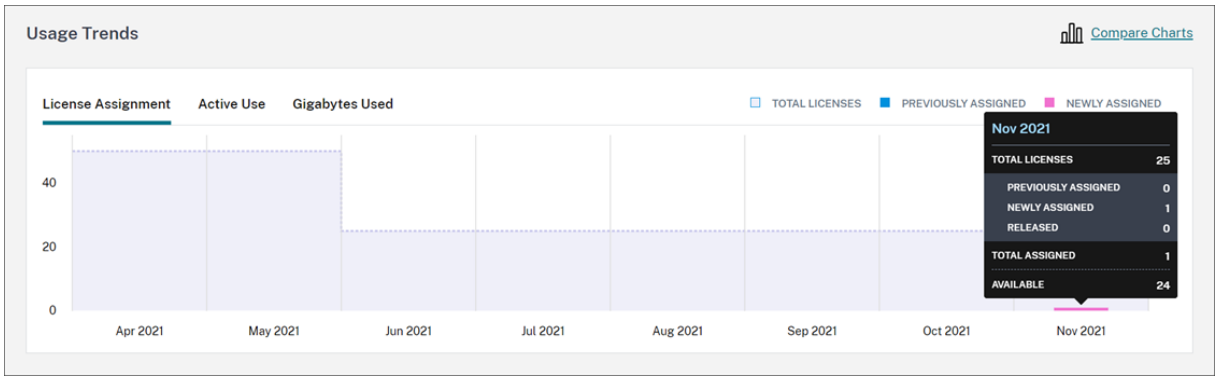
Tendencias de uso

Para obtener una vista detallada del uso de su banda ancha y de sus licencias, haga clic en **Ver detalles de uso**.



Citrix Cloud muestra un desglose del consumo de ancho de banda en función del tipo de aplicaciones a las que tienen acceso los usuarios.

También verá un desglose de las tendencias de uso y los usuarios individuales que utilizan ancho de banda y licencias de servicios de la nube.



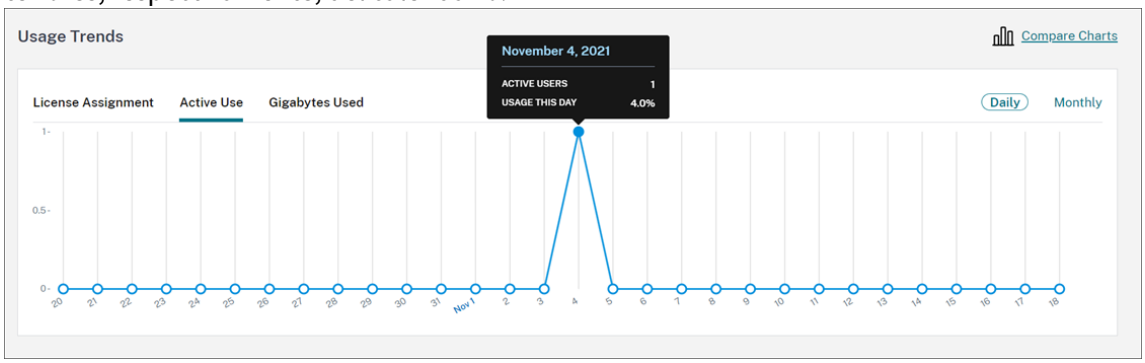
Este desglose, en **Tendencias de uso**, muestra la siguiente información:

- En la ficha **Asignación de licencias**:
  - **Total de licencias:** La cantidad total de licencias que ha comprado del servicio de la nube para todos los derechos incluidos.
  - **Asignadas previamente:** Las licencias del servicio Cloud que ya estaban asignadas al principio de cada mes. Por ejemplo, si a un usuario se le asigna una licencia en julio, Citrix Cloud cuenta esa asignación en la cantidad de "Asignadas previamente"en el mes de

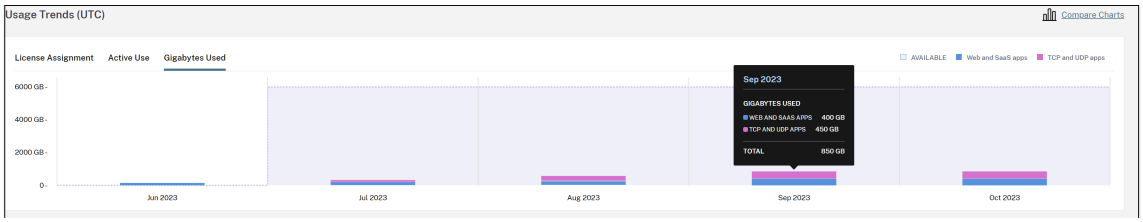
agosto.

- **Asignadas recientemente:** La cantidad de licencias que se asignaron cada mes. Por ejemplo, cuando accede al servicio de la nube por primera vez en julio y se le asigna una licencia. Citrix Cloud cuenta esa licencia en la cantidad de Asignadas recientemente de julio.

- En la ficha **Uso activo**: Tendencias del uso activo diario y mensual durante el mes y el año anteriores, respectivamente, del calendario.



- En la ficha **Gigabytes utilizados**: La cantidad de ancho de banda consumida con respecto al ancho de banda total disponible. Muestra información sobre el uso por usuario y por aplicación, como aplicaciones web y SaaS y aplicaciones TCP y UDP.

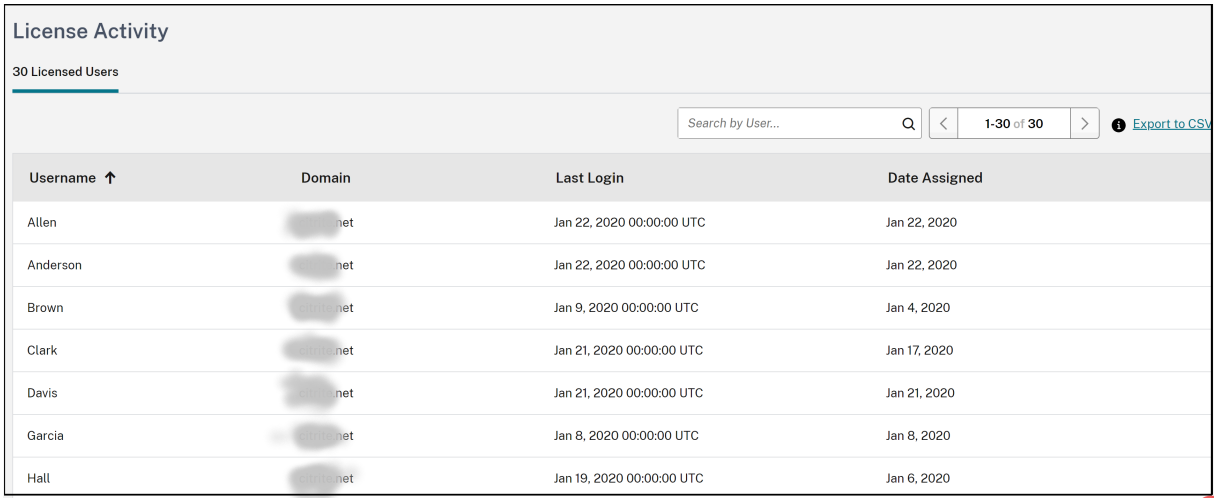


Para comparar las tendencias de asignación de licencias, uso activo y uso de ancho de banda, seleccione **Comparar gráficos**.

> **Nota:**
>
> Las tendencias de uso se acumulan durante el período de suscripción actual. Al renovar la suscripción, las tendencias de uso se restablecen al principio del nuevo período de suscripción.

Actividad de licencias

La sección **Actividad de licencias** también muestra la siguiente información:



- Una lista de los usuarios individuales que tienen licencias asignadas.
- El dominio al que pertenece el usuario.
- La fecha en que el usuario usó el servicio por última vez.
- La fecha en que se asignó una licencia al usuario.

Liberar licencias asignadas

Citrix Cloud libera automáticamente licencias si no ha utilizado el servicio en los últimos 30 días. No se necesita intervención del administrador de Citrix para liberar las licencias.

Cuando se libera una licencia, la cantidad de licencias restantes aumenta y el número de licencias asignadas disminuye en consecuencia. Una vez liberada la licencia, puede adquirir otra; solo debe iniciar sesión y utilizar el servicio de la nube.

Supervisar el consumo de recursos de Azure administrado por Citrix para Citrix DaaS

October 2, 2023

Cuando adquiere derechos para usar Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service), también puede adquirir fondos de consumo de Azure para Citrix que le permiten usar recursos en una suscripción de Azure administrado por Citrix. Puede usar estos recursos para entregar aplicaciones y escritorios a sus usuarios junto con los VDA locales.

Al adquirir fondos de consumo de Azure para Citrix, puede pagar el consumo mediante uno de estos métodos:

- Pago por uso: Para los recursos de Azure administrado por Citrix que utilice durante un mes determinado, Citrix se los factura durante el mes siguiente. Citrix Cloud muestra su uso como excedente.
- Consumo prepagado: Puede pagar por adelantado el consumo de forma mensual o anual (plazo estipulado). Para cualquier uso que supere el consumo prepagado, Citrix Cloud lo muestra como excedente. Para cualquier excedente en un mes determinado, Citrix se lo facturará durante el mes siguiente.

Cada unidad de consumo tiene un valor de 1,00 USD. La consola de licencias de Citrix Cloud le ayuda a realizar un seguimiento de las unidades que utiliza.

Para estimar los costes de consumo, use la calculadora de consumo de Azure administrado de Citrix. Para estimar los costes de consumo y licencias de Citrix DaaS Standard para Azure (antes denominado Citrix Virtual Apps and Desktops Standard para Azure), use la calculadora de licencias y consumo.

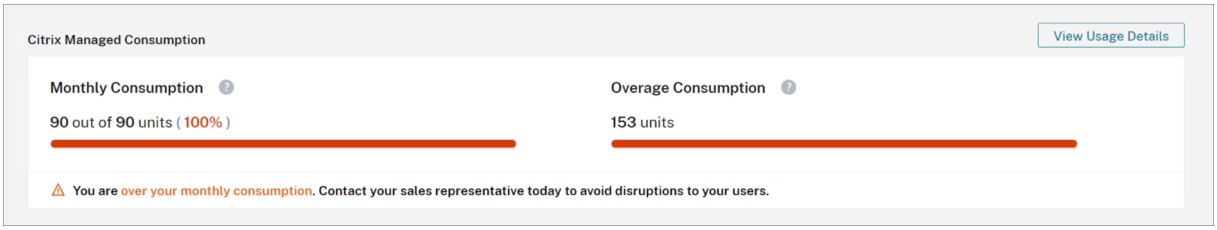
Productos compatibles

La supervisión del consumo está disponible para estas ediciones de Citrix DaaS:

- Citrix DaaS Advanced (antes denominado Virtual Apps Advanced)
- Citrix DaaS Premium (antes denominado Virtual Apps Premium)
- Citrix DaaS Advanced Plus (antes denominado Virtual Apps and Desktops Advanced)
- Citrix DaaS Premium (antes denominado Virtual Apps and Desktops Premium)
- Citrix DaaS Standard para Azure (antes denominado Virtual Apps and Desktops Standard para Azure)

Resumen del consumo

La sección Consumo administrado por Citrix muestra un resumen de las unidades utilizadas en sus fondos de consumo.



Consumo mensual muestra la cantidad de unidades de consumo utilizadas para el mes actual con respecto a la cantidad total de unidades de los fondos de consumo mensuales que adquirió. El consumo mensual se restablece cada mes. Las unidades de consumo no utilizadas no se transfieren al mes siguiente.

Consumo por plazos muestra la cantidad de unidades de consumo utilizadas con respecto a la cantidad total de unidades de los fondos de consumo por plazos que adquirió. Al igual que con las unidades de consumo mensual, las unidades de consumo por plazos no utilizadas no se trasladan al año siguiente.

Consumo excedente muestra la cantidad de unidades de consumo utilizadas más allá de la cantidad de unidades de sus fondos de consumo de Azure. Si utiliza recursos de Azure administrado por Citrix en forma de pago por uso, su consumo aparece como excedente de forma predeterminada.

Cómo se mide el excedente

Si usa fondos de consumo de Azure en forma de pago por uso, Citrix Cloud muestra la cantidad de unidades de consumo utilizadas durante el mes actual como excedente.

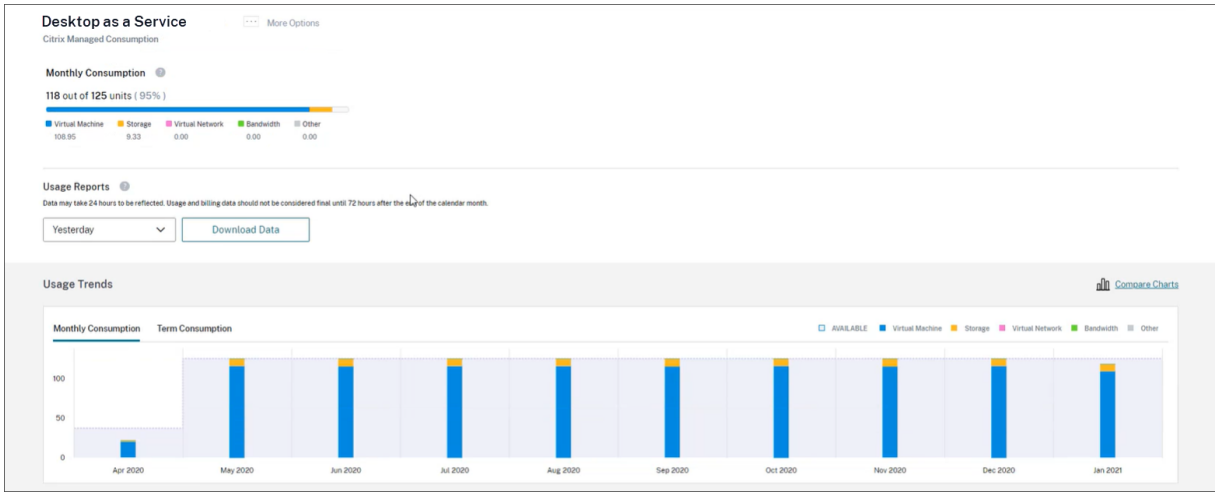
Si pagó por adelantado el consumo de forma mensual o anual, Citrix Cloud muestra la cantidad de unidades de consumo mensual o por plazos que utilizó para el mes o el año actuales. Si consume más unidades de las que adquirió, Citrix Cloud muestra las unidades sobrantes como excedente.

Si pagó por adelantado el consumo de forma mensual y anual, Citrix Cloud mide primero su consumo en relación con las unidades mensuales adquiridas. Una vez consumidas esas unidades, Citrix Cloud mide el consumo en relación con las unidades anuales. Una vez consumidas esas unidades, Citrix Cloud muestra cualquier las unidades sobrantes que haya consumido como excedente.

Si adquiere unidades de consumo adicionales y su cuenta tiene un excedente existente, las nuevas unidades de consumo no se aplicarán al excedente. Las nuevas unidades de consumo solo se aplican al uso que se produce después de adquirir esas unidades.

Detalles de consumo

Para obtener una vista detallada de sus unidades de consumo, haga clic en **Ver detalles de uso** en el extremo derecho del resumen. La página de detalles muestra un desglose de sus tendencias de consumo y uso.



Informes de uso

Puede descargar la información de uso como un archivo CSV durante un intervalo específico. Haga clic en **Descargar datos** para generar y descargar un archivo CSV en su máquina local.

Los datos pueden tardar hasta 72 horas después del final de un día o mes en reflejar todo el uso.

El archivo CSV incluye las siguientes secciones:

- Resumen del informe que muestra las unidades de consumo disponibles antes y después del intervalo de fechas del informe, los cargos totales por uso y el excedente pendiente.

Data may take 24 hours to be reflected. Usage and billing data should not be considered final until 72 hours after the end of the calendar month.			
Org ID	51938754		
Report Date	12/3/2021		
Date Start	11/1/2021		
Date End	11/30/2021		
Report Summary			
	Credits	Debits	
Monthly Consumption Units Available before 11/01/2021	$0		
Termed Consumption Units Available before 11/01/2021	$0		
Trial Consumption Units Available before 11/01/2021	$0		
Total Usage to Charge		$851.96	
Expired Consumption Commitment		$0.00	
Total	$0.00	$851.96	

Monthly Consumption Units Available after 11/30/2021	$0		
Termed Consumption Units Available after 11/30/2021	$0		
Trial Consumption Units Available after 11/30/2021	$0		
Pending Overage by 11/30/2021	$0.00		

- Resumen diario que muestra el cargo por uso total, los fondos mensuales y por plazos restantes y el cargo por excedente para cada día del intervalo de fechas del informe.

Daily Summary				
Date	Total Usage	Remaining Monthly Funds	Remaining Termed Funds	Overage Amount
11/1/2021	$28.40	$0	$0	$0
11/2/2021	$28.40	$0	$0	$0
11/3/2021	$28.40	$0	$0	$0
11/4/2021	$28.40	$0	$0	$0
11/5/2021	$28.39	$0	$0	$0
11/6/2021	$28.39	$0	$0	$0
11/7/2021	$28.40	$0	$0	$0
11/8/2021	$28.40	$0	$0	$0

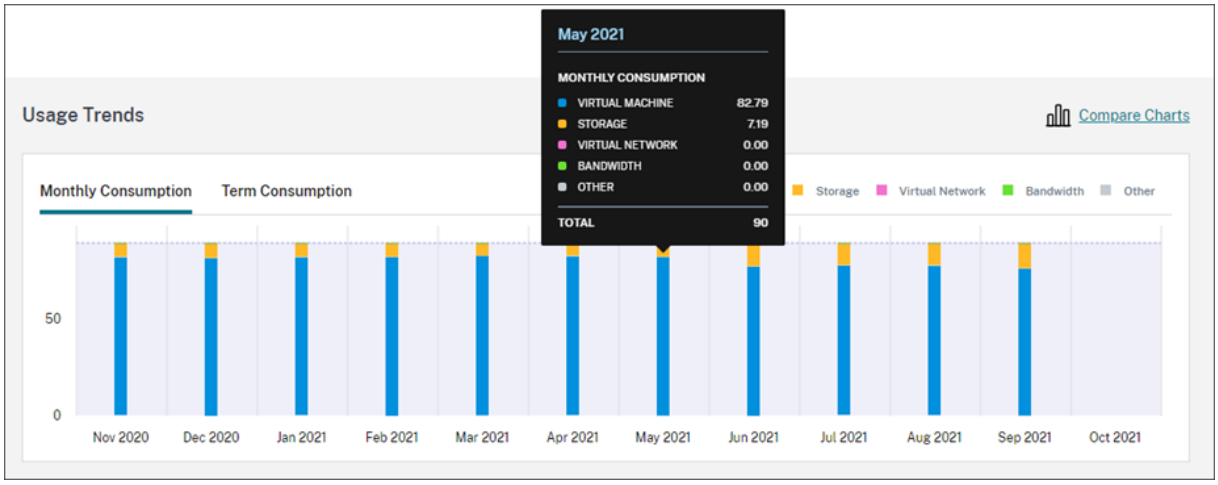
- Uso medido de máquinas virtuales de Azure, conexiones de red, almacenamiento de Azure y ancho de banda para cada día del intervalo de fechas del informe.

Date	Citrix Meter Name	Citrix Meter Description	Catalog Id	Catalog Name	Citrix Meter Region	Citrix Meter Category	Citrix Meter Sub Category	Citrix Meter Unit	Quantity	SRP	Total	Total Charged
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	None	Bandwidth		10 GB	0.0000444	$1.13	$0.00	$0.00
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	None	Bandwidth		10 GB	0.0000018	$1.13	$0.00	$0.00
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		N/A	N/A	None	Bandwidth		10 GB	0.0064263	$1.13	$0.01	$0.01
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		cb7516c0-33e7-485a-9eb0-d84b7f2e9c5a	Windows-11-MultiSession	None	Bandwidth		10 GB	0.0000137	$1.13	$0.00	$0.00
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	None	Bandwidth		10 GB	0.0000015	$1.13	$0.00	$0.00
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	None	Bandwidth		10 GB	0.0000073	$1.13	$0.00	$0.00
11/1/2021	Bandwidth - Data Transfer Out - Zone 1		e86cee4e-1930-4d87-b2e5-3b189bb3e6e3	Win-11-SS-22	None	Bandwidth		10 GB	0.0000334	$1.13	$0.00	$0.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		e86cee4e-1930-4d87-b2e5-3b189bb3e6e3	Win-11-SS-22	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		cb7516c0-33e7-485a-9eb0-d84b7f2e9c5a	Windows-11-MultiSession	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Network Peering - Ingress		N/A	N/A	None	VirtualNetwork		100 GB	0.00016714	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	None	VirtualNetwork		100 GB	0.00000034	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		cb7516c0-33e7-485a-9eb0-d84b7f2e9c5a	Windows-11-MultiSession	None	VirtualNetwork		100 GB	0.00000323	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	None	VirtualNetwork		100 GB	0.00000422	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	None	VirtualNetwork		100 GB	0.00000165	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	None	VirtualNetwork		100 GB	0.00000307	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		e86cee4e-1930-4d87-b2e5-3b189bb3e6e3	Win-11-SS-22	None	VirtualNetwork		100 GB	0.00000129	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		cb7516c0-33e7-485a-9eb0-d84b7f2e9c5a	Windows-11-MultiSession	None	VirtualNetwork		100 GB	0.00000148	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	None	VirtualNetwork		100 GB	0.00000115	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		e86cee4e-1930-4d87-b2e5-3b189bb3e6e3	Win-11-SS-22	None	VirtualNetwork		100 GB	0.00000342	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		N/A	N/A	None	VirtualNetwork		100 GB	0.00012714	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Egress		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	None	VirtualNetwork		100 GB	0.00000121	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	None	VirtualNetwork		100 GB	0.00000323	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering - Ingress		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	None	VirtualNetwork		100 GB	0.00000094	$1.30	$0.00	$0.00
11/1/2021	General Block Blob - Read Operations		N/A	N/A	None	Storage		100000000	0.00000016	$4.68	$0.00	$0.00
11/1/2021	Standard HDD Managed Disks - S10 - Disks - US East		N/A	N/A	US East	Storage		1 /Month	0.400032	$7.64	$3.06	$3.06
11/1/2021	Standard HDD Managed Disks - S10 - Disks - US East		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	US East	Storage		1 /Month	0.033336	$7.64	$0.25	$0.25
11/1/2021	Standard HDD Managed Disks - S10 - Disks - US East		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	US East	Storage		1 /Month	0.100008	$7.64	$0.76	$0.76
11/1/2021	Virtual Machines Av2 Series - A2 v2 - US East		N/A	N/A	US East	VirtualMachine		100 Hours	0.48	$11.83	$5.68	$5.68
11/1/2021	Premium SSD Managed Disks - P10 - Disks - US East		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	US East	Storage		1 /Month	0.033336	$19.22	$0.64	$0.64
11/2/2021	Bandwidth - Data Transfer Out - Zone 1		07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	None	Bandwidth		10 GB	0.0000235	$1.13	$0.00	$0.00

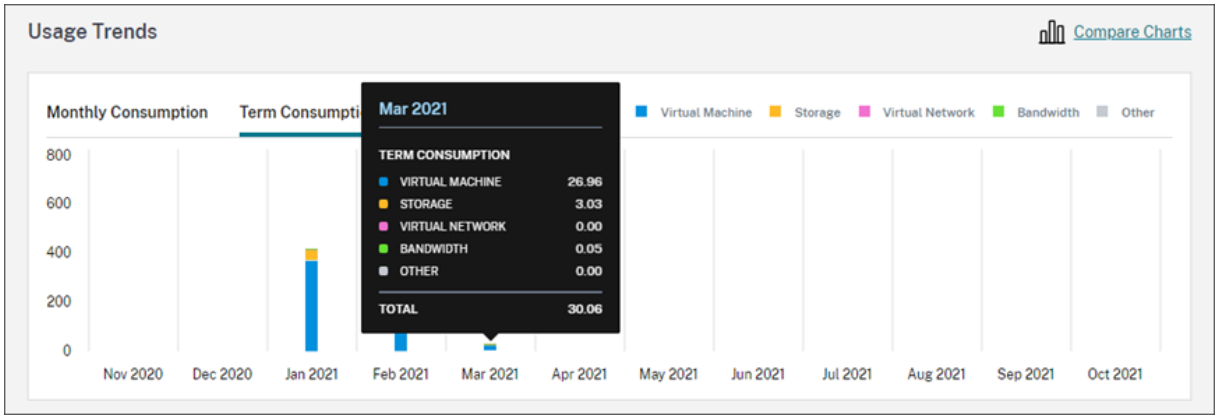
Tendencias de uso y actividad de consumo

La sección **Tendencias de uso** muestra un gráfico de los recursos de Azure administrado por Citrix que haya utilizado. Al señalar una barra del gráfico, se muestra la cantidad de recursos que consumió durante ese mes, incluidas las máquinas virtuales, el almacenamiento, los recursos de red virtual y el ancho de banda.

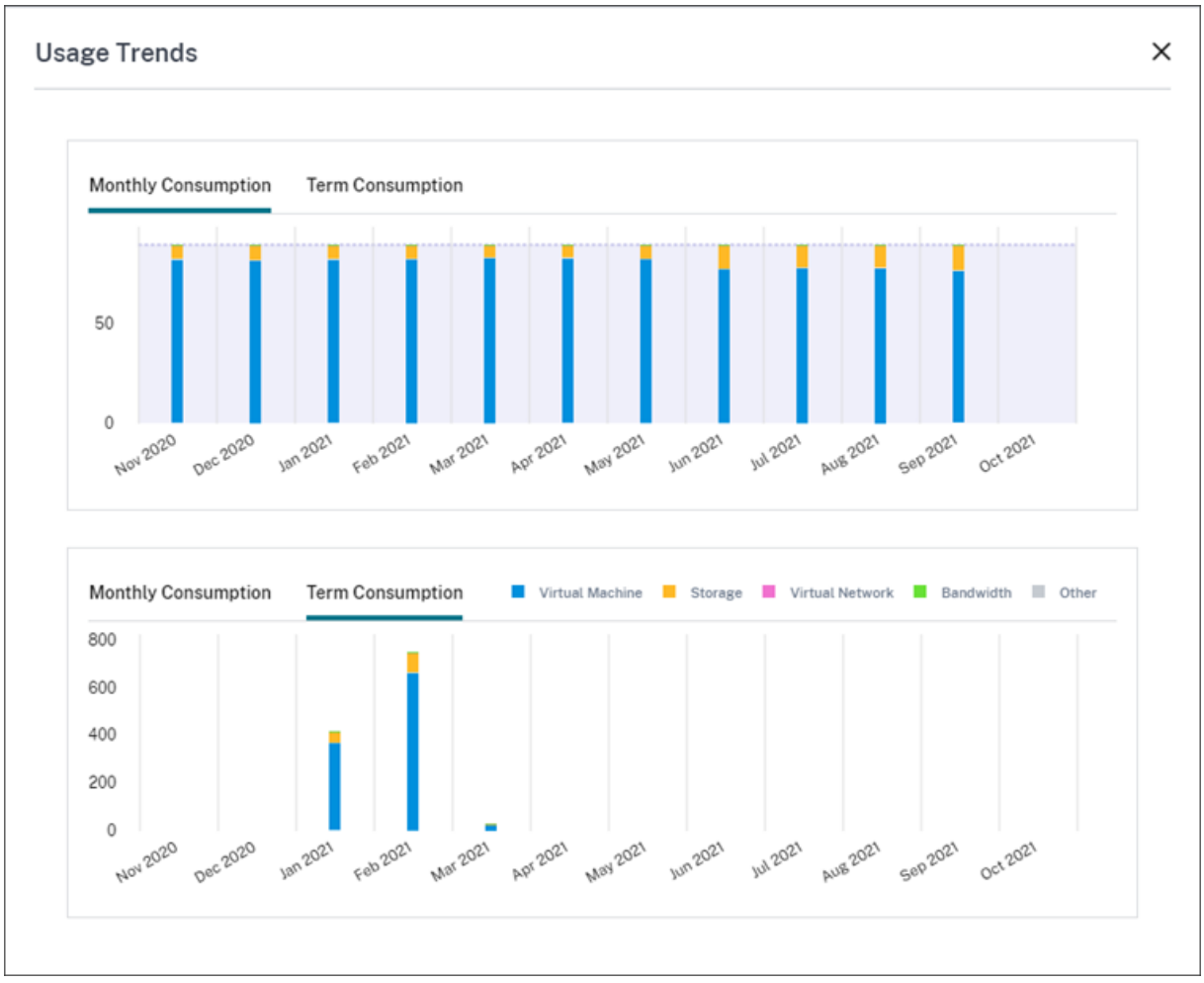
Seleccione **Consumo mensual** para ver su consumo mensual de los 12 meses anteriores.



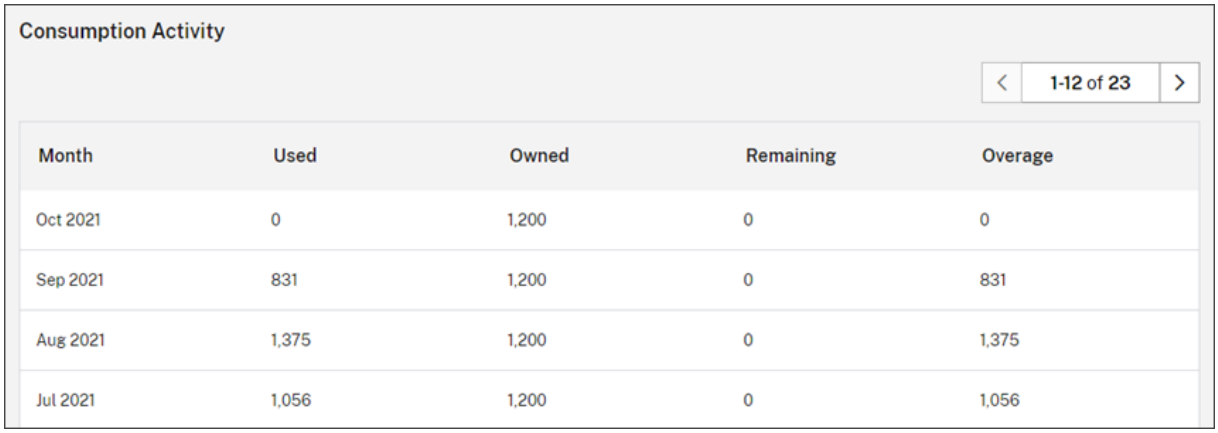
Seleccione **Consumo por plazos** para ver su consumo por plazos de cada mes durante el año anterior.



Si adquirió unidades de consumo mensuales y anuales, seleccione **Comparar gráficos** en el extremo derecho del gráfico para ver las tendencias de consumo mensual y por plazos en una sola vista.



La sección **Actividad de consumo** también muestra una lista de sus unidades de consumo para cada mes.



La actividad de consumo incluye la siguiente información:

- **En uso:** La cantidad de unidades que se usaron de cada mes.
- **En propiedad:** La cantidad total de unidades adquiridas de cada mes.
- **Restante:** La cantidad de unidades adquiridas que no se usaron de cada mes.
- **Excedente:** La cantidad de unidades consumidas que superaron las unidades adquiridas de cada mes.

Liberar licencias asignadas

El momento en que las asignaciones de licencias se pueden liberar depende de las unidades de fondos de consumo que haya adquirido.

Puede liberar licencias inactivas después de 30 días si:

- No usa una suscripción de Azure administrado por Citrix con la implementación de su servicio.
- Adquirió unidades de consumo anuales para usarlas con la implementación de su servicio.

Puede liberar licencias inactivas durante el mes en curso, siempre que ningún usuario ni dispositivo haya iniciado aplicaciones o escritorios, si:

- Adquirió unidades de fondos de consumo mensuales para usarlas con la implementación de su servicio.
- Adquirió unidades de fondos de consumo tanto mensuales como anuales.

Para obtener instrucciones sobre cómo liberar licencias aptas, consulte estos artículos:

- Citrix DaaS (modelo de usuario/dispositivo): Liberar licencias asignadas
- Citrix DaaS Standard para Azure: Liberar licencias asignadas

Supervisar las licencias y el uso de las implementaciones locales

October 2, 2023

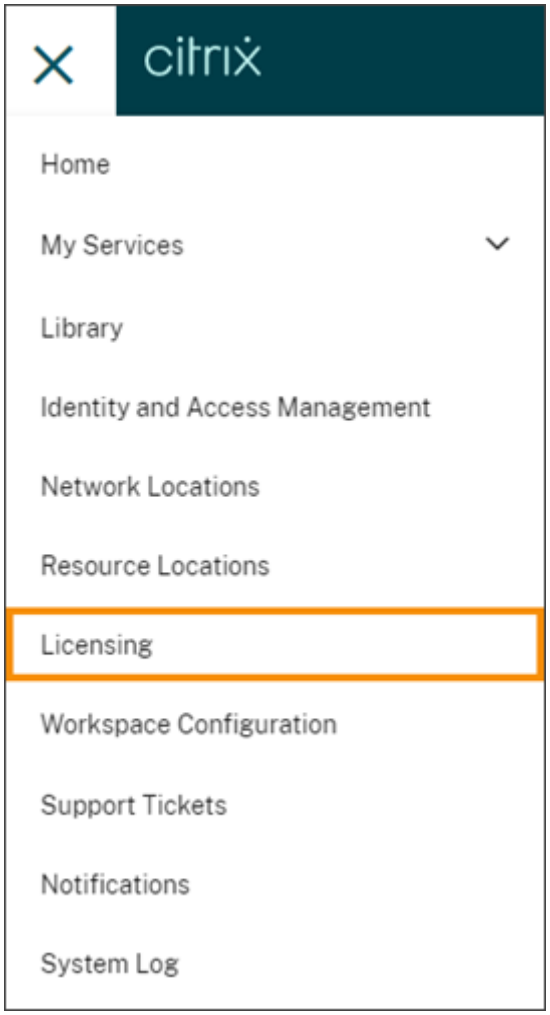
La experiencia de implementaciones con licencia en Citrix Cloud consta de las siguientes funciones:

- Registro de productos: Registre sus servidores de licencias Citrix existentes en Citrix Cloud para obtener informes e información adicional sobre el uso de sus implementaciones.
- Estado del servidor de licencias: Consulte el estado de sus servidores de licencias Citrix para saber cuáles informan correctamente del uso y cuándo notificaron por última vez del uso a Citrix Cloud.
- Información sobre el uso: Consulte cuántas licencias están instaladas y en uso en sus servidores de licencias Citrix y obtenga información sobre las tendencias históricas del uso de licencias.

Productos compatibles

La información sobre el uso del servidor de licencias Citrix está disponible para todas las ediciones de Citrix Virtual Apps and Desktops que tengan los modelos de licencias simultáneas y de usuario/dispositivo.

