Citrix Workspace

Contents

Descripción general de Citrix Workspace

November 21, 2023

Citrix Workspace es una solución digital de espacios de trabajo que ofrece un acceso seguro y unificado a las aplicaciones, escritorios y contenido (recursos) en cualquier dispositivo y en cualquier lugar. Estos recursos pueden ser Citrix DaaS, aplicaciones de contenido, aplicaciones locales y móviles, aplicaciones web y SaaS y aplicaciones para explorador web.

Cómo funciona Citrix Workspace

Citrix Workspace agrega e integra los Citrix Cloud Services, posibilitando un acceso unificado a todos los recursos disponibles para los usuarios finales (suscriptores) en una ubicación de recursos. Los usuarios finales de Citrix Workspace se denominan suscriptores porque usted "suscribe"a los empleados a los servicios que pone a su disposición a través de sus espacios de trabajo.

Para obtener una descripción general de los servicios disponibles en Citrix Workspace, consulte Servicios alojados en la nube a través de Citrix Workspace.

A los suscriptores se muestra una imagen completa y unificada de cada recurso que se pone a su disposición a través de estos servicios en la interfaz de usuario (IU) de Citrix Workspace. Para obtener más información sobre la experiencia del suscriptor con la interfaz de usuario de Citrix Workspace, consulte Administrar la experiencia de los espacios de trabajo.

Los suscriptores acceden a los servicios que configura y habilita en **Configuración de Workspace**, ya sea a través del explorador con la URL de Workspace o a través de la aplicación Citrix Workspace, que sustituye a Citrix Receiver. Para obtener más información sobre cómo acceden los usuarios a sus espacios de trabajo, consulte Acceso a Workspace.

Los suscriptores se autentican en sus espacios de trabajo mediante el proveedor de identidades principal, que se configura en **Administración de acceso e identidad** y se habilita en **Configuración de Workspace**. A continuación, el suscriptor se autentica automáticamente en cada servicio alojado en la nube adquirido para Citrix Workspace, lo que contribuye a aumentar la seguridad y reduce los problemas de usabilidad. Para obtener más información sobre cómo configurar la autenticación de Workspace, Consulte Espacios de trabajo seguros

Descripción general

Citrix Workspace se configura a través de la **consola de Citrix Cloud**, en la que se encuentra la pantalla **Administración de acceso e identidad** y una interfaz de administración de Citrix Workspace llamada

Configuración de Workspace. Comenzar a trabajar con Citrix Workspace implica las siguientes tareas.

1. Asegurarse de estar preparado para implementar Citrix Workspace en la **consola de Citrix Cloud**, donde:
    - Incorporar los servicios basados en la nube.
    - Reunir el equipo de implementación.
    - Configurar la infraestructura y recursos.
2. Definir proveedores de identidades y cuentas en **Administración de acceso e identidad** para:
    - Administradores de Citrix Cloud.
    - Suscriptores de Citrix Workspace.
3. Configurar los espacios de trabajo en **Configuración de Workspace**, que incluye:
    - Acceso externo e interno.
    - Integración en los espacios de trabajo de los servicios configurados en la consola de Citrix Cloud.
    - Personalización de la apariencia del espacio de trabajo y de la experiencia del suscriptor una vez que inician sesión

Más allá de esta configuración básica, tiene otras opciones de seguridad, privacidad y optimización entre las que elegir. Las más comunes son:

- Configurar Single Sign-On (SSO) en DaaS en Citrix Workspace con el Servicio de autenticación federada (FAS) de Citrix. Por lo general, se adopta FAS si se utiliza un método de autenticación federada, como Okta o Azure Active Directory.

Para obtener una descripción general de las tareas y la información necesaria a medida que avanza en la implementación, consulte Primeros pasos en Citrix Workspace. Cada paso le guía a través de la consola de Citrix Cloud con instrucciones para tareas como configurar un proveedor de identidades y habilitar los servicios. El tutorial también proporciona acceso rápido a información técnica necesaria para formar el equipo de implementación y configurar la infraestructura y los recursos.

Servicios alojados en la nube a través de Citrix Workspace

Los suscriptores usan Citrix Workspace para acceder a los recursos proporcionados por los servicios alojados en la nube. Los clientes actuales de Citrix Cloud pueden hacer la transición a la experiencia de espacio de trabajo digital completa si llevan estos servicios a la solución Citrix Workspace.

En esta sección se describen los principales servicios alojados en la nube que se pueden habilitar para Citrix Workspace, en función de los derechos con que se cuente. Para obtener información sobre cómo configurar y habilitar el acceso a los servicios adquiridos, consulte Primeros pasos en Citrix Workspace.

Para obtener una descripción completa de cada edición de Citrix Workspace y las funciones incluidas, consulte la Tabla de funciones de Citrix Workspace.

Citrix DaaS

Citrix Workspace es el punto de acceso multiarrendatario y alojado en la nube a Citrix DaaS. Para configurar Citrix DaaS, siga los pasos descritos en Citrix DaaS.

Si es cliente de Virtual Apps and Desktops local, hay diferentes opciones para acceder a sus recursos a través de Citrix Workspace. La opción que elija dependerá de si quiere migrar completamente a la nube o si prefiere adoptar una solución híbrida, y de si piensa permitir el acceso externo. Para obtener más información sobre estas opciones, consulte Entregar DaaS con Citrix Workspace.

Aplicaciones web y SaaS, protegidas con el servicio Citrix Secure Private Access

Citrix Secure Private Access (anteriormente **Secure Workspace Access** y **Access Control Service**) proporciona funcionalidad Single Sign-On (SSO) a las aplicaciones web y SaaS que se integran en Workspace. El servicio también permite administrar los privilegios de acceso y las directivas de control que rigen los niveles de acceso a las aplicaciones web alojadas en la empresa en función de las credenciales del suscriptor.

Para obtener más información sobre las ventajas del **servicio Citrix Secure Private Access**, consulte este resumen técnico sobre acceso privado seguro.

Citrix Gateway Service

Citrix Gateway Service (anteriormente el **NetScaler Gateway Service**) se usa con **Citrix Secure Private Access** para un entorno totalmente alojado en la nube administrado por Citrix.

Citrix Gateway Service ofrece una experiencia unificada con aplicaciones SaaS y Virtual Apps and Desktops, al proporcionar conectividad externa a los espacios de trabajo basada en una infraestructura de directivas avanzada.

Siga los pasos para configurar Citrix Gateway Service y, a continuación, pruebe y comparta la URL del espacio de trabajo con sus suscriptores para darles acceso remoto. Para obtener más información sobre la configuración de aplicaciones SaaS en Citrix Gateway Service, consulte Asistencia para aplicaciones de software como servicio.

Citrix Remote Browser Isolation Service

Integre **Citrix Remote Browser Isolation Service** en sus espacios de trabajo para aislar la navegación por Internet y proteger la red corporativa de los ataques por explorador web. Cuando los suscriptores

van a la URL de Workspace, se muestran sus exploradores web publicados, junto con otras aplicaciones y escritorios que se hayan configurado en otros servicios de Citrix Cloud.

Para dar a los suscriptores acceso a un explorador web aislado remoto, configure Remote Browser Isolation y, a continuación, pruebe y comparta la URL del espacio de trabajo con sus suscriptores.

Citrix Endpoint Management

Citrix Endpoint Management le permite administrar directivas de dispositivos y aplicaciones con una seguridad estricta en cuanto respecta a la identidad, los dispositivos, las aplicaciones, los datos y las redes. La integración con Citrix Workspace es diferente para clientes nuevos y existentes. Para obtener más información sobre la integración de Endpoint Management con Citrix Workspace, consulte Integración en la experiencia de Citrix Workspace.

Citrix Analytics

El servicio **Citrix Analytics** recopila y proporciona información sobre todos sus suscriptores de Citrix Workspace. Hay diferentes ofertas de Citrix Analytics disponibles para usted en función de sus derechos. Estas son **Citrix Analytics for Security**, **Citrix Analytics for Performance** y **Citrix Analytics (Uso)**. Para obtener más información sobre estos servicios, consulte Citrix Analytics.

Novedades

November 21, 2023

Citrix tiene como objetivo entregar nuevas funciones y actualizaciones a los clientes de Citrix Workspace tan pronto como estén disponibles. Las versiones iniciales se aplican en los sitios internos de Citrix y luego se aplican gradualmente en los entornos de los clientes.

Para obtener más información sobre el acuerdo de nivel de servicio en cuanto a su disponibilidad y la escalabilidad en la nube, consulte Contrato de nivel de servicio de Citrix Cloud. Para supervisar las interrupciones de servicio y el mantenimiento programado, consulte el Panel de estado del servicio.

Novedades de Citrix Workspace

Manténgase informado sobre las mejoras y actualizaciones más recientes de Citrix Workspace para aprovechar todo el potencial de nuestra tecnología. Incorpore las nuevas actualizaciones de Citrix Workspace para aumentar al máximo la productividad de los usuarios y mejorar la calidad de sus interacciones.

- Novedades de la plataforma Workspace
- Novedades de la interfaz de usuario de Workspace
- Novedades en Global App Configuration Service

Aplicación Citrix Workspace en diferentes plataformas

Utilice los siguientes enlaces para saber más acerca de las nuevas funciones y mejoras de la **aplicación Citrix Workspace** para sus plataformas favoritas.

- Android
- ChromeOS
- HTML5
- iOS
- Linux
- Mac
- Microsoft Teams
- Windows
- Tienda Windows

Consulte también las novedades de Citrix Enterprise Browser.

Novedades de la plataforma Workspace

November 21, 2023

Citrix tiene como objetivo entregar nuevas funciones y actualizaciones a los clientes de Citrix Workspace tan pronto como estén disponibles. Las nuevas versiones añaden valor al producto y no hay motivo para retrasar el momento de actualizar.

Para usted, este proceso es transparente. Las actualizaciones iniciales se aplican solo en los sitios internos de Citrix y luego se aplican gradualmente en los entornos de los clientes. La entrega por incrementos de actualizaciones maximiza la calidad de los productos y su disponibilidad.

Para obtener más información sobre el acuerdo de nivel de servicio en cuanto a su disponibilidad y la escalabilidad en la nube, consulte Contrato de nivel de servicio de Citrix Cloud. Para supervisar las interrupciones de servicio y el mantenimiento programado, consulte el Panel de estado del servicio.

Noviembre de 2023

Configurar un dominio personalizado: Disponibilidad general

La función de dominio personalizado ya está disponible de forma generalizada. Puede configurar un dominio personalizado para su espacio de trabajo, que le permite utilizar un dominio de su elección para acceder a su almacén de Citrix Workspace. A continuación, puede utilizar este dominio, en lugar del dominio de cloud.com asignado, para acceder desde un explorador web y desde las aplicaciones de Citrix Workspace. Para obtener más información, consulte Configurar un dominio personalizado.

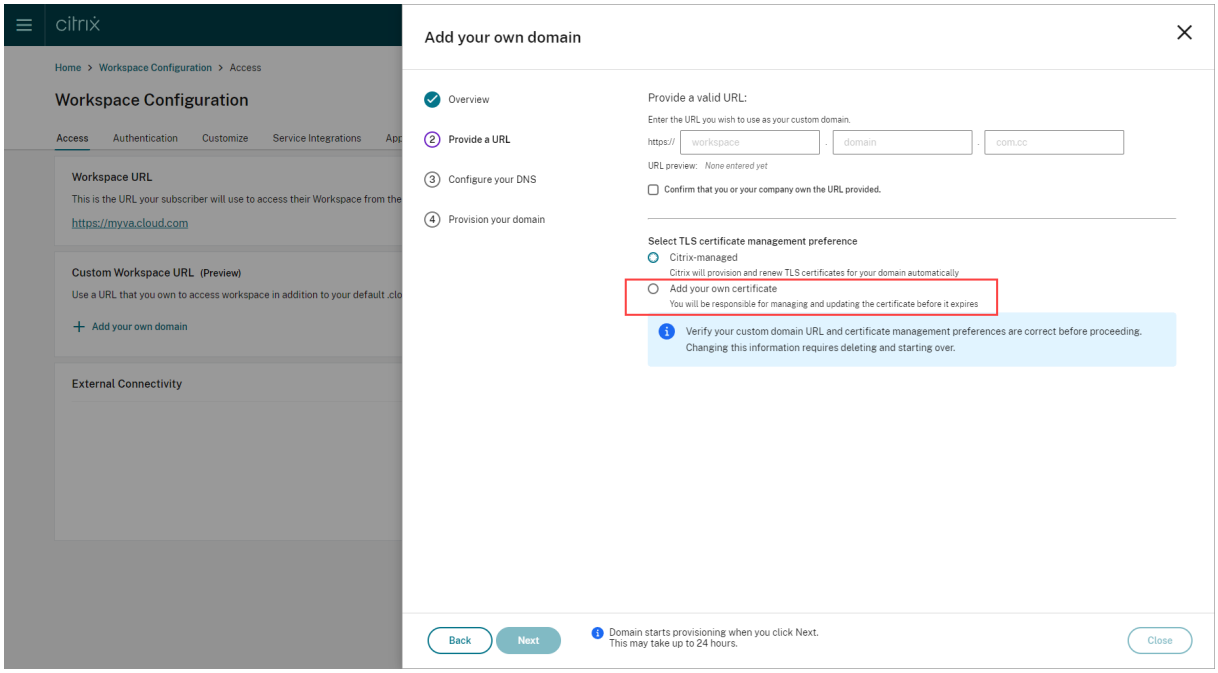
Agosto de 2023

Agregar su propio certificado TLS para un dominio personalizado (Technical Preview)

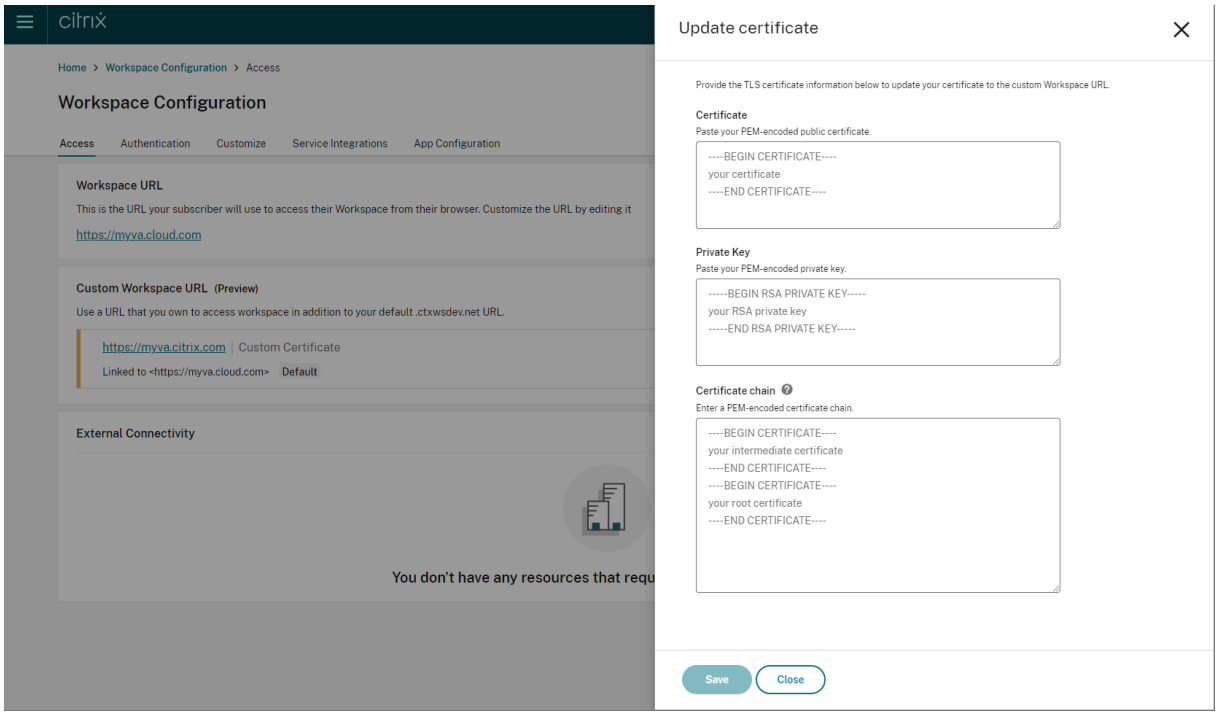
Ahora puede cargar su propio certificado TLS para la autenticación mientras configura una URL de Workspace personalizada. Antes de cargar un certificado, asegúrese de que dicho certificado cumple las siguientes condiciones.

- Debe estar codificado en PEM.
- Debe seguir siendo válido durante, al menos, los próximos 30 días.
- Debe usarse exclusivamente para la URL de Workspace personalizada; no se aceptan certificados comodín.
- El nombre común del certificado debe coincidir con el dominio personalizado.
- Los SAN del certificado deben ser para el dominio personalizado; no se permite ningún SAN adicional.
- La duración de la validez del certificado no debe superar los 10 años.

Para agregar un certificado, vaya a la página **Proporcione una URL** y seleccione la opción Agregue su propio certificado en **Seleccione la preferencia de administración de certificados TLS**.



A continuación, puede añadir su certificado en la página **Agregue su propio certificado**.



Para obtener más información, consulte Agregar un dominio personalizado.

> **Nota:**
>
> Puede enviar comentarios sobre esta función Technical Preview a través del formulario de Podio adjunto.

Mayo de 2023

Configurar un dominio personalizado (Technical Preview). Puede configurar un dominio personalizado para su espacio de trabajo, que le permite utilizar un dominio de su elección para acceder a su almacén de Citrix Workspace. A continuación, puede utilizar este dominio, en lugar del dominio de cloud.com asignado, para acceder desde un explorador web y desde las aplicaciones de Citrix Workspace. Para obtener más información, consulte Configurar un dominio personalizado (Technical Preview).

Marzo de 2023

Configuración adicional de tiempo de espera por inactividad:. Ahora puede habilitar una configuración adicional de tiempo de espera por inactividad para los usuarios de dispositivos de escritorio y móviles de la aplicación Workspace. Para obtener más información, consulte Personalizar las directivas de seguridad y privacidad.

Diciembre de 2022

Opción adicional de configuración para el envío de anuncios personalizados:. Ahora puede establecer la ubicación de la página al configurar el **envío de anuncios personalizados** en la parte superior o en la inferior. Para obtener más información, consulte Personalizar las directivas de seguridad y privacidad.

Disponible en chino tradicional. Citrix Workspace ya está disponible en chino tradicional.

Octubre de 2022

Disponible en coreano. Citrix Workspace ya está disponible en coreano.

Función para personalizar parámetros de la aplicación Citrix Workspace. Los administradores ya pueden configurar los parámetros de la aplicación Citrix Workspace para las plataformas iOS, Android, HTML5, Mac y Windows mediante Global App Configuration Service.

Agosto de 2022

Mejoras en la experiencia de inicio de Workspace Cuando un usuario inicia su espacio de trabajo a través de la web o un explorador, se desencadena una notificación que muestra el estado de inicio. Si el usuario intenta cerrar el explorador cuando hay un inicio en curso, se le pide que confirme la operación y se le informa de que hay un inicio de sesión en curso. Para obtener más información, consulte Primeros pasos en Citrix Workspace.

Junio de 2022

Función de continuidad del servicio con Safari. Las extensiones web de Citrix Workspace ponen la continuidad del servicio a disposición de los usuarios que acceden a sus aplicaciones y escritorios a través de un explorador. Para obtener más información, consulte Continuidad del servicio en exploradores.

Mayo de 2022

Nueva opción de configuración para el proveedor de identidades federadas: Habilite o inhabilite el proveedor de identidades federadas para permitir a los suscriptores que se autentiquen al iniciar sesión en Workspace. Para obtener más información, consulte Personalizar las interacciones en espacios de trabajo.

Período de reautenticación de la aplicación Workspace (disponibilidad general): Los períodos de reautenticación permiten a los suscriptores mantener la sesión abierta en Workspace sin que se les pida que inicien sesión cada vez que acceden a su espacio de trabajo. Al iniciar sesión a través de la aplicación Workspace, los suscriptores aceptan mantener la sesión abierta. Las sesiones de los suscriptores permanecen abiertas durante el período de reautenticación, siempre que utilicen sus aplicaciones y escritorios. Para obtener más información sobre esta función, consulte Establecer un período de reautenticación para la aplicación Citrix Workspace.

Compatibilidad con Continuidad del servicio en iOS: Continuidad del servicio ya está disponible en la aplicación Citrix Workspace para iOS de forma general. Para obtener más información, consulte Continuidad del servicio.

Nuevos códigos de error para Continuidad del servicio: Ya hay disponibles nuevos códigos de error para ayudar a solucionar problemas de conexiones fallidas de Continuidad de servicio. Para obtener más información, consulte Continuidad del servicio.

Marzo de 2022

Función de continuidad del servicio en Android y iOS: Ahora se ofrece la continuidad del servicio en la aplicación Citrix Workspace para Android como disponibilidad general y la aplicación Citrix Workspace para iOS en Tech Preview. Para obtener más información, consulte Continuidad del servicio.

Febrero de 2022

Función de continuidad del servicio en la aplicación Citrix Workspace para Android (disponibilidad general) y la aplicación Citrix Workspace para iOS (Tech Preview): La continuidad del servicio

permite a los usuarios conectarse a sus aplicaciones y escritorios virtuales incluso durante las interrupciones del servicio. Ahora se ofrece en la aplicación Citrix Workspace para Android como disponibilidad general y en la aplicación Citrix Workspace para iOS como Tech Preview. Para obtener más información, consulte Continuidad del servicio.

Envío de anuncios personalizados y directiva de inicio de sesión personalizada: Ahora hay dos nuevas funciones disponibles para todos los clientes. Estas funciones permiten a los administradores de Workspace mostrar su propia pancarta persistente después de iniciar sesión y un mensaje personalizado o el contrato de licencia antes de iniciar sesión en la aplicación Citrix Workspace. Para obtener más información, consulte Personalizar las directivas de seguridad y privacidad.

Diciembre de 2021

Elimine la pantalla de inicio de sesión dividida predeterminada para los usuarios empleados y clientes de Citrix Content Collaboration: Citrix Workspace ahora le permite habilitar un flujo de inicio de sesión único para los usuarios clientes y empleados. Para obtener más información, consulte Crear un flujo de inicio de sesión de usuario unificado.

Compatibilidad con la continuidad del servicio en exploradores con la aplicación Citrix Workspace para Mac: Las extensiones web de Citrix Workspace ponen la continuidad del servicio a disposición de los usuarios que acceden a sus aplicaciones y escritorios a través de un explorador web. Esta funcionalidad ahora es compatible en dispositivos que ejecutan la aplicación Citrix Workspace para Mac. Para obtener más información, consulte Continuidad del servicio.

Noviembre de 2021

Temas orientados a las directivas: Puede crear y priorizar temas de Workspace, y agregar cada tema a diferentes grupos de usuarios en **Configuración de Workspace**. Para obtener más información, consulte Personalizar la apariencia de los espacios de trabajo.

Octubre de 2021

Compatibilidad con idiomas en firma electrónica: La funcionalidad de firma electrónica ahora es compatible con italiano y portugués de Brasil, además de los siguientes idiomas: alemán, francés, español, japonés, holandés y chino simplificado. Para obtener más información, consulte RightSignature multi-language support.

Compatibilidad de FAS con múltiples ubicaciones de recursos (disponibilidad generalizada): Citrix Workspace admite ahora Single Sign-On en aplicaciones y escritorios virtuales a través de varias ubicaciones de recursos. Además, los servidores FAS de una ubicación de recursos se pueden designar como principales o secundarios a efectos de conmutación por error para servidores FAS de otras

ubicaciones de recursos. Para obtener más información, consulte Habilitar Single Sign-On para espacios de trabajo con el Servicio de autenticación federada de Citrix.

Septiembre de 2021

Presentación de la aplicación Citrix Workspace para HTML5 en Citrix Workspace: La aplicación Citrix Workspace para HTML5 ofrece al usuario la posibilidad de disfrutar de la experiencia de Citrix Workspace en exploradores web sin necesidad de instalar nada el dispositivo. Para obtener más información sobre la aplicación Citrix Workspace para HTML5, incluidas las nuevas funcionalidades, consulte la documentación de producto de la aplicación Citrix Workspace para HTML5.

Compatibilidad con la continuidad del servicio en exploradores (disponibilidad generalizada): Las extensiones web de Citrix Workspace ponen la continuidad del servicio a disposición de los usuarios que acceden a sus aplicaciones y escritorios a través de un explorador web. Esta funcionalidad está prevista para los exploradores Google Chrome y Microsoft Edge en dispositivos Windows. Para obtener más información, consulte Continuidad del servicio en exploradores.

Julio de 2021

Directiva de contrato de licencia de suscriptor personalizado: Puede presentar a los suscriptores una directiva de contrato de uso personalizado para que la lean y la acepten antes de iniciar sesión en su espacio de trabajo. Para obtener más información sobre esta función, consulte Configurar una directiva de inicio de sesión.

Período de reautenticación de la aplicación Workspace (Tech Preview): Los periodos de reautenticación permiten a los suscriptores mantener la sesión abierta en Workspace sin que se les pida que inicien sesión cada vez que acceden a su espacio de trabajo. Al iniciar sesión a través de la aplicación Workspace, los suscriptores aceptan mantener la sesión abierta. Las sesiones de los suscriptores permanecen abiertas durante el período de reautenticación, siempre que utilicen sus aplicaciones y escritorios. Para obtener más información sobre esta función de Tech Preview, consulte Establecer un período de reautenticación para la aplicación Citrix Workspace.

Configuración de la ubicación de red con Citrix Cloud: Ahora puede configurar las ubicaciones de red a través de la consola de administración de Citrix Cloud, además de utilizar el script de PowerShell proporcionado por Citrix. Para obtener más información sobre esta función, consulte Optimizar la conectividad a los espacios de trabajo con conexión directa de carga de trabajo.

Junio de 2021

Compatibilidad de FAS con múltiples ubicaciones de recursos (Tech Preview): Citrix Workspace admite ahora Single Sign-On en aplicaciones y escritorios virtuales a través de varias ubicaciones de

recursos. Los servidores FAS de una ubicación de recursos se pueden designar como principales o secundarios a efectos de conmutación por error para servidores FAS de otras ubicaciones de recursos. Para obtener más información sobre esta función en Tech Preview, consulte Habilitar Single Sign-On para espacios de trabajo con el Servicio de autenticación federada de Citrix.

Compatibilidad con la continuidad del servicio en exploradores (Technical Preview): Las extensiones web de Citrix Workspace ponen la continuidad del servicio a disposición de los usuarios que acceden a sus aplicaciones y escritorios a través de un explorador web. Esta modalidad de Technical Preview está prevista para los exploradores Google Chrome y Microsoft Edge en dispositivos Windows. Para obtener más información, consulte Continuidad del servicio en exploradores.

Disponibilidad general de continuidad del servicio: La continuidad del servicio permite a los usuarios conectarse a sus aplicaciones y escritorios virtuales, incluso durante interrupciones en componentes de Citrix Cloud o en nubes públicas y privadas. Para obtener más información, consulte Continuidad del servicio.

Aplicación Citrix RightSignature disponible: Aproveche la aplicación de Citrix, una solución de firmas electrónicas incluida en Workspace Premium y Premium Plus, para solicitar firmas electrónicas en documentos desde cualquier dispositivo a través de Citrix Workspace. Para obtener más información, consulte Configurar la aplicación Citrix RightSignature.

Mayo de 2021

Temas personalizados (Technical Preview): La personalización de la apariencia de Workspace para los suscriptores ahora admite temas personalizados que se pueden asignar a diferentes grupos de usuarios. Cree, personalice y priorice temas para que a los suscriptores de esos grupos de usuarios se les presente el tema de espacio de trabajo adecuado cuando inicien sesión. Para obtener más información, consulte Personalizar la apariencia de los espacios de trabajo.

Compatibilidad con idiomas en firma electrónica: La funcionalidad de firma electrónica ahora es compatible con los siguientes idiomas: alemán, francés, español, japonés, holandés y chino simplificado. Para obtener más información, consulte RightSignature multi-language support.

Febrero de 2021

Cambio de contraseña de cuenta: Los suscriptores pueden cambiar su contraseña de dominio desde Citrix Workspace. Los administradores también pueden proporcionar instrucciones relativas a las contraseñas a los suscriptores para crear contraseñas válidas complejas conforme a la directiva de contraseñas de la organización. Para obtener más información, consulte Permitir a los suscriptores cambiar la contraseña de su cuenta.

Diciembre de 2020

Continuidad del servicio (Technical Preview): La continuidad del servicio permite a los usuarios conectarse a Citrix DaaS, incluso durante interrupciones de servicio de componentes de Citrix Cloud o de nubes públicas o privadas. Para obtener más información, consulte Continuidad del servicio.

Octubre de 2020

Preparado para FedRAMP: Citrix Workspace está preparado para FedRAMP al implementarse en Citrix Cloud Government. FedRAMP es un programa que promociona estándares de seguridad para los servicios en la nube utilizados por organizaciones gubernamentales de Estados Unidos. Ahora las organizaciones gubernamentales estadounidenses que requieren servicios en la nube preparados para FedRAMP pueden usar Citrix Workspace y servicios de Citrix DaaS para entregar Citrix DaaS. Para obtener más información, consulte Citrix Cloud Government.

Mayo de 2020

Guía de primeros pasos en Citrix Workspace: Ahora Citrix Workspace incluye un tutorial paso a paso para ayudarle a entregar espacios de trabajo rápidamente a los usuarios finales. El tutorial le guía a través de la consola de Citrix Cloud para que pueda configurar un proveedor de identidades, agregar administradores y habilitar la autenticación y los servicios del espacio de trabajo. Para obtener una descripción general de las tareas y el acceso rápido a las instrucciones que necesita, consulte Primeros pasos en Citrix Workspace.

Diciembre de 2019

Servicio de ubicación de red: Ahora puede garantizar la redirección de usuarios que inician aplicaciones y escritorios en Workspace desde la red corporativa directamente a sus agentes VDA. De esta forma, se omite la puerta de enlace y se agilizan las sesiones de DaaS. Para obtener más información sobre este servicio y las instrucciones de configuración, consulte Optimizar la conectividad con los espacios de trabajo mediante el servicio de ubicación de red.

Mejoras para las aplicaciones recientes y favoritas: Las aplicaciones recientes y favoritas se cargan primero en Workspace, por lo que los usuarios pueden iniciar de inmediato las aplicaciones y escritorios que utilizan habitualmente.

Novedades en la interfaz de usuario (IU) de Workspace

November 21, 2023

En las siguientes secciones, se indican las nuevas funciones de la versión actual y las versiones anteriores de la interfaz de usuario en Workspace.

> **Nota:**
>
> - Para obtener más información sobre la nueva IU, consulte Nueva interfaz de usuario de Workspace.
> - Para obtener más información sobre el administrador de actividades, consulte Administrador de actividades.

Novedades de la versión 23.46

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

Problemas resueltos

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

Problemas conocidos

No hay nuevos problemas conocidos.

Versiones anteriores

En esta sección se proporciona información sobre las nuevas funciones y los problemas resueltos en las versiones anteriores que seguimos desarrollando.

23.45

Novedades

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

Problemas resueltos

- La indexación de Google Search se ha quitado de Citrix Web para evitar que las URL internas aparezcan en los resultados de búsqueda de Google. Sin embargo, si Google ya ha indexado sus URL, deberá seguir los pasos necesarios para quitarlas. Para obtener más información, consulte el documento Remove a page hosted on your site from Google.

23.44

Novedades

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

Problemas resueltos

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

23.43

Novedades

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

Problemas resueltos

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

23.42

Novedades

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

Problemas resueltos

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

23.41

Novedades

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

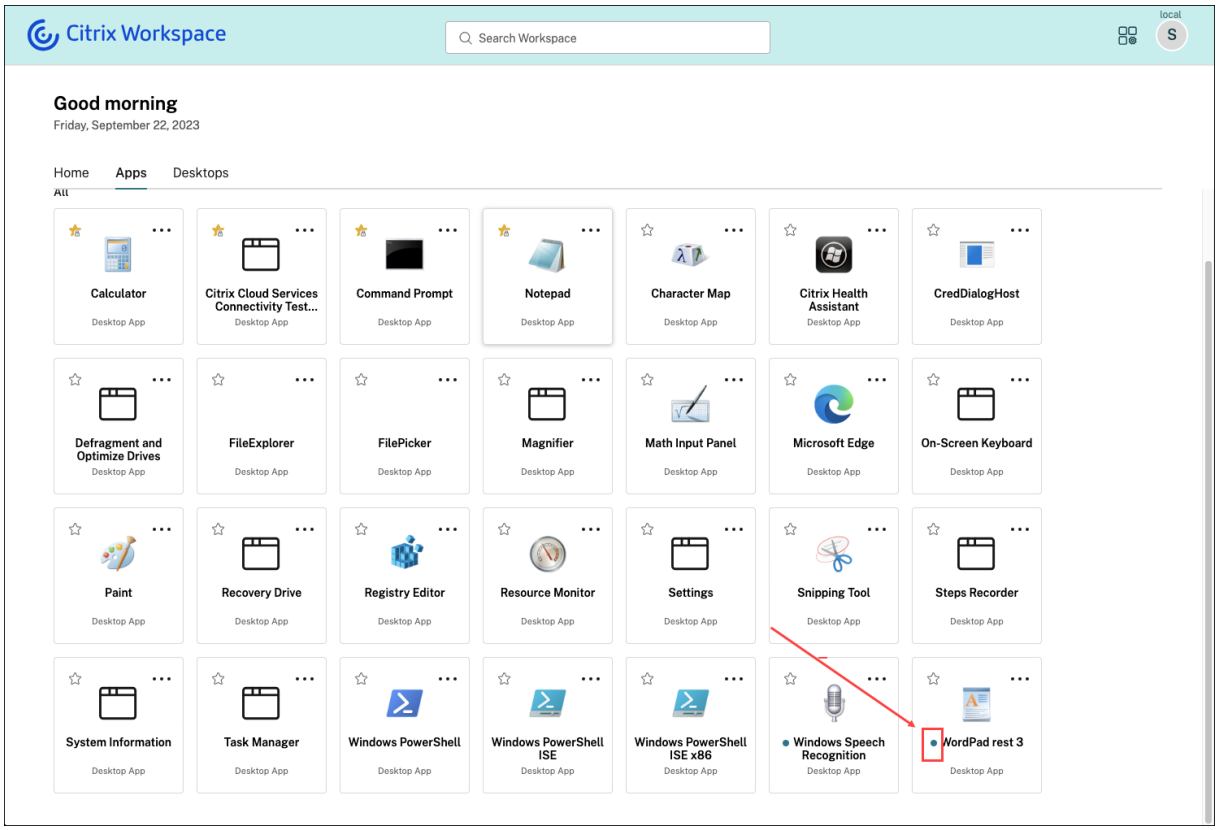
Problemas resueltos

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

23.40

Novedades

Detección simplificada de nuevas aplicaciones Los usuarios finales ahora pueden detectar fácilmente las aplicaciones recién agregadas, lo que facilita la búsqueda y el uso de las aplicaciones más recientes. Cuando un administrador entrega una nueva aplicación a un usuario final, aparece resaltada en el espacio de trabajo de este último y se muestra un punto verde en el mosaico de la aplicación.



Problemas resueltos

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

23.39

Novedades

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

Problemas resueltos

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

23.38

Novedades

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

Problemas resueltos

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

23.37

Novedades

Nueva interfaz de usuario de Workspace: Disponibilidad general La nueva interfaz de usuario de Workspace ya está disponible de forma general. Presenta nuevas prestaciones en su interfaz de usuario, además de un aspecto moderno y más despejado. Las mejoras de la interfaz de usuario se aprecian tanto en la web como en equipos de escritorio y dispositivos móviles. Los administradores pueden habilitarla para sus usuarios finales desde **Configuración de Workspace** > **Personalizar** > **Funciones**. Para obtener más información, consulte Nueva interfaz de usuario de Workspace.

> **Nota:**
>
> De forma predeterminada, el nuevo botón de la interfaz de usuario estará inhabilitado durante los próximos 6 meses, a menos que los administradores lo habiliten. Transcurridos 6 meses, la nueva interfaz de usuario se habilitará para todos los usuarios de forma predeterminada y se

> retirará la interfaz de usuario actual. Los administradores deben realizar la transición de sus usuarios a la nueva interfaz de usuario en los próximos 6 meses.

Administrador de actividades: Disponibilidad general La función del administrador de actividades ya está disponible de forma general en la nueva interfaz de usuario para la nube. El administrador de actividades es una función simple pero potente que permite a los usuarios administrar sus recursos de manera eficaz. Mejora la productividad al facilitar acciones rápidas en aplicaciones y escritorios activos y desconectados desde cualquier dispositivo. Los administradores pueden habilitar esta función para sus usuarios finales desde **Configuración de Workspace** > **Personalizar** > **Funciones** > **Administrador de actividades**. Para obtener más información, consulte Habilitar el administrador de actividades.

Una vez habilitada, las aplicaciones y los escritorios que están activos o desconectados se muestran en el panel del administrador de actividades. Los usuarios finales pueden hacer clic en el icono de tres puntos (...) para llevar a cabo acciones rápidas.

Se pueden realizar estas acciones para aplicaciones y escritorios activos.

- **Desconectar**: Desconecta la sesión remota, pero las aplicaciones y los escritorios están activos en segundo plano.
- **Cerrar sesión**: Cierra la sesión en curso. Se cierran todas las aplicaciones de las sesiones y se pierden los archivos no guardados.
- **Apagar**: Cierra los escritorios desconectados.
- **Forzar cierre**: Apaga el escritorio por la fuerza en caso de problemas técnicos.
- **Reiniciar**: Apaga el escritorio y lo inicia de nuevo.

El administrador de actividades también permite a los usuarios finales interactuar con sus aplicaciones y escritorios desconectados. Asegúrese de haber actualizado DDC a la versión más reciente (115). Para obtener más información, consulte Aplicaciones y escritorios desconectados.

Problemas resueltos

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

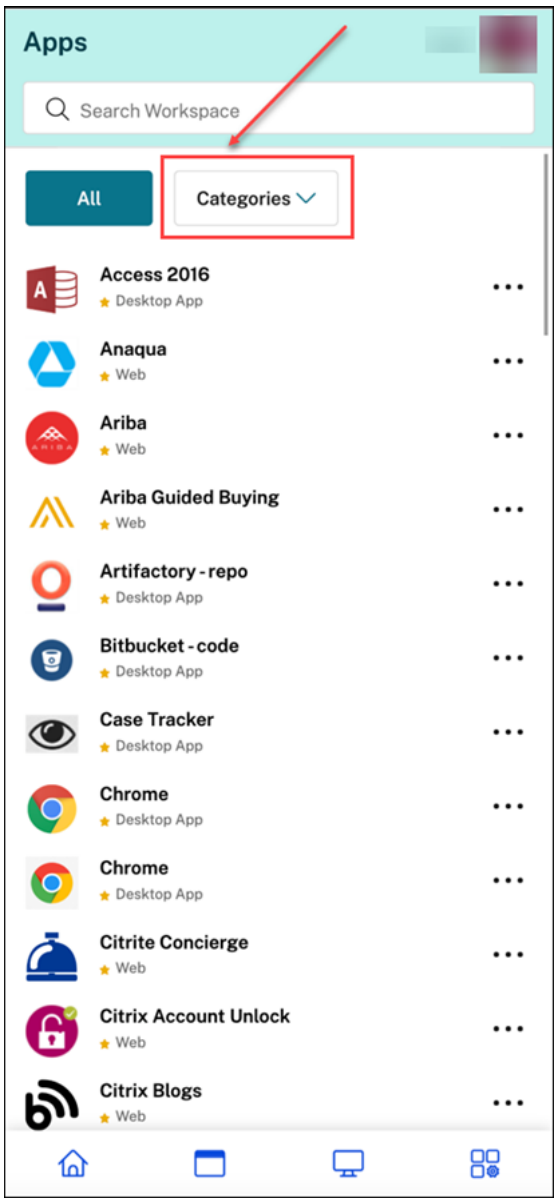
Problemas conocidos

- El panel del administrador de actividades muestra las sesiones activas en todos los almacenes en los que el usuario tiene la sesión iniciada.
- Las operaciones del administrador de actividades, como cerrar sesión, desconectar, etc., no están disponibles para aplicaciones que tienen habilitadas directivas de App Protection.

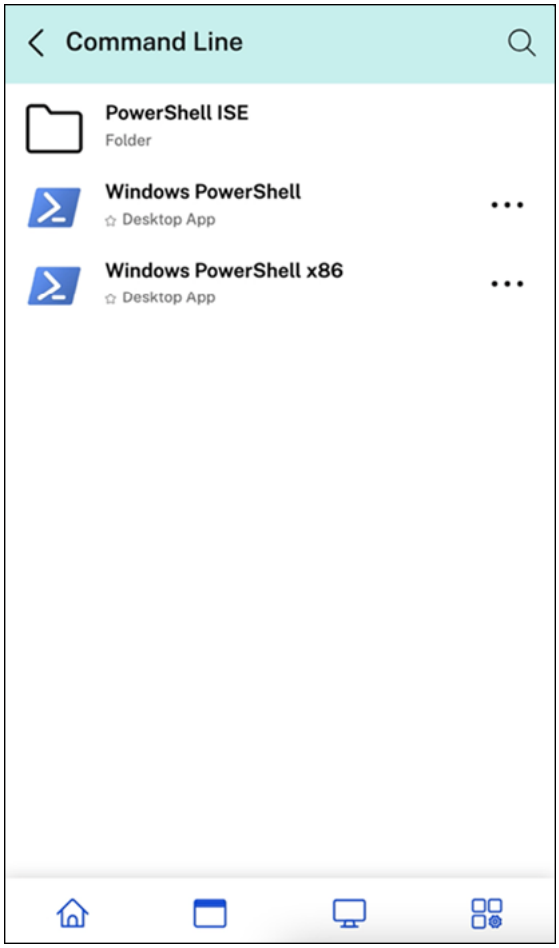
23.36

Novedades

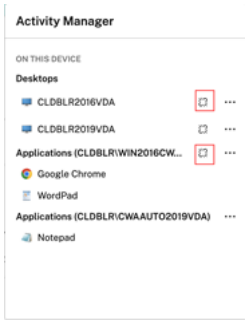
Ver subcategorías de aplicaciones en plataformas móviles Ahora, los usuarios finales pueden ver sus aplicaciones organizadas en categorías y subcategorías en dispositivos Android e iOS, lo que proporciona un acceso fácil y una agradable experiencia de navegación por las aplicaciones. Para ver las categorías, vaya a la ficha Aplicaciones y haga clic en el menú desplegable Categorías.



Seleccione la categoría correspondiente; se mostrará una lista de subcategorías y aplicaciones disponibles en función de la configuración realizada por el administrador. Las subcategorías se muestran como carpetas que pueden contener más subcarpetas o aplicaciones según la configuración de administración. Para obtener más información, consulte Agregar ruta de carpeta

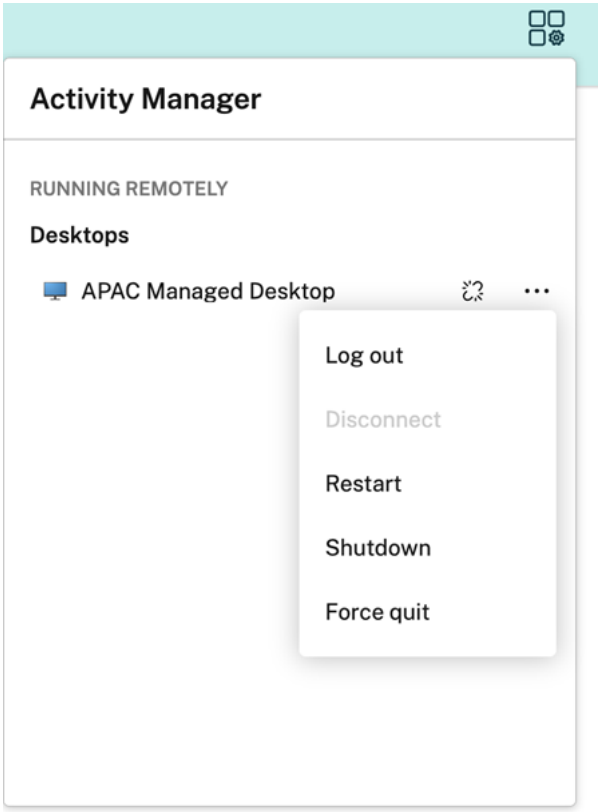


Administrar sesiones desconectadas en el administrador de actividades desde cualquier dispositivo Ahora, el administrador de actividades permite a los usuarios finales ver y realizar acciones en aplicaciones y escritorios que se ejecutan en modo desconectado, ya sea de forma local o remota. Las sesiones se pueden administrar desde dispositivos móviles o de escritorio, lo que permite a los usuarios finales realizar acciones sobre la marcha. Realizar acciones en sesiones desconectadas, como cerrar la sesión o el apagado, promueve el uso optimizado de recursos y reduce el consumo de energía.



- Las aplicaciones y los escritorios desconectados se muestran en el panel del administrador de

actividades y se indican mediante un icono de desconexión.
- Las aplicaciones desconectadas se agrupan en las sesiones respectivas y las sesiones se indican mediante un icono de desconexión.



Los usuarios finales pueden realizar estas acciones en sus escritorios desconectados al hacer clic en el botón de puntos suspensivos:

- **Cerrar sesión**: Use esta opción para cerrar sesión en el escritorio desconectado. Se cierran todas las aplicaciones de la sesión, y se pierden los archivos no guardados.
- **Apagar**: Use esta opción para cerrar los escritorios desconectados.
- **Forzar cierre**: Use esta opción para forzar el cierre de los escritorios desconectados en caso de problemas técnicos.
- **Reiniciar**: Use esta opción para apagar e iniciar de nuevo el escritorio desconectado.

Para obtener más información, consulte Aplicaciones y escritorios desconectados en el administrador de actividades.

Problemas resueltos

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

23.35

Novedades

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

Problemas resueltos

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

23.34

Novedades

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

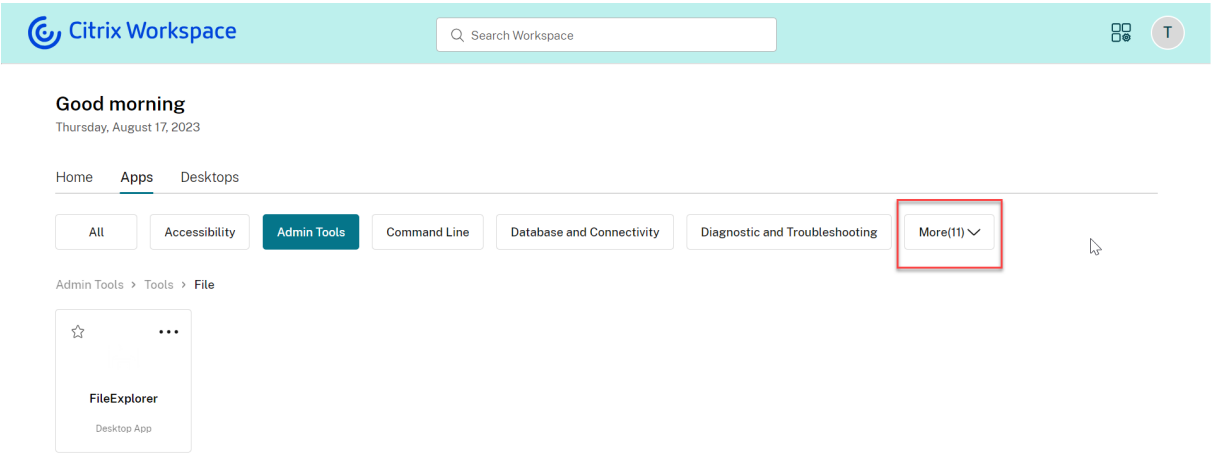
Problemas resueltos

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

23.33

Novedades

Experiencia de usuario mejorada con categorización de aplicaciones Los usuarios finales pueden ver sus aplicaciones organizadas en categorías y subcategorías en la interfaz de usuario de Workspace. Si la categorización incluye más de dos niveles, los usuarios finales verán sus aplicaciones organizadas dentro de una estructura de carpetas. Los usuarios pueden ver las rutas de navegación.
Cuando el número de categorías principales creadas por los administradores supera el espacio disponible en la pantalla del usuario, la interfaz de usuario se ajusta en función del tamaño de la pantalla y desplaza las categorías de forma dinámica bajo el menú desplegable **Más**.



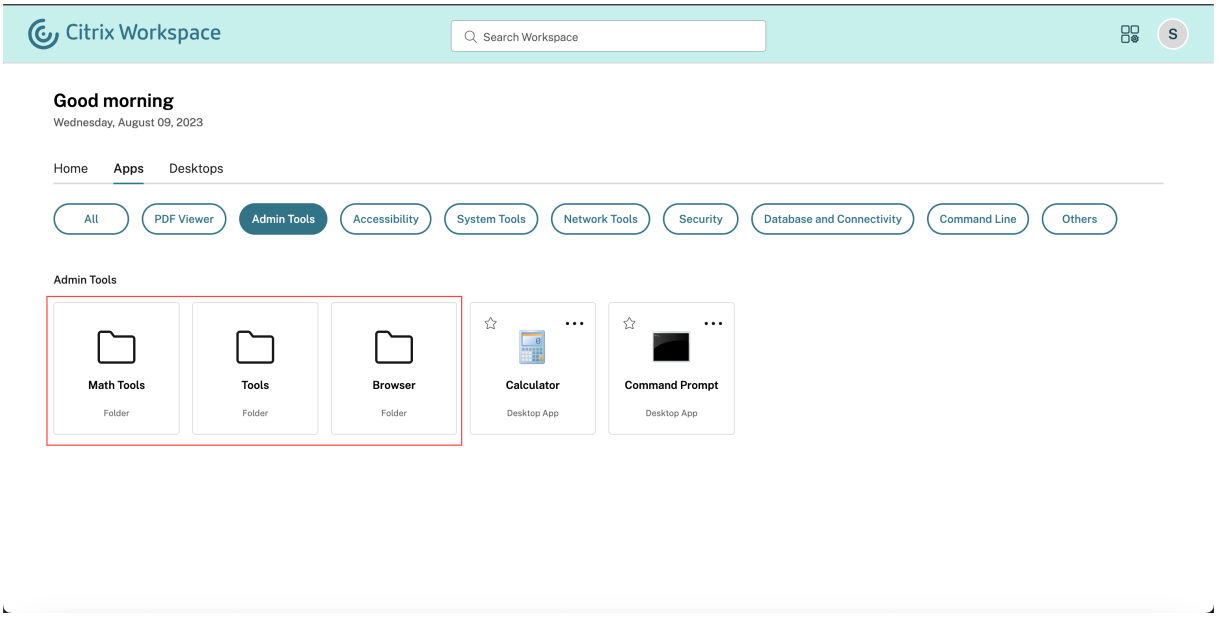
Problemas resueltos

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

23.32

Novedades

Categorización de aplicaciones para facilitar el acceso Los administradores pueden ofrecer aplicaciones organizadas en categorías y subcategorías, lo que mejora la experiencia de navegación de los usuarios finales. A partir del segundo nivel de categorización, los usuarios finales verán una estructura de carpetas. La estructura organizada en varios niveles ofrece una experiencia optimizada y ordenada que ayuda a aumentar la satisfacción general del usuario. Para obtener más información sobre la creación de carpetas y subcarpetas, consulte Crear grupos de entrega.



Problemas resueltos

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

23.31

Novedades

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento generales.

Problemas resueltos

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento generales.

23.30

Novedades

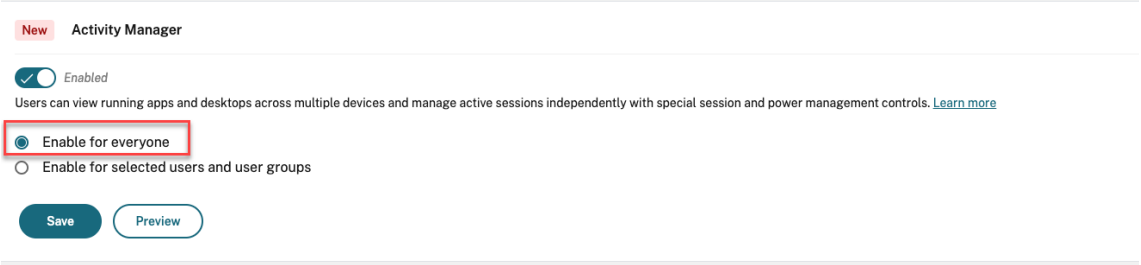
Administrar el administrador de actividades Como administrador, ahora puede habilitar o inhabilitar la función de administrador de actividades para sus usuarios finales. Según las directivas de su organización, puede habilitar la función para todos o para los usuarios y grupos de usuarios que seleccione. Al habilitarse, el panel del administrador de actividades permite a los usuarios finales ver

e interactuar con sus aplicaciones y escritorios activos. Para obtener más información, consulte administrador de actividades.

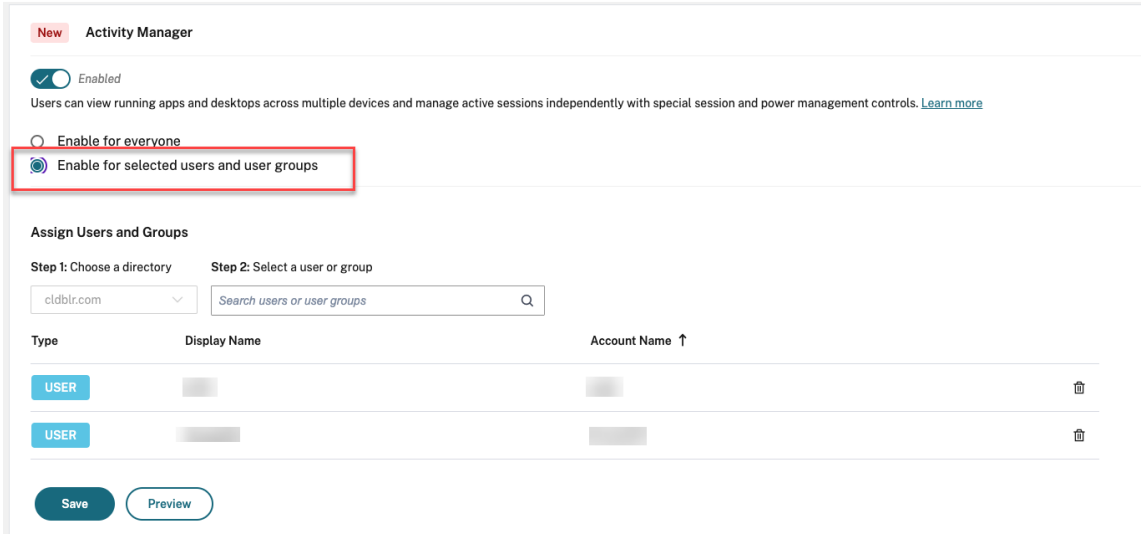
> **Nota:**
>
> Esta función solo es compatible con aplicaciones y escritorios virtuales. No se aplica a aplicaciones web ni SaaS.

Para habilitar el administrador de actividades:

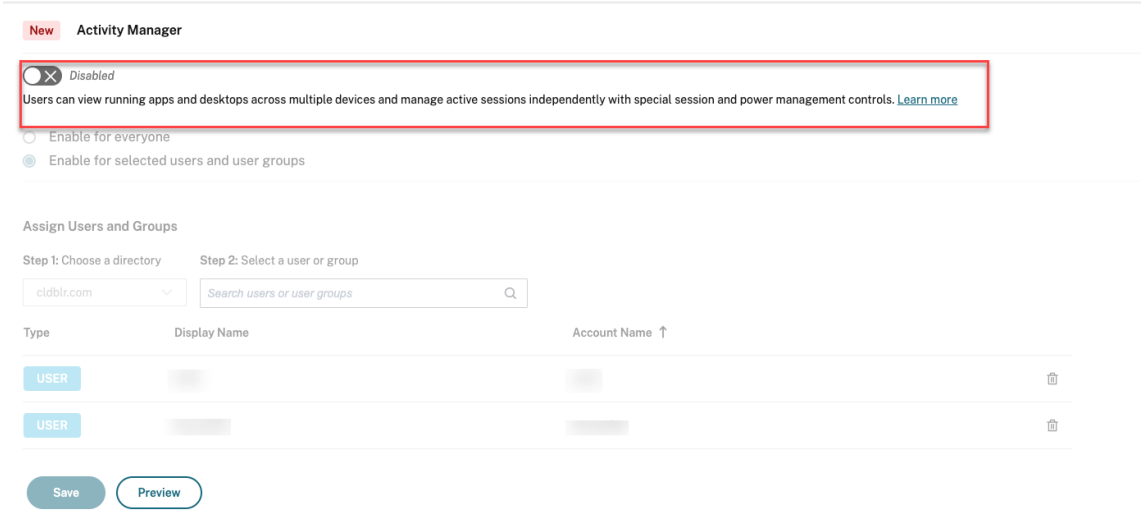
1. En la consola de administración, vaya a **Configuración de Workspace** > **Personalizar** > **Funciones**.
2. En la sección administrador de actividades, active el interruptor para habilitar el administrador de actividades.
3. A continuación, podrá personalizar los permisos de acceso de la siguiente manera.
    - Para habilitar el administrador de actividades para todos los usuarios finales, seleccione **Habilitar para todos**.



    - Para habilitar el administrador de actividades para usuarios y grupos de usuarios determinados, seleccione **Habilitar para los usuarios y grupos de usuarios seleccionados**. A continuación, puede seleccionar el directorio al que pertenecen los usuarios o grupos de usuarios. Una vez seleccionado el directorio apropiado, puede ver los usuarios y grupos de usuarios relevantes.



- Para inhabilitar el administrador de actividades para todos, desactive el interruptor.



4. Haga clic en **Guardar**.

Problemas resueltos

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento generales.

23.29

Novedades

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento generales.

Problemas resueltos

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento generales.

23.28

Novedades

Anuncio de retirada de compatibilidad con Internet Explorer La versión 23.26 de la interfaz de usuario de Citrix Workspace estará disponible en Internet Explorer hasta la última semana de 2023. Citrix no ofrecerá nuevas funciones, correcciones de errores ni parches de seguridad posteriores a la versión 23.26. Además, los administradores recibirán una notificación para actualizarse a los exploradores web compatibles y a la versión LTSR compatible (LTSR 2203 o una posterior).

Problemas resueltos

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento generales.

23.27

Novedades

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento generales.

Problemas resueltos

- En esta corrección, se implementaron el límite de errores y la gestión de errores al nivel del componente. [WSUI-7423]
- La pancarta sin conexión se minimiza al hacer clic en el icono de puntos suspensivos. [WSUI-7797]

23.26

Novedades

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento generales.

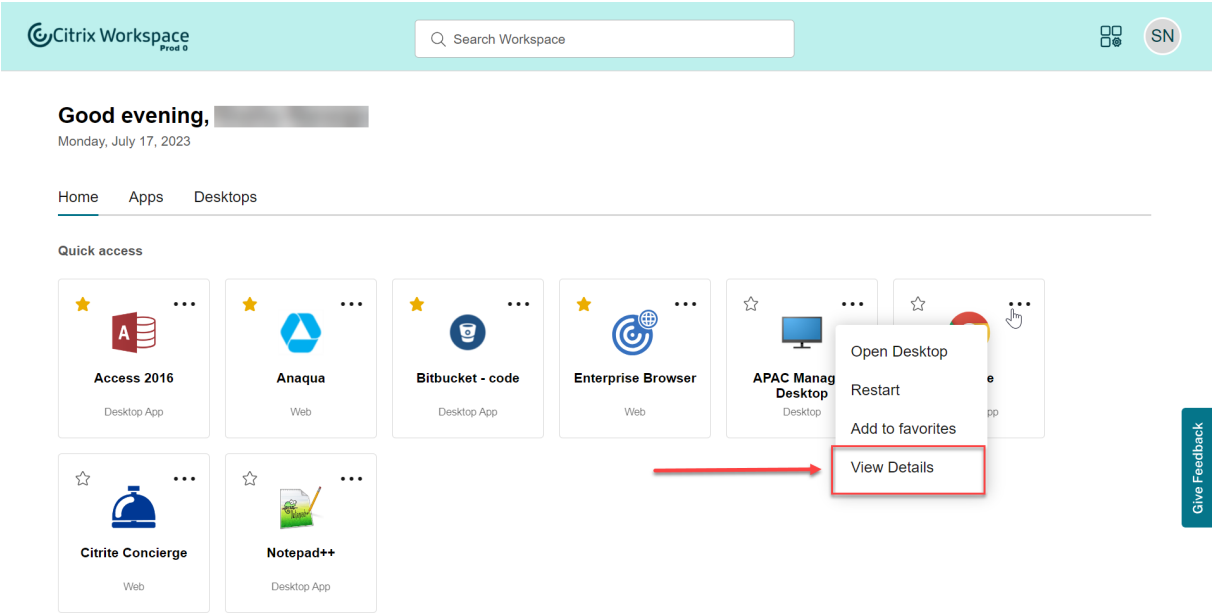
Problemas resueltos

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento generales.

23.25

Novedades

Ver la descripción de aplicaciones y escritorios Ahora, los usuarios finales pueden ver la descripción de aplicaciones y escritorios proporcionada por administradores. Estas descripciones ayudan a comprender la funcionalidad prevista de una aplicación o escritorio. Son especialmente útiles en caso de que existan varias aplicaciones con el mismo nombre, pero que difieran en su configuración, su ubicación, su entorno, etc.
Para ver la descripción de una aplicación o un escritorio, haga clic en los tres puntos del icono correspondiente y, a continuación, en **Ver detalles**.



Problemas resueltos

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento generales.

23.24

Novedades

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento generales.

Problemas resueltos

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento generales.

23.23

Novedades

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento generales.

Problemas resueltos

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento generales.

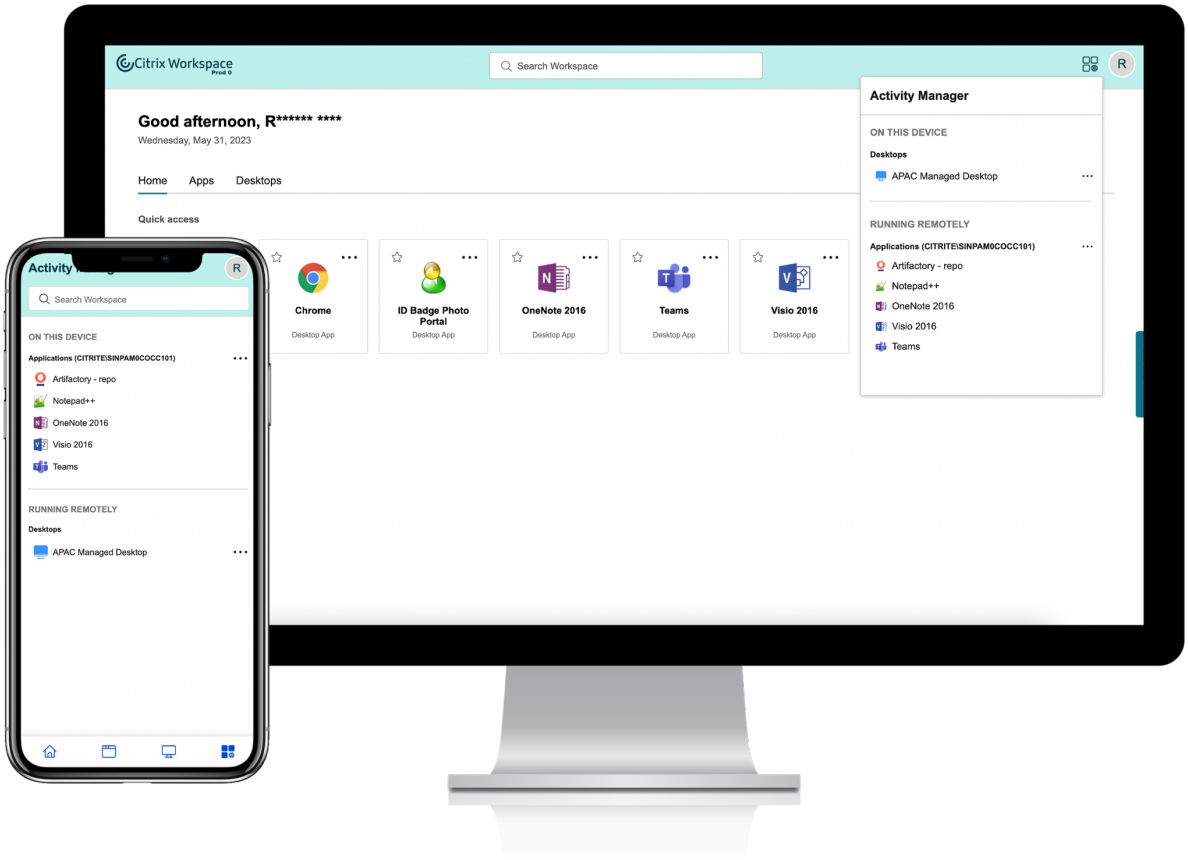
23.22

Novedades

Presentación del administrador de actividades En la interfaz de usuario de Workspace, ahora puede gestionar y realizar acciones rápidas en las aplicaciones y escritorios que estén activos en cualquier dispositivo desde un único panel. Todas las aplicaciones y escritorios activos se agrupan en la sesión que utilice actualmente.

El icono del administrador de actividades aparece en la ventana de la interfaz de usuario de Workspace, a la izquierda del icono del perfil. Al hacer clic en el icono, podrá ver lo siguiente:

- Una lista de las aplicaciones y los escritorios iniciados desde el dispositivo que está utilizando, en **On this device**.
- Una lista de aplicaciones y escritorios activos en otros dispositivos, en **Ejecución remota**.



Para obtener más información, consulte administrador de actividades.

> **Nota:**
>
> Si no puede ver el icono del administrador de actividades con claridad, considere cambiar el color seleccionado en el parámetro **Texto de pancarta y color de icono**. Es posible que el icono no se vea con claridad por el bajo contraste entre la pancarta y el icono del administrador de actividades. Para obtener más información, consulte Configurar temas personalizados.

Problemas conocidos

- Si se desconecta una sesión, los usuarios no podrán cerrar dicha sesión. Las sesiones desconectadas no se muestran en el panel del administrador de actividades.
- En la aplicación Citrix Workspace para Mac, la lista de aplicaciones y escritorios activos que

se muestra en el panel administrador de actividades muestra las sesiones activas de todos los almacenes.

23.15

Novedades

Nueva interfaz de usuario de Workspace La aplicación Citrix Workspace presenta nuevas capacidades en su interfaz de usuario, además de un aspecto moderno y más claro. Las mejoras de la interfaz de usuario se aprecian tanto en la web como en equipos de escritorio y dispositivos móviles.

Experiencia de usuario inicial mejorada Cuando inicie la aplicación Citrix Workspace descargada o Citrix desde un explorador web por primera vez, aparecerá una pantalla con una lista de las aplicaciones pertinentes. Estas aplicaciones las decide el administrador y usted puede agregarlas a sus favoritos con un solo clic.

Experiencia de búsqueda mejorada La función de **búsqueda** mejorada ofrece resultados más rápidos en los motores de búsqueda. La opción **Buscar** le permite hacer una búsqueda rápida e intuitiva desde la aplicación Workspace.

Tareas de administrador

Como administrador, puede personalizar la experiencia de usuario de sus suscriptores en la aplicación Workspace. Para obtener más información, consulte las secciones siguientes.

- Habilitar la nueva experiencia con Workspace para los usuarios
- Habilitar o inhabilitar la pantalla de inicio para los usuarios

Novedades en Global App Configuration Service

November 21, 2023

En las siguientes secciones se enumeran las nuevas funciones de las versiones actual y anteriores de Global App Configuration Service

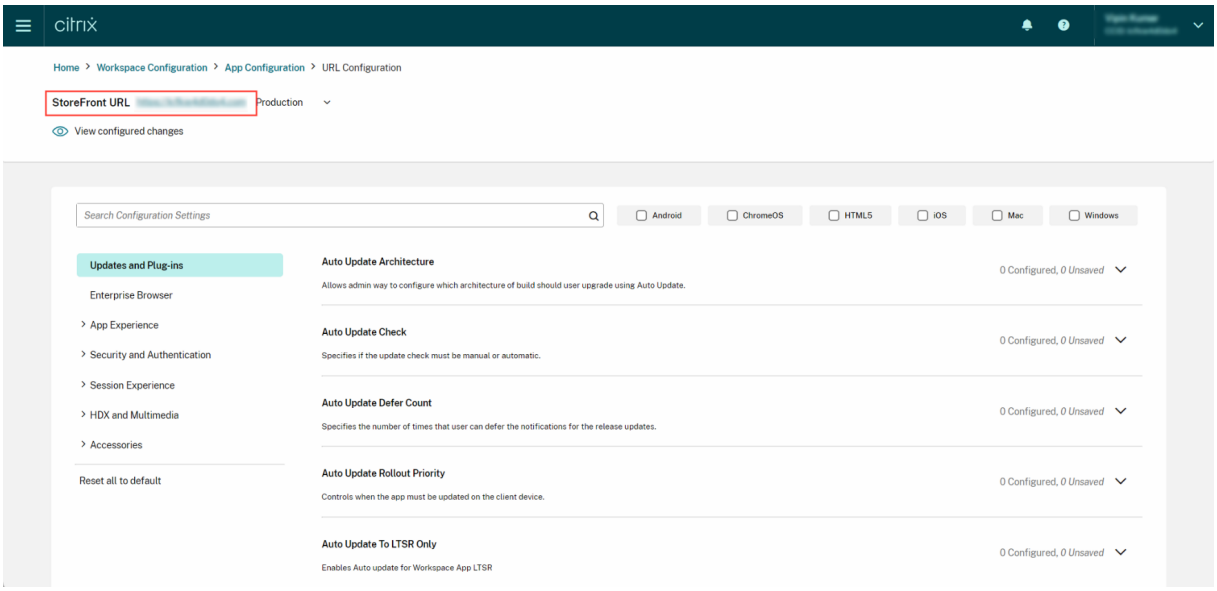
30 Oct 2023

Configurar los parámetros de los almacenes locales

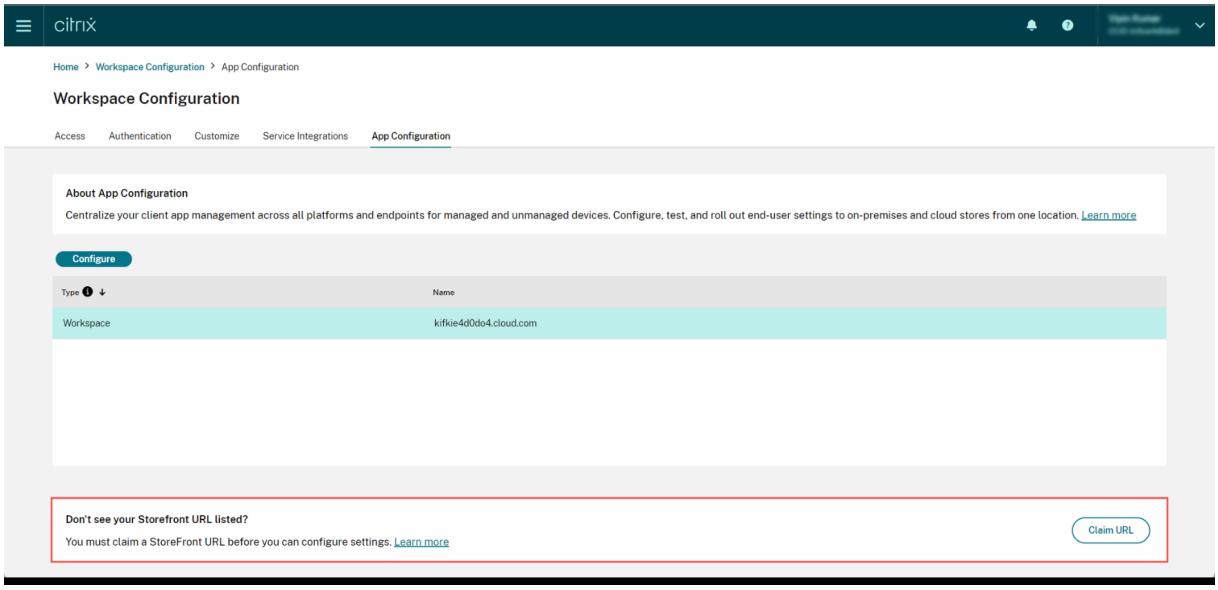
Ahora puede usar la interfaz de usuario de Global App Configuration Service para configurar los parámetros de los almacenes locales. Inicie sesión en su cuenta de Citrix Cloud y vaya a **Configuración de Workspace > Configuración de aplicaciones** para empezar.

> **Nota:**
>
> Si aún no tiene una cuenta de Citrix Cloud, vaya a la página Citrix Onboarding para crear una.

Antes de continuar, compruebe que ha establecido una reclamación sobre su URL de StoreFront. Si se ha reclamado la URL, aparecerá la siguiente pantalla y podrá empezar a configurar los parámetros de su almacén local.



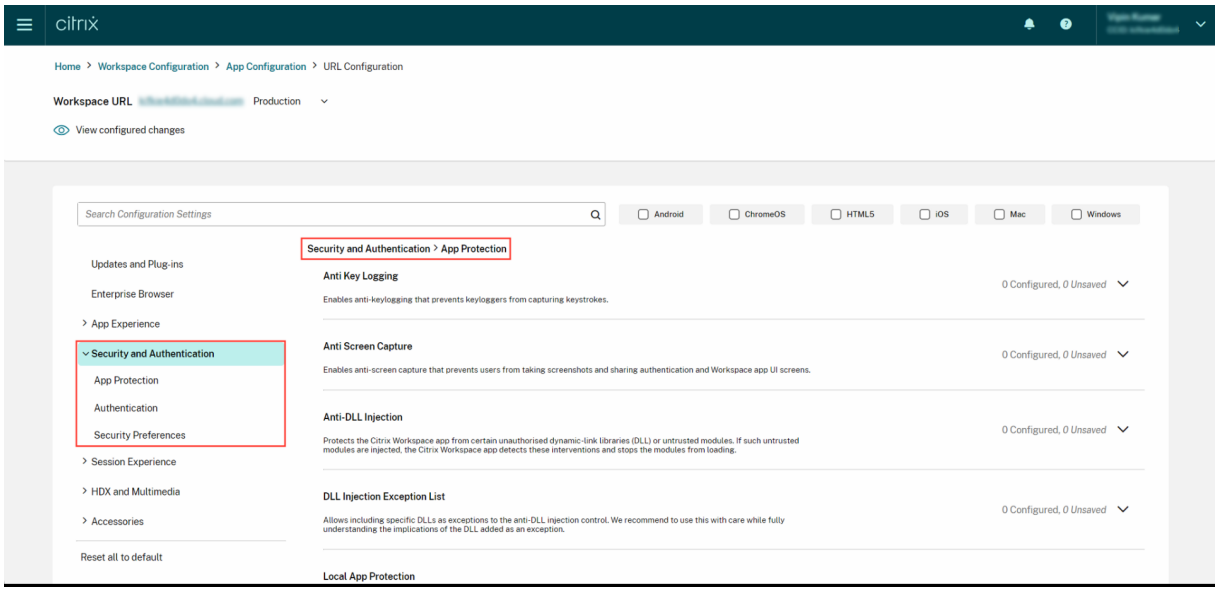
Si aún no ha reclamado su URL, aparecerá la siguiente pantalla. Haga clic en **Iniciar** en la sección **Configurar los parámetros de los almacenes locales** para reclamar su URL. Para obtener más información, consulte Introducción.



28 Sep 2023

Categorización simplificada de los parámetros para facilitar la navegación

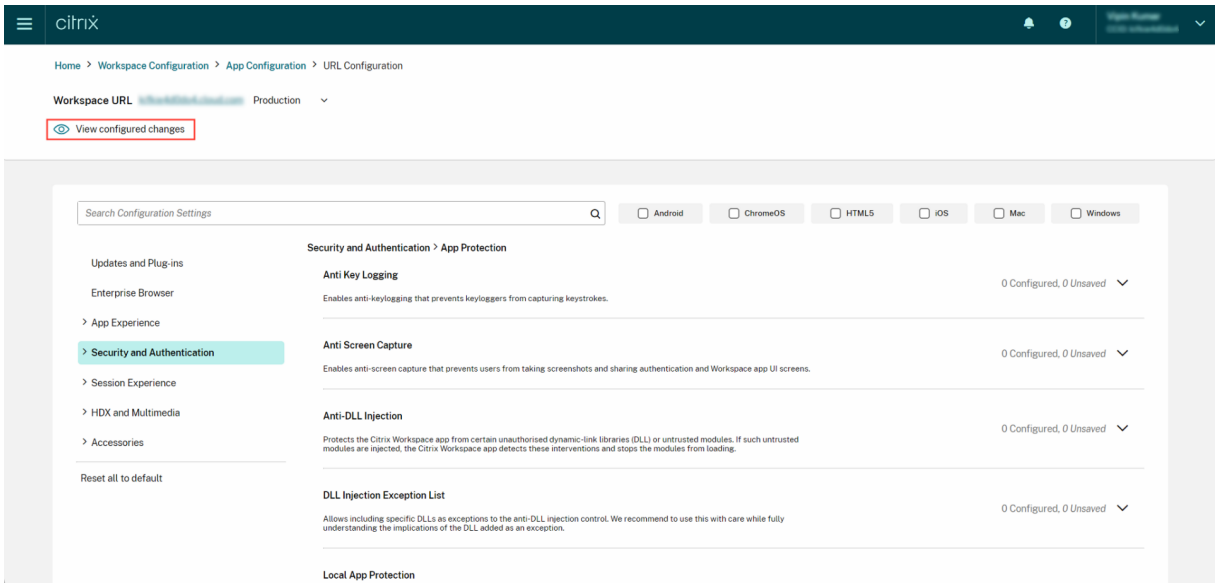
La interfaz de usuario de Global App Configuration Service se ha mejorado para ofrecer una categorización sencilla de los parámetros. Los parámetros se han clasificado en función de los temas y los flujos de trabajo del usuario final, y comprenden siete carpetas principales y varias subcarpetas. Esta manera ordenada de organizar las cosas hace que sea más fácil para los administradores navegar entre más de 300 parámetros.



28 Jul 2023

Ver un resumen de los parámetros configurados

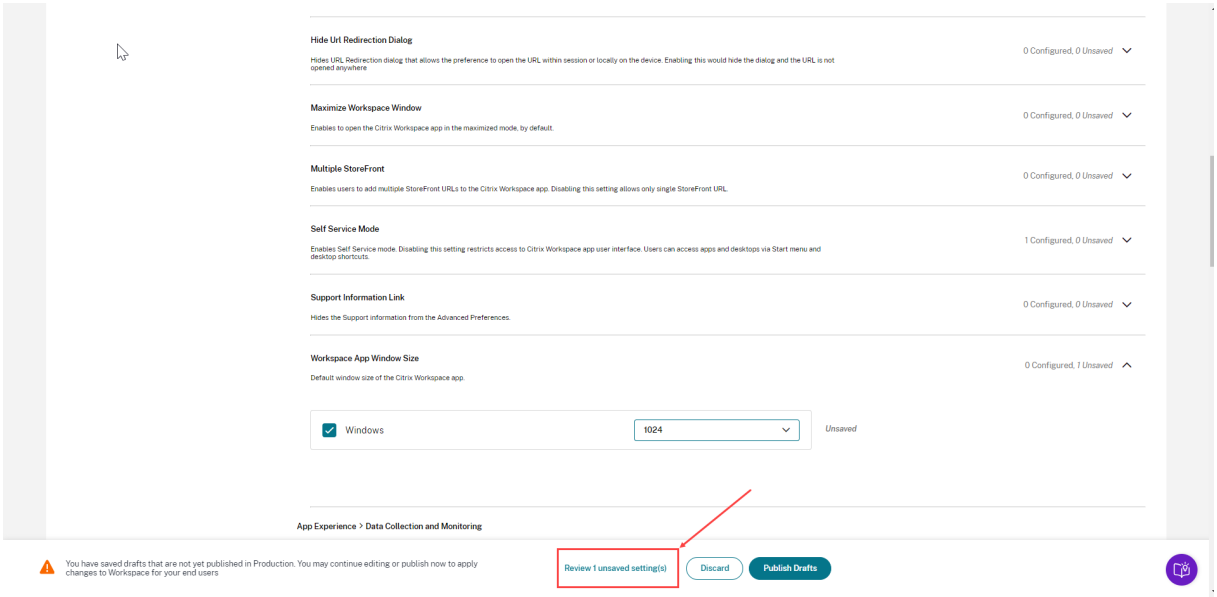
Los administradores ahora pueden ver un resumen de la configuración actual si hacen clic en el botón **Ver parámetros configurados**. De esta forma, se elimina la necesidad de expandir y revisar cada parámetro por separado. Una lista consolidada de todos los parámetros configurados permite a los administradores revisar exhaustivamente la configuración actual y evaluar el impacto en los usuarios.



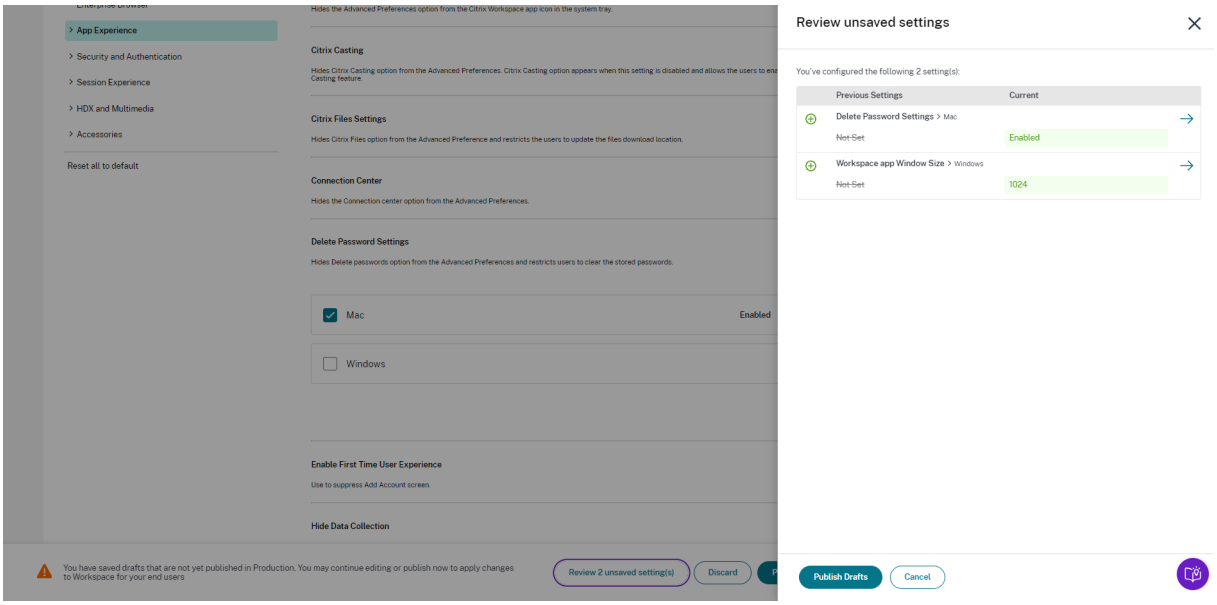
07 Jun 2023

Revisar cambios no guardados

Con esta mejora, los administradores pueden realizar una revisión final de los cambios no guardados antes de publicar la configuración. La cantidad de parámetros no guardados se muestra en la interfaz de usuario y los administradores pueden acceder a esta lista haciendo clic en la opción **Revisar parámetros sin guardar**. Esto permite a los administradores realizar cambios informados y mantener la precisión de los datos.



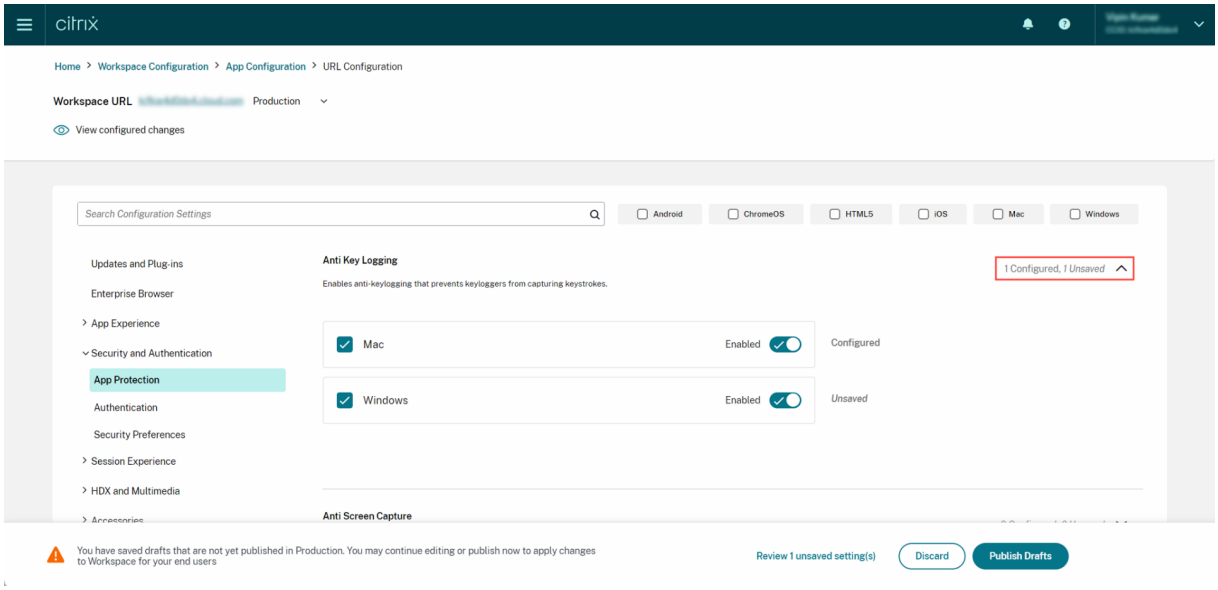
Los administradores también pueden ir a un parámetro no guardado haciendo clic en la flecha.



Interfaz de usuario mejorada

Los administradores ahora pueden ver el estado de cada parámetro sin expandirlo. Ahora se muestran las siguientes etiquetas para facilitar una toma de decisiones informada en cada paso.

- **Configurado**: Muestra la cantidad de plataformas (SO cliente) para las que ya se ha configurado el parámetro.
- **No guardado**: Muestra la cantidad de parámetros que están configurados pero que aún no se han guardado



23 de mayo de 2023

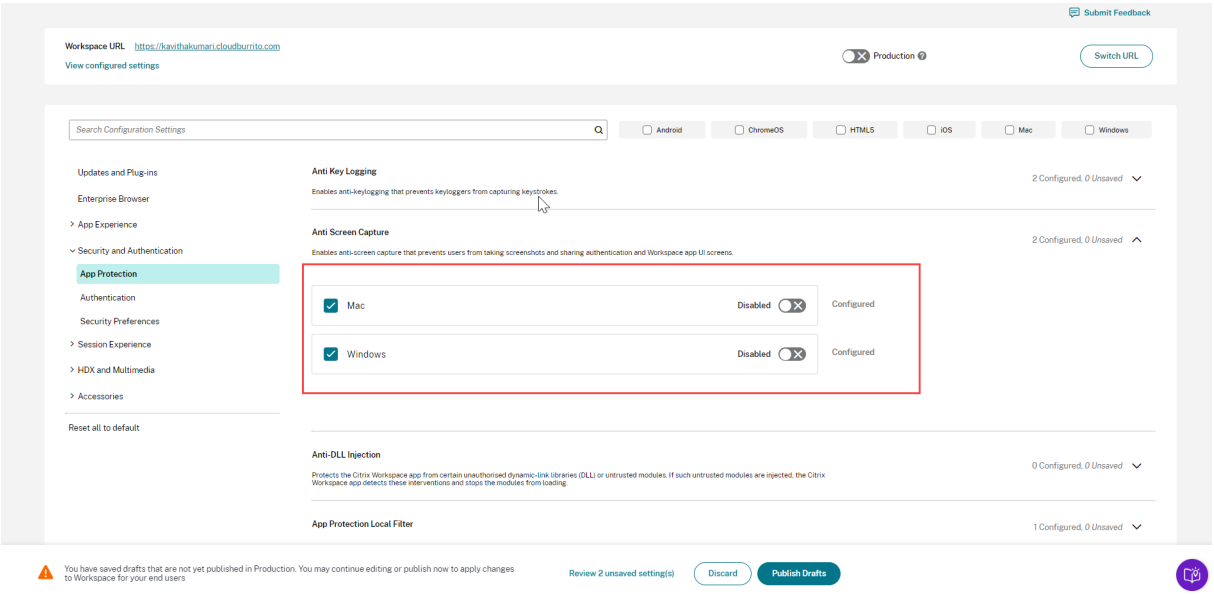
Funciones de búsqueda mejoradas

Con esta mejora, la experiencia de búsqueda se ha perfeccionado para ofrecer una experiencia sólida y fluida. Los administradores ahora pueden iniciar sesión en el portal en la nube y buscar los parámetros necesarios en la página Configuración de aplicaciones con facilidad. Pueden usar los siguientes métodos de búsqueda.

- **Búsqueda mediante la descripción del parámetro**
  Los administradores también pueden localizar un parámetro introduciendo las palabras clave que se encuentran en su descripción. Esto ofrece un enfoque de búsqueda más flexible, en el que se utilizan términos relevantes asociados al parámetro en cuestión.
- **Búsqueda mediante el nombre del parámetro de API**
  Los administradores tienen la opción de buscar un parámetro introduciendo el nombre del parámetro de API correspondiente. Este método ofrece una búsqueda más precisa y específica, lo que permite a los usuarios encontrar rápidamente el parámetro específico que necesitan.

Ver las plataformas aplicables a cada parámetro

Cada parámetro ahora muestra de forma dinámica solo las plataformas en las que es relevante y aplicable. Este filtrado inteligente garantiza que a los usuarios se les presente una lista de opciones concisa y personalizada, lo que elimina desorganización y confusión innecesarias.



Primeros pasos en Citrix Workspace

October 12, 2023

En este artículo, se describen los principales pasos necesarios para configurar Citrix Workspace y los componentes relacionados, de principio a fin. Para obtener un resumen de las fases implicadas, consulte Descripción general del flujo de trabajo.

Hay otras formas de hacer la transición a la experiencia integral con Citrix Workspace. Las más comunes son las siguientes:

- Entregar Citrix Virtual Apps and Desktops a través de espacios de trabajo.
  - Si quiere acceder a los recursos de su implementación local de Virtual Apps and Desktops a través de Workspace, consulte Agregación de sitios para soluciones híbridas.
  - Si quiere migrar a la nube, consulte Migración completa a la nube.

Descripción general del flujo de trabajo

Si configura Citrix Workspace como un cliente nuevo, hay 5 fases de trabajo generales:

1. Prepararse para Citrix Workspace en Citrix Cloud.
2. Configurar el acceso y la autenticación de los suscriptores.
3. Integrar servicios en espacios de trabajo.

4. Personalizar los espacios de trabajo con las preferencias específicas de la empresa, como logotipos y directivas de seguridad.
5. Implementar Citrix Workspace para los suscriptores.

En Success Center, se ofrece información y soluciones adicionales.

Fase 1: Prepararse para Citrix Workspace en Citrix Cloud

Antes de configurar Citrix Workspace, deberá registrarse en Citrix Cloud y cumplir con los requisitos técnicos para empezar a utilizar Citrix Workspace.

Si ya es cliente de Citrix Cloud, con administradores agregados a través de **Administración de acceso e identidad**, puede pasar a la Fase 2: Configurar el acceso y la autenticación de los suscriptores.

Los pasos involucrados en la fase 1 incluyen:

1. Registrarse en Citrix Cloud.
2. Agregar administradores con una identidad de Citrix.
3. Configurar la infraestructura mediante:
    - Creación de ubicaciones de recursos
    - Implementación de Cloud Connectors

La configuración de Citrix Identity implica una contraseña temporal de un solo uso (TOTP). Además de Citrix Identity, puede configurar la autenticación de Azure AD. Para obtener más información sobre cómo agregar administradores y configurar la autenticación para los administradores, consulte Administradores en la documentación de producto de Citrix Cloud.

Fase 2: Configurar el acceso y la autenticación de los suscriptores

La fase 2 implica configurar los controles de acceso, como la URL del espacio de trabajo y la conectividad externa, en **Configuración de Workspace**.

También puede configurar uno o más proveedores de identidades en **Administración de acceso e identidad** y, a continuación, habilitar uno de ellos como la forma principal en la que los suscriptores se autentican en los espacios de trabajo en **Configuración de Workspace**.

> **Nota:**
>
> Hay dos maneras de acceder a Citrix Workspace. Una es a través de la aplicación Citrix Workspace instalada de forma nativa, que sustituye a Citrix Receiver para ofrecer un acceso sencillo y seguro a los servicios y espacios de trabajo de Citrix Cloud. La otra forma de acceder a Citrix Workspace es a través de un explorador con la URL de Workspace. La URL de Workspace está habilitada de forma predeterminada, normalmente en el formato: `https://yourcompanyname.cloud`

> .com.
>
> Para obtener más información, visita Acceder al espacio de trabajo.

Configurar el acceso al espacio de trabajo

Puede configurar los controles de acceso en **Configuración de Workspace > Acceso**. Por lo general, esto implica las siguientes tareas:

- Configurar y habilitar la URL de Workspace.
- Configurar la conectividad externa con Citrix Gateway.

Después de estas dos tareas, Citrix recomienda instalar y promover entre los suscriptores el uso de la aplicación Citrix Workspace para disfrutar de una experiencia homogénea con los espacios de trabajo.

Configurar la autenticación de suscriptores en los espacios de trabajo

Definir la forma en que los suscriptores se autentican para iniciar sesión en sus espacios de trabajo es un proceso de dos pasos:

1. En **Administración de acceso e identidad**, configurar los proveedores de identidades.
2. En **Configuración de Workspace > Autenticación**, elegir uno de los métodos de autenticación ofrecidos por los proveedores de identidades configurados en el primer paso.

Si utiliza un proveedor de identidades federadas, también puede habilitar Single Sign-On (SSO) en DaaS con el Servicio de autenticación federada de Citrix (FAS).

Para obtener más información sobre cómo configurar la autenticación de suscriptores en los espacios de trabajo, consulte Espacios de trabajo seguros.

Fase 3: integrar servicios en espacios de trabajo

La integración de servicios en los espacios de trabajo es otro proceso de dos partes:

1. Configurar los servicios adquiridos en Citrix Cloud. Para obtener una lista de los servicios, consulte Citrix Cloud Services.
2. Habilitar el acceso a los servicios configurados en **Configuración de Workspace > Integraciones de servicios**. Para obtener más información sobre la integración de servicios, consulte Habilitar e inhabilitar servicios.

Fase 4: Personalizar los espacios de trabajo

En **Configuración de Workspace**, puede personalizar la experiencia del suscriptor de los espacios de trabajo para diferentes usuarios y para cumplir con los requisitos organizativos específicos haciendo lo siguiente:

- Personalizar la apariencia de los espacios de trabajo, incluidos los logotipos y los temas personalizados. Para obtener instrucciones sobre cómo personalizar la apariencia de Workspace, consulte Personalizar la apariencia de los espacios de trabajo.
- Elegir opciones de interacción, como permitir que los suscriptores creen **Favoritos** e inicien escritorios automáticamente. Para obtener instrucciones sobre cómo personalizar la forma en que los suscriptores interactúan con sus espacios de trabajo, consulte Personalizar las interacciones en espacios de trabajo.
- Personalizar la privacidad y la seguridad, lo que incluye establecer un período de tiempo de espera, crear una directiva de inicio de sesión y permitir que los suscriptores cambien sus contraseñas desde sus espacios de trabajo. Para obtener instrucciones sobre cómo personalizar las directivas de privacidad y seguridad de Workspace, consulte Personalizar las directivas de seguridad y privacidad.

Fase 5: Implementar Citrix Workspace para los suscriptores

Citrix recomienda que verifique la integridad de los espacios de trabajo con pruebas de aceptación operativa y se ponga en contacto con Success Center para planificar la forma de incorporar a los suscriptores. Las actividades generales de esta fase incluyen:

1. Probar espacios de trabajo.
    - Compruebe que puede iniciar sesión a través del explorador y con la aplicación Citrix Workspace.
    - Inicie y use todas las aplicaciones y escritorios disponibles.
    - Compruebe que puede acceder a las carpetas y archivos disponibles.
    - Compruebe que las notificaciones muestran las acciones y actividades previstas.
    - Si está habilitado, compruebe que puede acceder a los recursos para dispositivos de punto final en los dispositivos móviles.
2. Incorporar suscriptores.
    - Comunique las capacidades de Citrix Workspace a los suscriptores
    - Comparta la URL de Workspace del explorador.
    - Guíe a los usuarios en la instalación de la aplicación Citrix Workspace.

Para obtener más información sobre cómo probar espacios de trabajo e incorporar suscriptores a los mismos, consulte Recursos para la adopción de Citrix Workspace para usuarios finales.

Prepararse para Citrix Workspace

October 12, 2023

En este artículo se describen los requisitos y las actividades administrativas que le ayudarán en la preparación para implementar Citrix Workspace. Entre los pasos necesarios de la preparación para Citrix Workspace se incluyen los siguientes:

1. Asegúrese de que cumple con los requisitos del sistema y de conectividad de Citrix Cloud.
2. Planifique el entorno y la implantación de Citrix Workspace.
3. Inicie sesión o regístrese en Citrix Cloud.
4. Agregue administradores a Citrix Cloud y Citrix Workspace.
5. Compruebe sus derechos con relación a los servicios alojados en la nube.
6. Configure la infraestructura necesaria para Citrix Workspace.

Success Center complementa a la perfección esta documentación de producto. Los artículos de Success Center ofrecen un panorama general de las soluciones disponibles y detalles específicos del servicio.

La documentación del producto Citrix Cloud ofrece una guía más detallada para los administradores de TI y los desarrolladores sobre los requisitos previos y las actividades que implica la preparación para Citrix Workspace en Citrix Cloud.

Requisitos del sistema y de conectividad

Citrix Cloud es la consola a través de la cual puede ver y administrar sus derechos con respecto al servicio y acceder a **Configuración de Workspace**.

Si ya está preparado para Citrix Cloud, puede omitir los pasos descritos en Planificar el entorno e implantación.

En resumen, Citrix Cloud requiere la siguiente configuración:

- Un dominio de Active Directory para administrar la autenticación de suscriptores en los espacios de trabajo.
- Al menos dos Citrix Cloud Connectors por ubicación de recursos.
- Una máquina dedicada para cada Cloud Connector.
- Máquinas físicas o virtuales, unidas a su dominio, para alojar cargas de trabajo y otros componentes.

Necesita al menos dos máquinas físicas o virtuales, ya que no puede instalar otros componentes en una máquina que aloje un Citrix Cloud Connector.

Para obtener información sobre los requisitos de Cloud Connector, consulte Citrix Cloud Connector - Detalles técnicos. Para obtener información sobre la instalación de Cloud Connectors, consulte Instalar Cloud Connector.

Además, se debe poder contactar con las siguientes direcciones para hacer funcionar Citrix Workspace:

- `https://*.cloud.com`
- `https://*.citrixdata.com`

Para obtener una lista completa de las direcciones de contacto necesarias para los servicios de Citrix Cloud, consulte Requisitos de conectividad con los servicios.

Planificar el entorno e implantación

Citrix recomienda preparar un plan de soporte y administración de Citrix Workspace. Use el Plan de Success Center para establecer objetivos, definir casos de uso, identificar riesgos y crear una estrategia de implementación que incluya lo siguiente:

- Establecer resultados empresariales, servicios que quiere agregar y requisitos de los grupos de usuarios.
- Identificar los requisitos técnicos para configurar la infraestructura de Citrix Workspace.
- Crear el equipo de Workspace. Asigne tareas a los equipos de entrega y Agregue administradores a su cuenta de Citrix Cloud con acceso a la **Configuración de Workspace**.
- Planificar la interacción con los propietarios y suscriptores del proceso.
  - Preparar una estrategia de cambio y un plan de comunicación.
  - Desarrollar enfoques de capacitación y refuerzo.
  - Realizar análisis de impacto y de partes interesadas.

Para obtener más información sobre la planificación del entorno e implantación de Workspace, consulte el documento Success Readiness Checklist de Success Center.

Iniciar sesión o registrarse en Citrix Cloud

Para registrarse como cliente nuevo, siga las instrucciones que se indican en Registrarse en Citrix Cloud.

Si ya se creó una cuenta de administrador para su organización, el administrador principal debe agregarlo a la cuenta de la empresa. Consulte Agregar administradores para obtener más información.

Si ya tiene una cuenta, inicie sesión en Citrix Cloud con sus credenciales de citrix.com, My Citrix o Citrix Cloud.

Para obtener más información sobre cómo iniciar sesión o registrarse en Citrix Cloud, consulte el documento Citrix Cloud Services Kickoff Guide.

Agregar administradores

La primera cuenta de administrador se crea a través del proceso de incorporación inicial de Citrix Cloud. A partir de ahí, el administrador inicial puede invitar a otros administradores a unirse a Citrix Cloud. Esos administradores nuevos pueden utilizar sus credenciales de cuenta de Citrix o configurar una cuenta nueva.

Invitar a administradores

Los administradores se agregan a su cuenta de Citrix Cloud a través de **Administración de acceso e identidad** en el menú del lado izquierdo de la consola de Citrix Cloud. Introduzca la dirección de correo electrónico del administrador que quiere agregar para enviarle una invitación con instrucciones para el inicio de sesión.

Al agregar administradores a su cuenta de Citrix Cloud, se definen los permisos de administrador adecuados para su rol en la organización. Los administradores con **acceso completo** tienen acceso a **Configuración de Workspace** de forma predeterminada. Los administradores con **acceso personalizado** solo tienen acceso a las funciones y servicios que seleccione. Se pueden ajustar con mayor precisión los permisos de acceso de los administradores a los que se invita.

Para obtener más información sobre cómo agregar (y eliminar) administradores, consulte Administradores.

Configurar la autenticación de administrador

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. Los suscriptores deben autenticarse con uno de los proveedores de identidades que se indican en Espacios de trabajo seguros.

Cada administrador de su cuenta de Citrix Cloud debe configurar también la autenticación de varios factores (MFA).

El registro implica descargar e instalar una aplicación de autenticación que sigue el estándar de contraseña temporal de un solo uso (TOTP), como Citrix SSO. Para un registro sin problemas, Citrix recomienda descargar e instalar Citrix SSO *antes* de completar los pasos siguientes.

1. Inicie sesión en su cuenta de Citrix Cloud.
2. Seleccione su nombre y elija **Mi perfil** en el menú desplegable.

3. Seleccione **Configurar aplicación de autenticación** en **Seguridad en el inicio de sesión** para recibir un correo electrónico con el código de verificación necesario para el paso 4.
4. Cuando se le solicite, introduzca el código de verificación que se le envió en un correo electrónico desde Citrix y la contraseña de su cuenta y, a continuación, seleccione **Verificar**.
5. Escanee el código QR o introduzca la clave en una aplicación de autenticación que siga el estándar de contraseña temporal de un solo uso (TOTP), como Citrix SSO.
6. Para confirmar que la MFA se ha configurado correctamente, introduzca el código de 6 dígitos de la aplicación de autenticación y, a continuación, seleccione **Verificar**.
7. Seleccione **Agregar un teléfono de recuperación** e introduzca un número de teléfono con el que Citrix Support pueda comunicarse con usted para verificar su identidad para consultas relacionadas con MFA.
8. Seleccione **Generar código de reserva** para crear una lista de códigos de uso único que se pueden usar si pierde el acceso a su aplicación de autenticación.
9. Seleccione **Descargar códigos** y guarde el archivo de texto con sus códigos de reserva en una ubicación segura y accesible.
10. Seleccione la casilla de verificación y, luego, **Finalizar**.

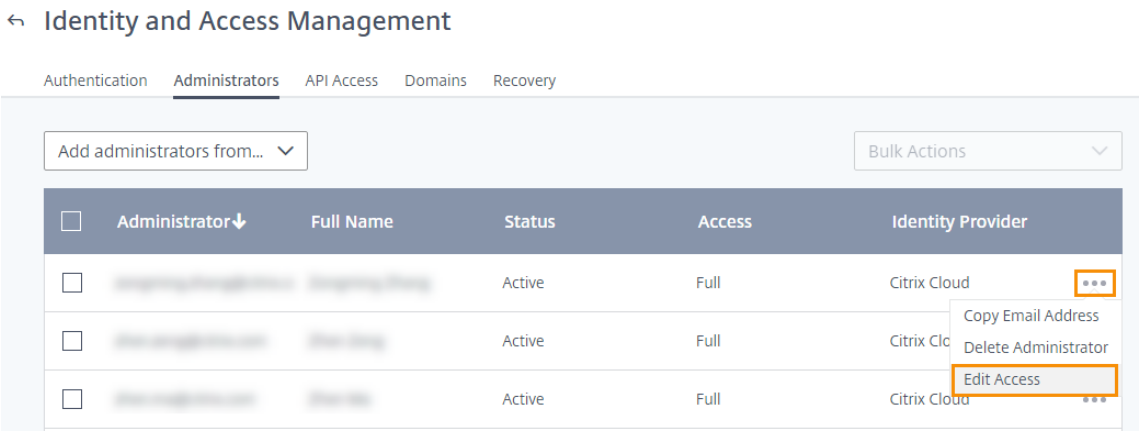
Las instrucciones para configurar la MFA también se pueden encontrar en Knowledge Center y en Configurar la autenticación de varios factores en la documentación de producto de Citrix Cloud.

Opcionalmente, también puede configurar Azure Active Directory (AD) para los administradores. Para obtener más información sobre los proveedores de identidades disponibles para los administradores de Citrix Cloud y los suscriptores de Workspace, consulte Proveedores de identidades.

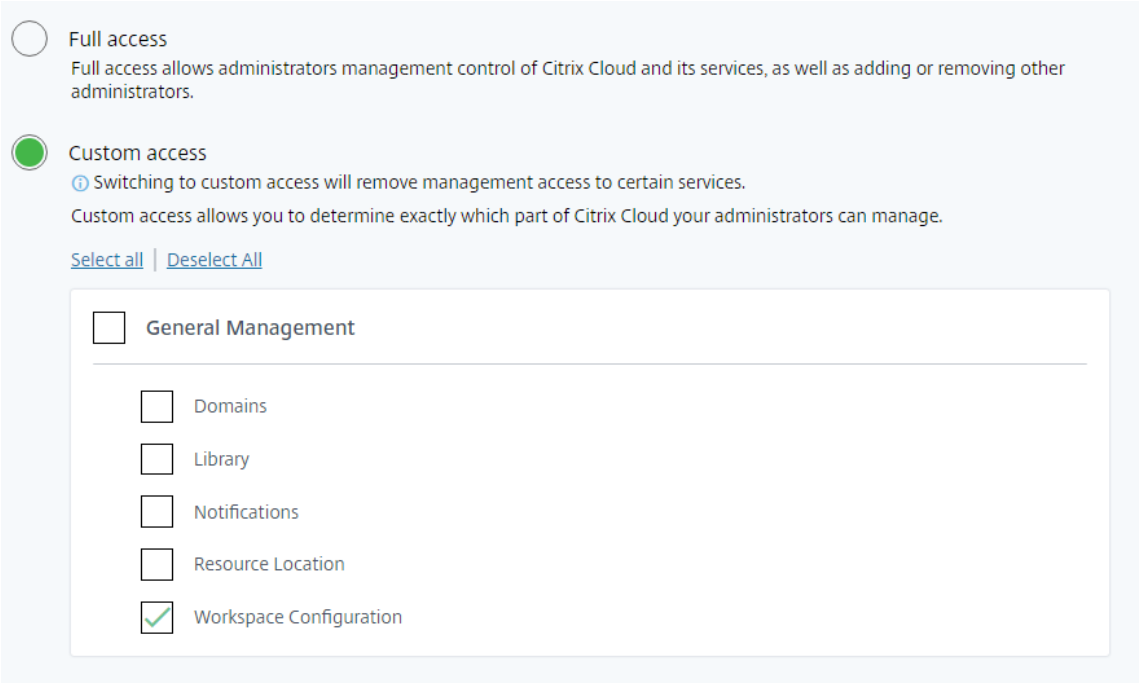
Modificar los permisos de administrador

Para configurar el acceso personalizado a **Configuración de Workspace**:

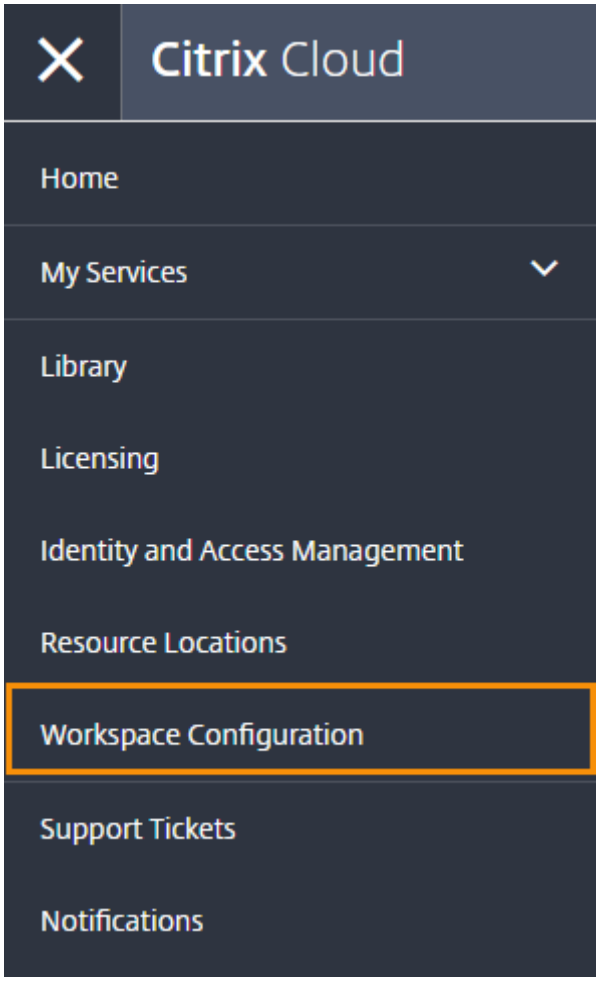
1. Desde el menú de **Citrix Cloud**, seleccione **Administración de acceso e identidad** y, luego, **Administradores**.
2. Busque al administrador que quiere gestionar, seleccione el botón de tres puntos y, a continuación, seleccione **Modificar acceso**.



3. Compruebe que el **acceso personalizado** esté habilitado.
4. Para habilitar solo el acceso a **Configuración de Workspace**, en **Administración general**, seleccione **Configuración de Workspace**.



Después de habilitar el acceso, los administradores pueden iniciar sesión en Citrix Cloud y seleccionar **Configuración de Workspace** en el menú de **Citrix Cloud**.



> **Nota:**
>
> En Citrix Virtual Apps Essentials, **Configuración de Workspace** está disponible en el menú de Citrix Cloud después de crear el primer catálogo.

Comprobar los derechos

Una vez que ha iniciado sesión en Citrix Cloud, puede administrar sus derechos (los productos y servicios de Citrix que ha adquirido). Los productos y servicios de Citrix se muestran en un diseño de tarjeta en el panel de mandos de Citrix Cloud. Productos y servicios adquiridos y suscritos para incluir un botón **Administrar**.

Si quiere probar un nuevo servicio, puede seleccionar **Solicitar prueba** o **Solicitar demostración** en el cuadro correspondiente en el panel de mandos de Citrix Cloud. Para obtener más información sobre las pruebas de servicios, consulte Pruebas de Citrix Cloud Service.

Si quiere comprar un nuevo servicio, puede convertir una prueba en un servicio de producción sin tener que volver a configurarlo ni crear una nueva cuenta. Para comprar un servicio, anote

el ID de su organización en la esquina superior derecha de la consola de Citrix Cloud y visite https://www.citrix.com/product/citrix-cloud.

Configurar la infraestructura

Configurar la infraestructura necesaria para Citrix Workspace implica conectar sus recursos a Citrix Cloud de la siguiente manera:

- Implementar conectores en su entorno.
- Crear 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 diferentes recursos en función de los servicios que utilice.

Para crear una ubicación de recursos, necesitará instalar al menos dos Cloud Connectors en su dominio.

Citrix Cloud Connector es un componente que proporciona un canal de comunicación entre Citrix Cloud y las ubicaciones de recursos. El canal establece conexiones a la nube a través del puerto HTTPS estándar (443) y el protocolo TCP. No se aceptan conexiones entrantes.

Para obtener más información, consulte Citrix Cloud Connector.

> **Nota:**
>
> Workspace no admite conexiones de clientes heredados que utilizan una URL de PNAgent para conectarse a recursos. Si su entorno incluye estos clientes heredados, debe implementar StoreFront localmente y habilitar la compatibilidad con clientes heredados. Para proteger estas conexiones de cliente, use un dispositivo local Citrix Gateway en lugar de Citrix Gateway Service.

Siguiente: Crear el espacio de trabajo

Ahora que está preparado para Citrix Workspace, estos son los siguientes pasos:

- Configurar el acceso a los espacios de trabajo, incluida la URL del espacio de trabajo y la conectividad externa.
- Configurar la autenticación del espacio de trabajo, con instrucciones en Espacios de trabajo seguros.
- Integrar servicios en espacios de trabajo.
- Personalice la experiencia en los espacios de trabajo:
  - Personalizar la apariencia de los espacios de trabajo.

- Personalizar las interacciones en espacios de trabajo.
- Personalizar las directivas de seguridad y privacidad.

Nueva interfaz de usuario de Workspace

November 21, 2023

La nueva interfaz de usuario (IU) de Workspace reduce la complejidad visual, facilita el acceso a las funciones esenciales y perfecciona el uso y la funcionalidad de la aplicación Workspace según sea necesario, lo que se traduce en una mejor experiencia de usuario.

Este artículo destaca algunas de las principales funciones que ven los suscriptores cuando inician sesión y resume cómo acceder a los espacios de trabajo e interactuar con ellos.

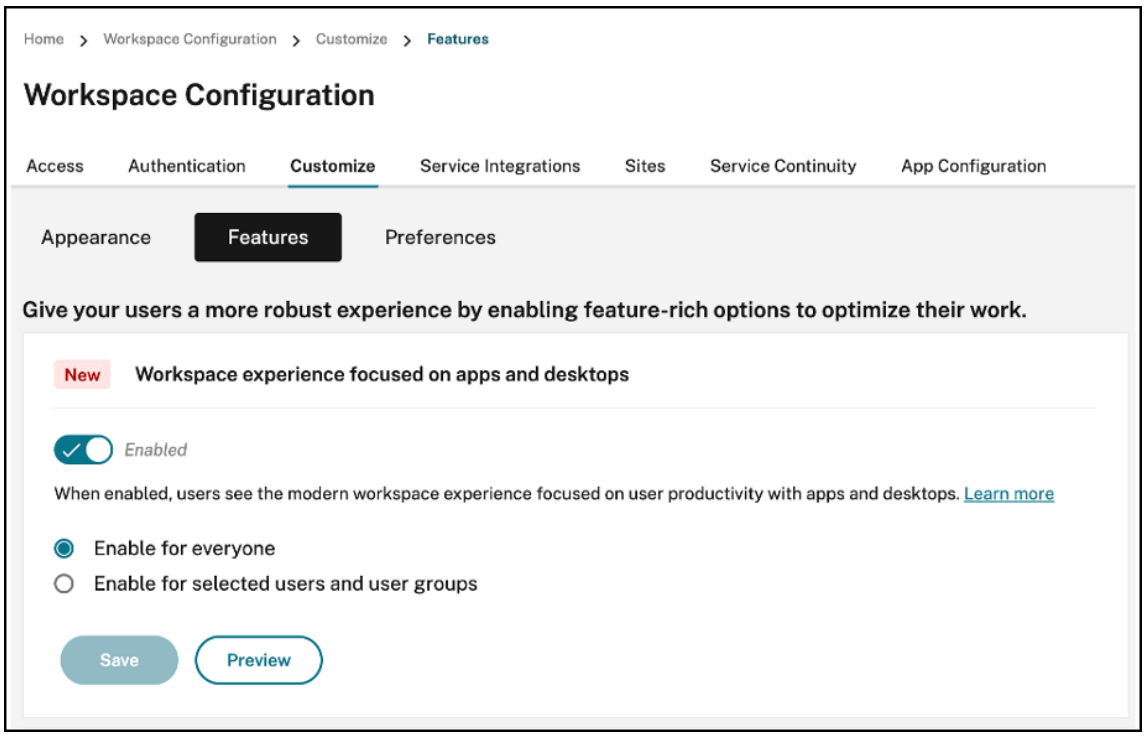
> **Nota:**
>
> La nueva interfaz de usuario es compatible con todas las versiones LTSR de la aplicación Citrix Workspace. También es compatible con todos los exploradores web, excepto con Internet Explorer (para el que la versión 23.26 de la interfaz de usuario de Citrix Workspace es fija).

Habilitar la nueva experiencia de Workspace

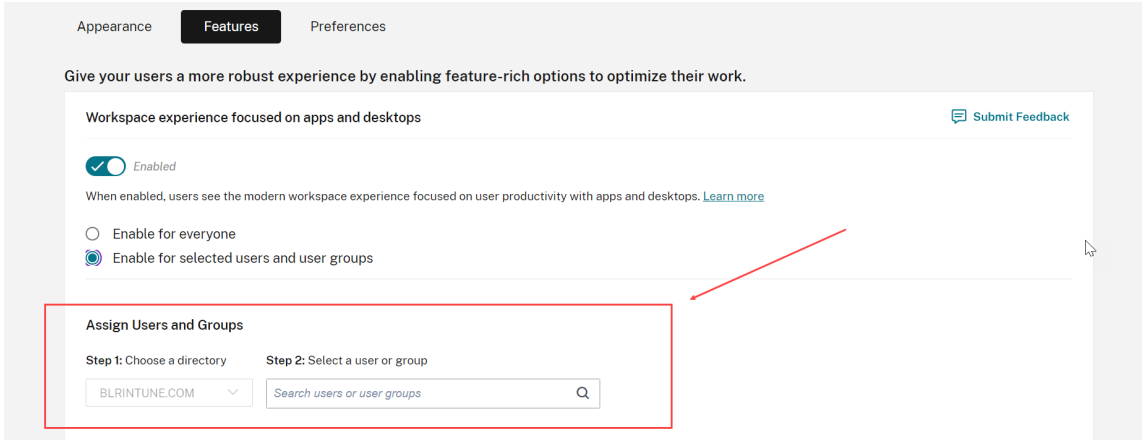
Puede habilitar la nueva interfaz de usuario de Workspace para los usuarios existentes. Al habilitarla, los usuarios pueden disfrutar de un espacio de trabajo moderno centrado en la productividad con aplicaciones y escritorios.

Para habilitar la nueva interfaz de usuario, siga estos pasos:

1. En la consola de administración, vaya a **Configuración de Workspace > Personalizar > Funciones**.
2. Active la opción **Experiencia de Workspace centrada en aplicaciones y escritorios**. De forma predeterminada, la opción está desactivada y la función inhabilitada.
   También tiene la opción de habilitar esta función para todos los usuarios o para los usuarios seleccionados.



- To enable the new UI for all end users, select **Enable for everyone**.
- To enable the new UI for selected users and user groups, select **Enable for selected user and user groups**. You can then select the directory to which the users or user groups belong. Once the appropriate directory is selected, you can view relevant users and user groups.



3. Haga clic en **Guardar**.
4. Reinicie la aplicación Workspace.

> **Nota:**
>
> La interfaz de usuario actualizada puede tardar unos cinco minutos en mostrarse. Puede que,

> temporalmente, los usuarios aún vean la versión anterior de la interfaz de usuario. Si se abre en un explorador, es posible que los usuarios tengan que actualizar la página.

Temas, iconos y fuentes

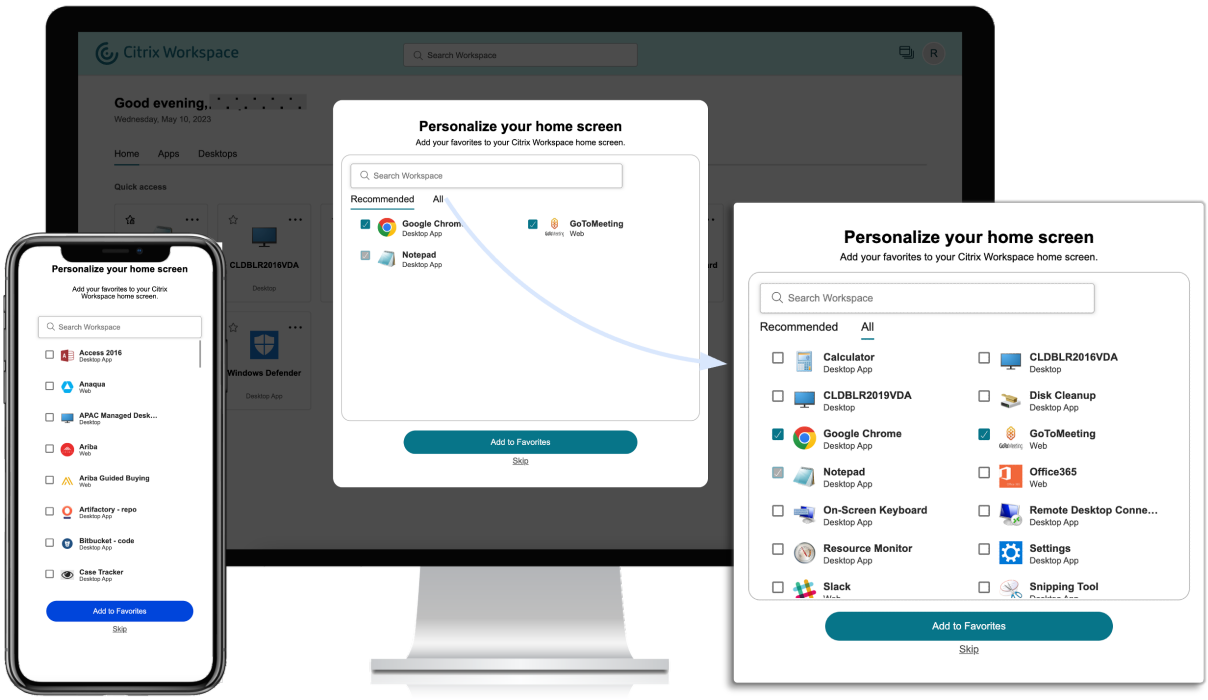
Los nuevos temas de color tienen un mejor contraste y una paleta de colores uniforme. La fuente se utiliza en la interfaz de usuario en todos los sistemas operativos compatibles. El nuevo conjunto de iconos tiene formas y colores más distinguibles, diseñados para una mayor legibilidad y claridad visual.

Experiencia de nuevo usuario con la aplicación Workspace

Al acceder por primera vez a la nueva interfaz, a los usuarios se les mostrará una ventana emergente en la que pueden marcar varias aplicaciones como favoritas en un simple paso.

La experiencia de nuevo usuario se activa cuando tiene más de 20 aplicaciones y no ha agregado ninguna a Favoritos. La experiencia es compatible con todos los exploradores y clientes nativos (Mac, Windows, Linux y ChromeOS), así como con dispositivos móviles (iOS y Android). Podrá disfrutarla la primera vez que inicie sesión.

Las aplicaciones recomendadas u obligatorias aparecen en la ficha **Recomendado** de la pantalla de nuevo usuario, tal como las configuran los administradores en la consola de DaaS para Citrix Virtual Apps and Desktops y en la consola de Secure Private Access para las aplicaciones web y SaaS. Las aplicaciones obligatorias se seleccionan de forma predeterminada y la casilla está inhabilitada. Las aplicaciones**recomendadas** y las favoritas automáticas se seleccionan de forma predeterminada y la casilla está habilitada para los usuarios. También puede seleccionar otras aplicaciones a las que suscribirse o agregar a Favoritos desde todas las fichas. Todas las aplicaciones seleccionadas se agregan automáticamente a Favoritos y aparecen en la página de inicio.



Cuando tiene cinco aplicaciones o menos, en la aplicación Citrix Workspace para Windows, aparece el acceso directo de escritorio.
Todas las aplicaciones mostradas se suscriben para los usuarios y se crean los accesos directos de escritorio correspondientes.

Limitaciones

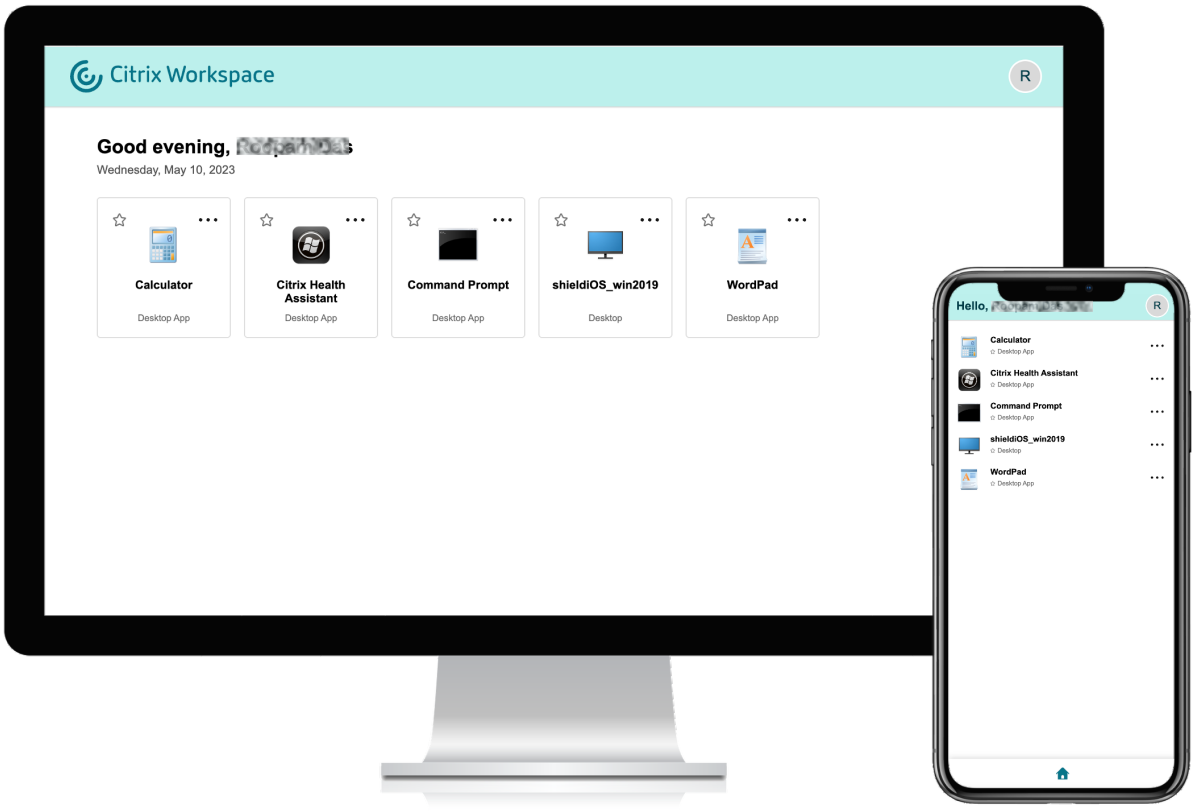
- Hasta que se mejore el *servicio de personalización de usuarios* para comprobar si un usuario es nuevo o no, la pantalla **Personalización** aparecerá una vez por dispositivo y explorador, y cada vez en modo incógnito, a menos que los usuarios marquen un favorito.
- Si el administrador elimina la etiqueta “obligatorio”o “recomendado”de las aplicaciones, no tendrá ningún efecto en las aplicaciones de **Favoritos**.
- Si el usuario final no ha agregado ninguna aplicación a **Favoritos**, la pantalla **Personalización** aparecerá cada vez que se abra la aplicación Workspace.
  Para evitar esto:
  - End users can add one or more apps to **Favorites**. This prevents the personalization screen from appearing everytime they start the app.
  - Administrators can add one or more apps to Favorites for end-users by using **Description and keyword settings** (keyword: Auto) in Citrix DaaS (**Manage** > **Full Configuration** >

Applications). This prevents the Personalization screen from appearing for all the end-users. For more information, see Customize workspace interactions.

Mejoras visuales y de diseño del espacio de trabajo

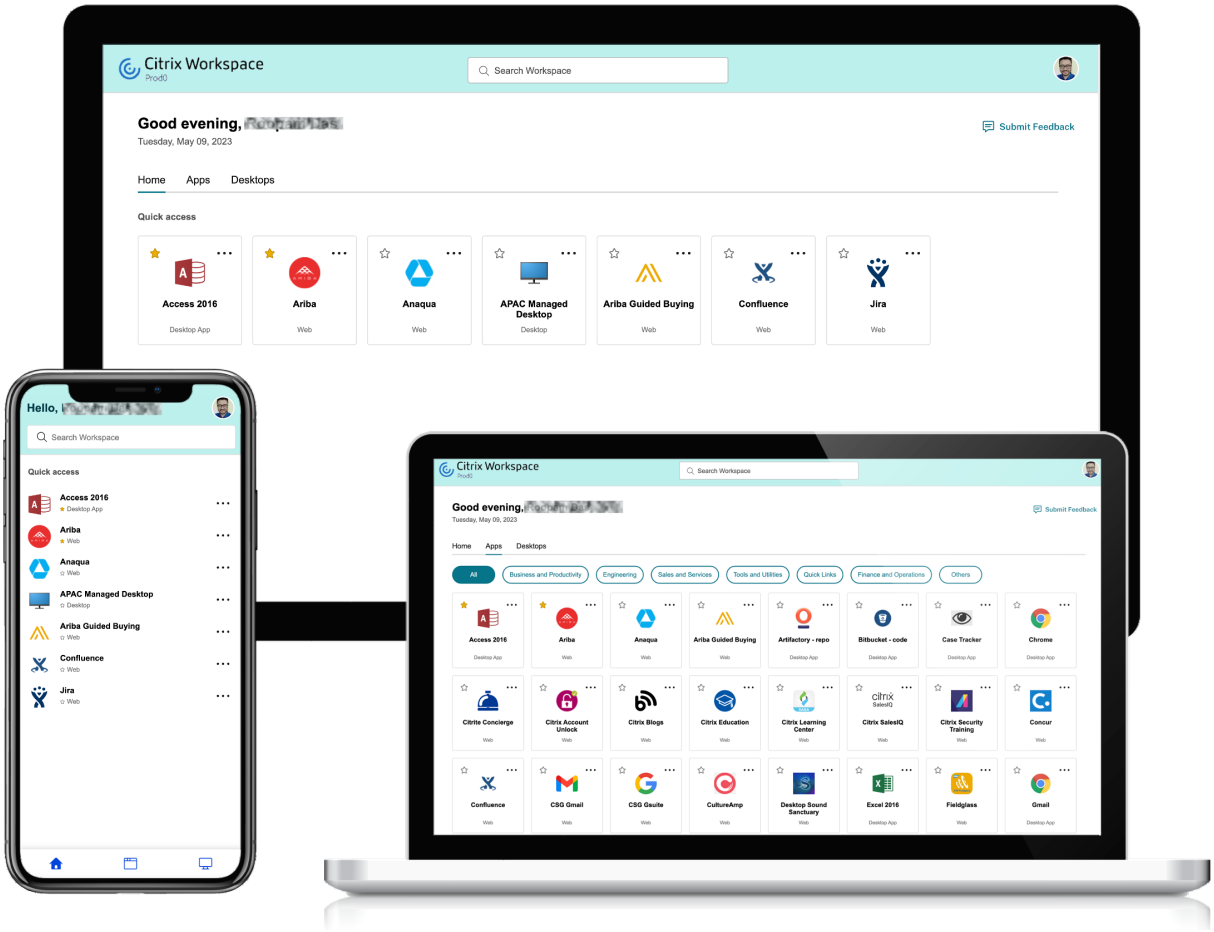
La experiencia de nuevo usuario se ha diseñado pensando en proporcionar facilidad de uso y un flujo intuitivo. Las aplicaciones y escritorios virtuales favoritos están organizados en la parte superior de la interfaz de usuario para facilitar su uso. Citrix también tiene una nueva página de inicio para mejorar la navegación por las aplicaciones y escritorios que se utilizan con más frecuencia.

Si tiene menos de 20 aplicaciones, accede a una pantalla con una vista sencilla sin fichas ni categorías. Todas las aplicaciones y escritorios aparecen en la misma página. En esta pantalla, aparecen primero las favoritas, seguidas del resto de aplicaciones en orden alfabético. Todas las aplicaciones tienen un icono de estrella que sirve para marcarlas como favoritas o no favoritas. Según la cantidad de aplicaciones que tenga, aparece esta sencilla vista de la aplicación Workspace y los administradores no controlan las aplicaciones.



Si tiene más de 20 aplicaciones, accederá a la página de inicio cuando inicie sesión. En esta pantalla aparecen primero todas sus aplicaciones favoritas, seguidas de las aplicaciones utilizadas más recientemente, con un límite de cinco aplicaciones. Los iconos de estrella de las aplicaciones **obligatorias**

están bloqueados y no se pueden quitar de Favoritos. Si el administrador no ha habilitado la página de inicio, accederá a la pantalla **Aplicaciones**. En esta pantalla, aparecen primero las favoritas, seguidas del resto de aplicaciones en orden alfabético. Si el administrador ha creado categorías y les ha adjuntado las aplicaciones, aparecerán las distintas categorías y podrá seleccionar la categoría de las aplicaciones que quiera ver.

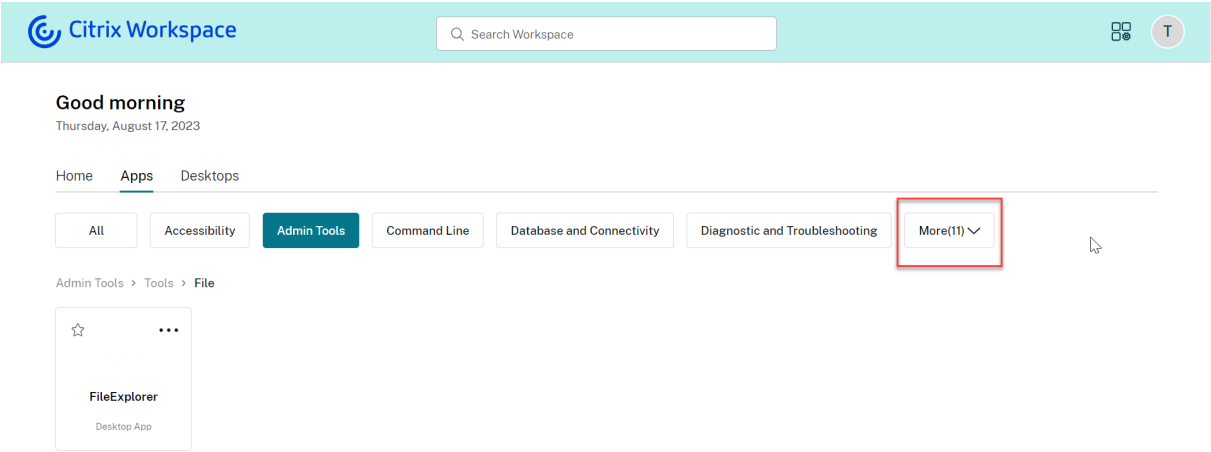


Categorización de aplicaciones

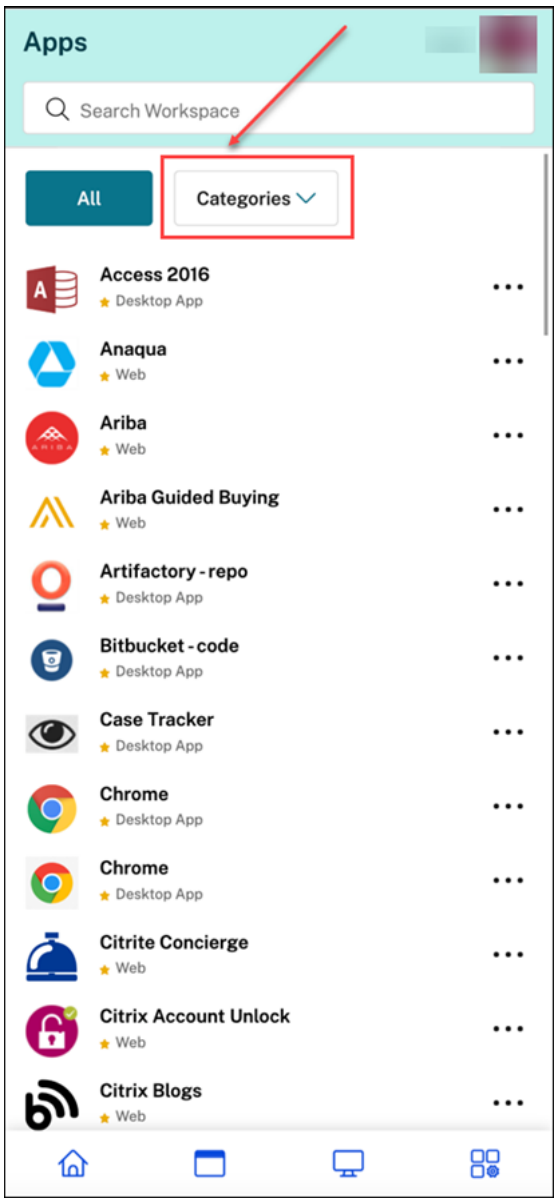
Los usuarios finales pueden ver sus aplicaciones organizadas en categorías y subcategorías en la interfaz de usuario de Workspace. Las subcategorías se muestran en una estructura de carpetas. La estructura organizada en varios niveles ofrece una experiencia optimizada y ordenada que ayuda a aumentar la satisfacción general del usuario.

> **Nota:**
>
> Para que las aplicaciones aparezcan en una estructura de carpetas, los administradores deben agregar una ruta de carpeta. Para obtener más información, consulte Agregar ruta de carpeta.

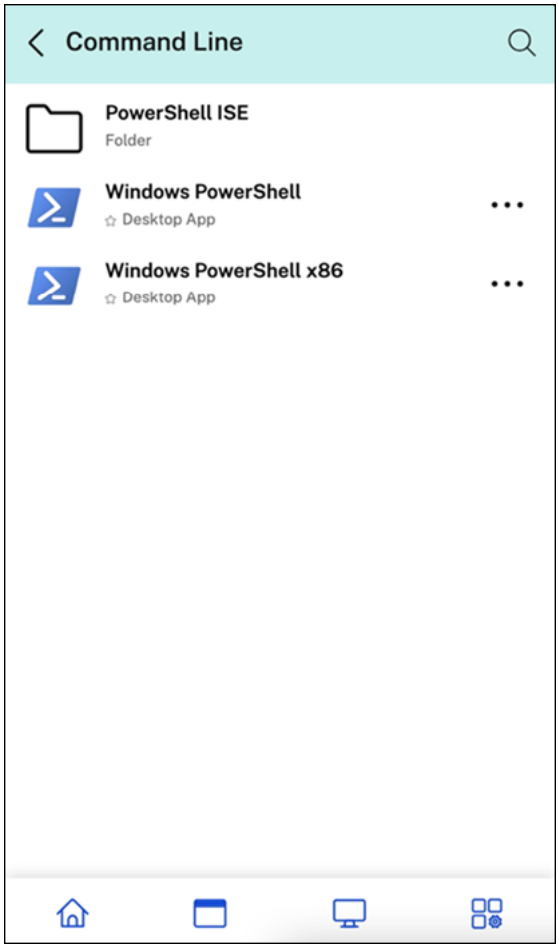
Cuando la cantidad de categorías principales creadas por los administradores supera el espacio disponible en la pantalla del usuario, la interfaz de usuario se ajusta en función del tamaño de la pantalla y desplaza las categorías de forma dinámica bajo el menú desplegable **Más**.
Las rutas de navegación también se muestran a los usuarios.



En plataformas móviles, vaya a la ficha Aplicaciones y haga clic en el menú desplegable **Categorías** para ver una lista de las categorías disponibles. Las subcategorías se muestran como carpetas que pueden contener más subcarpetas o aplicaciones según la configuración de administración.

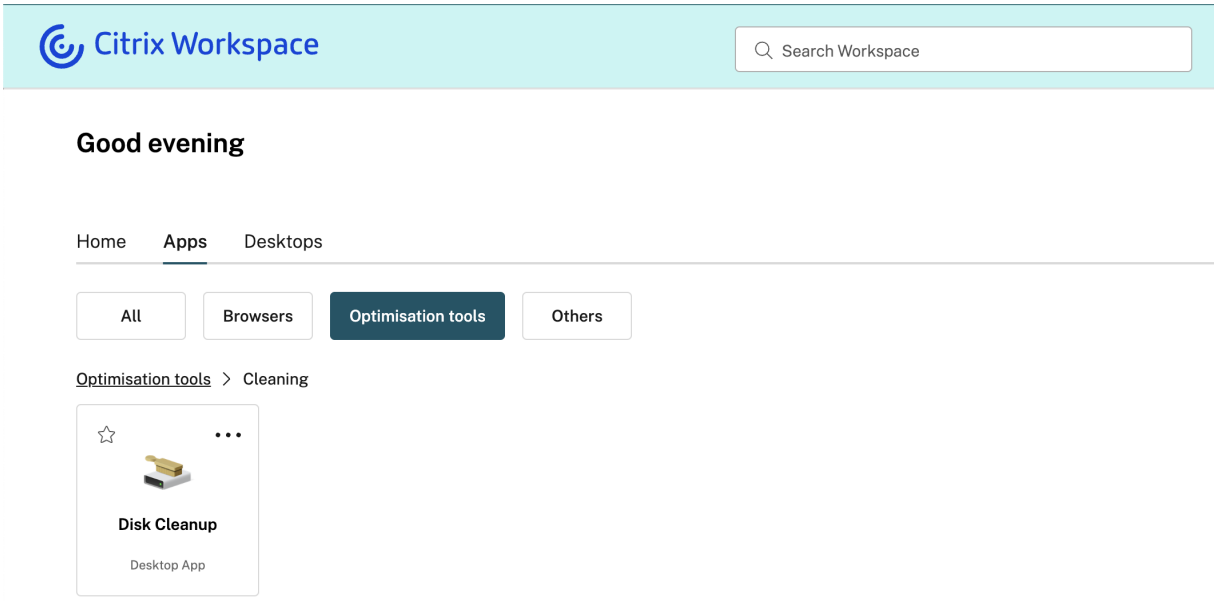


Seleccione la categoría correspondiente; se mostrará una lista de subcategorías y aplicaciones disponibles en función de la configuración realizada por el administrador.



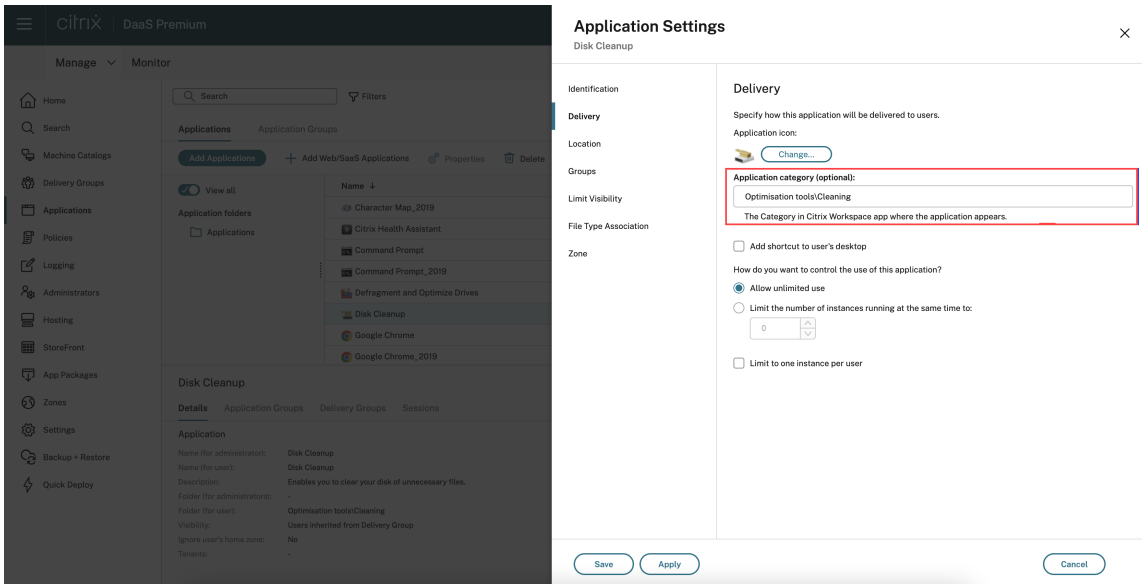
Agregar ruta de carpeta

La ruta de la carpeta le ayuda a definir las categorías en las que aparece una aplicación. Representa la estructura de carpetas que aparece en la pantalla para los usuarios finales.
Por ejemplo, considere una aplicación para la que la carpeta esté definida como `Optimisation tools/Cleaning`. Ahora, para acceder a esta aplicación, los usuarios finales deben ir a Optimisation tools > Cleaning, donde Optimisation tools es una categoría y Cleaning es su subcategoría.



Para definir la ruta de la carpeta de una aplicación:

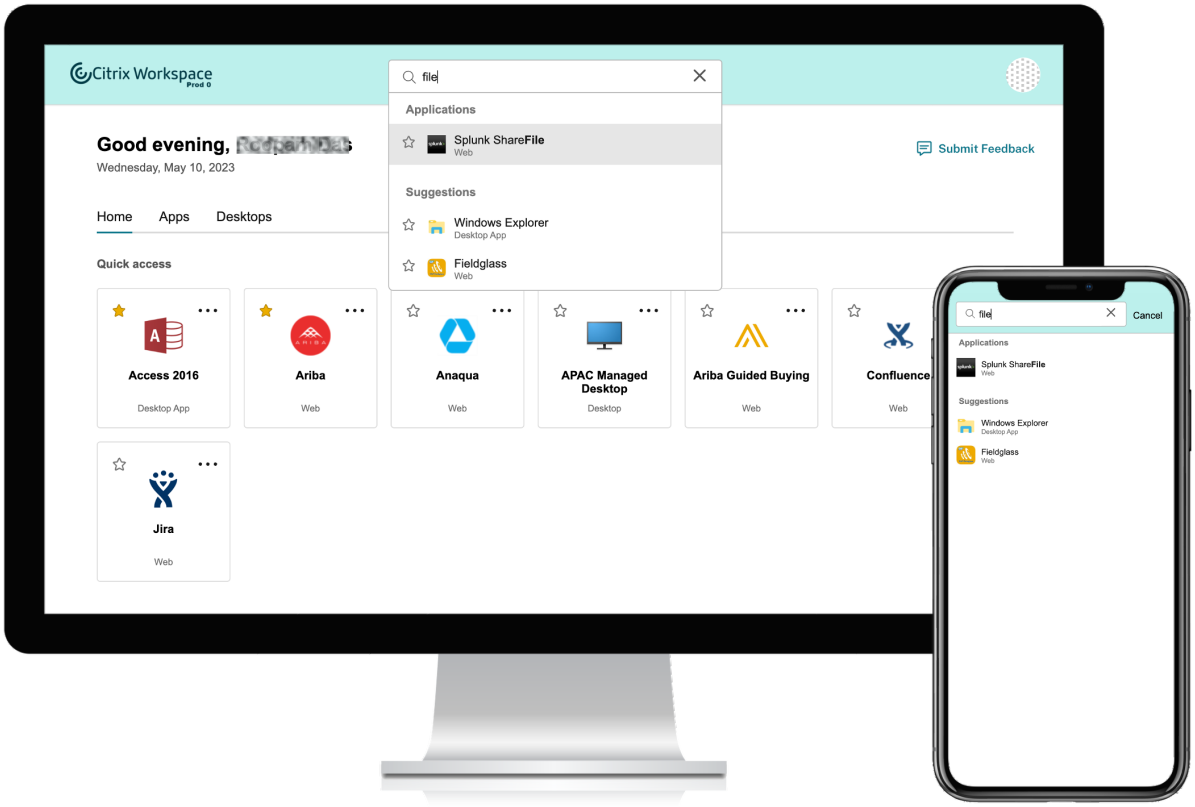
1. Vaya a **Citrix DaaS** en la consola de administración en la nube.
2. Vaya a **Aplicaciones** y localice la aplicación.
3. Haga clic con el botón secundario en la aplicación y seleccione **Propiedades**.
4. En el campo **Categoría de la aplicación**, defina la ruta de la carpeta.