Para ver información sobre el uso del servidor de licencias de Citrix, seleccione **Licencias** en el menú de la consola y, a continuación, seleccione **Implementaciones con licencia**.



Requisitos previos

Para ver la información sobre el uso del servidor de licencias Citrix, debe disponer de los siguientes elementos:

- Citrix License Server 11.15.0.0 o una versión posterior
- Una cuenta de Citrix Cloud
- Acceso de red desde Citrix License Server a Citrix Cloud

Requisitos de conectividad

Para registrar correctamente su servidor de licencias en Citrix Cloud, asegúrese de que se puede contactar con las siguientes direcciones:

- `https://citrix.cloud.com/` (para acceder a la consola de administración para introducir el código y ver el estado del servidor de licencias)

- https://trust.citrixnetworkapi.net (para obtener un código)
- https://trust.citrixworkspacesapi.net/ (para confirmar que el servidor de licencias está registrado)
- https://cis.citrix.com (para cargar datos)
- https://core-eastus-release-a.citrixworkspacesapi.net
- https://core.citrixworkspacesapi.net
- ocsp.digicert.com port 80
- crl3.digicert.com port 80
- crl4.digicert.com port 80
- ocsp.entrust.net port 80
- crl.entrust.net port 80

Conectarse a Citrix Cloud

Para habilitar la información sobre el uso del servidor de licencias Citrix, realice las siguientes tareas:

1. Habilite la información sobre el uso de sus servidores de licencias en la consola de Licensing Manager. Para obtener más información, consulte Compartir estadísticas de uso en la documentación de producto de las licencias.
2. Revise los requisitos de conectividad que se describen en la sección Requisitos de conectividad de este artículo y asegúrese de que se puede contactar con las direcciones. Si utiliza un servidor proxy con el servidor de licencias de Citrix, asegúrese de que el servidor proxy esté configurado tal y como se describe en el paso 5, Configurar un servidor proxy, en la documentación de producto de las licencias.
3. Registre su servidor de licencias en Citrix Cloud tal como se describe en Registrar productos locales en Citrix Cloud.

Ver el uso de licencias de productos locales

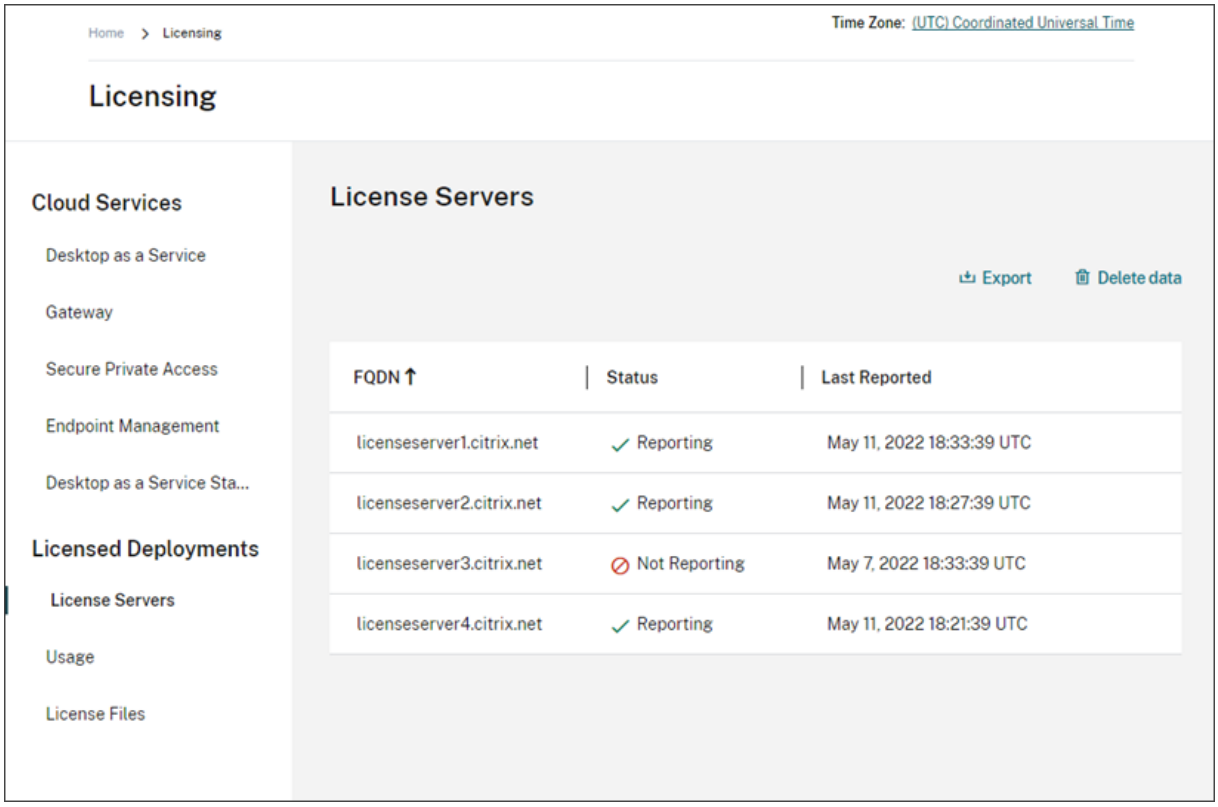
La información sobre el uso del servidor de licencias Citrix proporciona visibilidad sobre el uso de licencias en todo su entorno de Citrix. Puede acceder a los informes de uso que le ayudan a:

- Saber cuántos servidores de licencias se han implementado y registrado, y si informan del uso a Citrix Cloud.
- Ver el uso de licencias simultáneas y de usuario/dispositivo para Citrix Virtual Apps and Desktops.
- Obtener información sobre el uso adicional de licencias simultáneas y de usuario/dispositivo en varias implementaciones.
- Conocer el uso histórico de licencias y las tendencias mensuales del uso de licencias.

- Ver la hora del último inicio de sesión de usuarios específicos.
- Comparar la cantidad de licencias instaladas en relación con las licencias en uso en los servidores de licencias Citrix.
- Estar al tanto del descubierto de licencias.
- Ver desgloses del uso de licencias simultáneas y de usuario/dispositivo.

Ver el estado del servidor de licencias

En la vista de estado del servidor de licencias se muestra cada uno de los servidores de licencias que informan del uso a Citrix Cloud.



Los servidores de licencias muestran el estado "Informes"si han cargado correctamente informes de uso a Citrix Cloud en los últimos tres días. Los servidores de licencias muestran el estado "Ningún informe"si informaron del uso en los últimos 30 días, pero no en los últimos tres días. Los servidores de licencias que no hayan informado del uso en los últimos 30 días se eliminan de la lista.

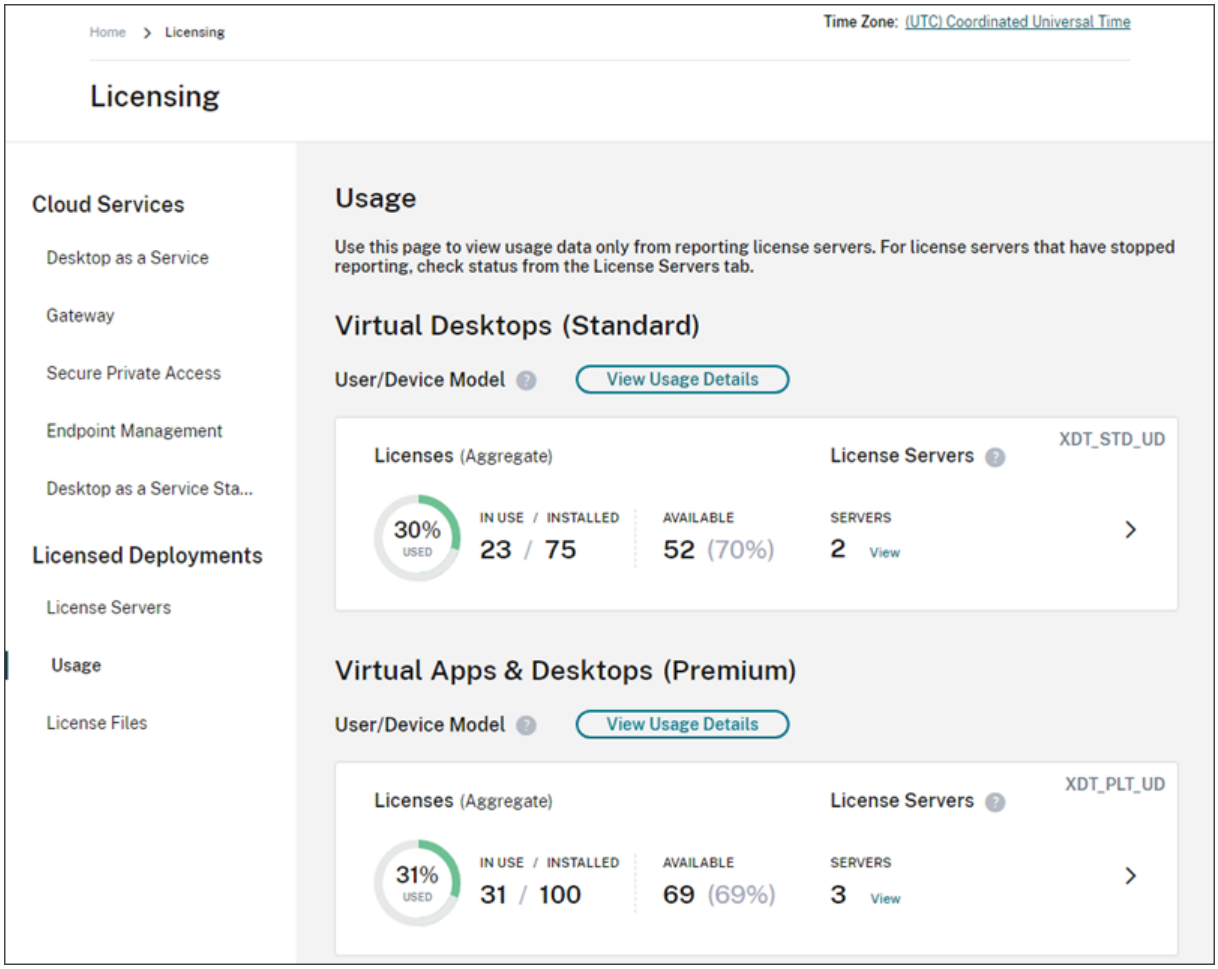
Impacto del estado del servidor de licencias en las vistas de uso de licencias

El estado de informes y la fecha de último informe de un servidor de licencias determinan si el uso de un servidor de licencias concreto se incluye o no en los informes y las vistas de uso.

- La información sobre las licencias actuales instaladas y en uso se basa exclusivamente en los datos de los servidores de licencias que envían informes. Si un servidor de licencias aparece con el estado "Ningún informe", las licencias instaladas y en uso de ese servidor no se reflejan en la experiencia de información de uso.
- La fecha del último informe de cada servidor de licencias determina hasta qué punto está actualizada la información de uso de licencias en la experiencia de información de uso. Los informes más recientes sobre el uso de licencias datan de la hora del último informe que haya enviado cada servidor de licencias.
- Los servidores de licencias Citrix configurados para obtener información sobre el uso y registrados en Citrix Cloud se actualizan una vez al día. Si es necesario, puede forzar una actualización desde la consola de administración de Citrix License Manager en el servidor de licencias.

Uso de licencias

La ficha Uso ofrece una vista consolidada del uso de licencias en las implementaciones de Citrix. La información de licencias proveniente de los informes de cada servidor de licencias se combina en una sola vista. Esta vista hace que sea fácil ver el uso total de las licencias en varias implementaciones y servidores de licencias diferentes.

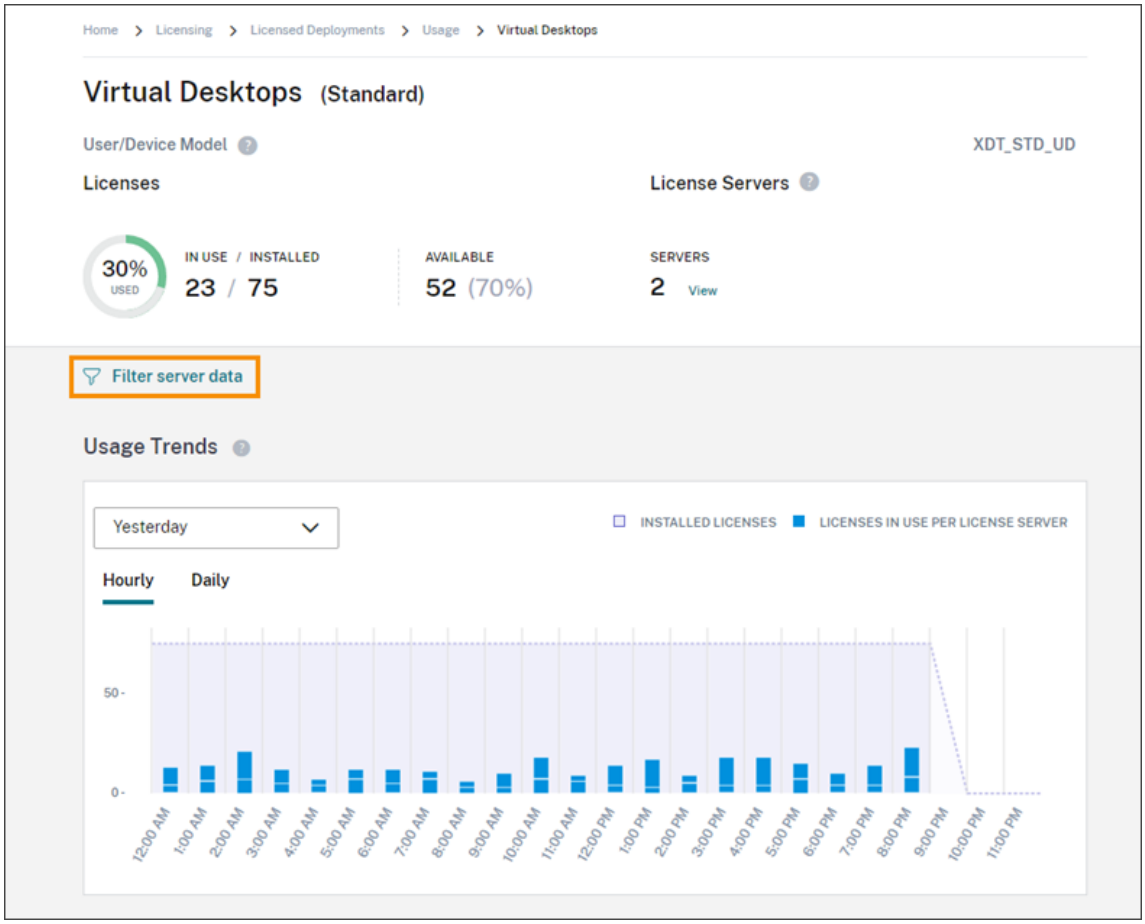


El uso de licencias se organiza y agrega de varios servidores de licencias según la edición del producto y el modelo de licencias. Se muestra una tarjeta resumen del uso de licencias para cada edición de licencia única que se encuentre en todos los servidores de licencias que envíen informes. Se muestra una tarjeta resumen para cada edición de producto detectada.

Uso por servidor de licencias

Para ver el uso de licencias de los productos de cada servidor de licencias, puede filtrar los datos de servidor.

1. En la página **Uso**, seleccione **Ver detalles de uso** del producto que quiera administrar.
2. Haga clic en **Filtrar datos de servidor** y, a continuación, seleccione los servidores de licencias cuyo uso quiera ver. De forma predeterminada, se seleccionan todos los servidores de licencias.



3. Seleccione **Aplicar**.

Después de aplicar el filtro, Citrix Cloud muestra las tendencias de uso, el desglose de servidores de licencias y la actividad de las licencias solo para los servidores que seleccionó.

Pico de uso máximo de licencias para el modelo de licencias simultáneas

La generación de informes sobre licencias simultáneas se organiza en torno a los siguientes puntos de datos:

- Licencias instaladas: El número de licencias instaladas en cada servidor de licencias.
- Pico de licencias en uso: El número máximo de licencias que se utilizaron en un período de tiempo específico.

Al calcular el pico de licencias en uso, Citrix Cloud recupera el número máximo de licencias utilizadas en los siguientes períodos de tiempo:

- Últimos 7 días: El número máximo de licencias utilizadas simultáneamente durante los últimos siete días.

- Este mes: El número máximo de licencias utilizadas simultáneamente en el mes del calendario actual.
- Siempre: El número máximo de licencias utilizadas simultáneamente desde que el servidor de licencias se registró con Citrix Cloud.

> **Importante:**
>
> Es posible que los datos de estos períodos de tiempo no coincidan con el número de licencias en uso en el servidor de licencias. El servidor de licencias informa solo del número de licencias en uso en un momento determinado. Citrix Cloud recibe estos puntos de datos individuales y calcula el pico para estos períodos de tiempo.

Consideraciones para interpretar el uso de licencias

Las licencias de Citrix admiten muchos casos de uso e incluyen información detallada. Tenga en cuenta los siguientes aspectos cuando supervise el uso de licencias:

- La información de uso se basa en las licencias instaladas en cada uno de los servidores de licencias que envían informes. Si un servidor de licencias se está quedando sin licencias disponibles, puede asignarle y colocar en él licencias adicionales para aumentar la cantidad de licencias disponibles.
- La información disponible en la vista de información sobre el uso de Citrix License Server incluye únicamente la información recopilada de los servidores de licencias Citrix registrados que envíen informes activamente. La experiencia de implementaciones con licencia no representa y puede que no coincida con la cantidad total de licencias que posee o adquirió.
- El porcentaje de licencias disponibles se calcula en función de la cantidad de licencias en uso en relación con las licencias instaladas en los servidores de licencias que envían informes.

Quitar el registro del servidor de licencias

Para eliminar por completo el registro del servidor de licencias de Citrix Cloud, hay que realizar las siguientes tareas:

1. Quite el servidor de licencias registrado de Citrix Cloud desde la consola de Citrix Licensing Manager. Para obtener instrucciones completas, consulte Eliminar el registro de su servidor de licencias.
2. Elimine cualquier dato de uso que se haya recopilado anteriormente.
3. Compruebe que Citrix Cloud ya no muestra el servidor de licencias en la página Registros de productos. Si el servidor de licencias sigue apareciendo en la lista, quite el servidor como se describe en Eliminar un registro de producto.

Eliminar datos de uso

Cuando quita un servidor de licencias registrado de Citrix Cloud, se siguen almacenando los datos de uso recopilados anteriormente. Si ya no quiere conservar estos datos, puede eliminarlos.

> **Importante:**
>
> La eliminación de los datos de uso es una acción permanente que no se puede deshacer. Si elimina los datos de uso, pero no elimina el registro del servidor de licencias, Citrix Cloud sigue recopilando datos de uso.

1. En el menú de Citrix Cloud, seleccione **Licencias**.
2. En la ficha **Servidores de licencias**, seleccione **Eliminar datos**.
3. Cuando se le pregunte, seleccione las casillas de verificación para confirmar que comprende el impacto de la eliminación.
4. Seleccione **Eliminar datos del servidor**.

Licencias para Citrix Service Providers

July 2, 2024

License Usage Insights Service de Citrix Cloud es un servicio de la nube gratuito que ayuda a los socios proveedores de servicios de Citrix (**Citrix Service Providers o CSP**) a comprender y notificar mejor los datos sobre el uso y las licencias de los productos. Solo los socios CSP tienen acceso a License Usage Insights.

> **Nota:**
>
> Citrix DaaS se llamaba Citrix Virtual Apps and Desktops Service. Citrix DaaS Standard para Azure se llamaba Citrix Virtual Apps and Desktops Standard para Azure. Por eso, puede que algunas pantallas aún contengan el nombre anterior.

License Usage Insights Service le permitirá:

- Recopilar y agregar automáticamente datos de uso de los productos, provenientes de los servidores de licencias de Citrix
- Agrupar automáticamente el uso y el consumo de las licencias de la nube para clientes arrendatarios únicos y multiarrendatario
- Ver fácilmente qué usuarios están accediendo cada mes a sus implementaciones de Virtual Apps and Desktops.
- Crear un desglose de uso de licencias por cliente

- Optimizar costes de licencia, identificando y haciendo un seguimiento de una lista de usuarios con acceso gratis.
- Ver y comprender la trayectoria histórica de su relación de negocio con Citrix
- Exportar el uso de licencias de Virtual Apps and Desktops y Citrix DaaS, datos de asignaciones de NetScaler VPX y datos de consumo y licencias de Citrix DaaS Standard para Azure en CSV

Información adicional

Para ver los requisitos y las instrucciones de configuración, consulte Primeros pasos en License Usage Insights.

Para ver el uso agregado de clientes arrendatarios únicos y socios multiarrendatario, consulte Informes y uso de licencias de los servicios de la nube para Citrix Service Providers.

Para ver el uso de los servicios admitidos por parte de los clientes mediante la consola Licencias, consulte los siguientes artículos:

- Supervisión del uso y las licencias de los clientes para Citrix DaaS
- Supervisión del uso y las licencias de los clientes para Citrix DaaS Standard para Azure

Primeros pasos en License Usage Insights

July 2, 2024

Productos Citrix admitidos

License Usage Insights Service proporciona información de uso para estos productos Citrix:

- Uso del producto Virtual Apps and Desktops (local)
- Citrix DaaS Premium (antes denominados servicios Virtual Apps Premium y Virtual Apps and Desktops Premium)
- Citrix DaaS Standard para Azure (antes denominado Citrix Virtual Apps and Desktops Standard para Azure)
- Asignaciones de NetScaler Console VPX

Requisitos

Para capturar información sobre el uso y las licencias de productos Citrix locales, se necesita Citrix License Server 11.16.3.0 o una versión posterior. Solo se admiten servidores de licencias basados en Windows y VPX.

Citrix License Server 11.16.3.0 (y versiones posteriores) contiene una serie de funciones clave que son importantes para los socios proveedores de servicios Citrix (CSP):

- Recopilación de datos de uso optimizada: License Server contiene nuevas funciones que optimizan el comportamiento y el seguimiento del sistema de licencias para ofrecer un mejor soporte a los socios CSP.
- Call Home: License Server incluye funciones "Call Home"que automatizan la recopilación de los datos de uso de los productos para los socios CSP. Estas funciones son exclusivas para los socios CSP y solo se activan cuando se detecta una licencia de CSP en el servidor de licencias.

Paso 1: Actualizar Citrix License Server

Si usa servidores de licencias anteriores a la versión 11.16.3.0, debe actualizarlos de versión antes de usar License Usage Insights. La actualización en contexto es rápida y sencilla. Lleve a cabo las siguientes tareas:

1. Descargue el software de License Server más reciente. Para obtener más información acerca de la versión más reciente de Citrix License Server, consulte la documentación de Citrix Licensing.
2. Actualice su servidor de licencias actual.
3. Repita el proceso de actualización en cada uno de los servidores de licencias que tenga.

Paso 2: Iniciar sesión en Citrix Cloud con credenciales de My Citrix

Antes de iniciar sesión, debe registrarse para obtener una cuenta de Citrix Cloud. Siga los pasos descritos en Registrarse en Citrix Cloud.

Al crear la cuenta, use las mismas credenciales de My Citrix que utiliza para asignar y descargar licencias de Citrix desde citrix.com. Citrix Cloud le enviará un correo electrónico a la dirección asociada a sus credenciales de My Citrix para confirmar la cuenta.

Cuando la cuenta de Citrix Cloud esté lista para usarse, inicie sesión en https://citrix.cloud.com con su dirección de correo electrónico y su contraseña.

Paso 3 (opcional): Anonimizar nombres de usuario a través del servidor de licencias

De forma predeterminada, los nombres de usuario asociados a extracciones de licencias de Virtual Apps and Desktops o Citrix DaaS se envían de forma segura a Citrix.

La información de nombres de usuario se envía para que los socios CSP puedan aprovechar mejor las ventajas de las funciones de License Usage Insights y del programa de licencias de CSP, que admite una cantidad determinada de usuarios de acceso gratuito, que pueden usar los productos con fines de evaluación, prueba y administración.

La información de usuario se limita a una entrada con formato usuario@dominio; no se envían más datos personales identificables. Citrix no comparte esta información.

Los socios que, por razones de confidencialidad, no quieren enviar la información de nombres de usuario pueden habilitar la anonimización de los nombres de usuario. Cuando está activada, la anonimización de los nombres de usuario convierte los nombres de usuario legibles en cadenas de texto de carácter exclusivo, mediante un algoritmo seguro e irreversible, antes de proceder al envío de los datos.

License Usage Insights usa estos identificadores únicos para hacer un seguimiento del uso de los productos en lugar de usar los nombres de usuario reales. Esto permite a los proveedores de servicios usar las estadísticas mes a mes, pero sin poder ver los nombres de usuario reales en la interfaz de usuario del servicio de la nube.

Para configurar la anonimización de los nombres de usuario

1. En el servidor de licencias, abra el archivo de configuración en un editor de texto. Por lo general, el archivo de configuración está en C:\Archivos de programa\Citrix\Licensing\WebServicesForLicensing\Simp
2. En la sección **Configurations**, agregue el parámetro **UsageBasedBillingScramble** de la siguiente manera:

```
<?xml version="1.0" encoding="utf-8"?>
<Configurations>
<EncoreConfiguration>
<SamplingPeriod>15</SamplingPeriod>
<RetentionTime>180</RetentionTime>
<Enabled>true</Enabled>
</EncoreConfiguration>
<SARenewalConfigOptions>Notify</SARenewalConfigOptions>
<UsageBasedBillingScramble>1</UsageBasedBillingScramble>
</Configurations>
<!--NeedCopy-->
```

3. Guarde el archivo.

Paso 4: Usar License Usage Insights Service

En la consola de Citrix Cloud, busque License Usage Insights Service y haga clic en **Administrar**. Para obtener una visión general de las funciones principales del servicio, consulte Administrar el uso de productos, servidores de licencias y notificaciones.

Detalles adicionales

Al usar Citrix License Server con License Usage Insights, tenga en cuenta lo siguiente:

- Es posible que un servidor de licencias recién actualizado tarde hasta 24 horas en aparecer en la consola de administración de License Usage Insights.
- Al cargar datos de uso desde un servidor de licencias, estos datos se procesan y se almacenan de manera segura para que License Usage Insights pueda acceder a ellos más adelante. Este proceso puede tardar hasta 24 horas en completarse.
- De forma predeterminada, los nombres de usuario asociados a extracciones de licencias de Virtual Apps and Desktops o Citrix DaaS se envían de forma segura a Citrix.
- La información de nombres de usuario se envía para que los socios CSP puedan aprovechar mejor las ventajas de las funciones de License Usage Insights y del programa de licencias de CSP, que admite una cantidad determinada de usuarios de acceso gratuito, que pueden usar los productos con fines de evaluación, prueba y administración.
- La información de usuario se limita a una entrada con formato usuario@dominio; no se envían más datos personales identificables. Citrix nunca compartirá esta información.

Ayuda y asistencia técnica

Si necesita asistencia con License Usage Insights, abra un tíquet de asistencia en el portal My Support. Para acceder a My Support desde Citrix Cloud:

1. Inicie sesión en Citrix Cloud.
2. Haga clic en el icono de **ayuda** de la parte superior derecha de la pantalla.
3. Seleccione **Abrir un tíquet**.
4. Seleccione **Ir a My Support** e inicie sesión con sus credenciales de My Citrix.
5. Rellene el formulario y envíelo.

Un miembro del equipo de asistencia técnica de Citrix se ocupará del caso y le ayudará.

Preguntas frecuentes

- **¿Qué información se está enviando? ¿Puedo ver la información que mis servidores de licencias envían a Citrix?** Sí, puede ver una copia de la información que se envía a Citrix. Para obtener información detallada, consulte Información del servidor de licencias incluida en las cargas de datos.
- **¿License Usage Insights está disponible para clientes o socios de Citrix que no son Citrix Service Providers?** No. License Usage Insights solo está disponible para socios Citrix Service Providers con un contrato de socio activo.
- **¿Puedo inhabilitar Call Home en el servidor de licencias?** No. En el contrato de licencia de los Citrix Service Providers, todos los servidores de licencias deben enviar datos de uso de los productos a Citrix. Los socios que, por razones de confidencialidad, tengan reservas acerca

del envío de datos, pueden usar la anonimización de nombre de usuario. Para obtener más información, consulte Anonimizar nombres de usuario a través del servidor de licencias.

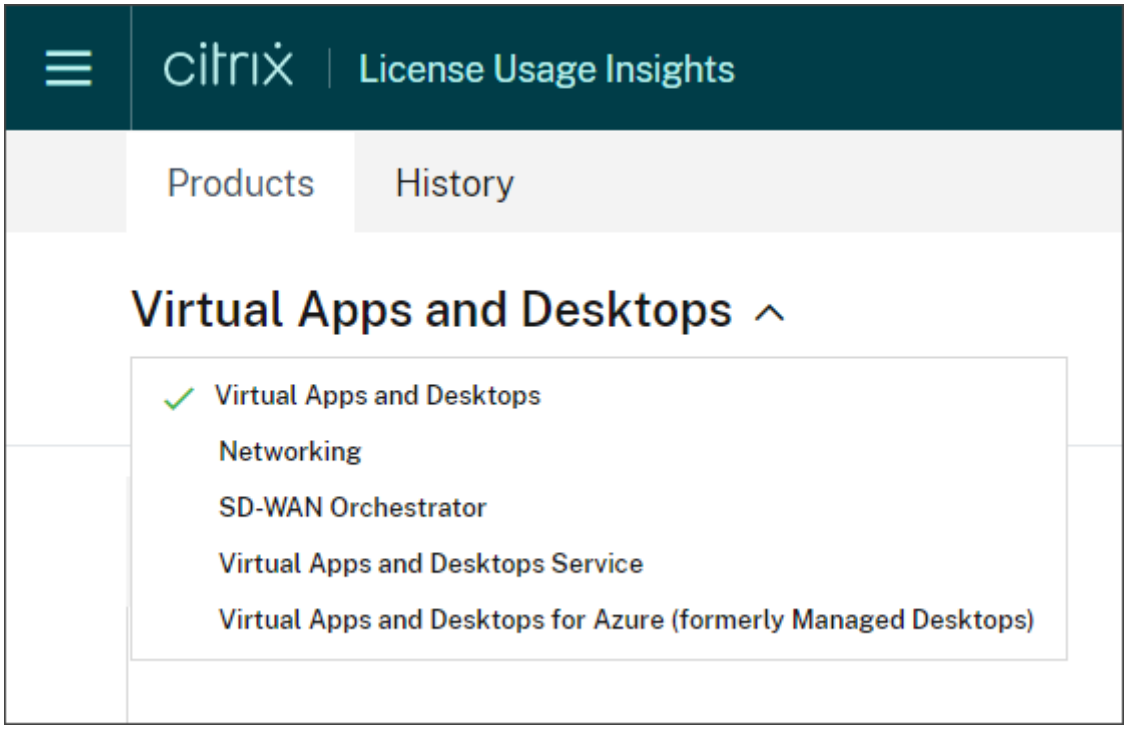
- **¿Se me facturará en función del uso de productos que aparezca en License Usage Insights?** No. License Usage Insights ayuda a los socios a comprender mejor cómo se usan los productos para que puedan notificarlo con más rapidez y precisión a su distribuidor de Citrix. Solo se facturará a los socios CSP en función del uso de productos que ellos notifiquen a su distribuidor de Citrix. Los distribuidores de Citrix seguirán siendo propietarios de la relación de facturación con los socios CSP.

Administrar el uso de productos, servidores de licencias y notificaciones

July 2, 2024

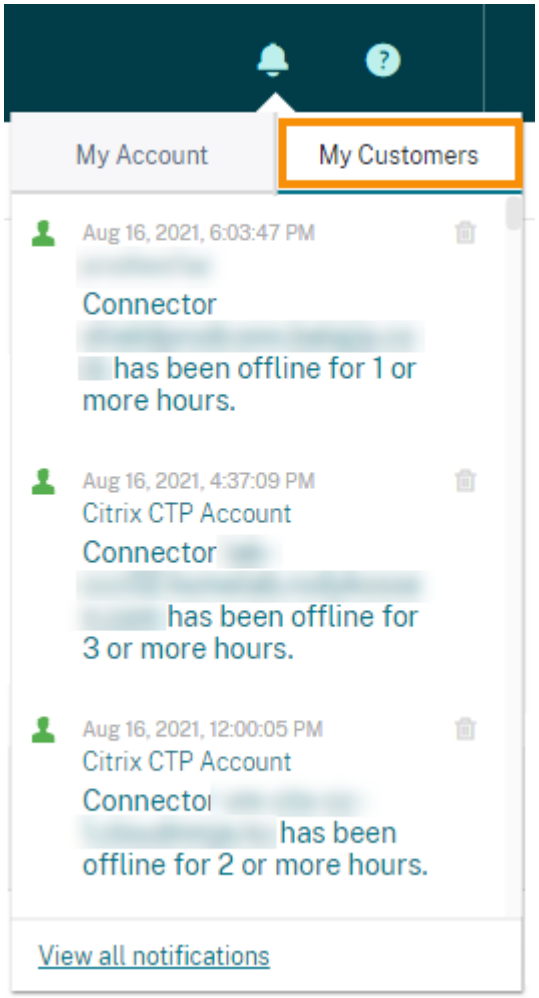
Selección del producto

Para ver los detalles de licencias de un producto diferente, haga clic en la flecha junto al nombre del producto y seleccione el producto o servicio que quiere ver.



Notificaciones de cliente

Es posible supervisar el estado de la solución en varios clientes sin tener que visitar cada implementación individualmente. El área Notificaciones en Citrix Cloud agrega las notificaciones de todos los clientes en el panel de mandos para garantizar que todas las alertas se tengan en cuenta y los servicios sigan funcionando.