5. Haga clic en **Guardar**

Función de búsqueda mejorada

La función de **búsqueda** mejorada ofrece resultados más rápidos en los motores de búsqueda. La opción **Buscar** aparece en la barra de herramientas para facilitar su uso y le permite hacer una búsqueda rápida e intuitiva desde la aplicación Workspace.



Incluye las siguientes mejoras:

- La búsqueda predeterminada muestra las cinco aplicaciones o escritorios utilizados más recientemente
- Las búsquedas se habilitan con corrector ortográfico y muestran resultados de autocompletar
- Los resultados de búsqueda incluyen aplicaciones de sesiones virtuales a las que se ha accedido recientemente y aplicaciones web y SaaS
- Realización de búsquedas por categorías creadas por el administrador
- Los resultados de búsqueda muestran los **favoritos** en la parte superior

Administrador de actividades

October 12, 2023

El administrador de actividades es una función sencilla pero eficaz de Citrix Workspace que permite a los usuarios administrar sus recursos de manera eficaz. Mejora la productividad al facilitar acciones rápidas en aplicaciones y escritorios activos desde cualquier dispositivo. Los usuarios pueden interactuar de forma fluida con sus sesiones para finalizar o desconectar las sesiones que ya no sean necesarias, liberar recursos y optimizar rendimiento desde cualquier lugar.

El panel del administrador de actividades muestra una lista consolidada de las aplicaciones y escritorios que están activos no solo en el dispositivo actual, sino también en cualquier dispositivo remoto que tenga sesiones activas. Los usuarios pueden ver esta lista al hacer clic en el icono del administrador de actividades situado junto al icono del perfil en escritorios y en la parte inferior de la pantalla en dispositivos móviles.

> **Nota:**
>
> Si no puede ver el icono del administrador de actividades en un tema de pancarta más oscuro, considere cambiar y probar el color seleccionado en el parámetro **Texto de pancarta y color de icono**. Es posible que el icono no se vea con claridad por el bajo contraste entre la pancarta y el icono del administrador de actividades. Para obtener más información, consulte Configurar temas personalizados.

Habilitar el administrador de actividades

Como administrador, ahora puede habilitar o inhabilitar la función de administrador de actividades para sus usuarios finales. Según las directivas de su organización, puede habilitar la función para todos o para los usuarios y grupos de usuarios que seleccione.

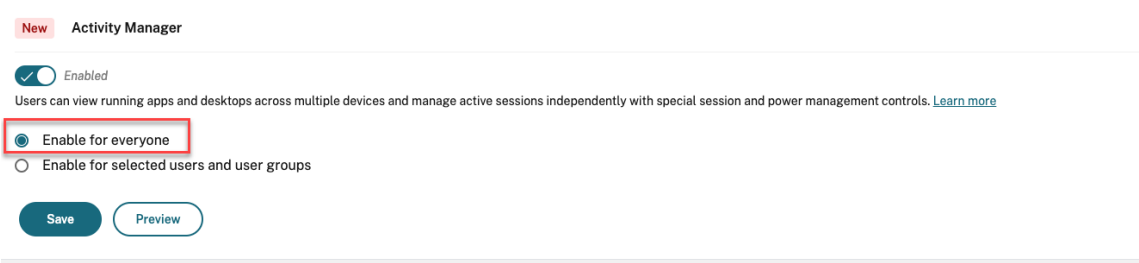
> **Nota:**
>
> La función del administrador de actividades solo se puede habilitar para la nueva interfaz de usuario. Para obtener más información sobre la nueva interfaz de usuario, consulte Habilitar la nueva experiencia de Workspace.

Para habilitar el administrador de actividades:

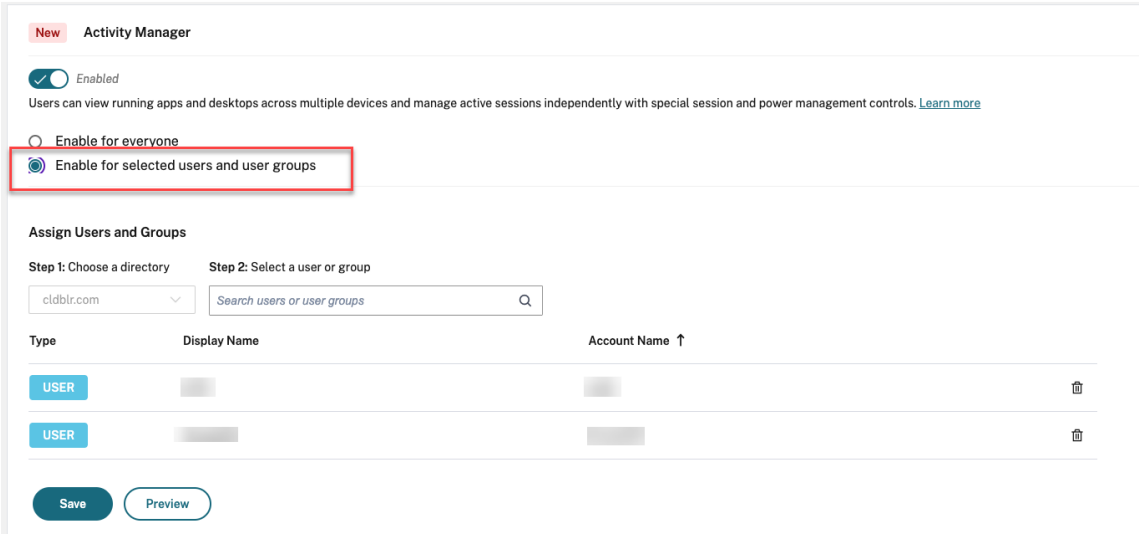
1. En la consola de administración, vaya a **Configuración de Workspace** > **Personalizar** > **Funciones**.
2. En la sección administrador de actividades, active el interruptor para habilitar el administrador de actividades.

3. A continuación, podrá personalizar los permisos de acceso de la siguiente manera.

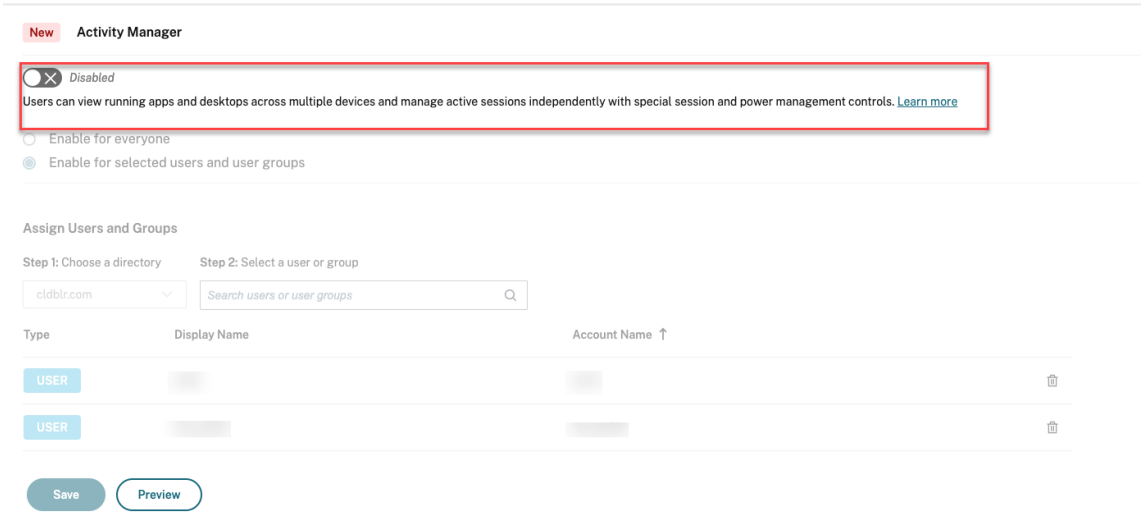
   - Para habilitar el administrador de actividades para todos los usuarios finales, seleccione **Habilitar para todos**.



   - Para habilitar el administrador de actividades para usuarios y grupos de usuarios determinados, seleccione **Habilitar para los usuarios y grupos de usuarios seleccionados**. A continuación, puede seleccionar el directorio al que pertenecen los usuarios o grupos de usuarios. Una vez seleccionado el directorio apropiado, puede ver los usuarios y grupos de usuarios relevantes.



   - Para inhabilitar el administrador de actividades para todos, desactive el interruptor.



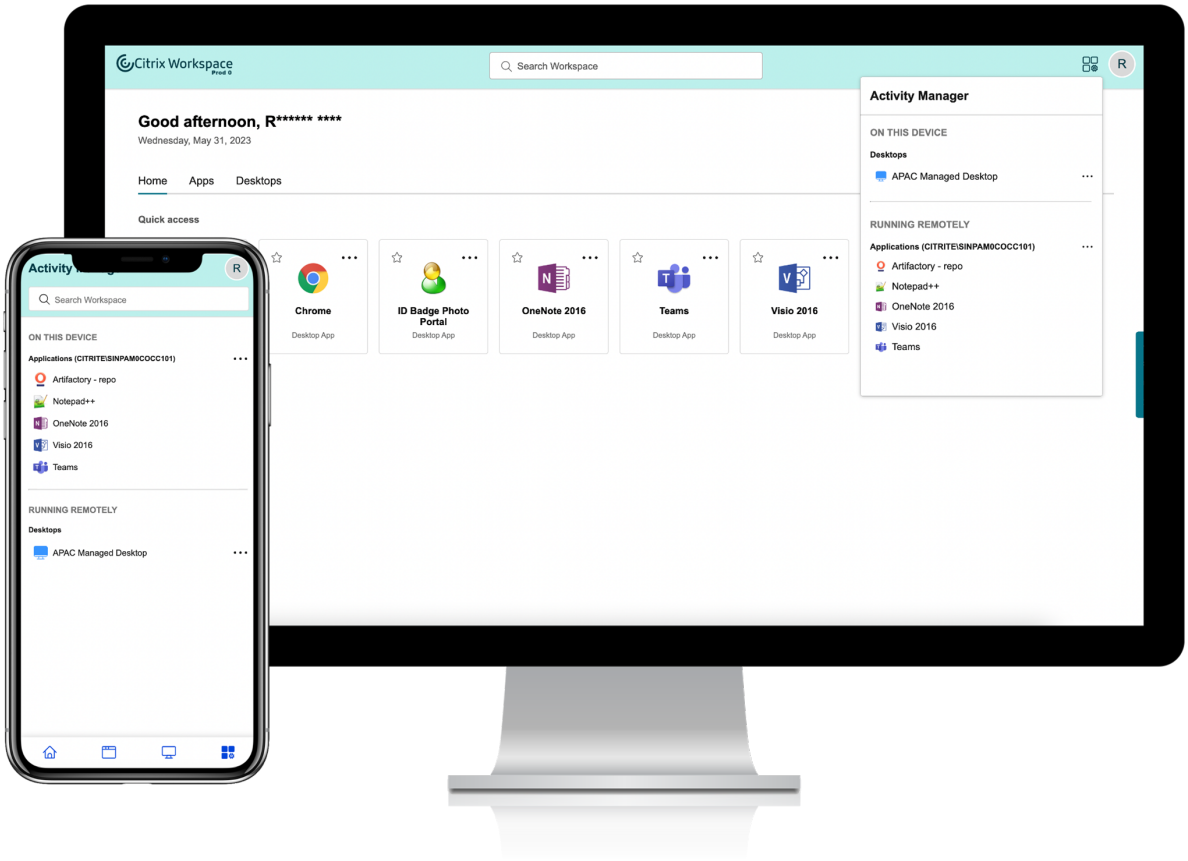
4. Haga clic en **Guardar**.

> **Nota:**
>
> Esta función solo es compatible con aplicaciones y escritorios virtuales. No se aplica a aplicaciones web ni SaaS.

Usar el administrador de actividades

Las aplicaciones y los escritorios activos se agrupan de esta manera en el administrador de actividades.

- La lista de aplicaciones y escritorios que están activos en el dispositivo actual se encuentra agrupada en **En este dispositivo**.
- Una lista de aplicaciones y escritorios activos en otros dispositivos se agrupan bajo **Ejecución remota**.



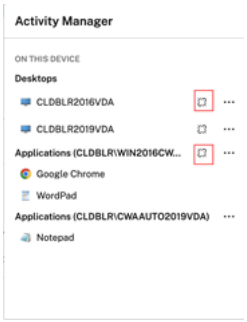
Los usuarios pueden realizar estas acciones en una aplicación o un escritorio al hacer clic en el botón de puntos suspensivos (…) correspondiente.

- **Desconectar**: La sesión remota se desconecta, pero las aplicaciones y los escritorios están activos en segundo plano.
- **Cerrar sesión**: Cierra la sesión en curso. Se cierran todas las aplicaciones de las sesiones y se pierden los archivos no guardados.
- **Apagar**: Cierra los escritorios desconectados.
- **Forzar cierre**: Apaga el escritorio por la fuerza en caso de problemas técnicos.
- **Reiniciar**: Apaga el escritorio y lo inicia de nuevo.

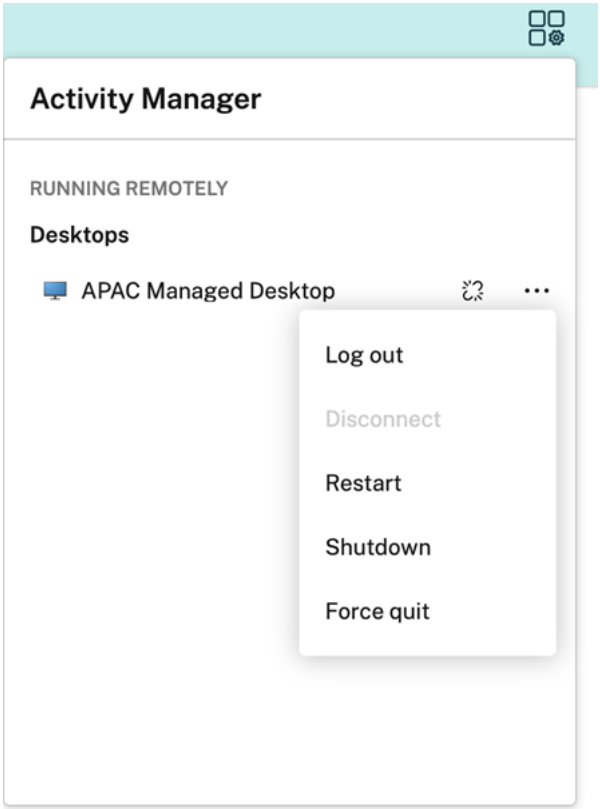
Aplicaciones y escritorios desconectados

Ahora, el administrador de actividades permite a los usuarios finales ver y realizar acciones en aplicaciones y escritorios que se ejecutan en modo desconectado, ya sea de forma local o remota. Las sesiones se pueden administrar desde dispositivos móviles o de escritorio, lo que permite a los usuarios finales realizar acciones sobre la marcha. Realizar acciones en sesiones desconectadas, como cerrar

la sesión o el apagado, promueve el uso optimizado de recursos y reduce el consumo de energía.



- Las aplicaciones y los escritorios desconectados se muestran en el panel del administrador de actividades y se indican mediante un icono de desconexión.
- Las aplicaciones desconectadas se agrupan en las sesiones respectivas y las sesiones se indican mediante un icono de desconexión.



Los usuarios finales pueden realizar estas acciones en sus escritorios desconectados al hacer clic en el botón de puntos suspensivos:

- **Cerrar sesión**: Use esta opción para cerrar sesión en el escritorio desconectado. Se cierran todas las aplicaciones de la sesión, y se pierden los archivos no guardados.
- **Apagar**: Use esta opción para cerrar los escritorios desconectados.

- **Forzar cierre**: Use esta opción para forzar el cierre de los escritorios desconectados en caso de problemas técnicos.
- **Reiniciar**: Use esta opción para apagar e iniciar de nuevo el escritorio desconectado.

El comportamiento de las sesiones desconectadas en el administrador de actividades difiere de esta manera.

- Si ha iniciado sesión en Citrix Workspace a través de un explorador web y desconecta una sesión local, la sesión se muestra primero en "En este dispositivo". Sin embargo, cuando cierra y abre de nuevo el administrador de actividades, la sesión desconectada pasará a "Ejecución remota" .
- Si ha iniciado sesión en la aplicación Citrix Workspace a través de un dispositivo nativo y desconecta una sesión local, la sesión desconectada desaparece de la lista. Sin embargo, cuando cierra y abre de nuevo el administrador de actividades, la sesión desconectada pasará a "Ejecución remota".

Entregar DaaS y Virtual Apps and Desktops con Citrix Workspace

October 12, 2023

Citrix Workspace es el servicio multiarrendatario en la nube que sustituye a StoreFront, que es la tienda de aplicaciones local de un solo arrendatario que combina las aplicaciones y los escritorios de Citrix DaaS. La plataforma Citrix Workspace es el componente de nube que proporciona las herramientas, los servicios y las funciones necesarias para el trabajo remoto, la extensibilidad y la personalización a través de Citrix Workspace.

Tiene diferentes opciones para combinar DaaS con Citrix Workspace. La opción que elija dependerá de:

- Si quiere migrar completamente a la nube o prefiere adoptar una solución híbrida.
- Si piensa permitir el acceso externo a DaaS.

Migración completa a la nube

Puede migrar su configuración local a la nube, lo que permite a los suscriptores acceder a DaaS a través de Workspace y, así, trasladar su infraestructura administrada por TI a un entorno administrado por Citrix. La migración completa a la nube significa que tiene menos componentes que administrar.

Citrix recomienda utilizar la herramienta de configuración automatizada para simplificar el proceso de migración de uno o más sitios locales a un servicio en la nube. Los principales pasos involucrados en este proceso son los siguientes:

1. Asegúrese de que cumple con los requisitos previos para migrar la configuración.
2. Exporte su configuración local. Para obtener información sobre este proceso, consulte Exportar la configuración local de Citrix Virtual Apps and Desktops.
3. Importe su configuración en la nube. Para obtener información sobre este proceso, visite Importar la configuración en Citrix DaaS.

Para obtener más información sobre la configuración automatizada, consulte Migrar a la nube y la guía de implementación de Tech Zone.

Agregación de sitios para soluciones híbridas

Puede realizar la transición a Citrix Workspace con su implementación local existente de Virtual Apps and Desktops. Este proceso se denomina agregación de sitios e implica sustituir la infraestructura administrada por TI por una infraestructura administrada por Citrix.

Puede elegir la agregación de sitios para hacer una transición lenta a Workspace, o si busca una solución híbrida que aloje algunos componentes, pero no todos, en la nube. Un modelo híbrido le permite administrar la capacidad de la nube junto con los recursos locales y ofrece una experiencia unificada para el usuario final, sin necesidad de migrar completamente a la nube.

Antes de pasar de StoreFront a Workspace con agregación de sitios, debe tener una configuración de Active Directory (AD) y Cloud Connectors instalados en las ubicaciones de recursos.

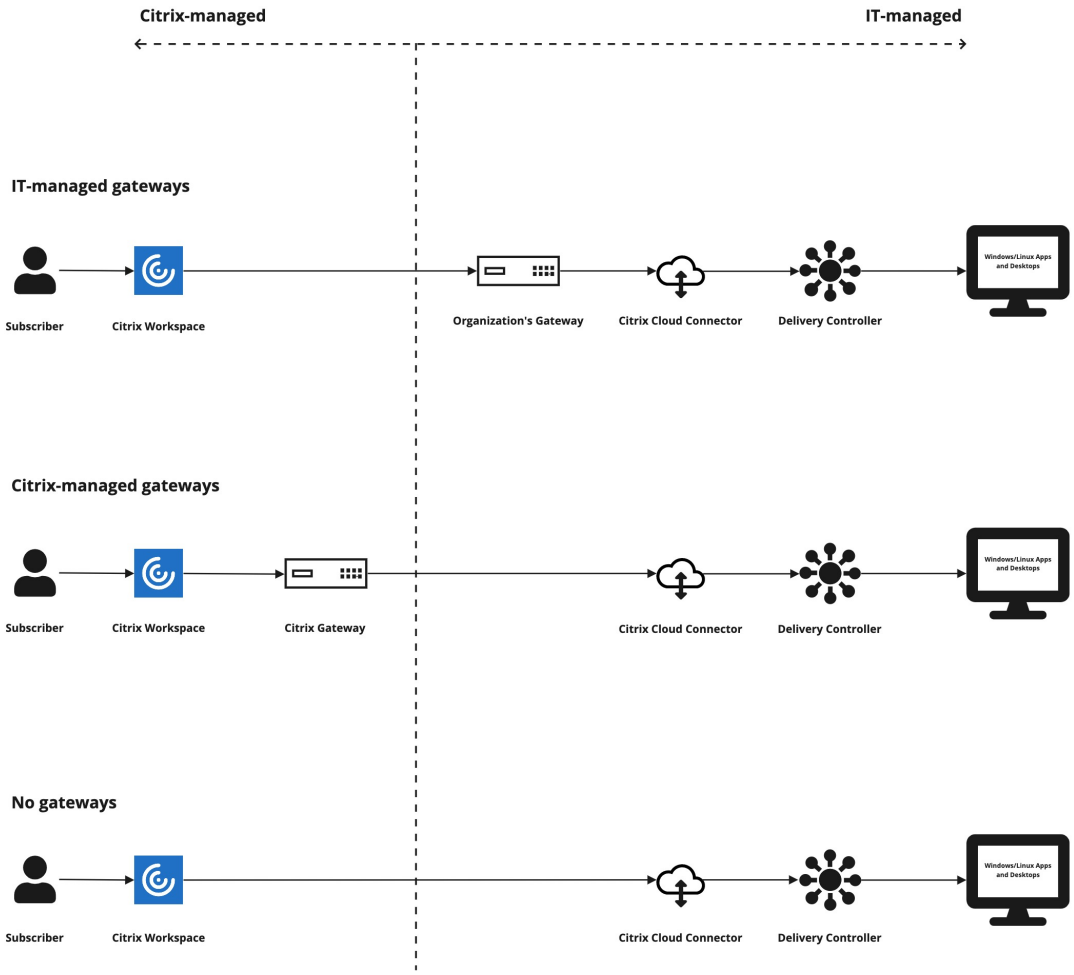
Hay tres pasos generales involucrados en la agregación de sitios:

1. **Detectar el sitio.** Un sitio comprende los componentes que conforman una implementación de producción. Es posible que tenga diferentes sitios para diferentes ubicaciones y sucursales.
2. **Verificar la conexión de Active Directory (AD).** Los suscriptores deben autenticarse en Citrix Workspace con AD. Asegúrese de que los suscriptores puedan autenticarse detectando los dominios de AD en los que están instalados sus Cloud Connectors.
3. **Elegir el tipo de implementación.** Hay tres opciones de conectividad para este paso:
    - Puertas de enlace administradas por TI
    - Puertas de enlace administradas por Citrix
    - Sin puerta de enlace

Para obtener más información, consulte Opciones de conectividad.

Opciones de conectividad

Las tres opciones siguientes proporcionan acceso a DaaS a través de Citrix Workspace y están diseñadas para diferentes requisitos empresariales.



Opción de conectividad	Caso
Puertas de enlace tradicionales (administradas por TI)	Elija esta opción si quiere usar su propia puerta de enlace para la conectividad externa a sus instancias de DaaS. Esto le permite aprovechar su inversión actual en puertas de enlace locales.

Opción de conectividad	Caso
Puertas de enlace administradas por Citrix	Elija esta opción si quiere usar **Citrix Gateway Service** para la conectividad externa a sus aplicaciones y escritorios virtuales. Las conexiones HDX entre los clientes y los VDA se realizan mediante proxy a través de **Citrix Gateway Service**.
Sin puerta de enlace (solo interna)	Elija esta opción si quiere que los suscriptores inicien DaaS *solo* con clientes de su red corporativa. Si elige esta opción, los suscriptores no tendrán acceso externo a DaaS.

Para obtener más información sobre el proceso de agregación de sitios y los pasos involucrados, consulte Agregación de aplicaciones y escritorios virtuales locales a espacios de trabajo.

Configurar la resiliencia y la optimización del espacio de trabajo

Para obtener información sobre cómo mejorar la eficiencia y la disponibilidad de DaaS a través de Citrix Workspace, consulte Optimizar DaaS en Citrix Workspace. Citrix proporciona instrucciones sobre cómo:

- Optimizar la conectividad con Conexión directa de carga de trabajo.
- Garantizar la continuidad del servicio durante una interrupción a efectos de resiliencia sin conexión.
- Configurar Single Sign-On (SSO) en aplicaciones y escritorios virtuales con el Servicio de autenticación federada (FAS) de Citrix.

Configurar el acceso a los espacios de trabajo

November 21, 2023

Citrix recomienda utilizar la versión más reciente de la aplicación Citrix Workspace para acceder a los espacios de trabajo. La aplicación Citrix Workspace sustituye a Citrix Receiver. También puede acceder a espacios de trabajo con las versiones más recientes de Microsoft Edge, Google Chrome, Mozilla Firefox y Apple Safari, con la URL de Workspace correspondiente.

En este artículo se resumen los pasos necesarios para configurar y usar:

- La URL de Workspace
- La aplicación Citrix Workspace (anteriormente Citrix Receiver).
- Citrix Gateway o Citrix Gateway Service para conectividad externa.
- Proveedores de identidades para la autenticación en los espacios de trabajo.

Introducción

Los suscriptores pueden acceder a Citrix Workspace por medio de un explorador con la URL del espacio de trabajo o a través de la aplicación Citrix Workspace instalada en sus dispositivos.

La URL del espacio de trabajo es personalizable y está habilitada de forma predeterminada. Para obtener instrucciones sobre cómo modificar la URL del espacio de trabajo, consulte URL del espacio de trabajo en este artículo

La aplicación Citrix Workspace sustituye a Citrix Receiver como la aplicación que se instala de forma nativa y proporciona acceso a la interfaz de usuario (IU) de Workspace. Para obtener información sobre la aplicación Citrix Workspace y la transición desde Citrix Receiver, consulte Aplicación Citrix Workspace (anteriormente Citrix Receiver) en este artículo.

Los suscriptores remotos pueden obtener acceso externo a sus espacios de trabajo si configura la conectividad externa con Citrix Gateway o Citrix Gateway Service. Para obtener información sobre cómo habilitar el acceso remoto a los espacios de trabajo, consulte Conectividad externa en este artículo.

Como alternativa, solo para la conectividad interna, puede utilizar Citrix Workspace solamente o alojar un almacén local de StoreFront. Para la conectividad interna, el dispositivo de punto final debe conectarse directamente a la dirección IP del Virtual Delivery Agent (VDA).

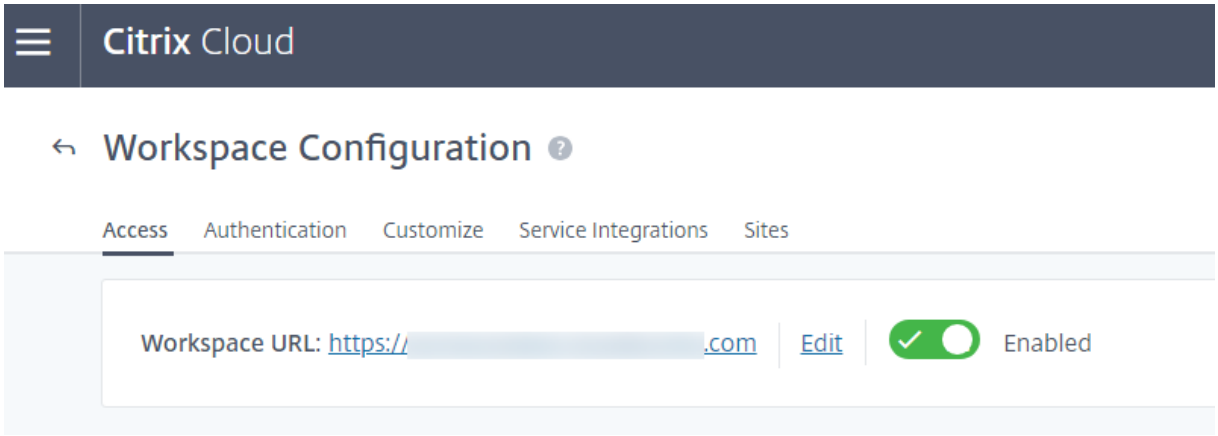
Citrix Workspace admite una lista creciente de proveedores de identidades que se conectan a Citrix Cloud y, a continuación, se habilitan en **Configuración de Workspace** para autenticar a los suscriptores en sus espacios de trabajo. Para obtener información sobre cómo configurar la autenticación para los suscriptores de Workspace, consulte la sección Autenticación en espacios de trabajo de este artículo

Citrix Workspace también admite las siguientes opciones de autenticación:

- Tokens como segundo factor de autenticación para iniciar sesión en los espacios de trabajo con Active Directory. Para obtener más información sobre cómo configurar la autenticación de varios factores (MFA) en Workspace, consulte Autenticación de dos factores.
- Servicio de autenticación federada (FAS) de Citrix para proporcionar Single Sign-On (SSO) a DaaS en Citrix Workspace. Para obtener más información sobre cómo configurar SSO con FAS, consulte Habilitar Single Sign-On para espacios de trabajo con el Servicio de autenticación federada de Citrix.

URL del espacio de trabajo

La URL de Workspace está lista para usarse y se puede encontrar en **Citrix Cloud > Configuración de Workspace > Acceso**, donde la puede habilitar, modificar e inhabilitar.



Personalizar la URL del espacio de trabajo

La primera parte de la URL de Workspace es personalizable. Por ejemplo, puede cambiar la URL de `https://example.cloud.com` a `https://newexample.cloud.com`.

Puede cambiar la dirección URL de Workspace solo cuando esté habilitada. Si la URL está inhabilitada, primero debe volver a habilitarla.

Para habilitar la URL de Workspace, vaya a **Configuración de Workspace > Acceso** y seleccione la opción para habilitarla. El proceso de habilitar la URL de Workspace puede tardar hasta 10 minutos en surtir efecto.

La primera parte de la URL de Workspace representa la organización que usa la cuenta de Citrix Cloud, y debe cumplir las condiciones del Contrato de usuario final de Cloud Software Group. El uso indebido de los derechos de propiedad intelectual de un tercero, incluidas las marcas comerciales, podría resultar en la revocación y reasignación de la URL de Workspace o en la suspensión de la cuenta de Citrix Cloud.

Para personalizar una URL, vaya a **Configuración de Workspace > Acceso** y seleccione **Modificar**. La parte personalizable de la URL:

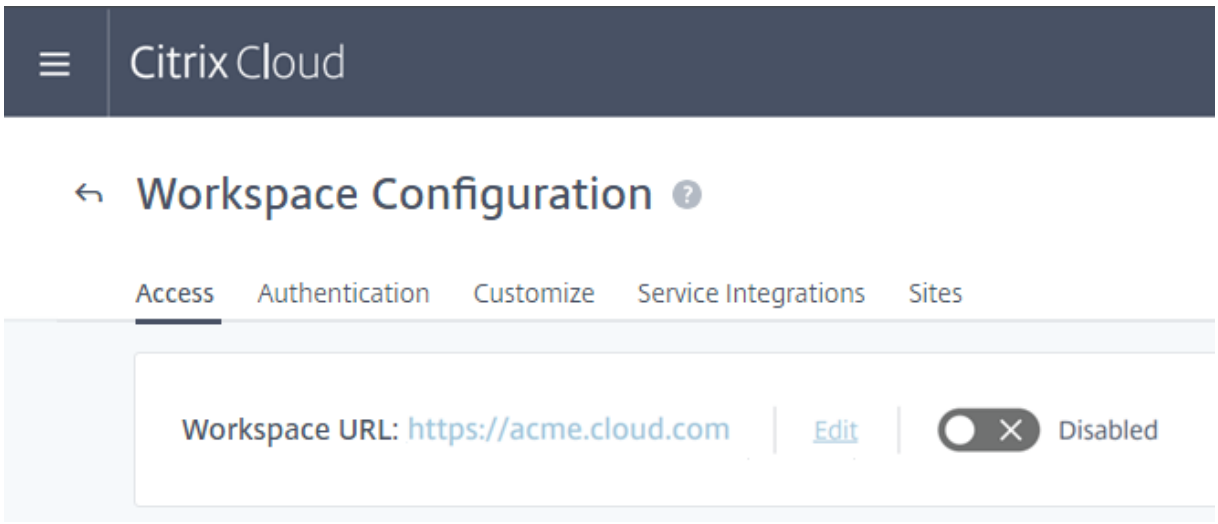
- Debe tener entre 6 y 63 caracteres. Si quiere cambiar la parte personalizable de la URL por un nombre de menos de 6 caracteres, cree un tíquet de asistencia en Citrix Cloud.
- Solo debe contener letras y números.
- No puede incluir caracteres Unicode.

Cuando se cambia el nombre de una URL, la URL anterior se elimina inmediatamente y deja de estar

disponible. Informe a los suscriptores de la nueva URL y actualice manualmente todas las aplicaciones locales de Citrix Workspace para que utilicen la nueva URL.

Inhabilitar la URL del espacio de trabajo

Puede inhabilitar la dirección URL de Workspace para evitar que los usuarios se autentiquen a través de Citrix Workspace. Por ejemplo, es posible que prefiera que los suscriptores usen la URL de una implementación local de StoreFront para acceder a los recursos, o bien puede que le interese impedir el acceso durante los períodos de mantenimiento.



El proceso de inhabilitar la URL de Workspace puede tardar hasta 10 minutos en surtir efecto.

Inhabilitar la URL del espacio de trabajo tiene los siguientes efectos:

- Todas las integraciones de servicios se inhabilitan. Los suscriptores no podrá acceder a los datos ni a las aplicaciones de los servicios en el espacio de trabajo de Citrix Workspace.
- No se puede personalizar la URL de Workspace. Debe volver a habilitar la URL para poder cambiarla.
- Cualquier persona que visite la URL recibirá un mensaje en su explorador que indica que no se puede encontrar el espacio de trabajo o que no se pueden cargar los recursos.

Aplicación Citrix Workspace (anteriormente Citrix Receiver)

> **Importante:**
>
> Citrix Receiver ha alcanzado el final de su ciclo de vida (EoL) y ya no se desarrollará más. Si continúa utilizando Citrix Receiver, la asistencia técnica se limita a las opciones descritas en Lifecycle Milestones and Definitions. Para obtener información sobre los hitos de Fin de vida de Citrix Receiver por plataforma, consulte Lifecycle milestones for Citrix Workspace app and Citrix

> Receiver.

La aplicación Citrix Workspace es una aplicación que se instala de forma nativa y sustituye a Citrix Receiver para acceder a los espacios de trabajo.

Métodos de autenticación admitidos para la aplicación Citrix Workspace

En esta tabla se muestran los métodos de autenticación admitidos en la aplicación Citrix Workspace. La tabla incluye métodos de autenticación relevantes para versiones específicas de Citrix Receiver, que la aplicación Citrix Workspace reemplaza.

Aplicación Citrix Workspace	Autenticación con Active Directory	Autenticación con Active Directory y token	Autenticación con Azure Active Directory
Citrix Workspace para Windows	Sí	Sí	Sí (aplicación Workspace; Receiver 4.9 LTSR CU2 y posteriores solamente; Receiver 4.11 CR y posteriores solamente)
Citrix Workspace para Linux	Sí	Sí	Sí (aplicación Workspace, Receiver 13.8 y posteriores solamente)
Citrix Workspace para Mac	Sí	Sí	Sí
Citrix Workspace para iOS	Sí	Sí	Sí
Citrix Workspace para Android	Sí	Sí	Sí (aplicación Workspace, Receiver 3.13 y posteriores solamente)

Para obtener más información acerca de las funciones admitidas en la aplicación Citrix Workspace por plataforma, consulte la Tabla de funciones de las aplicaciones Citrix Workspace.

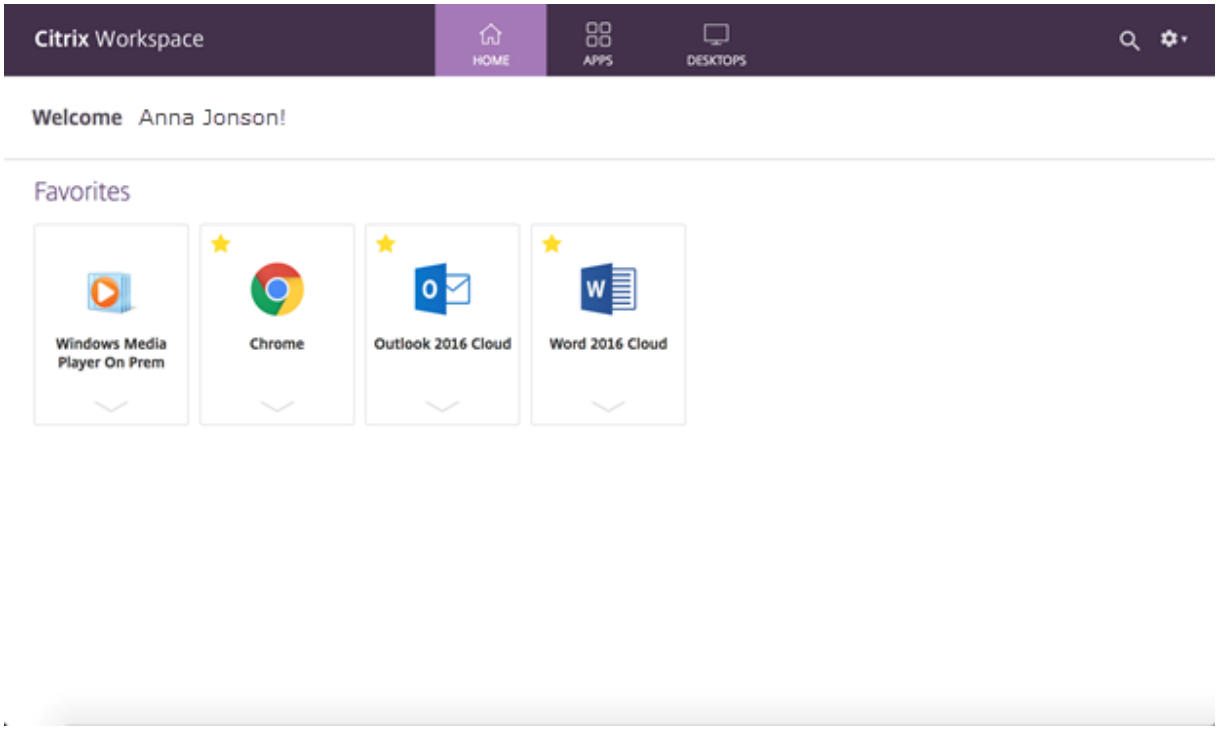
Para ver una descripción general de la compatibilidad de TLS y SHA2 con Citrix Receivers, consulte el artículo de asistencia CTX23226.

Transición de Citrix Receiver a la aplicación Citrix Workspace

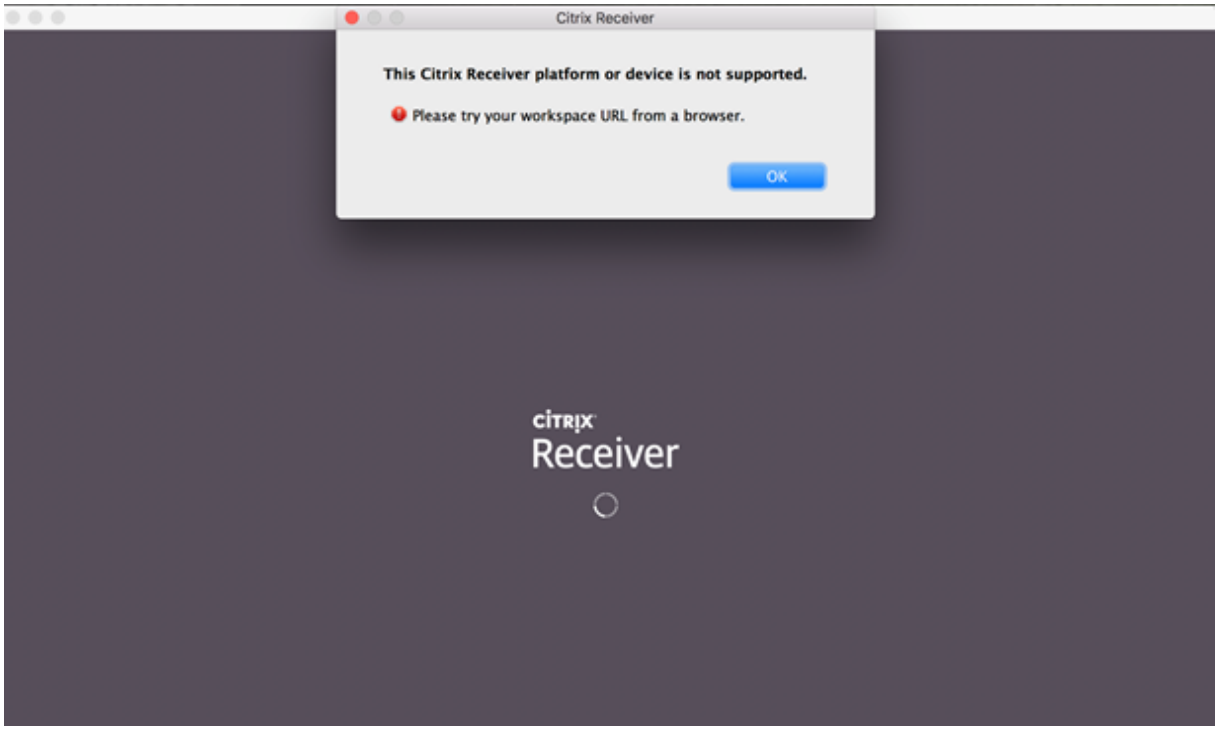
La aplicación Citrix Workspace reemplaza y amplía las prestaciones de Citrix Receiver.

La aplicación Citrix Workspace ofrece a los suscriptores acceso Single Sign-On (SSO) a aplicaciones SaaS, web y virtuales. Para obtener información sobre Single Sign-On para los suscriptores de espacios de trabajo, consulte Habilitar Single Sign-On para espacios de trabajo con el Servicio de autenticación federada de Citrix.

Citrix Receiver no ofrece esta función de control de acceso. Por lo tanto, con los mismos servicios y control de acceso habilitados, los usuarios de Citrix Receiver todavía ven la interfaz de usuario morada, pero sin aplicaciones web ni SaaS. Además, **Citrix Files** no se admite en Citrix Receiver y los suscriptores no pueden acceder a las aplicaciones de esta manera.



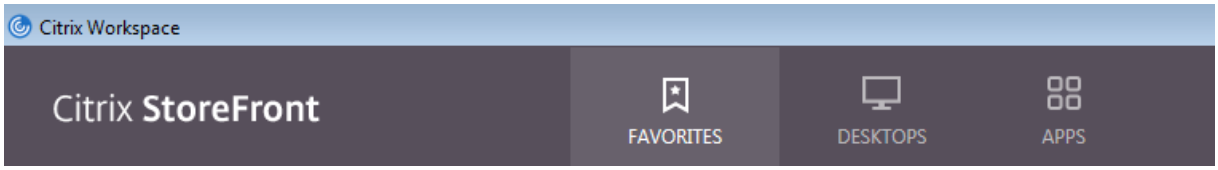
Azure Active Directory (AAD) tampoco es compatible con Citrix Receiver. Si los suscriptores intentan acceder a Workspace con Citrix Receiver cuando AAD está habilitado como método de autenticación, verán un mensaje que indica que el dispositivo no es compatible. Una vez que hayan actualizado Receiver a la aplicación Citrix Workspace, podrán acceder a sus espacios de trabajo.



Los clientes que actualizan a la aplicación Citrix Workspace (o usan un explorador web) pueden ver la nueva interfaz de usuario. Para obtener más información sobre la experiencia del suscriptor con esta interfaz de usuario, consulte Gestionar la experiencia en los espacios de trabajo.

Además de una nueva interfaz de usuario, la aplicación Citrix Workspace permite a los suscriptores usar todas las nuevas funciones que se hayan habilitado. Los suscriptores pueden acceder a **Archivos**, ver DaaS y acceder a aplicaciones web y SaaS a través de Citrix Gateway Service.

Si tiene una implementación de StoreFront (local), la actualización de Citrix Receiver a la aplicación Citrix Workspace solo cambia el icono para abrir la aplicación Citrix Workspace.



> **Nota:**
>
> Los usuarios de Citrix Cloud Government siguen viendo su interfaz de usuario de color morado cuando usan la aplicación Citrix Workspace o cuando acceden a Workspace desde un explorador web.

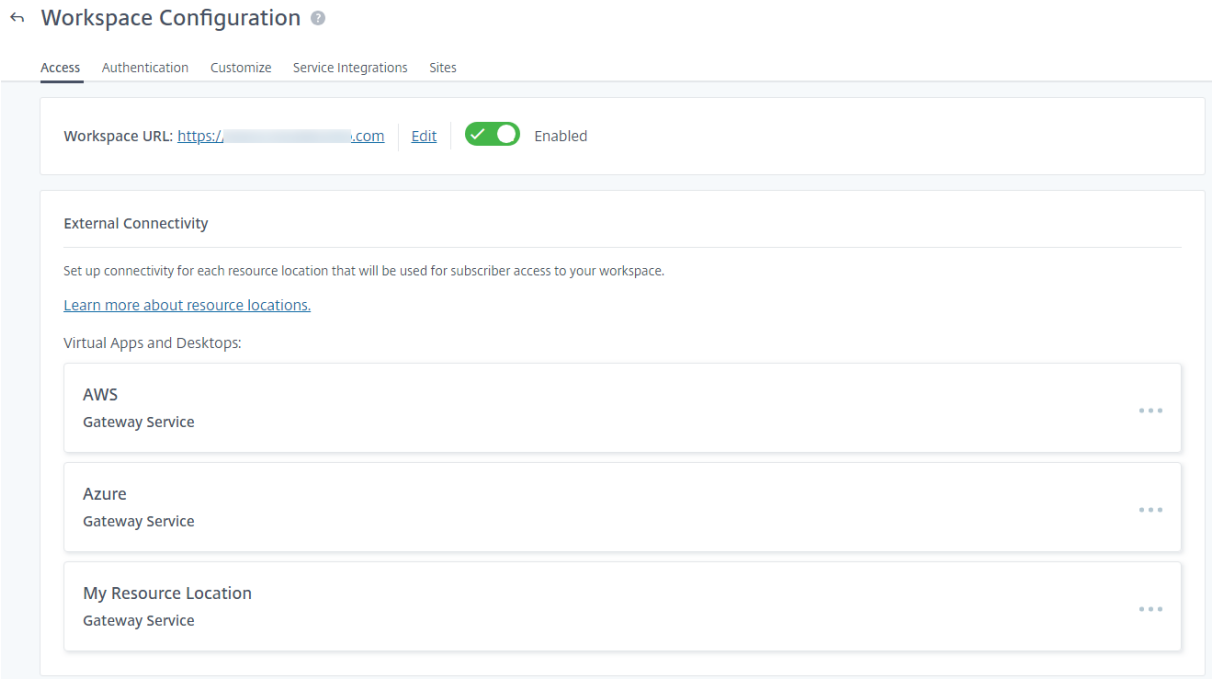
Conectividad externa

Proporcione acceso seguro a los suscriptores remotos agregando Citrix Gateways o Citrix Gateway Service a las ubicaciones de los recursos.

Citrix admite las siguientes opciones de conectividad externa:

- Citrix aloja Citrix Gateway y Citrix ADC
- Usted aloja Citrix Gateway y Citrix ADC de forma local

Puede agregar Citrix Gateways en **Configuración de Workspace > Acceso > Conectividad externa**, o en **Citrix Cloud > Ubicaciones de recursos**.



> **Nota:**
>
> La parte "Conectividad externa"de la página **Configuración de Workspace > Acceso** no está disponible en Citrix Virtual Apps Essentials. El servicio Citrix Virtual Apps Essentials utiliza Citrix Gateway Service, que no requiere configuración adicional.

Autenticación en los espacios de trabajo

Configurar la autenticación del espacio de trabajo para los suscriptores es un proceso de dos pasos:

1. Definir uno o más proveedores de identidades en **Administración de acceso e identidad**. Para obtener instrucciones, visite Administración de acceso e identidad.
2. Elegir uno de los proveedores de identidades configurados como método de autenticación utilizado por los suscriptores para iniciar sesión en sus espacios de trabajo en **Configuración de Workspace**. Para obtener instrucciones, consulte Elegir o cambiar los métodos de autenticación.

Al configurar más proveedores de identidades en **Administración de acceso e identidad**, hay más

opciones para elegir en **Configuración de Workspace** la forma en que los suscriptores inician sesión en sus espacios de trabajo.

Proveedores de identidades compatibles para autenticar suscriptores

Los suscriptores pueden autenticarse en sus espacios de trabajo mediante uno de los siguientes métodos:

- Active Directory
- Active Directory y token
- Azure Active Directory
- Citrix Gateway
- Okta
- SAML 2.0
- Google

Para obtener más información sobre los métodos compatibles para la autenticación de suscriptores en espacios de trabajo, consulte Espacios de trabajo seguros.

Active Directory (AD) requiere que tenga al menos dos Citrix Cloud Connectors instalados en el dominio de AD local. Para obtener información sobre Citrix Cloud Connector, consulte Citrix Cloud Connector.

AD y token es el proveedor de identidades predeterminado que se utiliza para autenticar a los suscriptores en los espacios de trabajo. Los suscriptores de espacios de trabajo generan tokens como un segundo factor de autenticación mediante cualquier aplicación que siga el estándar TOTP (contraseña temporal de un solo uso), como Citrix SSO. Para obtener información sobre cómo configurar la autenticación de dos factores basada en token, consulte Autenticación de dos factores.

Cambiar los proveedores de identidades

En **Configuración de Workspace**, se elige un proveedor de identidades como método de autenticación principal para Citrix Workspace. El proveedor de identidades elegido debe configurarse primero en **Administración de acceso e identidad**. Cambiar el proveedor de identidades en **Configuración de Workspace** no afecta a los proveedores de identidades que se hayan configurado en **Administración de acceso e identidad**.

Configurar proveedores de identidades en **Administración de acceso e identidad** no cambia el método de autenticación principal para iniciar sesión en Citrix Workspace. Para *cambiar* el método de autenticación principal para iniciar sesión en Citrix Workspace, deberá hacer lo siguiente:

1. Configurar el nuevo proveedor de identidades en **Administración de acceso e identidad**.

2. Cambiar el proveedor de identidades en **Configuración de Workspace**.

Puede configurar y cambiar el método de autenticación principal para Citrix Workspace sin interrumpir su entorno de producción. Si quiere probar el nuevo proveedor de identidades, puede crear una organización de Citrix Cloud de prueba o planificar el cambio del método de autenticación en **Configuración de Workspace** cuando los suscriptores no utilicen sus espacios de trabajo.

Single Sign-On (SSO) en aplicaciones web y SaaS

Citrix Workspace ofrece una experiencia fluida al proporcionar inicio de sesión único (SSO) a los recursos secundarios una vez que el suscriptor ha iniciado sesión en su espacio de trabajo. Junto con Citrix Gateway Service, Citrix Secure Private Access proporciona funcionalidad SSO a aplicaciones web y SaaS como parte integrada en Citrix Workspace.

Más allá de las capacidades de SSO, Citrix Secure Private Access le permite establecer directivas de seguridad mejoradas, configurar el acceso contextual y recopilar análisis. Para obtener más información sobre Citrix Secure Private Access, consulte Citrix Secure Private Access.

Single Sign-On (SSO) en DaaS

Junto con las aplicaciones web y SaaS, Active Directory (AD) y AD y token ya proporcionan SSO a escritorios y aplicaciones de DaaS una vez que los suscriptores hayan iniciado sesión en sus espacios de trabajo.

Si selecciona un proveedor de identidades diferente para la autenticación inicial del suscriptor en Citrix Workspace, también puede instalar y configurar Servicio de autenticación federada (FAS) de Citrix. Con FAS, los suscriptores introducen sus credenciales solo una vez para acceder a DaaS, al igual que lo hacen con las aplicaciones web y SaaS.

Por lo general, se adopta FAS si se utiliza uno de los siguientes proveedores de identidades para la autenticación de Workspace:

- Azure AD
- Okta
- SAML 2.0
- Citrix Gateway

> **Nota:**
>
> Según cómo configure Citrix Gateway, es posible que no necesite FAS para SSO en DaaS. Para obtener más información sobre cómo configurar Citrix Gateway, consulte Crear una directiva de IdP de OAuth en Citrix Gateway local.

Para obtener más información acerca de FAS, consulte Habilitar Single Sign-On para espacios de trabajo con el Servicio de autenticación federada de Citrix.

Más información

- Habilitar Single Sign-On para espacios de trabajo con Citrix Federated Authentication Service
- Reference Architecture: Federated Authentication Service
- Tech Insight: Federated Authentication Service

Configurar un dominio personalizado

November 21, 2023

La configuración de un dominio personalizado para su espacio de trabajo le permite utilizar un dominio de su elección para acceder a su almacén de Citrix Workspace. A continuación, puede utilizar este dominio, en lugar del dominio de cloud.com asignado, para acceder desde un explorador web y desde las aplicaciones de Citrix Workspace.

Un dominio personalizado no se puede compartir con otros clientes de Citrix Workspace. Cada dominio personalizado debe ser exclusivo de ese cliente. Asegúrese de elegir un dominio personalizado que no quiera asignar a otro cliente, a menos que piense eliminar el dominio personalizado más adelante.

Al inhabilitar la URL de Workspace en Citrix Cloud, no se inhabilita el acceso a Citrix Workspace a través del dominio personalizado. Para inhabilitar el acceso a Citrix Workspace cuando utilice un dominio personalizado, inhabilite también el dominio personalizado.

Casos compatibles

Casos	Compatible	No compatible
Proveedores de identidades	AD (+Token), Azure AD, Citrix Gateway, Okta y SAML	Google
Tipos de recursos	Aplicaciones y escritorios virtuales	Aplicaciones SaaS
Métodos de acceso	Explorador (excepto Internet Explorer), aplicación Citrix Workspace para Windows, Mac, Linux y iOS	-

Casos	Compatible	No compatible
Uso	Workspace	Cloud Connector y Consola de administrador de Cloud

¿En qué se diferencia de la URL de Workspace personalizada actual?

Si ya tiene habilitada una URL de Workspace personalizada para su cliente, aparecerá la siguiente vista.

Puede utilizar esta URL por el momento y continuar con los pasos descritos en este documento para incorporar una URL de Workspace personalizada diferente. Quedará obsoleta en el futuro.

Si quiere usar la misma URL, elimine la URL de Workspace personalizada anterior y todos los registros de DNS para continuar.

Requisitos previos

- Puede elegir un dominio recién registrado o uno que ya posea. El dominio debe tener formato de subdominio (su.empresa.com). Citrix no admite el uso únicamente de un dominio raíz (empresa.com).
- Citrix recomienda utilizar un dominio dedicado como dominio personalizado para el acceso a Citrix Workspace, de modo que pueda cambiarlo fácilmente si es necesario.
- Los dominios personalizados no pueden contener ninguna marca comercial de Citrix. Consulte la lista completa de marcas comerciales de Citrix aquí.
- El dominio que elija debe estar configurado en un DNS público. Citrix debe ser capaz de resolver todos los nombres y valores de los registros CNAME incluidos en la configuración de su dominio.

> **Nota:**
>
> No se admiten las configuraciones de DNS privadas.

- La longitud del nombre de dominio no debe superar los 64 caracteres.

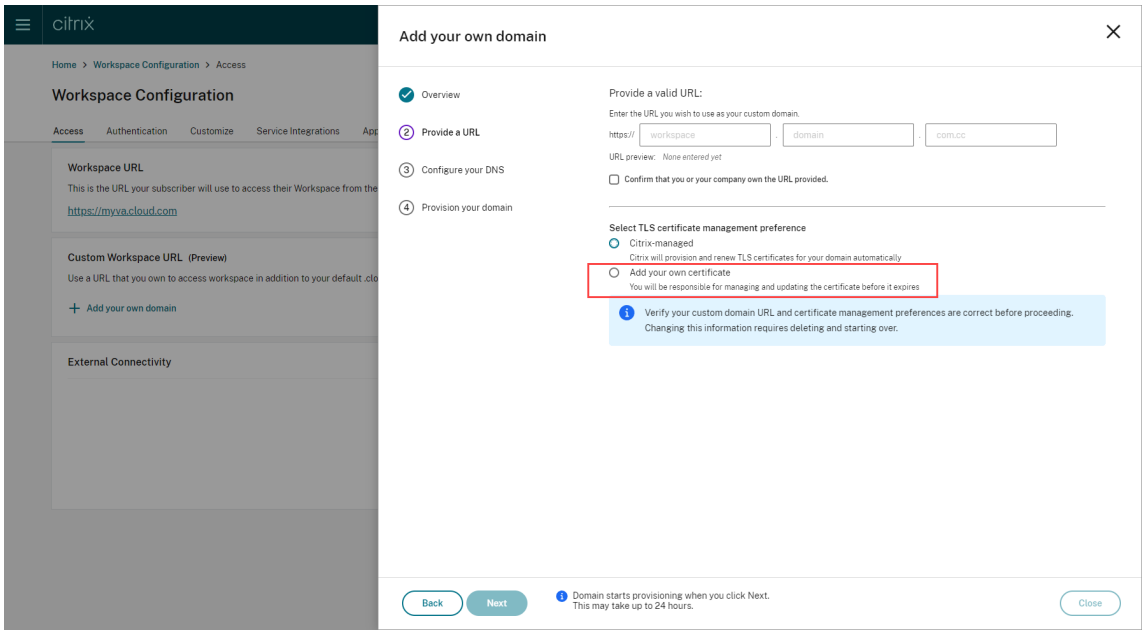
Configurar un dominio personalizado

Una vez establecido un dominio personalizado, no puede cambiar la URL ni el tipo de certificado. Solo puede eliminarlo. Asegúrese de que el dominio que elija no esté ya configurado en DNS. Quite todos los registros **CNAME** existentes antes de intentar configurar el dominio personalizado.

Si utiliza SAML para conectarse a su proveedor de identidades, debe seguir un paso adicional para completar la configuración de SAML. Para obtener más información, consulte SAML.

Agregar un dominio personalizado

1. Inicie sesión en Citrix Cloud, en https://citrix.cloud.com.
2. En el menú de Citrix Cloud, seleccione **Configuración de Workspace** y, luego, **Acceso**.
3. En la ficha **Acceso**, en **URL de espacio de trabajo personalizada**, seleccione **+ Agregue su propio dominio**.

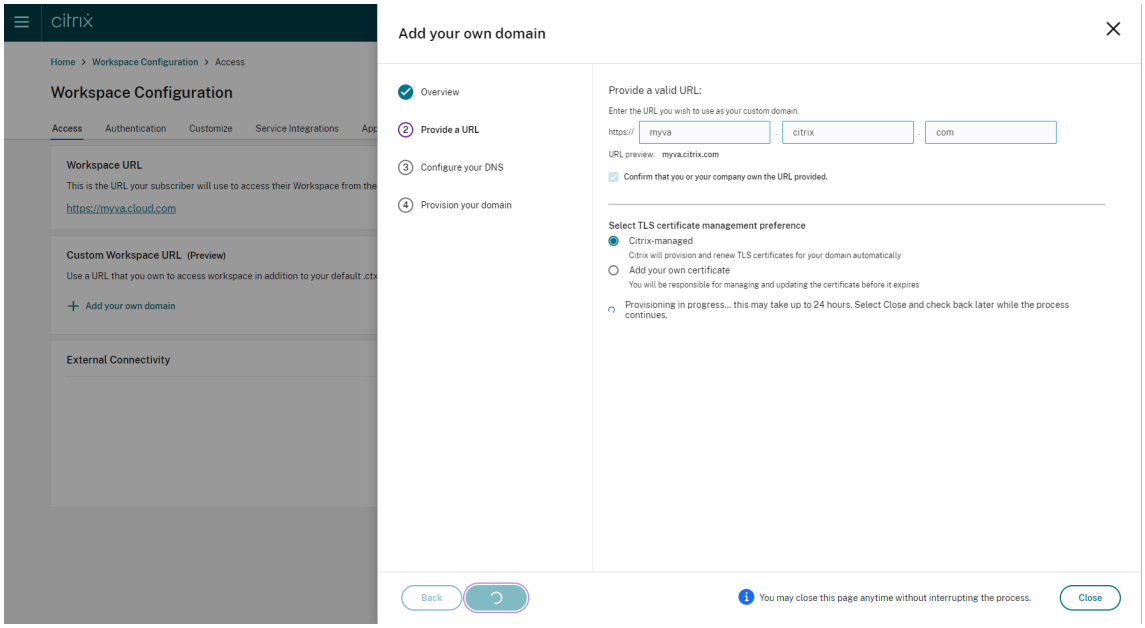


4. Lea la información que aparece en la página de **Vista general** y seleccione **Siguiente**.
5. Introduzca el dominio que haya elegido en la página **Proporcione una URL**. Confirme que es el propietario del dominio especificado; para ello, seleccione **Confirme que usted o su empresa son propietarios de la URL proporcionada** y elija la opción de administración de certificados TLS que prefiera. Citrix recomienda "Administrado", ya que las renovaciones de los certificados se gestionan por usted. Para obtener más información, consulte Proporcionar un certificado renovado. Haga clic en **Siguiente**.

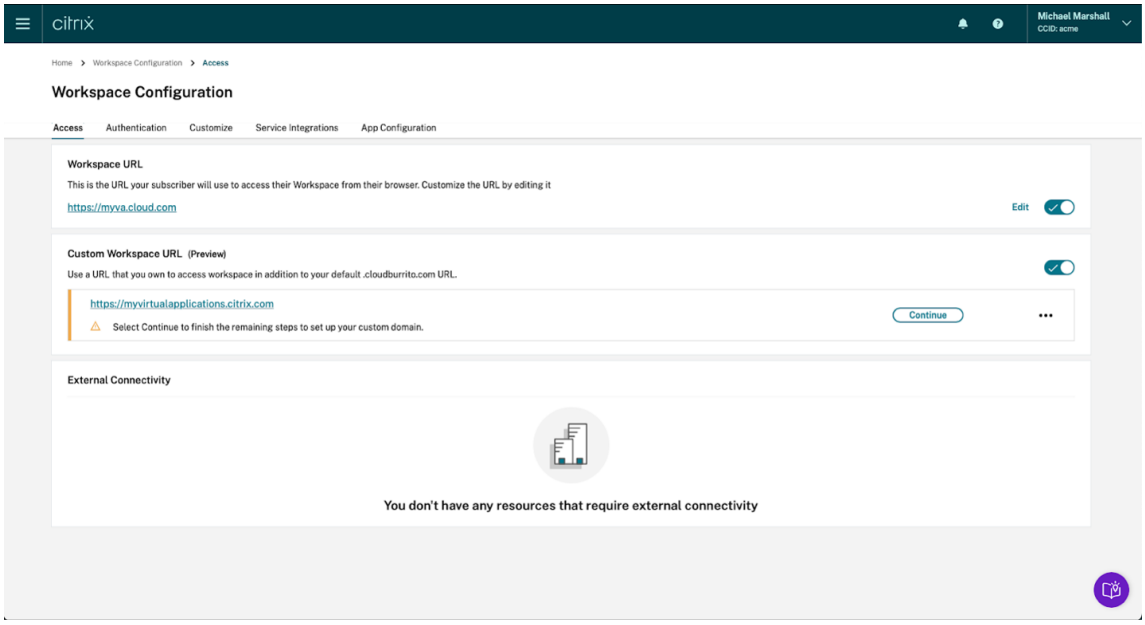
   Si aparece alguna advertencia en esta página, corrija el problema resaltado para continuar.

   Si ha decidido proporcionar su propio certificado, hay un paso adicional que debe completar en las instrucciones.

   El aprovisionamiento del dominio elegido lleva algún tiempo. Puede esperar con la página abierta o cerrarla mientras tiene lugar el aprovisionamiento.



6. Si tiene abierta la página **Proporcione una URL** mientras se completa el aprovisionamiento, la página **Configure su DNS** se abre automáticamente. Si ha cerrado la página, seleccione el botón **Continuar** para su dominio personalizado en la ficha **Acceso**.

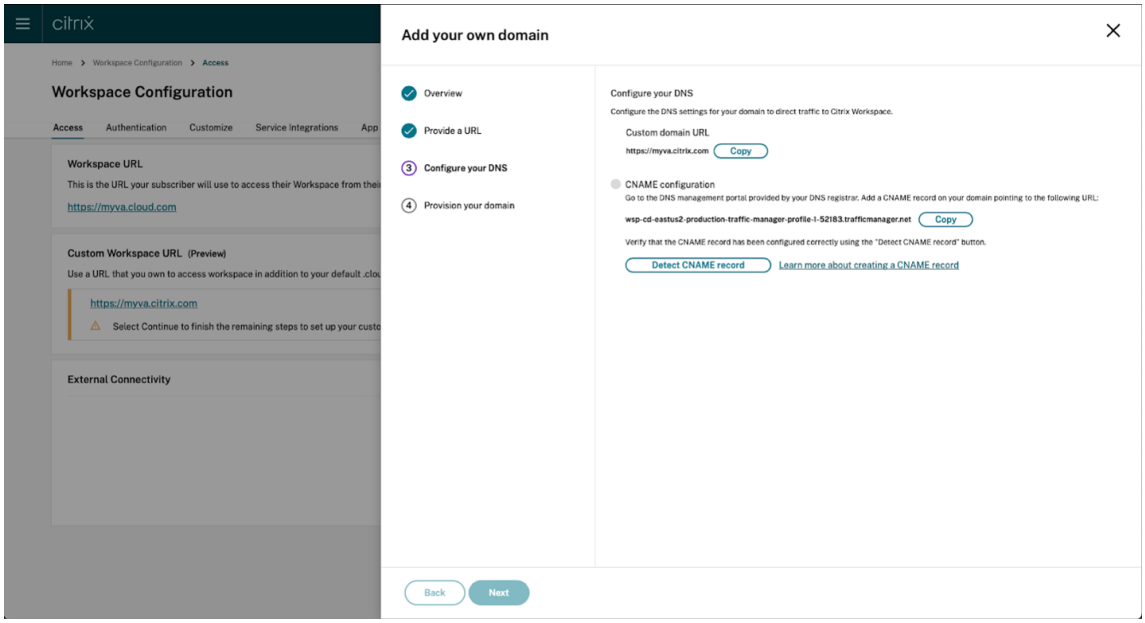


7. Siga este paso en el portal de administración proporcionado por su registrador de DNS. Agregue un registro **CNAME** para el dominio personalizado elegido que apunte al administrador de tráfico de Azure (Azure Traffic Manager) que se le ha asignado.

   Copie la dirección del administrador de tráfico de la página **Configure su DNS**. La dirección del ejemplo es la siguiente:

   wsp-cd-eastus2-production-traffic-manager-profile-1-52183.trafficmanager.net

Si tiene algún registro de "autorización de entidad de certificación"(CAA) configurado en su DNS, agregue uno que permita a *Let's Encrypt* generar certificados para su dominio. *Let's Encrypt* es la entidad de certificación (CA) que Citrix utiliza para generar un certificado para su dominio personalizado. El valor del registro CAA debe ser el siguiente: *0 issue "letsencrypt.org"*

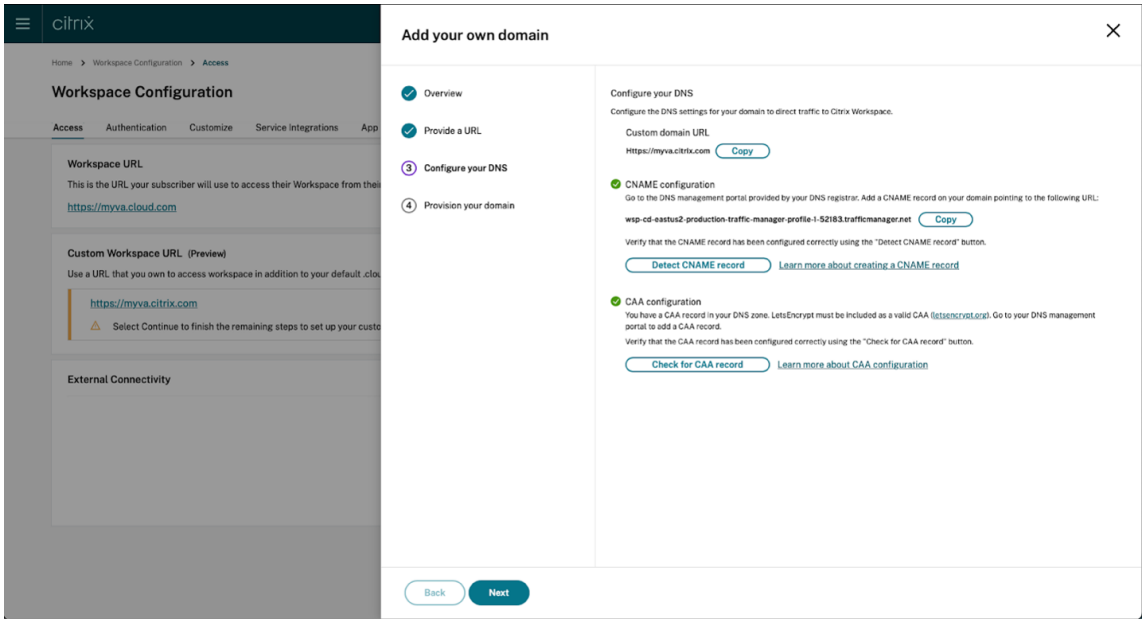


8. Una vez que haya configurado el registro CNAME con su proveedor de DNS, seleccione **Detectar registro CNAME** para comprobar que la configuración de DNS es correcta. Si el registro CNAME se ha configurado correctamente, aparecerá una marca verde junto a la sección **Configuración de CNAME**.

   Si aparece alguna advertencia en esta página, corrija el problema resaltado para continuar.

   Si tiene algún registro CAA configurado con su proveedor de DNS, aparecerá una **configuración de CAA** aparte. Seleccione **Detectar registro CAA** para comprobar que la configuración de DNS es correcta. Si la configuración del registro CAA es correcta, aparecerá una marca verde junto a la sección **Configuración de CAA**.

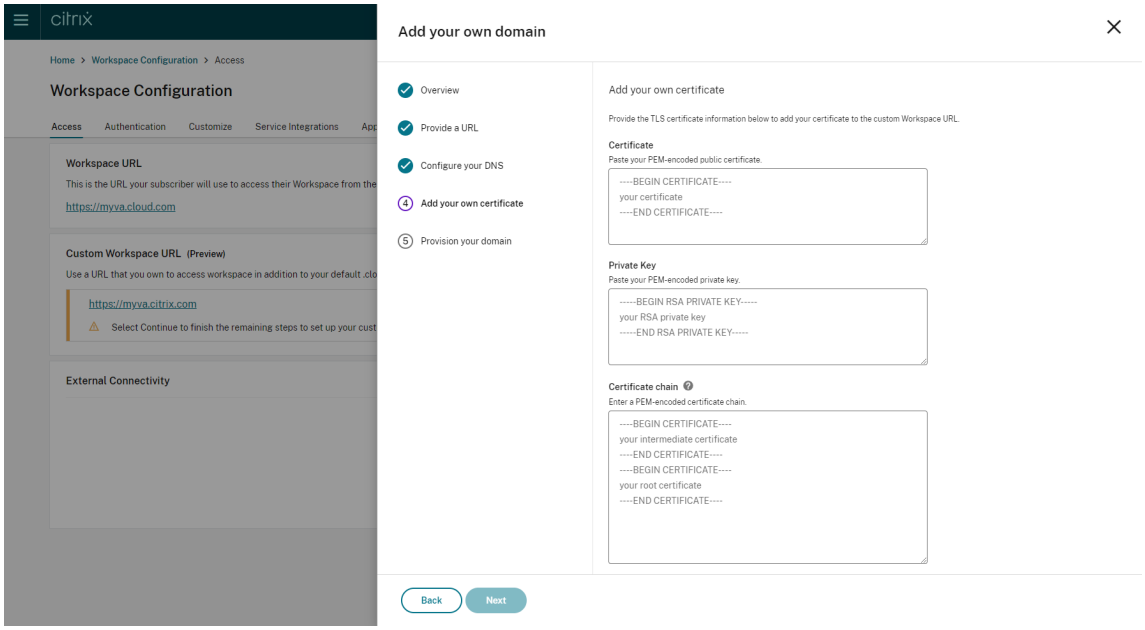
   Cuando se verifique la configuración de DNS, haga clic en **Siguiente**.



9. **Este es un paso opcional**. Si opta por agregar su propio certificado, complete la información requerida en la página **Agregar su propio certificado** .

   Si aparece alguna advertencia en esta página, corrija el problema resaltado para continuar. Asegúrese de que el certificado cumpla las siguientes condiciones.

   - Debe estar codificado en PEM.
   - Debe seguir siendo válido durante, al menos, los próximos 30 días.
   - Debe usarse exclusivamente para la URL de Workspace personalizada; no se aceptan certificados comodín.
   - El nombre común del certificado debe coincidir con el dominio personalizado.
   - Los SAN del certificado deben ser para el dominio personalizado; no se permite ningún SAN adicional.
   - La duración de la validez del certificado no debe superar los 10 años.



> **Nota:**
>
> Citrix recomienda usar un certificado que utilice una función hash criptográfica segura (SHA 256 o > superior). Usted es responsable de renovar el certificado. Si el certificado ha caducado o está a punto de caducar, consulte la sección Proporcionar un certificado renovado.

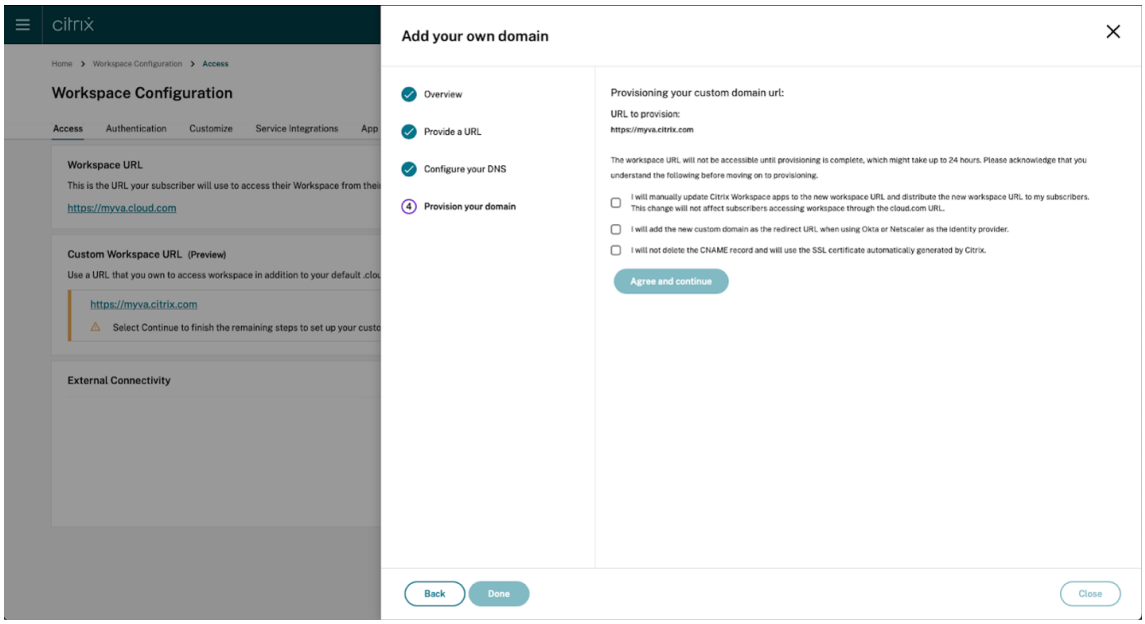
10. **Este es un paso opcional.** Si utiliza SAML como proveedor de identidades, proporcione la configuración correspondiente. Complete la información requerida en la **página Configurar para SAML**.

    Utilice los detalles siguientes al configurar la aplicación en su proveedor de identidades:

Propiedad	Valor
Audiencia	`https://saml.cloud.com`
Destinatario	`https://<your custom domain>/saml/acs`
Validador de URL de ACS	`https://<your custom domain>/saml/acs`
URL de consumidor de ACS	`https://<your custom domain>/saml/acs`
URL de cierre de sesión único	`https://<your custom domain>/saml/logout/callback`

11. Lea la información que aparece en la página **Aprovisione su dominio** y confirme las instrucciones proporcionadas. Cuando esté listo para continuar, seleccione **Aceptar y continuar**.

    Este último paso de aprovisionamiento puede tardar algún tiempo en completarse. Puede esperar con la página abierta mientras se completa la operación o cerrar la página.



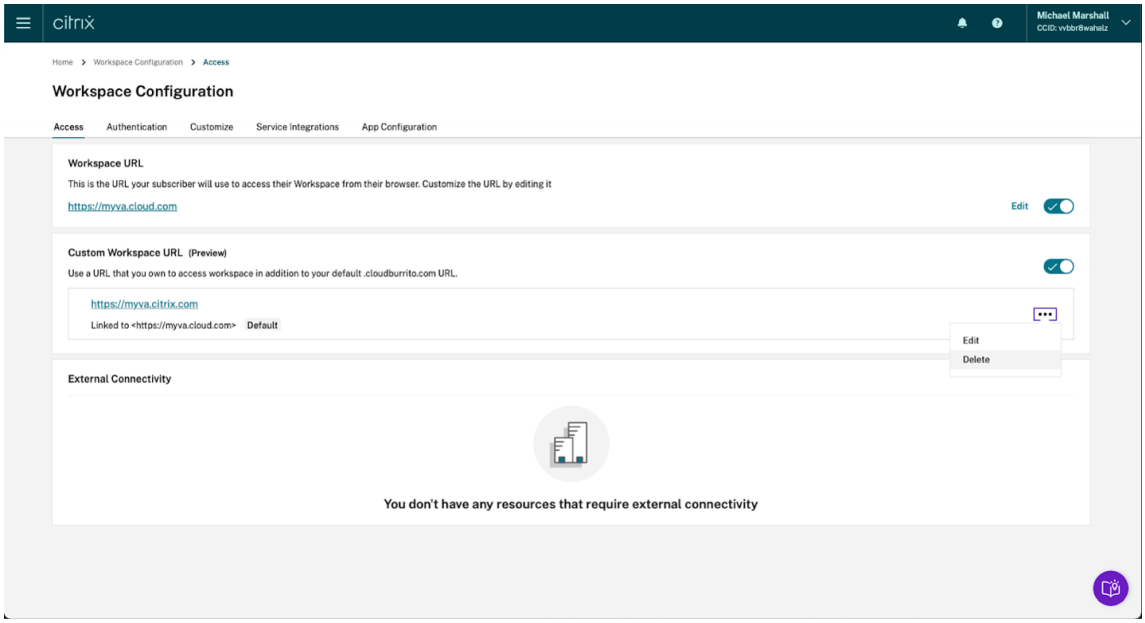
Eliminar un dominio personalizado

Al eliminar un dominio personalizado del cliente, se elimina la posibilidad de acceder a Citrix Workspace mediante un dominio personalizado. Tras eliminar el dominio personalizado, solo podrá acceder a Citrix Workspace utilizando la dirección cloud.com.

Cuando elimine un dominio personalizado, asegúrese de eliminar el registro CNAME de su proveedor de DNS.

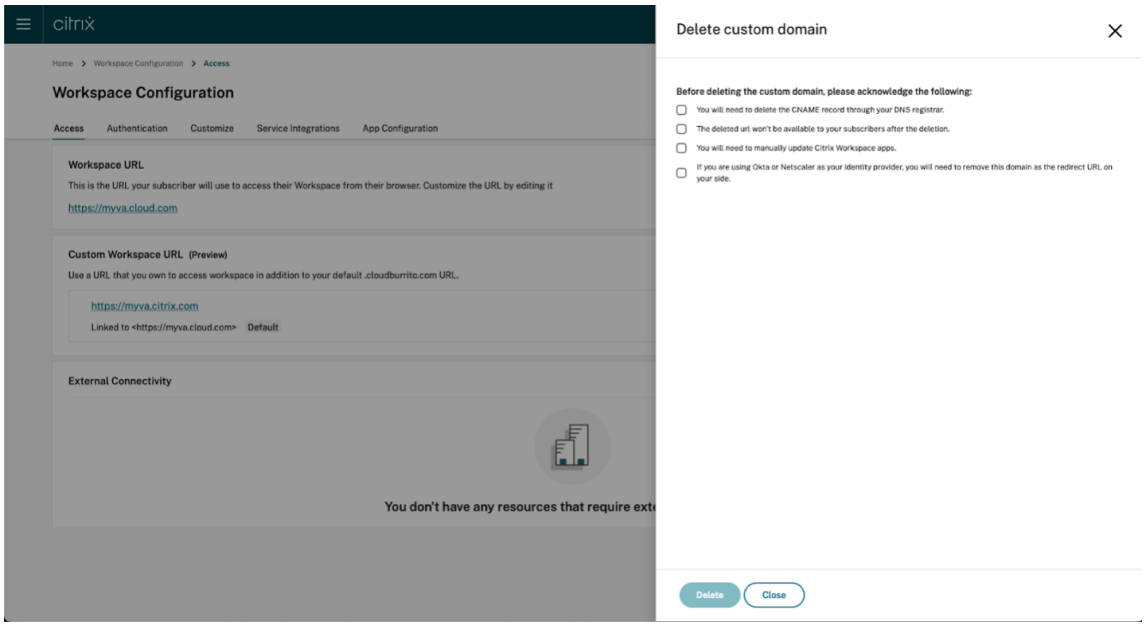
Para eliminar un dominio personalizado:

1. Inicie sesión en Citrix Cloud, en https://citrix.cloud.com.
2. En el menú de Citrix Cloud, seleccione **Configuración de Workspace > Acceso**.
3. Expanda el menú contextual **(...)** del dominio personalizado en la ficha **Acceso** y seleccione **Eliminar**.



4. Lea la información que aparece en la página **Eliminar dominio personalizado** y confirme las instrucciones proporcionadas. Cuando esté listo para continuar, seleccione **Eliminar**.

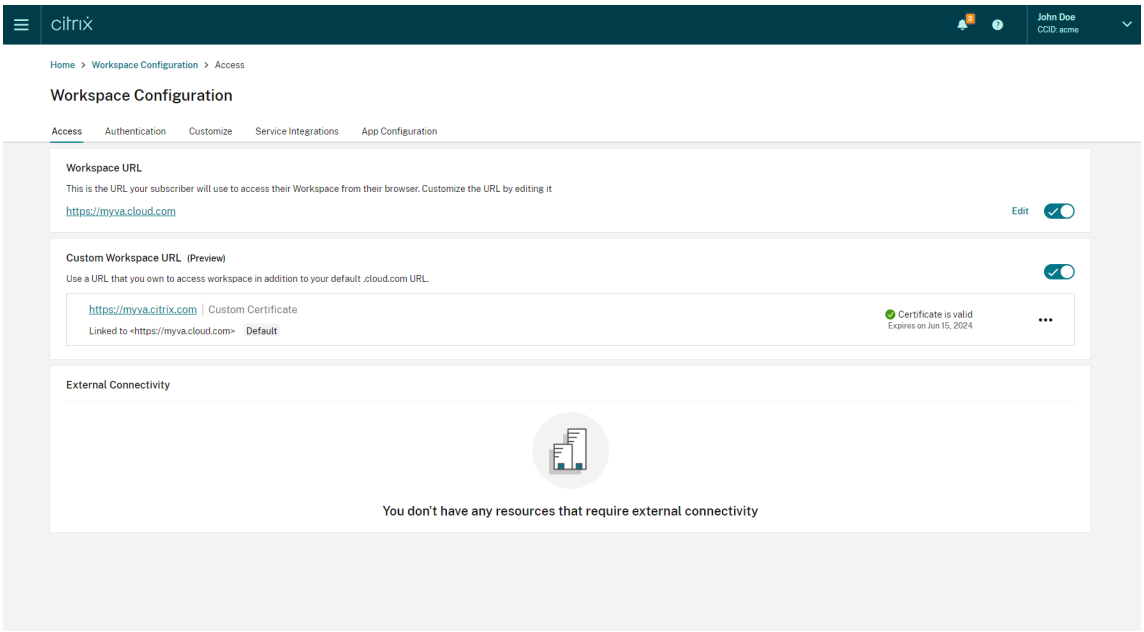
   La eliminación de un dominio personalizado tarda algún tiempo en completarse. Puede esperar con la página abierta mientras se completa la operación o cerrar la página.



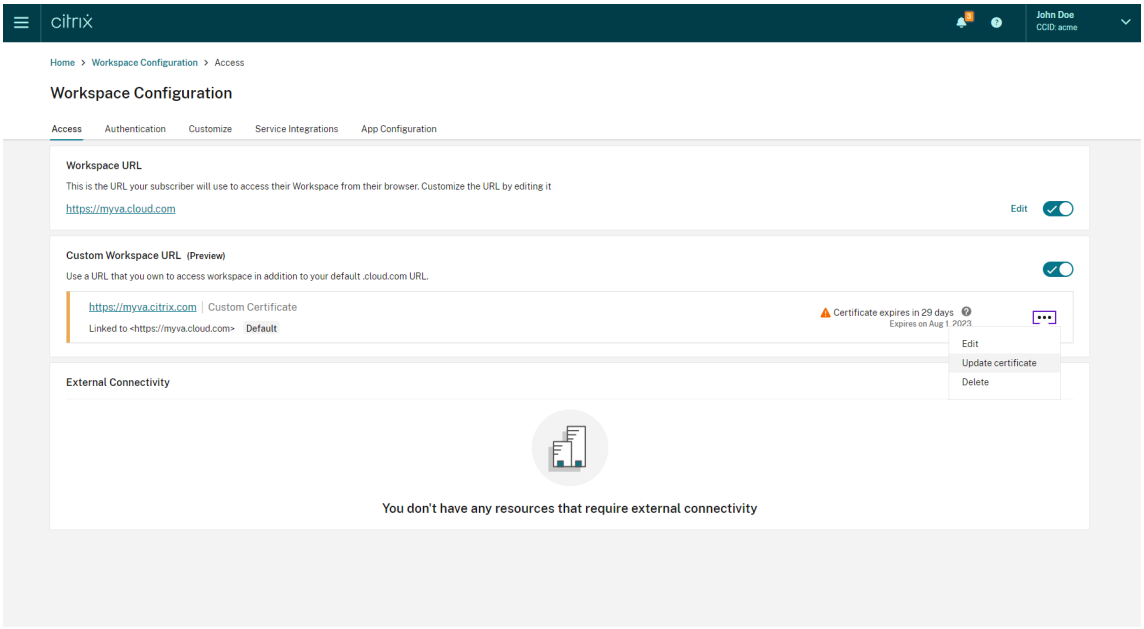
Proporcionar un certificado renovado

1. Inicie sesión en Citrix Cloud.
2. En el menú de Citrix Cloud, seleccione **Configuración de Workspace** > **Acceso**.

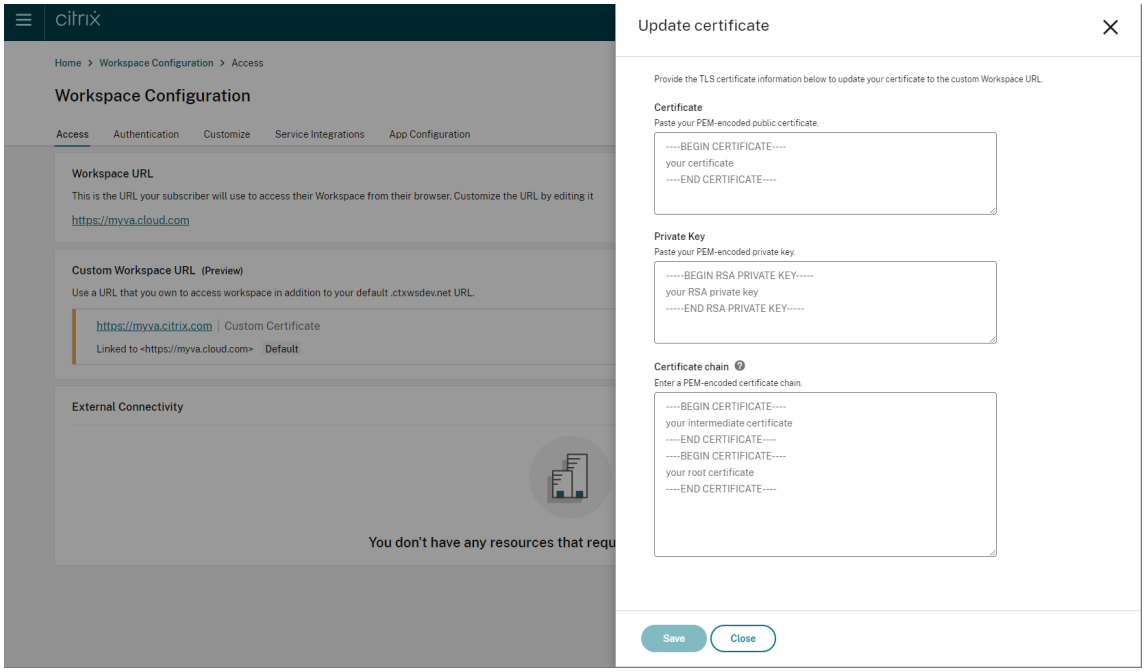
3. La fecha de caducidad del certificado se mostrará junto al dominio personalizado al que está asignado.



Cuando su certificado caduque en un plazo de 30 días o menos, su dominio personalizado mostrará una advertencia.



4. Expanda el menú contextual **(...)** del dominio personalizado en la ficha **Acceso**. Seleccione **Actualizar certificado**.



5. Introduzca la información requerida en la **página Actualizar certificado** y haga clic en **Guardar**.

Si aparece alguna advertencia en esta página, corrija el problema resaltado para continuar.

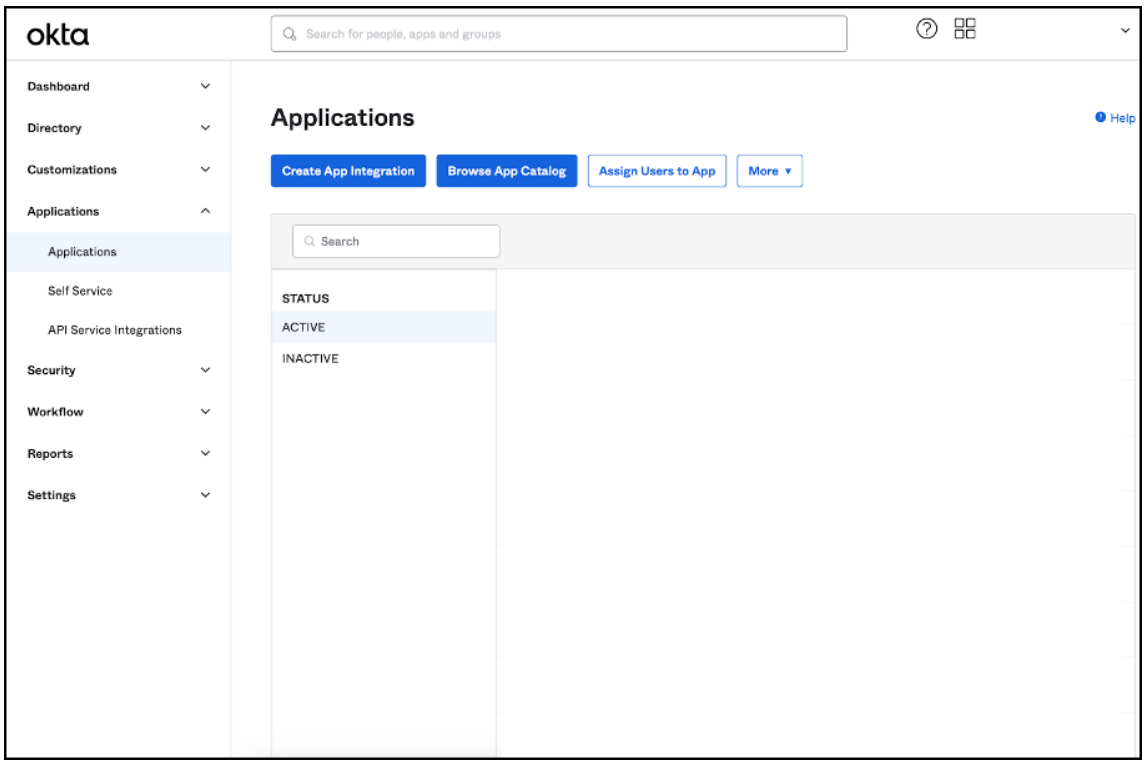
El certificado debe cumplir los mismos requisitos que cuando se creó el dominio personalizado y pueden consultarse aquí Agregar un dominio personalizado.

Configurar un proveedor de identidades

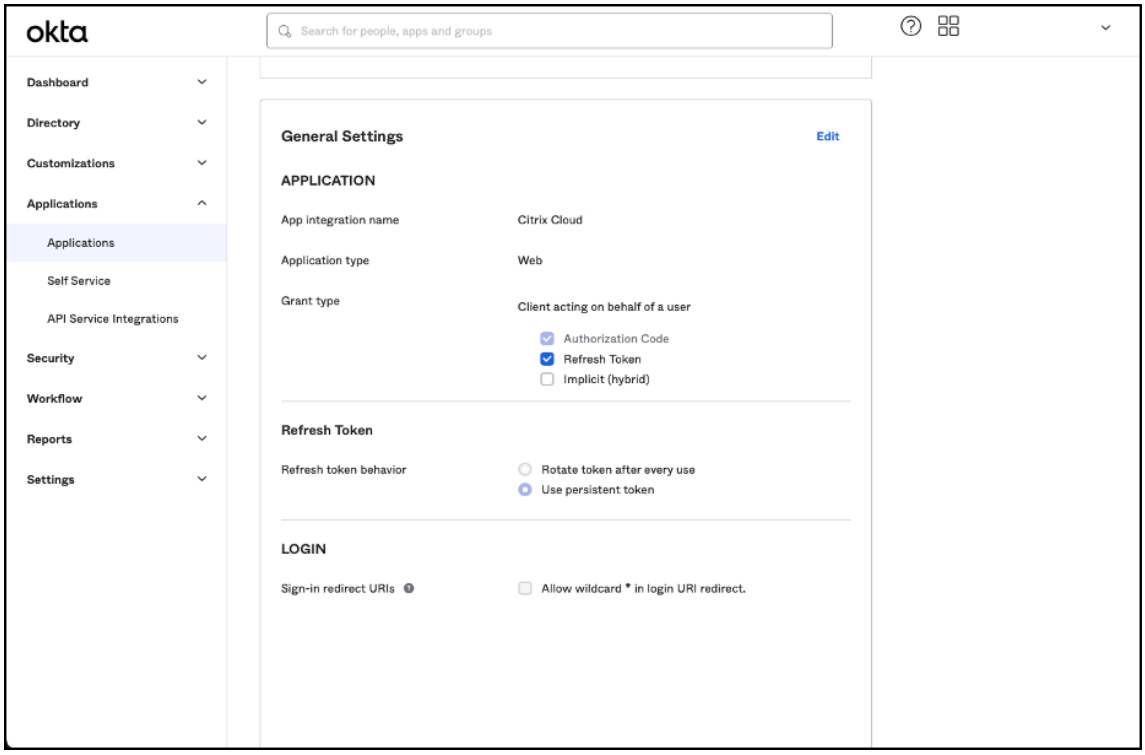
Configurar Okta

Siga estos pasos si utiliza Okta como proveedor de identidades para acceder a Citrix Workspace.

1. Inicie sesión en el portal de administrador de su instancia de Okta. Esta instancia contiene la aplicación que utiliza Citrix Cloud.
2. Expanda **Applications** y, a continuación, seleccione **Applications** en el menú.



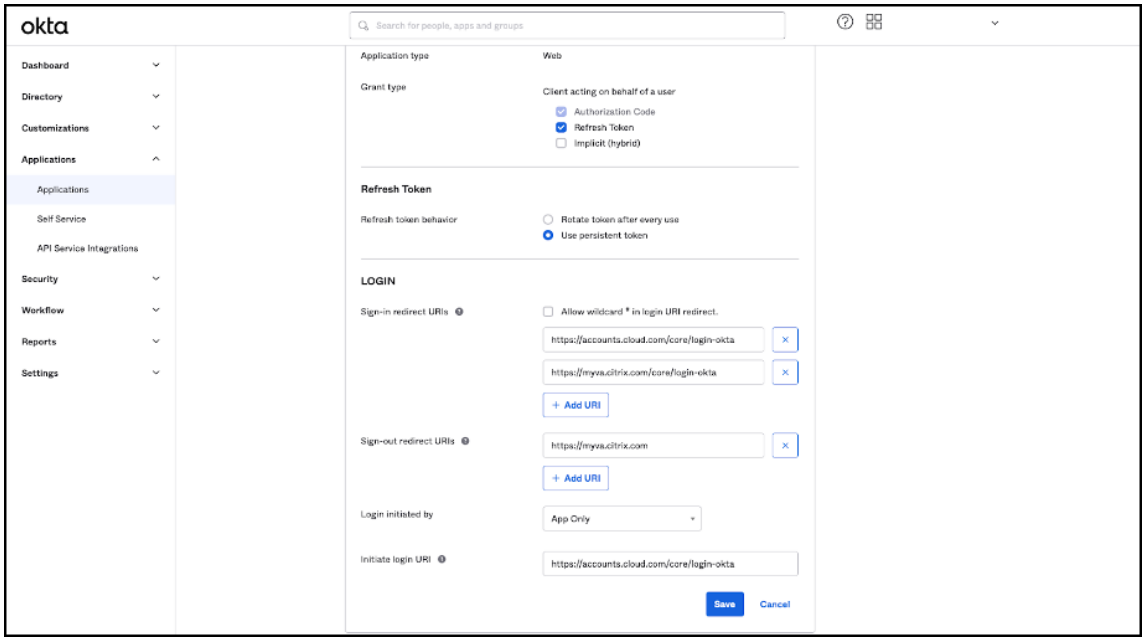
3. Abra la aplicación vinculada a Citrix Cloud.
4. Seleccione **Edit** en la sección **General Settings**.



5. En la sección **LOGIN** de **General settings**, agregue un nuevo valor para **Sign-in redirect URIs**.

Agregue el nuevo valor a los valores existentes; no los sustituya. El nuevo valor debe tener el siguiente formato: https://your.company.com/core/login-okta

6. En la misma sección, agregue un nuevo valor para **Sign-out redirect URIs**. Agregue el nuevo valor a los valores existentes; no los sustituya. El nuevo valor debe tener el siguiente formato: https://your.company.com



7. Haga clic en **Save** para guardar la nueva configuración.

Configuración de directivas y perfiles de OAuth

> **Importante**
>
> La directiva y el perfil de OAuth existentes que vinculan Citrix Cloud al par HA de autenticación adaptable o Citrix Gateway solo deben actualizarse si se pierden las credenciales de OAuth. Si se modifica esta directiva, se corre el riesgo de romper el enlace entre Citrix Cloud y los espacios de trabajo, lo que afectará a su capacidad para iniciar sesión en tales espacios de trabajo.

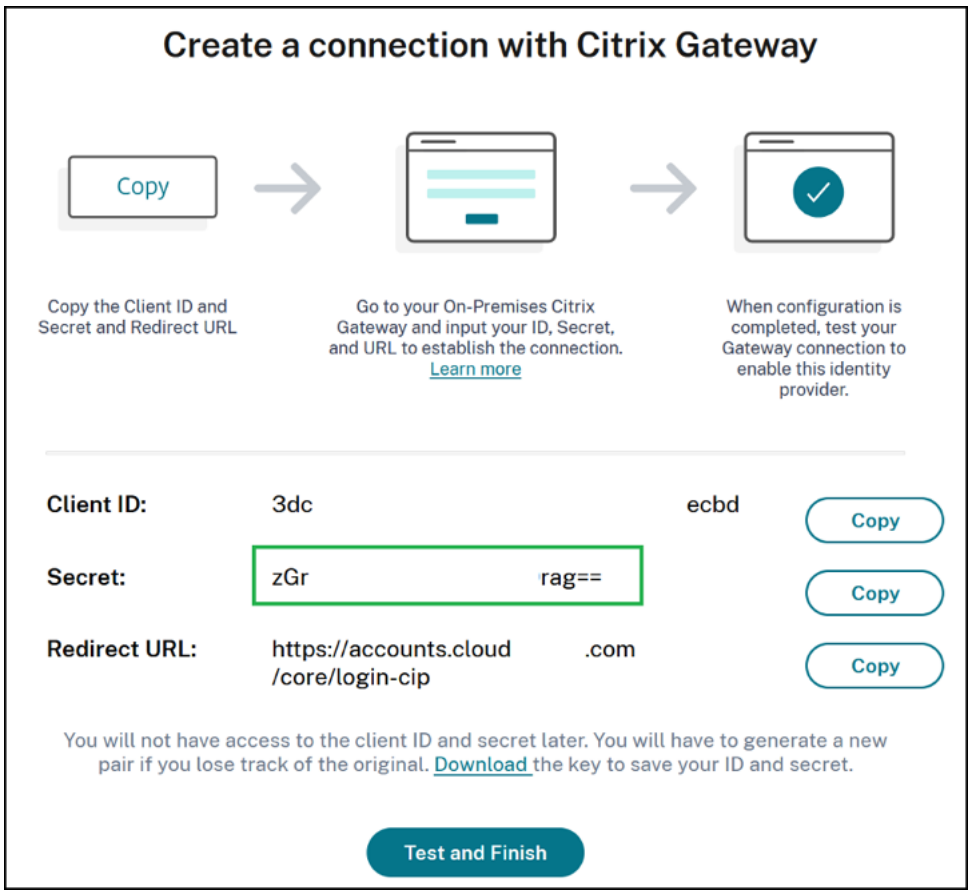
Configurar Citrix Gateway

El administrador de Citrix Cloud tiene acceso al secreto del cliente no cifrado. Citrix Cloud proporciona estas credenciales durante el proceso de enlace de Citrix Gateway en **Administración de acceso e identidad > Autenticación**. El administrador de Citrix crea manualmente el perfil y la directiva de OAuth en Citrix Gateway durante el proceso de conexión.

Se necesitan el ID de cliente y el secreto de cliente sin cifrar que se proporcionaron durante el proceso de conexión a Citrix Gateway. Citrix Cloud proporciona estas credenciales, que se habrán guardado

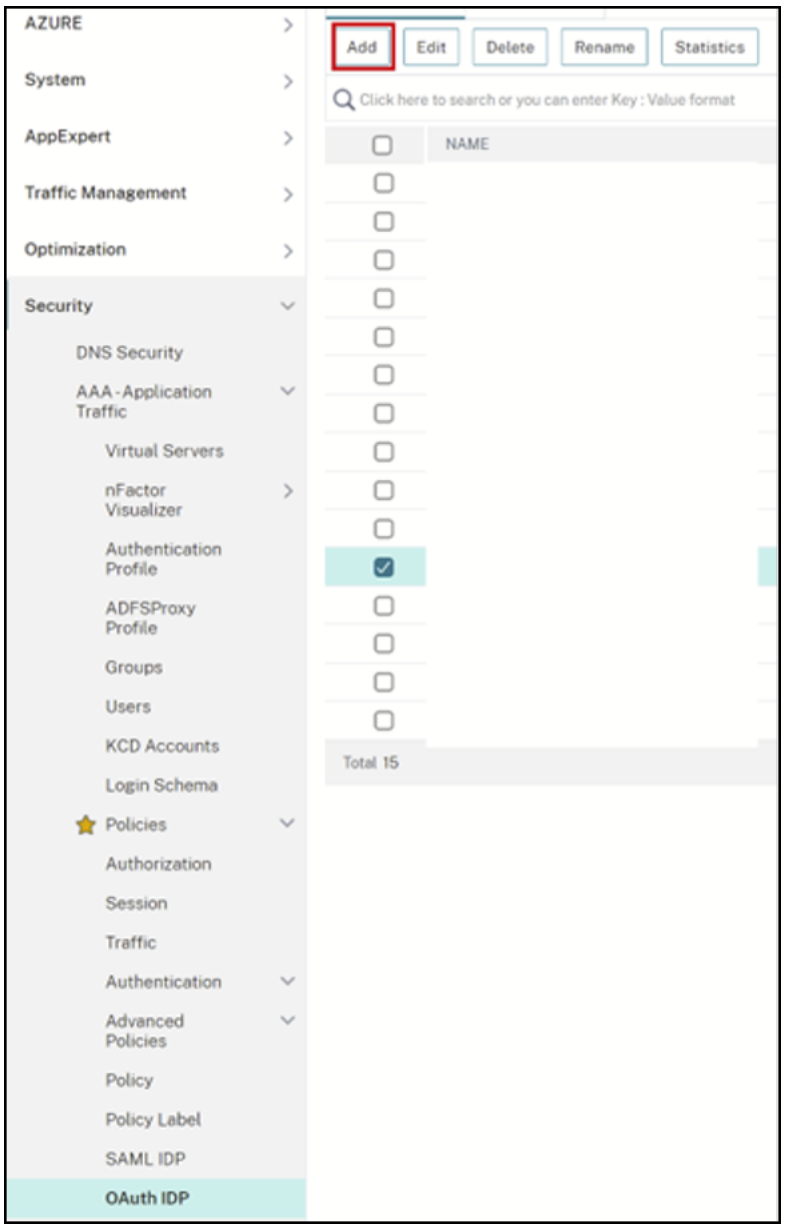
de forma segura.
El secreto sin cifrar es necesario cuando se utiliza la interfaz de Citrix ADC o la interfaz de línea de comandos (CLI) a fin de crear una directiva y un perfil de OAuth.

Este es un ejemplo de la interfaz de usuario en la que se proporcionan el ID y el secreto del cliente al administrador de Citrix. Si el administrador de Citrix no guarda las credenciales durante el proceso de conexión, no podrá obtener una copia del secreto sin cifrar una vez que se haya conectado a Citrix Gateway.

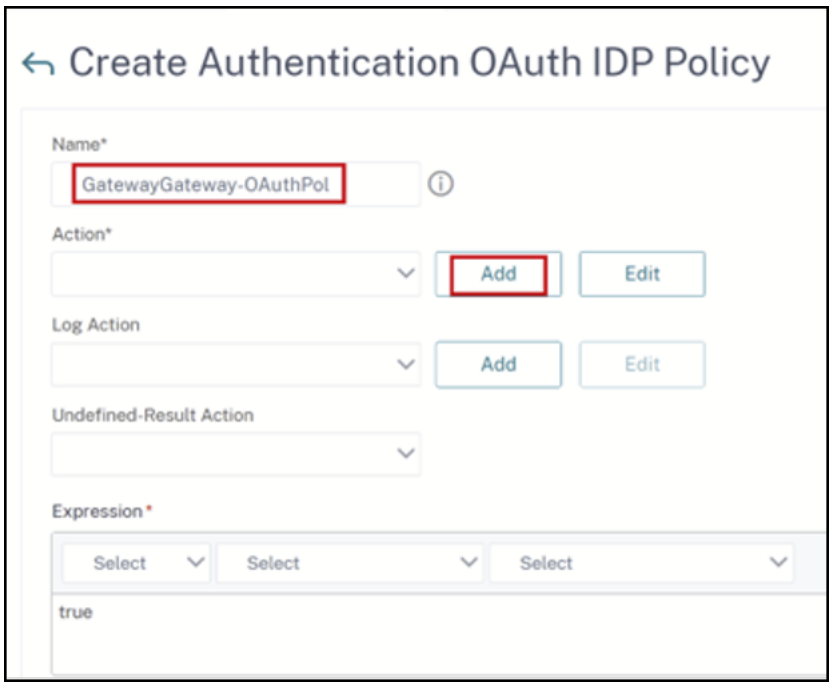


Uso de Citrix Cloud Siga estos pasos para agregar un perfil y una directiva de OAuth adicionales a través de la interfaz de Citrix Gateway:

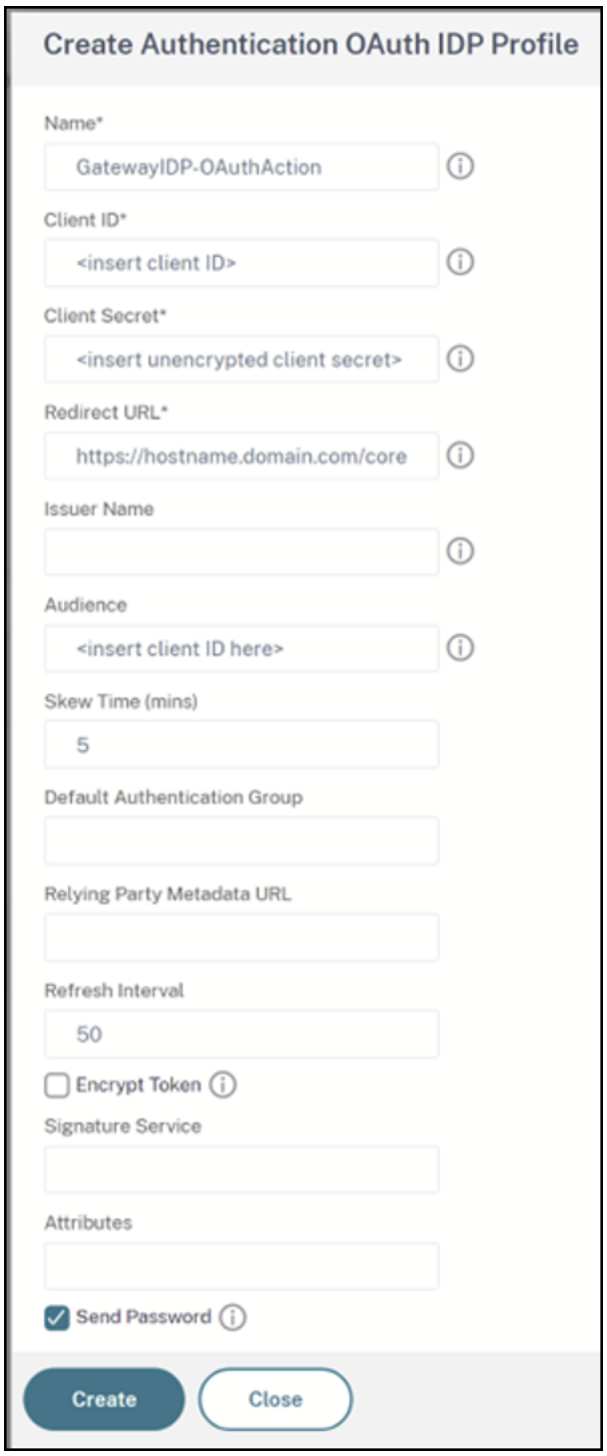
1. En el menú, seleccione **Security > AAA - Application Traffic > OAuth IDP**. Seleccione la directiva de OAuth existente y haga clic en **Add**.



2. Cuando se le indique, modifique el nombre de la nueva directiva de OAuth, de manera que sea distinto del nombre de la directiva seleccionada en el paso anterior. Citrix sugiere agregar la cadena *custom-url* al nombre.



3. En la GUI de Citrix Gateway, cree su perfil de OAuth.
4. En el mismo menú de la GUI, junto a **Action**, haga clic en **Add**.



5. En la GUI de Citrix Gateway, enlace la nueva directiva de OAuth a su servidor virtual de autenticación, autorización y auditoría existente.
6. Vaya a **Security > Virtual Servers > Edit**.

Uso de la interfaz de línea de comandos

> **Importante**
>
> Si no tiene una copia de las credenciales de OAuth guardadas de forma segura, debe desconectar y volver a conectar su instancia de Citrix Gateway y actualizar el perfil de OAuth existente con las nuevas credenciales de OAuth proporcionadas por Administración de acceso e identidad en Citrix Cloud. Actualice únicamente su perfil de OAuth con credenciales nuevas si no puede recuperar las credenciales antiguas. No se recomienda hacer esto, a menos que no tenga otra opción.

1. Utilice una herramienta SSH, como PuTTY, para conectarse a su instancia de Citrix Gateway.
2. Cree OAuthProfile y OAuthPolicy. Agregue la autenticación OAuthIDPProfile.

   ```
   "CustomDomain-OAuthProfile"-clientID "<clientID>"-clientSecret "<unencrypted client secret>"-redirectURL "https://hostname.domain.com/core/login-cip"-audience "<clientID>"-sendPassword ON

   add authentication OAuthIDPPolicy "CustomDomain-OAuthPol"-rule true -action "CustomDomain-OAuthProfile"
   ```

3. Enlace la directiva de OAuth al servidor virtual de autenticación, autorización y auditoría correcto con una prioridad inferior a la de la directiva existente. Esta instancia asume que la directiva existente tiene una prioridad 10, por lo que se utiliza 20 para la nueva directiva. Enlace el servidor virtual de autenticación.

   ```
   "CitrixGatewayAAAvServer"-policy "CustomDomain-OAuthPol"-priority 20
   ```

Configurar la autenticación adaptable

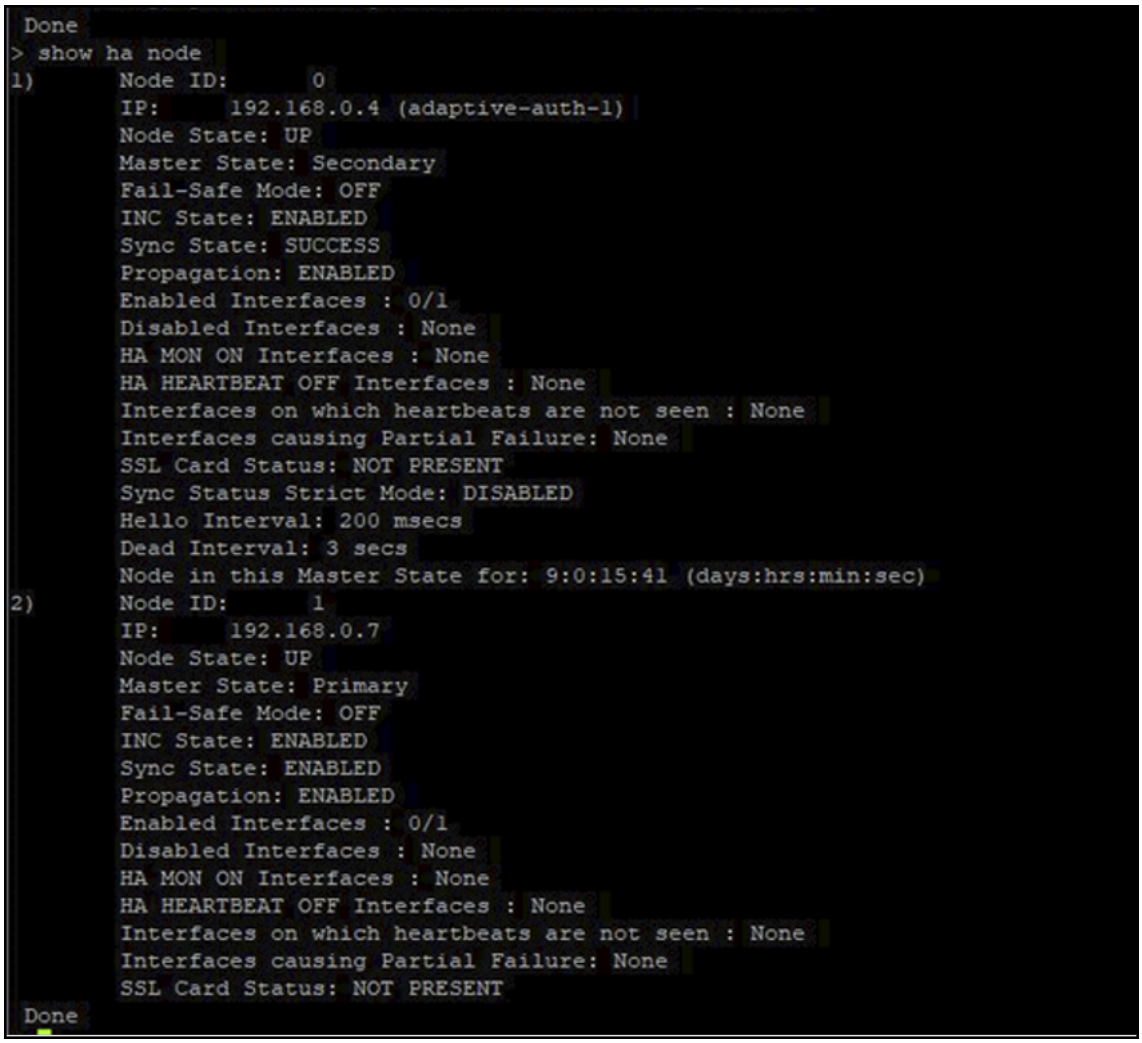
> **Importante**
>
> El secreto cifrado y los parámetros de cifrado del perfil de OAuth son diferentes en las puertas de enlace de alta disponibilidad (HA) principales y secundarias de la autenticación adaptable. Asegúrese de obtener el secreto cifrado de la puerta de enlace HA principal y también de ejecutar estos comandos en dicha puerta de enlace.

El administrador de Citrix Cloud no tiene acceso al secreto del cliente no cifrado. El servicio de autenticación adaptable de Citrix crea la directiva y el perfil de OAuth durante la fase de aprovisionamiento. Para crear perfiles de OAuth, es necesario utilizar el secreto cifrado y los comandos de CLI obtenidos

del archivo ns.conf. Esto no se puede hacer a través de la interfaz de usuario de Citrix ADC. Enlace la nueva directiva de OAuth con URL personalizada a su servidor virtual de autenticación, autorización y auditoría utilizando un número de prioridad más alto al de la directiva que está vinculada actualmente a dicho servidor. Tenga en cuenta que los números de prioridad más bajos se evalúan primero. Asigne a la directiva existente una prioridad 10 y a la nueva directiva una prioridad 20 para garantizar que se evalúen en el orden correcto.

1. Conéctese a su nodo principal de autenticación adaptable con una herramienta SSH como PuTTY.

   ```
   show ha node
   ```

2. Localice la línea dentro de la configuración en ejecución correspondiente a la puerta de enlace HA principal que contiene su perfil de OAuth.

   ```
   sh runn | grep oauth
   ```

3. Copie la salida de la CLI de Citrix ADC, incluidos todos los parámetros de cifrado.

4. Modifique la línea que copió en el paso anterior y utilícela para crear un nuevo comando de CLI que le permita crear un perfil de OAuth utilizando la versión cifrada del ID de cliente. Para esto, es necesario incluir todos los parámetros de cifrado.

   - Actualice el nombre del perfil de OAuth a *CustomDomain-OAuthProfile*
   - Actualice la URL de redirección a https://hostname.domain.com/core/login-cip

   Este es un ejemplo después de realizar ambas actualizaciones.

   ```
   add authentication OAuthIDPProfile "CustomDomain-OAuthProfile"-
   clientID b1656835-20d1-4f6b-addd-1a531fd253f6 -clientSecret <long
    encrypted client Secret> -encrypted -encryptmethod ENCMTHD_3
   -kek -suffix 2023_04_19_09_12_25 -redirectURL "https://hostname
   .domain.com/core/login-cip"-audience b1656835-20d1-4f6b-addd-1
   a531fd253f6 -sendPassword ON

   add authentication OAuthIDPPolicy "CustomDomain-OAuthPol"-rule
   true -action "CustomDomain-OAuthProfile"
   ```

5. Enlace la directiva de OAuth al servidor virtual de autenticación, autorización y auditoría correcto con una prioridad inferior a la de la directiva existente. El nombre del servidor virtual de autenticación, autorización y auditoría para todas las implementaciones de autenticación adaptable es *auth_vs*. Esta instancia asume que la directiva existente tiene una prioridad 10, por lo que se utiliza 20 para la nueva directiva.

   ```
   bind authentication vserver "auth_vs"-policy "CustomDomain-
   OAuthPol"-priority 20
   ```

Limitaciones conocidas

Algunas limitaciones conocidas de la solución de dominio personalizado son las siguientes:

Plataforma Workspace

- Actualmente, solo admite un dominio personalizado por cliente.
- Un dominio personalizado solo se puede vincular a la URL predeterminada de Workspace. Las demás URL de Workspace agregadas mediante la función de URL múltiple no pueden tener un dominio personalizado. La función URL múltiple se encuentra actualmente en Private Tech Preview y podría no estar disponible para todos los clientes.

- Si tiene un dominio personalizado configurado en la solución anterior y utiliza SAML o Azure AD para autenticar el acceso a Citrix Workspace, **no podrá** configurar un dominio personalizado en la nueva solución sin **eliminar primero el dominio personalizado existente**.

SAML

La compatibilidad con SAML se limita a uno de los siguientes casos de uso:

- SAML se puede usar exclusivamente con los dominios de cloud.com. En este caso, el uso de SAML cubriría el acceso a Citrix Workspace y el acceso de administrador a Citrix Cloud.
- SAML se puede usar exclusivamente con un dominio personalizado.

Aplicación Citrix Workspace para Windows

- Esta función no se admite en las versiones 2305 y 2307 de la aplicación Citrix Workspace para Windows. Actualice a la última versión compatible.

Espacios de trabajo seguros

October 12, 2023

Como administrador, puede elegir que sus suscriptores se autentiquen en sus espacios de trabajo mediante uno de los siguientes métodos de autenticación:

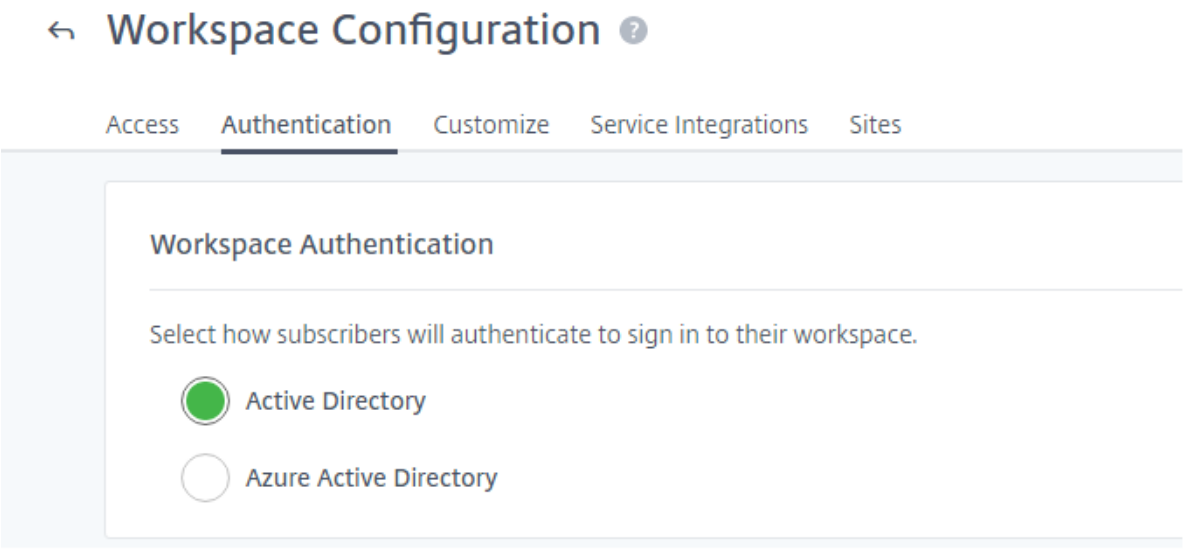
- Active Directory (AD)
- Active Directory y token
- Azure Active Directory (AAD)
- Citrix Gateway
- Google
- Okta
- SAML 2.0

Estas opciones de autenticación están disponibles para cualquier servicio de Citrix Cloud. Para obtener más información, consulte Tech Brief: Workspace Identity.

Citrix Workspace también permite usar el Servicio de autenticación federada (FAS) de Citrix para ofrecer Single Sign-On (SSO) a Citrix DaaS. SSO con FAS elimina la necesidad de que los suscriptores se autentiquen en DaaS después de haber iniciado sesión en sus espacios de trabajo mediante un método de autenticación federada. Para obtener más información, consulte Habilitar Single Sign-On para espacios de trabajo con el Servicio de autenticación federada de Citrix.

Elegir o cambiar los métodos de autenticación

Después de configurar los proveedores de identidades, puede elegir o cambiar la forma en que los suscriptores se autentican en su espacio de trabajo en **Configuración de Workspace > Autenticación > Autenticación de Workspace**.



> **Importante:**
>
> El cambio de un modo de autenticación a otro puede tomar hasta cinco minutos y provoca una interrupción de servicio para los suscriptores durante ese tiempo. Citrix recomienda hacer los cambios durante los períodos de bajo uso. Si tiene suscriptores que han iniciado sesión en Citrix Workspace mediante un explorador web o una aplicación de Citrix Workspace, recomiéndeles que cierren el explorador o salgan de la aplicación. Después de esperar aproximadamente cinco minutos, pueden volver a iniciar sesión con el nuevo método de autenticación.

Active Directory (AD)

De forma predeterminada, Citrix Cloud usa Active Directory (AD) para administrar la autenticación de los suscriptores en sus espacios de trabajo.

Para usar AD, debe tener al menos dos Citrix Cloud Connectors instalados en el dominio de AD local. Para obtener más información sobre la instalación de Cloud Connector, consulte Instalar Cloud Connector.

Active Directory (AD) y token

En pro de una mayor seguridad, Citrix Workspace admite el uso de un token temporal como segundo factor de autenticación para el inicio de sesión con AD.

En cada inicio de sesión, Workspace pide a los suscriptores que introduzcan un token de una aplicación de autenticación en el dispositivo inscrito. Antes de iniciar sesión, los suscriptores deben inscribir su dispositivo con una aplicación de autenticación que siga el estándar de "contraseña temporal de un solo uso"(TOTP), como Citrix SSO. Por ahora, los suscriptores solo pueden inscribir dispositivos de uno en uno.

Para obtener más información, consulte Tech Insight: Authentication - TOTP y Tech Insight: Authentication - Push.

Requisitos de AD y token

La autenticación con Active Directory y token necesita lo siguiente:

- Una conexión entre Active Directory y Citrix Cloud con al menos dos Cloud Connectors instalados en su entorno local. Para ver los requisitos y las instrucciones, consulte Conectar Active Directory con Citrix Cloud.
- Autenticación con **Active Directory y token** habilitada en la página **Administración de acceso e identidad**. Para obtener información, consulte Para habilitar la autenticación con Active Directory y token.
- Acceso de los suscriptores al correo electrónico para inscribir dispositivos.
- Un dispositivo en el que descargar la aplicación de autenticación.

Inscripción por primera vez

Los suscriptores pueden inscribir sus dispositivos siguiendo el proceso de inscripción descrito en Registrar dispositivos para la autenticación de dos factores.

Durante el primer inicio de sesión en Workspace, los suscriptores siguen las instrucciones para descargar la aplicación Citrix SSO, que genera cada 30 segundos una contraseña única de un solo uso en un dispositivo inscrito.

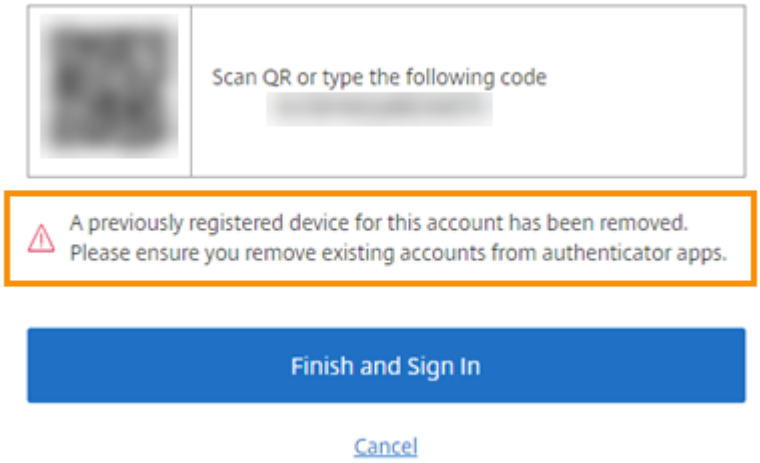
> **Importante:**
>
> Durante el proceso de inscripción del dispositivo, los suscriptores reciben un correo electrónico con un código de verificación temporal. Este código temporal sirve solo para inscribir el dispositivo del suscriptor. No se admite el uso de este código temporal como token para iniciar sesión en Citrix Workspace con autenticación de dos factores. Solo los códigos de verificación generados a partir de una aplicación de autenticación en un dispositivo inscrito son tokens compatibles

> con la autenticación de dos factores.

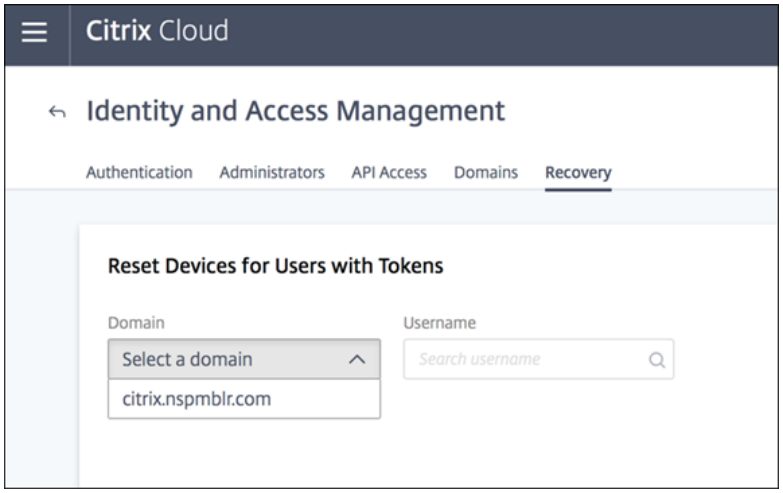
Reinscribir un dispositivo

Si un suscriptor ya no tiene su dispositivo inscrito o necesita volver a inscribirlo (por ejemplo, después de borrar el contenido del dispositivo), Workspace ofrece las siguientes opciones:

- Los suscriptores pueden volver a inscribir sus dispositivos mediante el mismo proceso de inscripción descrito en Registrar dispositivos para la autenticación de dos factores. Como los suscriptores solo pueden inscribir dispositivos de uno en uno, inscribir un dispositivo nuevo o volver a inscribir un dispositivo existente elimina el registro del dispositivo anterior.



- Los administradores pueden buscar suscriptores por nombre de Active Directory y restablecer su dispositivo. Para ello, vaya a **Administración de acceso e identidad > Recuperación**. Durante el siguiente inicio de sesión en Workspace, el suscriptor sigue los pasos de la primera inscripción.



Azure Active Directory

El uso de Azure Active Directory (AD) para administrar la autenticación de suscriptores en los espacios de trabajo presenta los siguientes requisitos:

- Azure AD con un usuario que tiene permisos de administrador global. Para obtener más información sobre las aplicaciones y los permisos de Azure AD que emplea Citrix Cloud, consulte Permisos de Azure Active Directory para Citrix Cloud.
- Un Citrix Cloud Connector instalado en el dominio de AD local. La máquina también debe estar unida al dominio que se sincroniza con Azure AD.
- VDA 7.15.2000 LTSR CU o la versión actual 7.18 de VDA o posterior.
- Una conexión entre Azure AD y Citrix Cloud. Para obtener más información, consulte Conectar Azure Active Directory a Citrix Cloud.

Al sincronizar su Active Directory con Azure AD, las entradas de UPN y SID deben incluirse en la sincronización. Si estas entradas no están sincronizadas, ciertos flujos de trabajo en Citrix Workspace fallan.

> **Advertencia:**
>
> - Si utiliza Azure Active Directory, no haga el cambio en el Registro que se describe en el artículo CTX225819. Si hace ese cambio, pueden producirse fallos al iniciar sesiones para los usuarios de Azure AD.
> - Se puede agregar un grupo como un miembro de otro grupo (anidamiento) si la función `DSAuthAzureAdNestedGroups` está habilitada. Para habilitar `DSAuthAzureAdNestedGroups`, envíe una solicitud a Citrix Support.

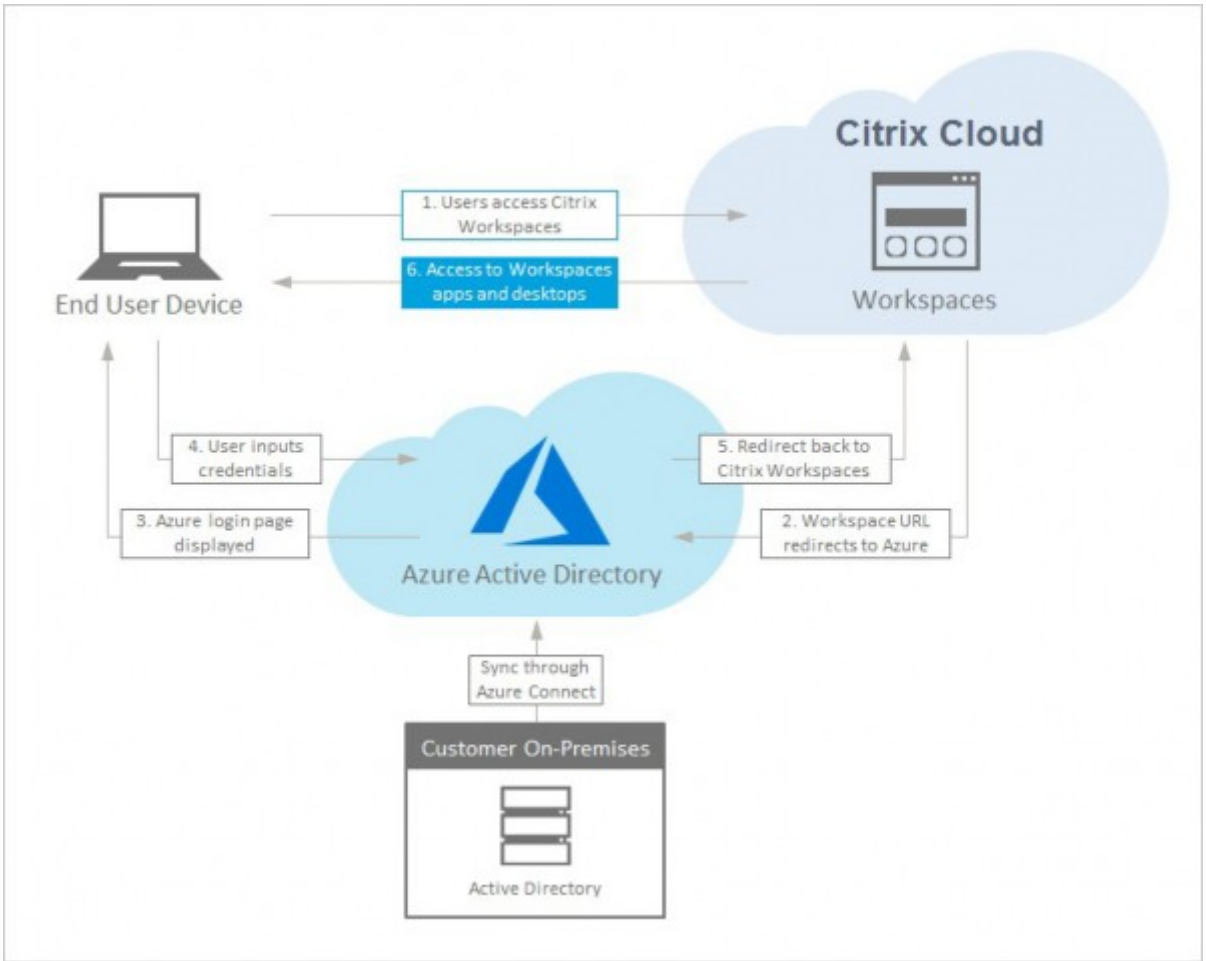
Después de habilitar la autenticación de Azure AD:

- **Mayor seguridad:** Por cuestiones de seguridad, se solicita a los usuarios que inicien sesión nuevamente al iniciar una aplicación o un escritorio. La información de la contraseña se transmite directamente desde el dispositivo del usuario hasta el VDA que aloja la sesión.
- **Experiencia de inicio de sesión:** La autenticación de Azure AD proporciona un inicio de sesión federado, no un inicio de sesión único (SSO). Los suscriptores inician sesión desde una página de inicio de sesión de Azure y es posible que tengan que autenticarse de nuevo al abrir Citrix DaaS.

Para el SSO, habilite el Servicio de autenticación federada de Citrix en Citrix Cloud. Consulte Habilitar Single Sign-On para espacios de trabajo con el Servicio de autenticación federada de Citrix para obtener más información.

Puede personalizar la experiencia de inicio de sesión para Azure AD. Para obtener información, consulte la documentación de Microsoft. Cualquier personalización de inicio de sesión (el logotipo) realizada en la Configuración de Workspace no afecta a la experiencia de inicio de sesión de Azure AD.

En el siguiente diagrama se muestra la secuencia de la autenticación de Azure AD.



Citrix Gateway

Citrix Workspace admite el uso de dispositivos Citrix Gateway locales como proveedores de identidades para administrar la autenticación de suscriptores en los espacios de trabajo. Para obtener más información, consulte Tech Insight: Authentication - Citrix Gateway.

Requisitos de Citrix Gateway

La autenticación de Citrix Gateway tiene los siguientes requisitos:

- Una conexión entre Active Directory y Citrix Cloud. Para ver los requisitos y las instrucciones, consulte Conectar Active Directory con Citrix Cloud.
- Los suscriptores deben ser usuarios de Active Directory para poder iniciar sesión en sus espacios de trabajo.

- Si lleva a cabo la federación, los usuarios de AD deben estar sincronizados con el proveedor de la federación. Citrix Cloud requiere los atributos de AD para permitir que los usuarios inicien sesión correctamente.
- Un dispositivo Citrix Gateway local:
  - Citrix Gateway 12.1 54.13 Advanced Edition o posterior
  - Citrix Gateway 13.0 41.20 Advanced Edition o posterior
- La autenticación de **Citrix Gateway** habilitada en la página **Administración de acceso e identidad**. De esta forma se genera el ID de cliente, el secreto y la URL de redirección necesarios para crear la conexión entre Citrix Cloud y el dispositivo Gateway local.
- En el dispositivo Gateway, se configura una directiva de autenticación de IdP de OAuth mediante el ID de cliente, el secreto y la URL de redirección que se han generado.

Para obtener más información, consulte Conectar un dispositivo Citrix Gateway local como proveedor de identidades con Citrix Cloud.

Experiencia de los suscriptores con Citrix Gateway

Cuando la autenticación con Citrix Gateway está habilitada, los suscriptores siguen este flujo de trabajo:

1. El suscriptor va a la URL del espacio de trabajo en el explorador o inicia la aplicación Workspace.
2. Se redirige al suscriptor a la página de inicio de sesión de Citrix Gateway y se le autentica con cualquier método configurado en el dispositivo Gateway. Este método puede ser la autenticación de varios factores, por federación, mediante directivas de acceso condicional, etc. Para personalizar la página de inicio de sesión de Gateway de modo que tenga el mismo aspecto que la página de inicio de sesión de Workspace, siga los pasos descritos en CTX258331.
3. Una vez que la autenticación se haya realizado correctamente, aparece el espacio de trabajo del suscriptor.

Google

Citrix Workspace admite el uso de Google como proveedor de identidades para administrar la autenticación de suscriptores en los espacios de trabajo.

Requisitos de Google

- Una conexión entre su Active Directory local y Google Cloud.

- Una cuenta de desarrollador con acceso a la consola de Google Cloud Platform. Esta cuenta es necesaria para crear una cuenta de servicio y una clave, y para habilitar la API del SDK de administración.
- Una cuenta de administrador con acceso a la consola de administración de Google Workspace. Esta cuenta es necesaria para configurar la delegación en todo el dominio y una cuenta de usuario de API de solo lectura.
- Una conexión entre el dominio local de Active Directory y Citrix Cloud, con la autenticación con **Google** habilitada en la página **Administración de acceso e identidad**. Para crear esta conexión, se necesitan al menos dos Cloud Connectors en la ubicación de recursos.

Para obtener más información, consulte Conectar Google como proveedor de identidades con Citrix Cloud.

Experiencia de los suscriptores con Google

Cuando la autenticación con Google está habilitada, los suscriptores siguen este flujo de trabajo:

1. El suscriptor va a la URL del espacio de trabajo en el explorador o inicia la aplicación Workspace.
2. Se redirige al suscriptor a la página de inicio de sesión de Google y se autentica con el método configurado en Google Cloud (por ejemplo, la autenticación de varios factores, las directivas de acceso condicional…).
3. Una vez que la autenticación se haya realizado correctamente, aparece el espacio de trabajo del suscriptor.

Okta

Citrix Workspace admite el uso de Okta como proveedor de identidades para administrar la autenticación de suscriptores en los espacios de trabajo. Para obtener más información, consulte Tech Insight: Authentication - Okta.

Requisitos de Okta

La autenticación con Okta tiene los siguientes requisitos:

- Una conexión entre su Active Directory local y su organización en Okta.
- Una aplicación web OIDC de Okta configurada para usarse con Citrix Cloud. Para conectar Citrix Cloud a su organización de Okta, tiene que proporcionar el ID del cliente y el secreto del cliente asociados a esta aplicación.
- Una conexión entre el dominio local de Active Directory y Citrix Cloud, con la autenticación con **Okta** habilitada en la página **Administración de acceso e identidad**.

Para obtener más información, consulte Conectar Okta como proveedor de identidades con Citrix Cloud.

Experiencia de los suscriptores con Okta

Cuando la autenticación con Okta está habilitada, los suscriptores siguen este flujo de trabajo:

1. El suscriptor va a la URL del espacio de trabajo en el explorador o inicia la aplicación Workspace.
2. Se redirige al suscriptor a la página de inicio de sesión de Okta y se autentica con el método configurado en Okta (por ejemplo, la autenticación de varios factores, las directivas de acceso condicional…).
3. Una vez que la autenticación se haya realizado correctamente, aparece el espacio de trabajo del suscriptor.

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 y es posible que tengan que autenticarse de nuevo al abrir Citrix DaaS. Para el SSO, habilite el Servicio de autenticación federada de Citrix en Citrix Cloud. Consulte Habilitar Single Sign-On para espacios de trabajo con el Servicio de autenticación federada de Citrix para obtener más información.

SAML 2.0

Citrix Workspace admite el uso de SAML 2.0 para administrar la autenticación de suscriptores en los espacios de trabajo. Puede utilizar el proveedor SAML que prefiera, siempre que sea compatible con SAML 2.0.

Requisitos de SAML 2.0

La autenticación con SAML presenta los siguientes requisitos:

- Proveedor SAML compatible con SAML 2.0.
- Dominio de Active Directory local.
- Dos Cloud Connectors implementados en una ubicación de recursos y unidos al dominio de AD local.
- Integración de AD con su proveedor SAML.

Para obtener más información sobre cómo configurar la autenticación SAML para espacios de trabajo, consulte Conectar SAML como proveedor de identidades con Citrix Cloud.

Experiencia de los suscriptores con SAML 2.0

1. El suscriptor va a la URL del espacio de trabajo en el explorador o inicia la aplicación Citrix Workspace.
2. Al suscriptor se le redirige a la página de inicio de sesión del proveedor de identidades SAML de su organización. El suscriptor se autentica con el mecanismo configurado para el proveedor de identidades SAML, como la autenticación de varios factores o las directivas de acceso condicional.
3. Una vez que la autenticación se haya realizado correctamente, aparece el espacio de trabajo del suscriptor.

Servicio de autenticación federada (FAS) de Citrix

Citrix Workspace permite usar el Servicio de autenticación federada (FAS) de Citrix para el acceso Single Sign-On (SSO) a Citrix DaaS. Sin FAS, a los suscriptores que utilizan un proveedor de identidades federadas se les pide que introduzcan sus credenciales más de una vez para acceder a sus instancias de DaaS.

Para obtener más información, consulte Servicio de autenticación federada (FAS) de Citrix.

Experiencia de los suscriptores en el cierre de sesión

Use **Parámetros > Cerrar sesión** para completar el proceso de cierre de sesión desde Workspace y Azure AD. Si los suscriptores cierran el explorador web en lugar de utilizar la opción **Cerrar sesión**, podrían permanecer conectados a Azure AD.

> **Importante:**
>
> Si Citrix Workspace agota el tiempo de espera en el explorador web debido a la inactividad, la sesión de los suscriptores en Azure AD no se cierra. De esta forma se evita que, al agotarse el tiempo de espera en Citrix Workspace, se cierren también forzosamente otras aplicaciones de Azure AD.

Más información

- Tech Brief: Workspace Single Sign-On
- Tech Insights - Citrix Workspace
- Proof of Concept Guides - Citrix Workspace

Integrar servicios en los espacios de trabajo

October 12, 2023

En este artículo, se describen los pasos necesarios para agregar servicios a Citrix Workspace, que es un proceso en dos pasos:

1. Configurar los servicios individuales en Citrix Cloud. Puede encontrar una lista de los servicios de Citrix Cloud con enlaces a las instrucciones de cada uno en Citrix Cloud Services.
2. Habilitar (e inhabilitar) el acceso a los servicios configurados en **Configuración de Workspace** > **Integraciones de servicios**.

Configurar servicios

Los servicios adquiridos se muestran en un diseño de tarjeta en el panel de mandos de Citrix Cloud. Los servicios que ha adquirido incluyen un botón **Administrar**.

Para configurar los servicios adquiridos:

1. Inicie sesión en Citrix Cloud.
2. Seleccione **Administrar** en el mosaico del servicio que quiere configurar.
3. Siga las instrucciones para configurar ese servicio.

Para obtener una breve descripción de los servicios alojados en la nube, consulte Servicios alojados en la nube a través de Citrix Workspace

Si quiere probar un nuevo servicio, puede solicitar una prueba o una demostración. Para obtener más información sobre las pruebas de servicios, consulte Pruebas de Citrix Cloud Service.