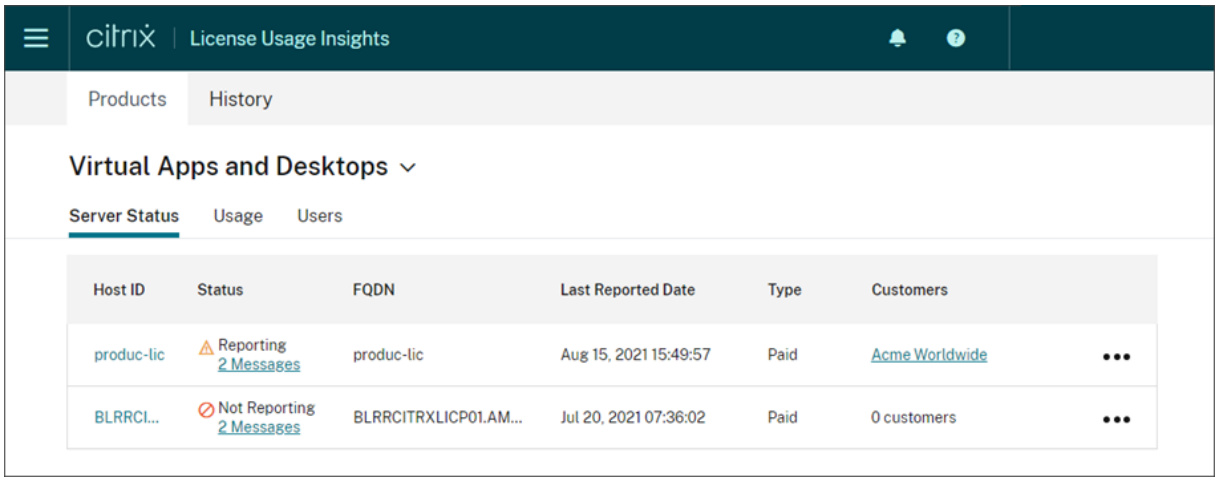
1. Desde la consola de administración de Citrix Cloud, haga clic en el icono de **Notificaciones** y luego haga clic en **Mis clientes**. Aparece una lista con las notificaciones más recientes.
2. Para ver una lista completa de las notificaciones de los clientes, haga clic en **Ver todas las notificaciones**.

Estado del servidor de licencias

Para actuar en conformidad con las directrices de licencia de Citrix Service Provider, todos los servidores de licencias activos deben estar actualizados y dando información. El estado del servidor de

licencias muestra los servidores de licencias que usted tiene y si están o no actualizados para poder usarlos con License Usage Insights.

El servicio muestra una lista de los servidores de licencias activos, con los datos de asignación de licencias almacenados en la infraestructura de administración de Citrix. Si el servidor de licencias está actualizado y creando informes correctamente, License Usage Insights lo muestra en la lista como servidor que está enviando información ("Reporting") e incluye la marca de hora de la carga más reciente.



Información del servidor de licencias incluida en las cargas de datos

Cuando Call Home de licencias se activa en un servidor de licencias, se carga diariamente la siguiente información:

- Versión del servidor de licencias
- Información del archivo de licencias:
  - Archivos de licencias instalados en el servidor
  - Fecha de caducidad de los archivos de licencias
  - Información sobre derechos para ediciones y componentes de los productos
  - Cantidad de licencias
- Uso de licencias:
  - Licencias utilizadas en el mes en curso
  - Nombres de usuario asociados a las licencias extraídas
  - Funciones y ediciones del producto activadas

Ver una carga de datos del servidor de licencias

Los socios CSP pueden inspeccionar la última carga de datos enviada en sus servidores de licencias para comprender mejor qué información se envía a Citrix. En el servidor de licencias, se guarda una copia de esta carga de datos como archivo .zip. De manera predeterminada, se encuentra en C:\Archivos de programa (x86)\Citrix\Licensing\LS\resource\usage\upload_1456166761.zip.

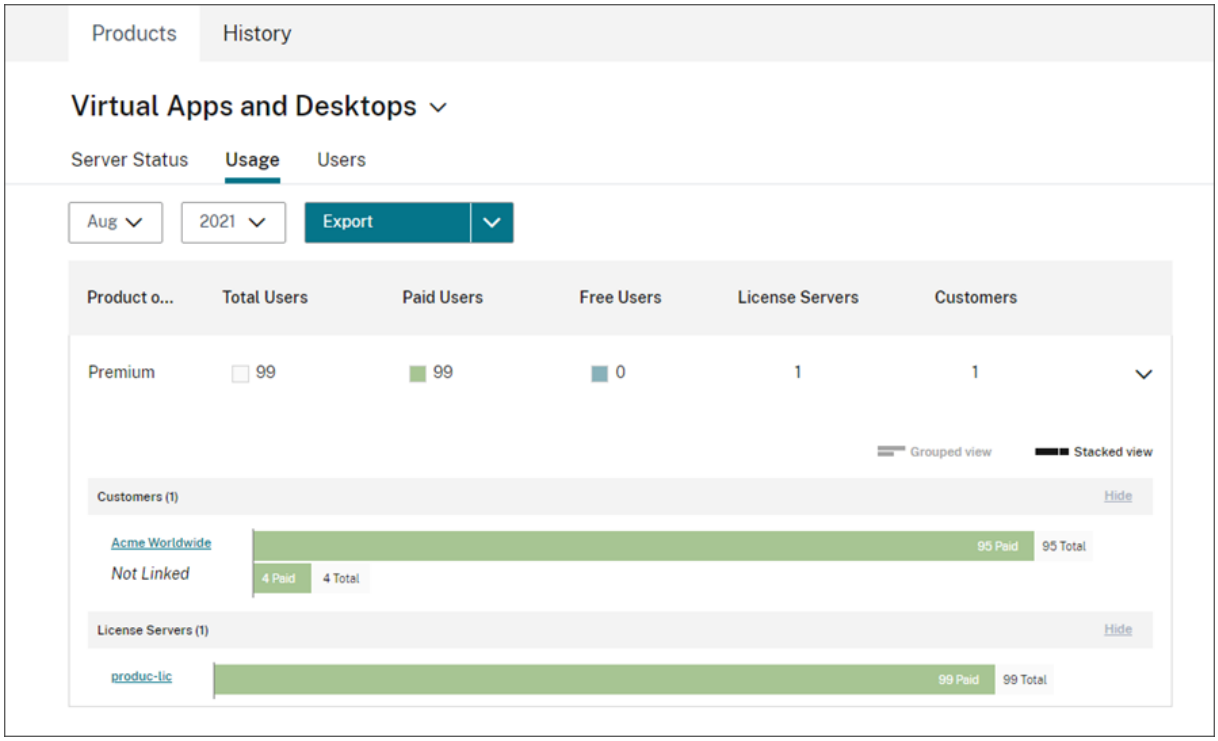
> **Nota:**
>
> Las cargas de datos que se realizan correctamente se eliminan después, excepto la última carga realizada. Las cargas de datos que no consiguen enviarse permanecen en el disco hasta que se realice el envío. En ese momento, se eliminan todas las cargas, excepto la última.

Recopilación de datos de uso

La recopilación de datos de uso le ayuda a entender mejor cómo se están usando los productos, mediante la recopilación y combinación automatizada de estos datos. No es necesario implementar herramientas adicionales.

License Usage Insights agrega automáticamente los datos de uso de los productos recopilados en todos los servidores de licencias de Citrix para ofrecer una visión completa del uso en todas las implementaciones. También puede crear desgloses de uso de licencias si asocia usuarios específicos a los clientes o arrendatarios a los que pertenecen.

Los servidores de licencias recopilan y hacen un seguimiento del uso de las licencias de producto y lo notifican a Citrix mediante un canal de comunicación seguro. Este enfoque automatizado le ofrece una secuencia continua de datos de uso siempre actualizada, lo que ahorra tiempo a los socios y les ayuda a comprender mejor las tendencias de uso dentro de sus implementaciones.



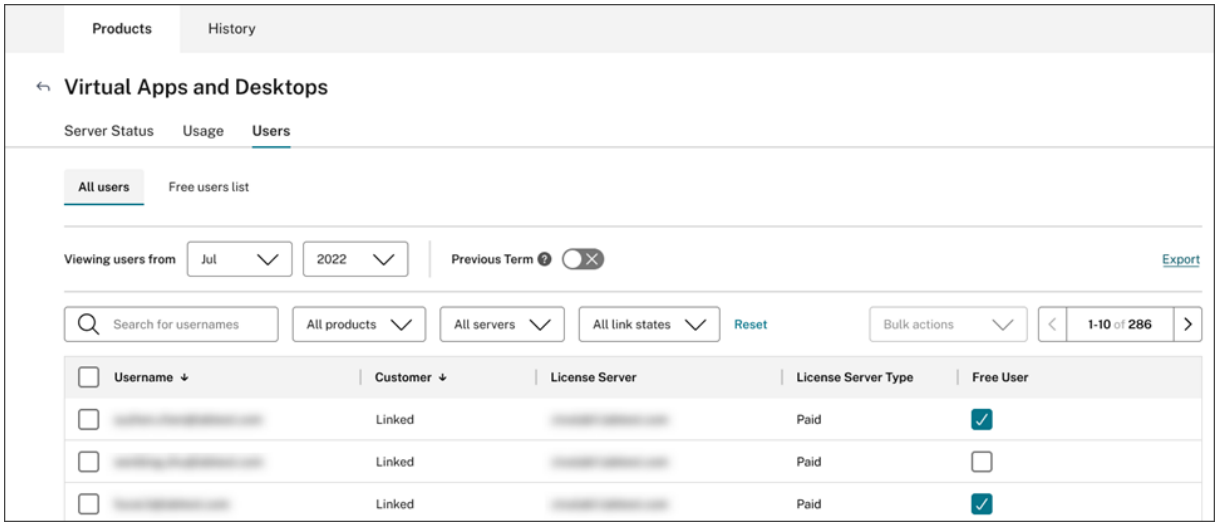
Crear un desglose de clientes del uso del producto Virtual Apps and Desktops

Para crear desgloses de uso de licencias, primero debe asociar usuarios específicos a los clientes o arrendatarios a los que pertenecen. Si no tiene clientes definidos en el panel de clientes, puede agregar clientes nuevos o conectarse con clientes existentes de Citrix Cloud.

1. Si corresponde, agregue clientes al panel de clientes: desde la página de inicio de la consola de administración de Citrix Cloud, haga clic en **Clientes**, haga clic en **Agregar o invitar** y luego siga las instrucciones en pantalla.
2. Haga clic en el botón de menú y luego seleccione **Mis servicios > License Usage Insights**.
3. Con el producto **Virtual Apps and Desktops** seleccionado, haga clic en **Users**.
4. Seleccione los usuarios que quiere asociar y luego haga clic en **Bulk Actions > Manage Link to Customer**.
5. En la lista, seleccione el cliente con el que quiere asociar a los usuarios.
6. Haga clic en **Guardar**.
7. Para ver el desglose por cliente, haga clic en la vista **Usage**.

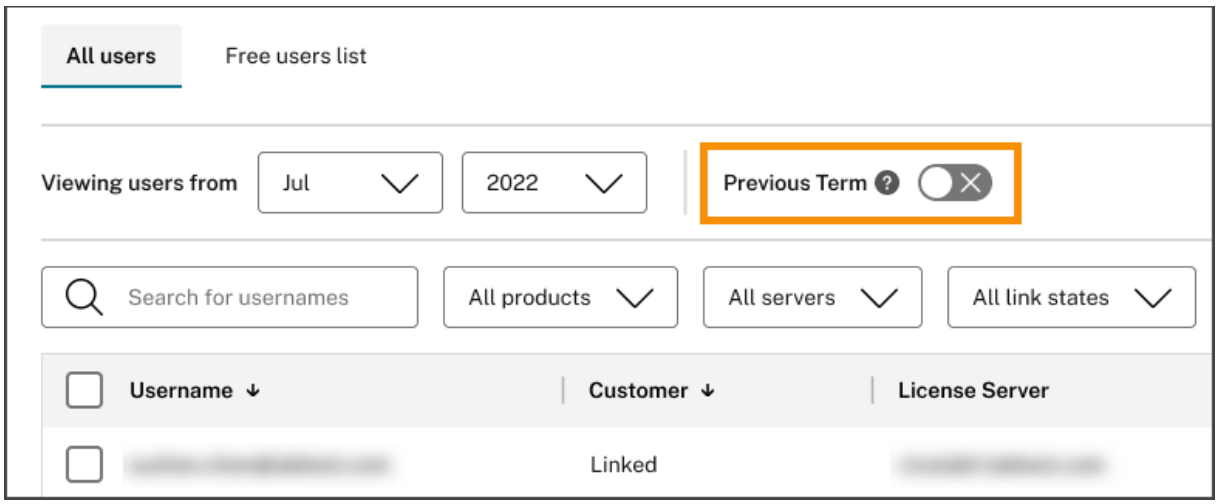
Administración de usuarios con acceso gratuito

License Usage Insights ofrece una vista exhaustiva del uso de los productos en todas las implementaciones, al tiempo que permite aprovechar todas las ventajas del programa de licencias de Citrix Service Provider, que tiene capacidad para usuarios administrativos, de prueba y de evaluación.



Para garantizar que se le facture adecuadamente por los usuarios de pago en un ciclo de facturación determinado, puede designar ciertos usuarios como usuarios gratuitos durante ese ciclo. Durante un mes determinado de su ciclo de facturación actual, puede seleccionar usuarios gratuitos en cualquier momento hasta el día 10 del mes siguiente. Por ejemplo, en marzo, puede seleccionar usuarios gratuitos en cualquier momento hasta el 10 de abril.

Entre el día 1 y el día 10 de cada mes, también puede seleccionar usuarios gratuitos para el ciclo de facturación anterior. Durante este período, puede activar el parámetro **Plazo anterior** y seleccionar los usuarios gratuitos de ese ciclo de facturación. Después del día 10 del mes, Citrix Cloud ya no mostrará el parámetro **Plazo anterior**.



Los usuarios gratuitos que seleccione en un mes determinado se contabilizarán cuando se le facturen los usuarios de pago. Al cambiar el estado de un usuario gratuito al de un usuario de pago, Citrix registra la fecha del cambio e incluye a ese usuario en el ciclo de facturación durante el cual se produjo el cambio.

Etiquetado de usuarios y clientes

Esta función proporciona un desglose de los datos de uso de licencias para cada cliente, que incluye funcionalidad de administración y la generación de informes sobre arquitecturas de servidores de licencias de un solo arrendatario y multiarrendatario. Los objetivos de License Usage Insights son:

- Servidor de licencias: un servidor de licencias "que informa"o "que no informa"sobre la lista.
- Usuario: un nombre de usuario único que se encuentra en los datos de uso de Call Home.
- NetScaler: una asignación única de licencias de NetScaler VPX (VPX sobre la Lista VPX).

> **Nota**
>
> La función de etiquetado de usuarios y clientes tiene el mismo comportamiento que el etiquetado de usuarios de acceso gratuito, en el que un CSP puede actualizar el etiquetado de los clientes para el ciclo de facturación actual hasta el día 10 del mes siguiente.

Etiquetado de servidores de acceso gratuito

Esta función proporciona flexibilidad a la hora de administrar recursos en el entorno de Citrix Cloud, ya que permite a los administradores organizar e identificar servidores en función de sus funciones, ubicaciones o cualquier otro criterio relevante, sin preocuparse por las implicaciones de las licencias.

> **Nota**
>
> Un CSP puede modificar el etiquetado del acceso gratuito o el etiquetado de clientes para el mes en curso exclusivamente y los cambios se aplicarán tanto al mes actual como a los meses próximos.

Etiquetado de clientes de servidores

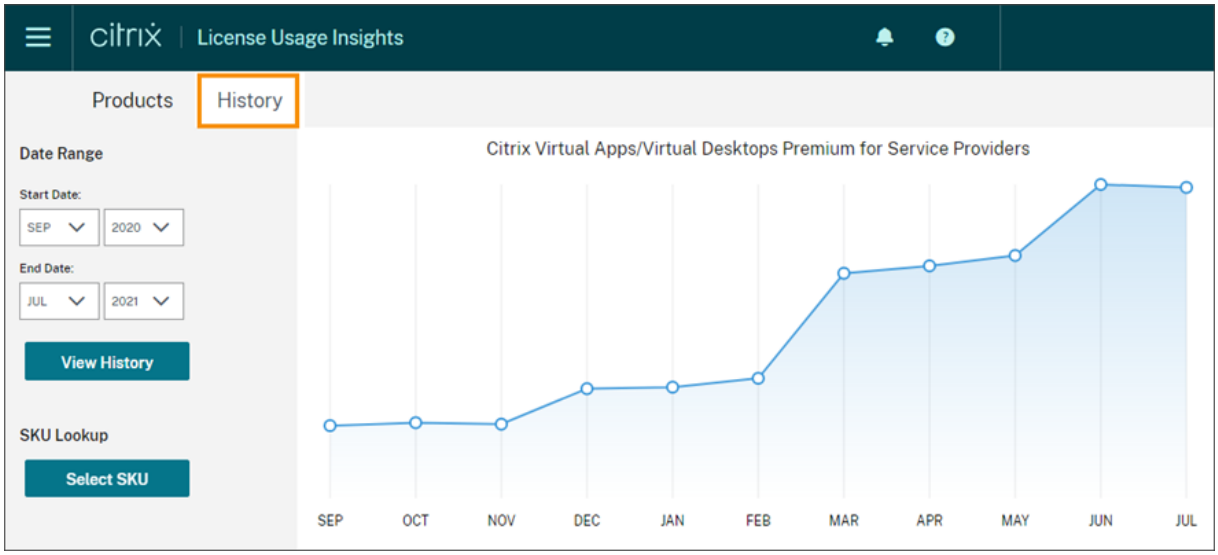
Esta función permite una mejor organización y administración de los recursos en el entorno de Citrix Cloud, lo que garantiza que los servidores se etiqueten de acuerdo con las necesidades específicas de los clientes. Al utilizar el etiquetado de clientes de servidores, los administradores pueden identificar y rastrear fácilmente los recursos asociados a diferentes clientes, lo que facilita una asignación y administración de recursos más eficiente.

> **Nota**
>
> Un CSP puede modificar el etiquetado del acceso gratuito o el etiquetado de clientes para el mes en curso exclusivamente y los cambios se aplicarán tanto al mes actual como a los meses próximos.

Tendencias históricas

Puede ver un registro histórico completo de toda su relación comercial con Citrix. Puede consultar los datos de uso notificados para el mes anterior, el año anterior, u otro período de tiempo configurable.

Las vistas históricas ofrecen información muy valiosa para la gestión de su negocio. Como proveedor de servicios de Citrix (CSP), usted podrá hacerse una buena idea de cuáles son las tendencias en su relación con Citrix y qué productos están creciendo más entre sus clientes y suscriptores.



Exportar datos de uso y asignación

Puede exportar estos tipos de datos en un archivo CSV desde License Usage Insights:

- Uso del producto Virtual Apps and Desktops y lista de usuarios correspondiente a un mes específico
- Detalles de asignación actual de NetScaler VPX

1. Seleccione **Virtual Apps and Desktops** o **Networking** en la lista de productos.
2. Si corresponde, seleccione la vista que quiere exportar. Por ejemplo, para exportar los detalles de uso de Virtual Apps and Desktops, haga clic en la vista **Usage**.
3. Si corresponde, seleccione el mes y el año cuyos datos quiere exportar.
4. En la parte derecha de la pantalla, haga clic en **Export**.

Acceder a los datos de las licencias con API

Citrix proporciona varias API que le permiten acceder a los datos de las licencias fuera de Citrix Cloud. Para obtener más información sobre estas API, consulte APIs to manage Citrix cloud licensing en la

documentación de Citrix Developer.

Para usar estas API, primero deberá crear un cliente seguro y generar un token de portador. Para crear un cliente seguro, debe tener el permiso **Cliente seguro** en Citrix Cloud. Para obtener más información, consulte Permisos de la consola.

Para obtener más información sobre las tareas necesarias para usar las API de Citrix Cloud, consulte Get started with Citrix Cloud APIs en la documentación de Citrix Developer.

Acceso de distribuidor a las API

Puede autorizar a su distribuidor de Citrix para que acceda a los datos de sus licencias a través de las API de Citrix Cloud sin concederle acceso de administrador total a su cuenta de Citrix Cloud. Puede hacer esto para que su distribuidor pueda validar sus informes de uso y garantizar una facturación correcta.

Para proporcionar a los distribuidores acceso a los datos de sus licencias, debe crear un administrador de acceso personalizado con permiso únicamente para crear clientes seguros y acceder a License Usage Insights Service. Esta cuenta tiene acceso limitado a las API de Citrix Cloud y no tiene acceso a otras funciones de Citrix Cloud. Una vez creada la cuenta, puede compartir las credenciales de esta con su distribuidor para que pueda iniciar sesión en su cuenta de Citrix Cloud y crear el cliente seguro necesario para usar las API de Citrix Cloud. También puede iniciar sesión como administrador de acceso personalizado, crear el cliente seguro y, a continuación, compartir los detalles del cliente seguro con su distribuidor.

Para crear la cuenta de acceso personalizada para su distribuidor:

1. Cree una nueva cuenta de administrador específica para su distribuidor de Citrix. Para obtener instrucciones, consulte Invitar a administradores individuales.
2. En **Establecer acceso**, seleccione **Acceso personalizado** y, a continuación, seleccione los siguientes permisos:
    - **General > Cliente seguro**
    - **Información del uso de licencias > Información sobre el uso de licencias: Acceso de distribuidor**

Para crear el cliente seguro:

1. Inicie sesión en Citrix Cloud con las credenciales de la nueva cuenta.
2. Cree un nuevo cliente seguro como se describe en Get started with Citrix Cloud APIs.
3. Anote el ID de cliente y el secreto del cliente que genera Citrix Cloud. Estos detalles son necesarios para acceder a todas las API de Citrix Cloud.

Datos de licencias disponibles para los distribuidores

En esta sección se describen las API y los datos de licencias a los que puede acceder su distribuidor de Citrix con los detalles de cliente seguro que usted proporciona. Use los enlaces que aparecen a continuación para obtener más información sobre cada API.

Informes de CSP sobre uso mensual e histórico de licencias de Virtual Apps and Desktops (Información del uso de licencias):

- Uso actual de Virtual Apps and Desktops
- Uso histórico de Virtual Apps and Desktops

Informes de CSP sobre uso de licencias de nube de un solo arrendatario y multiarrendatario (Información del uso de licencias):

- Uso actual de DaaS
- Uso histórico de DaaS

Uso de licencias de nube de CSP (Licencias):

- Uso actual de DaaS
- Uso histórico de DaaS

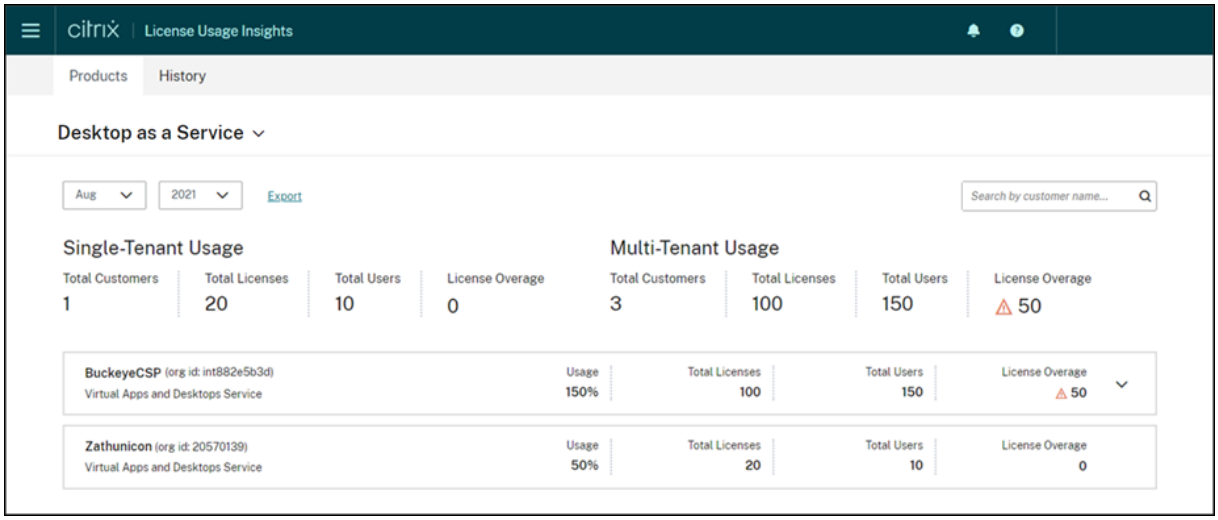
Uso de licencias de nube de arrendatario (Panel de mandos del cliente -> Ver licencias)

- Uso actual de licencias CCU de DaaS
- Uso histórico de licencias CCU de DaaS
- Uso actual de licencias UD de DaaS
- Uso histórico de licencias UD de DaaS

Informes y uso de licencias de los servicios de la nube para Citrix Service Providers

October 2, 2023

License Usage Insights agrega automáticamente el uso de los servicios de la nube para ofrecer una vista completa de todos los clientes arrendatarios únicos y todos los socios multiarrendatario. También puede exportar estos detalles de un mes determinado en un archivo CSV para un análisis más exhaustivo.



Servicios compatibles

El uso de licencias de un solo arrendatario está disponible para Citrix DaaS Premium (antes denominado Virtual Apps Premium y Virtual Apps and Desktops Premium).

El uso de licencias multiarrendatario está disponible para los siguientes servicios:

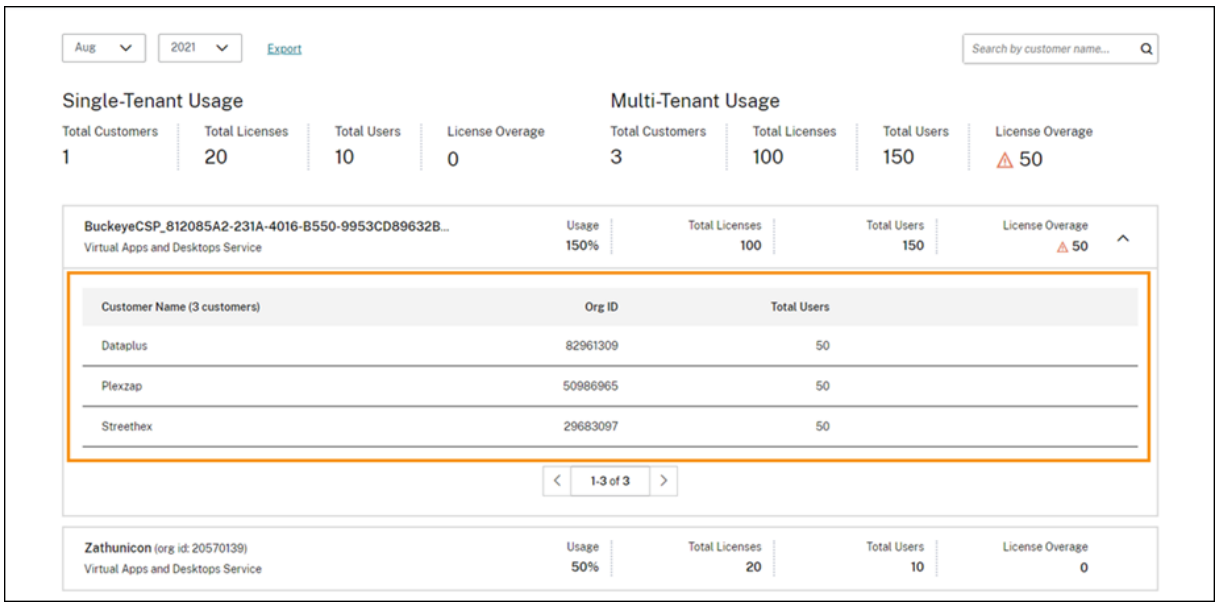
- Citrix DaaS (antes denominado Virtual Apps and Desktops Service)
- Citrix DaaS Standard para Azure (antes denominado Virtual Apps and Desktops Standard para Azure)

Resumen de las licencias

License Usage Insights ofrece este desglose del uso multiarrendatario y de arrendatarios únicos para Citrix Service Providers (CSP):

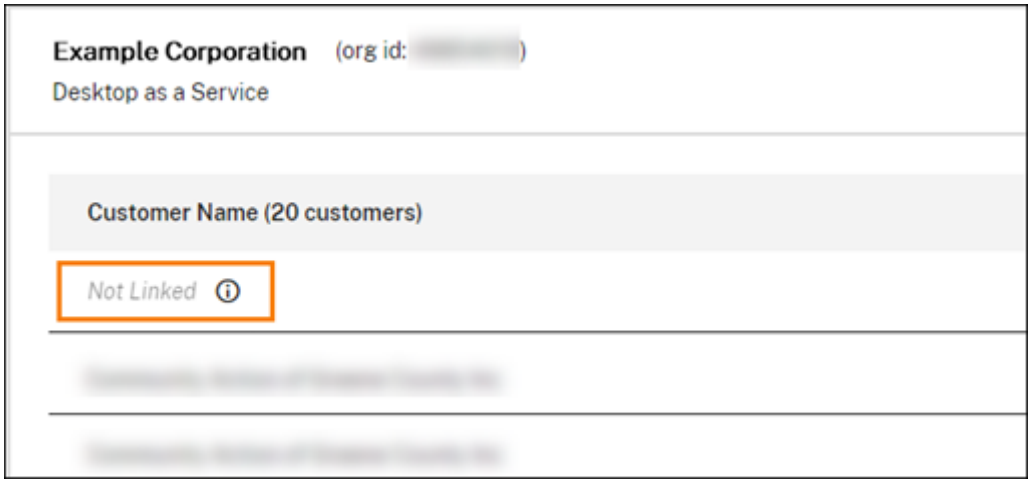
- Un resumen general agrupado por tipo de arrendatario que incluye el total de clientes y el total de licencias adquiridas, usuarios y licencias sobreasignadas en todos los clientes.
- Resumen de uso de cada cliente o socio que incluye el porcentaje del total de licencias en uso, el total de licencias adquiridas, los usuarios y la cantidad de licencias sobreasignadas.

Para los servicios multiarrendatario, puede expandir el resumen de uso para ver los clientes, el OrgID y el total de usuarios asociados a cada socio.



Los clientes arrendatarios no están vinculados

En algunos casos, es posible que un cliente arrendatario aparezca como "No vinculado". Este estado puede ocurrir cuando los usuarios de ese arrendatario acceden a un servicio de la nube a través de la URL del espacio de trabajo del CSP, en lugar de la URL del espacio de trabajo del arrendatario.

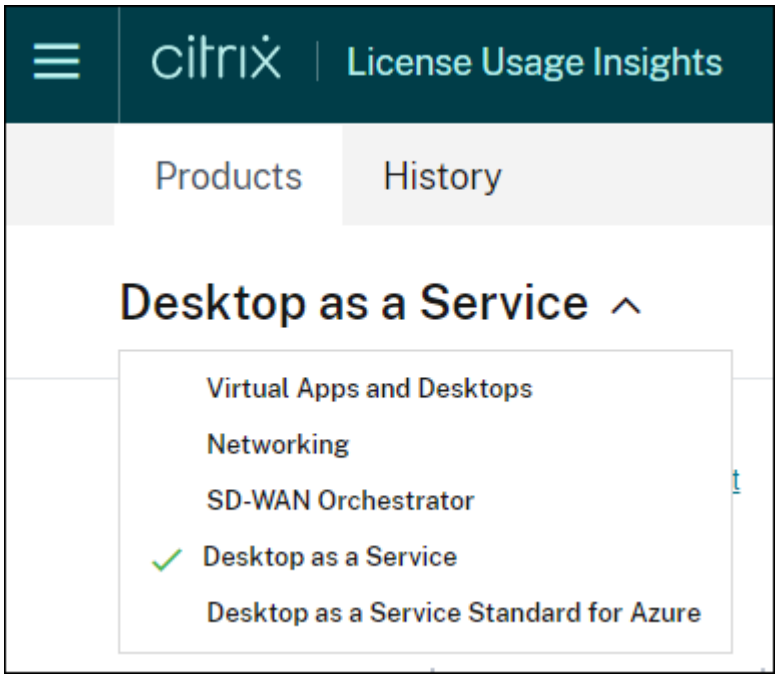


Cuando el usuario arrendatario accede al servicio a través de la URL del espacio de trabajo del arrendatario, Citrix Cloud considera que el usuario pertenece al arrendatario, y se quita el mensaje "No vinculado".

Ver y exportar el uso mensual

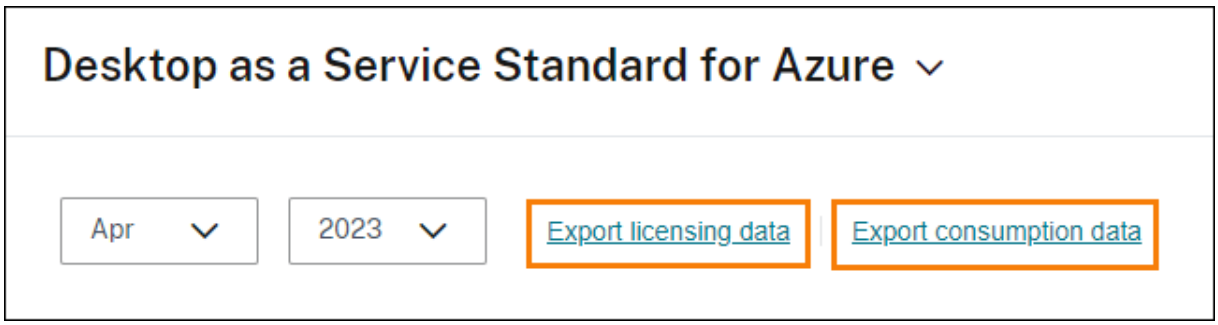
Puede ver el uso de las licencias de los meses anteriores para todos los clientes y socios en cualquier momento. También puede exportar estos datos en un archivo CSV para un análisis más exhaustivo. Para Citrix DaaS Standard para Azure, también puede exportar datos de consumo mensual.

1. En el menú del producto, seleccione el servicio de la nube que quiere ver.



Para Citrix DaaS, seleccione el mes y el año que quiere ver y seleccione **Exportar**.

Para Citrix DaaS Standard para Azure, seleccione el mes y el año que quiere ver y, a continuación, seleccione **Exportar datos de licencias** o **Exportar datos de consumo**.

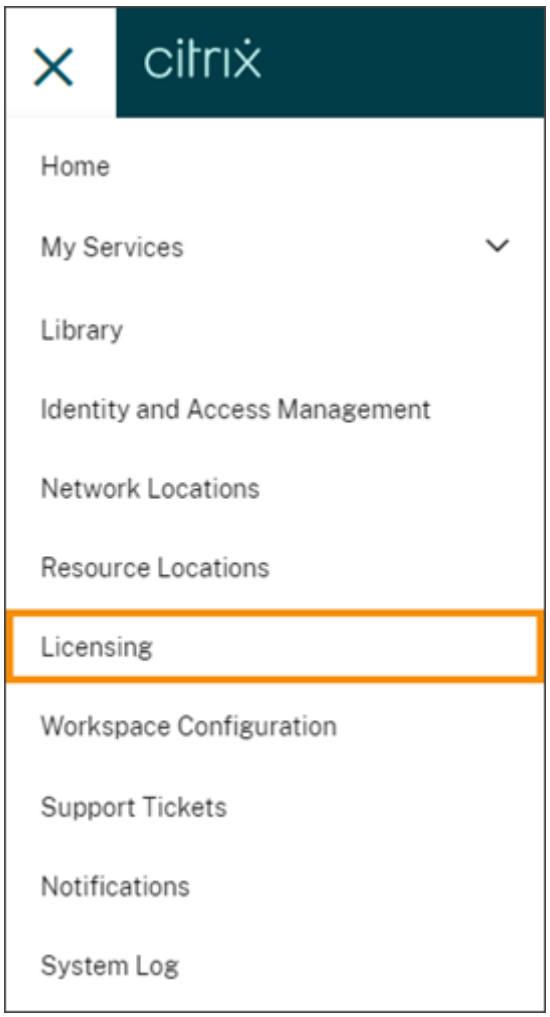


Supervisión del uso y las licencias de los clientes para Citrix DaaS

October 2, 2023

Los clientes de **Citrix Service Providers (CSP)** pueden supervisar fácilmente las licencias de Citrix DaaS para sus usuarios en Citrix Cloud. Como CSP, para acceder a estos datos, inicie sesión en la cuenta de su cliente en Citrix Cloud. Para ver información agregada sobre el uso de licencias en clientes arrendatarios únicos y multiarrendatario, consulte Informes y uso de licencias de los servicios de la nube para Citrix Service Providers.

Los clientes pueden ver sus datos de licencias al seleccionar **Licencias** en el menú de Citrix Cloud.



Asignación de licencias

Modelo de licencias de usuario/dispositivo: Citrix Cloud asigna una licencia cuando un usuario cliente único inicia una aplicación o escritorio por primera vez en el mes actual.

Modelo de licencias de usuario simultáneas: Citrix Cloud asigna una licencia cuando un usuario inicia una aplicación o un escritorio en su dispositivo. Cuando el usuario cierra sesión o se desconecta de la sesión, la licencia ya no se asigna. Dado que la asignación de licencias puede cambiar en función del número de dispositivos que acceden a aplicaciones o escritorios en un momento dado, Citrix Cloud evalúa el número de licencias en uso cada cinco minutos.

Para obtener más información sobre el modelo de licencias simultáneas, consulte Licencias simultáneas en la documentación de producto de Licensing.

Resumen de las licencias

Citrix Cloud muestra vistas resumidas de las licencias que se están usando en los modelos de licencias de usuario/dispositivo y de licencias de usuario simultáneas.

Resumen para usuarios y dispositivos

Para el modelo de usuario/dispositivo, el resumen de las licencias proporciona una visión general de las licencias que se están usando en relación con la cantidad total de licencias que usted posea.

El color del porcentaje cambia de verde a amarillo a medida que se aproxima al 100%. El color del porcentaje se vuelve rojo si se excede el 100%.

Citrix Cloud también muestra la relación entre las licencias asignadas y las licencias adquiridas, y la cantidad restante de licencias disponibles.

Resumen para licencias de usuario simultáneas

Para el modelo de licencias de usuario simultáneas, el resumen de las licencias proporciona una visión general de esta información:

- Porcentaje del total de licencias adquiridas actualmente en uso cuando Citrix Cloud evaluó por última vez las licencias en uso. Citrix Cloud calcula este porcentaje cada cinco minutos en función de los dispositivos únicos con conexiones activas al servicio. El total de licencias adquiridas es la suma de las licencias que se adquirieron para Citrix DaaS que utilizan el modelo de licencias simultáneas.
- La relación entre las licencias asignadas actualmente a las licencias adquiridas totales, y la cantidad restante de licencias disponibles. La cifra **Total** que se muestra en esta relación representa la cantidad total de licencias en propiedad actualmente (a partir de la fecha y la hora del último informe).
- Estadísticas de pico de uso. Al calcular el pico de licencias en uso, Citrix Cloud obtiene el máximo de licencias utilizadas en los siguientes períodos de tiempo:
  - **Últimas 24 horas:** El máximo de licencias utilizadas simultáneamente durante las últimas 24 horas.
  - **Este mes:** El máximo de licencias utilizadas simultáneamente en el mes del calendario actual.
  - **Siempre:** El máximo de licencias utilizadas simultáneamente desde el inicio de la suscripción.

La cifra **Total** mostrada para estos períodos de pico de uso representa el total de licencias en propiedad en ese momento. Si el total de licencias en propiedad aumenta o disminuye y hay un aumento correspondiente en las licencias asignadas, la cifra **Total** cambia para reflejar la nueva cantidad de licencias en propiedad en ese momento. Sin embargo, si no hay un pico de uso correspondiente, la cifra **Total** no cambia.

- Estadísticas de uso activo. Citrix Cloud muestra la cantidad total de conexiones únicas durante estos períodos:
  - **Mensual:** La cantidad total de conexiones del mes natural anterior.
  - **Diario:** La cantidad total de conexiones de las 24 horas anteriores. Estas cifras también se representan como porcentajes del total de licencias en su posesión durante estos períodos.

Calcular el pico de licencias en uso

Para reflejar con precisión el modelo de licencias simultáneas, Citrix Cloud cuenta la cantidad de dispositivos únicos que han accedido al servicio de forma simultánea cada cinco minutos. Si el recuento es mayor que el pico de uso actual que se muestra, Citrix Cloud muestra el nuevo pico de uso con la fecha y la hora en que se alcanzó. Si el recuento es menor que el pico de uso actual, el pico de uso actual no cambia.

> **Importante:**
>
> Si utiliza Supervisar en Director para obtener información acerca de las sesiones simultáneas, tenga en cuenta que el informe de Supervisar proporciona una interpretación diferente de las sesiones simultáneas y no refleja con precisión el número de licencias de usuario simultáneas en uso. Para obtener más información acerca de las diferencias entre los informes de Supervisar y los informes de Licencias, consulte las Preguntas frecuentes.

Calcular el uso activo mensual

Al principio de cada mes, Citrix Cloud toma una instantánea del mes natural anterior. Citrix Cloud muestra la cantidad total de conexiones únicas que hubo durante ese mes natural.

Calcular el uso activo diario

Todos los días, a la misma hora, Citrix Cloud toma una instantánea de las 24 horas anteriores. Citrix Cloud muestra la cantidad total de conexiones únicas que hubo durante ese período de 24 horas.

Tendencias de uso

Citrix Cloud muestra un desglose de las tendencias de uso de las licencias de usuario/dispositivo y de las licencias de usuario simultáneas. Para ver este desglose, seleccione **Ver detalles de uso** en la página de resumen de las licencias.

Tendencias para usuarios y dispositivos

En el caso de las licencias de usuario/dispositivo, la sección **Tendencias de uso** muestra un desglose de las licencias asignadas en forma de gráfico.

Al señalar un intervalo en el gráfico, se muestra esta información:

- **Total de licencias:** La cantidad total de licencias que ha comprado del servicio de la nube para todos los derechos incluidos.
- **Asignadas previamente:** La cantidad de licencias asignadas en el mes anterior. Por ejemplo, un usuario accede al servicio de la nube por primera vez en julio y se le asigna una licencia. Esta licencia se cuenta como "Asignada recientemente"para el mes de julio. Para el mes de agosto, esta licencia se cuenta como "Asignada previamente".
- **Asignadas recientemente:** La cantidad de licencias nuevas que se asignaron cada mes. Por ejemplo, un usuario accede al servicio de la nube por primera vez en julio y se le asigna una licencia. Esta licencia se cuenta como "Asignada recientemente"para el mes de julio.

Tendencias para licencias de usuario simultáneas

En el caso de las licencias de usuario simultáneas, la sección **Tendencias de uso** muestra esta información:

- **Total de licencias:** El total de licencias simultáneas adquiridas.
- **Pico de licencias en uso:** El máximo de licencias asignadas para el intervalo de fechas seleccionado. De forma predeterminada, Citrix Cloud muestra el pico de uso para cada mes del año natural actual. Para ver un desglose del pico de uso mensual o por horas, seleccione el mes o día del calendario que quiere ver en el menú desplegable.

  Si el intervalo de fechas seleccionado aún no ha terminado, Citrix Cloud muestra el pico de uso actual del último intervalo de tiempo. Por ejemplo, si desglosa un día natural que aún está en curso, se muestra el máximo de licencias por cada hora hasta el momento actual. Si el máximo de licencias aumenta en el siguiente intervalo de cinco minutos, Citrix Cloud actualiza el pico de uso de la hora actual.
- **Uso activo** muestra un gráfico con esta información:

- **Diario:** La cantidad total de conexiones de cada día durante los 30 días anteriores.
- **Mensual:** La cantidad total de conexiones de cada mes durante año natural anterior.

Al señalar un intervalo en los gráficos **Asignación de licencias** o **Uso activo**, se muestran los detalles de ese intervalo.

Usuarios con licencias

La sección **Actividad de licencias** muestra una lista de los usuarios clientes individuales que tienen licencias asignadas durante el mes actual. Esta lista también muestra el dominio al que pertenece cada usuario, la fecha en que se asignó la licencia y la última vez que se utilizó el servicio.

Liberación mensual de licencias

El primer día de cada mes, las licencias asignadas del mes anterior se liberan automáticamente. Cuando esto ocurre, la cantidad de licencias asignadas se restablece a cero y se borra la lista de usuarios clientes con licencias. Las licencias se reasignan cuando los usuarios inician aplicaciones o escritorios por primera vez en el nuevo mes.

Revisar el historial de licencias mensuales

El primer día de cada mes, la lista de usuarios clientes con licencias del mes anterior, en **Actividad de licencias**, se borra cuando la cantidad de licencias asignadas se restablece a cero. Sin embargo, puede acceder a los datos de usuario de los meses anteriores en cualquier momento y descargarlos como un archivo CSV, si fuera necesario.

1. En la sección **Actividad de licencias**, seleccione **Ver historial de licencias** en el extremo derecho de la sección.
2. Seleccione el mes que quiere ver. Aparecerá una lista con los detalles de usuario del mes seleccionado.
3. Para exportar la lista, seleccione **Exportar en CSV** en el extremo derecho de la sección y, a continuación, guarde el archivo.

Exportar detalles de las licencias

Los clientes pueden, en cualquier momento, exportar detalles de usuarios con licencia en un archivo CSV para un análisis más exhaustivo. El cliente puede usar el archivo CSV como quiera para analizar los detalles de las licencias.

Para exportar los detalles del mes actual, en la sección **Actividad de licencias**, seleccione **Exportar en CSV** en el extremo derecho de la sección y, a continuación, guarde el archivo.

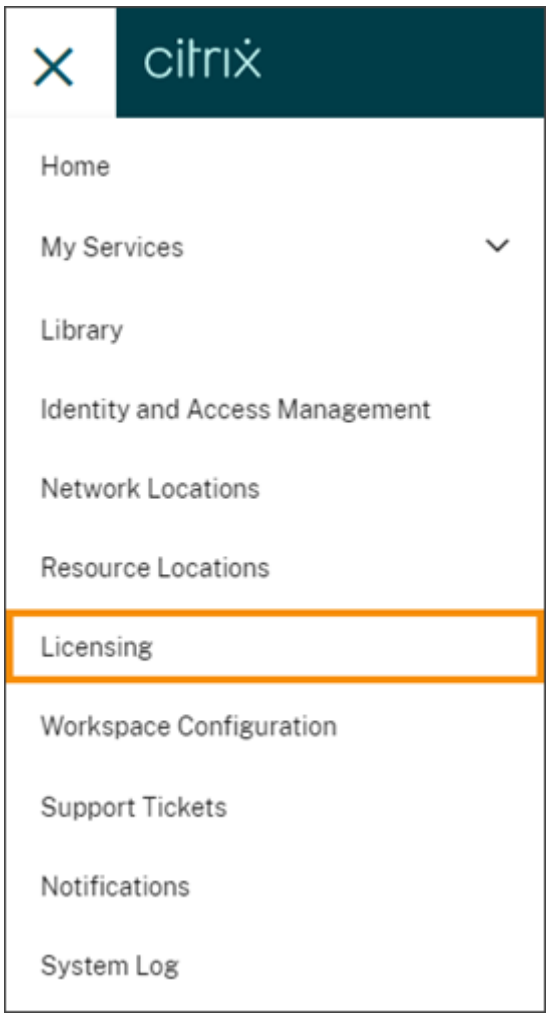
Para exportar los detalles de los meses anteriores, genere una lista para un mes seleccionado tal y como se describe en Revisar el historial de licencias mensuales. Seleccione **Exportar en CSV** y guarde el archivo.

Supervisión del uso y las licencias de los clientes para Citrix DaaS Standard para Azure

October 2, 2023

Los clientes de **Citrix Service Providers (CSP)** pueden supervisar fácilmente las licencias de Citrix DaaS Standard para Azure para sus usuarios en Citrix Cloud. Como CSP, para acceder a estos datos, inicie sesión en la cuenta de su cliente en Citrix Cloud. Para ver información agregada sobre el uso de licencias en clientes arrendatarios únicos y multiarrendatario, consulte Informes y uso de licencias de los servicios de la nube para Citrix Service Providers.

Los clientes pueden ver sus datos de licencias al seleccionar **Licencias** en el menú de Citrix Cloud.



Asignación de licencias

Modelo de licencias de usuario/dispositivo: Citrix Cloud asigna una licencia cuando un usuario o un dispositivo únicos inician un escritorio por primera vez.

Modelo de licencias de usuario simultáneas: Citrix Cloud asigna una licencia cuando un usuario inicia una aplicación o un escritorio en su dispositivo. Cuando el usuario cierra sesión o se desconecta de la sesión, la licencia ya no se asigna. Dado que la asignación de licencias puede cambiar en función del número de dispositivos que acceden a escritorios en un momento dado, Citrix Cloud evalúa el número de licencias en uso cada cinco minutos.

Para obtener más información sobre el modelo de licencias simultáneas, consulte Licencias simultáneas en la documentación de producto de Licensing.

Resumen de las licencias

Citrix Cloud muestra vistas resumidas de las licencias que se están usando en los modelos de licencias de usuario/dispositivo y de licencias de usuario simultáneas.

Resumen para usuarios y dispositivos

Para el modelo de usuario/dispositivo, el resumen de las licencias proporciona una visión general de las licencias que se están usando en relación con la cantidad total de licencias que usted posea.

El color del porcentaje cambia de verde a amarillo a medida que se aproxima al 100%. El color del porcentaje se vuelve rojo si se excede el 100%.

Citrix Cloud también muestra la relación entre las licencias asignadas y las licencias adquiridas, y la cantidad restante de licencias disponibles.

Resumen para licencias de usuario simultáneas

Para el modelo de licencias simultáneas, el resumen de las licencias proporciona una visión general de esta información:

- Porcentaje del total de licencias adquiridas actualmente en uso cuando Citrix Cloud evaluó por última vez las licencias en uso. Citrix Cloud calcula este porcentaje cada cinco minutos en función de los dispositivos únicos con conexiones activas al servicio. El total de licencias adquiridas es la suma de las licencias que se adquirieron para Citrix DaaS Standard para Azure que utilizan el modelo de licencias simultáneas.
- La relación entre las licencias asignadas actualmente a las licencias adquiridas totales, y la cantidad restante de licencias disponibles. La cifra **Total** que se muestra en esta relación representa la cantidad total de licencias en propiedad actualmente (a partir de la fecha y la hora del último informe).
- Estadísticas de pico de uso. Al calcular el pico de licencias en uso, Citrix Cloud obtiene el máximo de licencias utilizadas en los siguientes períodos de tiempo:
  - **Últimas 24 horas:** El máximo de licencias utilizadas simultáneamente durante las últimas 24 horas.
  - **Este mes:** El máximo de licencias utilizadas simultáneamente en el mes del calendario actual.
  - **Siempre:** El máximo de licencias utilizadas simultáneamente desde el inicio de la suscripción.

La cifra **Total** mostrada para estos períodos de pico de uso representa el total de licencias en propiedad en ese momento. Si el total de licencias en propiedad aumenta o disminuye y hay un aumento correspondiente en las licencias asignadas, la cifra **Total** cambia para reflejar la nueva cantidad de licencias en propiedad en ese momento. Sin embargo, si no hay un pico de uso correspondiente, la cifra **Total** no cambia.

Calcular el pico de licencias en uso

Para reflejar con precisión el modelo de licencias simultáneas, Citrix Cloud cuenta la cantidad de dispositivos únicos que han accedido al servicio de forma simultánea cada cinco minutos. Si el recuento es mayor que el pico de uso actual que se muestra, Citrix Cloud muestra el nuevo pico de uso con la fecha y la hora en que se alcanzó. Si el recuento es menor que el pico de uso actual, el pico de uso actual no cambia.

Tendencias de uso

Citrix Cloud muestra un desglose de las tendencias de uso de las licencias de usuario/dispositivo y de las licencias de usuario simultáneas. Para ver este desglose, seleccione **Ver detalles de uso** en la página de resumen de las licencias.

Tendencias para usuarios y dispositivos

En el caso de las licencias de usuario/dispositivo, la sección **Tendencias de uso** muestra un desglose de las licencias asignadas en forma de gráfico.

Al señalar un intervalo en el gráfico, se muestra esta información:

- **Total de licencias:** La cantidad total de licencias que ha comprado del servicio de la nube para todos los derechos incluidos.
- **Asignadas previamente:** La cantidad de licencias asignadas en el mes anterior. Por ejemplo, un usuario accede al servicio de la nube por primera vez en julio y se le asigna una licencia. Esta licencia se cuenta como "Asignada recientemente"para el mes de julio. Para el mes de agosto, esta licencia se cuenta como "Asignada previamente".
- **Asignadas recientemente:** La cantidad de licencias nuevas que se asignaron cada mes. Por ejemplo, un usuario accede al servicio de la nube por primera vez en julio y se le asigna una licencia. Esta licencia se cuenta como "Asignada recientemente"para el mes de julio.

Tendencias para licencias de usuario simultáneas

En el caso de las licencias de usuario simultáneas, la sección **Tendencias de uso** muestra esta información:

- **Total de licencias:** El total de licencias simultáneas adquiridas.
- **Pico de licencias en uso:** El máximo de licencias asignadas para el intervalo de fechas seleccionado. De forma predeterminada, Citrix Cloud muestra el pico de uso para cada mes del año natural actual. Para ver un desglose del pico de uso mensual o por horas, seleccione el mes o día del calendario que quiere ver en el menú desplegable.

  Si el intervalo de fechas seleccionado aún no ha terminado, Citrix Cloud muestra el pico de uso actual del último intervalo de tiempo. Por ejemplo, si desglosa un día natural que aún está en curso, se muestra el máximo de licencias por cada hora hasta el momento actual. Si el máximo de licencias aumenta en el siguiente intervalo de cinco minutos, Citrix Cloud actualiza el pico de uso de la hora actual.

Al señalar un intervalo en el gráfico, se muestran el total de licencias y los picos de licencias en uso durante ese intervalo.

Informes de uso

Puede descargar información de uso sobre un intervalo estándar o uno concreto.
La información incluye el uso de medidores para:

- Máquinas virtuales de Azure
- Conexiones de red, como el emparejamiento de redes virtuales
- Elementos de almacenamiento de Azure, como discos administrados, blobs en bloques y blobs en páginas

Los datos pueden tardar hasta 72 horas después del final de un día o mes en reflejar todo el uso.

En **Informes de uso**, seleccione un intervalo y, a continuación, seleccione **Descargar datos** para generar y descargar un archivo CSV en su máquina local.

Usuarios con licencias

Para las licencias de usuario/dispositivo, la sección **Actividad de licencias** muestra una lista de los usuarios clientes individuales que tienen licencias asignadas durante el mes actual. Esta lista también muestra el dominio al que pertenece cada usuario, la fecha en que se asignó la licencia y la última vez que se utilizó el servicio. Esta sección no está disponible para las licencias de usuario simultáneas.

Liberación mensual de licencias

El primer día de cada mes, las licencias asignadas del mes anterior se liberan automáticamente. Cuando esto ocurre, la cantidad de licencias asignadas se restablece a cero y se borra la lista de usuarios clientes con licencias. Las licencias se reasignan cuando los usuarios inician aplicaciones o escritorios por primera vez en el nuevo mes.

Revisar el historial de licencias mensuales

El primer día de cada mes, la lista de usuarios clientes con licencias del mes anterior, en **Actividad de licencias**, se borra cuando la cantidad de licencias asignadas se restablece a cero. Sin embargo, puede acceder a los datos de usuario de los meses anteriores en cualquier momento y descargarlos como un archivo CSV, si fuera necesario.

1. En la sección **Actividad de licencias**, seleccione **Ver historial de licencias** en el extremo derecho de la sección.
2. Seleccione el mes que quiere ver. Aparecerá una lista con los detalles de usuario del mes seleccionado.
3. Para exportar la lista, seleccione **Exportar en CSV** en el extremo derecho de la sección y, a continuación, guarde el archivo.

Exportar detalles de las licencias

Puede exportar, en cualquier momento, detalles de usuarios con licencia de un solo cliente en un archivo CSV para un análisis más exhaustivo. A continuación, puede usar el archivo CSV como quiera para analizar los detalles de la licencia.

Para exportar los detalles del mes actual, en la sección **Actividad de licencias**, seleccione **Exportar en CSV** en el extremo derecho de la sección y, a continuación, guarde el archivo.

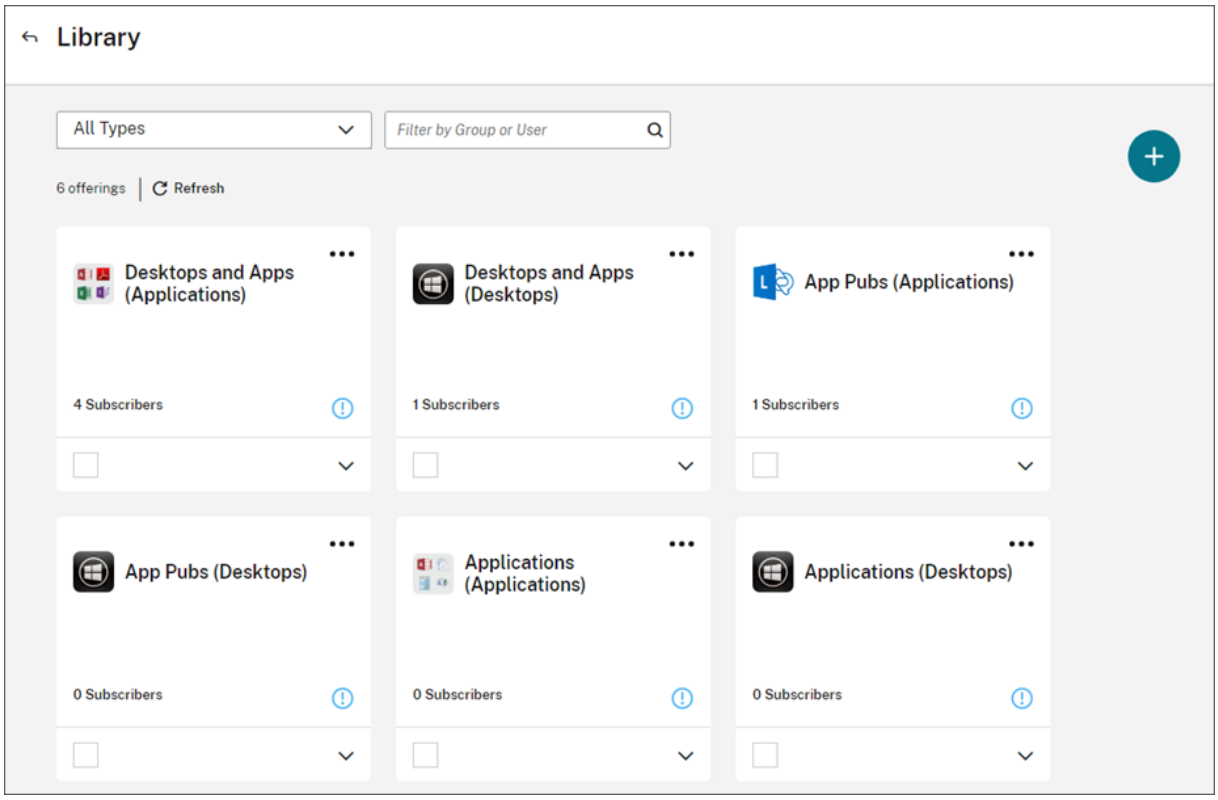
Para exportar los detalles de los meses anteriores, genere una lista para un mes seleccionado tal y como se describe en Revisar el historial de licencias mensuales. Seleccione **Exportar en CSV** y guarde el archivo.

Asignar usuarios y grupos a ofertas de servicios desde la biblioteca

April 26, 2024

> **Nota:**
>
> En el caso de los grupos de entrega de *administrados por Citrix Cloud*, las asignaciones de usuarios ahora se pueden administrar directamente en la consola de Web Studio. Para obtener más información, consulte la documentación de DaaS. Anteriormente, la administración de estos grupos de entrega se limitaba a la biblioteca, pero ahora se pueden usar las mismas capacidades de administración en la consola de Web Studio. Esta función ya está disponible para todos los clientes. En junio de 2024, los casos de uso específicos de DaaS en Cloud Library se retirarán en su totalidad.

Los recursos y otros elementos que se configuran en un servicio pueden asignarse a usuarios y grupos de Active Directory mediante la Biblioteca. Las ofertas pueden incluir aplicaciones, escritorios, recursos de datos compartidos y aplicaciones web que se crean mediante un servicio de Citrix. La biblioteca muestra todas las ofertas en una vista única.



Acceso de administrador

Para acceder a la biblioteca, los administradores deben cumplir estos requisitos:

- Autenticarse mediante el proveedor de identidades de Citrix o Azure AD.
- Iniciar sesión como administrador individual, no como miembro de un grupo de administradores.

- Tener acceso completo a Citrix Cloud o acceso personalizado con la función Biblioteca seleccionada.

Si tiene cuentas de administrador individuales y de grupo en Citrix Cloud, es posible que su acceso a la Biblioteca dependa de los permisos vigentes al iniciar sesión con cada cuenta. Para obtener más información, consulte Permisos resultantes para administradores con identidades de Citrix, AD, Azure AD y Google Cloud.

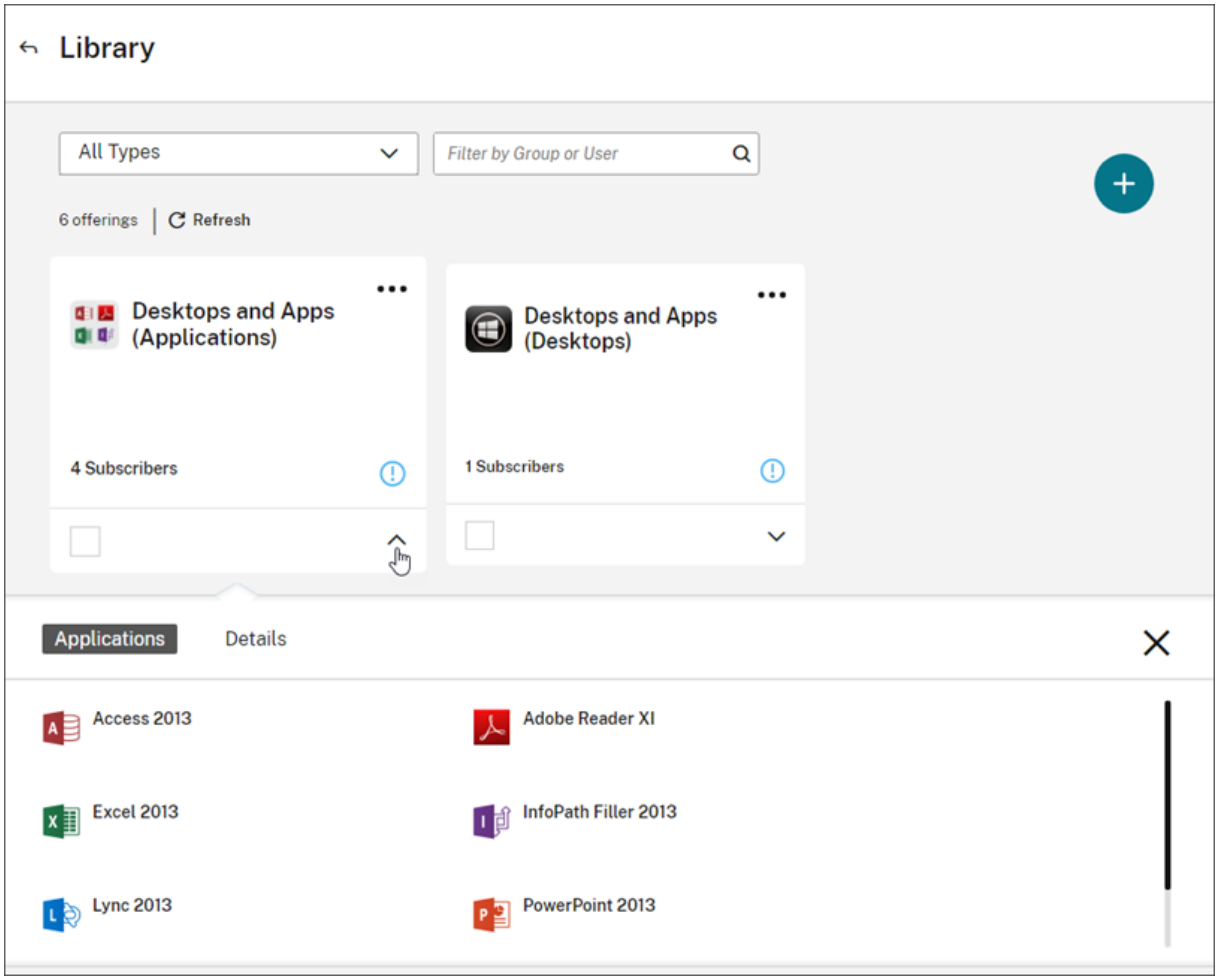
Consideraciones sobre el uso de StoreFront con Citrix DaaS

Si utiliza una instancia de StoreFront local con Citrix DaaS, no utilice Biblioteca para asignar recursos al crear grupos de entrega. En su lugar, use Studio para asignar recursos a los usuarios. Si utiliza Biblioteca en este caso, es posible que los recursos no se enumeren para los usuarios.

Al crear un grupo de entrega en Studio, en la página **Usuarios**, no seleccione **Dejar a Citrix Cloud la administración de usuarios**. En su lugar, seleccione una opción diferente (**Permitir que los usuarios autenticados usen este grupo de entrega** o **Restringir el uso de este grupo de entrega a los siguientes usuarios**).

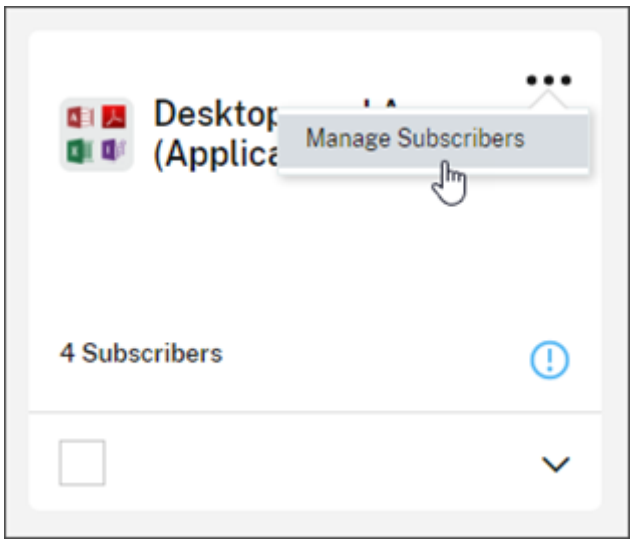
Ver los detalles de las ofertas

Para ver las aplicaciones, los escritorios, las directivas y cualquier otra información relacionada con la oferta, haga clic en la flecha situada en la tarjeta de la oferta.

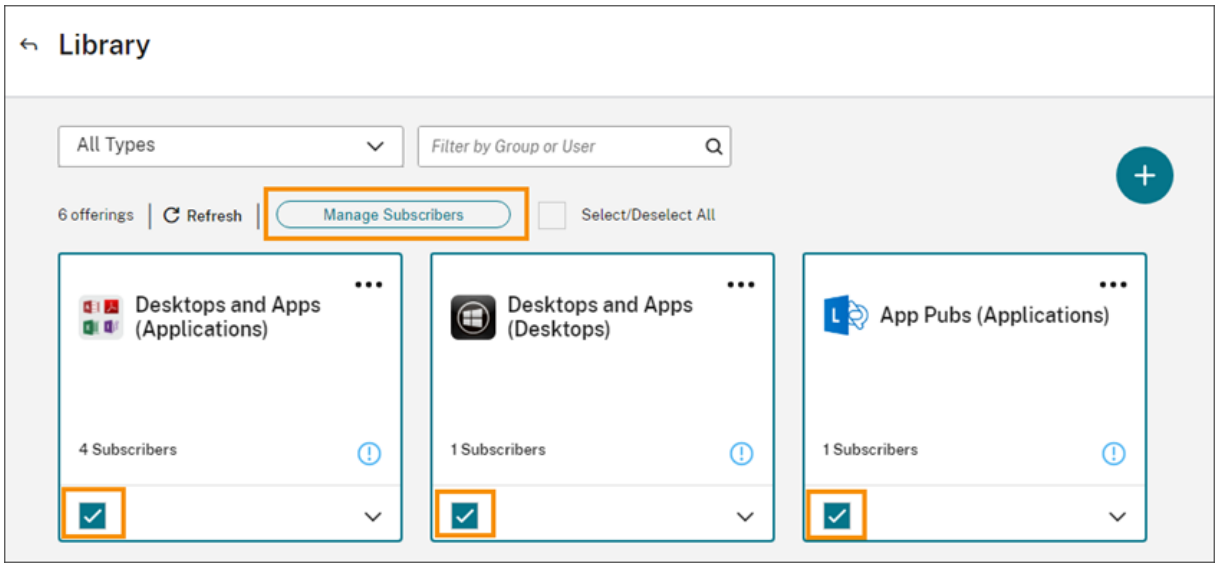


Agregar o quitar suscriptores

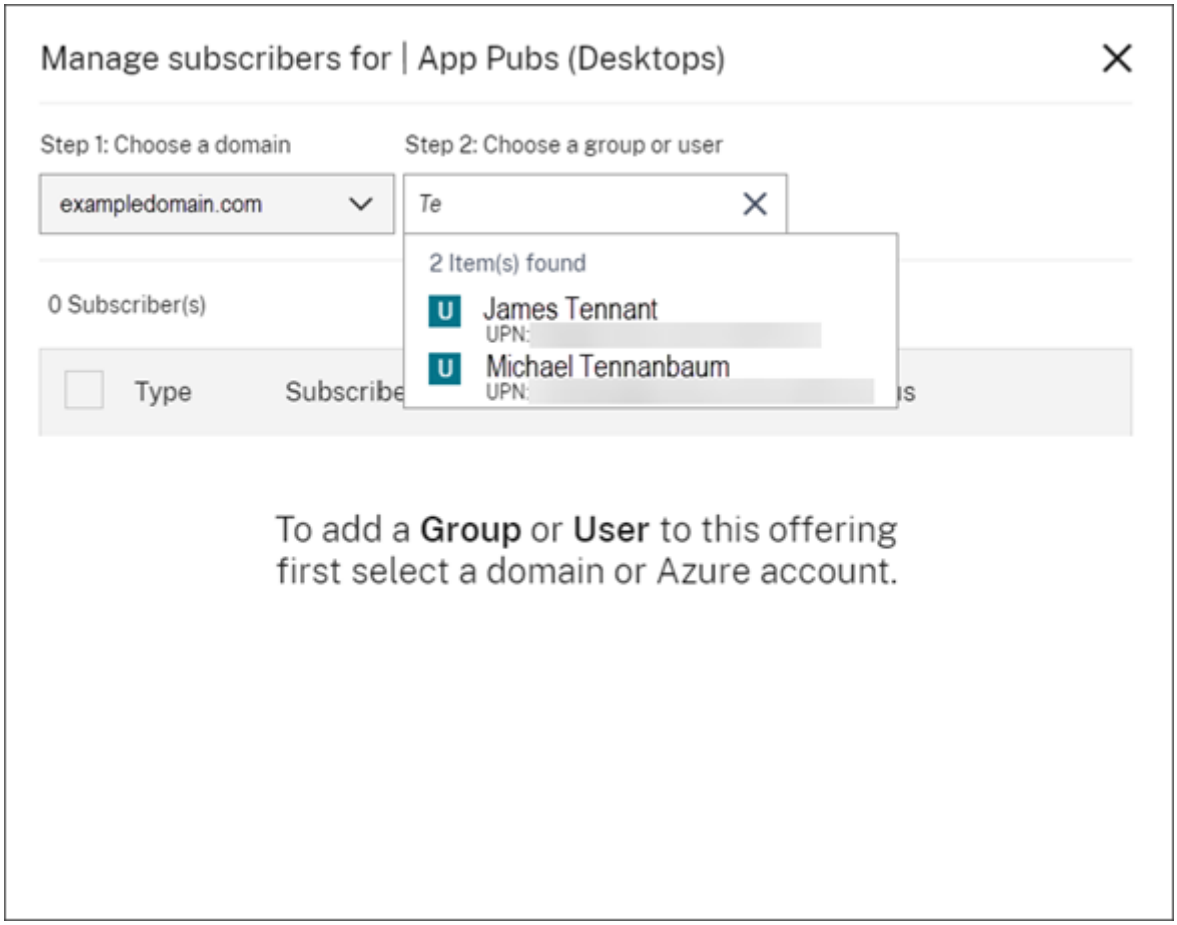
Para administrar usuarios o grupos para una misma oferta, haga clic en **Administrar suscriptores** desde el menú de la tarjeta de la oferta.