Habilitar servicios

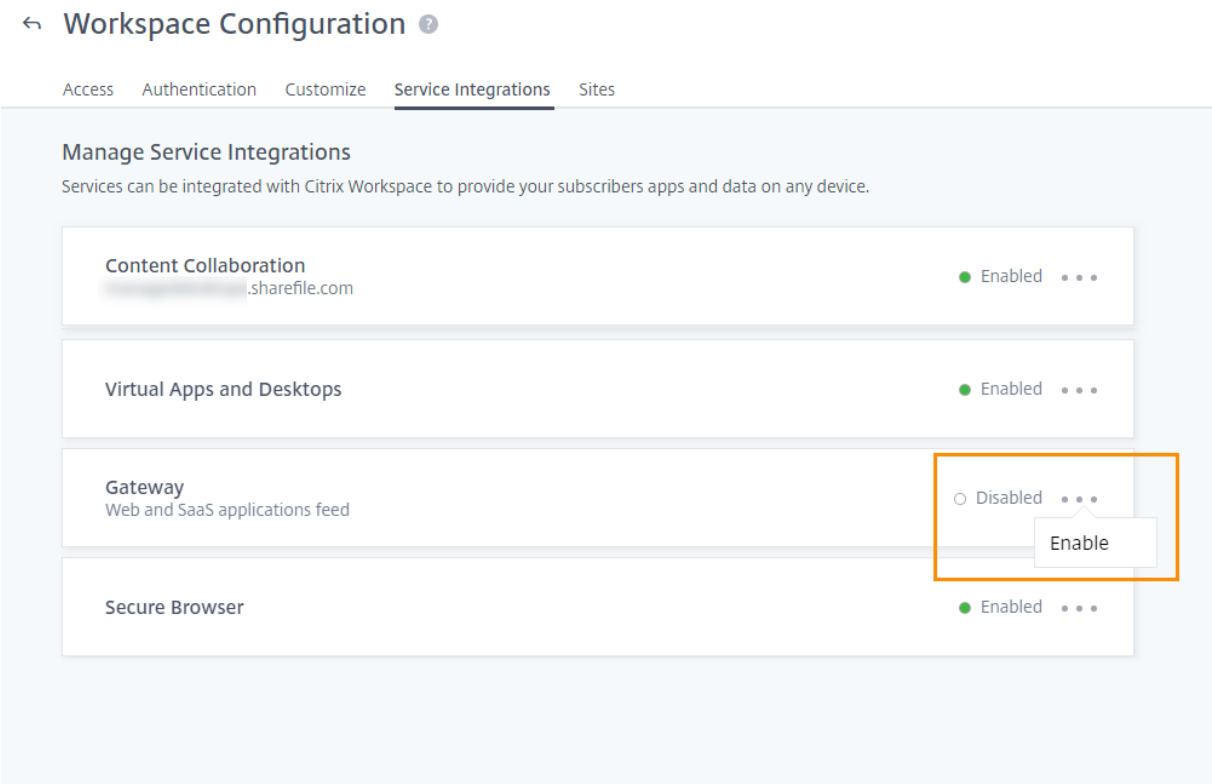
Una vez que haya configurado los servicios, podrá integrarlos en Citrix Workspace.

La suscripción a **DaaS** y a **Remote Browser Isolation Service** los habilita de forma predeterminada. De forma predeterminada, todos los demás servicios nuevos a los que se suscriba su organización están inhabilitados.

> **Nota:**
>
> Tanto **Citrix Apps Essentials Service** como **Citrix DaaS** se muestran como “Citrix DaaS”en la ficha **Integraciones de servicios** de **Configuración de Workspace**.

Para habilitar la integración de un servicio en el espacio de trabajo:

1. Vaya a **Configuración de Workspace** > **Integraciones de servicios**.
2. Seleccione los puntos suspensivos que hay junto al servicio y, a continuación, elija **Habilitar**.

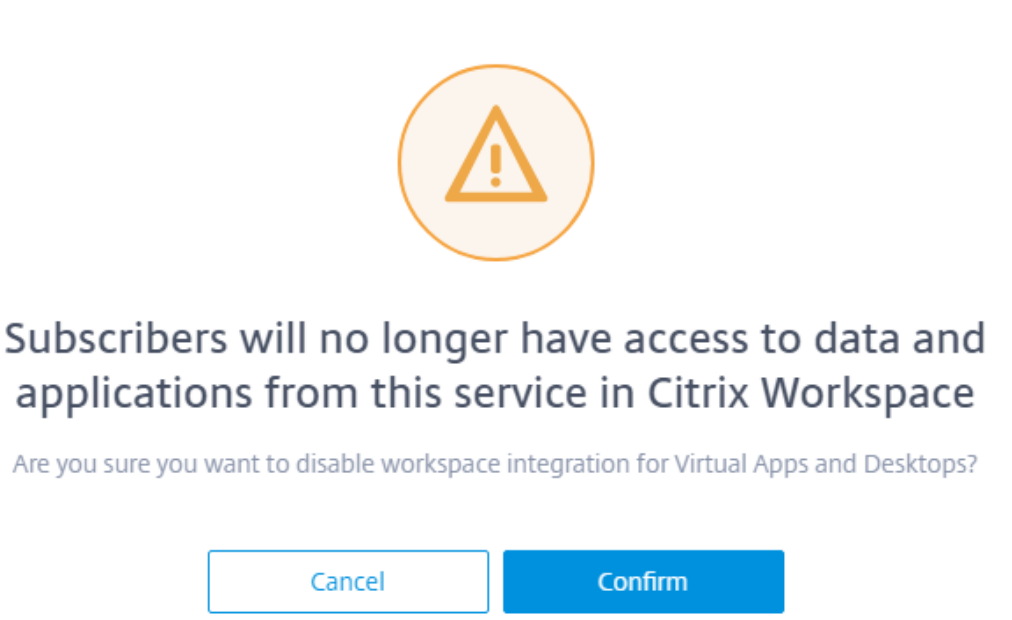


Inhabilitar servicios

Al inhabilitar la integración del espacio de trabajo, se bloquea el acceso de los suscriptores a ese servicio. Esto no inhabilita la URL del espacio de trabajo, pero los suscriptores no podrán acceder a los datos ni a las aplicaciones desde ese servicio en Citrix Workspace.

Para inhabilitar la integración de un servicio en el espacio de trabajo:

1. Vaya a **Configuración de Workspace** > **Integraciones de servicios**.
2. Seleccione los puntos suspensivos que hay junto al servicio y seleccione **Inhabilitar**.
3. Cuando se le solicite, seleccione **Confirmar** para confirmar que los suscriptores perderán el acceso a los datos o las aplicaciones del servicio.



Configurar la aplicación Citrix Workspace

November 21, 2023

Puede configurar la aplicación Citrix Workspace mediante Global App Configuration Service (GACS). Le ayuda a administrar los parámetros de la aplicación para usuarios finales tanto en dispositivos administrados como en dispositivos no administrados.
Los parámetros se pueden configurar tanto para entornos de la nube (Citrix Workspace) como para entornos locales (Citrix StoreFront) con uno de estos métodos:

- Interfaz de usuario (IU) de Global App Configuration Service:
  - Configurar los parámetros de los almacenes de la nube
  - Configurar los parámetros de los almacenes locales
- API: Para configurar parámetros mediante las API, consulte el portal para desarrolladores de Citrix.

Este servicio es compatible con las plataformas Windows, Mac, Android, iOS, HTML5 y ChromeOS.

Ventajas clave

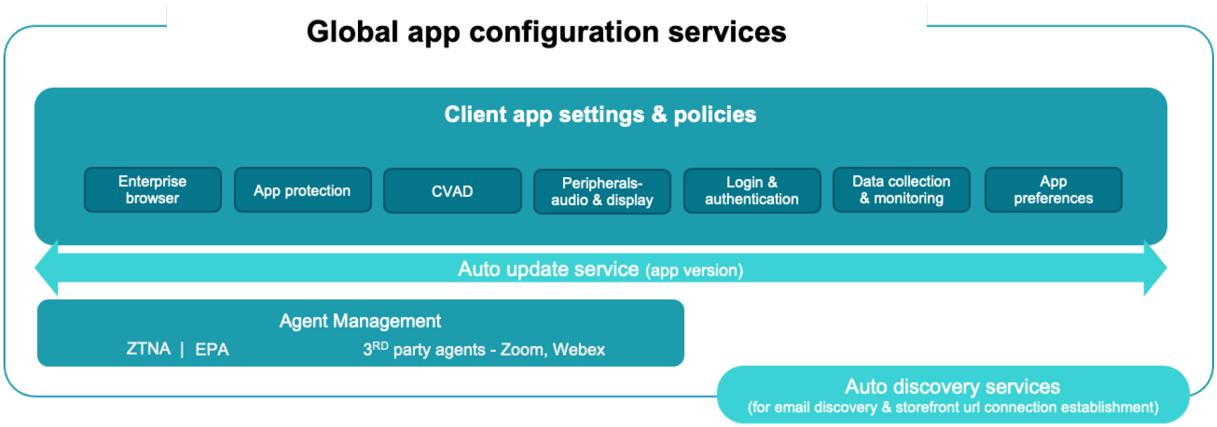
Global App Configuration Service le permite realizar estas funciones desde una interfaz centralizada:

- Configurar parámetros para dispositivos administrados y no administrados (dispositivos BYOD)
- Configurar parámetros para varios almacenes
- Actualizar y administrar agentes de aplicaciones cliente (por ejemplo, Endpoint Analysis, ZTNA) y agentes de terceros (por ejemplo, Zoom, Webex)
- Actualizar y administrar automáticamente la versión de la aplicación Citrix Workspace para los usuarios finales
- Probar la configuración antes de implantarla para los usuarios finales

¿Cómo funciona Global App Configuration Service?

Global App Configuration Service es una solución de IP de Citrix que se utiliza para configurar y administrar parámetros de aplicaciones cliente. Emplea estos servicios y parámetros para ofrecer una experiencia integrada a los usuarios finales.

- **Servicios de detección automática**: Asigna dominios a las URL de almacenamiento, lo que permite a los usuarios finales iniciar sesión con sus direcciones de correo electrónico. Los usuarios finales no están obligados a proporcionar las URL de su almacén al iniciar sesión.
- **Servicio de actualización automática y administración de agentes**: Actualiza automáticamente la aplicación Citrix Workspace a la versión especificada para los usuarios finales. Puede configurar diferentes versiones de aplicaciones para diferentes plataformas.
- **Directivas y parámetros de aplicaciones cliente**: Todos los parámetros de usuario final de la aplicación Citrix Workspace se pueden configurar y definir de forma centralizada. Incluye parámetros como la experiencia en el inicio de sesión, la seguridad, las opciones de autenticación y los parámetros de aplicaciones y escritorios virtuales.



Requisitos previos

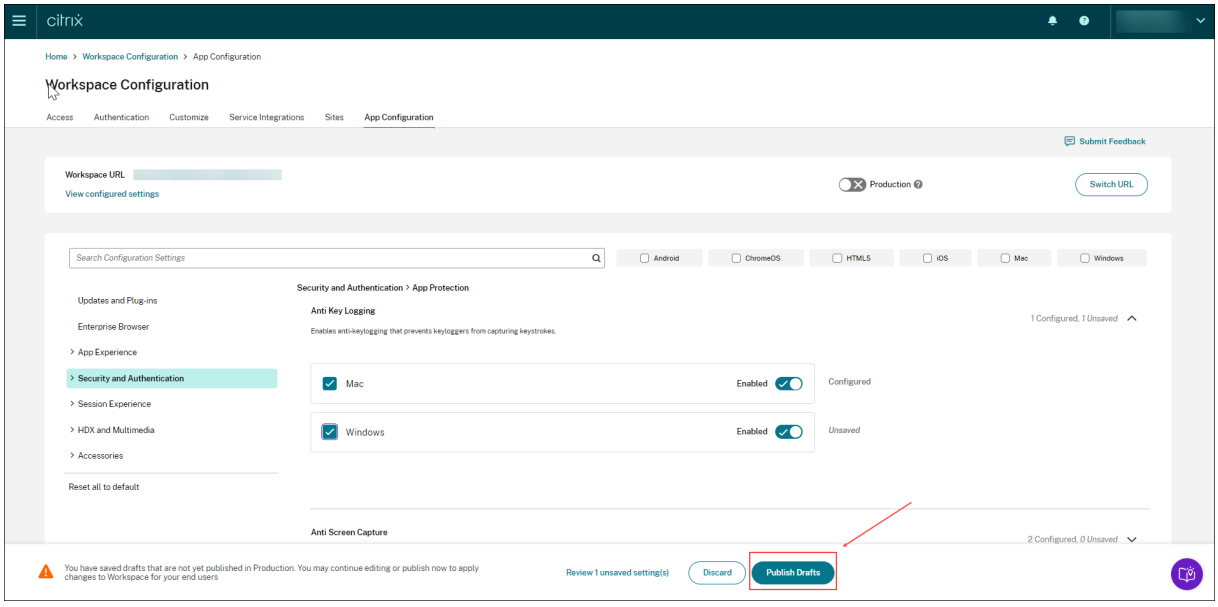
Antes de configurar los parámetros de aplicación, verifique que la versión de la aplicación Citrix Workspace sea igual o posterior a las versiones especificadas. Para obtener más información, consulte esta

tabla.

Plataforma de la aplicación Citrix Workspace	Versión mínima compatible
Windows	Versión Current Release: 2106, LTSR: 2203.1
Mac	2203.1
iOS	2104
HTML5	2111
ChromeOS	2203
Android	2104

¿Cómo utilizar Global App Configuration Service?

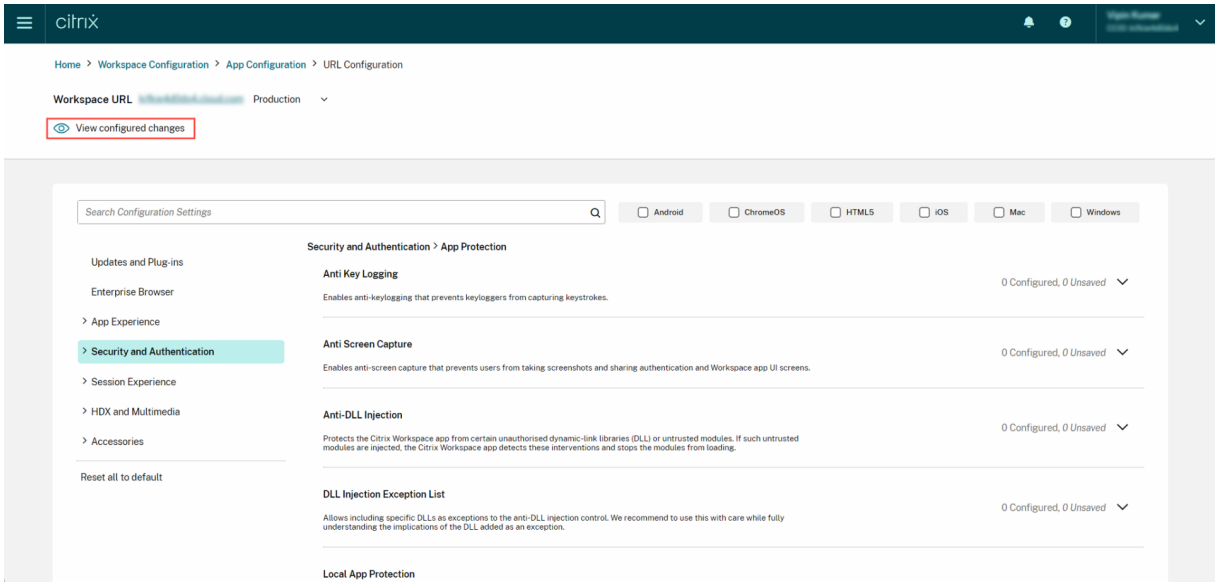
Para configurar los parámetros, inicie sesión en el portal de Citrix Cloud y vaya a **Configuración de Workspace** > **Configuración de la aplicación**. Modifique los parámetros de aplicación según las directivas de su organización. A continuación, puede hacer clic en **Publicar borradores** para guardar y publicar sus parámetros.



La interfaz de usuario también ofrece las siguientes opciones para garantizar una experiencia de usuario simplificada.

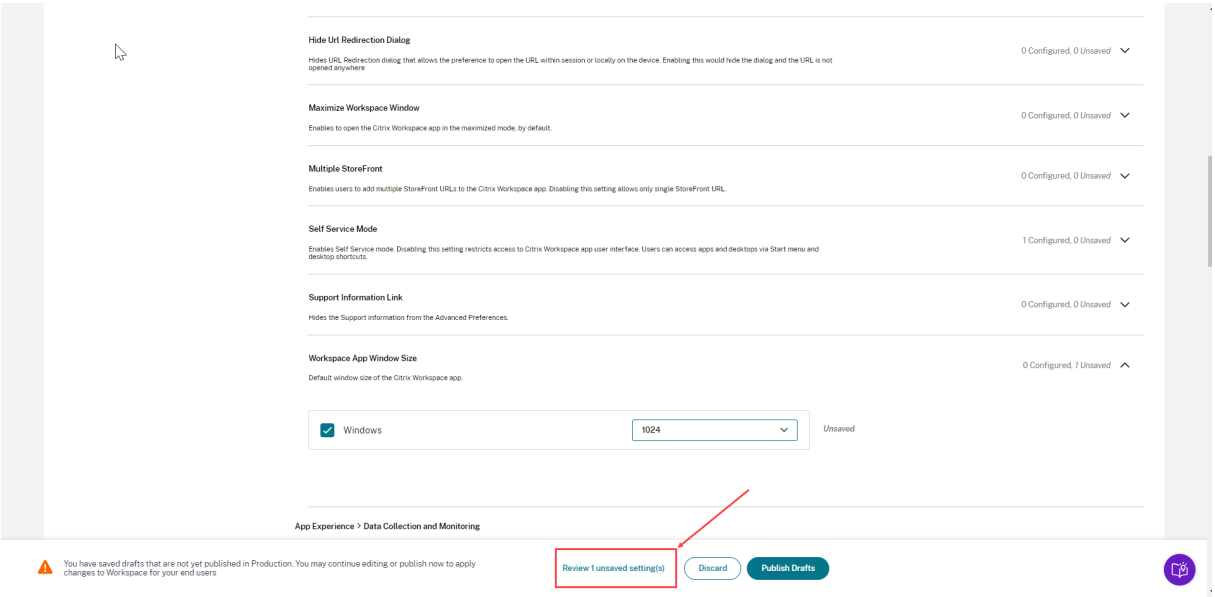
Ver un resumen de los parámetros configurados

Puede ver un resumen de la configuración actual si hace clic en el botón **Ver parámetros configurados** . De esta forma, se elimina la necesidad de expandir y revisar cada parámetro por separado. Una lista consolidada de todos los parámetros configurados le permite revisar exhaustivamente la configuración actual y evaluar el impacto en los usuarios.

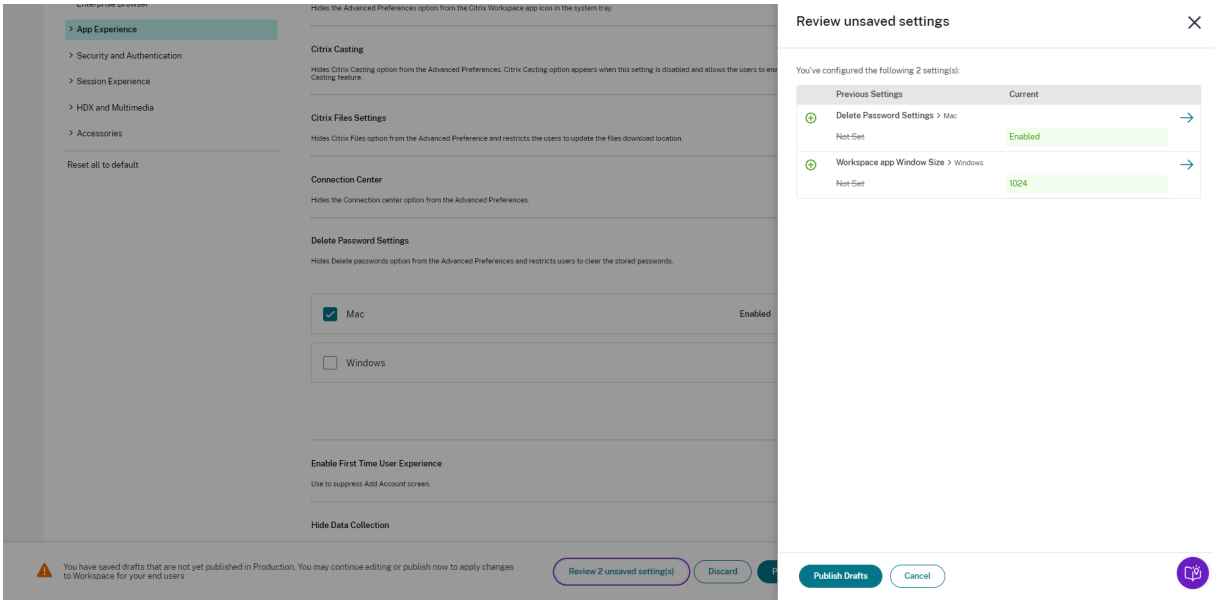


Revisar cambios no guardados

Haga una revisión final de los cambios no guardados antes de publicar la configuración. La cantidad de parámetros no guardados se muestra en la interfaz de usuario y puede acceder a esta lista haciendo clic en la opción **Revisar parámetros sin guardar**. Esto le permite realizar cambios informados y mantener la precisión de los datos.



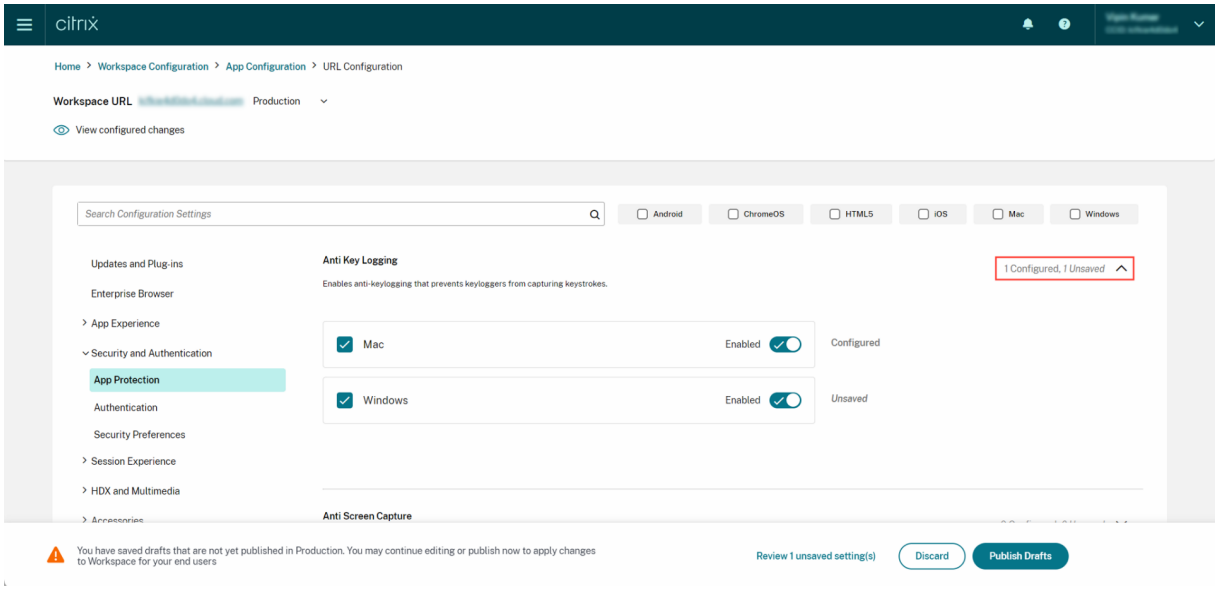
También puede ir a un parámetro no guardado haciendo clic en la flecha.



Interfaz de usuario mejorada

Vea el estado de cada parámetro sin expandirlo. Ahora se muestran las siguientes etiquetas para facilitar una toma de decisiones informada en cada paso.

- **Configurado**: Muestra la cantidad de plataformas (SO cliente) para las que ya se ha configurado el parámetro.
- **No guardado**: Muestra la cantidad de parámetros que están configurados pero que aún no se han guardado



Opción de búsqueda mejorada

La experiencia de búsqueda se ha mejorado para ofrecer una experiencia sólida y fluida. Los administradores ahora pueden iniciar sesión en el portal en la nube y buscar los parámetros necesarios en la página Configuración de aplicaciones con facilidad. Pueden usar los siguientes métodos de búsqueda.

- **Buscar mediante la descripción del parámetro**

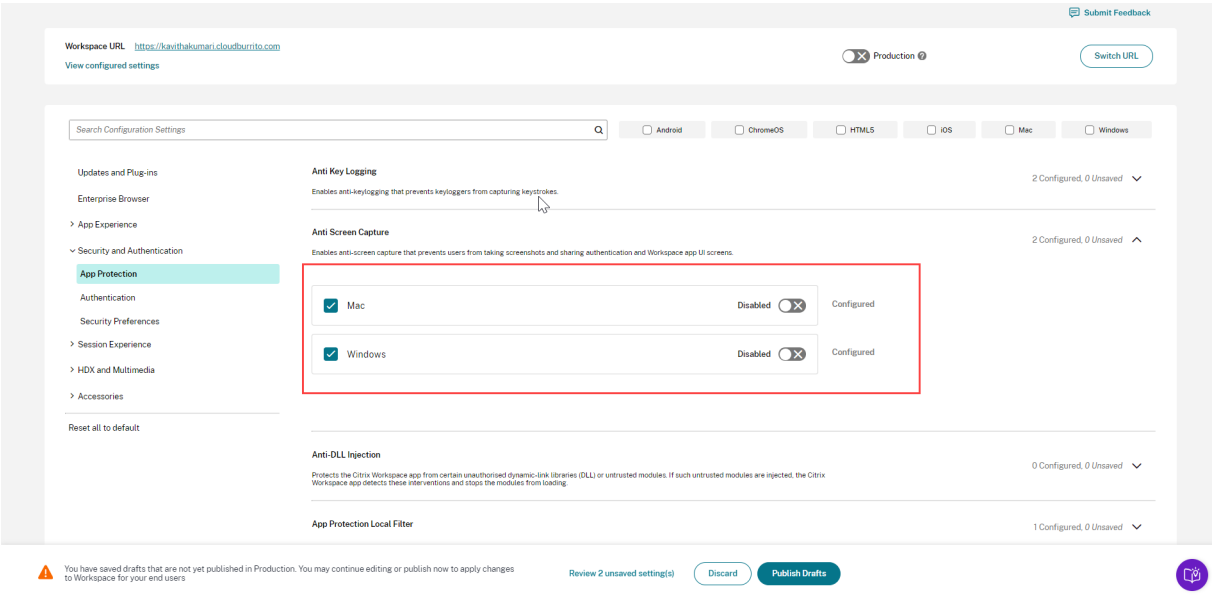
Para localizar un parámetro, introduzca las palabras clave que se encuentran en su descripción. Esto ofrece un enfoque de búsqueda más flexible, en el que se usan términos relevantes asociados al parámetro en cuestión.

- **Buscar mediante el nombre del parámetro de API**

Puede buscar un parámetro introduciendo el nombre del parámetro de API correspondiente. Este método ofrece una búsqueda más precisa y específica, lo que permite a los usuarios encontrar rápidamente el parámetro específico que necesitan.

Ver las plataformas aplicables a cada parámetro

Cada parámetro ahora muestra de forma dinámica solo las plataformas en las que es relevante y aplicable. Este enfoque garantiza que se presente a los usuarios una lista de opciones concisa y personalizada.



Frecuencia de obtención de parámetros actualizados

Una vez publicada la configuración, es posible que los parámetros tarden unas horas en actualizarse en el lado del cliente.

- En la misma sesión, los parámetros se actualizan de esta manera.

Plataforma	Tiempo máximo necesario para actualizar los parámetros
Aplicación Citrix Workspace para Windows	hasta 6 horas
Aplicación Citrix Workspace para macOS	hasta 6 horas
Aplicación Citrix Workspace para HTML5	hasta 3 horas
Aplicación Citrix Workspace para ChromeOS	hasta 3 horas
Aplicación Citrix Workspace para iOS	hasta 6 horas
Aplicación Citrix Workspace para Android	hasta 6 horas

- Para Windows y macOS, los parámetros se pueden actualizar inmediatamente si los usuarios finales salen de la aplicación Citrix Workspace y la reinician.
- Cuando un usuario final agrega un almacén a su aplicación Citrix Workspace, los parámetros de ese almacén se actualizan automáticamente.

Orden de prioridad para la aplicación de los parámetros

Además de Global App Configuration Service, existen herramientas específicas de la plataforma (como GPO para Windows) que se pueden utilizar para configurar parámetros de usuario final.
En caso de conflicto entre los parámetros configurados a través de Global App Configuration Service y otras herramientas de la plataforma, los parámetros se aplican en este orden.

Plataforma	Tipo de almacén	Orden de prioridad
Aplicación Citrix Workspace para Windows	StoreFront y Cloud	**Objeto de directiva de grupo (GPO) > Global App Configuration Service > Registro**
Aplicación Citrix Workspace para Mac	StoreFront y Cloud	**MDM > Global App Configuration Service > UserDefaults**
Aplicación Citrix Workspace para HTML5	StoreFront	Global App Configuration Service > Configuration.js
	Cloud	Global App Configuration Service
Aplicación Citrix Workspace para ChromeOS	StoreFront	**Directiva de administración de Google > Global App Configuration Service >** Configuration.js
	Cloud	**Directiva de administración de Google > Global App Configuration Service**
Aplicación Citrix Workspace para iOS	StoreFront y Cloud	Global App Configuration Service
Aplicación Citrix Workspace para Android	StoreFront y Cloud	Global App Configuration Service

Limitaciones

- Global App Configuration Service no es compatible con Linux.
- No puede agregar más de un almacén habilitado para Global App Configuration Service en Windows y Mac.

Recursos adicionales

- Resumen técnico de Global App Configuration Service
- Preguntas frecuentes: Parámetros y comportamientos de Global App Configuration Service
- Grabación de seminario web: Cómo usar Global App Configuration Service
- Explicación de funciones de Citrix: Global App Configuration Service

Configurar los parámetros de los almacenes de la nube

November 22, 2023

Introducción

Puede configurar los parámetros de la aplicación Citrix Workspace para almacenes de la nube mediante Global App Configuration Service (GACS). Ayuda a administradores a configurar y administrar la aplicación Citrix Workspace para los usuarios finales en dispositivos administrados y no administrados. Este servicio es compatible con las plataformas Windows, Mac, Android, iOS, HTML5 y ChromeOS.

Requisito previo

- Debe poder contactarse con la dirección https://discovery.cem.cloud.us. Es necesario para el funcionamiento de los servicios de detección por correo electrónico y de Global App Configuration Service.
- Verifique que tiene acceso a una cuenta de Citrix Cloud. Si no, puede crear una cuenta desde https://onboarding.cloud.com/. Para obtener más información, consulte Registrarse en Citrix Cloud.
- Verifique que tiene una suscripción a Workspace.

Introducción

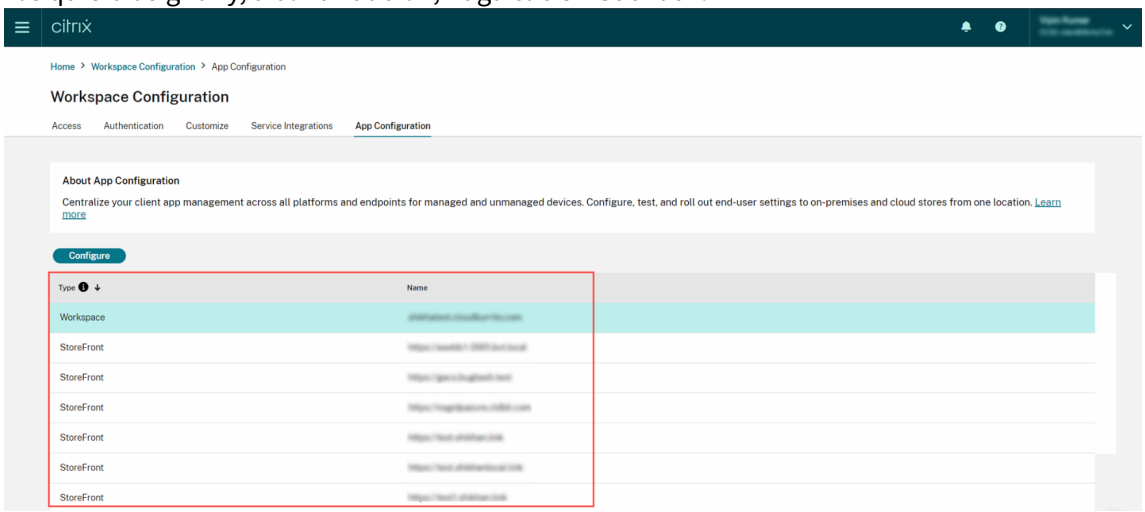
Puede iniciar sesión en su cuenta de Citrix Cloud y configurar los parámetros desde **Configuración de Workspace** > **Configuración de aplicaciones**.
Antes de continuar, compruebe si tiene los siguientes permisos.

- **Suscripción a Workspace:** La suscripción a Workspace es necesaria para crear una URL de Workspace. Si no tiene una suscripción, no podrá agregar ni configurar almacenes de la nube. Solo se le presentará la opción de configurar los almacenes locales.
- **URL de Workspace:** Si tiene una suscripción a Workspace, pero aún no ha agregado su URL, aparecerá la siguiente pantalla. Puede hacer clic en **Iniciar** en **Configurar los parámetros de los almacenes de la nube** para crear la URL.

Configurar parámetros

Puede configurar parámetros de la aplicación Citrix Workspace desde el portal de Citrix Cloud. Si se han configurado varios almacenes para su organización, puede configurar cada uno de los almacenes por separado.

1. Vaya a Citrix Cloud e inicie sesión con sus credenciales de Citrix Cloud.
2. Vaya a **Configuración de Workspace** > **Configuración de aplicaciones**.
3. Haga clic en **Cambiar URL** para seleccionar el almacén para el que quiere configurar parámetros.
4. En la lista de direcciones URL de almacén configuradas, seleccione el almacén cuyos parámetros quiera asignar y, a continuación, haga clic en **Guardar**.



5. Modifique los parámetros de sus plataformas preferidas según sus necesidades.
6. Haga clic en **Publicar borradores** para guardar los parámetros.

> **Nota:**
>
> Es posible que los parámetros de los clientes de la aplicación Citrix Workspace tarden unas horas

> en actualizarse. Para obtener más información, consulte Frecuencia de obtención de parámetros actualizados.

Configurar la detección por correo electrónico

El servicio de detección por correo electrónico permite a los usuarios finales iniciar sesión automáticamente con sus direcciones de correo electrónico. No están obligados a proporcionar las URL de su almacén.
Para habilitar este servicio en los almacenes de la nube, siga estos pasos.

1. Reclamar un dominio
2. Crear una asignación de dominio con URL

Reclamar un dominio

Para reclamar un dominio:

1. Vaya a https://adsui.cloud.com.
2. Vaya a **Notificaciones** > **Dominios** > **Agregar dominio**.
3. Introduzca el dominio que quiere reclamar (por ejemplo, ace.ejemplo.com).
4. Haga clic en **Confirmar**.
5. Copie el token DNS que aparece en la pantalla.
6. Para crear un registro de DNS en TXT, vaya al portal del proveedor de servicios y agregue el token DNS.
7. Para iniciar el proceso de verificación:
    a) Vaya a **Notificaciones** > **Dominios**.
    b) Vaya al dominio que agregó y haga clic en el menú de tres puntos.
    c) Seleccione **Verificar dominio**.
    d) Haga clic en **Iniciar comprobación de DNS**.

Una vez finalizada la verificación, el estado del dominio cambiará de *pendiente* a *verificado*.

Crear una asignación de dominio con URL

1. Vaya a **Notificaciones** > **Dominios**.
2. Vaya al dominio que agregó y haga clic en el menú de tres puntos.

3. Haga clic en **Agregar otra URL de servidor**.
4. Introduzca la URL del almacén que quiere asignar a este dominio.
5. Haga clic en **Guardar**.

Configurar los parámetros de los almacenes locales

November 21, 2023

Introducción

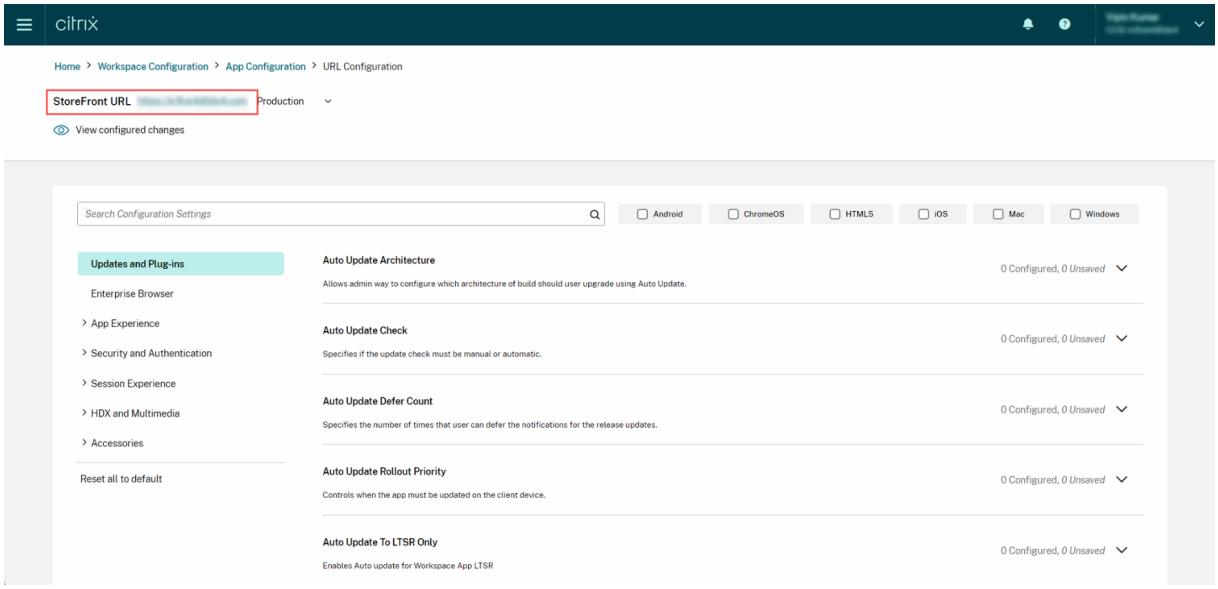
Puede configurar los parámetros de la aplicación Citrix Workspace para almacenes locales mediante Global App Configuration Service (GACS). Le ayuda a configurar y administrar la aplicación Citrix Workspace para los usuarios finales en dispositivos administrados y no administrados. Global App Configuration Service es compatible con las plataformas Windows, Mac, Android, iOS, HTML5 y ChromeOS.

Requisito previo

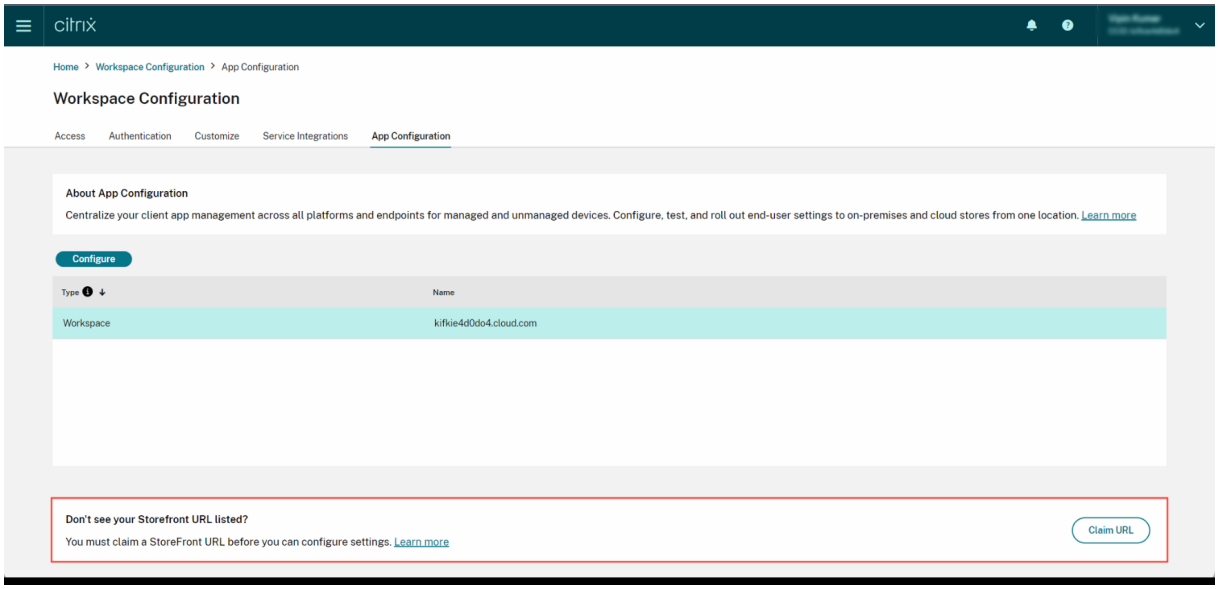
- Debe poder contactarse con la dirección https://discovery.cem.cloud.us. Es necesario para el funcionamiento de los servicios de detección por correo electrónico y de Global App Configuration Service.
- Verifique que tiene acceso a una cuenta de Citrix Cloud. Si aún no tiene una cuenta, puede crear una desde https://onboarding.cloud.com/. Para obtener más información, consulte Registrarse en Citrix Cloud.
- En entornos locales, debe reclamar una URL antes de poder configurar los parámetros. Para obtener más información, consulte Reclamar una URL.

Introducción

Para configurar los parámetros de un almacén local, inicie sesión en su cuenta de Citrix Cloud y vaya a **Configuración de Workspace** > **Configuración de aplicaciones**.
Si ha reclamado la propiedad de su URL de StoreFront, aparecerá la siguiente pantalla en la que podrá empezar a configurar los parámetros. Para obtener más información, consulte la sección Configurar parámetros.



Si aún no ha reclamado la propiedad de su URL de StoreFront, aparecerá la siguiente pantalla en la que se le pedirá que proteja su URL antes de continuar. Para obtener más información, consulte Reclamar una URL para almacenes locales.



Reclamar una URL para almacenes locales

Es obligatorio establecer una reclamación sobre la URL antes de empezar a configurar los parámetros de la misma.

Para reclamar una URL:

1. Vaya a https://adsui.cloud.com/url e inicie sesión con sus credenciales de Citrix Cloud.

2. Vaya a **Notificaciones** > **URL** > **Agregar URL**.
3. Introduzca la URL que quiera reclamar.
4. Haga clic en **Confirmar**. Aparece la ventana emergente de verificación.

   > **Nota:**
   >
   > Si el entorno local no tiene instalado NetScaler Gateway, no podrá realizar el proceso de verificación (a partir del paso 5). En este caso, lleve a cabo los pasos 1 a 4 tal y como se describe en el procedimiento anterior y contacte con nuestro equipo de asistencia con su ID de cliente y la URL en cuestión.

5. Si tiene NetScaler Gateway instalado en la configuración local, puede comprobar la URL siguiendo estos pasos.

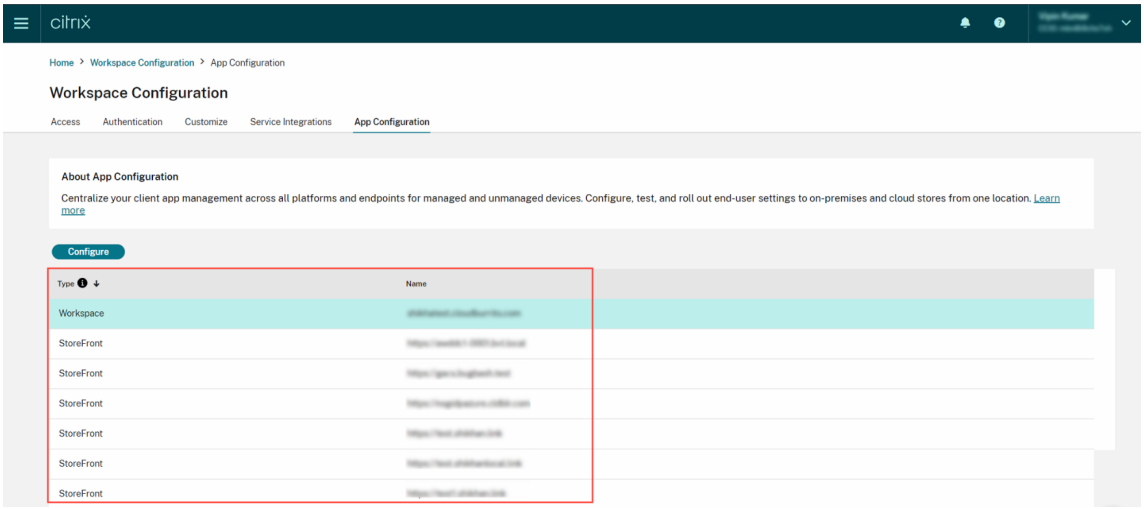
   a) **Copie** el token que aparece en la ventana emergente.
   b) Cree y configure una directiva de respuesta y una acción de respuesta en su Citrix ADC.
   c) Vincule su directiva de respuesta globalmente.
   d) Vaya a `https://<customergatewayurl>/vpn/CitrixClaims` para comprobar si la directiva de respuesta está configurada correctamente.
   e) Vuelva a **Notificaciones** > **URL** y busque la URL que agregó.
   f) Haga clic en el icono del menú de tres puntos para ver la URL agregada.
   g) Seleccione **Verificar URL**.
   h) Haga clic en **Iniciar comprobación de reclamación** para iniciar el proceso de verificación.

   Una vez finalizada la configuración, el estado del dominio cambiará de *Pendiente* a *Verificado*.

Configurar parámetros

Puede configurar los parámetros de la aplicación Citrix Workspace una vez que haya reclamado la URL. Si se han configurado varios almacenes para su empresa, puede configurar los parámetros de cada almacén por separado.

1. Vaya al portal de Citrix Cloud e inicie sesión con sus credenciales.
2. Vaya a **Configuración de Workspace** > **Configuración de aplicaciones**.
3. Haga clic en **Cambiar URL** para seleccionar el almacén para el que quiere configurar parámetros.
4. En la lista de direcciones URL de almacén configuradas, seleccione el almacén cuyos parámetros quiera asignar y, a continuación, haga clic en **Guardar**.



5. Modifique los parámetros de sus plataformas preferidas según sus necesidades.
6. Haga clic en **Publicar borradores** para guardar los parámetros.

> **Nota:**
>
> Es posible que los parámetros de los clientes de la aplicación Citrix Workspace tarden unas horas en actualizarse. Para obtener más información, consulte Frecuencia de obtención de parámetros actualizados.

Configurar la detección basada en correo electrónico

El servicio de detección por correo electrónico permite a los usuarios finales iniciar sesión automáticamente con sus direcciones de correo electrónico. No están obligados a proporcionar las URL de su almacén.
Para habilitar este servicio en los almacenes de la nube, siga estos pasos.

1. Reclamar un dominio
2. Crear una asignación de dominio con URL

Reclamar un dominio

Para reclamar un dominio:

1. Vaya a AutoDiscovery Service.
2. Vaya a **Notificaciones** > **Dominios** > **Agregar dominio**.
3. Introduzca el dominio que quiere reclamar (por ejemplo, ace.ejemplo.com).
4. Haga clic en **Confirmar**.

5. Copie el token de DNS que aparece en la pantalla en el Portapapeles.
6. Para crear un registro de DNS en TXT, vaya al portal del proveedor de servicios y agregue el token DNS.
7. Para iniciar el proceso de verificación:

    a) Vaya a **Notificaciones** > **Dominios**.
    b) Vaya al dominio que agregó y haga clic en el menú de tres puntos.
    c) Seleccione **Verificar dominio**.
    d) Haga clic en **Iniciar comprobación de DNS**.

Una vez finalizada la verificación, el estado del dominio cambiará de *Pendiente* a *Verificado*.

> **Nota:**
>
> Puede reclamar 10 dominios como máximo. Si quiere reclamar más de 10 dominios, póngase en contacto con Citrix Support e indique su ID de cliente y su URL.

Crear una asignación de dominio con URL

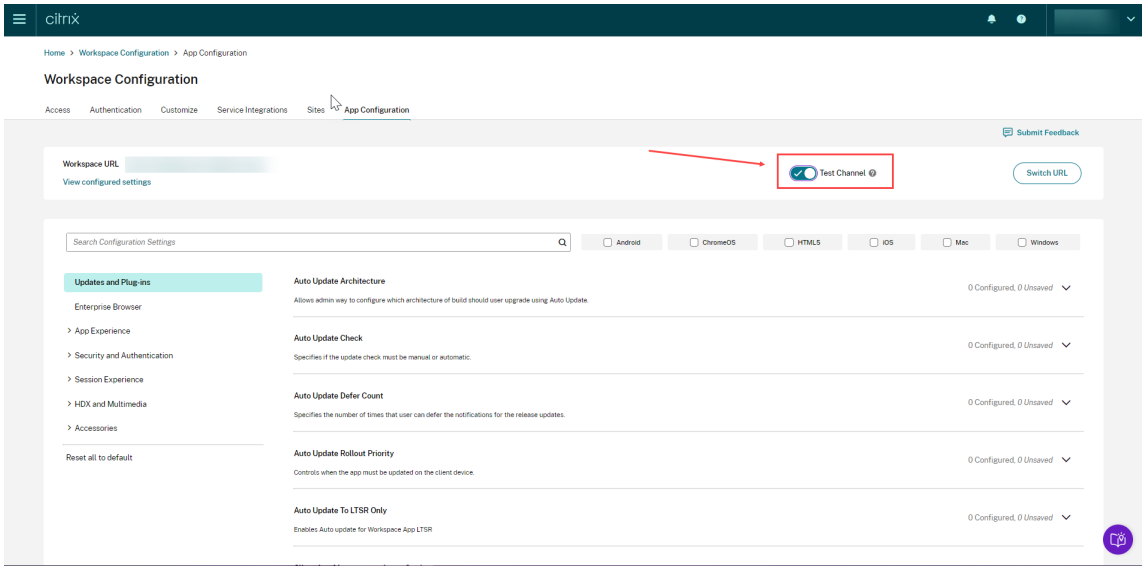
1. Vaya a **Notificaciones** > **Dominios**.
2. Vaya al dominio que agregó y haga clic en el menú de tres puntos.
3. Haga clic en **Agregar otra URL de servidor**.
4. Introduzca la URL del almacén que quiere asignar a este dominio y guarde.

Configuración del canal de prueba

November 21, 2023

Puede probar la configuración antes de habilitarla para los usuarios finales. Le ayuda a detectar y resolver cualquier problema que pueda surgir después de la implementación.
La función de prueba reduce significativamente la probabilidad de interrupciones o errores durante el proceso de implementación, y aumenta la satisfacción general de los usuarios.
Para probar la configuración:

1. Vaya al portal de Cloud e inicie sesión con sus credenciales de Citrix Cloud.
2. Vaya a **Configuración de Workspace** > **Configuración de aplicaciones**.
3. Cambie el botón a **Canal de prueba**. Está configurado en **Producción** de forma predeterminada.



4. Modifique los parámetros de sus plataformas preferidas según sus necesidades.
5. A continuación, puede hacer clic en **Publicar borradores** para publicar sus parámetros en el canal de prueba.

> **Nota:**
>
> Global App Configuration Service solo admite dos canales por almacén, un canal de producción (predeterminado) y un canal de prueba.

Configurar la función de canales en dispositivos de usuario final

Windows

Para probar la configuración definida por administradores en un dispositivo Windows, los usuarios deben crear este Registro.

```
    Path- HKEY_CURRENT_USER\SOFTWARE\Citrix\Receiver
    Name- AppConfigChannelName
    Type- REG_SZ
    Value- testrolloutchannel1

<!--NeedCopy-->
```

Mac

Para probar la configuración definida por el administrador en un dispositivo Mac, los usuarios deben seguir estos pasos.

1. Defina el nombre del canal de prueba de Global App Configuration Service mediante este comando:

```
defaults write com.citrix.receiver.nomas GACSChannelName
   testrolloutchannel1

<!--NeedCopy-->
```

2. Reinicie Citrix Workspace Helper con estos comandos:

```
launchctl unload /Library/LaunchAgents/com.citrix.ReceiverHelper.
   plist

launchctl load /Library/LaunchAgents/com.citrix.ReceiverHelper.
   plist

<!--NeedCopy-->
```

Una vez reiniciado el dispositivo, la configuración del canal de prueba se obtiene automáticamente.

iOS

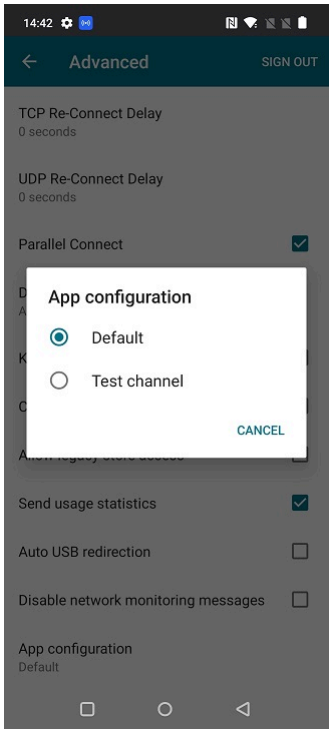
Para probar la configuración definida por el administrador en un dispositivo iOS, proceda de esta manera.

1. Inicie sesión en la aplicación Citrix Workspace.
2. Vaya a **Parámetros** > **Avanzado** > **Configuración de la aplicación**.
3. Seleccione el canal de prueba.
4. Ya puede probar la configuración definida por el administrador.

Android

Para probar la configuración definida por el administrador en un dispositivo Android, proceda de esta manera.

1. Inicie sesión en la aplicación Citrix Workspace.
2. Vaya a **Parámetros** > **Avanzado** > **Configuración de la aplicación**.
3. Seleccione el canal de prueba.
4. Ya puede probar la configuración definida por el administrador.



Gestionar la experiencia en los espacios de trabajo

November 21, 2023

Este artículo ofrece una descripción general de cómo los suscriptores pueden acceder a sus espacios de trabajo e interactuar con ellos. Analiza las opciones de personalización para mejorar la experiencia del espacio de trabajo y proporciona soluciones para problemas comunes.

Acceso a Workspace

Los suscriptores pueden acceder a Citrix Workspace de dos maneras:

- A través de un explorador con la URL de Workspace.
- Con la aplicación Citrix Workspace, instalada en los dispositivos de los suscriptores.

Acceso con explorador

Los suscriptores deben usar la versión más reciente de Edge, Chrome, Firefox o Safari al iniciar sesión a través del explorador web. Los usuarios pueden introducir su URL de Workspace para acceder a sus espacios de trabajo. Para obtener más información, consulte Workspace Browser Compatibility.

La URL del espacio de trabajo está habilitada de forma predeterminada, normalmente en el formato: `https://yourcompanyname.cloud.com`. Para obtener información sobre cómo configurar la URL de Workspace, consulte URL del espacio de trabajo.

Acceso con la aplicación Citrix Workspace

Citrix recomienda utilizar la versión más reciente de la aplicación Citrix Workspace para acceder a los espacios de trabajo.

La aplicación Citrix Workspace es una aplicación instalada de forma nativa que sustituye a Citrix Receiver y proporciona una experiencia de usuario homogénea con la interfaz de usuario (IU) de Workspace en las distintas plataformas. La aplicación Citrix Workspace está disponible para varios sistemas operativos. Para obtener información detallada, consulte la documentación de producto de la aplicación Citrix Workspace.

Si ha estado utilizando Citrix Receiver, guíe a los usuarios para que la actualicen a la aplicación Citrix Workspace, de modo que puedan disfrutar de todas las funciones de la interfaz de usuario de Workspace. Para obtener más información acerca de las funciones admitidas en la aplicación Citrix Workspace por plataforma, consulte la Tabla de funciones de las aplicaciones Workspace.

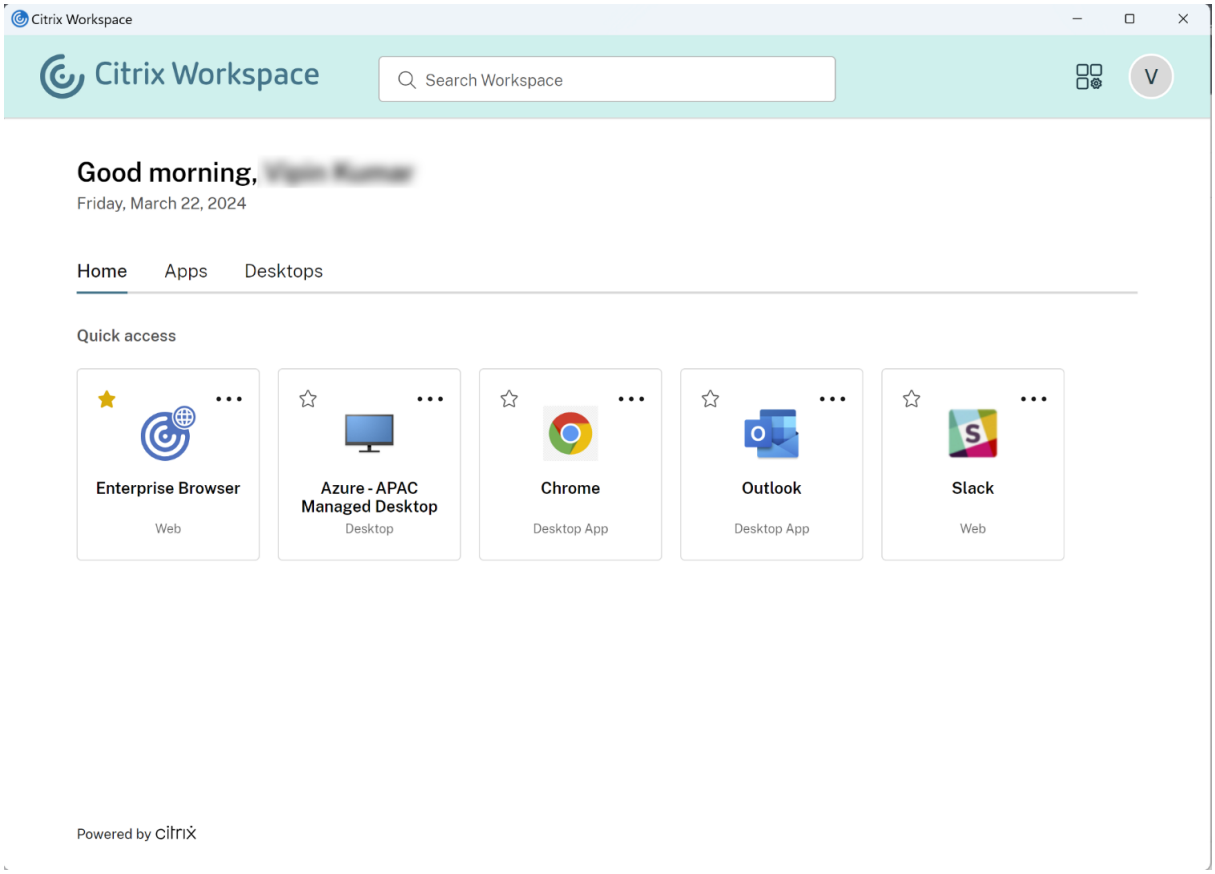
Para obtener información sobre cómo instalar la aplicación Citrix Workspace, consulte Descargar la aplicación Citrix Workspace.

Para los dispositivos donde no se puede instalar el software de la aplicación Citrix Workspace, la aplicación Citrix Workspace para HTML5 ofrece una conexión a través de un explorador compatible con HTML5.

Interfaz de usuario y funciones de Workspace

Nuevos clientes. Si es la primera vez que utiliza los espacios de trabajo, obtendrá la versión más reciente de la interfaz de usuario cuando esté disponible.

Clientes existentes. Si ha estado utilizando una versión anterior de la aplicación Citrix Workspace, la interfaz de usuario actualizada puede tardar unos cinco minutos en mostrarse. Puede que, temporalmente, aún vea la versión anterior de la interfaz de usuario.



La interfaz de usuario de Citrix Workspace presenta estas funciones:

Single Sign-On (SSO)

Citrix Workspace ofrece una experiencia de "inicio de sesión único"(Single Sign-On/SSO) fluida para acceder a los recursos secundarios que, de otro modo, requerirían otra forma de autenticación.

Diseño de tarjeta

Las **aplicaciones**, los **escritorios**, los **archivos**, las **acciones** y el **feed de actividades** se presentan en un diseño de "tarjeta". Una ventana emergente muestra más detalles y acciones.

Parámetros

Los suscriptores acceden a **Parámetros** desde un menú que aparece cuando seleccionan el icono de su perfil en la esquina superior derecha de la interfaz de usuario de Workspace.

Icono del perfil

Los suscriptores pueden cargar una imagen para su perfil. Si no se establece una imagen para el perfil, se muestra de forma predeterminada un icono basado en el nombre simplificado del suscriptor en Active Directory.

Buscar

La herramienta de búsqueda situada en la parte superior de la interfaz de usuario busca en todos los recursos del espacio de trabajo y permite a los suscriptores abrir aplicaciones directamente desde los resultados de la búsqueda. La búsqueda requiere al menos tres caracteres.

Vista Recientes y Favoritos

Los suscriptores pueden elegir entre la vista **Recientes** y **Favoritos** de sus aplicaciones, escritorios y archivos.

Puede configurar **Favoritos** para que esta funcionalidad esté disponible o no para los suscriptores en **Configuración de Workspace**. Para obtener más información sobre cómo habilitar e inhabilitar la funcionalidad **Favoritos** en Citrix Workspace, consulte Permitir favoritos.

Autenticación de dos factores (opcional)

Antes de que los suscriptores puedan utilizar la autenticación de dos factores en Citrix Workspace, deben registrar su dispositivo. Durante el registro, Workspace presenta un código QR que el suscriptor puede escanear con una aplicación de autenticación. La aplicación de autenticación debe seguir el estándar "contraseña temporal de un solo uso"(TOTP), como Citrix SSO.

> **Nota:**
>
> Para seguir un proceso de registro sin problemas, Citrix recomienda, de antemano, descargar e instalar Citrix SSO en el dispositivo de destino.

Para registrarse en la autenticación de dos factores, indique al suscriptor que:

1. Abra un explorador web, vaya a la página de inicio de sesión de Workspace y seleccione **¿No tiene un token?**
2. Introduzca su nombre de usuario en formato `domain\username` o la dirección de correo electrónico de su empresa y seleccione **Siguiente**. A continuación, Citrix Cloud enviará al suscriptor un correo electrónico con un código de verificación temporal.

3. Introduzca el código de verificación y la contraseña de la cuenta de Active Directory cuando se le solicite y seleccione **Siguiente**.

   > **IMPORTANTE:**
   >
   > El código de verificación es un token temporal con un período de validez de 24 horas y solo se usa para registrar el dispositivo del suscriptor. El suscriptor no debe usar este código para iniciar sesión en su espacio de trabajo con la autenticación de dos factores.

4. Desde la aplicación de autenticación, escanee el código QR o introduzca el código de verificación manualmente.
5. Seleccione **Finalizar** e **Iniciar sesión** para completar el registro.

Una vez completado el registro, los suscriptores pueden volver a la página de inicio de sesión de Citrix Workspace e introducir sus credenciales de Active Directory, junto con el token de la aplicación de autenticación.

Solo los códigos de verificación generados a partir de una aplicación de autenticación en un dispositivo inscrito son tokens compatibles con la autenticación de dos factores. Los suscriptores no deben usar el token de correo electrónico temporal enviado durante el proceso de registro.

Personalizar los espacios de trabajo

En **Configuración de Workspace**, puede personalizar la experiencia del suscriptor de los espacios de trabajo para diferentes usuarios y para cumplir con los requisitos organizativos específicos.

- Para configurar las notificaciones selectivas de la tarjeta **Feed de actividades** y **Acciones** de los espacios de trabajo, consulte Personalizar las notificaciones del espacio de trabajo.
- Para personalizar la apariencia de los espacios de trabajo, incluidos los logotipos y los temas personalizados, consulte Personalizar la apariencia de los espacios de trabajo.
- Para elegir cómo interactúan los suscriptores con sus espacios de trabajo, como permitir que los suscriptores creen **Favoritos** e inicien escritorios automáticamente, consulte Personalizar las interacciones en espacios de trabajo.
- Para personalizar las directivas de privacidad y seguridad, consulte Personalizar las directivas de seguridad y privacidad. Las directivas de privacidad y seguridad incluyen parámetros como el período de tiempo de espera, la directiva de inicio de sesión y la administración de contraseñas para los usuarios finales.

Solución de problemas

Cerrar sesión y volver a iniciarla después de cambiar el método de autenticación

Después de cambiar el método de autenticación, es posible que a los suscriptores que ya están conectados a una sesión se les muestre un mensaje de error. Para iniciar sesión nuevamente, los suscriptores deberán cerrar sesión en Citrix Workspace y cerrar el explorador o la aplicación Citrix Workspace y esperar aproximadamente 5 minutos. A continuación, los suscriptores podrán iniciar sesión con el nuevo método de autenticación.

Para obtener más información, consulte Elegir o cambiar los métodos de autenticación.

Actualizar después de hacer cambios en la suscripción a los servicios

Si ha cambiado la suscripción a los servicios, es posible que los suscriptores tengan que actualizar manualmente la aplicación Citrix Workspace local. Para actualizar la aplicación Citrix Workspace para Windows:

1. En la bandeja del sistema de Windows, haga clic con el botón secundario en el icono de Citrix Workspace y seleccione **Preferencias avanzadas > Restablecer Citrix Workspace**.
2. Abra la aplicación Citrix Workspace para Windows y seleccione **Cuentas > Agregar**.
3. Introduzca la URL del espacio de trabajo y, a continuación, seleccione **Agregar**.

También puede actualizar la aplicación Citrix Workspace desde el explorador. Si se actualiza desde el explorador:

1. En la bandeja del sistema de Windows, haga clic con el botón secundario en el icono de Citrix Workspace y seleccione **Preferencias avanzadas > Restablecer Citrix Workspace**.
2. Introduzca la URL del espacio de trabajo en el explorador e inicie sesión.
3. Descargue el archivo de configuración desde **Parámetros > Parámetros de cuenta > Avanzado > Descargar configuración de Workspace**.

Se descargará un archivo con la extensión **CR** que agrega el espacio de trabajo a la aplicación Citrix Workspace local.

Personalizar la apariencia de los espacios de trabajo

October 12, 2023

Personalizar la interfaz de usuario de Workspace

En esta sección, se describe cómo se puede personalizar la apariencia de los espacios de trabajo actualizando los temas en **Configuración > Personalizar > Apariencia**.

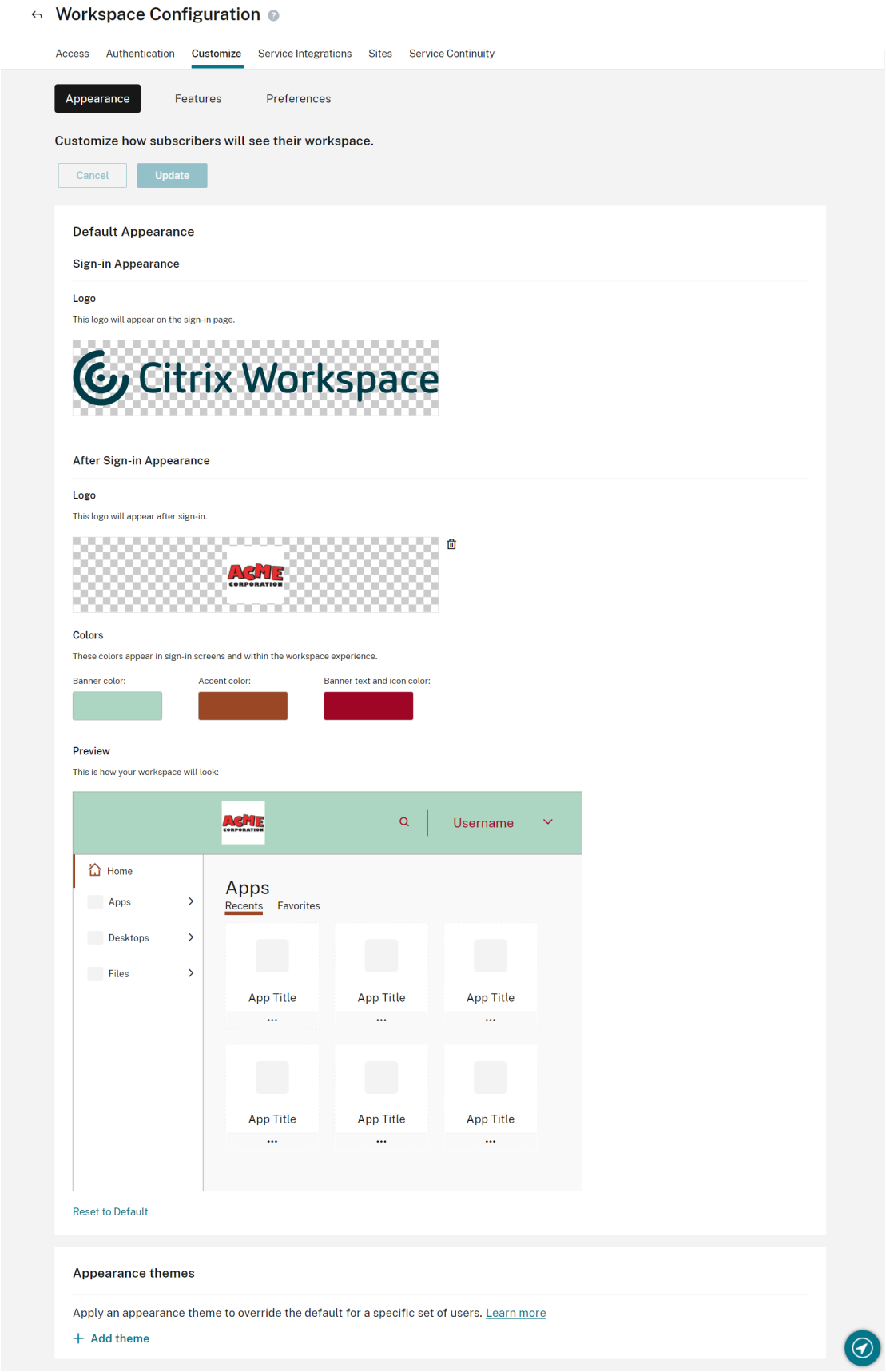
Los temas le permiten configurar los colores y logotipos de su espacio de trabajo. Los logotipos deben cumplir con las dimensiones requeridas para evitar que aparezcan distorsionados o que den lugar a mensajes de error.

Logotipo	Dimensiones requeridas	Tamaño máximo	Formatos de archivo admitidos
Logotipo de inicio de sesión	480 x 120 píxeles	2 MB	JPEG, JPG o PNG
Logotipo posterior al inicio de sesión	340 x 80 píxeles	2 MB	JPEG, JPG o PNG

Los cambios en la apariencia del espacio de trabajo surten efecto inmediatamente después de seleccionar **Guardar**.

Personalizar el tema predeterminado

El tema predeterminado incluye el logotipo de inicio de sesión, el logotipo del espacio de trabajo y los colores que los suscriptores ven después de iniciar sesión. Puede cambiar uno, varios o todos estos elementos del tema predeterminado.



Personalizar la apariencia de inicio de sesión

Para la página de inicio de sesión, solo puede reemplazar el logotipo. El resto de la página de inicio de sesión, incluidos los colores, no se verá afectado.

Los cambios en la apariencia del espacio de trabajo tienen efecto inmediatamente. La interfaz de usuario actualizada puede tardar unos cinco minutos en mostrarse en las aplicaciones Citrix Receiver locales.

> **Nota:**
>
> Los cambios en el logotipo de inicio de sesión no afectan a los usuarios que se autentican en su espacio de trabajo a través de proveedores de identidades de terceros, como Azure AD y Okta.
>
> Para obtener información sobre cómo personalizar una página de inicio de sesión de Azure AD, consulte la documentación de Microsoft. Para obtener información sobre cómo personalizar la página de inicio de sesión alojada por Okta, consulte la documentación para desarrolladores de Okta.

También puede personalizar la página de inicio de sesión de Citrix Gateway local, configurada en el dispositivo Citrix ADC en lugar de en **Configuración de Workspace**. Para obtener más información, consulte el artículo de asistencia de Knowledge Center.

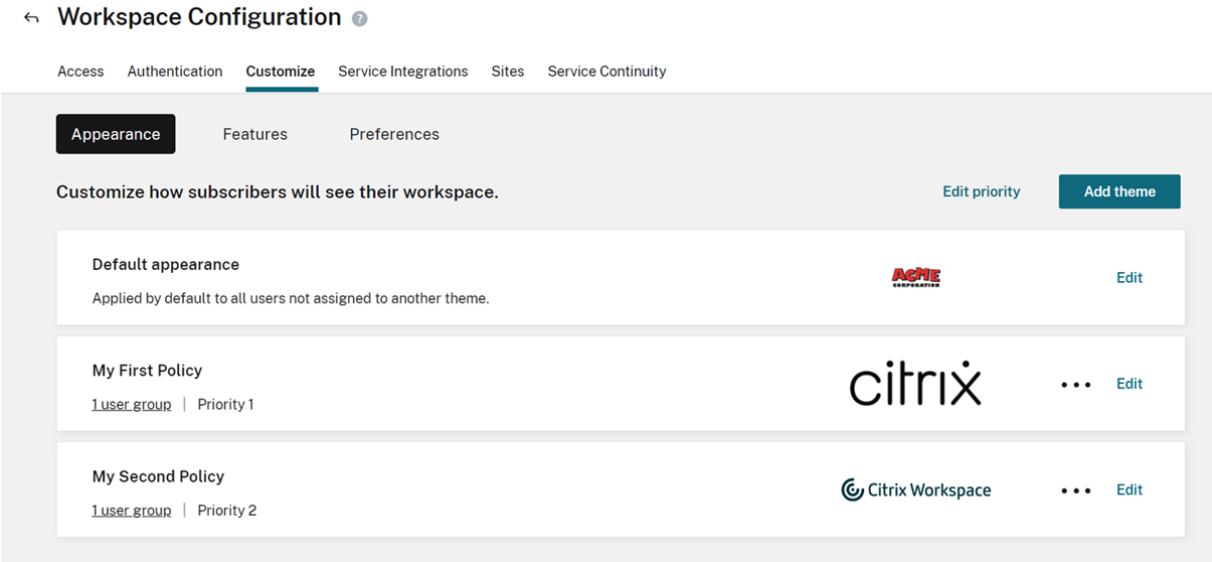
Personalizar la apariencia del espacio de trabajo

El logotipo de inicio de sesión no tiene por qué ser el mismo que el logotipo que aparece en la parte superior izquierda del espacio de trabajo después de que un suscriptor inicie sesión. Además de reemplazar el logotipo del espacio de trabajo, puede definir la pancarta, el énfasis y los colores de texto e icono del espacio de trabajo.

Crear varios temas personalizados

> **Importante:**
>
> Esta es una **función de arrendatario único**. Si el cliente es un arrendatario de Citrix Service Provider, debe tener su propia ubicación de recursos, Cloud Connectors y dominio dedicado de Active Directory. En la actualidad, no se admiten arrendatarios de Citrix Service Provider que compartan una ubicación de recursos, Cloud Connectors y un dominio dedicado de Active Directory (multiarrendatario).

Puede configurar y priorizar varios temas de Citrix Workspace para grupos de usuarios específicos. Estos temas personalizados se indican en tarjetas individuales bajo el tema predeterminado. Si no configura varios temas, se aplicará el tema existente (predeterminado) a todos los usuarios.



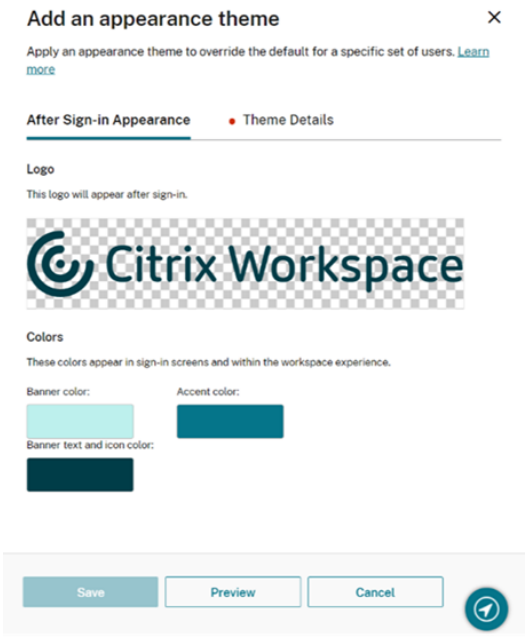
Configurar temas personalizados

Para agregar el primer tema personalizado bajo el tema predeterminado, seleccione **Agregar tema** en la parte inferior izquierda de la tarjeta, en la sección **Apariencia predeterminada**.

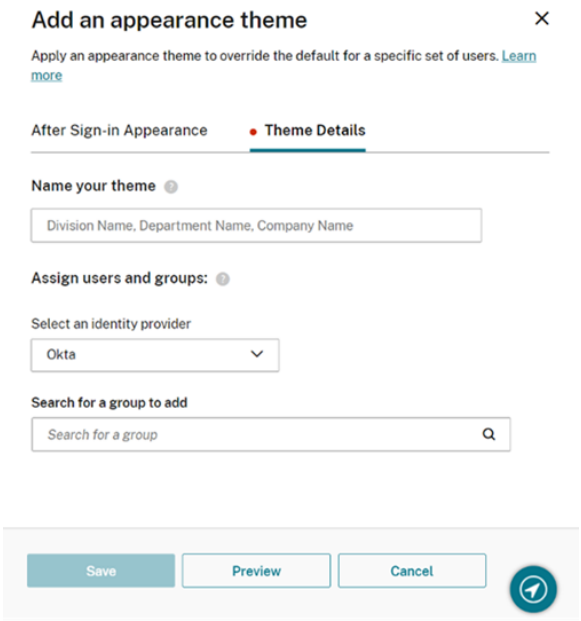
Si ya tiene al menos un tema personalizado bajo el tema predeterminado, seleccione **Agregar tema** en la parte superior derecha de la lista de temas existentes.

1. Configure el tema personalizado:

    a) Cargue el **logotipo** (opcional).
    b) Defina la pancarta, el énfasis y los **colores** de texto e icono (opcional).



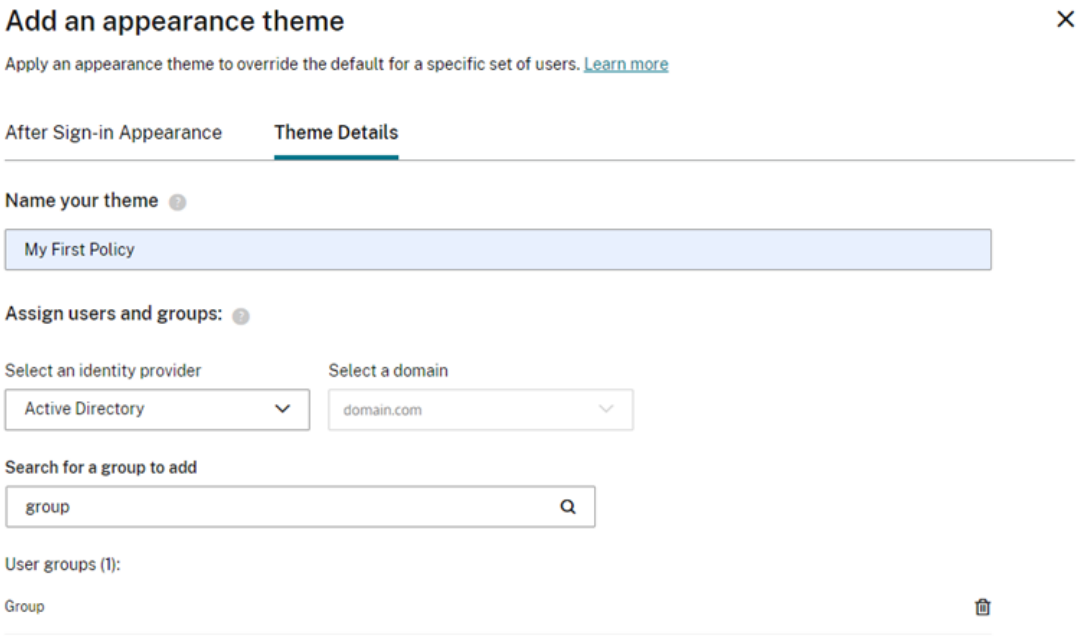
2. Seleccione **Detalles del tema** e introduzca un nombre representativo para el mismo.



3. Asigne grupos de usuarios al tema:

    a) Seleccione un proveedor de identidades y su dominio si se le solicita.
    b) Busque el grupo de usuarios que quiere agregar al tema personalizado.

c) Seleccione el botón de signo más (**+**) situado junto a ese grupo.
d) Repita este proceso para cada grupo que quiera agregar al tema.



4. Seleccione **Vista previa** para ver el aspecto del espacio de trabajo para los suscriptores. Cuando haya terminado, guarde el tema.

> **Nota:**
>
> **Vista previa del espacio de trabajo** no muestra una vista previa si actualmente está trabajando con la interfaz de usuario morada más antigua.

5. Repita los pasos 1 a 4 para seguir agregando nuevos temas personalizados.

Priorizar temas personalizados

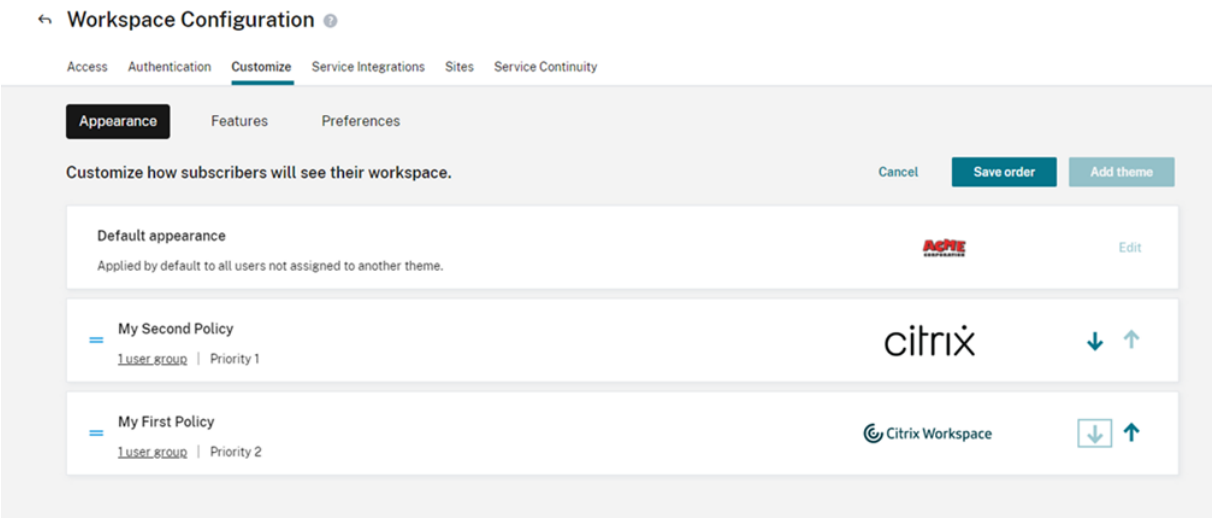
Un usuario puede pertenecer a varios grupos de usuarios, a cada uno de los cuales puede corresponder un tema diferente. Puede definir qué tema verá un suscriptor si hay más de uno, estableciendo la prioridad de los diferentes temas personalizados.

> **Importante**
>
> Para que funcione la priorización relativa de los temas personalizados, debe configurar dos o más temas personalizados bajo el tema predeterminado.

1. Seleccione **Modificar prioridad** en la parte superior derecha de la lista de temas, junto a **Agregar tema**.
2. Puede reordenar la prioridad de los temas de una de estas dos maneras:

- Utilice las flechas situadas en el lado derecho de cada tema.
- Arrastre los temas individuales hacia arriba y hacia abajo en la lista con el asa situada en el lado izquierdo de la tarjeta.

3. Una vez que haya reordenado los artículos, seleccione **Guardar orden**.



Personalizar las interacciones en espacios de trabajo

November 21, 2023

Puede personalizar el modo en que los suscriptores interactúan con su espacio de trabajo desde **Configuración de Workspace> Personalizar > Preferencias**.

Si quiere personalizar las preferencias del espacio de trabajo que afectan a la experiencia de inicio de sesión para adaptarla a los requisitos de su empresa, consulte Personalizar las directivas de seguridad y privacidad del espacio de trabajo.

Si quiere personalizar la apariencia del espacio de trabajo previa y posterior al inicio de sesión, consulte Personalizar la apariencia de los espacios de trabajo

Permitir almacenamiento en caché

El parámetro **Permitir almacenamiento en caché** mejora el rendimiento para los suscriptores que acceden a Citrix Workspace a través de un explorador web. El almacenamiento en caché está disponible al acceder a Citrix Workspace con un explorador web compatible. El almacenamiento en caché no está disponible cuando se utiliza una aplicación Citrix Workspace instalada localmente.

Cuando se habilite el almacenamiento en caché, es posible que algunos datos confidenciales se almacenen localmente en los dispositivos de los suscriptores. Estos datos constan de metadatos de archivo y se cifran con una clave que es exclusiva de la identidad autenticada del suscriptor. Los datos cifrados se almacenan en la propiedad `localStorage` del explorador web, en el dispositivo del suscriptor.

Si inhabilita el almacenamiento en caché, los datos cifrados se purgarán la próxima vez que el suscriptor inicie sesión en Citrix Workspace a través de su explorador web. Además, el suscriptor puede purgar estos datos manualmente borrando los datos de navegación de su explorador web.

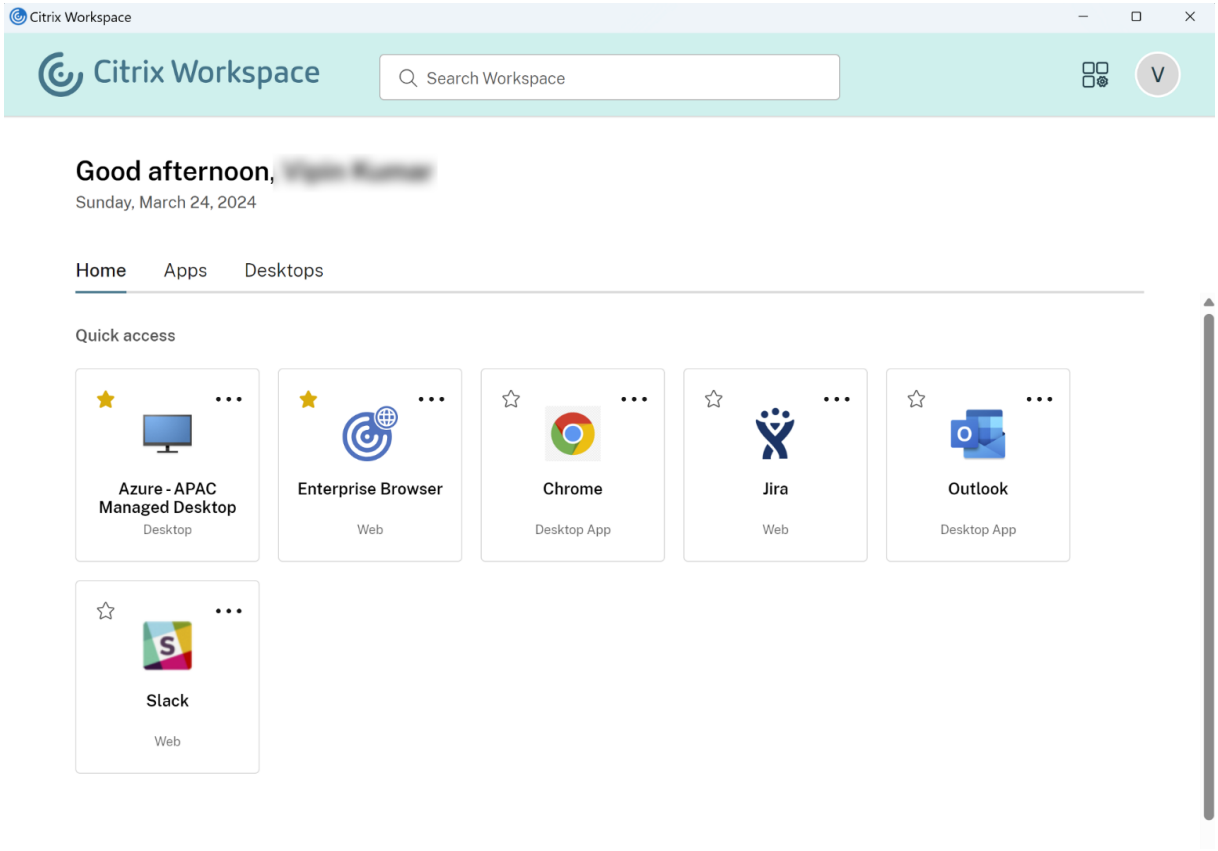
Permitir favoritos

Los clientes que tienen acceso a **Configuración de Workspace** y a la nueva experiencia de Workspace pueden permitir a los suscriptores establecer como favoritos y no favoritos recursos de aplicaciones y escritorios. La función **Permitir favoritos** está habilitada de forma predeterminada.

> **Nota:**
>
> - Para algunos clientes (que empezaron a usar Workspace entre diciembre de 2017 y abril de 2018), la opción **Permitir favoritos** está **inhabilitada** de manera predeterminada. El administrador puede decidir cuándo habilitar esta función para sus suscriptores.

La experiencia del suscriptor con Permitir favoritos

Cuando está habilitada (predeterminado), los suscriptores pueden agregar hasta 250 **favoritos** mediante el icono de estrella situado en la esquina superior izquierda de cada tarjeta (no obligatoria) de aplicación y escritorio. La estrella cambia de no tener relleno a un relleno amarillo cuando se incluye en favoritos.



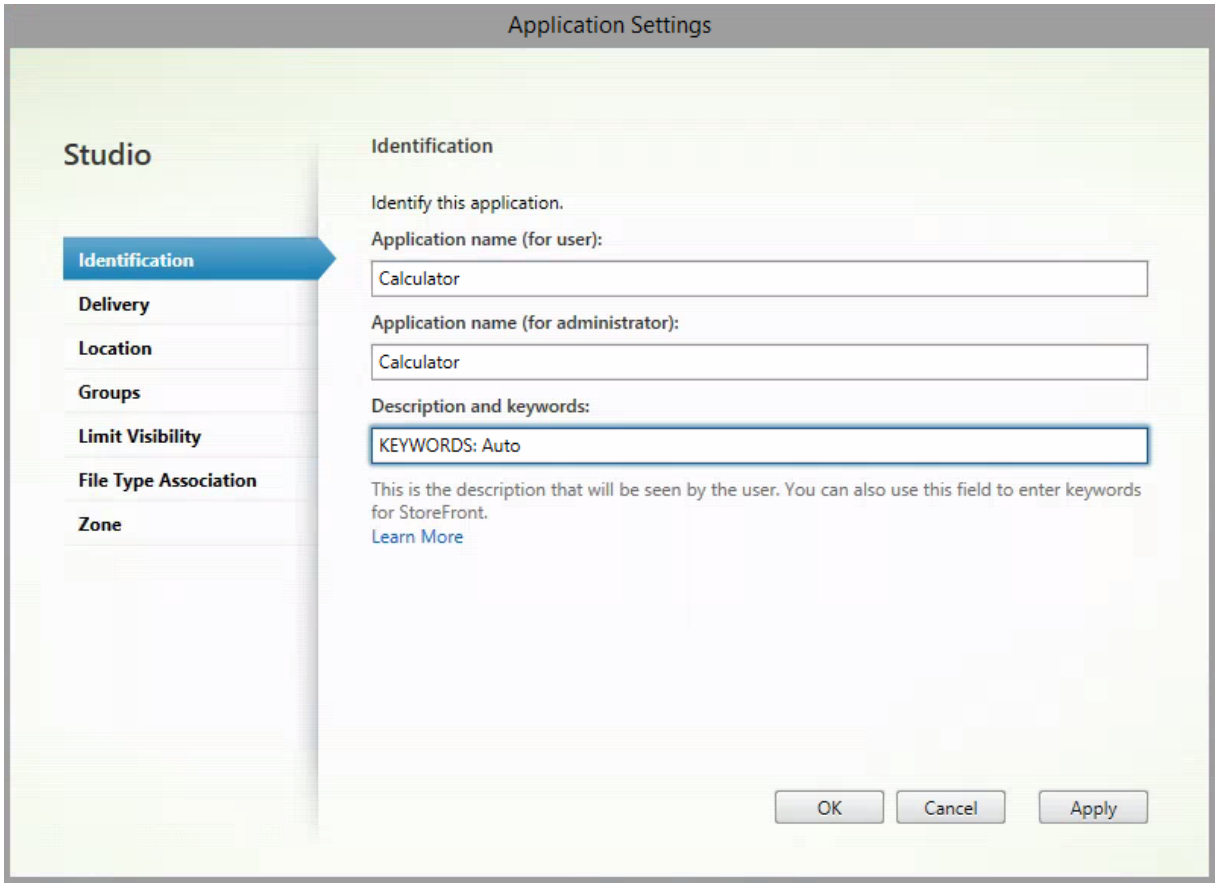
Si un suscriptor agrega más de 250 recursos a favoritos, se quitará el "recurso favorito más antiguo" (o el que más se aproxime para conservar los **Favoritos** más recientes).

Cuando se inhabilita, los suscriptores de espacios de trabajo no pueden ver estrellas en las tarjetas de aplicaciones y escritorios, ni en los submenús **Todas las aplicaciones** y **Favoritos** de estos recursos en la barra de navegación. Los **Favoritos** de aplicaciones y escritorios no se eliminan y pueden recuperarse si vuelve a habilitar **Favoritos**.

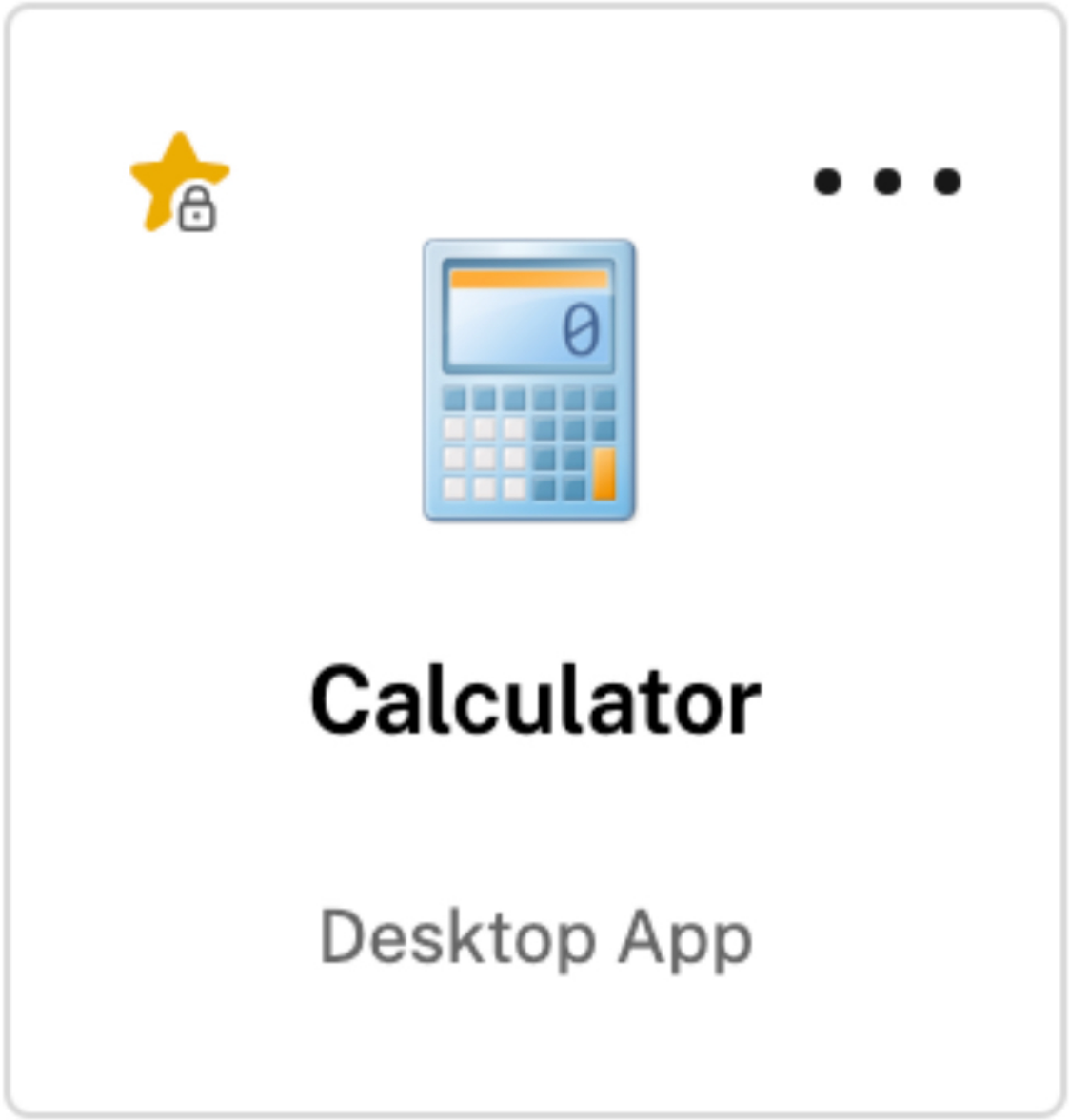
> **Nota:**
>
> Si sus suscriptores no tienen acceso a escritorios configurados, no aparecerá la selección de escritorios en la barra lateral.

Palabras clave de aplicaciones y escritorios

Los administradores pueden agregar automáticamente **Aplicaciones favoritas** para los suscriptores mediante los parámetros `KEYWORDS:Auto` y `KEYWORDS:Mandatory` en Citrix DaaS (**Administrar** > **Configuración completa** > **Aplicaciones**).



- **KEYWORDS:Auto**. La aplicación o escritorio se agregan como **favoritos** y los suscriptores pueden quitarlos de los **favoritos**.
- **KEYWORDS:Mandatory**. La aplicación o escritorio se agregan como **favoritos** y los suscriptores no pueden quitarlos de los **favoritos**. Las aplicaciones y escritorios obligatorios muestran un icono de estrella con un candado para indicar que no se puede quitar de los favoritos.



> **Nota:**
>
> Si utiliza ambas palabras clave, **Mandatory** y **Auto**, para una aplicación, la palabra clave **Mandatory** invalida a la palabra clave **Auto** y la aplicación o escritorio favoritos no se pueden quitar.

Para un suscriptor con acceso solo a aplicaciones y escritorios que tienen la palabra clave **Mandatory** :

- El suscriptor solo puede ver la página **Aplicaciones** en el panel de navegación izquierdo en Workspace. La página **Favorito** no aparece en el panel izquierdo porque no hay diferencia entre las aplicaciones que aparecen en la página **Aplicaciones** y en la página **Favorito**.
- El suscriptor no puede ver la ficha **Favorito** en la página de inicio. Solo se muestra la ficha

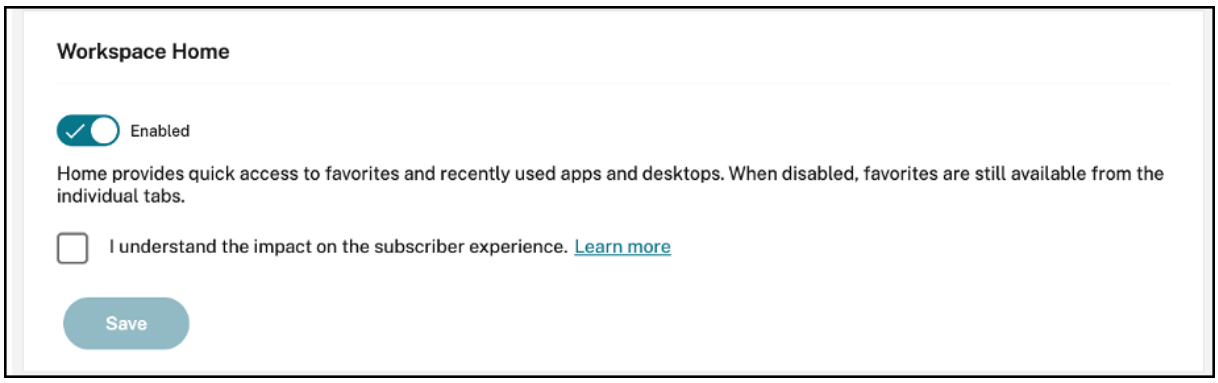
Recientes.

Habilitar o inhabilitar la pantalla de inicio para los usuarios (Technical Preview)

Es posible habilitar o inhabilitar la página de **inicio** para que los puedan organizar mejor sus aplicaciones.

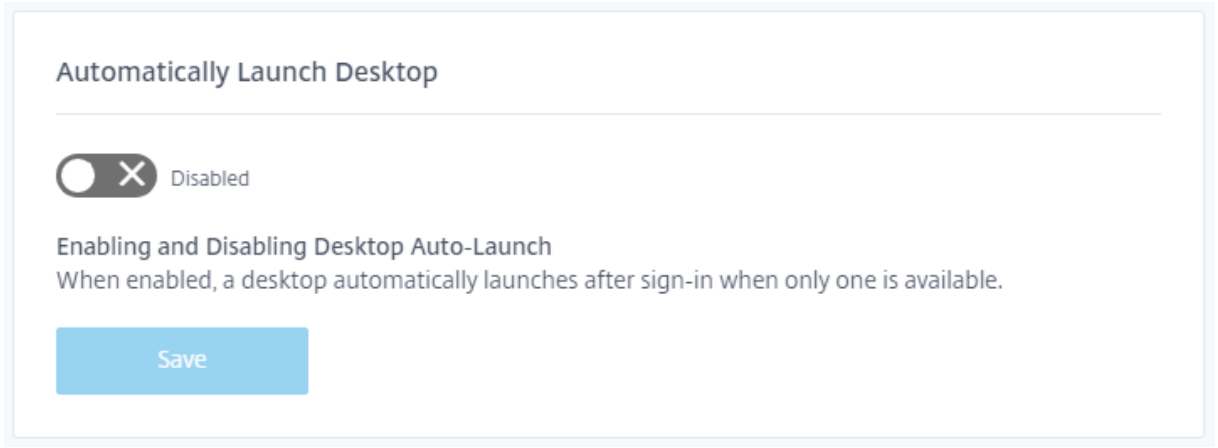
Esta función es aplicable cuando los usuarios tienen más de 20 aplicaciones en sus escritorios. Si los usuarios tienen 20 aplicaciones o menos, verán una sola vista sin opciones de navegación ni búsqueda.

Para configurar los ajustes, vaya a **Configuración de Workspace > Personalizar > Apariencia**. Cuando la opción está activada, los usuarios acceden a la página de **inicio**. Si se desactiva la opción, los usuarios acceden directamente a la página **Aplicaciones**. De forma predeterminada, la opción está activada y la función habilitada.



Iniciar escritorio automáticamente

La opción **Iniciar escritorio automáticamente** está disponible para los clientes que tienen acceso a la **Configuración de Workspace** y a la nueva experiencia de Workspace. La preferencia solo se aplica al acceso al espacio de trabajo desde exploradores web.



Cuando está inhabilitado (valor predeterminado), el parámetro impide que Citrix Workspace inicie automáticamente un escritorio cuando un suscriptor inicia sesión. Los suscriptores deben iniciar su escritorio manualmente después de iniciar sesión.

Cuando está habilitado, si un suscriptor tiene solo un escritorio disponible, el escritorio se inicia automáticamente cuando el suscriptor inicia sesión en su espacio de trabajo.

Las aplicaciones del suscriptor no se vuelven a conectar, independientemente de la configuración de control del espacio de trabajo.

> **Nota:**
>
> Para permitir que Citrix Workspace inicie los escritorios automáticamente, los suscriptores que acceden al sitio mediante Internet Explorer deben agregar la URL de Workspace a las zonas de Intranet local o Sitios de confianza.

Sesiones de proveedores de identidad federada

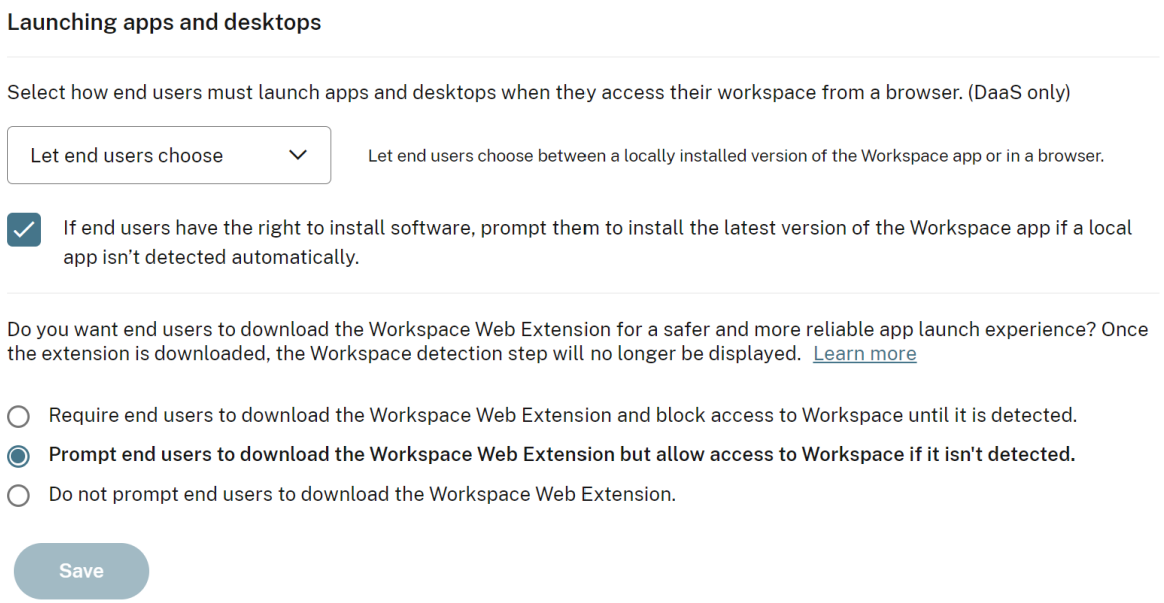
Cuando Workspace está configurado para usar un proveedor de identidades federadas, la sesión de autenticación y su duración suelen estar controladas por el proveedor de identidades. El parámetro **Sesiones de proveedores de identidad federada** permite transferir el control al proveedor de servicios. Al habilitarse (de forma predeterminada), Workspace fuerza una solicitud de inicio de sesión con el proveedor de identidades cuando se necesita una nueva sesión de Workspace. Al inhabilitarse, no se le solicitará al suscriptor que se autentique con el proveedor de identidades si accede a Workspace con una sesión válida.

Si el parámetro está habilitado y utiliza Azure AD para la autenticación en el espacio de trabajo, es posible que se pida a los suscriptores que inicien sesión de nuevo, incluso si existe un token de autenticación de Microsoft válido para la sesión. Para obtener más información sobre este supuesto, consulte CTX253779.

Inicio de aplicaciones y escritorios

El parámetro para **iniciar aplicaciones y escritorios** está disponible para aquellos clientes que tienen acceso a **Configuración de Workspace** y a la nueva experiencia de Workspace. La preferencia está disponible para clientes nuevos y existentes. Sin embargo, la introducción de esta función no cambia ninguna configuración para los clientes existentes.

La preferencia se aplica solo a la forma en que los usuarios abren las aplicaciones y los escritorios que ofrezca **Citrix DaaS**. Puede ser el servicio **Citrix DaaS** o la instalación local con la función Agregación de sitios. **Iniciar aplicaciones y escritorios** no se aplica, por ejemplo, a las aplicaciones SaaS entregadas por Citrix Gateway Service.



Elija una de las siguientes opciones:

- **En una aplicación nativa** (valor predeterminado): Los usuarios finales deben usar una versión instalada localmente de la aplicación Workspace.
- **En un explorador Web:** Los usuarios finales deben usar una versión para explorador de la aplicación Workspace para HTML5.
- **Dejar que los usuarios elijan:** Los usuarios finales pueden elegir entre una versión instalada localmente de la aplicación Workspace o iniciar las aplicaciones y escritorios en un explorador web.

Una opción adicional para los parámetros **En una aplicación nativa** y **Dejar que los usuarios elijan** solicita a los usuarios que instalen la versión más reciente de la aplicación Citrix Workspace si no se detecta automáticamente ninguna aplicación local. Desmarque esta opción si los suscriptores no tienen derecho a instalar software.

Integrar Microsoft Teams en Workspace

Con la integración de Microsoft Teams, los suscriptores pueden compartir tarjetas de sus **feeds de actividades** de Workspace con otros suscriptores a través de canales en Microsoft Teams.

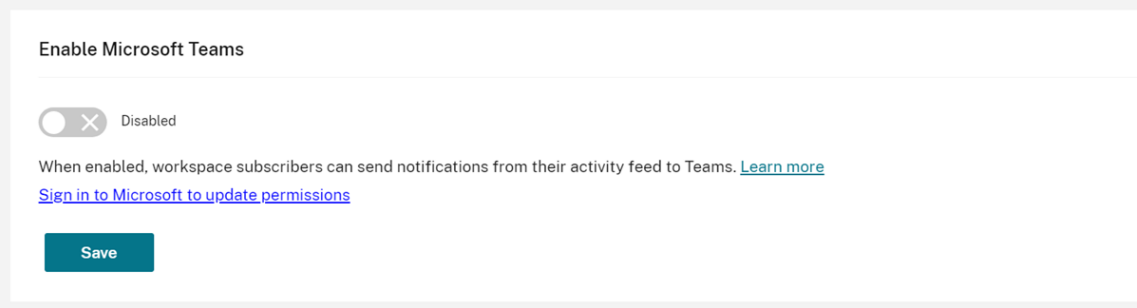
Requisitos

- Debe ser un administrador con **acceso total** en Citrix Cloud para habilitar la integración de Microsoft Teams. Los administradores con **acceso personalizado** no tienen los permisos necesarios para habilitar la integración de Microsoft Teams.

- Debe configurar la autenticación de Azure AD en **Administración de acceso e identidad**. Para obtener más información sobre cómo configurar la autenticación de Azure AD, consulte Conectar Azure Active Directory a Citrix Cloud.
- Solo puede utilizar una instancia de Azure AD con Microsoft Teams. Si la instancia de Azure AD que configure tiene Microsoft Teams habilitado a través de otra cuenta de Citrix Cloud, no puede habilitar la integración de Microsoft Teams para su cuenta de Citrix Cloud.
- La funcionalidad **IwsMicrosoftTeams** debe estar habilitada.
- Debe tener habilitada la función **Feed de actividades y acciones** para los espacios de trabajo.
- Los suscriptores de los espacios de trabajo deben tener instalado el cliente de escritorio de Microsoft Teams.

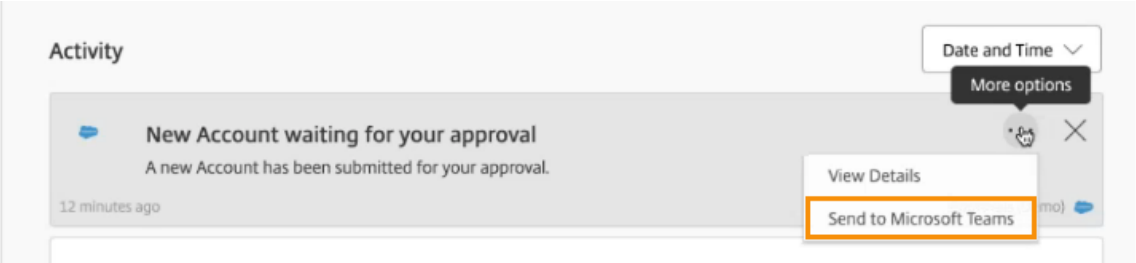
Habilitar la integración de Microsoft Teams

1. Después de iniciar sesión en Citrix Cloud, seleccione **Configuración de Workspace**.
2. Seleccione **Personalizar** y, a continuación, la ficha **Preferencias**.
3. En **Habilitar Microsoft Teams**, active la opción.



4. Seleccione **Guardar**.

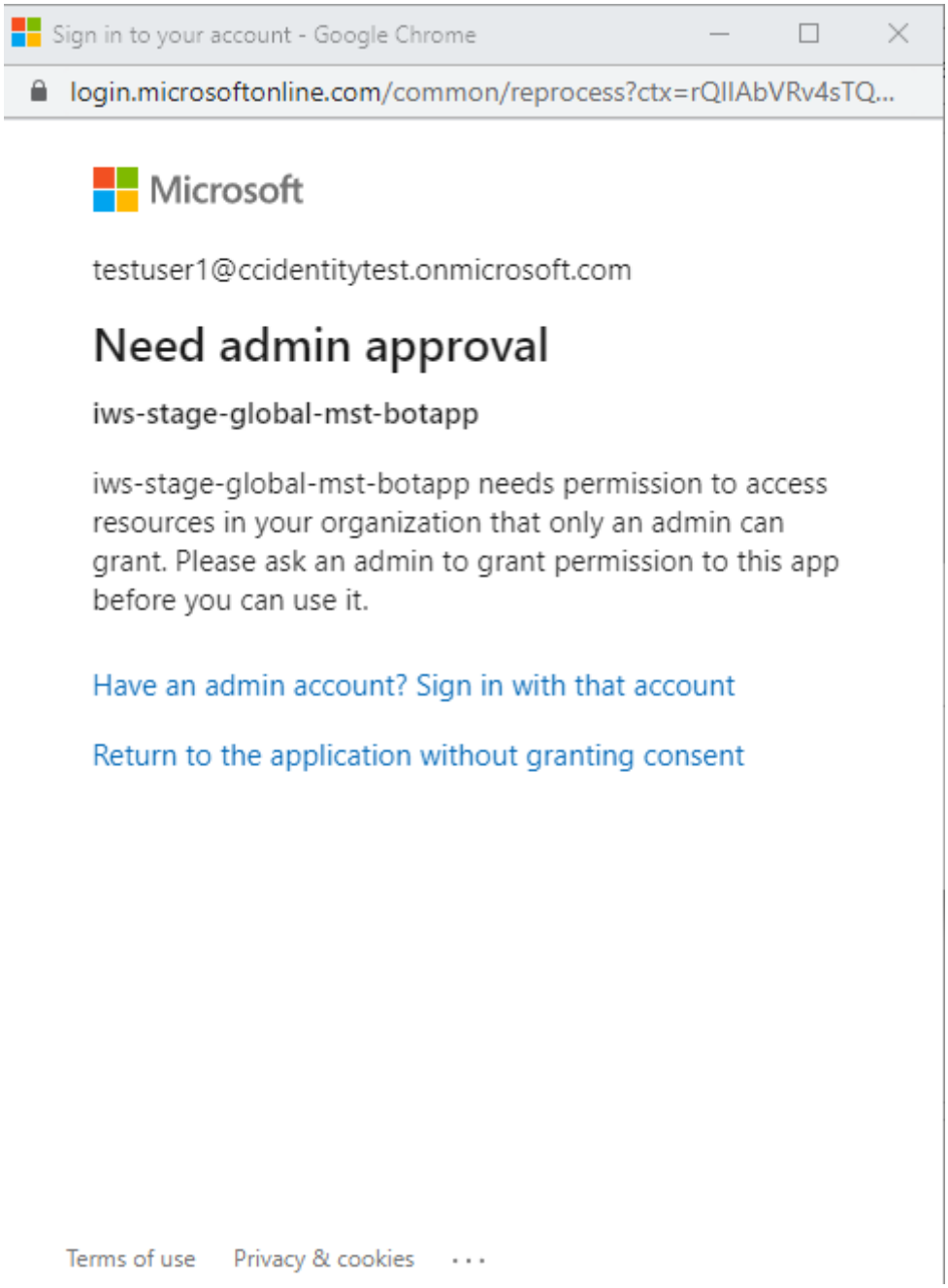
   Los usuarios de Workspace ahora pueden ver la opción **Enviar a Microsoft Teams** y compartir tarjetas desde Workspace. Es posible que los usuarios tengan que actualizar sus pantallas (Ctrl+F5).



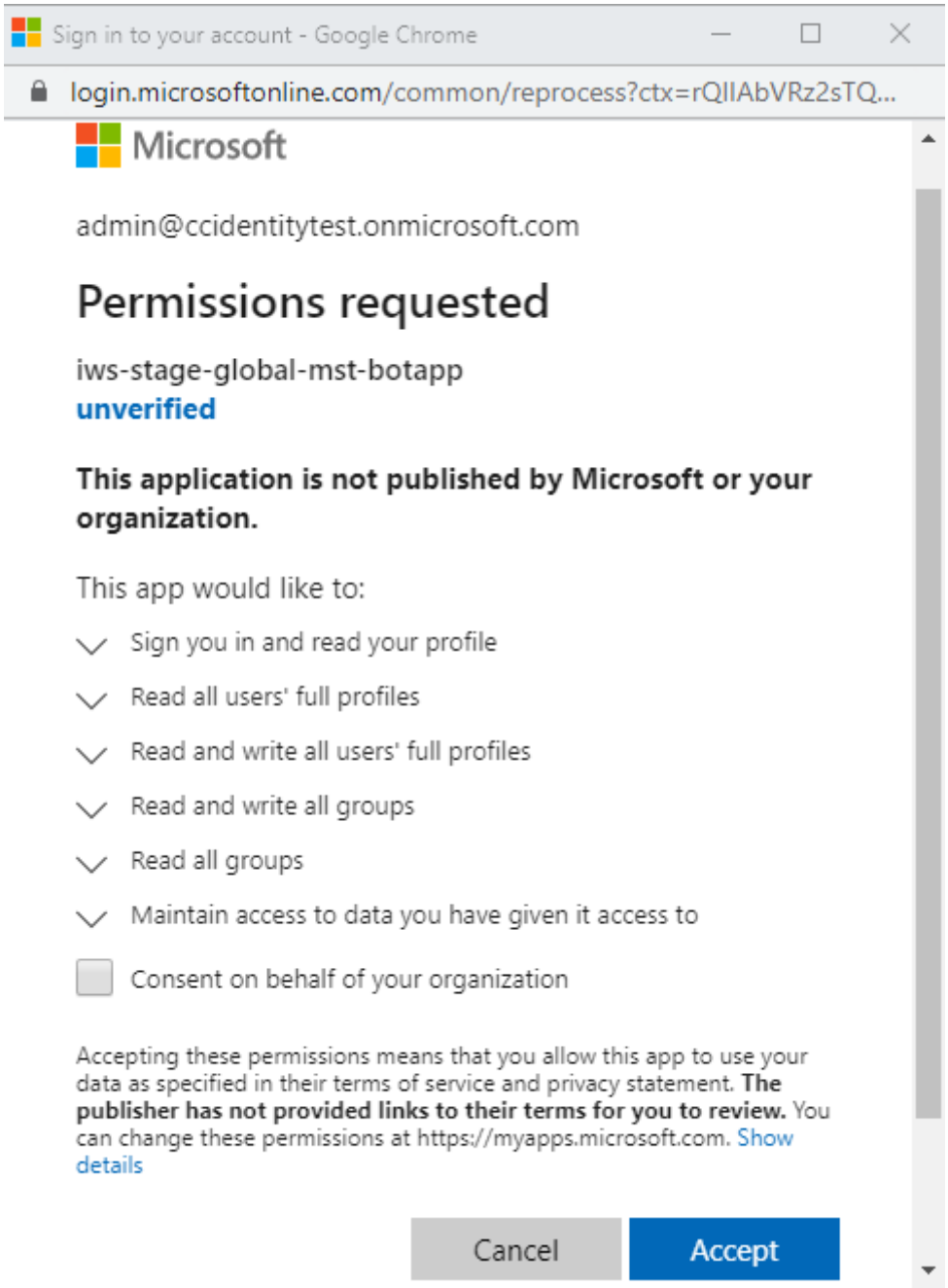
Aceptar permisos de Workspace

Hay otros pasos de configuración que es necesario seguir para habilitar esta integración. La cuenta de **administrador de Microsoft** debe aceptar los permisos de la integración en la interfaz de usuario de Workspace para que los usuarios de su organización puedan compartir tarjetas con Microsoft Teams.

1. Inicie sesión en cualquier cuenta de espacio de trabajo e intente compartir una tarjeta.
2. Si la cuenta de **administrador de Microsoft** no ha aceptado permisos para la integración en Microsoft Teams e intenta iniciar sesión con una cuenta que no sea de administrador, aparece el siguiente mensaje:



3. Para aceptar permisos, inicie sesión en su cuenta de administrador seleccionando **Have an admin account? Sign in with that account**. Se necesitan los siguientes permisos de acceso a los datos para habilitar la integración de Microsoft Teams en Citrix Workspace:



4. Cuando se abra el cuadro de diálogo **Permissions accepted**, revise las opciones. La opción **Consent on behalf of your organization** concede permisos a todos los suscriptores de Workspace asociados a este administrador. De lo contrario, los permisos se conceden solo a la cuenta de administrador.
5. Seleccione **Aceptar**.

Personalizar las directivas de seguridad y privacidad

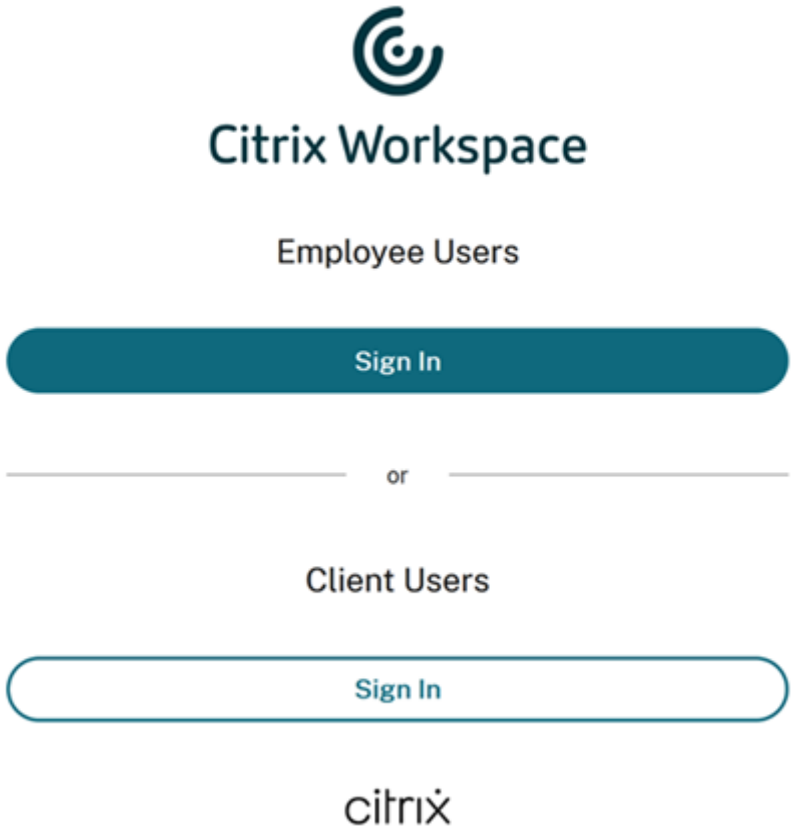
November 21, 2023

En este artículo se proporciona orientación sobre cómo personalizar la experiencia de inicio de sesión después de configurar el acceso y la autenticación del espacio de trabajo.

Para obtener una descripción general de los pasos necesarios para configurar el acceso y la autenticación del espacio de trabajo, consulte Configurar el acceso. Para obtener información sobre cómo configurar la autenticación de suscriptores en los espacios de trabajo, consulte Espacios de trabajo seguros.

Crear un flujo de inicio de sesión de usuario unificado

La experiencia de inicio de sesión predeterminada es una pantalla dividida para los usuarios empleados y los usuarios clientes (externos).

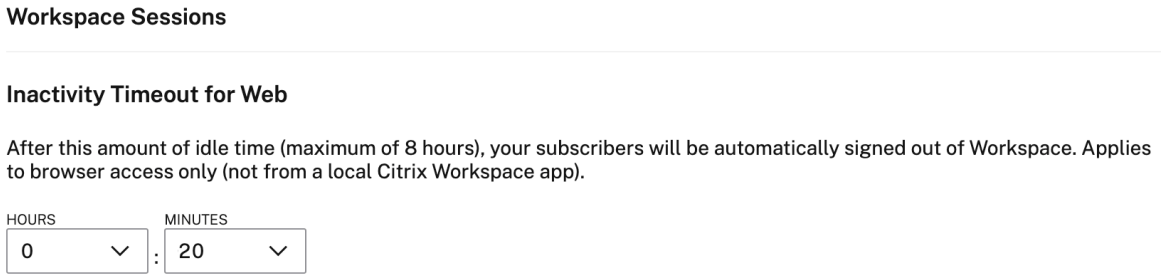


Para quitar la división de pantalla, vaya a **Configuración de Workspace > Autenticación > Flujo de inicio de sesión de usuario unificado** y seleccione **Habilitar**. Al habilitar esta función, se presenta a

todos los usuarios la misma opción de inicio de sesión.

Establecer el tiempo de espera por inactividad para dispositivos móviles y de escritorio en la web y en la aplicación Workspace

Utilice el parámetro **Tiempo de espera de inactividad para la web** de **Configuración de Workspace > Personalizar > Preferencias** para especificar la cantidad de tiempo de inactividad permitida (máximo de 8 horas) antes de que se desconecte automáticamente a los suscriptores de Citrix Workspace. También puede habilitar el tiempo de espera por inactividad para la aplicación Workspace en dispositivos móviles y de escritorio seleccionando la casilla de configuración correspondiente.

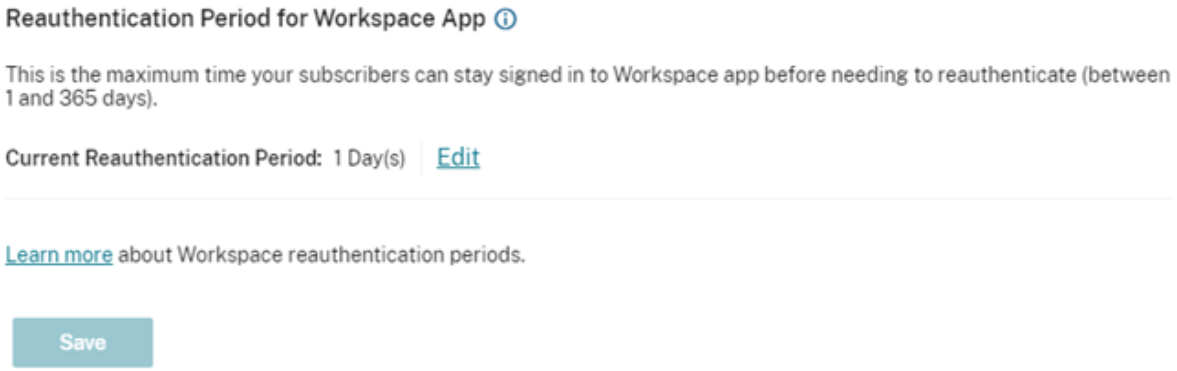


A diferencia del cierre manual de sesiones, que desconecta las sesiones de DaaS, los suscriptores per-

manecen conectados a sus sesiones de DaaS cuando se agota el tiempo de espera por inactividad.

Establecer un período de reautenticación para la aplicación Citrix Workspace

Utilice el parámetro **Período de reautenticación de la aplicación Workspace** en **Configuración de Workspace > Personalizar > Preferencias** para especificar el período de tiempo que los suscriptores pueden permanecer conectados a la aplicación Citrix Workspace antes de tener que volver a iniciar sesión.



De forma predeterminada, este parámetro requiere que los suscriptores inicien sesión cada 24 horas (un día). Puede especificar un período de reautenticación más largo, de hasta 365 días. Los periodos de reautenticación más largos requieren el consentimiento del suscriptor para mantener la sesión abierta. Los usuarios aprovisionados después del 27 de septiembre de 2021 necesitan 30 días para que los suscriptores deban iniciar sesión de nuevo.

Durante el período de reautenticación establecido, los suscriptores mantienen la sesión abierta, a menos que estén inactivos durante 14 días seguidos o más. Si un suscriptor está inactivo durante 14 o más días, se le pedirá que se vuelva a autenticarse la siguiente vez que intente acceder a su espacio de trabajo.

Puede invalidar la sesión para sus suscriptores descargando este script de PowerShell y siguiendo las instrucciones que se incluyen en la descarga. Una vez que haya invalidado las sesiones, los suscriptores deberán volver a autenticarse en sus espacios de trabajo en las próximas 24 horas.

Si necesita establecer el período de reautenticación de la aplicación Citrix Workspace en menos de 24 horas, puede hacerlo a través de PowerShell.
Para obtener más información, consulte Steps to configure InactivityTimeoutInMinutes.

Clientes de la aplicación Workspace compatibles

Las siguientes versiones de la aplicación Citrix Workspace admiten esta funcionalidad:

- Aplicación Workspace 2106 para Windows o una versión posterior

- Aplicación Workspace 2106 para Mac o una versión posterior
- Aplicación Workspace 21.6.5 para iOS o una versión posterior
- Aplicación Workspace 21.6.0 para Android o una versión posterior

Métodos de autenticación admitidos

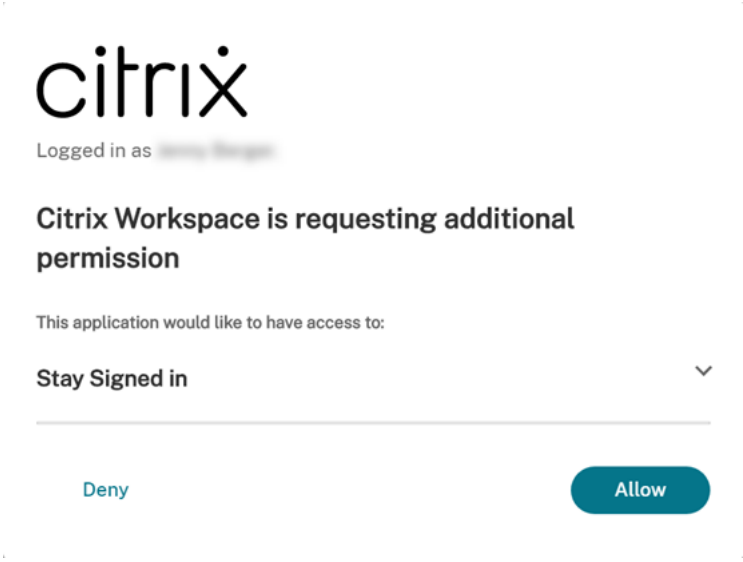
Se admite mantener la sesión abierta en la aplicación Citrix Workspace para los siguientes métodos de autenticación:

- Active Directory
- Active Directory y token
- Azure Active Directory
- Citrix Gateway
- Okta

> **Nota:**
>
> Para disfrutar de la misma experiencia que un cliente de Citrix DaaS con Okta o Azure Active Directory, configure el Servicio de autenticación federada (FAS) de Citrix. Para obtener más información acerca de FAS, consulte Habilitar Single Sign-On para espacios de trabajo con el Servicio de autenticación federada de Citrix.

Experiencia del suscriptor al mantener la sesión abierta

Cuando los suscriptores inician sesión en Workspace en sus dispositivos, Workspace les pide que den su consentimiento para mantener la sesión abierta.



Cuando el suscriptor selecciona **Permitir**, la sesión permanece abierta durante el período de reautenticación. Si no se detecta actividad en el dispositivo de un suscriptor durante cuatro días, se le

pedirá automáticamente que vuelva a autenticarse. Después de iniciar sesión en la aplicación Citrix Workspace, el período de reautenticación permanece vigente mientras utilicen sus aplicaciones y escritorios en el dispositivo.

Si el suscriptor selecciona **Denegar**, Workspace le pide que inicie sesión de nuevo. Posteriormente, Workspace pide al suscriptor que vuelva a iniciar sesión transcurridas 24 horas.

Si la contraseña del suscriptor cambia, este deberá cerrar sesión y volver a iniciarla a través de la aplicación Citrix Workspace para que el período de reautenticación siga funcionando.

Permitir a los suscriptores cambiar la contraseña de su cuenta

> **Nota:**
>
> Esta función se está implantando progresivamente para los clientes. Es posible que no pueda ver la funcionalidad hasta que se haya completado el proceso de implantación.
>
> Citrix tiene como objetivo entregar nuevas funciones y actualizaciones de productos a los clientes de Citrix Workspace tan pronto como estén disponibles. Para usted, este proceso es transparente. Las actualizaciones iniciales solo se aplican en los sitios internos de Citrix; luego se aplican gradualmente en los entornos de los clientes. La entrega por incrementos de actualizaciones ayuda a garantizar la calidad de los productos y maximizar su disponibilidad.

El parámetro **Permitir que se cambie la contraseña de la cuenta** en **Configuración de Workspace > Personalizar > Preferencias** controla si los suscriptores pueden cambiar su contraseña de dominio desde Citrix Workspace. También puede proporcionar orientación a los suscriptores, de manera que puedan crear contraseñas válidas conforme a la directiva de contraseñas de su organización.

Cuando esté habilitada (lo está de forma predeterminada), los suscriptores podrán cambiar su contraseña en cualquier momento, según los parámetros de Active Directory de su organización. Si está inhabilitada, Workspace pedirá a los suscriptores que cambien su contraseña cuando caduque, pero no podrán cambiar su contraseña, si esta no ha caducado, dentro de Workspace.

Métodos de autenticación admitidos

- Active Directory
- Active Directory y token

Clientes de la aplicación Workspace compatibles

Las siguientes versiones de la aplicación Citrix Workspace admiten esta funcionalidad:

- Aplicación Workspace para Windows 2101 o una versión posterior

- Aplicación Workspace para Mac 2012 o una versión posterior
- Aplicación Workspace para Chrome 2010 o una versión posterior
- Aplicación Workspace para HTML5 2101 o una versión posterior
- Aplicación Workspace para Android 21.1.0 o una versión posterior

Los suscriptores también pueden usar esta funcionalidad al acceder a los espacios de trabajo con la versión más reciente de los exploradores web Edge, Chrome, Firefox o Safari.

Esta función no se admite en versiones anteriores de la aplicación Citrix Workspace y la aplicación Citrix Workspace para Linux.

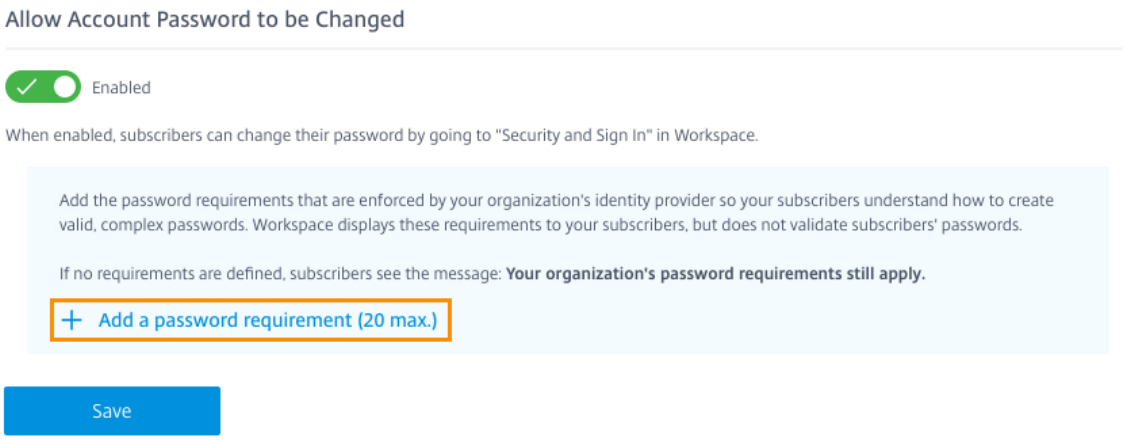
Directrices sobre contraseñas

Puede agregar hasta 20 requisitos relativos a las contraseñas que se adapten a la directiva de seguridad de su organización y que el proveedor de identidades imponga. Workspace muestra estos requisitos como directriz cuando los suscriptores cambian su contraseña desde la página **Parámetros de cuenta** en Workspace. Si no agrega ningún requisito relativo a la contraseña, Workspace muestra el mensaje "Los requisitos de contraseña de su organización siguen aplicándose".

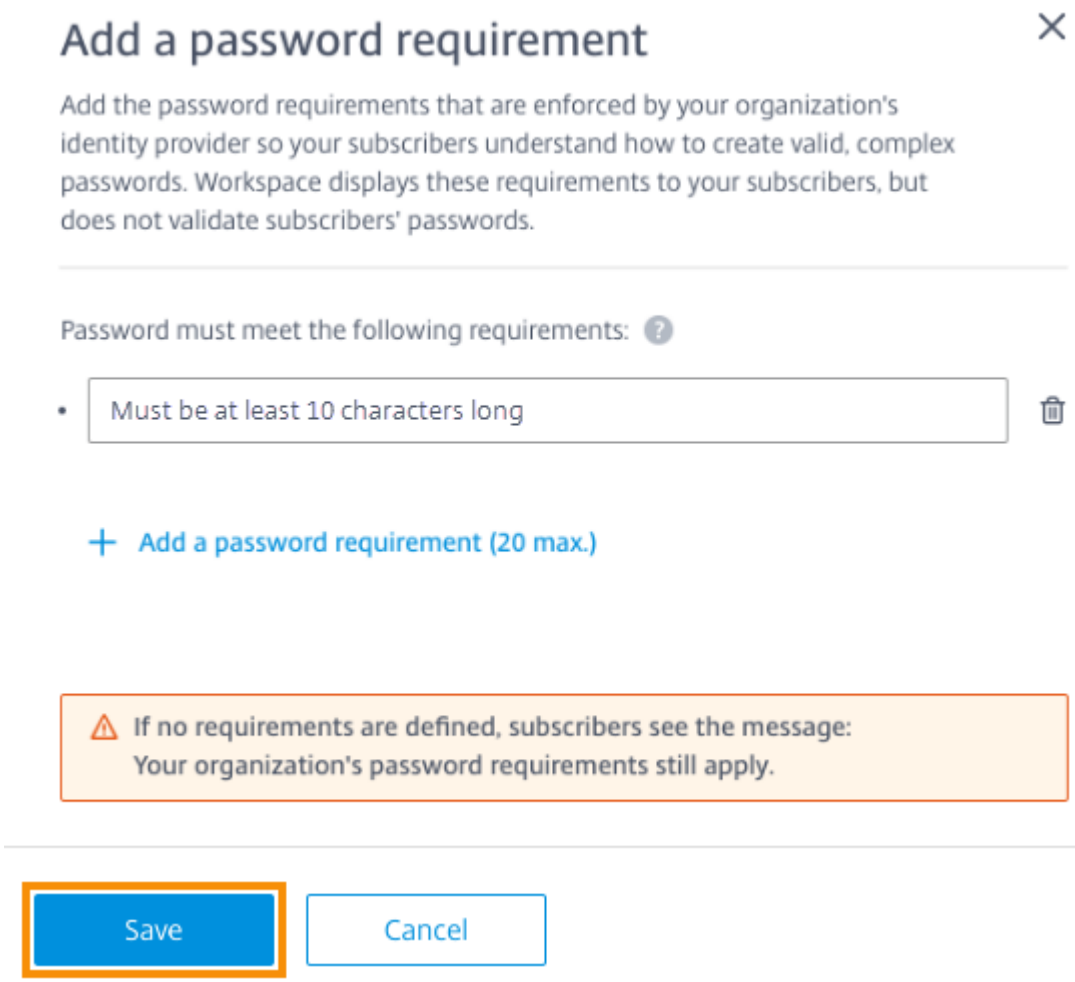
> **Importante:**
>
> Citrix Workspace no valida las nuevas contraseñas que introducen los suscriptores. Si un suscriptor intenta cambiar su contraseña válida a una no válida a través de Workspace, el proveedor de identidades rechaza la nueva contraseña. La contraseña existente no cambia.

Para agregar requisitos de contraseña:

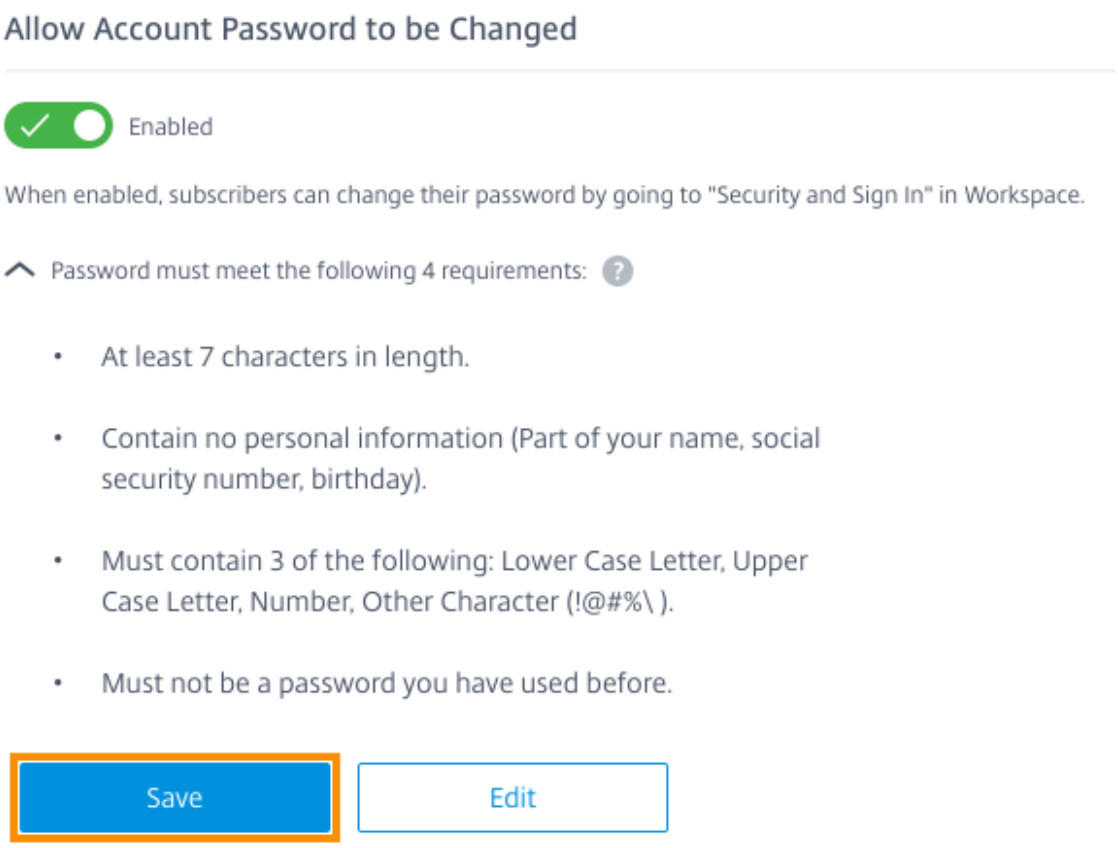
1. Vaya a **Configuración de Workspace > Personalizar > Preferencias**.
2. En **Permitir que se cambie la contraseña de la cuenta**, compruebe que la opción está habilitada. Si está inhabilitada, habilítela.
3. Seleccione **Agregar un requisito de contraseña**.



4. Introduzca un requisito conforme a los requisitos de seguridad existentes en su organización para las contraseñas válidas. Por ejemplo, puede especificar que una contraseña tenga una longitud de caracteres determinada. Seleccione **Agregar un requisito de contraseña** para agregar otros elementos para los suscriptores cuando cambien sus contraseñas.



5. Cuando haya terminado de agregar requisitos, seleccione **Guardar**.
6. Seleccione **Guardar** de nuevo para guardar todos los cambios de configuración.

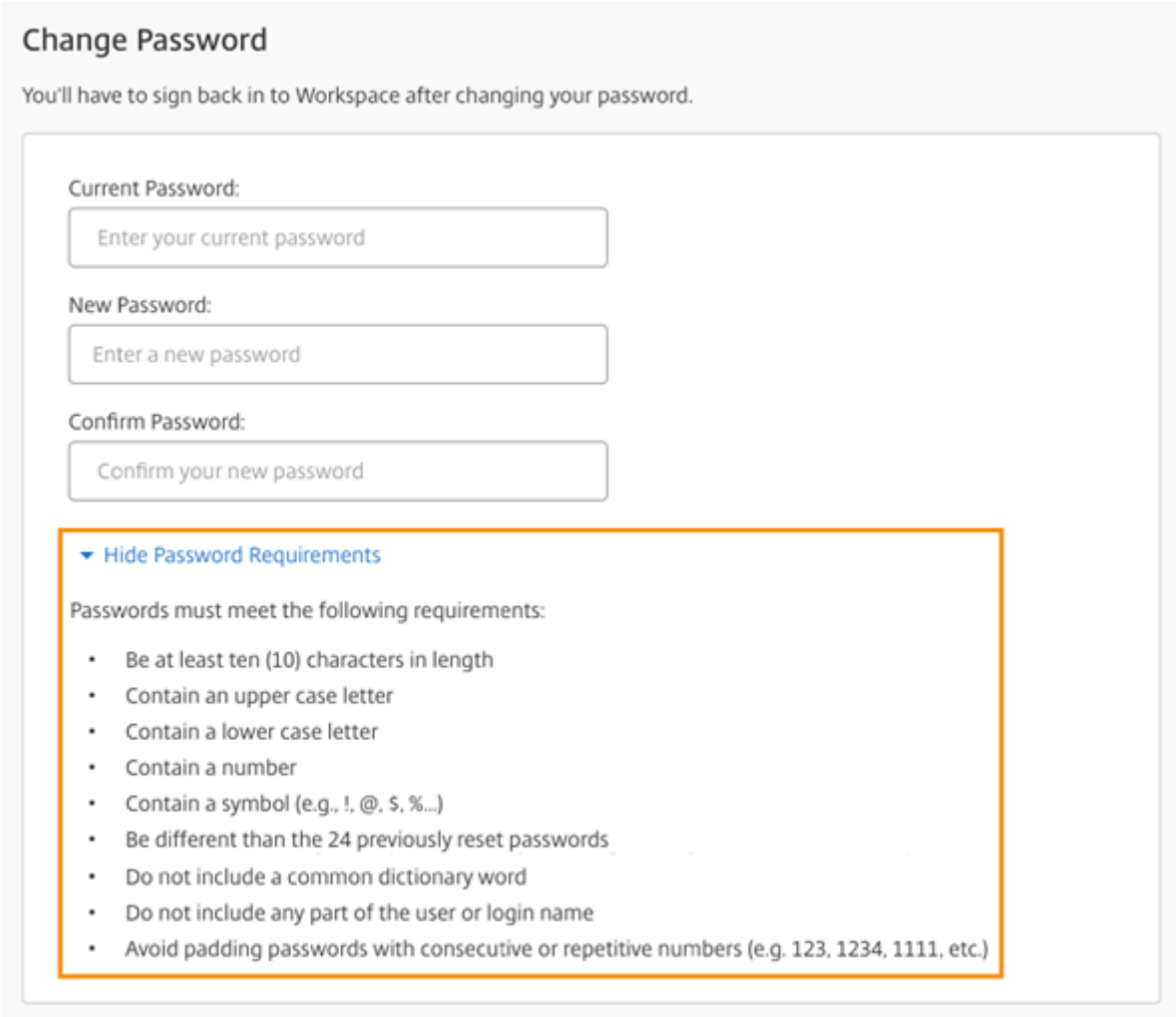


Experiencia de los suscriptores al cambiar contraseñas

> **Sugerencia:**
>
> Para dar a conocer esta función entre sus suscriptores, considere la posibilidad de incluir una recomendación en su base de conocimientos interna para que los suscriptores cambien sus contraseñas de dominio a través de Workspace. Descargue este archivo PDF para obtener instrucciones que puede incluir en sus comunicaciones y en los artículos de su base de conocimientos.

Al habilitar **Permitir que se cambie la contraseña de la cuenta**, los suscriptores pueden cambiar su contraseña en Workspace desde **Parámetros de cuenta > Seguridad e inicio de sesión**.