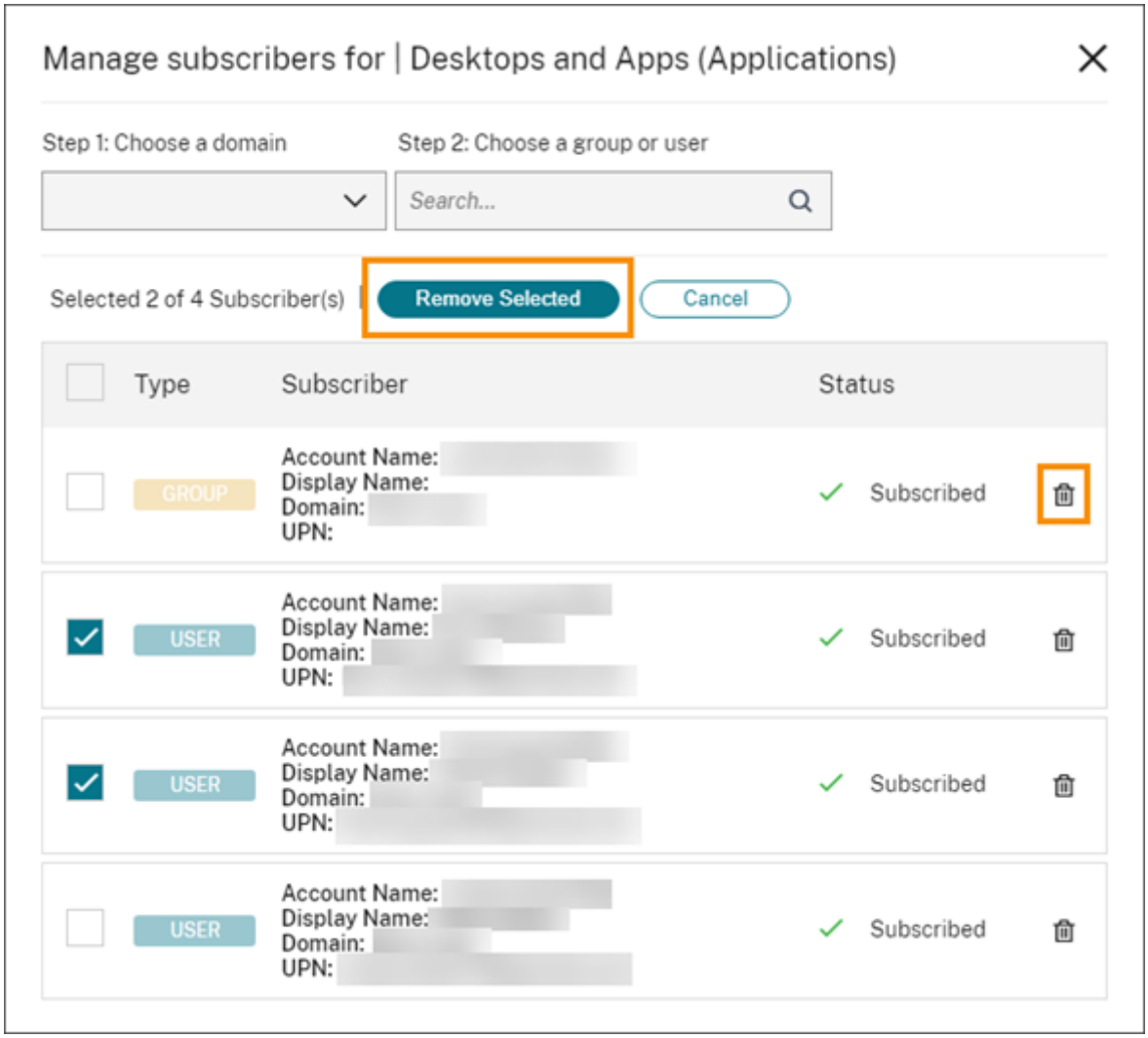
Para administrar suscriptores para varias ofertas, marque la casilla junto a las ofertas que quiera, y haga clic en **Administrar suscriptores**.



Para agregar suscriptores a la oferta, elija un dominio y, a continuación, seleccione los usuarios o los grupos que quiera agregar.



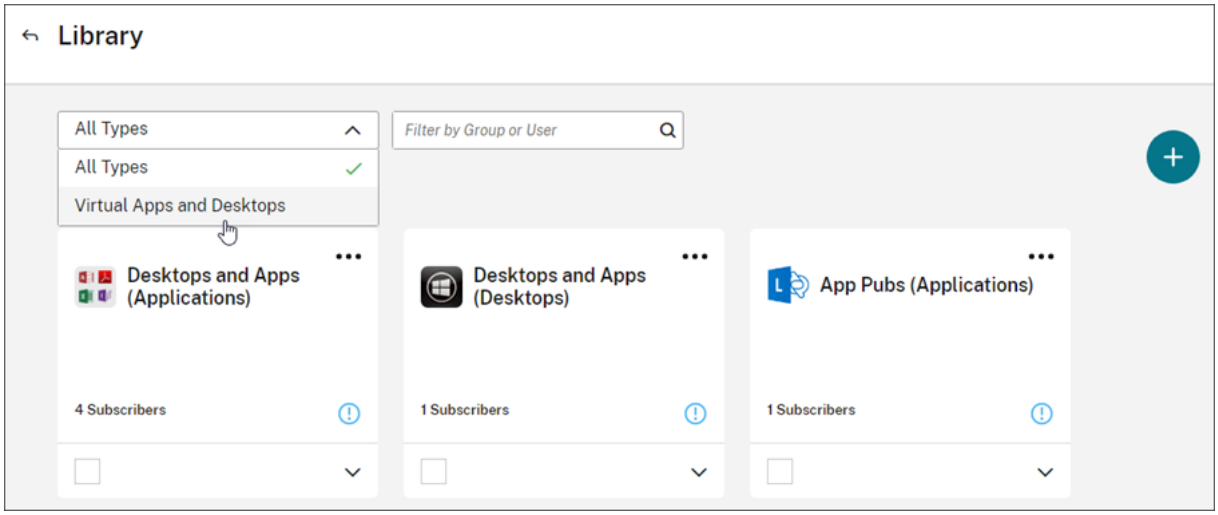
Para quitar un único suscriptor, haga clic en el icono de papelera correspondiente al usuario o grupo en cuestión. Para quitar varios suscriptores, seleccione los usuarios o grupos y haga clic en **Quitar seleccionados**.



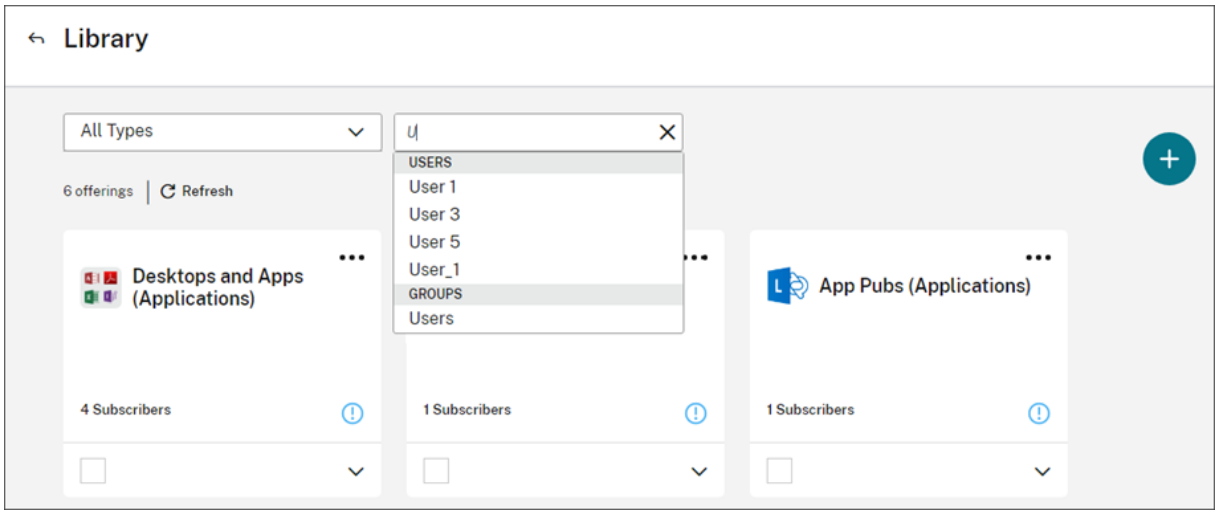
Después de agregar o quitar suscriptores en una oferta, la tarjeta de la oferta muestra la cantidad actual de suscriptores.

Filtrar las ofertas

De forma predeterminada, la biblioteca muestra todas las ofertas. Para ver rápidamente las ofertas de un servicio específico, seleccione el filtro para ese servicio.



También puede hacer una búsqueda de un usuario o un grupo que esté suscrito actualmente a una oferta de la biblioteca. Citrix Cloud muestra solo las ofertas del usuario o grupo seleccionado. Para ver todas las ofertas para todos los usuarios, haga clic en la X para borrar el filtro.



Página de destino personalizada

April 5, 2024

Muchos administradores acceden a Cloud Console para realizar tareas específicas, como administrar aplicaciones en la consola de Web Studio o ver datos en DaaS - Monitor.
No obstante, estas tareas requieren varios clics y la navegación por varias páginas cada vez que los administradores inician sesión, lo que puede llevar bastante tiempo. Esta nueva función permite a los administradores establecer o modificar una página de destino personalizada, lo que ahorra tiempo y proporciona una experiencia de uso de la consola mejorada.

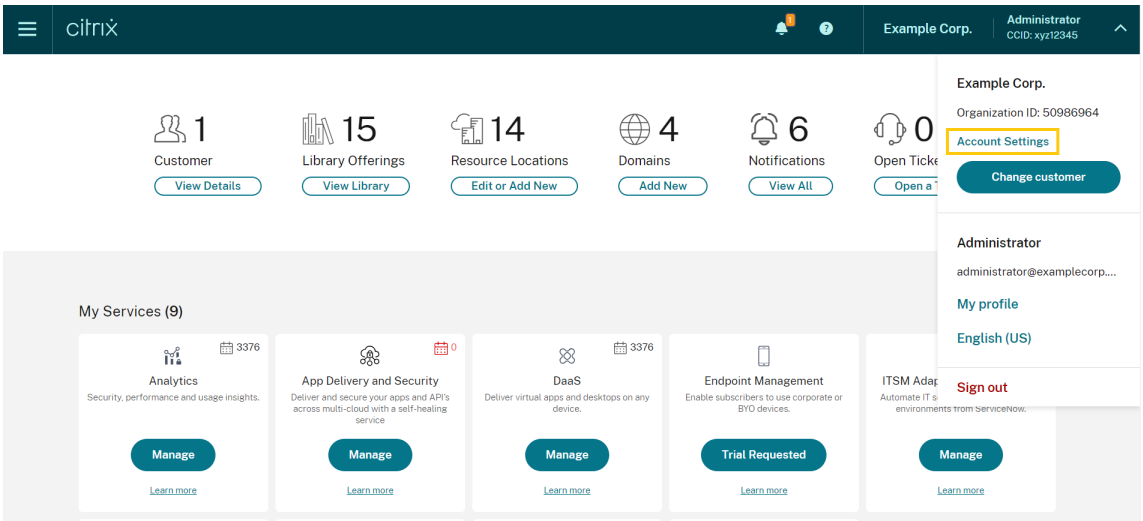
Actualmente, las siguientes páginas están disponibles para configurarlas como páginas de destino personalizadas y se espera que se agreguen más en el futuro:

- DaaS
- DaaS-Monitor
- NetScaler Console
- CAS
- Seguridad de CAS
- Rendimiento de CAS
- WEM
- General

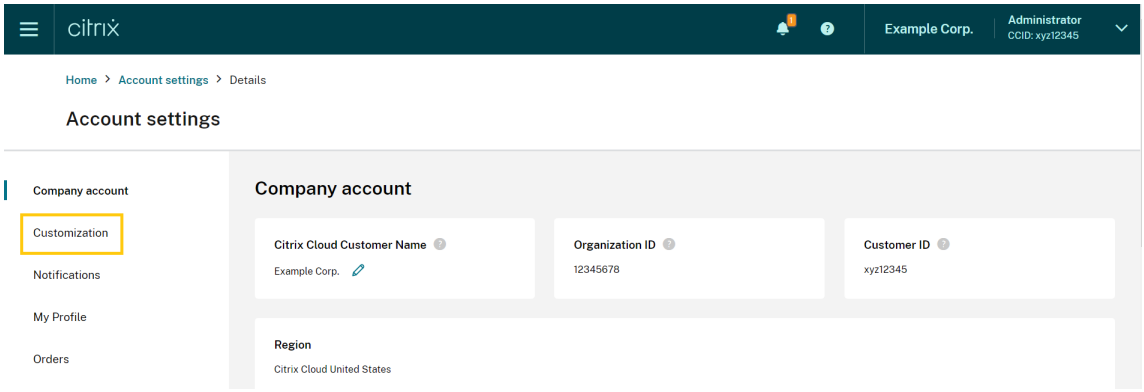
> **Nota:**
>
> La configuración de la página de destino personalizada es opcional y se establece para cada cuenta. Así, cada administrador puede personalizar su propia experiencia en Citrix Cloud. Todos los administradores (ya sean personalizados o totales) tienen acceso a esta función.

Configurar una página de destino personalizada

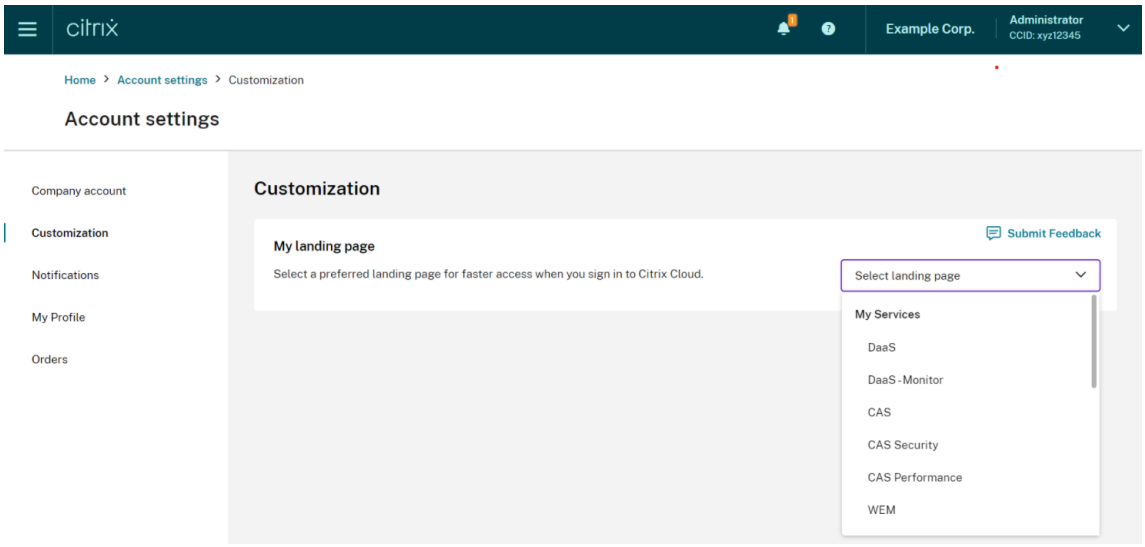
1. Haga clic en el nombre del perfil y seleccione **Parámetros de cuenta**.



2. Haga clic en **Personalización**.



3. Seleccione el servicio que quiere configurar como página de destino personalizada.



4. Haga clic en **Aplicar**.

   Su página de destino personalizada ahora está configurada.

> **Nota:**
>
> - Para restablecer en cualquier momento su página de destino personalizada a la página de inicio predeterminada de la nube, haga clic en **Restablecer predeterminada**.
> - Si vuelve a iniciar sesión en la misma página en la que acaba de cerrar sesión, accederá a la última página que visitó en vez de ir a su nueva página de destino.

Permitir a los clientes eliminar la cuenta de Citrix Cloud y volver a incorporarla

April 26, 2024

Citrix Cloud ofrece a los clientes la posibilidad de eliminar de forma segura su cuenta de Citrix Cloud y volver a incorporarla sin problemas cuando sea necesario.

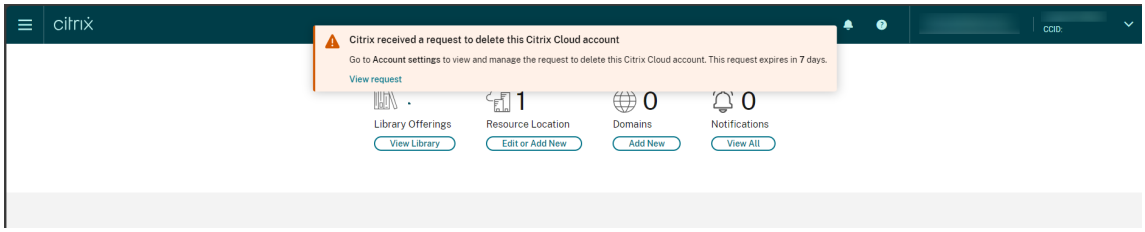
Requisitos previos

- Si su cuenta tiene derechos de DaaS activos y su entorno de DaaS está aprovisionado, contacte con el servicio de asistencia técnica de Citrix para ejecutar Desmantelamiento rápido antes de continuar. Consulte el artículo La consola de Studio muestra "Habilitar DaaS"al usarla por primera vez para obtener más información sobre cómo comprobar si su entorno de DaaS está aprovisionado.
- Elimine todos los Cloud Connector y Connector Appliance asociados a esta cuenta.

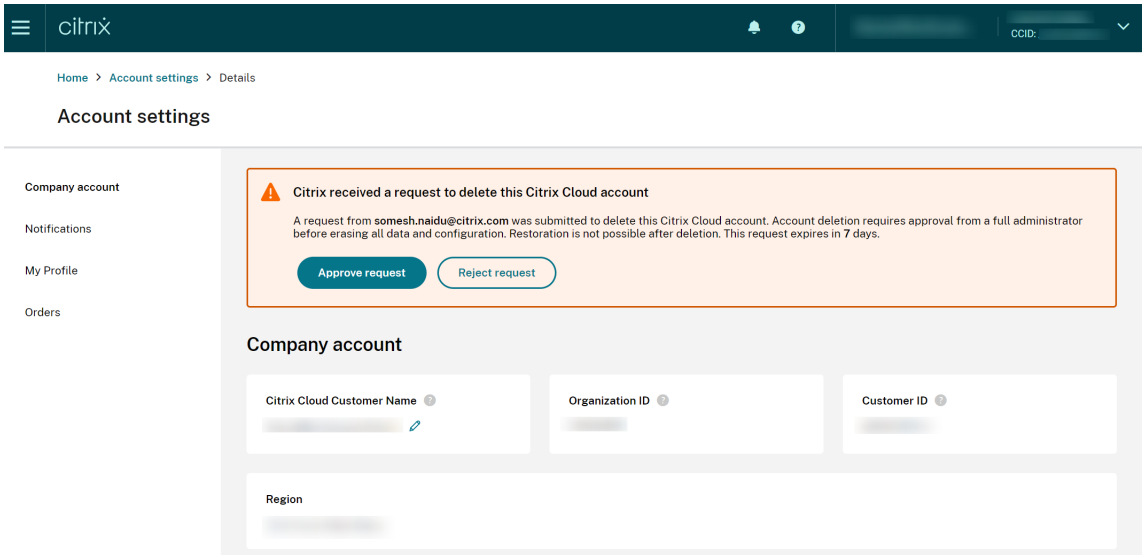
> **Importante**
>
> Tenga en cuenta los siguientes puntos antes de eliminar una cuenta de Citrix Cloud:
>
> - Se eliminan de las bases de datos de Citrix todos los datos relacionados con el cliente.
> - Se eliminarán todos los recursos relacionados con los servicios de Citrix Cloud, incluidas las máquinas virtuales administradas por Citrix, que Citrix aprovisionó en su entorno de nube. Consulte en Servicios de Citrix Cloud la descripción de los componentes administrados por Citrix que se incluyen en servicios específicos de Citrix Cloud.
> - El acceso de administradores y usuarios a Citrix Cloud y a los servicios está inhabilitado.
> - Los administradores o usuarios que utilicen activamente el servicio sufrirán interrupciones del servicio.
> - Esta acción no es reversible. Una vez borrados los datos, no se pueden recuperar.

Pasos

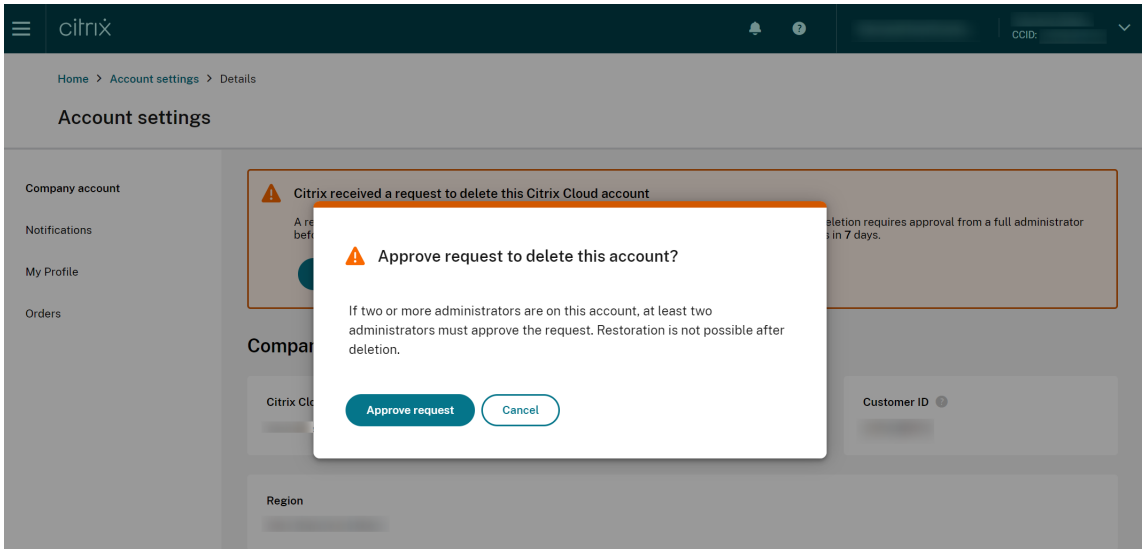
1. Póngase en contacto con el Servicio de atención al cliente de Citrix para enviar una solicitud de eliminación. Para enviar esta solicitud, se necesita un *Administrador total* de la cuenta de Citrix Cloud.
2. Una vez iniciada la solicitud, inicie sesión en su cuenta de Citrix Cloud. Allí verá el flujo de trabajo de eliminación de la cuenta de Citrix Cloud.



3. Siga las instrucciones que se muestran en pantalla para aprobar o rechazar esta solicitud.



4. Para aprobar esta solicitud de eliminación, inicie sesión en la cuenta, vaya a **Parámetros de cuenta** y haga clic en **Aprobar solicitud** en la pancarta del flujo de trabajo de aprobación.



Para cancelar la solicitud de eliminación, inicie sesión en la cuenta, vaya a **Parámetros de cuenta** y haga clic en **Rechazar y eliminar la solicitud** en la pancarta del flujo de trabajo de eliminación de aprobación.

> **Nota:**
>
> - Si esta cuenta tiene dos o más administradores asociados, al menos dos administradores deben aprobar la solicitud.
> - Esta solicitud caduca si no se reciben las aprobaciones necesarias en un plazo de 7 días.

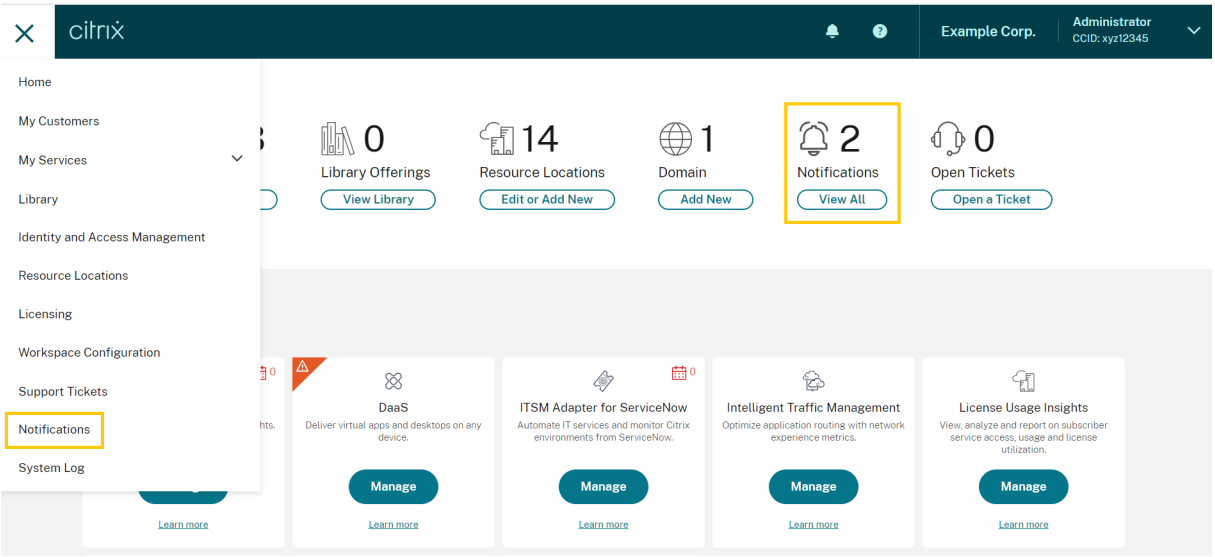
Notificaciones

October 2, 2023

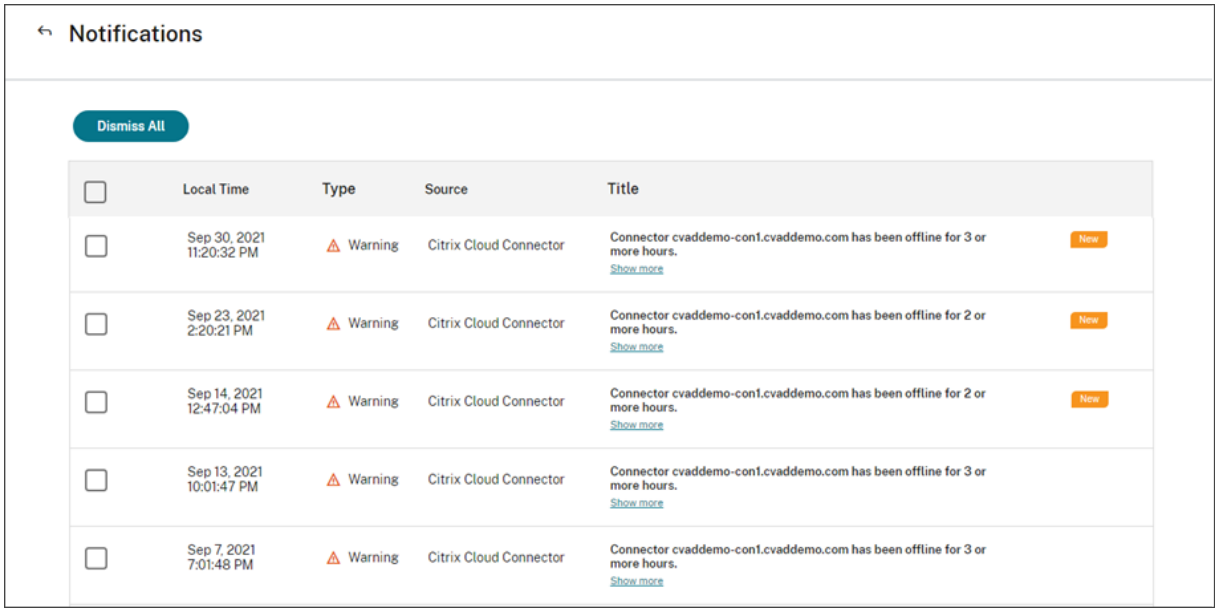
Las notificaciones proporcionan información sobre los problemas o eventos que pueden ser de interés para los administradores, tales como nuevas funciones de Citrix Cloud, o problemas de una máquina en una ubicación de recursos. Las notificaciones pueden proceder de cualquier servicio de Citrix Cloud.

Ver notificaciones

La cantidad de notificaciones aparece en la parte superior de la página de la consola de Citrix Cloud. Para obtener más información, en la consola, haga clic en **Ver todo** debajo de **Notificaciones**, o seleccione **Notificaciones** en el menú de la consola.



La página Notificaciones muestra las notificaciones que recibe. Las notificaciones más recientes están en la parte superior de la lista.

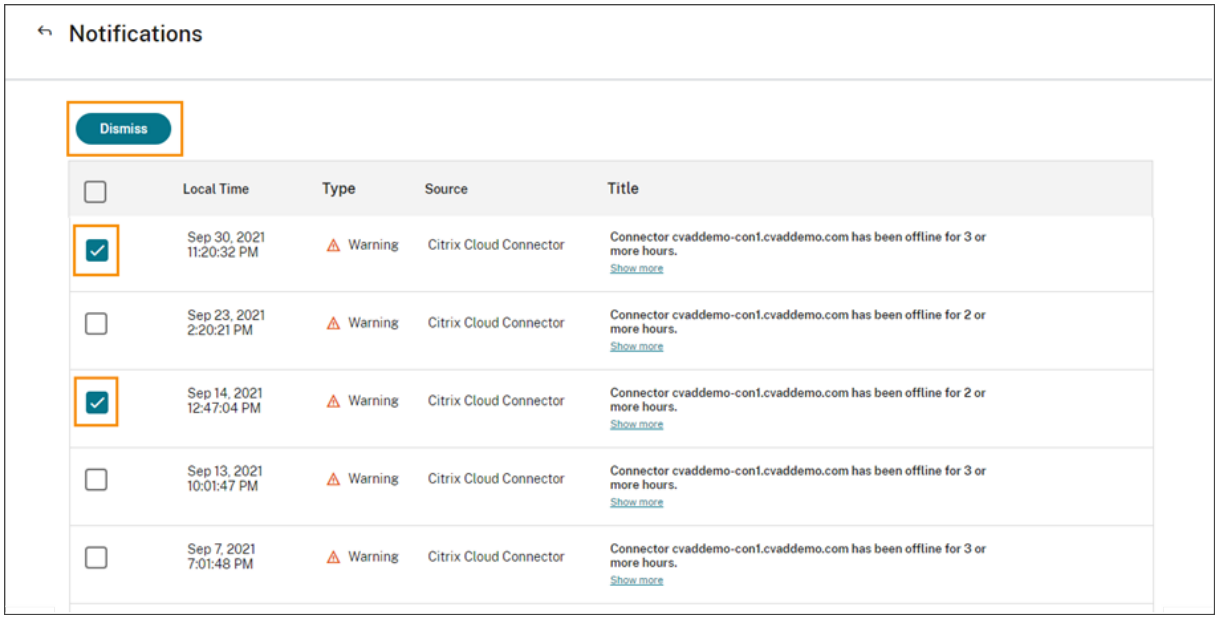


Descartar notificaciones

Los administradores gestionan las notificaciones. Al descartar las notificaciones, usted las ignora con su propia identidad de administrador en Citrix Cloud. Otros administradores pueden seguir viendo y descartando sus propias notificaciones, aunque usted las descarte todas.

Para descartar todas las notificaciones que haya recibido, seleccione **Descartar todo** en la parte superior de la página.

Para descartar notificaciones individuales, seleccione cada notificación y, a continuación, seleccione **Descartar**.



Recibir notificaciones por correo electrónico

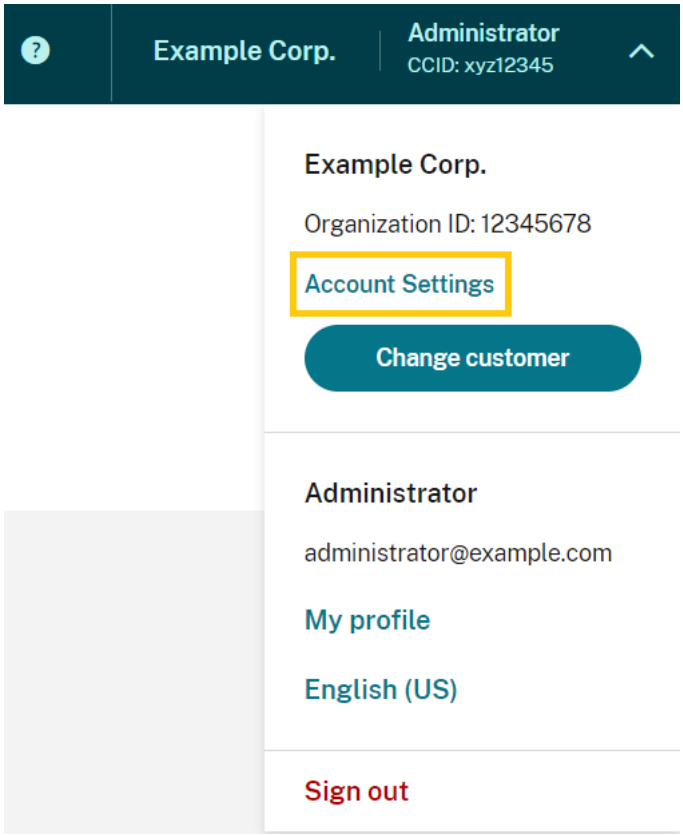
Puede elegir recibir notificaciones por correo electrónico en lugar de iniciar sesión para verlas. De forma predeterminada, las notificaciones por correo electrónico están desactivadas.

También puede habilitar las notificaciones por correo electrónico para otras partes interesadas que no tengan acceso de administrador a su cuenta de Citrix Cloud, como los miembros de los equipos de seguridad y auditoría de su organización.

Cuando habilita las notificaciones por correo electrónico, Citrix Cloud envía un correo electrónico por cada notificación. Las notificaciones se envían lo antes posible. No se agrupan en un solo correo electrónico ni se agrupan para enviar en otro momento.

Para habilitar sus notificaciones por correo electrónico

1. Desde la consola de administración de Citrix Cloud, haga clic en **Parámetros de cuenta**.



2. Seleccione **Notificaciones**.
3. Active el parámetro **Mis notificaciones de correo**.
4. En **Administrar parámetros de mis notificaciones**, seleccione los tipos de notificaciones que quiera recibir. Se seleccionan todos los tipos de notificaciones de forma predeterminada.

5. Haga clic en **Aplicar** para guardar los parámetros.

Para habilitar notificaciones por correo electrónico para usuarios que no son administradores

Siga los pasos de esta sección para agregar usuarios que no son administradores como contactos para las notificaciones enviadas por correo electrónico. Si intenta agregar como contacto un administrador que ya existe, Citrix Cloud muestra un error.

1. Desde la consola de administración de Citrix Cloud, haga clic en **Parámetros de cuenta**.
2. Seleccione **Notificaciones**.
3. En **Administración de contactos**, seleccione **Agregar contacto**.
4. Introduzca el nombre, la dirección de correo electrónico y el idioma de preferencia del contacto.
5. En **Administrar parámetros de notificaciones**, seleccione los tipos de notificaciones que quiera enviar.
6. Seleccione **Agregar contacto** para guardar la información del contacto.

Modificar parámetros de notificaciones

Como administrador, para cambiar los tipos de notificaciones que reciba, solo debe marcar o desmarcar las casillas de **Administrar parámetros de mis notificaciones**. Cambiar sus notificaciones no afecta a las notificaciones que reciban otros administradores.

También puede modificar las notificaciones que reciben los usuarios que no son administradores.

Para modificar las notificaciones de usuarios que no son administradores

1. Desde la consola de administración de Citrix Cloud, haga clic en **Parámetros de cuenta**.
2. Seleccione **Notificaciones**.
3. En **Administración de contactos**, busque el contacto que quiera administrar.
4. Apunte al contacto y, a continuación, seleccione el icono del lápiz.
5. En **Administrar parámetros de notificaciones**, seleccione o desmarque las casillas de cada tipo de notificación.

Para modificar la dirección de correo electrónico de un contacto, primero debe eliminar el contacto y, a continuación, agregarlo como un contacto nuevo con su nueva dirección de correo electrónico.

Inhabilitar notificaciones por correo electrónico

Como administrador, para inhabilitar sus propias notificaciones enviadas por correo electrónico en un momento dado, desactive el parámetro **Mis notificaciones de correo**.

Para que los usuarios que no son administradores dejen de recibir notificaciones, haga clic en el enlace de cancelación de suscripción que aparece en cada correo electrónico de notificación. Los contactos que han cancelado la suscripción a los correos tienen el estado de notificación **No suscrito** en la tabla de la sección **Administración de contactos**.

Para inhabilitar las notificaciones de usuarios que no son administradores, puede hacer lo siguiente:

- Desactive todas las casillas de **Administrar parámetros de notificaciones** del contacto.
- Elimine el contacto de la tabla de **Administración de contactos**.

Eliminar contactos que no son administradores

1. Desde la consola de administración de Citrix Cloud, haga clic en **Parámetros de cuenta**.
2. Seleccione **Notificaciones**.
3. En **Administración de contactos**, busque el contacto que quiera administrar.
4. Apunte al contacto y, a continuación, seleccione el icono de la papelera.

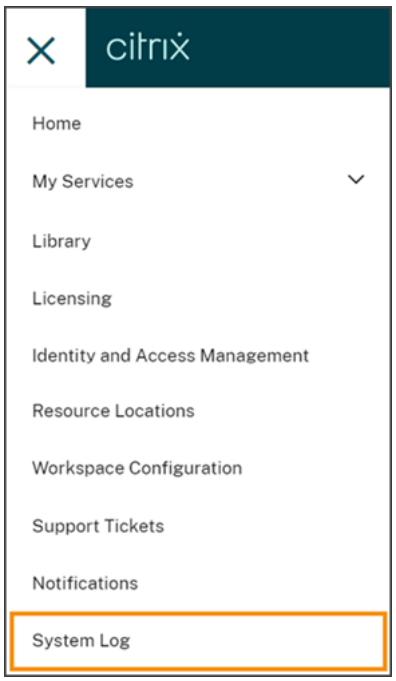
Citrix Cloud quita el contacto de la tabla.

Registro del sistema

October 2, 2023

El registro del sistema muestra una lista con marca de hora de los eventos ocurridos en Citrix Cloud. Puede exportar estos cambios en formato de archivo CSV para cumplir con los requisitos de cumplimiento normativo de su organización o reforzar los análisis de seguridad.

Para ver el registro del sistema, seleccione **Registro del sistema** en el menú de Citrix Cloud.

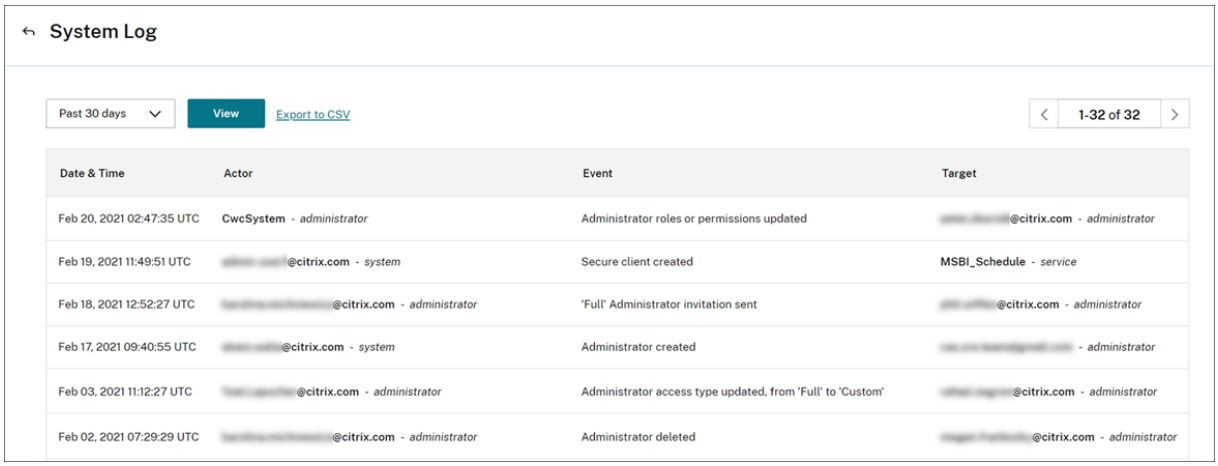


Para obtener más información sobre la retención de datos en los registros del sistema, consulte Retención de datos en este artículo.

Eventos registrados

El registro del sistema captura eventos de ciertas operaciones de la plataforma Citrix Cloud y de los servicios de la nube. Para obtener una lista completa de estos eventos y de las descripciones de los datos capturados, consulte Referencia de eventos del registro del sistema.

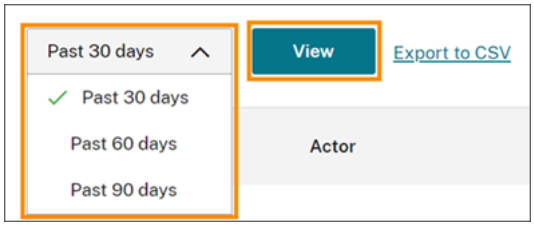
De forma predeterminada, el registro del sistema muestra los eventos ocurridos en los últimos 30 días. Los eventos más recientes se muestran primero.



La lista que se muestra incluye la siguiente información:

- Fecha y hora (UTC) en que se produjo el evento.
- Agente que inició el evento, como un administrador o un cliente seguro. Las entradas con el agente **CwcSystem** indican que Citrix Cloud realizó la operación.
- Breve descripción del evento, como modificar un administrador o crear un nuevo cliente seguro.
- Objetivo del evento. El objetivo es el objeto del sistema que se ha visto afectado o modificado como resultado del evento. Por ejemplo, un usuario que se ha agregado como administrador.

Para ver los eventos ocurridos hace más de 30 días, filtre la lista seleccionando el periodo de tiempo que quiere ver y seleccione **Ver**. Puede ver, como máximo, los eventos ocurridos hace 90 días.

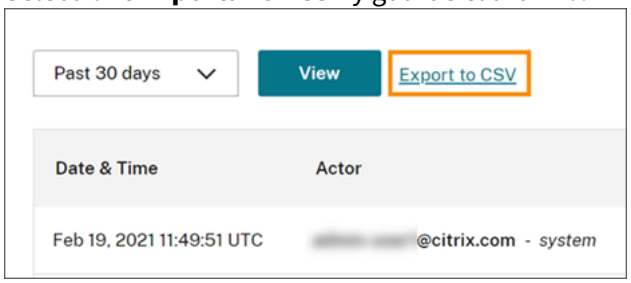


Para recuperar eventos antiguos ocurridos durante un período de tiempo especificado, puede utilizar la API de SystemLog. Para obtener más información, consulte Recuperar eventos de un período de tiempo específico en este artículo.

Exportar eventos

Puede exportar un archivo CSV con eventos de registro del sistema ocurridos en los últimos 90 días. El nombre del archivo descargado sigue el formato `SystemLog-CustomerName-OrgID-DateTimeStamp.csv`.

1. En el menú de Citrix Cloud, seleccione **Registro del sistema**.
2. Si es necesario, filtre la lista para mostrar el período de tiempo del que quiere exportar eventos.
3. Seleccione **Exportar en CSV** y guarde el archivo.



El archivo CSV incluye la siguiente información:

- Marca de hora UTC de cada evento
- Detalles del agente que inició el evento, incluidos el nombre e ID del mismo.
- Detalles del evento, como el tipo de evento y el texto del evento

- Detalles del objetivo del evento, como el ID de destino, el nombre del administrador o un cliente seguro.

Recuperar eventos de un período de tiempo específico

Si necesita recuperar eventos de periodos de tiempo específicos, puede utilizar la API de SystemLog. Antes de utilizar la API, tendrá que crear un cliente seguro tal y como se describe en Getting Started, en el sitio web de documentación de Citrix Developer.

Para obtener más información sobre el uso de la API de SystemLog, consulte Citrix Cloud-SystemLog en el sitio web de documentación de Citrix Developer.

Reenviar eventos de registro del sistema

El complemento Citrix System Log Add-on for Splunk le permite conectar su instancia de Splunk con Citrix Cloud. Con esta conexión, puede reenviar los datos de registro del sistema a Splunk. Para obtener más información, consulte la documentación del complemento en el repositorio de Citrix en GitHub.

Retención de datos

Citrix comparte la responsabilidad con usted, el cliente, de conservar los datos de registro del sistema que Citrix Cloud captura.

Citrix conserva los registros del sistema durante 90 días después de que se registren los eventos correspondientes.

Usted es responsable de descargar los registros del sistema que quiere conservar para cumplir con los requisitos de conformidad de su organización y de almacenar estos registros en una solución de almacenamiento a largo plazo.

Referencia de eventos del registro del sistema

October 2, 2023

Para ver todos los datos de eventos del registro del sistema de su cuenta de Citrix Cloud, puede:

- Descargar un archivo CSV de todos los eventos que ocurrieron durante los 30, 60 o 90 días anteriores.
- Usar la API de SystemLog para obtener eventos durante un período de tiempo específico.

Consulte Descripciones de datos de eventos en este artículo para obtener descripciones de los datos que se capturan al obtener eventos del registro del sistema. Consulte Servicios y componentes de la nube que generan eventos para ver valores de eventos específicos, como el texto del mensaje del evento, los tipos de eventos o si los datos de los campos de objetos se registran antes y después de que ocurran los eventos.

Servicios y componentes de la nube que generan eventos

El registro del sistema registra eventos de estas entidades, componentes y servicios de Citrix Cloud:

- Plataforma Citrix Cloud: Eventos relacionados con las funciones de la plataforma Citrix Cloud, como la gestión de administradores, el restablecimiento de dispositivos para suscriptores de Workspace, los arrendatarios de Azure AD y la administración de dominios y ubicaciones de red.
- Conectores: Eventos relacionados con el registro y la actualización de Citrix Cloud Connectors y Connector Appliances.
- Licencias: Eventos relacionados con el registro de servidores de licencias locales, la administración de licencias asignadas para los servicios de la nube y la exportación de datos de licencias.
- Secure Private Access Service: Eventos relacionados con las configuraciones de Secure Private Access Service.
- Citrix Workspace: Eventos relacionados con los parámetros de Configuración de Workspace.

Descripción de datos de eventos

Al descargar eventos del registro del sistema o al obtenerlos mediante la API de SystemLog, se incluyen estos datos:

- **RecordID:** El identificador único del evento.
- **UtcTimestamp:** La fecha y la hora en UTC en que se produjo el evento.
- **CustomerID:** El identificador único de la organización de la cuenta de Citrix Cloud.
- **EventType:** El identificador del tipo de evento que se registró. El tipo de evento se graba con el formato `OriginatingService`/`Actor`/`Action`. Por ejemplo, el tipo de evento para crear un administrador es `platform`/`administrator`/`create`.
- **TargetID:** El ID del objeto del sistema que se cambió o que resultó afectado.
- **TargetDisplayName:** El nombre simplificado del objeto del sistema que se cambió o que resultó afectado. Por ejemplo, el nombre de un administrador que se creó.

- **TargetEmail:** La dirección de correo electrónico del objeto del sistema. Por ejemplo, la dirección de correo electrónico de un administrador que se creó.
- **TargetUserID:** El ID de usuario del objeto del sistema que se cambió o que resultó afectado. Por ejemplo, al crear un administrador, el ID de usuario de destino es el ID de usuario del administrador que se creó.
- **TargetType:** La categoría de destino del evento.
- **BeforeChanges** y **AfterChanges:** El contenido de los campos de objetos antes y después de que se produjera el evento, respectivamente. Para algunos eventos, estos campos de objetos incluyen:
  - CustomerID
  - Entidad principal de usuario
  - UserID
  - Tipo de acceso de administrador, como Personalizado o Total
  - CreatedDate
  - UpdatedDate
  - DisplayName
- **AgentID:** La categoría del evento.
- **ActorID:** El ID del objeto del sistema que inició el evento. Por ejemplo, para crear un administrador, este es el ID de objeto del administrador que invitó a otro usuario a la cuenta de Citrix Cloud.
- **ActorDisplayName:** El nombre simplificado de la persona o entidad que inició el evento. Por ejemplo, el nombre del administrador que invitó a otro usuario a la cuenta de Citrix Cloud.
- **ActorType:** El servicio que generó el evento.
- **EventMessage:** Una breve descripción del evento que ocurrió.

Eventos del registro del sistema para la plataforma Citrix Cloud

July 11, 2023

En este artículo se describen los datos de eventos que el registro del sistema captura para la plataforma Citrix Cloud. Para obtener más información sobre los datos de eventos del registro del sistema, consulte Referencia de eventos del registro del sistema.

Para obtener más información sobre el registro del sistema, consulte Registro del sistema.

Arrendatarios de Azure AD

Mensaje de evento	Tipo de evento	Tipo de destino	Tipo de actor	ID de actor	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Arrendatario de Azure AD conectado	platform/identityprovider/azuread/connect	tenant	administrator		Sí	No
Arrendatario de Azure AD desconectado	platform/identityprovider/azuread/disconnect	tenant	administrator		Sí	No
Se cambió el nombre del dominio de autenticación de Azure AD	platform/identityprovider/azuread/authdomain/updatename	customerID	administrator		No	No
No se pudo cambiar el nombre del dominio de autenticación de Azure AD	platform/identityprovider/azuread/authdomain/updatename	customerID	administrator		No	No

Administradores y clientes seguros de Citrix Cloud

Mensaje de evento	Tipo de evento	Tipo de destino	Tipo de actor	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Administrador creado	platform/administrator/create	administrator	system	No	Sí
Invitación de administrador enviada	platform/administrator/invite	administrator	administrator	No	Sí
Permisos o roles de administrador actualizados	platform/administrator/update	administrator	administrator	Sí	Sí
Administrador eliminado	platform/administrator/delete	administrator	administrator	No	Sí
Cliente seguro creado	platform/clientadministrator/create	service	system	No	Sí
Cliente seguro eliminado	platform/clientadministrator/delete	service	administrator	Sí	No
Grupo de administradores creado	platform/administrator/group/create	administratorgroup	administrator	No	Sí
Roles o permisos del grupo de administradores actualizados	platform/administrator/group/update	administratorgroup	administrator	Sí	Sí
Grupo de administradores eliminado	platform/administrator/group/delete	administratorgroup	administrator	Sí	No

Restablecimiento de dispositivo para Active Directory y token

Mensaje de evento	Tipo de evento	Tipo de destino	Tipo de actor	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Se completó el restablecimiento del token del dispositivo del suscriptor	platform/authentication/device/delete	subscriber	administrator	No	Sí

Administración de dominios

Mensaje de evento	Tipo de evento	Tipo de destino	Tipo de actor	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Dominio eliminado	platform/domain/remove	service	administrator	No	No

Ubicaciones de red

Mensaje de evento	Tipo de evento	ID de destino	ID de actor	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Ubicación de red creada	sdwan/networklocation/create	El ID de la ubicación de red creada	El nombre del administrador que agregó la ubicación de red	No	Sí
Ubicación de red actualizada	sdwan/networklocation/edit	El ID de la ubicación de red modificada	El nombre del administrador que modificó la ubicación de red	Sí	Sí
Ubicación de red eliminada	sdwan/networklocation/delete	El ID de la ubicación de red eliminada	El nombre del administrador que eliminó la ubicación de red	Sí	No

Ubicaciones de recursos

Mensaje de evento	Tipo de evento	ID de destino	ID de actor	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Ubicación de recursos creada	platform/resourcelocation/create	El nombre de la ubicación de recursos que se creó	El nombre del administrador que creó la ubicación de recursos	Sí	Sí

Mensaje de evento	Tipo de evento	ID de destino	ID de actor	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Ubicación de recursos actualizada	platform/resourcelocation/update	El nombre de la ubicación de recursos que se modificó	El nombre del administrador que modificó la ubicación de recursos	Sí	Sí
Ubicación de recursos eliminada	platform/resourcelocation/delete	El nombre de la ubicación de recursos que se eliminó	El nombre del administrador que eliminó la ubicación de recursos	Sí	Sí

Eventos del registro del sistema para conectores

April 7, 2022

En este artículo se describen los datos de eventos que el registro del sistema captura para Citrix Cloud Connectors y dispositivos Connector de Cloud Services. Para obtener más información sobre los datos de eventos del registro del sistema, consulte Referencia de eventos del registro del sistema.

Para obtener más información sobre el registro del sistema, consulte Registro del sistema.

Registro de conectores

Mensaje de evento	Tipo de evento	Tipo de destino	ID de actor	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Conector registrado	platform/edgeserver/cloud/create	**Cloud Connector** o **dispositivo Connector**	El administrador que registró el conector	Sí	Sí
Conector eliminado	platform/edgeserver/cloud/delete	**Cloud Connector** o **dispositivo Connector**	El administrador que eliminó el conector	Sí	Sí

Novedades del Connector

Mensaje de evento	Tipo de evento	ID de destino	ID de actor	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Se actualizó la ventana de mantenimiento de la ubicación de recursos	platform/resourcelocation/maintenancewindow/update	El nombre de la ubicación de recursos que se modificó	El administrador que cambió la configuración	Sí	Sí
Actualización de versión del conector desencadenada por el administrador	platform/edgeserver/cloud/manualupgrade	**Cloud Connector** o **dispositivo Connector**	El administrador que inició la actualización	No	No

Mensaje de evento	Tipo de evento	ID de destino	ID de actor	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Actualización de versión del conector iniciada	platform/edgeserver/upgradestarted	**Cloud Connector** o **dispositivo Connector**	**Automático** o el administrador que inició la actualización	Sí	No
Actualización de versión del conector completada	platform/edgeserver/upgradecompleted	**Cloud Connector** o **dispositivo Connector**	**Automático** o el administrador que inició la actualización	No	Sí

Claves públicas del conector

Mensaje de evento	Tipo de evento	ID de destino	ID de actor	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Clave pública agregada para que se confíe en ella	platform/authentication/createedgeserverkey	El	administrador que realizó la operación	No	No
Clave pública quitada para que no se confíe en ella	platform/authentication/deleteedgeserverkey	El	administrador que realizó la operación	No	No

Eventos del registro del sistema para licencias en Citrix Cloud

April 7, 2022

En este artículo se describen los datos de eventos que el registro del sistema captura para el registro local de Citrix Licensing en Citrix Cloud. Para obtener más información sobre los datos de eventos del registro del sistema, consulte Referencia de eventos del registro del sistema.

Para obtener más información sobre el registro del sistema, consulte Registro del sistema.

Servidores de licencias locales

Mensaje de evento	Tipo de evento	Tipo de destino	ID de actor	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Servidores de licencias locales eliminados	lui/onpremlicenseservers/delete	Licencias	El administrador que eliminó el servidor de licencias	No	No
No se pudieron eliminar servidores de licencias locales	lui/onpremlicenseservers/deletefailed	Licencias	El administrador que intentó eliminar el servidor de licencias	No	No

Licencias de servicios de la nube

Mensaje de evento	Tipo de evento	Tipo de destino	ID de actor	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Licencias de servicio de Citrix Cloud liberadas	lui/cloudlicense/release	CloudLicense	El administrador que liberó licencias para el servicio de la nube	No	No
No se pudieron liberar licencias de servicio de Citrix Cloud	lui/cloudlicense/releasefailed	CloudLicense	El administrador que intentó liberar licencias para el servicio de la nube	No	No

Información del uso de licencias para Citrix Service Providers

Mensaje de evento	Tipo de evento	Tipo de destino	ID de actor	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Datos de la lista de usuarios locales de socios exportados	lui/csp/userlistdataexport	Licenses	El administrador que exportó los datos de la lista de usuarios de socios	No	No

Mensaje de evento	Tipo de evento	Tipo de destino	ID de actor	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
No se pudieron exportar datos de la lista de usuarios locales de socios	lui/csp/userlistdataexportfailed	Licensing	El administrador que intentó exportar los datos de la lista de usuarios de socios	No	No

Uso de licencias para servicios de la nube y productos locales

Mensaje de evento	Tipo de evento	Tipo de destino	ID de actor	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Datos de uso de licencias exportados	lui/cloudlicense/usagedataexport	CloudLicensing o Licensing	El administrador que exportó los datos de uso de las licencias	No	No
No se pudieron exportar datos de uso de licencias	lui/cloudlicense/usagedataexportfailed	CloudLicensing o Licensing	El administrador que intentó exportar los datos de uso de las licencias	No	No

Eventos del registro del sistema para Secure Private Access

October 14, 2022

En este artículo se describen los datos de eventos que el registro del sistema captura para Secure Private Access Service. Para obtener más información sobre los datos de eventos del registro del sistema, consulte Referencia de eventos del registro del sistema.

Para obtener más información sobre el registro del sistema, consulte Registro del sistema.

Aplicaciones web y SaaS

Mensaje de evento	Tipo de evento	Tipo de destino	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Aplicación web/SaaS creada	swa/websaasppplicationcreate	web/saasapplication	No	Sí
Aplicación web/SaaS actualizada	swa/websaasppplicationupdate	web/saasapplication	Sí	Sí
Aplicación web/SaaS eliminada	swa/websaasppplicationdelete	web/saasapplication	Sí	No
No se pudo crear la aplicación web/SaaS	swa/websaaspplicationcreatefailed	web/saasapplication	No	No
No se pudo actualizar la aplicación web/SaaS	swa/websaaspplicationupdatefailed	web/saasapplication	Sí	Sí
No se pudo eliminar la aplicación web/SaaS	swa/websaaspplicationdeletefailed	web/saasapplication	Sí	Sí

Suscripciones de usuarios y grupos

Mensaje de evento	Tipo de evento	Tipo de destino	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Suscripción de usuario/grupo agregada	swa/websaaspplicationsubscription/subscribers	websaaspplicationsubscription/subscribers	No	Sí
Suscripción de usuario/grupo quitada	swa/websaaspplicationsubscription/unsubscribe	websaaspplicationsubscription/subscribers	No	Sí
Error en la suscripción de usuario/grupo	swa/websaaspplicationsubscription/subscribefailed	websaaspplicationsubscription/subscribefailed	No	No
Error al cancelar la suscripción de usuario/grupo	swa/websaaspplicationsubscription/unsubscribefailed	websaaspplicationsubscription/unsubscribefailed	No	No

Directivas contextuales

Mensaje de evento	Tipo de evento	Tipo de destino	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Directiva contextual creada	swa/contextualpolicy/create	contextualpolicy	No	Sí
Directiva contextual actualizada	swa/contextualpolicy/update	contextualpolicy	Sí	Sí
Directiva contextual eliminada	swa/contextualpolicy/delete	contextualpolicy	Sí	No

Mensaje de evento	Tipo de evento	Tipo de destino	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
No se pudo crear la directiva contextual	swa/contextualpolicy/createfailed	contextualpolicy	No	No
No se pudo actualizar la directiva contextual	swa/contextualpolicy/updatefailed	contextualpolicy	No	No
No se pudo eliminar la directiva contextual	swa/contextualpolicy/deletefailed	contextualpolicy	Sí	No

Dominios de aplicación

Mensaje de evento	Tipo de evento	Tipo de destino	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Dominio de la aplicación creado	swa/applicationdomain/create	applicationdomain	No	Sí
Dominio de la aplicación actualizado	swa/applicationdomain/update	applicationdomain	Sí	Sí
Dominio de la aplicación eliminado	swa/applicationdomain/delete	applicationdomain	Sí	No
No se pudo crear el dominio de la aplicación	swa/applicationdomain/createfailed	applicationdomain	No	No

Mensaje de evento	Tipo de evento	Tipo de destino	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
No se pudo actualizar el dominio de la aplicación	swa/applicationdomain/update/failed	application domain	Sí	No
No se pudo eliminar el dominio de la aplicación	swa/applicationdomain/delete/failed	application domain	Sí	No

Parámetros de la extensión para exploradores web

Mensaje de evento	Tipo de evento	Tipo de destino	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Parámetros actualizados de la extensión para exploradores web	swa/browserextensionsettings/update/success	browserextensionsettings	Sí	Sí
No se pudieron actualizar los parámetros de la extensión para exploradores web	swa/browserextensionsettings/update/failed	browserextensionsettings	Sí	No

Categorías de filtro y listas de URL de sitios web

Mensaje de evento	Tipo de evento	Tipo de destino	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Listas y categorías de filtro de sitios web habilitadas	swa/website/filterlists/enabled/update	swa/website/filterlists/enabled	Sí	Sí
Listas de filtros de sitios web habilitadas y categorías de filtro inhabilitadas	swa/website/filterlists/enabled/update	swa/website/filterlists/enabled	Sí	Sí
Listas de filtros de sitios web inhabilitadas y categorías de filtro habilitadas	swa/website/filterlists/enabled/update	swa/website/filterlists/enabled	Sí	Sí
Listas y categorías de filtro de sitios web inhabilitadas	swa/website/filterlists/enabled/update	swa/website/filterlists/enabled	Sí	Sí
No se pudieron habilitar las listas y categorías de filtro de sitios web	swa/website/filterlists/enabled/update	swa/website/filterlists/enabled	Sí	failed
No se pudieron habilitar las listas de filtros de sitios web ni inhabilitar las categorías de filtro	swa/website/filterlists/enabled/update	swa/website/filterlists/enabled	Sí	failed

Mensaje de evento	Tipo de evento	Tipo de destino	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
No se pudieron inhabilitar las listas de filtros de sitios web ni habilitar las categorías de filtro	swa/website/filterlists/disable/failed	website/filterlist	Sí	Sí
No se pudieron inhabilitar las listas y categorías de filtro de sitios web	swa/website/filterlists/disable/failed	website/filterlist	Sí	Sí
Lista de URL de sitios web creada	swa/websiteurlfiltering/create	website/urlfilteringlist	No	Sí
Lista de URL de sitios web actualizada	swa/websiteurlfiltering/update	website/urlfilteringlist	Sí	Sí
Lista de URL de sitios web eliminada	swa/websiteurlfiltering/delete	website/urlfilteringlist	Sí	No
No se pudo crear la lista de URL de sitios web	swa/websiteurlfiltering/create/failed	website/urlfilteringlist	No	No
No se pudo actualizar la lista de URL de sitios web	swa/websiteurlfiltering/update/failed	website/urlfilteringlist	Sí	No
No se pudo eliminar la lista de URL de sitios web	swa/websiteurlfiltering/delete/failed	website/urlfilteringlist	Sí	No
Categoría de filtro de URL de sitios web creada	swa/websiteurlfiltercategory/create	category	No	Sí

Mensaje de evento	Tipo de evento	Tipo de destino	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Categoría de filtro de URL de sitios web actualizada	swa/websiteurlfiltercategory/update	category	Sí	Sí
Categoría de filtro de URL de sitios web eliminada	swa/websiteurlfiltercategory/delete	category	No	No
No se pudo crear la categoría de filtro de URL de sitios web	swa/websiteurlfiltercategory/createfailed	category	No	No
No se pudo actualizar la categoría de filtro de URL de sitios web	swa/websiteurlfiltercategory/updatefailed	category	Sí	No
No se pudo eliminar la categoría de filtro de URL de sitios web	swa/websiteurlfiltercategory/deletefailed	category	Sí	No

Parámetros preestablecidos de categorías de filtros de sitios web

Mensaje de evento	Tipo de evento	Tipo de destino	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Parámetro preestablecido de categoría de filtro de sitios web actualizado	swa/websiteurlfiltercategorypreset/update	categorypreset/category	Sí	Sí
No se pudo actualizar el parámetro preestablecido de categoría de filtro de sitios web	swa/websiteurlfiltercategorypreset/update	categorypreset/category	Sí	Sí

Categorías de filtro y listas de URL de sitios web bloqueadas

Mensaje de evento	Tipo de evento	Tipo de destino	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Lista de URL de sitios web bloqueados creada	swa/websiteurlfilterwebsiteblocklist/create	websiteblocklist/urllist	No	Sí
Lista de URL de sitios web bloqueados actualizada	swa/websiteurlfilterwebsiteblocklist/update	websiteblocklist/urllist	No	Sí

Mensaje de evento	Tipo de evento	Tipo de destino	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Lista de URL de sitios web bloqueados eliminada	swa/websiteurlfilterwebsite/blocked/list	website/blocked/list	No	Sí
No se pudo crear la lista de URL de sitios web bloqueados	swa/websiteurlfilterwebsite/blocked/list	website/blocked/list	No	Sí
No se pudo actualizar la lista de URL de sitios web bloqueados	swa/websiteurlfilterwebsite/blocked/list	website/blocked/list	No	Sí
No se pudo eliminar la lista de URL de sitios web bloqueados	swa/websiteurlfilterwebsite/blocked/list	website/blocked/list	No	Sí
Categoría de filtro de URL de sitios web bloqueados creada	swa/websiteurlfiltercategory/blocked/list	category/blocked/list	No	Sí
Categoría de filtro de URL de sitios web bloqueados actualizada	swa/websiteurlfiltercategory/blocked/list	category/blocked/list	No	Sí
Categoría de filtro de URL de sitios web bloqueados eliminada	swa/websiteurlfiltercategory/blocked/list	category/blocked/list	No	Sí
No se pudo crear la categoría de filtro de URL de sitios web bloqueados	swa/websiteurlfiltercategory/blocked/list	category/blocked/list	No	Sí

Mensaje de evento	Tipo de evento	Tipo de destino	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
No se pudo actualizar la categoría de filtro de URL de sitios web bloqueados	swa/websiteurlfilter	category/blocked/list	Nofailed	Sí
No se pudo eliminar la categoría de filtro de URL de sitios web bloqueados	swa/websiteurlfilter	category/blocked/list	Nofailed	Sí

Categorías de filtro y listas de URL de sitios web permitidas

Mensaje de evento	Tipo de evento	Tipo de destino	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Lista de URL de sitios web permitidos creada	swa/websiteurlfilter	website/allowed/list	No	Sí
Lista de URL de sitios web permitidos actualizada	swa/websiteurlfilter	website/allowed/list	No	Sí
Lista de URL de sitios web permitidos eliminada	swa/websiteurlfilter	website/allowed/list	No	Sí

Mensaje de evento	Tipo de evento	Tipo de destino	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
No se pudo crear la lista de URL de sitios web permitidos	swa/websiteurlfilterwebsiteallowlist/create	website/allowlist	failed	Sí
No se pudo actualizar la lista de URL de sitios web permitidos	swa/websiteurlfilterwebsiteallowlist/update	website/allowlist	failed	Sí
No se pudo eliminar la lista de URL de sitios web permitidos	swa/websiteurlfilterwebsiteallowlist/delete	website/allowlist	failed	Sí
Categoría de filtro de URL de sitios web permitidos creada	swa/websiteurlfiltercategory/allowlist/create	category/allowlist	Nada	Sí
Categoría de filtro de URL de sitios web permitidos actualizada	swa/websiteurlfiltercategory/allowlist/update	category/allowlist	Nada	Sí
Categoría de filtro de URL de sitios web permitidos eliminada	swa/websiteurlfiltercategory/allowlist/delete	category/allowlist	Nada	Sí
No se pudo crear la categoría de filtro de URL de sitios web permitidos	swa/websiteurlfiltercategory/allowlist/create	category/allowlist	failed	Sí

Mensaje de evento	Tipo de evento	Tipo de destino	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
No se pudo actualizar la categoría de filtro de URL de sitios web permitidos	swa/websiteurlfiltercategory/allowed/update	category/allowed/list	Nulo	Sí
No se pudo eliminar la categoría de filtro de URL de sitios web permitidos	swa/websiteurlfiltercategory/allowed/delete	category/allowed/list	Nulo	Sí

Categorías de filtro y listas de URL de sitios web redirigidos a Remote Browser Isolation (antes denominado Secure Browser)

Mensaje de evento	Tipo de evento	Tipo de destino	Tipo de actor	ID de agente	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Lista de URL de sitios web redirigidos a Secure Browser creada	swa/websiteurlfilteringlist/redirected/create	websi
Lista de URL de sitios web redirigidos a Secure Browser actualizada	swa/websiteurlfilteringlist/redirected/update
Lista de URL de sitios web redirigidos a Secure Browser eliminada	swa/websiteurlfilteringlist/redirected/delete	we
No se pudo crear la lista de URL de sitios web redirigidos a Secure Browser	swa/websiteurlfilteringlist/redirected/c
No se pudo actualizar la lista de URL de sitios web redirigidos a Secure Browser	swa/websiteurlfilteringlist/redirect
No se pudo eliminar la lista de URL de sitios web redirigidos a Secure Browser	swa/websiteurlfilteringlist/redirecte
Categoría de filtro de URL de sitios web redirigidos a Secure Browser creada	swa/websiteurlfiltercategory/redirecte
Categoría de filtro de URL de sitios web redirigidos a Secure Browser actualizada	swa/websiteurlfiltercategory/red
Categoría de filtro de URL de sitios web redirigidos a Secure Browser eliminada	swa/websiteurlfiltercategory/redir
No se pudo crear la categoría de filtro de URL de sitios web redirigidos a Secure Browser	swa/websiteurlfiltercatego
No se pudo actualizar la categoría de filtro de URL de sitios web redirigidos a Secure Browser	swa/websiteurlfilterca
No se pudo eliminar la categoría de filtro de URL de sitios web redirigidos a Secure Browser	swa/websiteurlfiltercat

Eventos del registro del sistema para Citrix Workspace

April 7, 2022

En este artículo se describen los datos de eventos que el registro del sistema captura para Citrix Workspace. Para obtener más información sobre los datos de eventos del registro del sistema, consulte Referencia de eventos del registro del sistema.

Para obtener más información sobre el registro del sistema, consulte Registro del sistema.

URL del espacio de trabajo

Mensaje de evento	Tipo de evento	Tipo de destino	ID de actor	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
URL del espacio de trabajo actualizada	wxp/url/update	subscriber	El administrador que actualizó la URL	Sí	Sí
No se pudo actualizar la URL del espacio de trabajo	wxp/url/updatefailed	subscriber	El administrador que intentó actualizar la URL	Sí	Sí
URL del espacio de trabajo habilitada	wxp/url/enable	subscriber	El administrador que habilitó la personalización de la URL del espacio de trabajo	No	Sí

Mensaje de evento	Tipo de evento	Tipo de destino	ID de actor	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
No se pudo habilitar la URL del espacio de trabajo	wxp/url/enablefailed	subscriber	El administrador que intentó habilitar la personalización de la URL del espacio de trabajo	No	Sí
URL del espacio de trabajo inhabilitada	wxp/url/disable	subscriber	El administrador que inhabilitó la personalización de la URL del espacio de trabajo	No	Sí
No se pudo inhabilitar la URL del espacio de trabajo	wxp/url/disablefailed	subscriber	El administrador que intentó inhabilitar la personalización de la URL del espacio de trabajo	No	Sí

Autenticación de Workspace

Mensaje de evento	Tipo de evento	Tipo de destino	ID de actor	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Proveedor de identidades del espacio de trabajo actualizado	wxp/identityprovider/update	subscriber	El administrador que actualizó el método de autenticación de Workspace	Sí	Sí
No se pudo actualizar el proveedor de identidades del espacio de trabajo	wxp/identityprovider/updatefailed	subscriber	El administrador que intentó actualizar el método de autenticación del espacio de trabajo	Sí	Sí

Servicio de autenticación federada de Citrix

Mensaje de evento	Tipo de evento	Tipo de destino	ID de actor	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Servicio de autenticación federada (FAS) del espacio de trabajo habilitado	wxp/fas/enable	subscriber	El administrador que habilitó FAS	No	Sí

Mensaje de evento	Tipo de evento	Tipo de destino	ID de actor	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
No se pudo habilitar el Servicio de autenticación federada (FAS) del espacio de trabajo	wxp/fas/enablefailed	subscriber	El administrador que intentó habilitar FAS	No	Sí
Servicio de autenticación federada (FAS) del espacio de trabajo inhabilitado	wxp/fas/disable	subscriber	El administrador que inhabilitó FAS	No	Sí
No se pudo inhabilitar el Servicio de autenticación federada (FAS) del espacio de trabajo	wxp/fas/disablefailed	subscriber	El administrador que intentó inhabilitar FAS	No	Sí

Favoritos

Mensaje de evento	Tipo de evento	Tipo de destino	ID de actor	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Favoritos de Workspace habilitados	wxp/favorites/enable	subscriber	El administrador que habilitó los favoritos	No	Sí
No se pudo habilitar los favoritos de Workspace	wxp/favorites/enable/failed	subscriber	El administrador que intentó habilitar favoritos	No	Sí
Favoritos de Workspace inhabilitados	wxp/favorites/disable	subscriber	El administrador que inhabilitó los favoritos	No	Sí
No se pudo inhabilitar los favoritos de Workspace	wxp/favorites/disable/failed	subscriber	El administrador que intentó inhabilitar los favoritos	No	Sí

Cambiar contraseña

Mensaje de evento	Tipo de evento	Tipo de destino	ID de actor	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Directiva de opciones de cambio de contraseña del espacio de trabajo actualizada	wxp/changepasswordoptions/update	workspaceconfiguration	El administrador que actualizó la directiva para cambiar contraseñas en Citrix Workspace	Sí	Sí
No se pudo actualizar la directiva de opciones de cambio de contraseña del espacio de trabajo	wxp/changepasswordoptions/updatepolicyfailed	workspaceconfiguration	El administrador que intentó actualizar la directiva para cambiar contraseñas en Citrix Workspace	Sí	Sí
Directiva de opciones de cambio de contraseña del espacio de trabajo habilitada	wxp/changepasswordoptions/enable	workspaceconfiguration	El administrador que habilitó el parámetro para cambiar contraseñas en Citrix Workspace	No	Sí

Mensaje de evento	Tipo de evento	Tipo de destino	ID de actor	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
No se pudieron habilitar las opciones de cambio de contraseña del espacio de trabajo	wxp/changepasswordoptions/enable	subscription	El administrador que intentó habilitar el parámetro para cambiar contraseñas en Citrix Workspace	No	Sí
Directiva de opciones de cambio de contraseña del espacio de trabajo inhabilitada	wxp/changepasswordoptions/disable	subscription	El administrador que inhabilitó el parámetro para cambiar contraseñas en Citrix Workspace	No	Sí
No se pudieron inhabilitar las opciones de cambio de contraseña del espacio de trabajo	wxp/changepasswordoptions/disable	subscription	El administrador que intentó inhabilitar el parámetro para cambiar contraseñas en Citrix Workspace	No	Sí

Tokens de larga duración

Mensaje de evento	Tipo de evento	Tipo de destino	ID de actor	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Configuración de token de larga duración del espacio de trabajo actualizada	wxp/longlivedtoken/update	subscription	El administrador que actualizó la configuración del token	Sí	Sí
No se pudo actualizar la configuración de token de larga duración del espacio de trabajo	wxp/longlivedtoken/updatefailed	subscription	El administrador que intentó actualizar la configuración del token	Sí	Sí

Tiempo de espera por inactividad para la web

Mensaje de evento	Tipo de evento	Tipo de destino	ID de actor	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Configuración de sesiones de Workspace actualizada	wxp/sessions/updatesubscriber		El administrador que actualizó el tiempo de inactividad del parámetro Tiempo de espera por inactividad para la web	Sí	Sí
No se pudo actualizar la configuración de sesiones del espacio de trabajo	wxp/sessions/updatefailed		El administrador que intentó actualizar el tiempo de inactividad del parámetro Tiempo de espera por inactividad para la web	Sí	Sí

Implantación de funciones

Mensaje de evento	Tipo de evento	Tipo de destino	ID de actor	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Usuarios y grupos asignados actualizados para la experiencia en espacios de trabajo inteligentes	wxp/iws/features/subscribers	usersgroups	El administrador que actualizó los usuarios y grupos asignados para acceder a las notificaciones del feed de actividades en Citrix Workspace	No	No
No se pudieron asignar usuarios y grupos actualizados para la experiencia en espacios de trabajo inteligentes	wxp/iws/features/subscribers	usersgroups	El administrador que intentó actualizar los usuarios y grupos asignados para acceder a las notificaciones del feed de actividades en Citrix Workspace	No	No

Mensaje de evento	Tipo de evento	Tipo de destino	ID de actor	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
Experiencia en espacios de trabajo inteligentes habilitada	wxp/iws/features/enable	subscriber	El administrador que habilitó las notificaciones del feed de actividades en Citrix Workspace	No	No
No se pudo habilitar la experiencia en espacios de trabajo inteligentes	wxp/iws/features/enablefail	subscriber	El administrador que intentó habilitar las notificaciones del feed de actividades en Citrix Workspace	No	No
Experiencia en espacios de trabajo inteligentes inhabilitada	wxp/iws/features/disable	subscriber	El administrador que inhabilitó las notificaciones del feed de actividades en Citrix Workspace	No	No

Mensaje de evento	Tipo de evento	Tipo de destino	ID de actor	Campos de objetos actuales registrados antes del evento	Campos de objetos actualizados registrados después del evento
No se pudo inhabilitar la experiencia en espacios de trabajo inteligentes	wxp/iws/features/disable/failed	Suscripción	El administrador que intentó inhabilitar las notificaciones del feed de actividades en Citrix Workspace	No	No

SDK y API

July 2, 2024

Citrix Cloud proporciona varias API que puede usar para obtener información y automatizar tareas complejas y repetitivas, entre las que se incluyen:

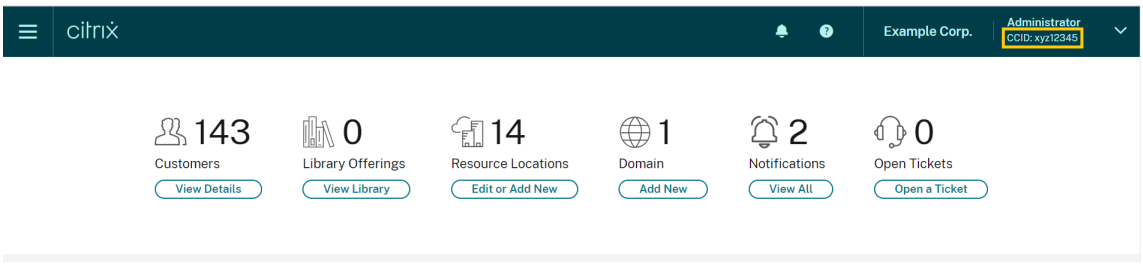
- Instalación silenciosa de Citrix Cloud Connector
- Crear y usar informes para administrar licencias de la nube
- Determinar el estado de los derechos de un cliente
- Enviar notificaciones a administradores de Citrix Cloud
- Obtener eventos del registro del sistema
- Obtener detalles sobre las ubicaciones de recursos para usarlos con otras API

Varios servicios de Citrix Cloud también proporcionan SDK y API que le permiten obtener información, consultar datos y realizar tareas administrativas.

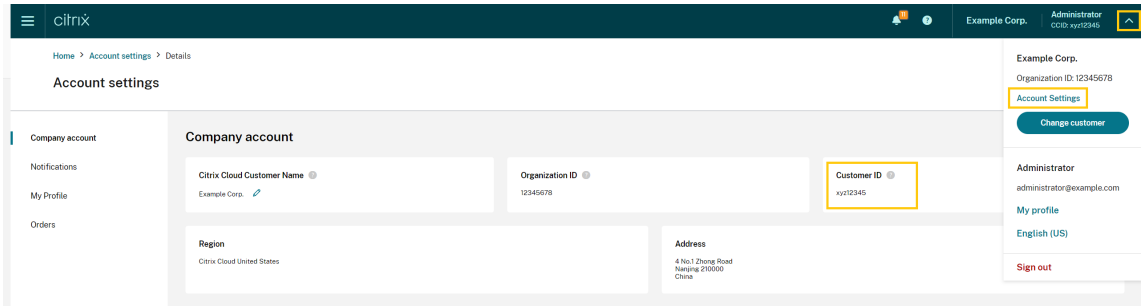
Clientes seguros

Para usar las API de Citrix Cloud, debe crear un cliente seguro que acceda a Citrix Cloud en su nombre. Para crear un cliente seguro, tendrá que proporcionar el ID de cliente de su cuenta de Citrix Cloud. Su ID de cliente se encuentra en estos lugares de la consola de administración:

- En la esquina superior derecha de la consola, debajo de su nombre de usuario.



- En la página **Parámetros de cuenta**.



- En la página **Acceso a API**.

Permisos heredados

Los clientes seguros están vinculados a un único administrador y a un único ID de cliente en Citrix Cloud. Esto significa que sus clientes seguros heredan el mismo nivel de permisos que tiene usted con un ID de cliente específico. Por lo tanto, si tiene permisos de acceso total, sus clientes seguros también tendrán permisos de acceso total. Si el nivel de permisos se reduce más adelante, los clientes seguros que ya ha creado heredan automáticamente los permisos reducidos.

Para obtener instrucciones sobre cómo crear clientes seguros, consulte Get started with Citrix Cloud APIs en la documentación para desarrolladores de Citrix.

API de licencias de la nube

Los clientes de empresa pueden usar API de licencias de la nube para realizar tareas de administración, como exportar datos de uso y liberar licencias asignadas. Los socios de Citrix pueden usar estas API para obtener datos resumidos e históricos de Citrix Virtual Apps and Desktops local y Citrix DaaS.

Para obtener más información, consulte APIs to manage Citrix Cloud licensing en la documentación para desarrolladores de Citrix.

API de SystemLog

La API de SystemLog le permite obtener eventos que ocurrieron en su cuenta de Citrix Cloud durante los períodos de tiempo que especifique. Para obtener más información sobre el uso de esta API, consulte Citrix Cloud - SystemLog en la documentación para desarrolladores de Citrix.

API de ubicaciones de recursos

La API de ubicaciones de recursos le permite obtener información sobre las ubicaciones de sus recursos para utilizarla con otras aplicaciones y scripts. Por ejemplo, supongamos que quiere instalar Citrix Cloud Connector de forma silenciosa en una de las varias ubicaciones de recursos de su cuenta de Citrix Cloud. Puede usar esta API para obtener el ID de la ubicación de recursos y pasarlo al script de instalación.

Para obtener más información sobre el uso de esta API, consulte Citrix Cloud - Resource Location en la documentación para desarrolladores de Citrix.

API de derechos de servicio

La API de derechos de servicio obtiene los servicios para los que un cliente tiene derechos de uso, los días restantes de cada derecho y la cantidad de derechos que el cliente adquirió. Para obtener más información sobre el uso de esta API, consulte Citrix Cloud - Service Entitlement en la documentación para desarrolladores de Citrix.

API de notificaciones

La API de notificaciones le permite enviar mensajes a otros administradores de Citrix Cloud. Los destinatarios reciben sus mensajes a través de la página Notificaciones de la consola de administración.

SDK y API para otros servicios

Para obtener más información sobre los SDK y las API disponibles para otros servicios de Citrix Cloud, consulte estos artículos:

- Digital workspaces: Incluye SDK y API para servicios de espacios de trabajo como Citrix DaaS y Citrix Workspace.
- App delivery and security: Incluye SDK y API para redes y servicios de entrega de aplicaciones, como Console, Intelligent Traffic Management y SD-WAN Orchestrator.

Más información

Para obtener más información sobre cómo las API y los clientes seguros de Citrix Cloud pueden ayudarle a realizar operaciones complejas, como migrar a la nube y configurar la autenticación con tokens push, consulte estos artículos de Tech Zone:

- PoC Guide: nFactor for Citrix Gateway Authentication with Push Token
- Deployment Guide: Migrating Citrix Virtual Apps and Desktops from VMware vSphere to Citrix Virtual Apps and Desktops service on Microsoft Azure
- PoC Guide: Automated Configuration Tool

Citrix Cloud para socios

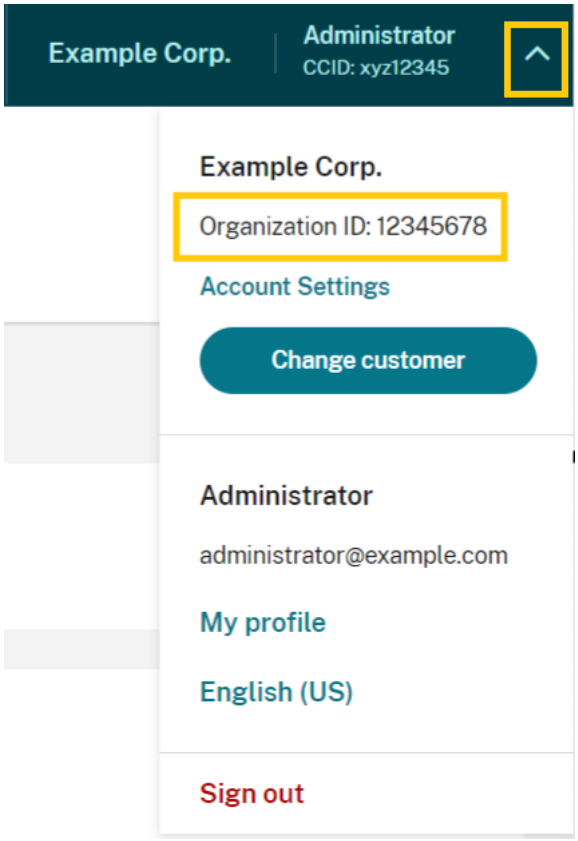
April 5, 2024

Citrix Cloud incluye servicios, funciones y tareas diseñadas tanto para clientes como para socios. En esta sección se describen las funciones disponibles para los socios de Citrix, pensadas para ayudarles en su colaboración con los clientes de los servicios y las soluciones de Citrix Cloud.

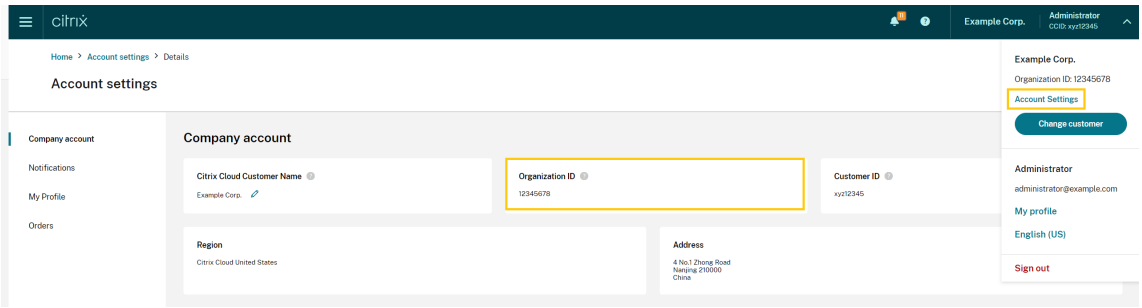
Identificación de socios

En Citrix Cloud, los socios se identifican con su ID de la organización de Citrix (ORGID). Los socios pueden ver el ORGID asociado a su cuenta de Citrix Cloud en las siguientes ubicaciones de la consola de administración de Citrix Cloud:

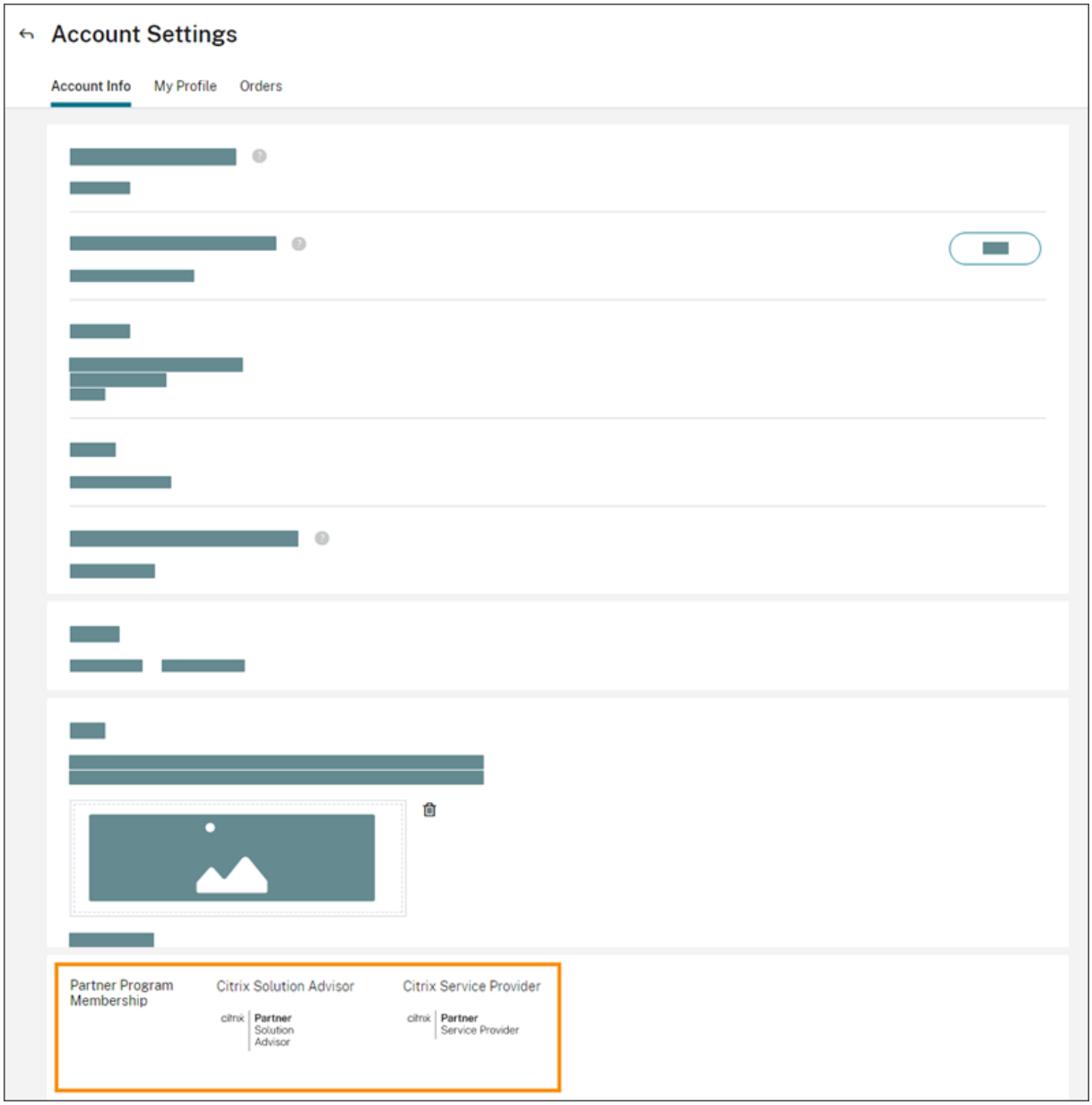
- En el menú de clientes. Haga clic en el nombre del cliente en la esquina superior derecha de la consola. Su ORGID aparece debajo del nombre de su empresa en el menú.



- En la página **Parámetros de cuenta**. En el menú del cliente en la esquina superior derecha, seleccione **Parámetros de cuenta**.

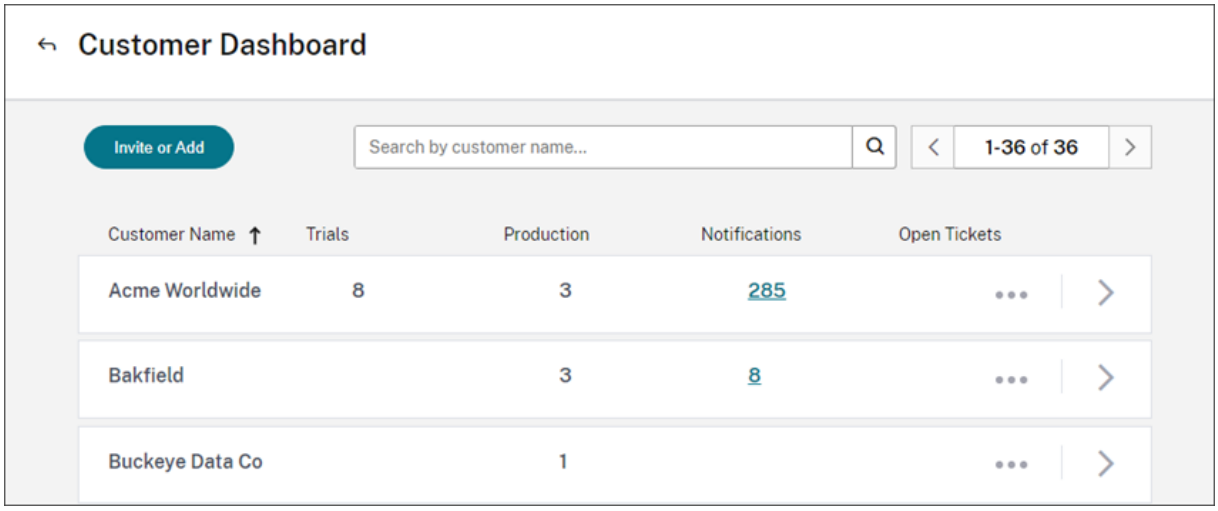


Si el ORGID de la cuenta es un miembro activo de un programa de socios de Citrix (por ejemplo, Citrix Solution Advisor o Citrix Service Provider), la etiqueta del programa en cuestión indica que esa cuenta es propiedad de un socio de Citrix. La identificación de socios se utiliza para controlar el acceso a funciones o servicios adicionales en la nube.

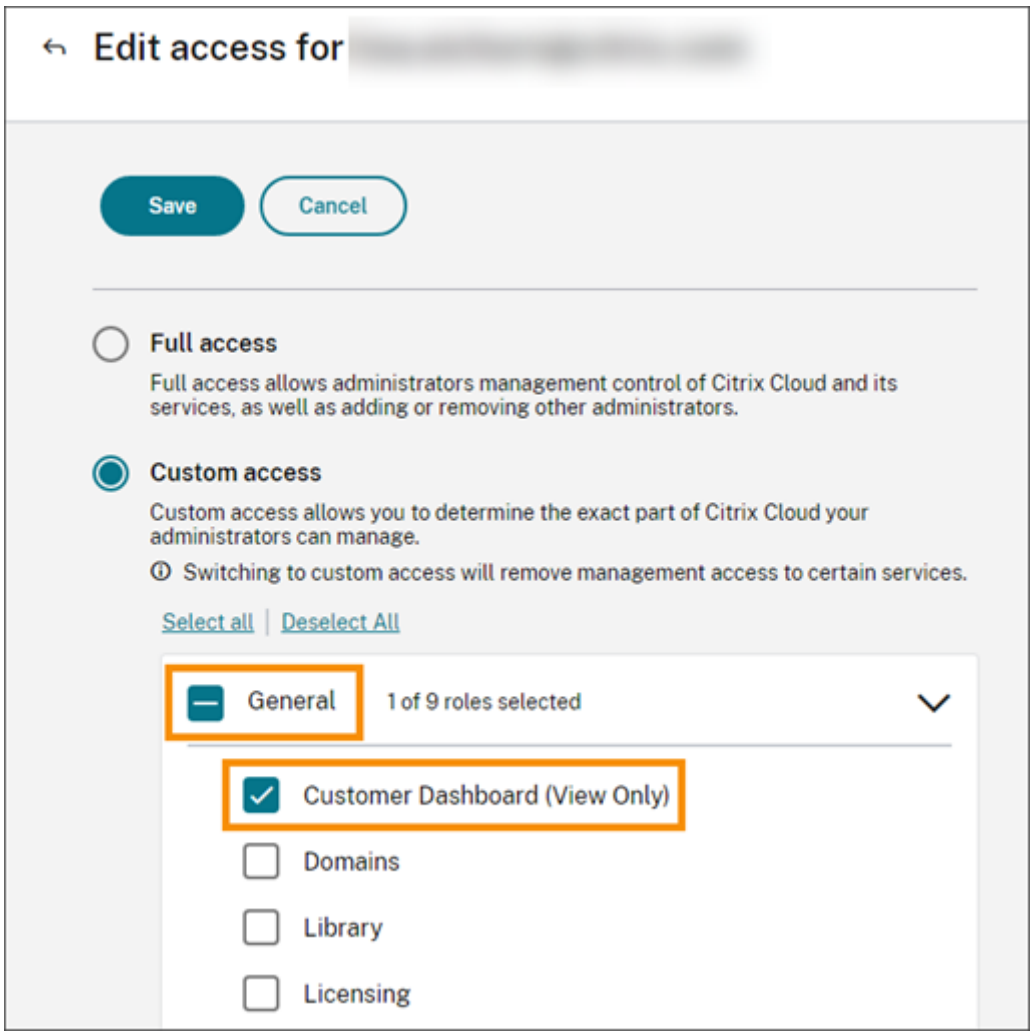


Panel de mandos de clientes

El panel de mandos de clientes está diseñado para que los socios vean el estado de varios clientes de Citrix Cloud en una sola vista. Para que un cliente aparezca en el panel de mandos, debe establecerse una conexión entre el cliente y el socio. El panel de mandos de clientes está disponible en las cuentas de Citrix Cloud clasificadas como pertenecientes a socios.



De forma predeterminada, los administradores con acceso total pueden ver el panel de mandos de los clientes. Los administradores con acceso personalizado pueden ver el panel si se selecciona el permiso **Panel de mandos del cliente (solo lectura)**. Para obtener más información sobre los permisos de administrador en Citrix Cloud, consulte Modificar permisos de administrador.



Conexiones de socios con clientes

Los socios que colaboren con clientes en las soluciones de Citrix Cloud pueden establecer un vínculo de confianza entre sus cuentas. Esta relación entre las cuentas permite que un cliente comparta fácilmente información específica con un socio. Al conectar con un socio, el cliente concede a ese socio la posibilidad de ver información sobre su cuenta de Citrix Cloud y su relación con Citrix.

Al establecer una conexión de socio sucede lo siguiente:

- El cliente aparece en el panel de mandos del socio
- El socio aparece como una conexión activa en los parámetros de la cuenta del cliente
- El socio tiene visibilidad de los servicios de Citrix Cloud del cliente
- El socio tiene visibilidad sobre el uso de licencias y el uso activo de los derechos de Citrix Cloud

Una vez establecida la conexión entre un socio y un cliente, los administradores del socio pueden ver la información básica de la cuenta del cliente, los pedidos que ha hecho el cliente y datos sobre las

prestaciones a las que tiene derecho (por ejemplo, servicios, licencias y fechas de caducidad).

Las conexiones de los socios con los clientes no caducan.

Conexiones con varios socios o clientes

Los socios pueden establecer conexiones con varios clientes. Los socios pueden asociarse a un máximo de 100 cuentas de clientes. Si un socio necesita administrar más de 100 cuentas de clientes, debe crear una cuenta de socio independiente con una dirección de correo electrónico diferente para administrar los clientes adicionales. Como alternativa, es posible que el socio considere la posibilidad de quitar cuentas de cliente que ya no necesite administrar.

Los clientes pueden establecer conexiones con varios socios. No hay límite para la cantidad de conexiones entre socios y clientes.

Notificaciones de conexión

Citrix Cloud envía notificaciones a los socios cuando:

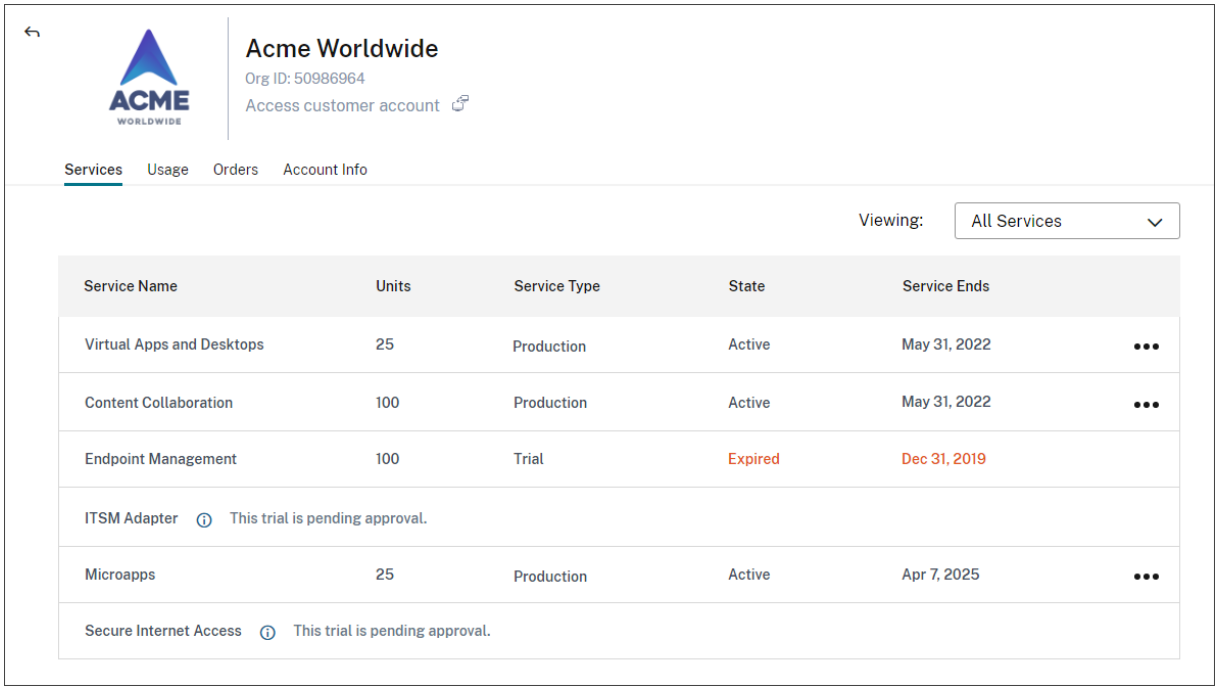
- El socio crea una conexión con un cliente
- Un cliente termina su conexión con el socio

Citrix Cloud envía notificaciones a los clientes cuando el socio finaliza su conexión con el cliente.

Visibilidad del socio de los servicios

Cuando está conectado a un cliente, el socio puede ver el estado de los servicios de ese cliente. Esta información incluye el estado de las prestaciones relacionadas tanto con pruebas de servicios, como con servicios en producción. Los socios también pueden ver la siguiente información:

- Pruebas de servicios activas
- Solicitudes de pruebas de servicios pendientes
- Pruebas de servicios caducadas
- Derechos de servicios activos (servicios adquiridos u otros servicios que el cliente tiene habilitados o permitidos)
- Recuento y fecha de caducidad de las licencias para cada servicio o prestación



La visibilidad de licencias se limita a la visualización de resúmenes de asignaciones de licencias y tendencias históricas de uso.

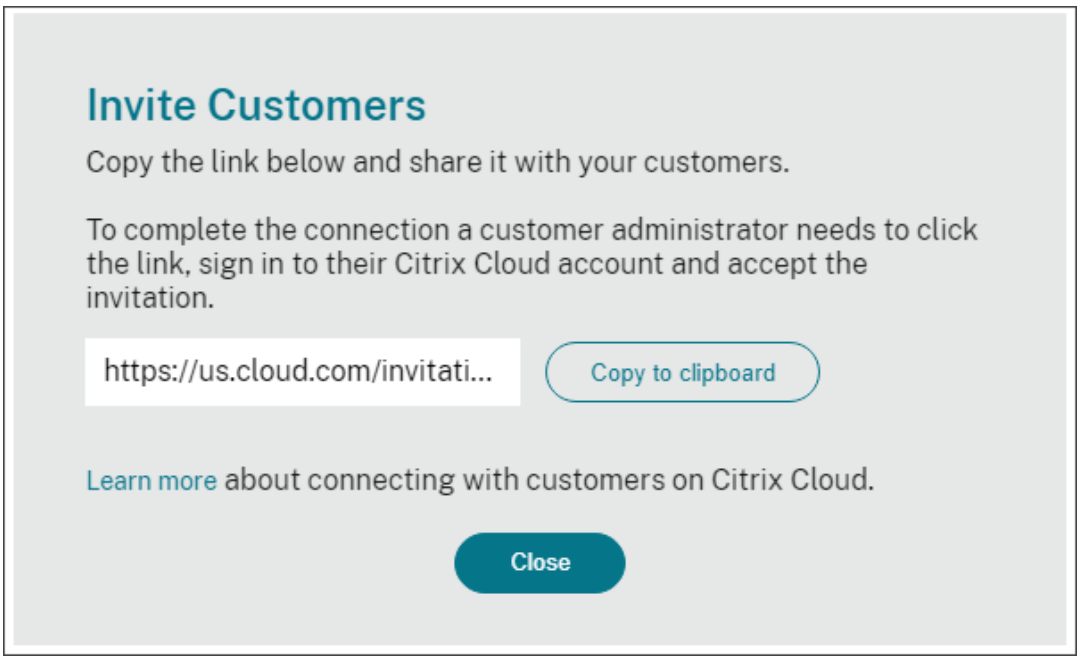
Crear conexiones con clientes

Los socios crean conexiones con los clientes mediante un enlace de invitación único. Este enlace es fijo y no se puede cambiar ni personalizar.

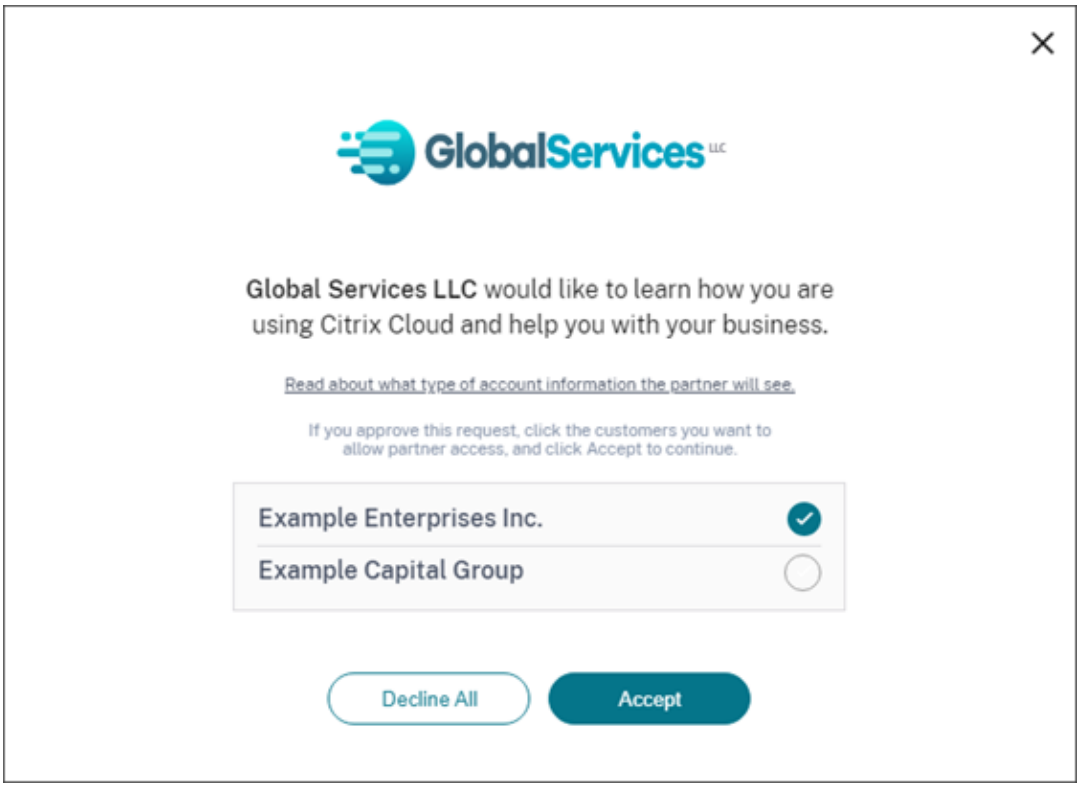
Los socios pueden usar su enlace de invitación un número ilimitado de veces para crear o volver a crear conexiones. Los enlaces de invitación no caducan.

Para crear una conexión:

1. En el menú de Citrix Cloud, seleccione **Mis clientes**.
2. En el panel de mandos de clientes, seleccione **Invitar o Agregar**.
3. Para conectar con un cliente actual de Citrix Cloud:
    a) Seleccione **Invitar a un cliente de Citrix Cloud** y, luego, seleccione **Continuar**.
    b) Copie el enlace de la invitación y envíelo al cliente.



Para completar la conexión, el cliente debe hacer clic en el enlace de invitación, iniciar sesión en Citrix Cloud y aceptar la invitación.



4. Para conectar con un cliente nuevo que aún no tiene una cuenta de Citrix Cloud:

   a) Seleccione **Agregar un cliente** y, a continuación, selecciona **Continuar**.

b) Introduzca los detalles de contacto del cliente y, a continuación, seleccione **Finalizar**. Citrix Cloud crea una nueva cuenta para el cliente.

Posteriormente, el cliente recibe una notificación en la que se indica que el socio se ha agregado como administrador a la nueva cuenta. El cliente puede establecer una contraseña para la nueva cuenta mediante la opción **¿Olvidó la contraseña?** que aparece en la página de inicio de sesión de Citrix Cloud. Tras configurar su contraseña, el cliente puede iniciar sesión en su cuenta con la dirección de correo electrónico de su empresa y completar el proceso de incorporación tal y como se describe en Registrarse en Citrix Cloud.

Eliminar conexiones de socios o clientes

Tanto el socio como el cliente pueden finalizar una conexión en cualquier momento.

Quitar una conexión con un cliente

Para finalizar una conexión con un cliente, el socio debe seguir estos pasos:

1. En el menú de Citrix Cloud, en la esquina superior derecha de la consola, seleccione **Mis clientes**.
2. En el panel de mandos de clientes, localice el cliente que quiere administrar.
3. Haga clic en el menú de puntos suspensivos del cliente y, a continuación, seleccione **Quitar la conexión de cliente**.
4. Cuando se le pida que confirmes la eliminación, seleccione **Quitar**.

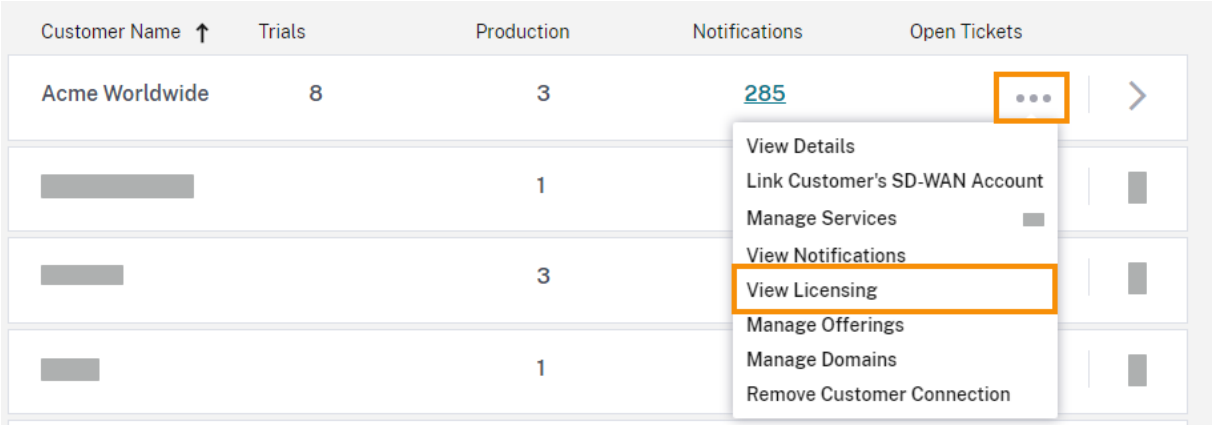
Quitar una conexión con un socio

Para finalizar una conexión con un socio, el cliente debe seguir estos pasos:

1. En el menú de usuario de la esquina superior izquierda, seleccione **Parámetros de cuenta**.
2. En la página **Cuenta de empresa**, busque la sección **Conexiones de socio**.
3. Busque el partner que quiere administrar y, a continuación, seleccione **Quitar**.
4. Cuando se le pida que confirme la eliminación, seleccione **Confirmar**.

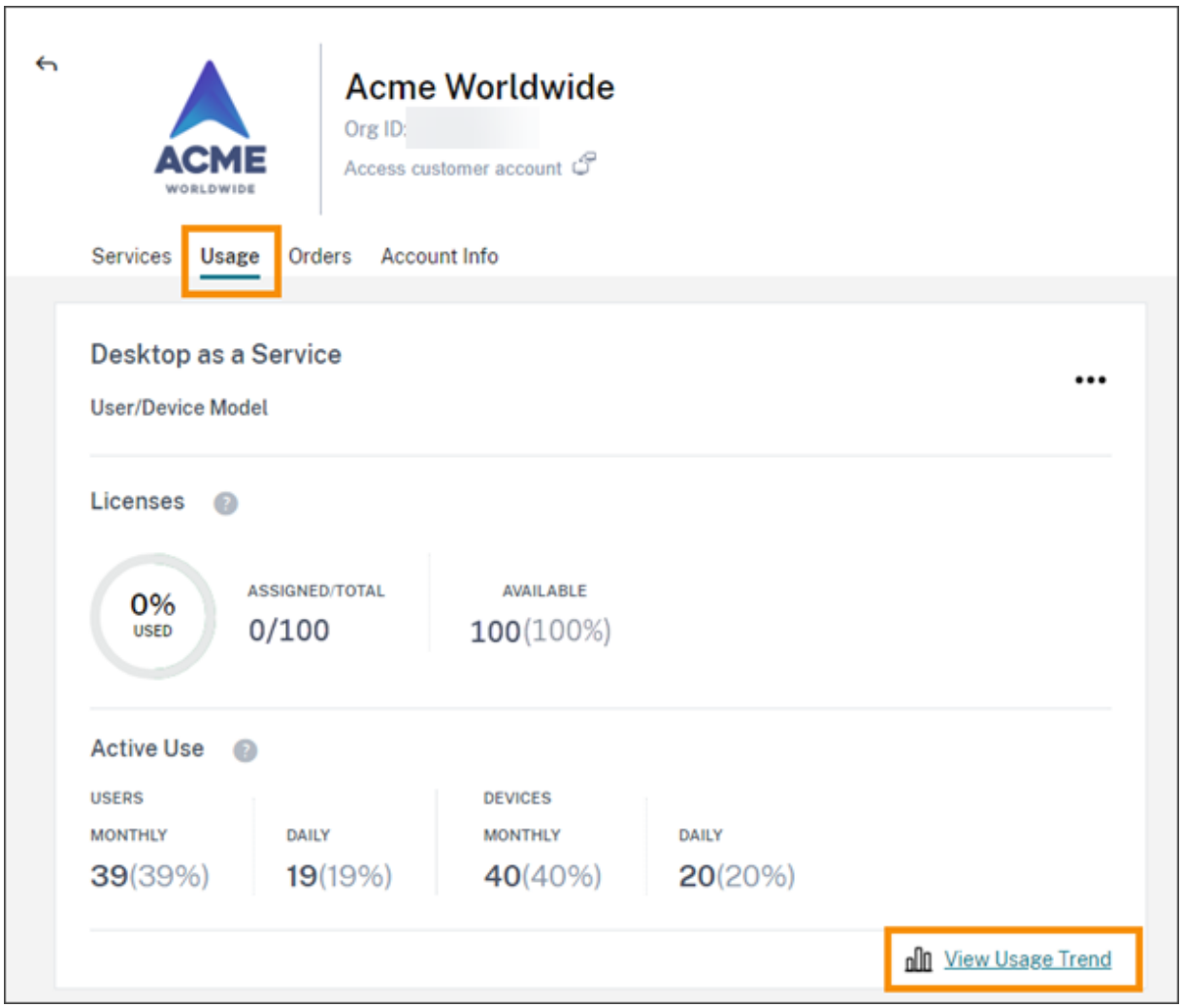
Tendencias de licencias

Los socios pueden ver la información sobre licencias de un cliente al seleccionar **Ver licencias** en el menú de tres puntos del panel de mandos del cliente.



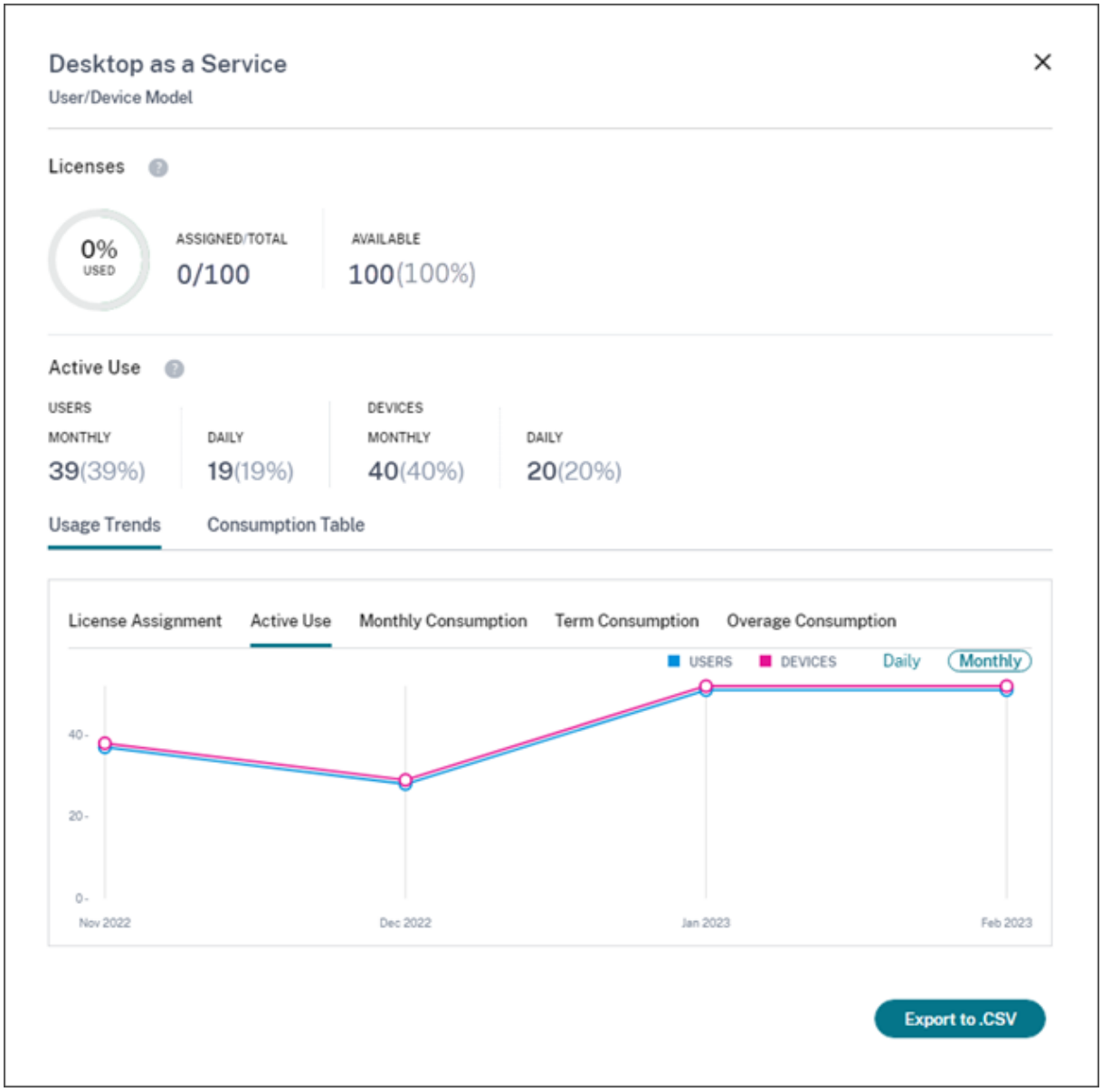
> **Nota:**
>
> Los socios de Citrix solo pueden ver la vista de resumen de Licencias y las tendencias históricas del uso activo. No pueden ver usuarios individuales que utilizan licencias para un servicio determinado.

Para ver el resumen sobre licencias del cliente para cada servicio, seleccione la ficha **Uso**. Para obtener más información sobre el uso, seleccione **Ver tendencia de uso** para el derecho de uso de los servicios que quiere ver.



Según el servicio, las tendencias de uso incluyen esta información:

- La proporción entre licencias asignadas y el total adquirido
- Usuarios activos mensuales y diarios
- Un desglose visual de las asignaciones de licencias, el uso activo de estas, el consumo por derecho de uso y el excedente de licencias.



Si fuera necesario, los socios pueden exportar esta información en un archivo CSV.

Uso del ancho de banda

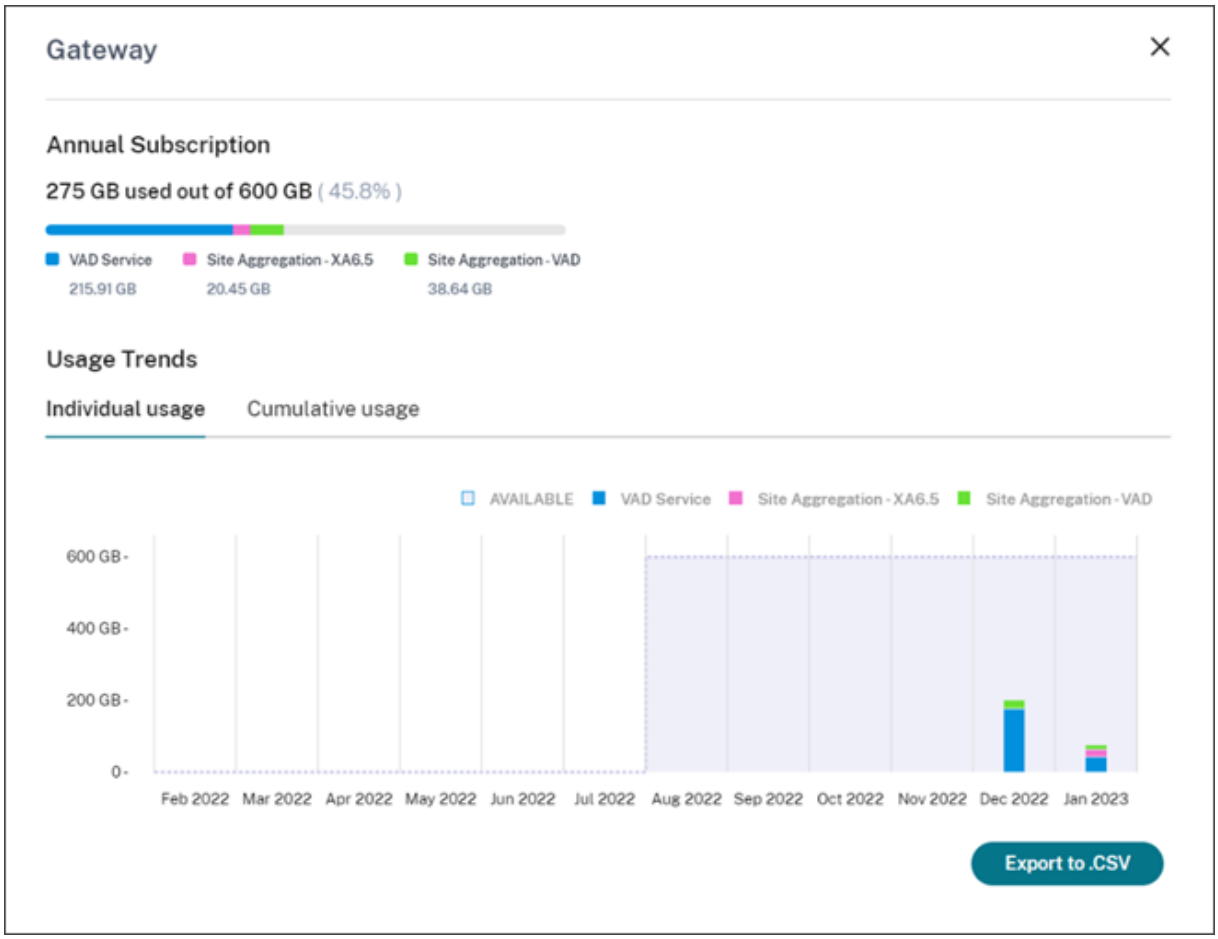
Para Citrix Gateway Service, el resumen sobre licencias incluye esta información:

- Uso total del ancho de banda en todos los derechos de uso del cliente.
- Uso total del ancho de banda desglosado según los derechos de uso mensuales, anuales y con plazos estipulados del cliente.
- Excedente total del mes actual. Para obtener más información sobre cómo se calcula el excedente, consulte Excedente.

Seleccione **Ver tendencia de uso** en el extremo derecho de la página de un derecho de uso para ver el resumen de uso. Selecciona **Ver gráfico de excedente** para ver el excedente de los últimos 12 meses.

Según el derecho de uso, las tendencias de uso incluyen esta información:

- La cantidad de ancho de banda consumido entre la implementación de Citrix DaaS (**VAD Service**) y la implementación local de Virtual Apps and Desktops con agregación de sitios.
- Un desglose visual del uso del ancho de banda para cada mes en el que se utilizó. (Derechos de uso mensuales)
- Un desglose visual del **Uso individual** del ancho de banda de cada mes del período de facturación. (Derechos de uso anuales y con plazos estipulados)
- Un desglose visual del **Uso acumulado** del ancho de banda acumulado durante cada mes del período de facturación. (Derechos de uso anuales y con plazos estipulados)



Si fuera necesario, los socios pueden exportar esta información en un archivo CSV.

Uso y licencias de cliente para Citrix Service Providers

La función de licencias de Citrix Cloud permite a los clientes de Citrix Service Providers (CSP) supervisar sus licencias y el uso de los productos de Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops) admitidos. Los CSP pueden iniciar sesión en la cuenta de Citrix Cloud de su cliente para ver y exportar esta información. Para obtener información, consulte estos artículos:

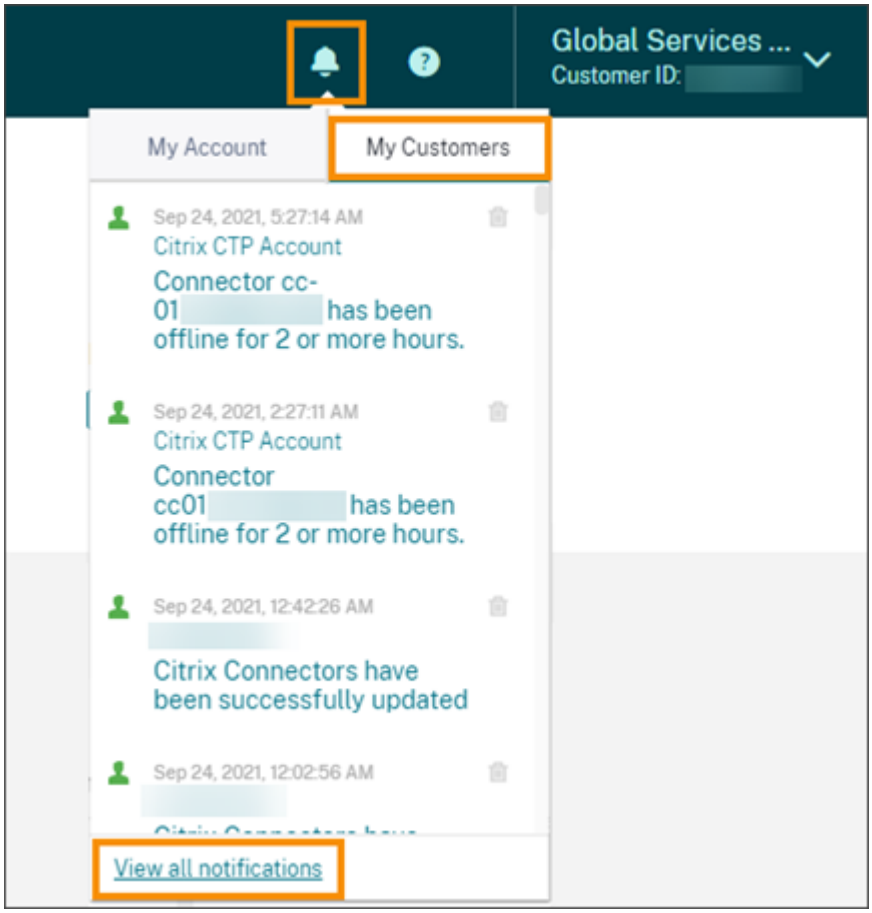
- Supervisión del uso y las licencias de los clientes para Citrix DaaS
- Supervisión del uso y las licencias de los clientes para Citrix DaaS Standard para Azure

Visibilidad de los socios en notificaciones y tíquets de asistencia de los clientes

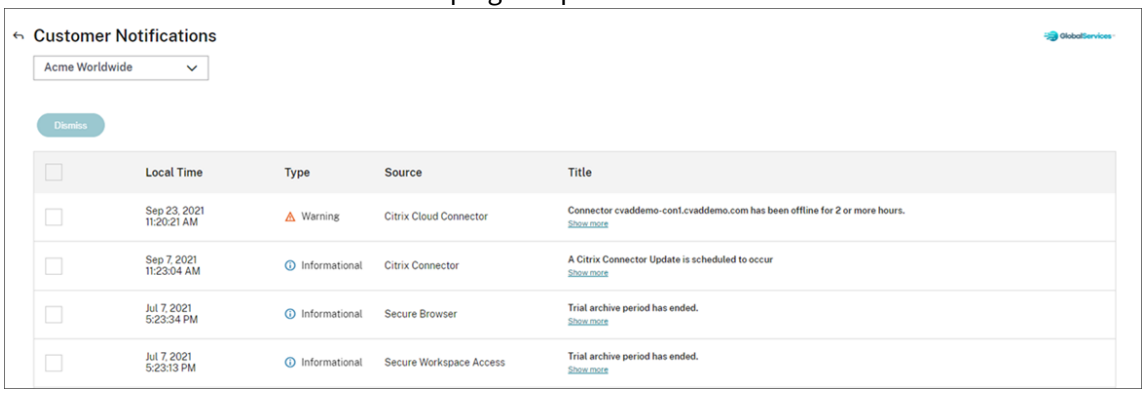
Los socios pueden ver notificaciones de sus clientes conectados. Los socios también pueden filtrar notificaciones específicas de un cliente y actuar con respecto a ellas, por ejemplo, descartarlas. Las notificaciones descartadas no aparecen para el socio. Sin embargo, los clientes pueden seguir viendo la notificación en su cuenta después de iniciar sesión en Citrix Cloud.

Para ver notificaciones de clientes:

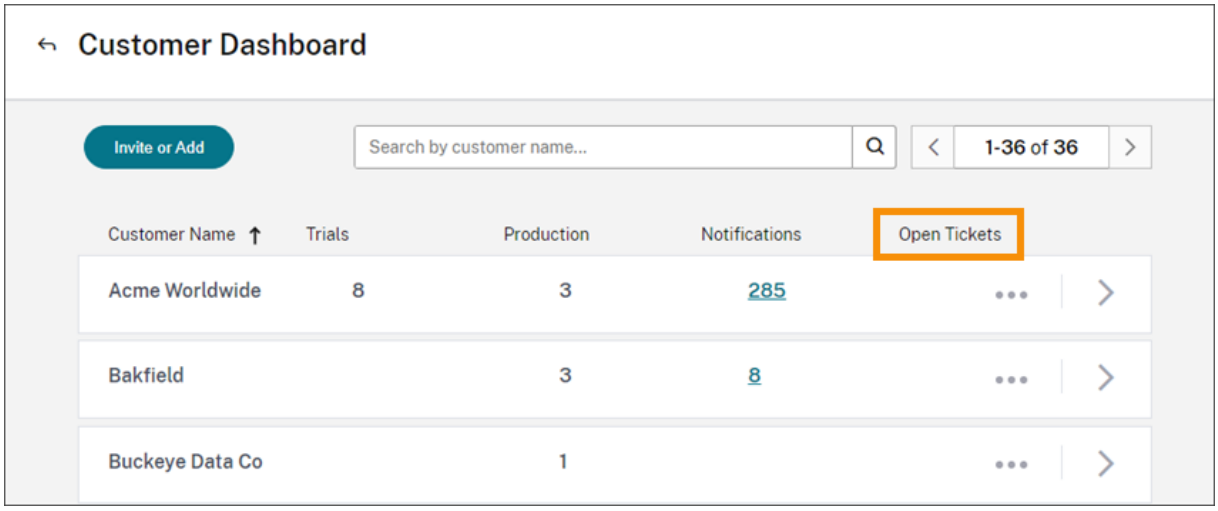
1. Haga clic en el icono de campana situado en la parte superior de la consola de administración, seleccione **Mis clientes** y, a continuación, seleccione **Ver todas las notificaciones**.



2. Seleccione un cliente en el menú desplegable para ver las notificaciones de ese cliente.



Los socios pueden ver la cantidad de tíquets de asistencia de sus clientes a través del panel de mandos de clientes.



Dominios federados para Citrix Service Providers (CSP)

Los *dominios federados* permiten a los usuarios del cliente utilizar credenciales de un dominio asociado a la ubicación de recursos del CSP para iniciar sesión en el espacio de trabajo. Esto le permite proporcionar espacios de trabajo dedicados a los usuarios de sus clientes con una URL de espacio de trabajo personalizada, como *customer.cloud.com*. La ubicación del recurso sigue estando en su cuenta de socio de Citrix Cloud. Puede proporcionar espacios de trabajo dedicados, junto con el espacio de trabajo compartido, a los que los clientes pueden acceder mediante la URL del espacio de trabajo del CSP (por ejemplo, csppartner.cloud.com). Para que los clientes puedan acceder a su espacio de trabajo dedicado, debe agregarlos a los dominios correspondientes que administre. Después de configurar el espacio de trabajo, los usuarios clientes pueden iniciar sesión en su espacio de trabajo y acceder a las aplicaciones y escritorios que haya puesto a disposición a través de Citrix DaaS.

Cuando quita un cliente de un dominio federado, los usuarios de ese cliente ya no pueden acceder a sus espacios de trabajo mediante las credenciales del dominio del socio.

Para obtener más información sobre el uso de dominios federados para entregar aplicaciones y escritorios, consulte Citrix DaaS para Citrix Service Providers.

Opciones de apariencia del espacio de trabajo para Citrix Service Providers

Puede configurar los colores y logotipos de su espacio de trabajo con temas personalizados. Para obtener información sobre cómo crear temas personalizados, consulte Personalizar la apariencia de los espacios de trabajo.

> **Nota**
>
> La temática personalizada es una función de arrendatario único. En la actualidad, no se admiten

> Citrix Service Providers en los que los arrendatarios del proveedor de servicios comparten una ubicación de recursos, Cloud Connectors y dominios de Active Directory (multiarrendatario). Los arrendatarios de Citrix Service Provider que tienen su propia ubicación de recursos dedicada, Cloud Connectors y dominio dedicado de Active Directory (arrendatario único) son plenamente compatibles.

Servicios de la nube

July 2, 2024

En este artículo se enumeran los servicios de la nube que se ofrecen a través de Citrix Cloud y se vincula a la documentación de producto de cada servicio. Para obtener descripciones de estos servicios y las ofertas en las que se incluyen, consulte Service Descriptions for Citrix Services.

Citrix Services

Análisis

- Analytics para la seguridad
- Analytics para el rendimiento
- Analytics: Uso

Citrix DaaS

Citrix DaaS Standard para Azure

Endpoint Management

Gateway

Adaptador ITSM para ServiceNow

Remote Browser Isolation

Secure Private Access

Servicio de grabación de sesiones

Virtual Apps Essentials

Virtual Desktops Essentials

Workspace Environment Management

NetScaler Services

Consola

Seguridad y entrega de aplicaciones

SD-WAN Orchestrator

Secure Internet Access

Web App Firewall