Seleccione **Ver requisitos de contraseña** para mostrar todos los requisitos especificados en **Configuración de Workspace**.



Al cambiar su contraseña, la sesión de los suscriptores se cierra automáticamente en Workspace y deben volver a iniciar sesión con su nueva contraseña.

Enviar anuncios personalizados

Envíe un anuncio personalizado para mostrar un mensaje durante el tiempo limitado de su elección, como durante un período de mantenimiento próximo.

El anuncio personalizado se muestra para todos los suscriptores en todos los clientes, tanto dispositivos web como móviles. Los suscriptores ven el mensaje después de iniciar sesión. Los suscriptores no pueden descartar este anuncio, pero pueden contraerlo en su dispositivo móvil.

1. En el menú de **Citrix Cloud**, seleccione **Configuración de Workspace > Personalizar > Preferencias > Enviar anuncio personalizado > Configurar**.
2. Introduzca el título y el texto del mensaje que quiere mostrar, y seleccione las fechas, las horas y la ubicación (arriba o abajo) en que mostrar el mensaje a los suscriptores.

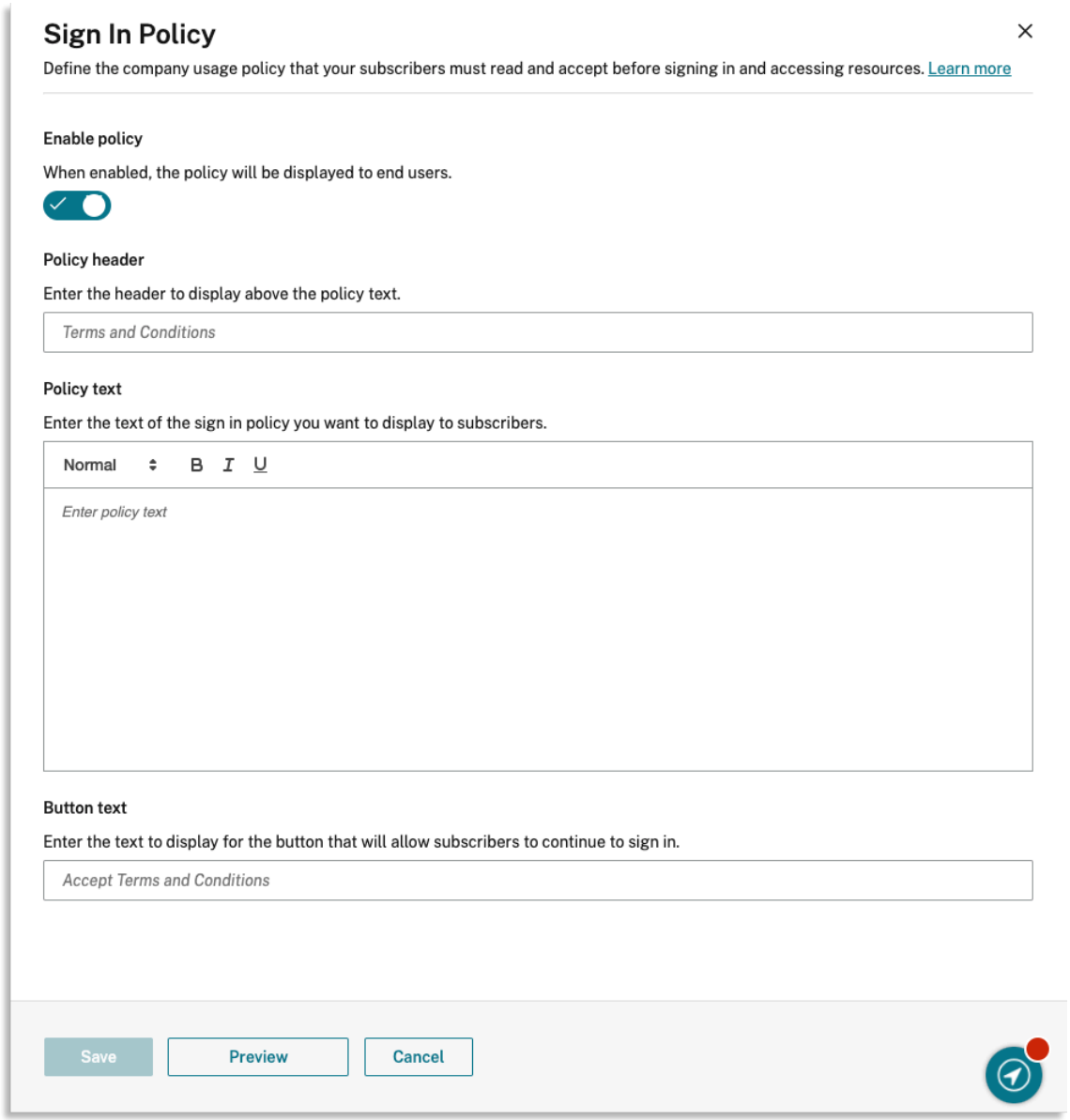
3. Para ver el aspecto del mensaje a ojos de los suscriptores, seleccione **Vista previa**.
4. Cuando haya terminado, seleccione **Guardar**.

Configurar una directiva de inicio de sesión

Cree una directiva de inicio de sesión personalizada para informar a los suscriptores del Contrato de licencia de usuario final (CLUF) de su organización cuando inicien sesión en su espacio de trabajo.

Cuando está habilitada y configurada, la directiva de inicio de sesión se muestra en todos los clientes, tanto dispositivos web como móviles. Los suscriptores pueden ver la directiva de inicio de sesión cuando inician sesión. Los suscriptores no pueden omitir la directiva y deben aceptarla para iniciar sesión en su espacio de trabajo.

1. En el menú de **Citrix Cloud**, seleccione **Configuración del espacio de trabajo > Personalizar > Preferencias**.
2. En la sección **Directiva de inicio de sesión**, seleccione **Configurar**. Si ya existe una directiva, el botón indica **Modificar**.
3. Habilite la función con el conmutador de **Habilitar directiva**.
4. En el **encabezado Directiva**, introduzca un título para la directiva.
5. Escriba el texto de la directiva que deben aceptar los suscriptores antes de iniciar sesión. Si es necesario, agregue la traducción en otros idiomas en el mismo cuadro de texto.
6. Escriba el nombre del botón que los suscriptores deben seleccionar para aceptar la directiva.



7. Seleccione **Vista previa** para ver el aspecto de la directiva a ojos de los suscriptores.
8. Cuando haya terminado, seleccione **Guardar**.

> **Nota**
>
> Si configuró Citrix Gateway como su proveedor de identidades de Workspace, es posible que ya tenga una directiva de inicio de sesión como parte de su flujo de autenticación AAA y nFactor. Citrix recomienda configurar solo una directiva de inicio de sesión, ya sea como parte del flujo de autenticación nFactor existente o fuera del flujo mediante la consola de administración de Citrix Cloud.

Optimizar DaaS en Citrix Workspace

October 12, 2023

Puede mejorar la eficiencia y la disponibilidad de sus aplicaciones y escritorios de DaaS con estas opciones:

- Hacer que la implementación de escritorios y aplicaciones virtuales locales existentes esté disponible para los suscriptores de Workspace con la agregación de sitios.
- Optimizar la conectividad con la conexión directa de carga de trabajo, que implica configurar las ubicaciones de red en Citrix Cloud.
- Garantizar la continuidad del servicio durante una interrupción a efectos de resiliencia sin conexión.
- Configurar Single Sign-On (SSO) en DaaS con el Servicio de autenticación federada (FAS) de Citrix.

Agregación de sitios

La agregación de sitios le permite agregar su implementación de escritorios y aplicaciones virtuales locales a su espacio de trabajo para que los suscriptores puedan acceder a estos recursos junto con los recursos administrados en la nube.

Para obtener más información sobre la agregación de sitios, consulte Agregación de aplicaciones y escritorios virtuales locales a espacios de trabajo.

Para obtener más información sobre los límites de escalabilidad, consulte Límites de escalabilidad de la plataforma Workspace.

Conexión directa de carga de trabajo

Conexión directa de carga de trabajo utiliza ubicaciones de red para cambiar entre rutas internas y externas a las máquinas virtuales que alojan sus aplicaciones y escritorios virtuales.

Con la conexión directa de carga de trabajo, permite que los clientes de su red corporativa cambien a inicios directos de Citrix DaaS. Los inicios directos no requieren que las conexiones HDX entre los clientes y los VDA se realicen mediante proxy a través de una puerta de enlace. La conexión directa de carga de trabajo requiere al menos una ubicación de red interna.

Para obtener más información, consulte Optimizar la conectividad con la conexión directa de carga de trabajo.

Continuidad del servicio

La continuidad del servicio garantiza que los suscriptores mantengan el acceso a las aplicaciones y escritorios esenciales a través de la aplicación Citrix Workspace si se produce una interrupción de Citrix Cloud.

La continuidad del servicio almacena las concesiones de conexión en discos de cliente que tienen la aplicación Citrix Workspace instalada. Las concesiones de conexión se actualizan periódicamente cuando los clientes acceden al almacén de Workspace. Los clientes pueden iniciar instancias de Citrix DaaS a las que podían acceder antes de la interrupción del servicio. Para obtener más información, consulte Continuidad del servicio.

Servicio de autenticación federada (FAS) de Citrix

Citrix Workspace permite usar el Servicio de autenticación federada (FAS) de Citrix para el acceso Single Sign-On (SSO) a Citrix DaaS. FAS permite a los suscriptores que utilizan un proveedor de identidades federadas, como Azure AD u Okta, introducir sus credenciales solo una vez, cuando inician sesión en sus espacios de trabajo. Sin FAS, a los suscriptores que utilizan un proveedor de identidades federadas se les pide que introduzcan sus credenciales más de una vez para acceder a sus aplicaciones y escritorios virtuales.

El uso de FAS con Workspace tiene los siguientes requisitos:

- Servidor FAS configurado como se describe en la sección Requisitos de la documentación de producto de FAS.
- Una conexión entre el servidor FAS y Citrix Cloud, creada a través de la opción **Connect to Citrix Cloud** del instalador de FAS.
- Una conexión entre el dominio local de Active Directory y Citrix Cloud, con FAS habilitado en **Configuración de Workspace**.

Para obtener información acerca de la implementación de FAS, consulte Habilitar Single Sign-On para espacios de trabajo con el Servicio de autenticación federada de Citrix.

Agregación de aplicaciones y escritorios virtuales locales a espacios de trabajo

October 12, 2023

Puede agregar su sitio (implementación de Virtual Apps and Desktops) a Citrix Workspace para que sus aplicaciones y escritorios existentes estén disponibles para los suscriptores. Después de agregar

el sitio, los suscriptores pueden acceder a todas sus aplicaciones y escritorios virtuales, junto con sus archivos y otros recursos, al iniciar sesión en su espacio de trabajo. Este proceso se conoce como *agregación de sitios*.

La agregación de sitios está disponible en todas las ediciones de Citrix Workspace. Para obtener más información sobre las funciones incluidas en cada edición de Workspace, consulte la tabla de funciones de Citrix Workspace.

Entornos admitidos

La agregación de sitios se admite en las implementaciones locales de los siguientes productos de Citrix:

- Virtual Apps and Desktops 7 1808 o versiones posteriores
- XenApp y XenDesktop de la versión 7.0 a la 7.18

Los sitios locales que ejecutan versiones anteriores de XenApp o de XenApp y XenDesktop no se admiten para usarlos con Citrix Workspace.

> **Importante:**
>
> XenApp y XenDesktop 7.x incluyen versiones que han alcanzado el estado Fin de vida (EoL). Las versiones de XenApp y XenDesktop anteriores a 7.14 llegaron al fin de vida útil el 30 de junio de 2018. La compatibilidad de la agregación de sitios de Workspace con las versiones de XenApp y XenDesktop 7.x que han llegado al final de su ciclo de vida depende de la enumeración e inicio correctos de recursos con la implementación de StoreFront.

Para utilizar la agregación de sitios con una implementación local que incluya el servicio de autenticación federada (FAS) de Citrix, el sitio debe usar una de las siguientes versiones de productos Citrix:

- Virtual Apps and Desktops 7 1808 o versiones posteriores
- XenApp y XenDesktop de la versión 7.16 a la 7.18

Para usar FAS con Citrix Workspace, es necesario conectarse a Citrix Cloud. Para poder conectarse a Citrix Cloud, actualice sus servidores FAS con la versión más reciente del software FAS. Para obtener más información, consulte Habilitar Single Sign-On para espacios de trabajo con el Servicio de autenticación federada de Citrix.

Límites de escalabilidad de la plataforma Workspace

Estos límites de escalabilidad se aplican a la plataforma Workspace:

Tipo de límite	Métrica SLI	Límite del umbral de SLO
Límites de uso	Usuarios finales simultáneos para todos los sitios locales agregados de Citrix Virtual Apps and Desktops	500
Límites adicionales de integración de backend/frontend	Cantidad de sitios locales de Citrix Virtual Apps and Desktops	4

> **Nota:**
>
> Si la cantidad de sitios de la integración de backend/frontend supera los cuatro, los sitios pueden sufrir tiempos de respuesta lentos. Continuidad del servicio o la función de caché de host local tampoco están presentes para los sitios locales.

Descripción general de tareas

Cuando agregue un sitio local a Citrix Workspace, el asistente para **agregar sitios** le guiará por las siguientes tareas:

1. Detectar el sitio y seleccionar la ubicación de recursos que quiere usar.
2. Detectar los dominios de Active Directory donde están instalados los Cloud Connectors.
3. Especificar la conectividad que quiere usar entre Citrix Cloud y su sitio.

La ubicación de recursos especifica el dominio y el método de conectividad para todos los usuarios que acceden al sitio. Durante este proceso, Citrix Cloud prueba la conectividad para verificar que se pueda acceder al sitio desde los Cloud Connectors. A continuación, Citrix Cloud muestra una lista de las ubicaciones de recursos. Si tiene ubicaciones de recursos que aún no tienen Cloud Connectors instalados, descargue e instale el software requerido.

Para la conectividad externa, puede usar su propio Citrix Gateway o usar el servicio Citrix Gateway. Para garantizar que solo los usuarios que están en la misma red que el sitio puedan acceder a las aplicaciones, especifique el acceso solo interno.

Requisitos previos

Cloud Connectors

Los Cloud Connectors permiten a Citrix Cloud localizar su sitio y comunicarse con él. Para una interrupción mínima, Citrix recomienda instalar los Cloud Connectors antes de agregar el sitio a Citrix Workspace.

En pro de una alta disponibilidad, Citrix recomienda instalar el software Citrix Cloud Connector en, al menos, dos (2) servidores. Estos servidores deben:

- Cumplir los requisitos del sistema descritos en los Detalles técnicos de Cloud Connector.
- No tener instalados otros componentes de Citrix.
- No ser un controlador de dominio de Active Directory.
- No ser una máquina que sea esencial para la infraestructura de ubicaciones de recursos.
- Unirse al dominio de su sitio. Si los usuarios acceden a las aplicaciones del sitio en varios dominios, instale al menos dos Cloud Connectors en cada dominio.
- Estar conectados a una red que puede contactar con el sitio.
- Estar conectados 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.

Configurar el proxy web

Si tiene un proxy web en el entorno, compruebe que los Cloud Connectors puedan validar la conectividad con el servicio XML en su sitio. Agregue cada servidor XML del sitio a la lista de omisión de proxys en cada Cloud Connector. No utilice comodines ni direcciones IP porque Cloud Connector solo admite la gestión de nombres de dominio completos.

1. Agregue los servidores XML a la lista de omisión de proxys:
    a) En Cloud Connector, seleccione **Inicio** y, a continuación, escriba **Opciones de Internet**.
    b) Seleccione la ficha **Conexiones** y, a continuación, seleccione **Configuración de LAN**.
    c) En **Servidor proxy**, seleccione **Avanzado**.
    d) En **Excepciones**, agregue el nombre de dominio completo (FQDN) de cada servidor XML del sitio con letras minúsculas. Si se utiliza una mezcla o mayúsculas, la agregación de sitios podría fallar. Para obtener más información, consulte CTX272160 en Knowledge Center de Citrix Support.
2. Importe la lista para que los servicios de Cloud Connector puedan consumirlos. En el símbolo del sistema, escriba `netsh winhttp import proxy source=ie`.
3. Desde la consola **Servicios**, reinicie todos los servicios de Citrix Cloud en cada máquina que aloja Cloud Connector o reinicie todas las máquinas.

Active Directory

La agregación de sitios admite sitios que usan un Active Directory local.

Configurar Azure Active Directory Para agregar sitios con Azure Active Directory a Citrix Workspace, configure su sitio para que confíe en las solicitudes de XML Service. Para obtener instrucciones detalladas, consulte los siguientes artículos:

Para XenApp y XenDesktop 7.x y Citrix Virtual Apps and Desktops 7 1808, consulte CTX236929.

> **Importante:**
>
> Si usa Azure Active Directory, Okta, SAML u otro proveedor de identidades federado con espacios de trabajo y agregación de sitios, se les pide a los usuarios que se autentiquen en cada aplicación que inician.
>
> FAS proporciona una experiencia de Single Sign-On (SSO) para iniciar recursos mediante autenticación federada. Para habilitar SSO para los suscriptores, registre uno o más servidores FAS con la misma ubicación de recursos que configuró para agregar su sitio.

Relaciones de confianza de Active Directory Si tiene bosques de usuario y recursos separados en Active Directory, debe tener Cloud Connectors instalados en cada bosque antes de agregar su sitio local. Citrix Cloud detecta estos bosques durante el proceso de detección del sitio, a través de los Cloud Connectors. Luego, puede usar los usuarios y recursos de los bosques para crear espacios de trabajo para sus usuarios.

Limitaciones:

Al definir la ubicación de recursos mientras agrega el sitio, no puede usar bosques de recursos y usuarios separados. Debido a que los Cloud Connectors no participan en ningún tipo de relación de confianza que pueda establecerse entre bosques, Citrix Cloud no puede detectar su sitio a través de los Cloud Connectors en estos bosques. Puede usar estos bosques cuando defina una ubicación de recursos secundaria que proporcione una opción de conectividad diferente para sus usuarios. Para obtener más información, consulte Agregar intervalos de IP para diferentes opciones de conectividad.

Los bosques que no son de confianza no son compatibles con la agregación de sitios. Aunque Citrix Cloud y Citrix Workspace admiten a usuarios de bosques que no son de confianza, estos usuarios no pueden usar Citrix Workspace después de que se haya agregado un sitio local a través de la agregación de sitios. Solo los usuarios ubicados en los bosques que son de confianza para el sitio pueden iniciar sesión y usar Citrix Workspace. Si los usuarios de un bosque que no es de confianza intentan iniciar sesión en Citrix Workspace, reciben el mensaje de error "Su sesión ha caducado. Vuelva a iniciar una sesión para continuar".

Conectividad interna y externa con los recursos del espacio de trabajo

Durante el proceso de agregar un sitio a Citrix Workspace, puede especificar si proporcionar acceso interno o externo a los recursos que están a disposición de los usuarios. Si tiene la intención de per-

mitir el acceso al sitio a través de Citrix Workspace solo a usuarios internos, los usuarios deben estar en la misma red que el sitio para poder acceder a las aplicaciones.

Si quiere permitir que los usuarios externos accedan a estos recursos, tiene las siguientes opciones:

- Use su Citrix Gateway existente para gestionar el tráfico entre el sitio local y Citrix Cloud. Su Citrix Gateway debe estar configurado para usar los Cloud Connectors como servidores Secure Ticket Authority (STA) **antes** de agregar el sitio a Citrix Workspace. Para obtener instrucciones, consulte CTX232640.
- Use Citrix Gateway Service para permitir que Citrix gestione por usted el tráfico entre el sitio y Citrix Cloud. Puede activar una prueba de servicio y configurar el servicio al agregar el sitio. Si ya se ha registrado en Citrix Gateway Service, Citrix Cloud detecta su suscripción cuando selecciona esta opción.

> **Nota:**
>
> Para que Citrix Cloud detecte su suscripción a Citrix Gateway Service, debe usar el mismo OrgID (ID de organización) que utilizó cuando se inscribió en Citrix Gateway Service. Para obtener más información sobre los OrgID en Citrix Cloud, consulte ¿Qué es un OrgID?

Credenciales y puertos para la detección del sitio

Durante el proceso de agregar el sitio a Citrix Workspace, Citrix Cloud detecta el sitio y comprueba que el Controller que usted especifique está disponible. Antes de agregar el sitio local, compruebe lo siguiente:

- Tiene credenciales de administrador de Citrix con permisos de **solo lectura** (como mínimo). Durante el proceso de detección del sitio, Citrix Cloud le pide que proporcione estas credenciales. Citrix Cloud no almacena estas credenciales ni las usa para hacer cambios en su sitio.

Para habilitar la detección del sitio sin las credenciales del sitio Solo XenApp y XenDesktop 7.x y Virtual Apps and Desktops 7 1808: Si no quiere proporcionar sus credenciales del sitio por razones de seguridad, puede permitir que Citrix Cloud detecte el sitio sin pedir las credenciales del mismo. Complete esta tarea **antes** de agregar el sitio a Citrix Workspace.

1. Instale al menos dos Cloud Connectors en el dominio de su sitio.
2. Cree un grupo de seguridad de Active Directory e incluya en él los Cloud Connectors del dominio.
3. Reinicie los Cloud Connectors.
4. En Studio, conceda permisos de **solo lectura**, como mínimo, al grupo de seguridad.

Tarea 1: Detectar el sitio

En este paso, debe proporcionar la información que Citrix Cloud necesita para encontrar el sitio y seleccionar la ubicación de recursos. La ubicación de recursos especifica el dominio y la opción de conectividad para todos los usuarios que acceden al sitio. Si necesita instalar Cloud Connectors en el dominio del sitio, puede hacerlo ahora. Si ya tiene instalados los Cloud Connectors, puede seleccionarlos cuando se le solicite.

1. En el menú de Citrix Cloud, vaya a **Configuración de Workspace > Sitios > Agregar sitio**.
2. Seleccione el tipo de sitio local que quiere agregar y continúe.

   Citrix Cloud intenta detectar cualquier ubicación de recursos y Cloud Connector en su dominio y muestra una lista para que seleccione.
3. Realice una de las siguientes acciones:

   - Si no tiene Cloud Connectors instalados en el dominio del sitio, haga clic en **Instalar Connector**. Citrix Cloud le solicita que descargue el software de Cloud Connector y complete el asistente de instalación.
   - Si tiene Cloud Connectors instalados, Citrix Cloud muestra los conectores en los dominios en los que fueron detectados. Seleccione la ubicación de recursos que quiere agregar al espacio de trabajo de Citrix Workspace. Esta ubicación de recursos se convierte en la ubicación de recursos predeterminada.
   - Si tiene Cloud Connectors instalados, pero no se muestran, seleccione **Detectar**.
4. Seleccione la ubicación de recursos y el par de Cloud Connectors que quiera usar para detectar el sitio.
5. En **Introducir la dirección del servidor**, agregue la dirección IP o el FQDN de un Controller del sitio y seleccione **Detectar**.

   > **Nota:**
   >
   > Si usa un FQDN, debe tener un registro de DNS que apunte al Delivery Controller que quiere detectar.
   >
   > Para sitios de XenApp y XenDesktop 7.x, Citrix Cloud detecta automáticamente el puerto del servidor XML.
6. Si se le solicita, introduzca las credenciales de administrador de Citrix del sitio.

   Citrix Cloud prueba la conectividad para verificar que el sitio es accesible. La detección puede tardar unos minutos en completarse, en función del tipo y del tamaño del sitio.
7. Si aparece un mensaje de éxito que indica que el sitio se ha detectado correctamente, seleccione **Continuar**.

Tarea 2: Verificar la conexión con Active Directory

En **Verificar conexión de Active Directory**, Citrix Cloud muestra los dominios usados con el sitio y si hay Cloud Connectors instalados en esos dominios.

Si no hay Cloud Connectors en un dominio, los usuarios no pueden usar Citrix Workspace para acceder a las aplicaciones publicadas allí. Si solo tiene un Cloud Connector en su dominio, tiene dos opciones:

- Instale más Cloud Connectors seleccionando **Instalar Connector**.
- Para continuar sin instalar más Cloud Connectors, seleccione **Comprendo que la alta disponibilidad requiere tener dos conectores instalados en cada dominio**.

Si tiene usuarios locales asignados a aplicaciones en el sitio, seleccione **Descargar lista de usuarios (.csv)**.

Después de verificar la conexión de Active Directory, seleccione **Continuar**.

Tarea 3: Configurar la conectividad

En este paso, debe especificar si quiere permitir solamente el acceso al sitio de usuarios externos, o solamente el acceso de usuarios internos, a través de Citrix Workspace. La conectividad interna requiere que los usuarios estén en la misma red que el sitio y los VDA que alojan los recursos publicados. Para la conectividad externa, puede usar su Citrix Gateway local o el servicio Citrix Gateway Service alojado en la nube.

Seleccione una de las siguientes opciones en **Seleccionar tipo de conectividad > Configurar conectividad**:

- **Agregar un Gateway existente:** Seleccione esta opción para usar su Citrix Gateway existente para proporcionar acceso externo.
- **Citrix Gateway Service:** Seleccione esta opción para activar una prueba de este servicio o para usar una suscripción existente con el sitio.
- **Solo interna:** Seleccione esta opción si no se necesita ninguna otra configuración.

Si selecciona **Agregar un Gateway existente**, realice las siguientes acciones:

1. Seleccione **Modificar** e introduzca la URL pública de Citrix Gateway.
2. Verifique que Citrix Gateway está configurado para usar sus Cloud Connectors como servidores STA, que se describe en CTX232640.
3. Seleccione **Probar STA** y, a continuación, cuando la prueba sea satisfactoria, **Continuar**. Si la prueba falla, consulte el artículo de resolución de problemas CTX232517.

Si se selecciona **Citrix Gateway Service**, pero no está habilitado para su cuenta de Citrix Cloud como una prueba de servicio o como una compra, puede seleccionar **Comenzar una prueba de 60 días**. Citrix Cloud permite el servicio como una prueba para usted. Si el servicio fue habilitado en un momento anterior, Citrix Cloud detecta el servicio y muestra los días de prueba restantes.

Después de completar las tareas anteriores, seleccione **Continuar**.

Tarea 4: Confirmar la agregación del sitio

En este paso, debe confirmar la agregación del sitio, que implica revisar el puerto XML, los servidores XML, los dominios de Active Directory y el tipo de conectividad elegidos anteriormente.

Citrix Cloud muestra hasta cinco servidores XML con los que se puede conectar. Si tiene más de un servidor XML en el sitio, pero solo se muestra uno, Citrix Cloud muestra una alerta. Para solucionar este problema, consulte el artículo CTX232516.

1. En **Confirmar agregación de sitios**, revise el puerto XML, los servidores XML, los dominios de Active Directory y el tipo de conectividad que eligió anteriormente.
2. Seleccione **Guardar y finalizar**. En la página **Sitios** se muestra el sitio recién agregado.

Si quiere especificar servidores XML diferentes, puede modificar el sitio para cambiar estos valores después de seleccionar **Guardar y finalizar**.

Tarea 5: Administrar las integraciones de servicios

Después de agregar el primer sitio, debe habilitar la **integración de servicios** para los sitios locales de Virtual Apps and Desktops, que está inhabilitada de forma predeterminada. Los suscriptores no podrán ver los recursos del sitio hasta que la habilite.

1. Vaya a **Configuración de Workspace > Integraciones de servicios > Sitios locales de Virtual Apps and Desktops** y seleccione los puntos suspensivos para abrir el menú de acciones del sitio.
2. Habilite la integración de servicios para que los suscriptores puedan iniciar sesión en sus espacios de trabajo y ver los recursos del sitio.

Cambiar la configuración del sitio

Volver a detectar el sitio

Si agrega Delivery Controllers al sitio o cambia los puertos XML, puede verificar que el sitio sigue siendo accesible en Citrix Workspace mediante un proceso de nueva detección.

1. Vaya a **Configuración de Workspace > Sitios**, seleccione los puntos suspensivos del sitio que quiere actualizar y, a continuación, seleccione **Modificar sitio**.
2. En **Dirección del servidor**, escriba la dirección IP o el FQDN de un Delivery Controller del sitio y seleccione **Volver a detectar**.

Agregar o modificar servidores XML

Cuando agrega un sitio a Citrix Workspace, Citrix Cloud detecta automáticamente los servidores XML del sitio y muestra hasta cinco servidores XML presentes en la configuración. Puede agregar y eliminar servidores XML de la configuración del sitio, según sea necesario; se mostrará un máximo de cinco servidores XML.

Para agregar un servidor XML

1. Vaya a **Configuración de Workspace > Sitios**, seleccione los puntos suspensivos del sitio que quiere actualizar y seleccione **Modificar sitio**.
2. En la sección **Servidores XML**, introduzca el puerto del servidor XML y seleccione **Usar SSL** si es necesario.
3. Seleccione un método de conectividad:
    - **Equilibrio de carga:** Esta opción permite que Citrix Cloud elija un servidor XML de la lista aleatoriamente.
    - **Conmutación por error:** Esta opción permite a Citrix Cloud utilizar los servidores XML, en el orden en que aparecen en la lista. Solo se utiliza el primer servicio XML de la lista para el inicio, a menos que no esté disponible, en cuyo caso se utilizará el segundo servidor. Puede volver a ordenar la lista arrastrando y soltando cada uno de los servidores.
4. Seleccione **Guardar cambios**.

Si observa un error al agregar un servidor XML, consulte CTX232516 para seguir los pasos de resolución de problemas.

Agregar intervalos de IP para diferentes opciones de conectividad

Si tiene los VDA o hosts de sesiones en subredes diferentes, puede especificar intervalos de IP con un tipo de conectividad diferente para cada uno. Cada intervalo de IP puede tener también su propia ubicación de recursos asociada. Por ejemplo, puede tener un intervalo de IP para las máquinas de la Unión Europea donde los usuarios se conectan internamente, otro intervalo de IP para las máquinas de la Unión Europea donde los usuarios se conectan a través de su Citrix Gateway, y otro intervalo de IP para las máquinas ubicadas en los EE. UU. donde los usuarios se conectan a través de Citrix Gateway Service.

1. Vaya a **Configuración de Workspace > Sitios**, seleccione el botón de tres puntos del sitio que quiere actualizar y seleccione **Modificar sitio**.
2. En la sección **Conectividad**, seleccione **Agregar un intervalo de IP con una opción de conectividad diferente** e introduzca un intervalo de direcciones IP en formato CIDR.

Para crear una ubicación de recursos para el intervalo de IP:

1. Seleccione **Agregar una nueva ubicación de recursos** e introduzca un nombre fácil de recordar.
2. En **Seleccionar la conectividad**, seleccione si proporcionar solo acceso interno o si quiere permitir también el acceso externo mediante un dispositivo Citrix Gateway o mediante Citrix Gateway Service.

Para asignar una ubicación de recursos existente al intervalo de IP:

1. Elija **Seleccionar una ubicación de recursos existente**
2. Seleccione la ubicación de recursos que quiere usar.
3. Si elige una ubicación de recursos que solo tiene un Cloud Connector instalado, seleccione **Comprendo que la alta disponibilidad requiere tener dos conectores instalados en una ubicación de recursos**.
4. Seleccione **Agregar**.

Agregar más dominios de Active Directory

Si instala Cloud Connectors en otros dominios con usuarios de Active Directory en el sitio, puede comprobar que se agregan a la configuración del sitio en Citrix Workspace.

1. Vaya a **Configuración de Workspace > Sitios**, seleccione los puntos suspensivos del sitio que quiere actualizar y, a continuación, seleccione **Modificar sitio**.
2. En Active Directory, seleccione **Actualizar**.

Inhabilitar sitios

Si ya no quiere que su sitio local esté disponible para los usuarios en el espacio de trabajo de Citrix Workspace, puede inhabilitarlo. Puede inhabilitar un sitio local individual o inhabilitar todos los sitios locales que haya agregado a Citrix Workspace.

Cuando los sitios están inhabilitados, los usuarios no pueden acceder a las aplicaciones locales de esos sitios a través de Citrix Workspace. Sin embargo, se conserva la configuración de esos sitios. Si vuelve a habilitar un sitio más adelante, se conservan la configuración predeterminada de ubicación del recurso, el dominio, el servidor XML y la conectividad del sitio.

Para inhabilitar un sitio local

1. Vaya a **Configuración de Workspace > Sitios**, seleccione los puntos suspensivos del sitio que quiere inhabilitar y, a continuación, seleccione **Inhabilitar**.
2. Aparece un mensaje de confirmación. Seleccione **Inhabilitar** de nuevo.

Para inhabilitar todos los sitios locales

Para inhabilitar todos los sitios de la página **Sitios**, inhabilite la integración de Workspace Service para todos los sitios locales de Virtual Apps and Desktops. Para obtener instrucciones, consulte Para inhabilitar la integración de espacios de trabajo para un servicio.

Para volver a habilitar un sitio local individual o agregar otro sitio más adelante, primero debe volver a habilitar la integración de Workspace Service para todos los sitios en la página **Integraciones de servicios**.

Eliminar un sitio de Citrix Workspace

Si ya no quiere que su sitio local esté disponible para los usuarios en Citrix Workspace, puede eliminarlo. Cuando se elimina un sitio, solo se elimina la configuración del sitio en Citrix Workspace. Citrix Cloud no hace cambios en el sitio.

Para eliminar un sitio, vaya a **Configuración de Workspace > Sitios**, seleccione los puntos suspensivos del sitio que quiere eliminar y, a continuación, seleccione **Eliminar**.

Optimizar la conectividad a los espacios de trabajo con la conexión directa de carga de trabajo

November 21, 2023

Con la conexión directa de carga de trabajo en Citrix Cloud, puede optimizar el tráfico interno dirigido a las aplicaciones y escritorios en los espacios de trabajo para agilizar las sesiones HDX. Normalmente, tanto los usuarios de redes internas como los de redes externas se conectan a VDA a través de una puerta de enlace externa. Es posible que esta puerta de enlace esté en su organización o se proporcione como un servicio de Citrix y se agregue a la ubicación de recursos dentro de Citrix Cloud. La conexión directa de carga de trabajo permite a los usuarios internos omitir la puerta de enlace y conectarse directamente a los VDA, lo que reduce la latencia del tráfico de las redes internas.

Para configurar la conexión directa de carga de trabajo, necesita ubicaciones de red que correspondan al lugar en el que los clientes inician aplicaciones y escritorios en su entorno. Agregue una dirección

pública para la ubicación de cada oficina en la que residan estos clientes mediante el servicio de ubicación de red (NLS). Dispone de dos opciones para configurar las ubicaciones de red:

- Usar la opción de menú **Ubicaciones de red** de Citrix Cloud.
- Usar un módulo de PowerShell que proporciona Citrix.

Las ubicaciones de red corresponden a los rangos IP públicos de las redes desde las que se conectan los usuarios internos, como las sucursales u oficinas. Citrix Cloud usa direcciones IP públicas para determinar si las redes desde las que se inician aplicaciones o escritorios virtuales son internas o externas a la red de la empresa. Si un suscriptor se conecta desde la red interna, Citrix Cloud redirige la conexión directamente al VDA sin pasar por NetScaler Gateway. Si un suscriptor se conecta externamente, Citrix Cloud lo redirige a través de NetScaler Gateway y, a continuación, dirige el tráfico de la sesión a través del Citrix Cloud Connector al VDA de la red interna. Si se usa Citrix Gateway Service y el protocolo Rendezvous está habilitado, Citrix Cloud redirige a los usuarios externos a través de Gateway Service al VDA de la red interna. Es posible que haya clientes itinerantes, como los equipos portátiles, que usen cualquiera de estas rutas de red, según si el cliente se encuentra dentro o fuera de la red corporativa cuando se produce el inicio.

> **Importante:**
>
> Si su entorno incluye Citrix DaaS Standard para Azure junto con VDA locales, la configuración de la conexión directa de carga de trabajo provoca un error en los inicios que tienen lugar en la red interna.

Los inicios de recursos de Remote Browser Isolation, Citrix Virtual Apps Essentials y Citrix Virtual Desktops Essentials se redirigen siempre a la puerta de enlace. Estos inicios no mejoran el rendimiento de la configuración de la conexión directa de carga de trabajo.

Requisitos

Requisitos de la red

- La red corporativa y las redes Wi-Fi de invitados deben tener direcciones IP públicas independientes. Si sus redes corporativas y de invitados comparten direcciones IP públicas, los usuarios de la red de invitados no podrán iniciar sesiones de DaaS.
- Utilice los rangos de direcciones IP públicas de las redes desde las que se conectan los usuarios internos. Los usuarios internos de estas redes deben tener una conexión directa con los VDA. De lo contrario, los recursos virtuales fallan al iniciarse, ya que Workspace intenta redirigir a los usuarios internos directamente al VDA, lo que no es posible.
- Si bien los VDA suelen estar ubicados dentro de la red local, también puede usar VDA alojados en una nube pública, como Microsoft Azure. Los inicios de los clientes deben tener una ruta de

red para contactar con los VDA sin que un firewall los bloquee. Esto requiere un túnel VPN desde su red local hasta una red virtual en la que residan los VDA.

Requisitos de TLS

TLS 1.2 debe estar habilitado en PowerShell al configurar las ubicaciones de red. Para forzar a PowerShell para que utilice TLS 1.2, use el siguiente comando antes de usar el módulo de PowerShell:

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
```

Requisitos del espacio de trabajo

- Debe tener un espacio de trabajo configurado en Citrix Cloud.
- Citrix DaaS se habilita en **Configuración de Workspace > Integraciones de servicios**.

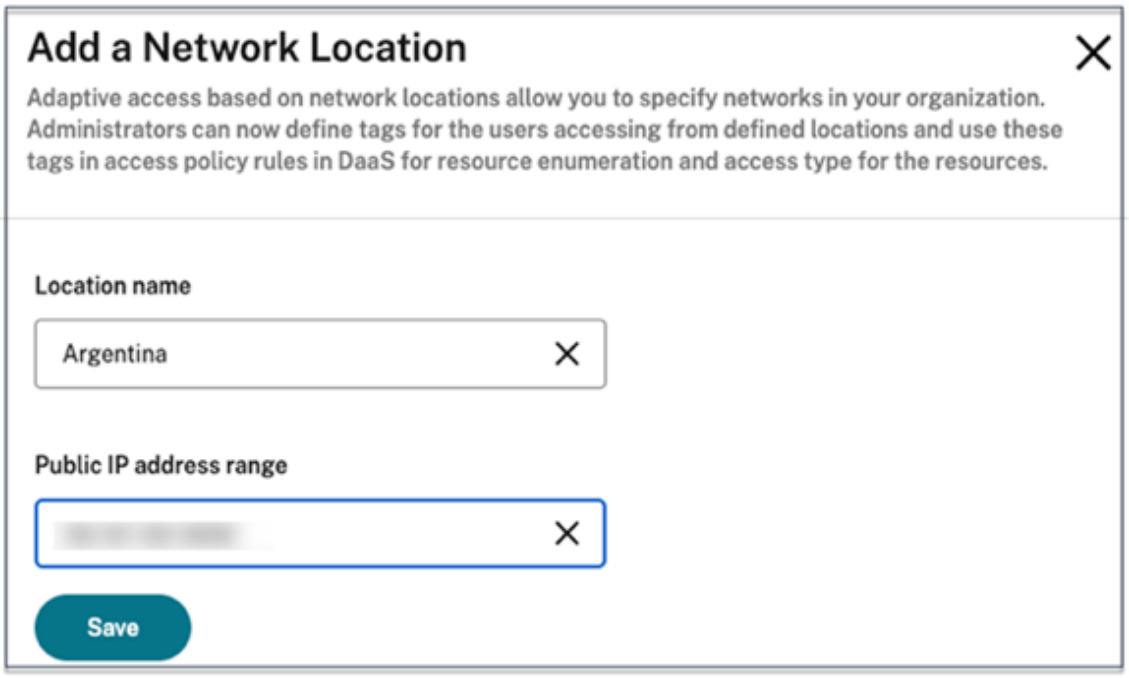
Habilitar TLS para la aplicación Workspace para conexiones HTML5

Si sus suscriptores utilizan la aplicación Citrix Workspace para HTML5 para iniciar aplicaciones y escritorios, Citrix recomienda tener configurado TLS en los VDA de su red interna. La configuración de los VDA para que usen conexiones TLS garantiza que sean posibles los inicios directos de los VDA. Si los VDA no tienen TLS habilitado, los inicios de aplicaciones y escritorios deben redirigirse a través de una puerta de enlace cuando los suscriptores utilizan la aplicación Citrix Workspace para HTML5. Los inicios que utilizan Desktop Viewer no se ven afectados. Para obtener más información acerca de cómo proteger las conexiones directas de VDA con TLS, consulte el artículo CTX134123 en Knowledge Center de Citrix Support.

Agregar ubicaciones de red a través de la GUI

La configuración de la conexión directa de carga de trabajo a través de Citrix Cloud implica crear ubicaciones de red mediante los intervalos de direcciones IP públicas de cada ubicación de sucursal desde la que se conectan los usuarios internos.

1. En la consola de Citrix Cloud, vaya a **Ubicaciones de red**.
2. Haga clic en **Agregar ubicación de red**.
3. Introduzca un nombre de ubicación de red y un rango de direcciones IP públicas para la ubicación.

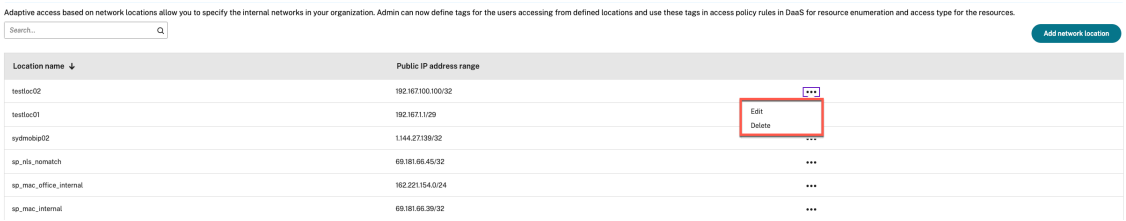


4. Haga clic en **Guardar**.
5. Repita estos pasos para cada nueva ubicación de red que quiera agregar.

> **Nota:**
>
> Las etiquetas de ubicación no son necesarias para la conexión directa de carga de trabajo porque el tipo de conectividad siempre es **Interna**. El campo **Etiquetas de ubicación** de la página **Agregar una ubicación de red** (**Citrix Cloud > Ubicaciones de red > Agregar una ubicación de red > Etiquetas de ubicación**) solo es visible si la función Acceso adaptable está habilitada. Para obtener detalles, consulte Habilitar la función Acceso adaptable.

Modificar o quitar ubicaciones de red

1. En la consola de Citrix Cloud, vaya a **Ubicaciones de red** en el menú principal.
2. Busque la ubicación de red que quiere administrar y haga clic en el botón de tres puntos.



3. Seleccione uno de estos comandos:

- Seleccione **Modificar** para modificar la ubicación de la red. Después de realizar los cambios, haga clic en **Guardar**.
- Seleccione **Eliminar** para quitar la ubicación de red. Seleccione **Sí, eliminar** para confirmar la eliminación. Esta acción no se puede deshacer.

Agregar y modificar ubicaciones de red con PowerShell

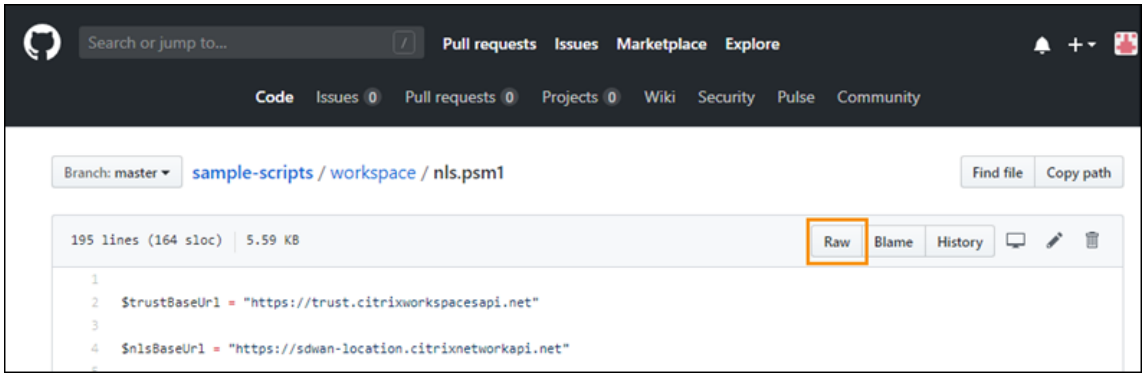
En lugar de usar la interfaz de la consola de administración de Citrix Cloud, puede usar un script de PowerShell para configurar la conexión directa a la carga de trabajo. La configuración de la conexión directa de carga de trabajo con PowerShell conlleva las siguientes tareas:

1. Determine los intervalos de direcciones IP públicas de cada ubicación de sucursal desde la que se conectan los usuarios internos.
2. Descargue el módulo de PowerShell.
3. Cree un cliente de API seguro en Citrix Cloud y anote el ID y el secreto del cliente.
4. Importe el módulo de PowerShell y conéctese al servicio de ubicación de red (NLS) con los detalles del cliente API.
5. Cree sitios NLS para cada una de sus ubicaciones de sucursal con los rangos de direcciones IP públicas que haya determinado previamente. La conexión directa de carga de trabajo se habilita automáticamente para cualquier inicio que provenga de las ubicaciones de red internas que haya especificado.
6. Inicie una aplicación o escritorio desde un dispositivo de la red interna y compruebe que la conexión va directamente al VDA, sin pasar por la puerta de enlace. Para obtener más información, consulte Registros de archivos ICA en este artículo.

Descargar el módulo de PowerShell

Antes de configurar las ubicaciones de red, descargue el módulo de PowerShell (nls.psm1) suministrado por Citrix desde el repositorio de GitHub para Citrix. Con este módulo, puede configurar tantas ubicaciones de red como sea necesario para los VDA.

1. En un explorador web, vaya a https://github.com/citrix/sample-scripts/blob/master/workspace/NLS2.psm1.
2. Presione **ALT** mientras hace clic en el botón **Raw**.



3. Seleccione una ubicación en la máquina y haga clic en **Save**.

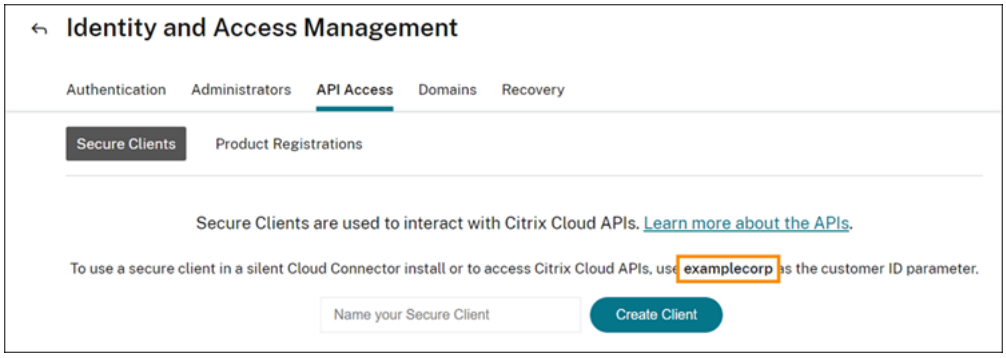
Detalles de configuración requeridos

Para configurar las ubicaciones de red, necesita la siguiente información:

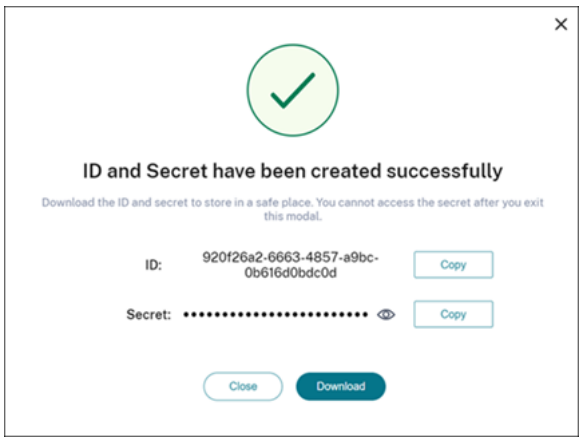
- El ID de cliente seguro de Citrix Cloud, el ID de cliente y el secreto de cliente. Para obtener estos valores, consulte Crear un cliente seguro en este artículo.
- Rangos de direcciones IP públicas de las redes desde las que se conectan los usuarios internos. Para obtener más información acerca de estos rangos de direcciones IP públicas, consulte la sección Requisitos de este artículo.

Crear un cliente seguro

1. Inicie sesión en Citrix Cloud desde `https://citrix.cloud.com`.
2. Desde el menú de Citrix Cloud, seleccione **Administración de acceso e identidad** y, luego, **Acceso a API**.
3. En la ficha **Clientes seguros**, anote su ID de cliente.



4. Escriba un nombre para el cliente y, a continuación, seleccione **Crear cliente**.
5. Copie el ID del cliente y el secreto del cliente.



Configurar ubicaciones de red

1. Abra una ventana de comandos de PowerShell y vaya hasta el mismo directorio donde guardó el módulo de PowerShell.
2. Importe el módulo: `Import-Module .\nls.psm1 -Force`
3. Establezca las variables requeridas con la información de cliente seguro desde Crear un cliente seguro:
   - `$clientId = "YourSecureClientID"`
   - `$customer = "YourCustomerID"`
   - `$clientSecret = "YourSecureClientSecret"`
4. Conéctese al servicio de ubicación de red con sus credenciales de cliente seguro:

```
Connect-NLS -clientId $clientId -clientSecret $clientSecret -
    customer $customer
```

5. Cree una ubicación de red. Para ello, sustituya los valores de los parámetros por los valores que corresponden a la red interna desde la que los usuarios internos se conectan directamente:

```
New-NLSSite -name "YourSiteName" -tags @("YourTags") -ipv4Ranges @
    ("PublicIpsOfYourNetworkSites") -longitude 12.3456 -latitude
    12.3456 -internal $True
```

   Para especificar una única dirección IP en lugar de un intervalo, agregue **/32** al final de la dirección IP. Por ejemplo:

```
New-NLSSite -name "YourSiteName" -tags @("YourTags") -ipv4Ranges @
    ("PublicIpOfYourNetworkSite/32") -longitude 12.3456 -latitude
    12.3456 -internal $True
```


> **Importante:**
>
> Al utilizar el comando `New-NLSSite`, incluya al menos un valor para cada parámetro. Si ejecuta este comando sin argumentos de línea de comandos, PowerShell le pedirá que introduzca los valores adecuados para cada parámetro, de uno en uno. La propiedad `internal` es una propiedad booleana obligatoria con valores posibles `$True` o `$False` que se asigna a la interfaz de usuario a través de PowerShell. Por ejemplo: `(UI)Network Internal -> (PowerShell)-internal=$True`.

Cuando la ubicación de red se crea correctamente, la ventana de comandos muestra los detalles de la ubicación de red.

6. Repita el paso 5 para todas las ubicaciones de red desde las que se conectan los usuarios.
7. Ejecute el comando `Get-NLSSite` para ver una lista de todos los sitios que haya configurado con NLS y compruebe que los datos de esos sitios son correctos.

Modificar ubicaciones de red

Para cambiar una ubicación de red existente:

1. Desde una ventana de comandos de PowerShell, indique todas las ubicaciones de red existentes: `Get-NLSSite`
2. Para modificar el intervalo de IP de una ubicación de red específica, escriba

   ```
   (Get-NLSSite)[N] | Set-NLSSite -ipv4Ranges @("1.2.3.4/32","4.3.2.1/32")
   ```

   donde `[N]` es el número correspondiente a la ubicación en la lista (a partir de cero) y `"1.2.3.4/32","4.3.2.1/32"` son los intervalos de IP, separados por comas, que quiere usar. Por ejemplo, para modificar la primera ubicación de la lista, escriba el siguiente comando:

   ```
   (Get-NLSSite)[0] | Set-NLSSite -ipv4Ranges @("98.0.0.1/32","141.43.0.0/24")
   ```

Eliminar ubicaciones de red

Para eliminar las ubicaciones de red que ya no quiere utilizar:

1. Desde una ventana de comandos de PowerShell, indique todas las ubicaciones de red existentes: `Get-NLSSite`
2. Para quitar todas las ubicaciones de red, escriba `Get-NLSSite | Remove-NLSSite`

3. Para quitar ubicaciones de red específicas, escriba `(Get-NLSSite)[N] | Remove-NLSSite`, donde `[N]` es el número correspondiente a la ubicación de la lista. Por ejemplo, para quitar la primera ubicación de la lista, escriba `(Get-NLSSite)[0] | Remove-NLSSite`.

Verificar que los inicios internos se redirigen correctamente

Para comprobar que los inicios internos acceden directamente a los VDA, utilice uno de los métodos siguientes:

- Consulte las conexiones de VDA a través de la consola de DaaS.
- Utilice los registros de archivos ICA para verificar la dirección correcta de la conexión del cliente.

Consola de Citrix DaaS

Seleccione **Administrar > Supervisar** y, a continuación, busque un usuario con una sesión activa. En la sección **Detalles de la sesión** de la consola, las conexiones VDA directas se muestran como conexiones UDP, mientras que las conexiones de la puerta de enlace se muestran como conexiones TCP.

Si no ve UDP en la consola de DaaS, debe habilitar la directiva de transporte adaptable de HDX para los VDA.

Registros de archivos ICA

Habilite los registros de archivos ICA en el equipo cliente, tal y como se describe en Para habilitar la captura de registros del archivo launch.ica. Después de iniciar las sesiones, consulte las entradas **Address** y **SSLProxyHost** en el archivo de registro.

Conexiones de VDA directas Para las conexiones directas de VDA, la propiedad **Address** contiene la dirección IP y el puerto del VDA.

A continuación, se muestra un ejemplo de un archivo ICA cuando un cliente inicia una aplicación mediante NLS:

```
1 [Notepad++ Cloud]
2 Address=;10.0.1.54:1494
3 SSLEnable=Off
4 <!--NeedCopy-->
```

La propiedad **SSLProxyHost** no está presente en este archivo. Esta propiedad se incluye solo para inicios a través de una puerta de enlace.

Conexiones de puerta de enlace Para las conexiones de puerta de enlace, la propiedad **Address** contiene el tíquet STA de Citrix Cloud, la propiedad **SSLEnable** se establece en **On** y la propiedad **SSLProxyHost** contiene el FQDN y el puerto de la puerta de enlace.

A continuación, se muestra un ejemplo de un archivo ICA cuando un cliente tiene una conexión a través de Citrix Gateway Service e inicia una aplicación:

```
[PowerShell ISE Cloud]
Address=;40;CWSSTA;027C02199068B33889A40C819A85CBB4
SSLEnable=On
SSLProxyHost=global.g.nssvcstaging.net:443
<!--NeedCopy-->
```

A continuación, se muestra un ejemplo de un archivo ICA cuando un cliente tiene una conexión a través de una puerta de enlace local e inicia una aplicación mediante una puerta de enlace local que está configurada dentro de la ubicación de recursos:

```
[PowerShell ISE Cloud]
Address=;40;CWSSTA;027C02199068B33889A40C819A85CBB5
SSLEnable=On
SSLProxyHost=onpremgateway.domain.com:443
<!--NeedCopy-->
```

> **Nota:**
>
> Los servidores virtuales de la puerta de enlace local que se utilizan para iniciar aplicaciones y escritorios virtuales deben ser servidores virtuales VPN, no servidores virtuales de autenticación nFactor. Los servidores virtuales de autenticación nFactor son solo para la autenticación de usuarios y no hacen de intermediarios del tráfico de inicios ICA ni HDX de recursos.

Ejemplo de script

El script de ejemplo incluye todos los comandos que puede necesitar para agregar, modificar y quitar los rangos de direcciones IP públicas de las ubicaciones de sucursal. Sin embargo, no es necesario ejecutar todos los comandos para realizar una sola función. Para que se ejecute el script, incluya siempre las primeras 10 líneas, desde **Import-Module** hasta **Connect-NLS**. Después, puede incluir solo los comandos de las funciones que quiere realizar.

```
Import-Module .\nls.psm1 -Force

$clientId = "XXXX" #Replace with your clientId
$clientSecret = "YYY"    #Replace with your clientSecret
$customer = "CCCCCC"  #Replace with your customerid

# Connect to Network Location Service
Connect-NLS -clientId $clientId -clientSecret $clientSecret -customer
    $customer
```



```
9
10 # Create a new Network Location Service Site (Replace with details
       corresponding to your branch locations)
11 New-NLSSite -name "New York" -tags @("EastCoast") -ipv4Ranges @("
       1.2.3.0/24") -longitude 40.7128 -latitude -74.0060 -internal $True
12
13 # Get the existing Network Location Service Sites (optional)
14 Get-NLSSite
15
16 # Update the IP Address ranges of your first Network Location Service
       Site (optional)
17 $s = (Get-NLSSite)[0]
18 $s.ipv4Ranges = @("1.2.3.4/32","4.3.2.1/32")
19 \$s | Set-NLSSite
20
21 # Remove all Network Location Service Sites (optional)
22 Get-NLSSite | Remove-NLSSite
23
24 # Remove your third site (optional)
25 \(Get-NLSSite)\[2] | Remove-NLSSite
```

Solución de problemas

Fallos de inicio del VDA

Si no se inician sesiones de VDA, compruebe que está utilizando rangos de direcciones IP públicas de la red correcta. Al configurar las ubicaciones de red, debe utilizar los intervalos de direcciones IP públicas de la red desde la que se conectan los usuarios internos para llegar a Internet. Para obtener más información, consulte la sección Requisitos de este artículo.

Los inicios internos de VDA siguen redirigiéndose a través de la puerta de enlace

Si las sesiones de VDA iniciadas internamente siguen redirigiéndose a través de la puerta de enlace como si fueran sesiones externas, compruebe que está utilizando la dirección IP pública correcta desde la que se conectan los usuarios internos para llegar a su espacio de trabajo. La dirección IP pública que aparece en el sitio NLS debe corresponder a la dirección que utiliza el cliente que inicia los recursos para acceder a Internet. Para obtener la dirección IP pública correcta para el cliente, inicie sesión en la máquina del cliente, visite un motor de búsqueda e introduzca “what is my IP”en la barra de búsqueda.

Todos los clientes que inician recursos dentro de la misma ubicación de oficina suelen acceder a Internet con la misma dirección IP pública de salida de la red. Estos clientes deben tener una ruta de red de Internet a las subredes en las que residen los VDA, que no esté bloqueada por un firewall. Para obtener más información, consulte la sección Requisitos de este artículo.

Errores al ejecutar cmdlets de PowerShell en plataformas que no son de Windows

Si se encuentra con errores al ejecutar cmdlets con los parámetros correctos en PowerShell Core, compruebe que la operación se llevó a cabo correctamente. Por ejemplo, si ve errores al ejecutar el cmdlet New-NLSSite, ejecute `Get-NLSSite` para comprobar que se creó el sitio. La ejecución de estos cmdlets en plataformas macOS o Linux con PowerShell Core puede provocar un error, aunque la operación se haya ejecutado correctamente.

Si ve este problema al ejecutar cmdlets con los parámetros correctos en una plataforma Windows mediante PowerShell, compruebe que está utilizando la versión más reciente del módulo de PowerShell. Con la versión más reciente del módulo de PowerShell, este problema no se produce en plataformas Windows.

Asistencia y ayuda adicionales

Si tiene dudas o necesita ayuda para solucionar problemas, contacte con su representante de ventas de Citrix o con Citrix Support.

Continuidad del servicio

November 21, 2023

La continuidad del servicio elimina o minimiza la dependencia de la disponibilidad de los componentes involucrados en el proceso de conexión. Los usuarios pueden iniciar sus aplicaciones y escritorios de Citrix DaaS, independientemente del estado de los servicios en la nube.

La continuidad del servicio permite a los usuarios conectarse a sus aplicaciones y escritorios de DaaS durante interrupciones del servicio, siempre y cuando el dispositivo de usuario mantenga una conexión de red a una ubicación de recursos. Los usuarios pueden conectarse a las aplicaciones y escritorios de DaaS durante interrupciones del servicio en componentes de Citrix Cloud o en nubes públicas y privadas. Los usuarios pueden conectarse a la ubicación del recurso directamente o a través de Citrix Gateway Service.

La continuidad del servicio mejora la representación visual de los recursos publicados durante las interrupciones, gracias al uso de la tecnología de trabajador de servicio con aplicaciones web progresivas para almacenar en caché los recursos en la interfaz de usuario.

La continuidad del servicio utiliza concesiones de conexión de Workspace para permitir a los usuarios acceder a las aplicaciones y los escritorios durante las interrupciones. Las concesiones de conexión de Workspace son tokens de autorización de larga duración. Los archivos de concesión de conexión de Workspace se almacenan de forma segura en caché, en el dispositivo del usuario Cuando un usuario

inicia sesión en Citrix Workspace, los archivos de concesión de conexión de Workspace se guardan en el perfil de usuario para cada recurso publicado para dicho usuario. La continuidad del servicio permite a los usuarios acceder a las aplicaciones y escritorios durante una interrupción, incluso si el usuario nunca ha iniciado una aplicación o escritorio antes. Los archivos de concesión de conexión de Workspace están firmados y cifrados, y están asociados al usuario y al dispositivo del usuario. Cuando se habilita la continuidad del servicio, una concesión de conexión de Workspace permite a los usuarios acceder a las aplicaciones y escritorios durante siete días de forma predeterminada. Puede configurar las concesiones de conexión de Workspace para permitir el acceso durante un máximo de 30 días.

Cuando los usuarios salen de la aplicación Citrix Workspace, esta se cierra, pero se conservan las concesiones de conexión de Workspace. Para salir de la aplicación Citrix Workspace, los usuarios deben hacer clic con el botón secundario en su icono de la bandeja del sistema o reiniciar el dispositivo de usuario. Puede configurar la continuidad del servicio para eliminar o conservar las concesiones de conexión de Workspace cuando los usuarios cierran sesión en Citrix Workspace durante una interrupción. De forma predeterminada, las concesiones de conexión de Workspace se eliminan de los dispositivos de usuario cuando los usuarios cierran sesión durante una interrupción.

La continuidad del servicio es compatible con casos de doble salto cuando la aplicación Citrix Workspace está instalada en un escritorio virtual.

Para ver un artículo técnico detallado sobre las funciones de resiliencia de Citrix Cloud, incluida la continuidad del servicio, consulte Citrix Cloud Resiliency.

> **Nota:**
>
> La antigua función de Citrix DaaS conocida como "concesión de conexiones"se asemeja a las concesiones de conexión de Workspace en que mejoraba la resiliencia de la conexión durante las interrupciones de servicio. Por lo demás, esa funcionalidad, ya retirada, no está relacionada con la continuidad del servicio.

Configuración del dispositivo de usuario

Para acceder a los recursos durante una interrupción, los usuarios deben haber iniciado sesión en Citrix Workspace antes de que esta ocurra. Cuando habilita la continuidad del servicio, los usuarios deben seguir estos pasos en sus dispositivos:

1. Descargar e instalar una versión compatible de la aplicación Citrix Workspace.
2. Agregar la URL de Workspace de su organización a la aplicación Citrix Workspace (por ejemplo, `https://example.cloud.com`).
3. Iniciar sesión en Citrix Workspace.

Cuando un usuario inicia sesión en Citrix Workspace por primera vez, la continuidad del servicio descarga las concesiones de conexión de Workspace en el dispositivo del usuario.

Al iniciar sesión por primera vez, la descarga de las concesiones de conexión de Workspace puede tardar hasta 15 minutos. Los usuarios pueden seguir iniciando recursos publicados durante el período de descarga.

Experiencia del usuario durante una interrupción

Cuando se habilita la continuidad del servicio, la experiencia del usuario durante una interrupción varía en función de:

- El tipo de interrupción del servicio
- Si la aplicación Citrix Workspace está configurada con autenticación PassThrough de dominio
- Si las sesiones compartidas están habilitadas para el escritorio o la aplicación a los que se conecta el usuario

En el caso de algunas interrupciones de servicio, los usuarios continúan accediendo a DaaS sin ningún cambio en su experiencia de usuario. Con otras interrupciones, es posible que el usuario advierta un cambio en la forma en que aparece Workspace o que se le pida que lleve a cabo alguna acción.

En esta tabla, se resume cómo la continuidad del servicio ayuda a los usuarios a acceder a aplicaciones y escritorios durante diferentes tipos de interrupciones.

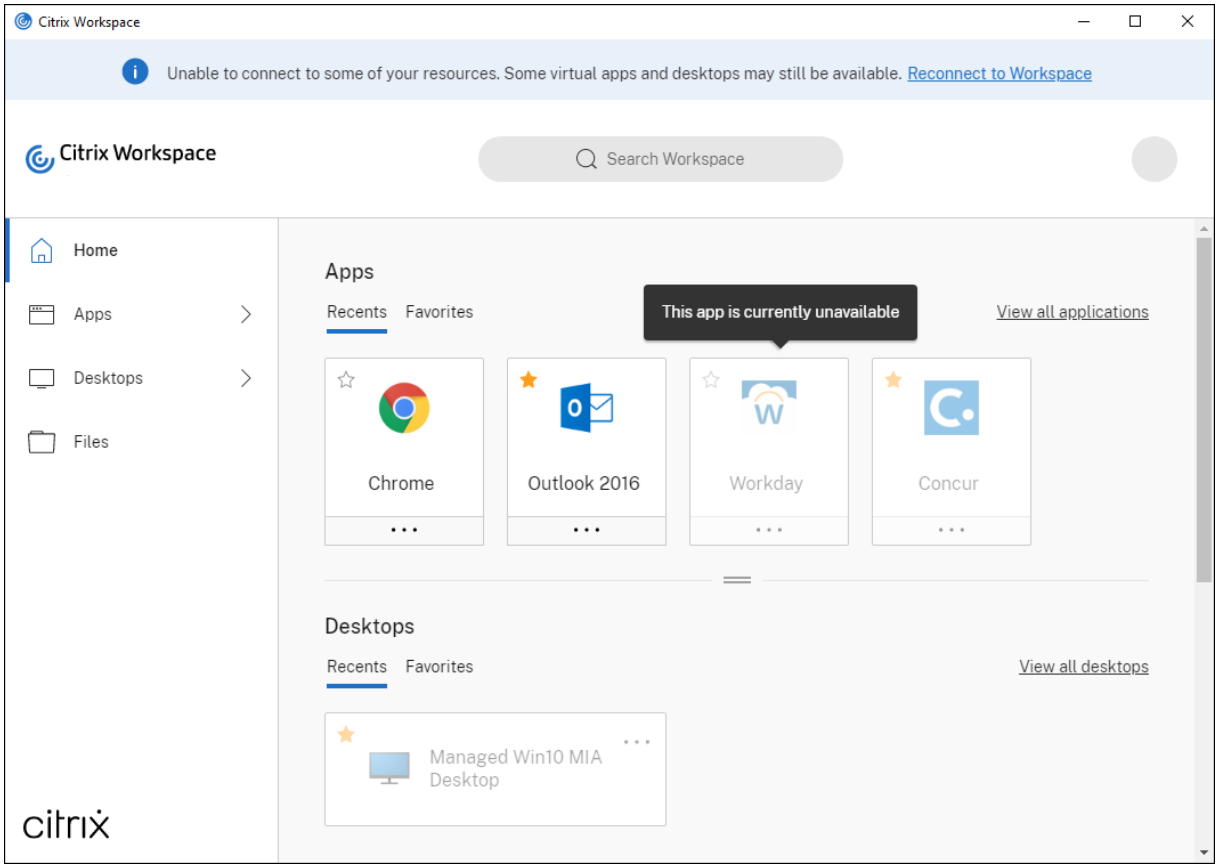
Dónde se produce la interrupción	Cómo se mantiene el acceso de los usuarios con continuidad del servicio	Experiencia de usuario durante una interrupción
Citrix Workspace Service	La aplicación Citrix Workspace enumera las aplicaciones y los escritorios en función de la caché local del dispositivo del usuario.	Los iconos de las aplicaciones y escritorios no disponibles aparecen atenuados. Los usuarios pueden seguir accediendo a las aplicaciones y escritorios que tienen iconos sin atenuar. Después de hacer clic en un icono sin atenuar, es posible que se pida a los usuarios que vuelvan a introducir sus credenciales en el VDA. Para recuperar el acceso a todas sus aplicaciones y escritorios, los usuarios pueden intentar establecer la conexión con Workspace haciendo clic en el enlace "Conectarse de nuevo a Workspace".
Proveedor de identidades	La aplicación Citrix Workspace enumera las aplicaciones y los escritorios en función de la caché local del dispositivo del usuario.	Es posible que los usuarios no puedan iniciar sesión en Workspace. Los usuarios hacen clic en el enlace "Usar Workspace sin conexión"para acceder a algunas aplicaciones y escritorios en una experiencia idéntica a una interrupción del servicio de Workspace.

Dónde se produce la interrupción	Cómo se mantiene el acceso de los usuarios con continuidad del servicio	Experiencia de usuario durante una interrupción
Broker Service de Citrix Cloud	High Availability Service (Servicio de alta disponibilidad) en el Cloud Connector se hace cargo de la intermediación. Todos los VDA que se registraron en Cloud Broker Service se registran en High Availability Service.	Es posible que algunos usuarios no puedan acceder a los recursos virtuales mientras los VDA se registran en High Availability Service. Las sesiones existentes no se ven afectadas. No es necesaria ninguna acción por parte del usuario.
Secure Ticket Authority	Las concesiones de conexión de Workspace proporcionan acceso a los recursos virtuales cuando los archivos ICA no pueden hacerlo.	Los inicios de sesión pueden tardar unos segundos más. No es necesaria ninguna acción por parte del usuario.
Citrix Gateway Service	Tiene lugar un proceso de conmutación por error del tráfico de red al punto de presencia (POP) de Citrix Gateway Service más cercano.	Es posible que las sesiones existentes tarden unos segundos en volver a conectarse. No es necesaria ninguna acción por parte del usuario.

Dónde se produce la interrupción	Cómo se mantiene el acceso de los usuarios con continuidad del servicio	Experiencia de usuario durante una interrupción
Conexión a Internet en la LAN	La aplicación Citrix Workspace enumera las aplicaciones y los escritorios en función de la caché local del dispositivo del usuario. Si un usuario tiene una conexión de red directa a la ubicación de recursos, la aplicación Citrix Workspace omite Citrix Gateway Service cuando el usuario hace clic en iconos sin atenuar. La aplicación Citrix Workspace se pone en contacto con Cloud Connector a través del puerto TCP 2598 y con los VDA a través de los puertos TCP 2598 o UDP 2598.	Los iconos de las aplicaciones y escritorios no disponibles aparecen atenuados. Los usuarios pueden seguir accediendo a las aplicaciones y escritorios que tienen iconos sin atenuar. Después de hacer clic en un icono sin atenuar, es posible que se pida a los usuarios que vuelvan a introducir sus credenciales en el VDA. Para recuperar el acceso a todas sus aplicaciones y escritorios, los usuarios pueden intentar establecer la conexión con Workspace haciendo clic en el enlace "Conectarse de nuevo a Workspace".

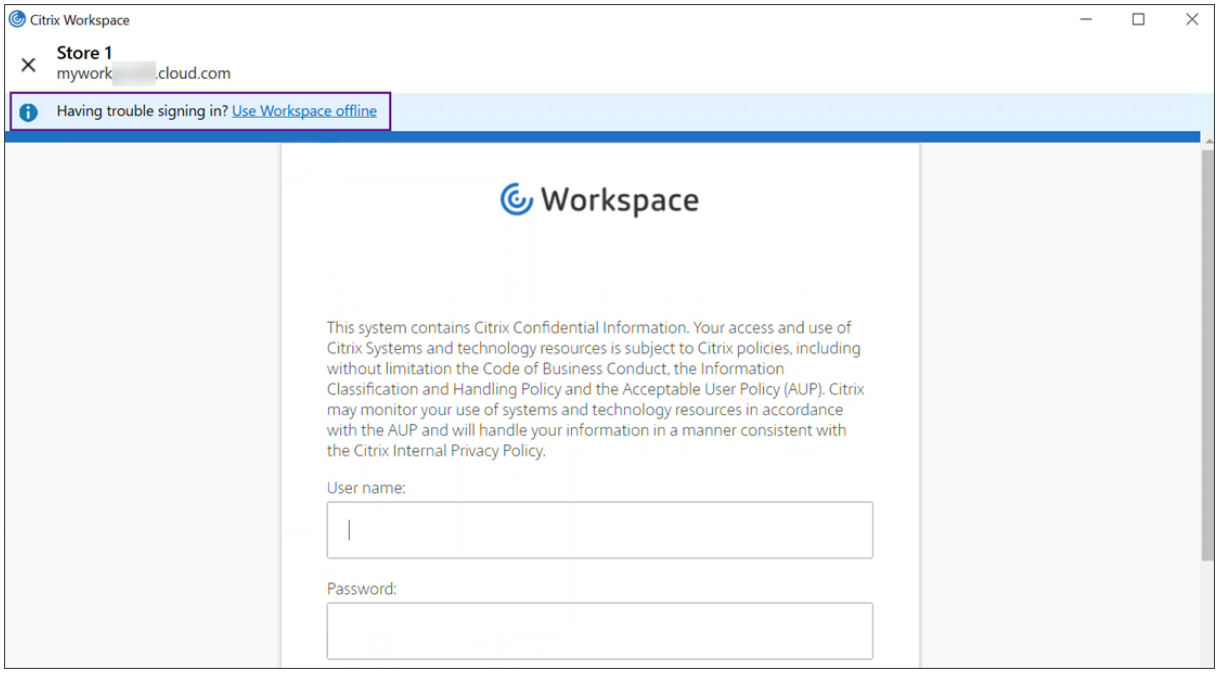
> **Nota:**
>
> Para obtener información sobre la validación de casos de interrupción del servicio en un entorno que no sea de producción, consulte la guía Service Continuity Companion Guide.

Durante una interrupción de Citrix Workspace, se muestra el siguiente mensaje a los usuarios en la parte superior de la página de inicio de Citrix Workspace: "No se puede conectar con algunos de sus recursos. Es posible que algunas aplicaciones y escritorios virtuales sigan estando disponibles". Durante la interrupción, los usuarios pueden ver las aplicaciones y escritorios a los que pueden conectarse. Si una aplicación o el escritorio no están disponibles, su icono aparece atenuado.



Para acceder a recursos disponibles durante una interrupción del servicio, los usuarios deben seleccionar un icono de recurso que no esté atenuado. Si se le pide, el usuario deberá reintroducir sus credenciales de AD en el VDA para poder acceder a los recursos.

Durante una interrupción con el proveedor de identidades para la autenticación del espacio de trabajo, es posible que los usuarios no puedan iniciar sesión en Citrix Workspace a través de la página de inicio de sesión de Workspace. Después de 40 segundos, este mensaje aparece en la parte superior de la página de inicio de Citrix Workspace.



A continuación, aparecerá la página de inicio de Citrix Workspace. Los usuarios podrán entonces acceder a los recursos como lo harían durante una interrupción de Citrix Workspace.

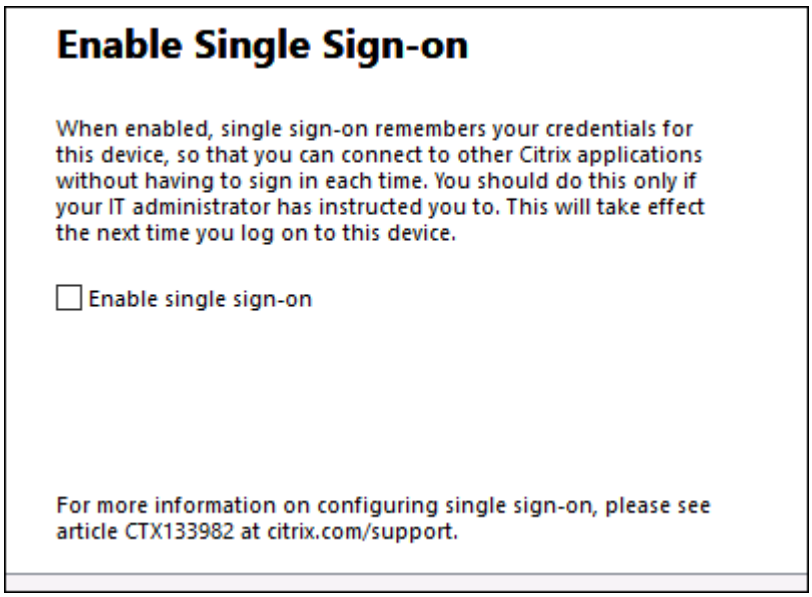
Independientemente del tipo de interrupción, los usuarios pueden seguir accediendo a los recursos si cierran la aplicación Citrix Workspace y la reinician. Los usuarios pueden reiniciar sus dispositivos de usuario sin perder el acceso a los recursos.

En la configuración predeterminada de continuidad del servicio, los usuarios pierden el acceso a sus recursos si cierran sesión en Citrix Workspace. Si quiere que los usuarios conserven el acceso a sus recursos después de cerrar la sesión, especifique que las concesiones de conexión de Workspace se conserven cuando los usuarios cierran sesión. Consulte Configurar la continuidad del servicio.

Según cómo estén configurados la aplicación Citrix Workspace y los VDA, durante una interrupción del servicio, es posible que el VDA pida los usuarios que introduzcan sus credenciales en la interfaz de usuario de inicio de sesión de Windows. En tal caso, los usuarios deberán introducir sus credenciales de Active Directory (AD) o el PIN de tarjeta inteligente para acceder a la aplicación o al escritorio. Este paso es necesario cuando las credenciales de usuario no se transfieren durante las interrupciones del servicio. Antes de acceder a una aplicación o escritorio, los usuarios deben volver a autenticarse en el VDA.

Los usuarios pueden acceder a los recursos sin introducir sus credenciales de AD si:

- Citrix Workspace se configura para Single Sign-On durante la instalación al marcar la casilla Single Sign-On.



- La aplicación Citrix Workspace se configura con autenticación PassThrough de dominio. Los usuarios pueden acceder a cualquier recurso disponible durante una interrupción de Citrix Workspace sin introducir sus credenciales. Para obtener información sobre cómo configurar la autenticación Pass Through de dominio para la aplicación Citrix Workspace para Windows, consulte Configurar Single Sign-On mediante la interfaz gráfica de usuario, que se encuentra en la documentación de **Autenticación**.

  > **Nota**
  >
  > StoreFront no es necesario para permitir Single Sign-On en el VDA durante una interrupción del servicio.

- Las sesiones compartidas están habilitadas. Los usuarios pueden acceder a las aplicaciones o escritorios alojados en el mismo VDA después de proporcionar sus credenciales para un recurso de ese VDA. Las sesiones compartidas están configuradas para el grupo de aplicaciones que contiene el recurso en el VDA. Para obtener información sobre cómo configurar grupos de aplicaciones, consulte Crear grupos de aplicaciones.

En todas las demás configuraciones, se pide a los usuarios que vuelvan a introducir sus credenciales de AD en el VDA antes de acceder a los recursos.

Requisitos y limitaciones

Requisitos del sitio

- Compatible con todas las ediciones de Citrix DaaS y Citrix DaaS Standard para Azure cuando se utiliza la experiencia de Workspace.

- No compatible con Citrix Workspace con agregación de sitios a Virtual Apps and Desktops local.
- No compatible cuando se usa Citrix Gateway local como proxy ICA (sí es compatible cuando se usa Citrix Gateway como método de autenticación de Workspace).

Requisitos del dispositivo del usuario

Versiones mínimas compatibles de la aplicación Citrix Workspace:

- Aplicación Citrix Workspace para Windows 2106
- Aplicación Citrix Workspace para Linux 2106
- Aplicación Citrix Workspace para Mac 2106
- Aplicación Citrix Workspace para Android 22.2.0
- Aplicación Citrix Workspace para iOS 22.4.5
- Aplicación Citrix Workspace para ChromeOS 2301

> **Nota:**
>
> Para obtener información sobre la instalación de la aplicación Citrix Workspace para Linux, incluida la información sobre cómo instalarla para usarla con la continuidad del servicio, consulte Aplicación Citrix Workspace para Linux.

- Para los usuarios que acceden a sus aplicaciones y escritorios mediante exploradores:
  - Google Chrome o Microsoft Edge.
  - Aplicación Citrix Workspace 2109 para Windows, como mínimo. Compatible con Google Chrome y Microsoft Edge.
  - Versión 2112 de la aplicación Citrix Workspace para Mac como mínimo para que pueda usarse con Google Chrome.
  - Versión 2206 de la aplicación Citrix Workspace para Mac como mínimo para que pueda usarse con el explorador Safari.

  Consulte Continuidad del servicio en exploradores.
- Solo se admite un usuario por dispositivo. Los dispositivos de usuario de tipo quiosco o "hot desk"(escritorio compartido) no son compatibles.

Métodos de autenticación de espacio de trabajo compatibles

- Active Directory
- Active Directory y token
- Azure Active Directory
- Okta

- Citrix Gateway (la notificación de usuario principal debe ser de AD)
- SAML 2.0

Limitaciones de autenticación

- No se admite Single Sign-On con el Servicio de autenticación federada (FAS) de Citrix. Los usuarios introducen sus credenciales de AD en la interfaz de usuario de Inicio de sesión de Windows del VDA.
- No se admite Single Sign-On en VDA.
- No se admiten cuentas asignadas locales.
- No se admiten los VDA unidos a Azure AD. Todos los VDA deben unirse a un dominio de AD.

Escala y tamaño de Citrix Cloud Connector

- 4 CPU virtuales o más
- 4 GB de memoria o más

Seguridad de PowerShell en Citrix Cloud Connector

Para asegurarse de que la ejecución del script esté habilitada, configure la directiva de ejecución en el valor **remotedSigned** adecuado para su entorno.
También pueden funcionar otros privilegios de ejecución de scripts, como **Default** o **AllSigned**.

Conectividad de Citrix Cloud Connector

Citrix Cloud Connector debe poder llegar a `https://rootoftrust.apps.cloud.com`. Configure el cortafuegos para permitir esta conexión. Para obtener información sobre el firewall de Cloud Connector, consulte Configuración del proxy y del firewall de Cloud Connector.

Conectividad de red de la aplicación Workspace

Si configura la conexión a la ubicación de recursos desde fuera de su LAN, la aplicación Workspace en los dispositivos de los usuarios debe poder alcanzar el FQDN de Citrix Gateway Service, `https://*.g.nssvc.net`. Asegúrese de que el firewall está configurado para permitir el tráfico saliente hacia `https://global-s.g.nssvc.net:433`, de modo que los dispositivos de los usuarios puedan conectarse a Citrix Gateway Service en todo momento.

Limitaciones de la optimización de conectividad

No se admite Advanced Endpoint Analysis (EPA).

No se admite Enlightened Data Transport (EDT) durante las interrupciones.

Requisitos y limitaciones de VDA

- Se admite VDA 7.15 LTSR o cualquier versión actual que no haya llegado al fin de vida.
- No se admiten los VDA unidos a Azure AD. Todos los VDA deben unirse a un dominio de AD.
- Los agentes VDA deben estar en línea para que los usuarios accedan a los recursos del VDA durante una interrupción. Los recursos de VDA no están disponibles cuando el VDA se ve afectado por interrupciones en:
  - AWS
  - Azure
  - Cloud Delivery Controller, a menos que Autoscale esté habilitado para el grupo de entrega que entrega el recurso
- Cargas de trabajo de VDA admitidas durante las interrupciones:
  - Aplicaciones y escritorios compartidos alojados
  - Escritorios aleatorios no persistentes (escritorios VDI agregados) con administración de energía
  - Escritorios estáticos no persistentes
  - Escritorios estáticos persistentes, incluido acceso con Remote PC

> **Nota:**
>
> Asignar en el primer uso no se admite durante las interrupciones de servicio. Los escritorios aleatorios no persistentes con administración de energía no están disponibles de forma predeterminada si los Cloud Connectors pierden la conectividad con Citrix Cloud, a menos que se configure `ReuseMachinesWithoutShutdownInOutage` para el grupo de entrega. Consulte Compatibilidad con aplicaciones y escritorios para obtener más información detallada.

Para obtener más información sobre las funciones de VDA disponibles durante las interrupciones, consulte Administración de VDA durante las interrupciones.

Requisitos y limitaciones de la asignación de teclado local

La interfaz de usuario de inicio de sesión de Windows que pide a los usuarios que vuelan a autenticarse en el VDA no admite la asignación de idioma del teclado local. Para que los usuarios puedan volver

a autenticarse durante una interrupción si tienen asignaciones de idioma de teclado locales en sus dispositivos, precargue las distribuciones de teclado correspondientes.

> **Advertencia:**
>
> Si se modifica el Registro de forma incorrecta, pueden producirse problemas graves que obliguen a reinstalar el sistema operativo. Citrix no puede garantizar que los problemas derivados de la utilización inadecuada del Editor del Registro puedan resolverse. Use el Editor del Registro bajo su propia responsabilidad. Haga una copia de seguridad del Registro antes de modificarlo.

Modifique esta clave de Registro en la imagen de VDA:

```
HKEY_USERS\.DEFAULT\Keyboard Layout\Preload
```

Debe instalarse el paquete de idioma correspondiente en la imagen del escritorio virtual.

Para obtener una lista de los identificadores de teclado asociados a los idiomas de teclado, consulte Identificadores de teclado y editores de métodos de entrada para Windows.

Configurar la conectividad de red de la ubicación de recursos para la continuidad del servicio

Puede configurar su ubicación de recursos para que acepte conexiones internas de la red de área local (LAN), conexiones externas a la LAN o ambas.

Configurar para conexiones internas de su LAN

1. En el menú de Citrix Cloud, vaya a **Configuración de Workspace > Acceso**.
2. Seleccione **Configurar conectividad**.
3. Seleccione **Solo interna** como tipo de conectividad.
4. Haga clic en **Guardar**.

Configure los firewalls de Citrix Cloud Connector y VDA para que acepten conexiones a través del puerto TCP 2598 con CGP. Esta es la configuración predeterminada.

Configurar conexiones externas a su LAN

1. En el menú de Citrix Cloud, vaya a **Configuración de Workspace > Acceso**.
2. Seleccione **Configurar conectividad**.
3. Seleccione **Gateway Service** como tipo de conectividad.
4. Haga clic en **Guardar**.

Configurar para conexiones tanto desde el exterior como desde el interior de la red LAN

Ejecute este comando de PowerShell:

```
Set-ConfigZone -InputObject (get-configzone -ExternalUid YourResourceLocationE
)-EnableHybridConnectivityForResourceLeases $true
```

Reemplace `YourResourceLocationExternalUid` por el identificador único global (UID) externo de la ubicación de recursos.

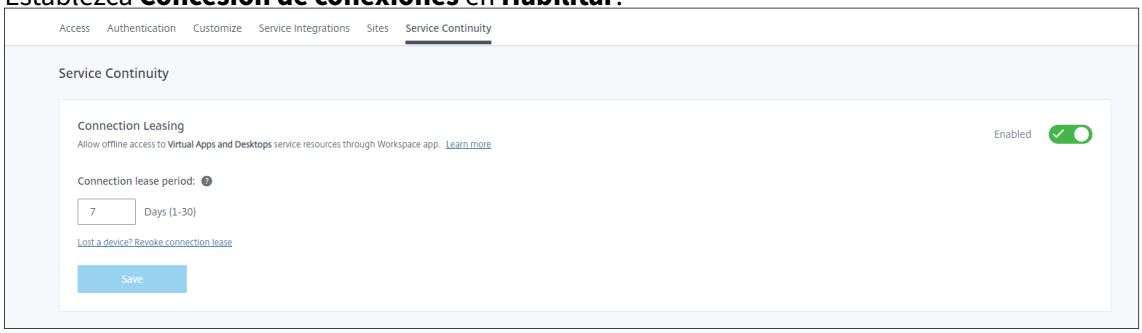
Este comando permite conexiones directas al FQDN del Citrix Cloud Connector a través del TCP 2598 durante las interrupciones del servicio. Si se produce un error en esa conexión, se usa Gateway Service como opción de reserva. Al permitir que los usuarios internos omitan la puerta de enlace y se conecten directamente a la ubicación de recursos, se reduce la latencia del tráfico de red interno.

> **Nota:**
>
> Este comando de PowerShell se parece a Conexión directa de carga de trabajo en que optimiza la conectividad a los espacios de trabajo permitiendo que los usuarios internos omitan la puerta de enlace y se conecten a los VDA directamente. Al habilitar la continuidad del servicio, la conexión directa de carga de trabajo no está disponible durante las interrupciones de servicio

Configurar la continuidad del servicio

Para habilitar la continuidad del servicio en su sitio:

1. En el menú de Citrix Cloud, vaya a **Configuración de Workspace > Continuidad del servicio**.
2. Establezca **Concesión de conexiones** en **Habilitar**.



3. Establezca el **Período de la concesión de conexiones** en el número de días que se puede utilizar una concesión de conexiones de Workspace para mantener una conexión. El período de concesión de conexiones de Workspace se aplica a todas las concesiones de conexión de Workspace a través del sitio. El período de concesión de conexiones de Workspace comienza la primera vez que un usuario inicia sesión en el almacén de Citrix Cloud Workspace. Las concesiones de conexiones de Workspace se actualizan cada vez que el usuario inicia sesión, hasta una vez al día. El período de concesión de conexiones de Workspace puede ser de un día a 30 días. El valor predeterminado es siete días.

4. Haga clic en **Guardar**.

Cuando habilita la continuidad del servicio, se habilita para todos los grupos de entrega de su sitio. Para inhabilitar la continuidad del servicio para un grupo de entrega, use el siguiente comando de PowerShell:

```
Set-BrokerDesktopGroup -name <deliverygroup> -ResourceLeasingEnabled $false
```

Sustituya `deliverygroup` por el nombre del grupo de entrega.

De forma predeterminada, las concesiones de conexión de Workspace se eliminan del dispositivo de usuario si el usuario cierra sesión en Citrix Workspace durante una interrupción. Si quiere que las concesiones de conexión de Workspace permanezcan en los dispositivos de usuario después de que estos cierren sesión, utilice el siguiente comando de PowerShell:

```
Set-BrokerSite -DeleteResourceLeasesOnLogOff $false
```

> **Nota:**
>
> Para los usuarios que conectan con la aplicación Citrix Workspace para Mac, las concesiones de conexión de Workspace no pueden configurarse de manera que permanezcan en los dispositivos de los usuarios después de que estos cierren sesión. Citrix Workspace para Mac no puede leer el valor de la propiedad `DeleteResourceLeaseOnLogOff`.

Cómo funciona la continuidad del servicio

Si no hay interrupciones de servicio, los usuarios acceden a las aplicaciones y escritorios virtuales mediante archivos ICA. Citrix Workspace genera un archivo ICA único cada vez que un usuario selecciona un icono de aplicación o escritorio virtual. Cada archivo ICA contiene un tíquet de STA y un tíquet de inicio de sesión que solo se puede canjear una vez para obtener acceso autorizado a los recursos virtuales. Los tíquets de cada archivo ICA caducan al cabo de unos 90 segundos. Tras utilizar el tíquet de un archivo ICA, o una vez que caduca, el usuario necesita otro archivo ICA de Citrix Workspace para poder acceder a los recursos. Cuando la continuidad del servicio no está habilitada, las interrupciones de servicio pueden impedir que los usuarios accedan a los recursos si Citrix Workspace no puede generar un archivo ICA.

Citrix Workspace genera archivos ICA cuando los usuarios inician aplicaciones y escritorios virtuales, independientemente de si la continuidad del servicio está habilitada. Cuando se habilita la continuidad del servicio, Citrix Workspace genera también el conjunto único de archivos que forman una concesión de conexiones de Workspace. A diferencia de los archivos ICA, los archivos de concesión de conexiones de Workspace se generan cuando el usuario inicia sesión en Citrix Workspace, no cuando el usuario inicia el recurso. Cuando un usuario inicia sesión en Citrix Workspace, se generan archivos de concesión de conexiones para cada recurso publicado para ese usuario. Las concesiones de

conexión de Workspace contienen información que otorga al usuario acceso a los recursos virtuales. Si una interrupción del servicio impide que un usuario inicie sesión en Citrix Workspace o acceda a recursos mediante un archivo ICA, la concesión de conexiones otorga al usuario acceso autorizado al recurso.

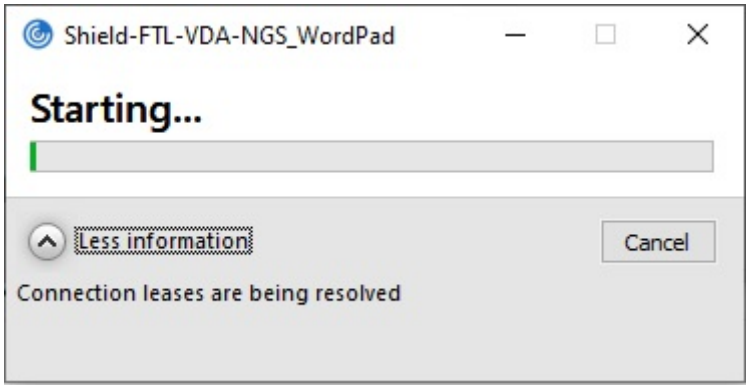
Cómo se inician las sesiones durante las interrupciones

Cuando los usuarios hacen clic en un icono de una aplicación o escritorio durante una interrupción de servicio, la aplicación Citrix Workspace encuentra la concesión de conexión de Workspace correspondiente en el dispositivo del usuario. A continuación, la aplicación Citrix Workspace abre una conexión. Si la conectividad con la ubicación de recursos que aloja la aplicación o el escritorio está configurada para aceptar conexiones de fuera de la LAN, se abre una conexión a Citrix Gateway Service. Si configura la conectividad con la ubicación de recursos que aloja la aplicación o el escritorio para aceptar solamente conexiones del interior de la LAN, se abre una conexión a Cloud Connector.

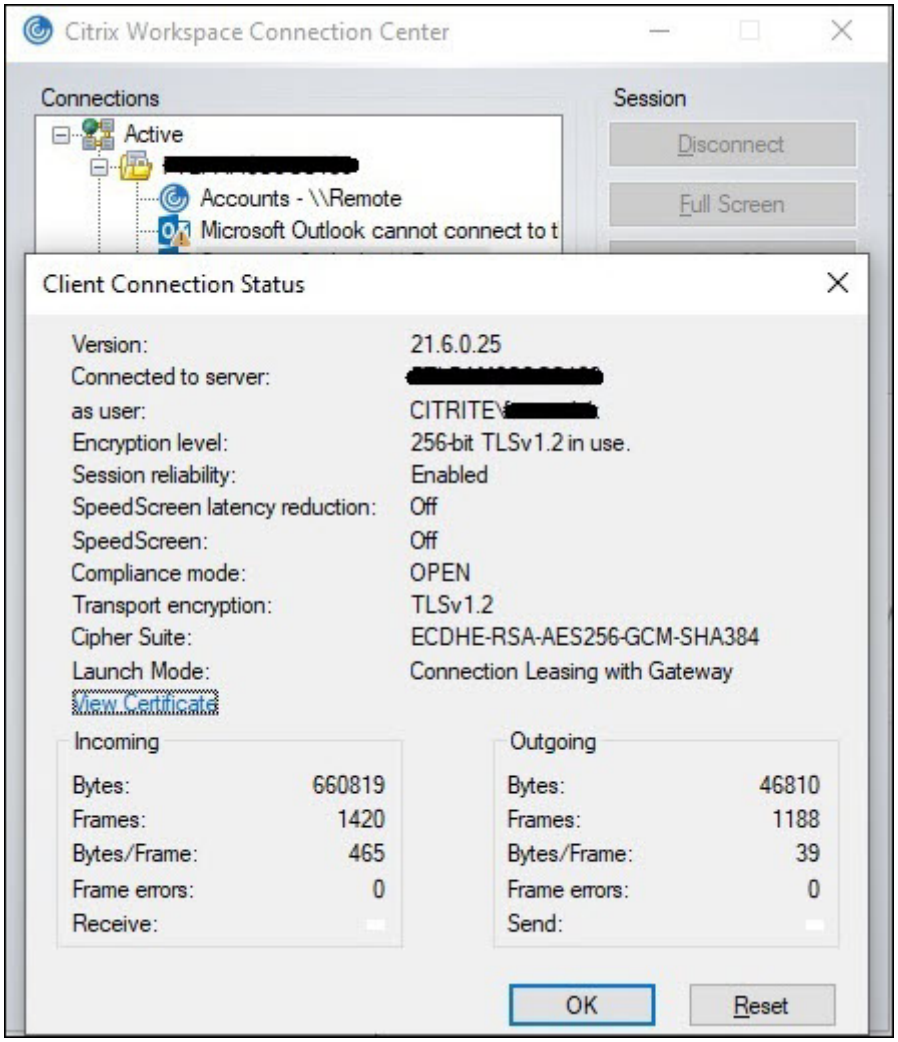
Cuando el broker de Citrix Cloud está en línea, Cloud Connector utiliza el broker de Citrix Cloud para resolver qué VDA está disponible. Cuando el broker de Citrix Cloud no está conectado, el broker secundario del Cloud Connector (también conocido como servicio de alta disponibilidad) escucha las solicitudes de conexión y las procesa.

Los usuarios que están conectados cuando se produce una interrupción pueden seguir trabajando sin interrupciones. En las conexiones nuevas y las reconexiones se dan demoras mínimas de conexión. Esta funcionalidad es similar a la caché de host local, pero no requiere un StoreFront local.

Cuando un usuario inicia una sesión durante una interrupción, aparece esta ventana que indica que se han utilizado concesiones de conexión de Workspace para el lanzamiento de la sesión:



Una vez que el usuario ha terminado de iniciar sesión, estas propiedades aparecen en la Central de conexiones de Workspace:



La propiedad de modo de inicio proporciona información sobre las concesiones de conexión de Workspace utilizadas para iniciar la sesión.

En los dispositivos que ejecutan la aplicación Citrix Workspace para Mac, Citrix Viewer muestra información que indica que las concesiones de conexión de Workspace se utilizaron para el inicio de la sesión:

Qué garantiza la seguridad

Toda la información confidencial de los archivos de concesión de conexiones de Workspace se cifra con cifrado AES-256. Las concesiones de conexión de Workspace están vinculadas a un par de claves público-privadas, asociadas exclusivamente al dispositivo cliente específico y no pueden utilizarse en otro dispositivo. Un mecanismo criptográfico integrado obliga al uso del par de claves único en cada dispositivo.

Las concesiones de conexión de Workspace se almacenan en el dispositivo de usuario, en AppData\ Local\ Citrix\ SelfService\ ConnectionLeases.

La arquitectura de seguridad de continuidad del servicio se basa en criptografía de clave pública, de manera similar a una infraestructura de clave pública (PKI), pero sin cadenas de certificados ni entidades de certificación (CA). En su lugar, todos los componentes establecen una confianza transitiva al confiar en un nuevo servicio de Citrix Cloud llamado "raíz de confianza"que actúa como una entidad de certificación.

Bloquear concesiones de conexión

Si se pierde o roba un dispositivo de usuario, o si una cuenta de usuario se cierra o está en situación de riesgo, puede bloquear las concesiones de conexión de Workspace. Cuando bloquea las concesiones de conexión de Workspace asociadas a un usuario, el usuario no puede conectarse a los recursos. Citrix Cloud ya no genera ni sincroniza las concesiones de conexión de Workspace para el usuario.

Al bloquear concesiones de conexión de Workspace asociadas a una cuenta de usuario, se bloquean las conexiones a esa cuenta en todos los dispositivos asociados a ella. Puede bloquear las concesiones de conexión de Workspace para un usuario o para todos los usuarios de un grupo de usuarios.

Para revocar las concesiones de conexión de Workspace para un solo usuario o grupo de usuarios, utilice este comando de PowerShell:

```
Set-BrokerConnectionLeaseRevocationDate -Name username -LeaseRevocationDays
 Days
```

Reemplace `username` por el usuario asociado a la cuenta que quiere impedir que se conecte. Reemplace `username` por un grupo de usuarios para bloquear la conexión de todas las cuentas del grupo de usuarios. Reemplace `Days` por la cantidad de días que quiere bloquear las conexiones.

Por ejemplo, para bloquear conexiones para xd.local/user1 durante los próximos 7 días, escriba:

```
1 Set-BrokerConnectionLeaseRevocationDate -Name xd.local/user1 -
     LeaseRevocationDays 7
```

Para ver el período de tiempo durante el que se revocan las concesiones de conexión de Workspace, utilice este comando de PowerShell:

```
Get-BrokerConnectionLeaseRevocationDate -Name username
```

Reemplace `username` por el usuario o grupo de usuarios para el que quiere ver el período de tiempo.

Por ejemplo, para ver el período de tiempo durante el que se revocan las concesiones de conexión de Workspace para xd.local/user1, escriba:

```
1 Get-BrokerConnectionLeaseRevocationDate -Name xd.local/user2
```

Aparece esta información:

```
1 FullName                          :
2 Name                              : XD\user2
3 UPN                               :
4 Sid                               : S-1-5-21-nnnnnn
5 LeaseRevocationDays               : 2
6 LeaseRevocationDateTimeInUtc      : 2020-12-17T17:34:25Z
7 LastUpdateDateTimeInUtc           : 2020-12-19T17:34:25Z
```

En este resultado se puede ver que el usuario xd.local/user2 tiene las concesiones de conexión de Workspace revocadas dos días, del 17 de diciembre de 2020 al 19 de diciembre de 2020, a las 17:34:25 UTC de los dos días.

Para permitir que una cuenta de usuario que con concesiones de conexión de Workspace revocadas reciba de nuevo la conexión, quite el bloqueo con este comando de PowerShell:

```
Remove-BrokerConnectionLeaseRevocationDate -Name username
```

Reemplace `username` por el usuario o grupo de usuarios bloqueados que quiere que reciban la conexión. Para permitir que todas las cuentas de usuario bloqueadas reciban conexiones, ignore la opción `Name`.

Casos de doble salto

La continuidad del servicio puede permitir a los usuarios acceder a recursos virtuales durante las interrupciones de servicio en casos de doble salto si iniciaron sesión en Citrix Workspace antes de producirse la interrupción. En un caso de doble salto, un dispositivo físico de usuario se conecta a un escritorio virtual que tiene instalada la aplicación Citrix Workspace. A continuación, el escritorio virtual se conecta a otro recurso virtual.

En el caso de doble salto, la continuidad del servicio puede permitir a los usuarios acceder a recursos virtuales durante una interrupción del servicio, independientemente del tipo de escritorio virtual. Si el escritorio virtual conserva los cambios del usuario, la continuidad del servicio también puede proporcionar acceso a recursos virtuales durante interrupciones que se producen cuando el usuario no ha iniciado sesión.

La continuidad del servicio trata el dispositivo físico de usuario y el dispositivo virtual en un caso de doble salto como dispositivos de punto final de cliente individuales. Cada dispositivo tiene su propio conjunto de concesiones de conexión de Workspace. Cuando un usuario inicia sesión en Citrix Workspace en un dispositivo físico, los archivos de concesión de conexión de Workspace se descargan y guardan en el perfil de usuario en el dispositivo físico. A continuación, el usuario accede a un escritorio virtual e inicia sesión en Citrix Workspace en el escritorio virtual. En este punto, se descarga un conjunto diferente de concesiones de conexión de Workspace y se guarda el perfil de usuario en el escritorio virtual. Los archivos de concesión de conexión de Workspace están asociados al dispositivo en el que se descargan. Los archivos de concesión de conexión de Workspace no se pueden copiar en otro dispositivo y reutilizarse, incluso por un mismo usuario. Por ello, la continuidad del servicio no puede proporcionar acceso a los recursos durante las interrupciones que se producen después de que finalice la sesión si el escritorio virtual descarta los cambios realizados durante una sesión de usuario. Para este tipo de escritorio virtual, las concesiones de conexión de Workspace se encuentran entre los cambios descartados.

A continuación, se explica cómo funciona la continuidad del servicio en casos de doble salto con cada tipo de escritorio virtual compatible.

Para dobles saltos que incluyen…	Continuidad del servicio puede proporcionar acceso a recursos virtuales durante interrupciones…
Escritorios compartidos alojados	Si la interrupción se produce cuando el usuario ha iniciado sesión en el escritorio virtual.
Escritorios aleatorios no persistentes (escritorios VDI agregados)	Si la interrupción se produce cuando el usuario ha iniciado sesión en el escritorio virtual.
Escritorios estáticos no persistentes	Si el escritorio virtual no se ha reiniciado desde la última vez que el usuario inició sesión.

Para dobles saltos que incluyen…	Continuidad del servicio puede proporcionar acceso a recursos virtuales durante interrupciones…
Escritorios estáticos persistentes	Cada vez que se produce una interrupción.

Administración de VDA durante las interrupciones

La continuidad del servicio utiliza la función Caché de host local en Citrix Cloud Connector. La caché de host local permite que la intermediación de conexiones en un sitio continúe cuando se interrumpa la conexión entre el Cloud Delivery Controller y el Cloud Connector. Dado que la continuidad del servicio depende de la caché de host local, comparte algunas limitaciones con esta.

> **Nota:**
>
> Aunque la continuidad del servicio utiliza la caché de host local dentro del Cloud Connector, a diferencia de la caché de host local no es compatible con StoreFront local.

Administración de energía de los VDA durante las interrupciones

Si los Cloud Connectors pierden la conectividad con Citrix Cloud, los Connectors no pueden recibir las credenciales de hipervisor de Citrix Cloud. Esto significa:

- Durante interrupciones del servicio, todas las máquinas se hallan en el estado de energía desconocido (unknown) y no se pueden emitir operaciones de administración de energía. No obstante, las máquinas virtuales del host que estén encendidas se pueden utilizar para las solicitudes de conexión.

De forma predeterminada, los VDA de escritorio con administración de energía de los grupos de entrega agrupados que tienen habilitada la propiedad **ShutdownDesktopsAfterUse** no están disponibles para nuevas conexiones si los Cloud Connectors pierden la conectividad con Citrix Cloud. Para cambiar este parámetro con el que permitir el uso de esos escritorios si los Cloud Connectors pierden la conectividad con Citrix Cloud, configure el indicador `ReuseMachinesWithoutShutdownInOutage` en sus grupos de entrega. Si cambia el parámetro `ReuseMachinesWithoutShutdownInOutage` a $true, es posible que los datos de las sesiones de usuario anteriores estén presentes en el VDA hasta que este se reinicie.

La administración de energía se reanuda al reanudarse las operaciones normales después de una interrupción.

Asignación de máquinas e inscripción automática

Una máquina asignada solo se puede usar si la asignación se dio durante el funcionamiento normal. No se pueden realizar asignaciones nuevas durante una interrupción del servicio.

No se puede configurar ni inscribir automáticamente las máquinas de acceso con Remote PC. En cambio, las máquinas que se inscribieron y configuraron durante el funcionamiento normal se pueden usar.

Recursos de VDA en diferentes zonas

Si los recursos están en zonas diferentes, es posible que los usuarios de aplicaciones y escritorios alojados en servidores superen la cantidad de sesiones indicadas en el límite configurado de sesiones.

A diferencia de la caché de host local, la continuidad del servicio puede iniciar aplicaciones y escritorios desde VDA registrados en zonas diferentes, siempre y cuando el recurso se publique en más de una zona. La aplicación Citrix Workspace puede tardar más en encontrar una zona en buen estado, ya que recorre secuencialmente todas las zonas de la concesión de conexiones de Workspace.

Supervisión y solución de problemas

La continuidad del servicio realiza dos acciones principales:

- Descargar las concesiones de conexión de Workspace en el dispositivo del usuario. Las concesiones de conexión de Workspace se generan y sincronizan con la aplicación Citrix Workspace.
- Iniciar los escritorios y las aplicaciones virtuales mediante concesiones de conexión de Workspace.

Solución de problemas de descarga de concesiones de conexión de Workspace

Se pueden ver las concesiones de conexión de Workspace en esta ubicación, en el dispositivo del usuario.

En dispositivos Windows:

`C:\Users\Username\AppData\Local\Citrix\SelfService\ConnectionLeases\Store GUID\User GUID\leases`

`Username` es el nombre de usuario.

`Store GUID` es el identificador único global del almacén de Workspace.

`User GUID` es el identificador único global del usuario.

En dispositivos Mac:

`$HOME/Library/Application Support/Citrix Receiver/CLSyncRoot`

Por ejemplo, abrir `/Users/luca/Library/Application Support/Citrix Receiver/CLSyncRoot`

En Linux:

`$HOME/.ICAClient/cache/ConnectionLease`

Por ejemplo, abrir `/home/user1/.ICAClient/cache/ConnectionLease`

Las concesiones de conexión de Workspace se generan cuando la aplicación Citrix Workspace se conecta al almacén de Workspace. Los valores de clave de Registro en el dispositivo del usuario sirven para determinar si la aplicación Citrix Workspace ha podido contactar con el servicio de concesión de conexiones de Workspace en Citrix Cloud.

Abra regedit en el dispositivo del usuario y consulte esta clave:

`HKCU\Software\Citrix\Dazzle\Sites\store-xxxx`

Si aparecen estos valores en la clave de Registro, la aplicación Citrix Workspace ha contactado o intentado contactar con el servicio de concesión de conexiones de Workspace:

- `leaseLastCallHomeTime`
- `leaseLastSyncStatus`

Si la aplicación Citrix Workspace no ha logrado contactar con el servicio de concesión de conexiones de Workspace, `leaseLastCallHomeTime` muestra un error con una marca de hora no válida:

```
leaseLastCallHomeTime REG_SZ 1/1/0001 12:00:00 AM
```

Si no se ha inicializado `leaseLastCallHomeTime`, la aplicación Citrix Workspace nunca intentó contactar con el servicio de concesión de conexiones de Workspace. Para resolver este problema, quite la cuenta de la aplicación Citrix Workspace y vuelva a agregarla.

Códigos de error de la aplicación Citrix Workspace para concesiones de conexión de Workspace

Cuando se produce un error de continuidad del servicio en el dispositivo del usuario, aparece un código de error en el mensaje de error. Entre los errores comunes se incluyen:

Código de error	Descripción
3000	No hay archivos de concesión de conexiones presentes
3002	No se puede leer o encontrar la concesión de conexiones

Código de error	Descripción
3003	No se ha encontrado ninguna ubicación de recursos
3004	Faltan detalles de conexión en las concesiones
3005	El archivo ICA está vacío
3006	La concesión de conexiones ha caducado. Vuelve a iniciar sesión en Workspace.
3007	La concesión de conexiones no es válida
3008	Resultado de validación de concesión de conexiones: vacío
3009	Resultado de validación de concesión de conexiones: no válido
3010	Faltan parámetros
3020	Error en la validación de concesión de conexiones
3021	No se encontró ninguna ubicación de recursos donde se haya publicado la aplicación
3022	Resultado de la validación de concesión de conexiones: denegar
3023	Tiempo de espera de la aplicación Citrix Workspace agotado
3024	El usuario canceló el inicio por arrendamiento mientras estaba en curso
3025	Se superó la cantidad de reintentos de inicio
3026	No se puede iniciar el recurso negociado (aplicación o escritorio)

Acceder a selfservice.txt

Para acceder al archivo `selfservice.txt` para la solución de problemas de autoservicio, siga estos pasos:

1. Cree un archivo de texto vacío y denomínelo `enableshieldandlogging.reg`.
2. Copie este texto en el archivo y guárdelo:

   Windows Registry Editor Version 5.00

   [HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Citrix\Dazzle]

"Tracing"="True"
"AuxTracing"="True"
"DefaultTracingConfiguration"="global all -detail"
"ConnectionLeasingEnabled"="True"

[HKEY_CURRENT_USER\Software\Citrix\Dazzle]
"RemoteDebuggingPort"="8088"

3. Coloque el archivo guardado en el dispositivo de punto final del cliente.
4. Ahora, el archivo `selfservice.txt` se podrá detectar en esta ruta: `%LocalAppData%\Citrix\SelfService`.

Continuidad del servicio en exploradores

Las extensiones para Google Chrome y Microsoft Edge ponen la continuidad del servicio a disposición de los usuarios de Windows que acceden a sus aplicaciones y escritorios con esos exploradores. Las extensiones se denominan extensiones web de Citrix Workspace y están disponibles en Chrome Web Store y en el sitio web de complementos de Microsoft Edge.

Estas extensiones de explorador requieren una aplicación Citrix Workspace nativa en el dispositivo del usuario para admitir la continuidad del servicio. Se admiten estas versiones:

- Aplicación Citrix Workspace 2109 para Windows, como mínimo. Compatible con Google Chrome y Microsoft Edge.
- Aplicación Citrix Workspace para Mac versión 2112, como mínimo. Compatible con Google Chrome.
- Versión 2206 de la aplicación Citrix Workspace para Mac como mínimo para que pueda usarse con el explorador Safari.

La aplicación Citrix Workspace para Tienda Windows no es compatible.

La aplicación Workspace nativa se comunica con la extensión web de Citrix Workspace mediante el protocolo del host de mensajería nativa para extensiones de explorador. Juntos, la aplicación Workspace nativa y la extensión web de Workspace utilizan las concesiones de conexión de Workspace para proporcionar a los usuarios del explorador acceso a sus aplicaciones y escritorios durante las interrupciones.

Este vídeo muestra cómo instalar y utilizar la continuidad del servicio en exploradores.

Esto es un vídeo incrustado. Haga clic en el enlace para ver el vídeo.

Configuración de dispositivos de usuario para usuarios de explorador

Para utilizar la continuidad del servicio en un explorador web, los usuarios deben seguir estos pasos en sus dispositivos:

1. Descargar e instalar una versión de la aplicación Citrix Workspace apta para los usuarios de exploradores.
2. Descargar e instalar la extensión web de Citrix Workspace para Chrome o Edge.

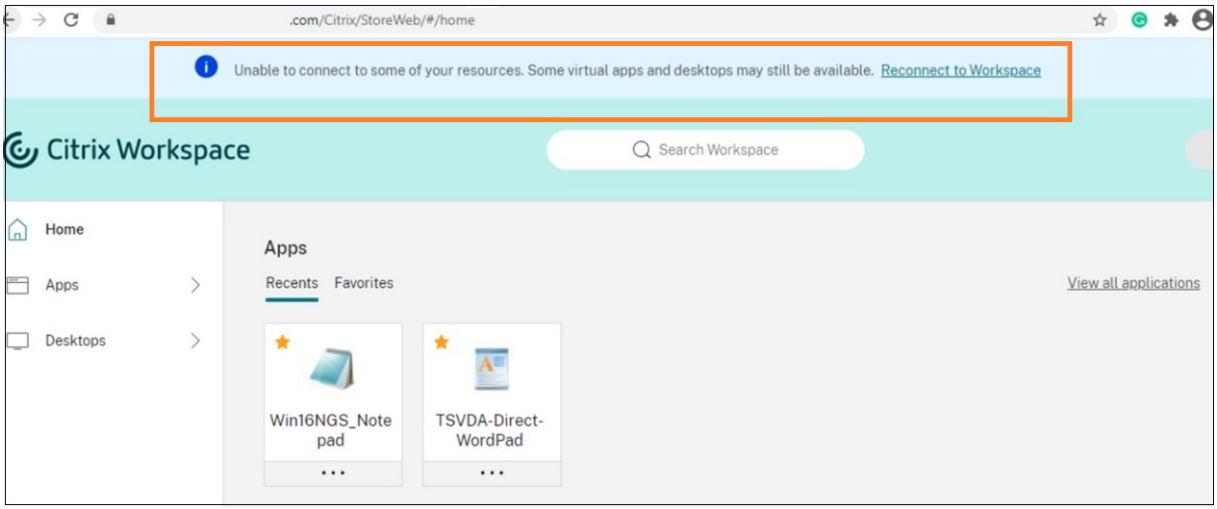
Experiencia de usuario de explorador

Cuando los usuarios hacen clic en sus aplicaciones o escritorios, la aplicación o el escritorio se abren sin solicitarles que abran **Citrix Workspace Launcher**.

Experiencia del usuario de explorador durante las interrupciones

Los usuarios pueden acceder a sus aplicaciones y escritorios desde un explorador web durante interrupciones del servicio, siempre y cuando el dispositivo de usuario mantenga una conexión de red a una ubicación de recursos.

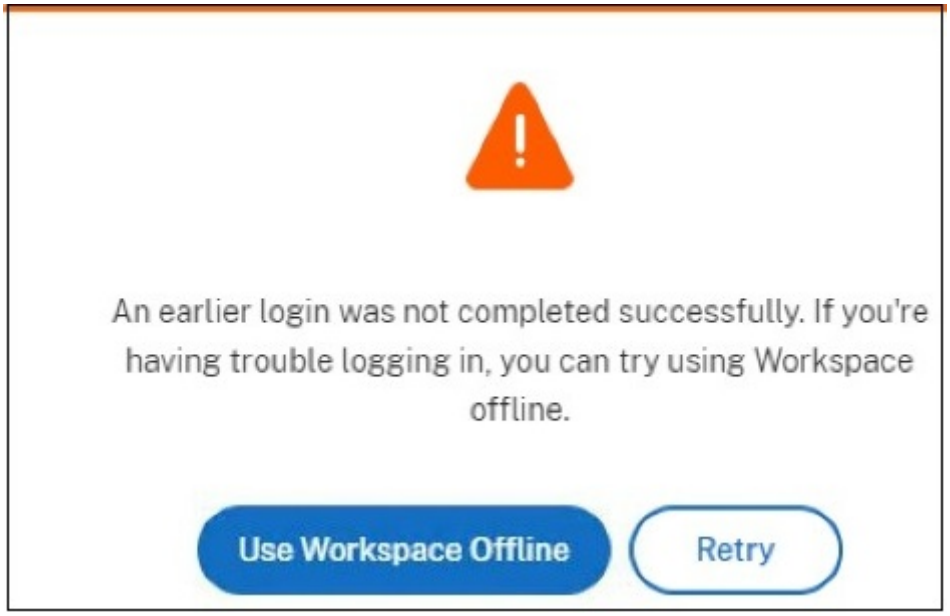
Si se produce una interrupción mientras el usuario está conectado a Workspace a través de un explorador web, aparece este mensaje en la parte superior de la ventana del explorador:



Los usuarios pueden acceder a aplicaciones y escritorios que están disponibles sin conexión al hacer clic en cualquier icono que no esté atenuado. Los usuarios también pueden intentar conectarse de nuevo al hacer clic en **Conectarse de nuevo a Workspace**.

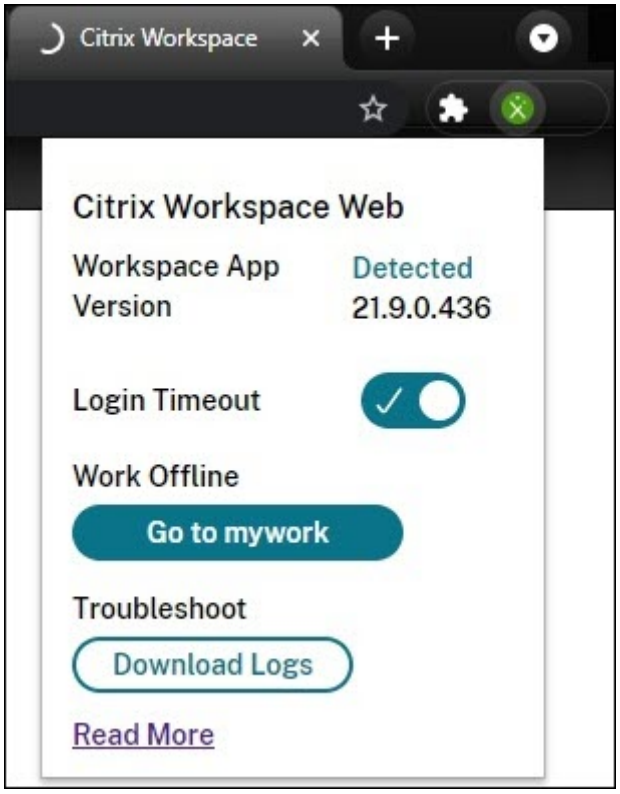
Si una interrupción del servicio impide a los usuarios iniciar sesión en Workspace a través de un explorador web, se les solicita que trabajen sin conexión o que intenten iniciar sesión de nuevo. Para

acceder a aplicaciones y escritorios disponibles sin conexión, los usuarios deben hacer clic en **Usar Workspace sin conexión**.



Si una interrupción del servicio impide a los usuarios iniciar sesión en el espacio de trabajo después de ir a la URL del espacio de trabajo, la ventana aparece una vez transcurrido un tiempo de espera especificado. De forma predeterminada, la ventana aparece 30 segundos después de que el usuario vaya a la URL del espacio de trabajo. Puede establecer este valor en 15, 30, 45 o 60 segundos. También puede inhabilitar el tiempo de espera en los inicios de sesión. Si se inhabilita el tiempo de espera en los inicios de sesión, la ventana que solicita a los usuarios que trabajen sin conexión aparece cuando los usuarios van a la URL del espacio de trabajo.

Para definir el parámetro del tiempo de espera en los inicios de sesión, haga clic en el icono de extensión en el explorador web del dispositivo de usuario. Use la ventana que aparece para habilitar o inhabilitar el tiempo de espera en los inicios de sesión y defina el tiempo de espera:



Es posible que una interrupción del servicio impida a los usuarios iniciar sesión si se redirigió el explorador web al sitio de autenticación de un proveedor de identidades de terceros. En este caso, los usuarios pueden escribir la URL del espacio de trabajo en el explorador web, lo que hace aparecer la ventana que solicita a los usuarios que trabajen sin conexión. Los usuarios no tienen que esperar a que se agote el tiempo de espera en los inicios de sesión para que aparezca la ventana.

Los usuarios también pueden acceder a aplicaciones y escritorios disponibles durante una interrupción del servicio de este modo:

1. Haga clic en el icono de extensión del explorador web.
2. En la ventana que aparece, haga clic en el botón que hay debajo de **Trabajar sin conexión**. Este botón dice **Ir a** más el nombre del almacén de Workspace.
3. En la ventana que aparece, haga clic en **Usar Workspace sin conexión**.

Durante algunas interrupciones de servicio, la ventana de advertencia que solicita a los usuarios que trabajen sin conexión aparece automáticamente cuando la extensión detecta problemas en el lado de Workspace. Los usuarios no necesitan hacer nada más ni dejar que se agote el tiempo de espera en los inicios de sesión.

Limitaciones del explorador

Si los usuarios borran las cookies y otros datos de sitios en sus exploradores web durante una interrupción del servicio, la continuidad del servicio no funciona hasta que se autentiquen de nuevo en Workspace.

La continuidad del servicio no es compatible en modo incógnito, a no ser que el usuario permita que la extensión funcione de ese modo.

Solución de problemas para los usuarios de explorador

En el menú **Avanzado** de los parámetros de cuenta de la aplicación del explorador de Citrix Workspace, asegúrese de que el método actual de preferencia para inicio de aplicaciones y escritorios esté establecido en **Usar la aplicación Citrix Workspace**. Si esta opción se establece en **Usar el explorador web**, la continuidad del servicio no se admite en el explorador.

Compruebe que el icono de extensión del explorador web aparezca en verde después de que el explorador cargue la URL de Workspace.

Para descargar registros, haga clic en el icono de la extensión del explorador web. A continuación, haga clic en **Download Logs**.

Habilitar Single Sign-On para espacios de trabajo con Citrix Federated Authentication Service

October 12, 2023

Servicio de autenticación federada (FAS) de Citrix para proporcionar Single Sign-On (SSO) a DaaS en Citrix Workspace. Por lo general, se adopta FAS si se utiliza uno de los siguientes proveedores de identidades para la autenticación de Citrix Workspace:

- Azure Active Directory
- Okta
- SAML 2.0
- Citrix Gateway
- Google Cloud Identity

Con FAS, los suscriptores introducen sus credenciales solo una vez para acceder a sus aplicaciones y escritorios de DaaS.

FAS no es necesario para SSO en DaaS si utiliza Active Directory (AD), AD y token o configuraciones específicas de Citrix Gateway. Para obtener más información sobre cómo configurar Citrix Gateway, consulte Crear una directiva de IdP de OAuth en Citrix Gateway local.

Servidores FAS

En cada ubicación de recursos, se pueden conectar varios servidores de FAS a Citrix Cloud para el equilibrio de carga y la conmutación por error.

Citrix Cloud admite el uso de servidores FAS en los siguientes casos.

En ambos supuestos, los suscriptores que inician sesión en sus espacios de trabajo a través de un proveedor de identidades federado introducen sus credenciales una sola vez para acceder a sus aplicaciones y escritorios.

Servidores FAS conectados con una única ubicación de recursos

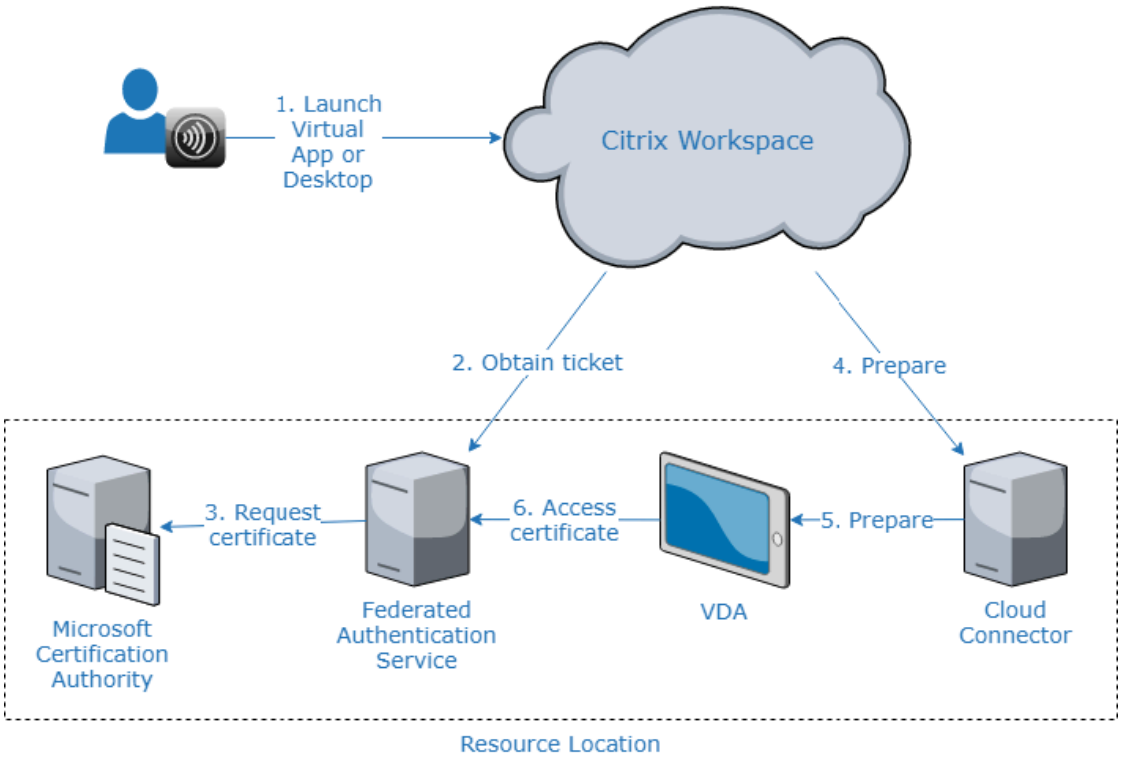
Si las ubicaciones de recursos contienen una infraestructura variada (por ejemplo, las distintas ubicaciones de recursos contienen bosques de AD diferentes), implementará los servidores FAS en la misma ubicación de recursos en la que se encuentran los VDA. Single Sign-On solo está activo en las ubicaciones de recursos donde están conectados uno o varios servidores FAS.

Servidores FAS conectados con varias ubicaciones de recursos

Si tiene conectividad de red entre sus ubicaciones de recursos y estos contienen una infraestructura similar, puede conectar los servidores de FAS con varias ubicaciones de recursos. SSO está activo para los suscriptores del espacio de trabajo que se conectan a aplicaciones y escritorios en esas ubicaciones de recursos. En este caso, no es necesario conectar servidores FAS distintos a cada ubicación de recursos.

Cuando los suscriptores inician una aplicación o un escritorio virtual, Citrix Cloud selecciona un servidor de FAS que se encuentre en la misma ubicación de recursos que la aplicación o el escritorio que se inician. Citrix Cloud contacta con el servidor FAS seleccionado para obtener un tíquet que conceda acceso a un certificado de usuario almacenado en el servidor FAS. Para autenticar al suscriptor, el VDA se conecta al servidor de FAS y presenta el tíquet.

Puede utilizar el mismo servidor FAS tanto de forma local como en Citrix Cloud con la configuración de reglas adecuada.



Prioridad de conmutación por error para varias ubicaciones de recursos

Cuando se utilizan servidores FAS con varias ubicaciones de recursos, los servidores FAS de una ubicación de recursos pueden proporcionar la funcionalidad de conmutación por error a los servidores FAS de otras ubicaciones de recursos. Cuando agrega servidores FAS a otras ubicaciones de recursos, designa cada servidor como principal o secundario. Cuando los suscriptores inician una aplicación o un escritorio virtual, Citrix Cloud utiliza esta designación de la siguiente manera para seleccionar un servidor FAS:

- Se consideran en primer lugar los servidores de FAS designados como principales en la ubicación de recursos dada.
- Si no hay servidores principales disponibles, se consideran los servidores de FAS designados como secundarios.
- Si no hay servidores secundarios disponibles, el proceso de inicio continúa, pero sin Single Sign-On.

Resumen del vídeo

Para obtener información general sobre el servicio de autenticación federada (FAS) para Citrix Workspace, consulte este vídeo de Tech Insight:

Requisitos

Requisitos de conectividad

Para conectar un servidor de FAS con Citrix Cloud, utilice la consola de administración de FAS. Esta consola sirve para configurar un servidor FAS local o remoto. Para habilitar Single Sign-On para espacios de trabajo con FAS, la consola de administración FAS y el servicio FAS acceden a las siguientes direcciones con la cuenta del usuario de la consola y la cuenta del servicio de red, respectivamente.

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

Requisitos de sistema de FAS

Los requisitos de esta sección se aplican a todos los servidores FAS a los que piense conectar con Citrix Cloud.

Todos los requisitos de sistema del servidor FAS se describen en la sección Requisitos del sistema de la documentación de producto de FAS.

Los servidores FAS de su entorno Citrix Virtual Apps and Desktops local deben tener instalado Servicio de autenticación federada 2003 (versión 10.1) o posterior.

Si su servidor FAS existente es anterior a la versión 10, puede descargar el software de FAS más reciente de Citrix y actualizar el servidor in situ antes de crear esta conexión. Al crear la conexión, seleccione la ubicación de recursos de su servidor FAS. Single Sign-On solo está activo para los suscriptores en las ubicaciones de recursos donde están presentes los servidores FAS.

Para obtener más información sobre la actualización de un servidor FAS existente, consulte Instalar y configurar en la documentación del producto FAS. Se puede utilizar el mismo servidor FAS para las implementaciones locales y Workspace.

Citrix Workspace

Debe tener Citrix DaaS aprovisionado y habilitado en Workspace. De forma predeterminada, DaaS está habilitado en la configuración de Workspace después de suscribirse al servicio. Sin embargo, el servicio requiere que se implemente Citrix Cloud Connectors para permitir que Citrix Cloud se comunique con el entorno local.

Cloud Connectors

Los Cloud Connectors de Citrix posibilitan la comunicación entre la ubicación de recursos (donde están los VDA) y Citrix Cloud. Implemente al menos dos Cloud Connectors para garantizar una alta disponibilidad. Los servidores en los que instale el software Cloud Connector deberán cumplir los siguientes requisitos:

- Requisitos del sistema descritos en los Detalles técnicos de Cloud Connector.

- No haber ningún otro componente de Citrix instalado, el servidor no es un controlador de dominio de Active Directory ni ser cualquier otra máquina de importancia crítica para la infraestructura de la ubicación de recursos.
- Estar unidos al dominio en el que se encuentran los VDA.

Para obtener más información sobre cómo implementar Cloud Connectors, consulte los siguientes artículos:

- Configuración del proxy y del firewall de Cloud Connector
- Instalación de Cloud Connector

Introducción a la configuración

1. Si va a implementar nuevos servidores FAS, revise los Requisitos y siga las instrucciones que se indican en Instalar y configurar FAS, en este artículo.
2. Conecte el servidor FAS a Citrix Cloud como se describe en Conectar un servidor FAS a Citrix Cloud, en este artículo. Al completar esta tarea, el servidor FAS se conecta a una única ubicación de recursos.
3. Si piensa conectar el servidor FAS a varias ubicaciones de recursos, siga las instrucciones que se indican en Agregar un servidor FAS a varias ubicaciones de recursos, en este artículo.

Instalar y configurar FAS

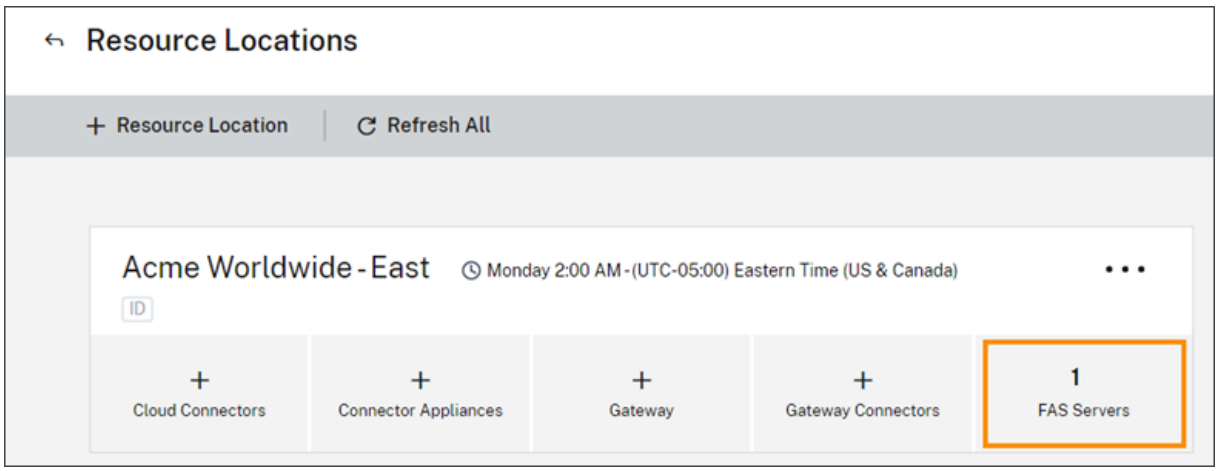
Siga el proceso de instalación y configuración de FAS descrito en la documentación del producto FAS. No se requieren los pasos de configuración para StoreFront y el Delivery Controller.

> **Sugerencia:**
>
> También puede descargar el instalador del Servicio de autenticación federada desde la consola de Citrix Cloud:
>
> 1. En el menú de Citrix Cloud, seleccione **Ubicaciones de recursos**.
> 2. Seleccione el icono **Servidores FAS** y, a continuación, haga clic en **Descargar**.

Conectar servidores FAS a Citrix Cloud

Utilice la consola de administración FAS para conectar el servidor FAS a Citrix Cloud, tal y como se describe en Instalar y configurar, en la documentación del producto FAS.

Después de completar el paso de configuración para **conectar con Citrix Cloud**, Citrix Cloud registra el servidor FAS y lo muestra en la página Ubicaciones de recursos de su cuenta de Citrix Cloud.



Si ya tiene la página Ubicaciones de recursos cargada en su explorador, actualice la página para mostrar el servidor FAS registrado.

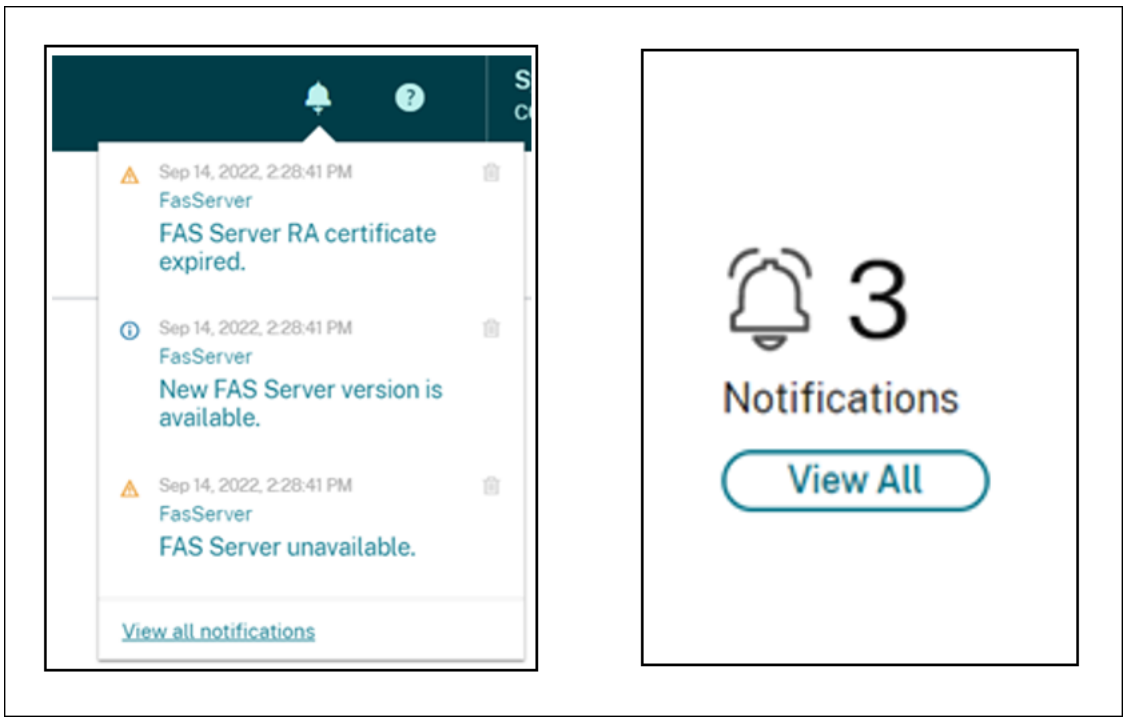
Función de notificaciones de Cloud

Ahora, FAS ofrece notificaciones de Cloud. Con las nuevas notificaciones de Cloud para servidores de FAS, recibirá notificaciones en estos casos:

- Un servidor de FAS no funciona o no está disponible.
- El certificado de la autoridad de Registro (RA) de un servidor de FAS ha caducado o está a punto de caducar.
- Hay una nueva versión de FAS disponible para descargarse.

Generar notificaciones

Se realiza una comprobación periódica de nuevas notificaciones en la consola de administración de Citrix Cloud. Las notificaciones aparecen en el icono de la campana de la esquina superior derecha de la consola de administración de Citrix Cloud. Seleccione **Ver todo** en el icono de notificaciones para ver todas las notificaciones. Para obtener más información, consulte Notificaciones.

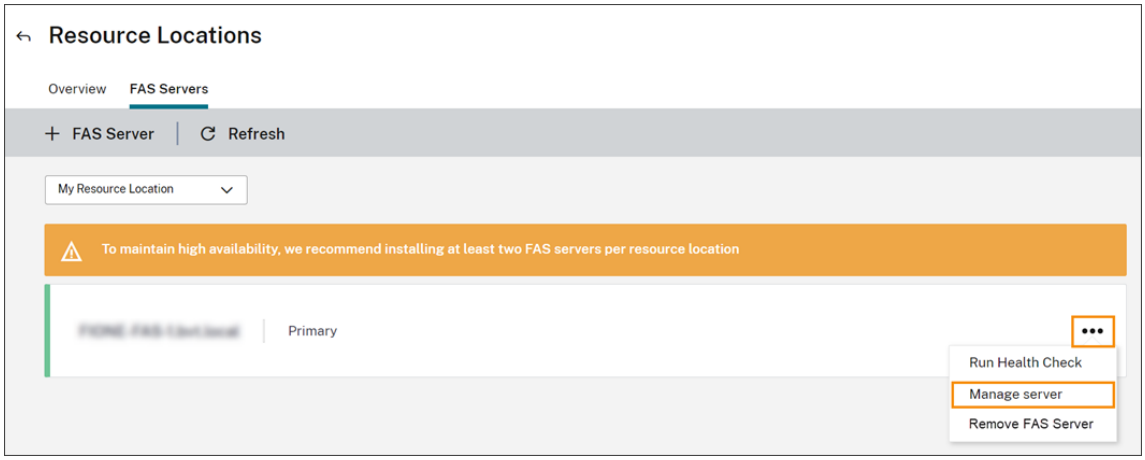


> **Nota:**
>
> Cuando se genera una notificación, se generará de nuevo periódicamente solamente si el problema no se ha resuelto.

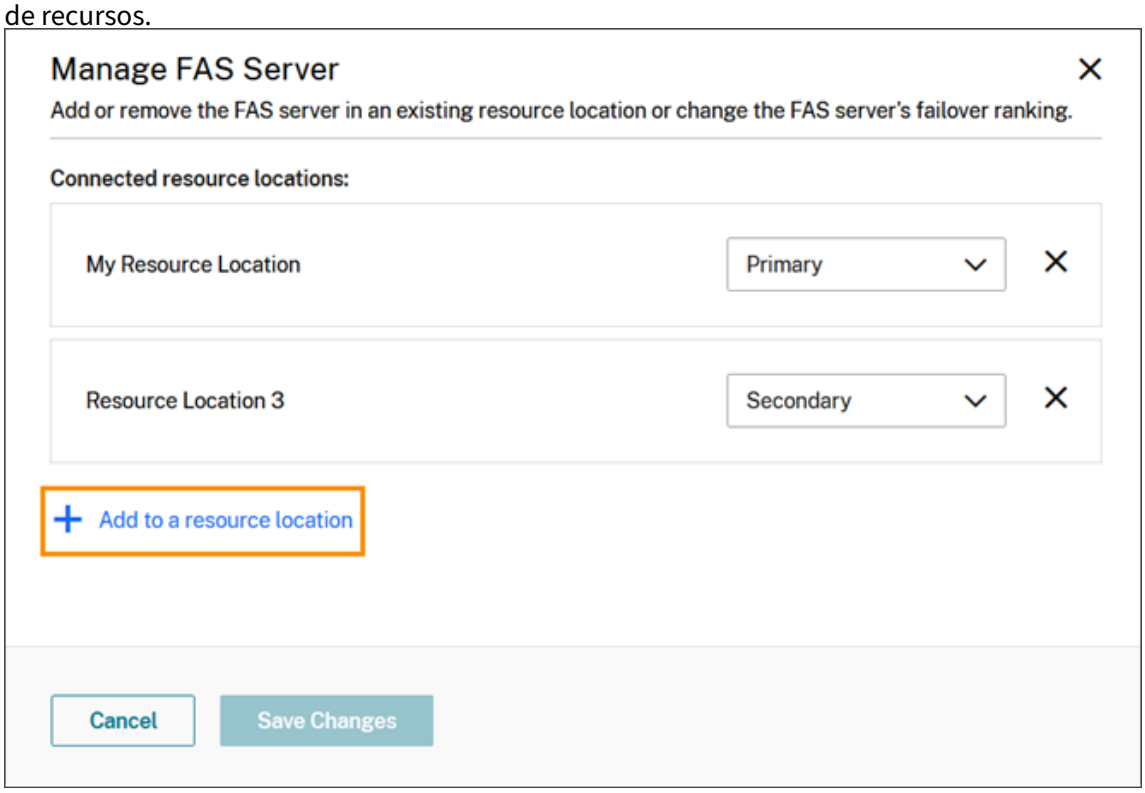
Todas las notificaciones contienen el FQDN del servidor de FAS afectado. La notificación de caducidad del certificado de la autoridad de registro solo se muestra para los servidores de FAS con la versión 10.10.0.14 o una posterior.

Agregar un servidor FAS a varias ubicaciones de recursos

1. En el menú de Citrix Cloud, seleccione **Ubicaciones de recursos** y, a continuación, seleccione la ficha **Servidores de FAS**.
2. Busque el servidor de FAS que quiere administrar, haga clic en los puntos suspensivos (…) en la sección derecha de la entrada y, a continuación, seleccione **Administrar servidor**.



3. Seleccione **Agregar a una ubicación de recursos** y, a continuación, seleccione las ubicaciones de recursos.

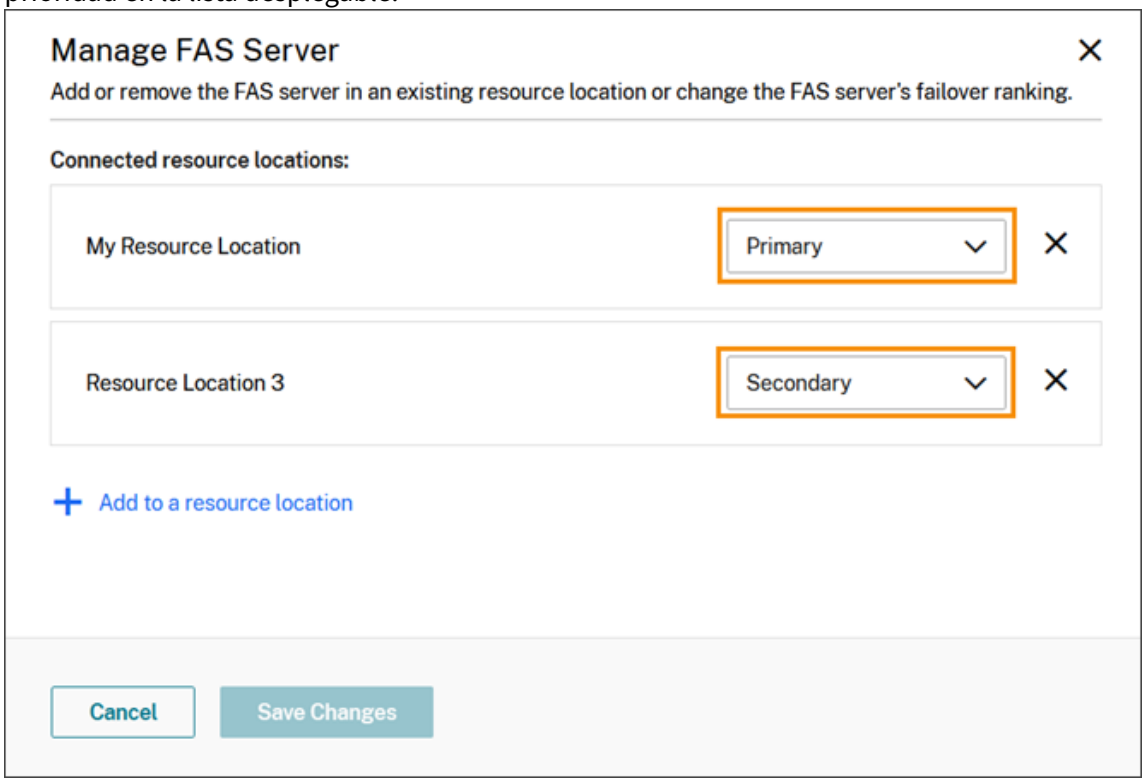


4. Seleccione **Principal** o **Secundario** para la prioridad de conmutación por error del servidor FAS en cada ubicación de recursos seleccionada.
5. Seleccione **Guardar cambios**.

Para ver el servidor FAS agregado, seleccione **Ubicaciones de recursos** en el menú de **Citrix Cloud** y, a continuación, seleccione la ficha **Servidores de FAS**. Aparecerá una lista de todos los servidores de FAS de todas las ubicaciones de recursos conectadas. Para mostrar los servidores de FAS de una ubicación de recursos específica, seleccione la ubicación de recursos en la lista desplegable.

Cambiar la prioridad de conmutación por error de un servidor de FAS

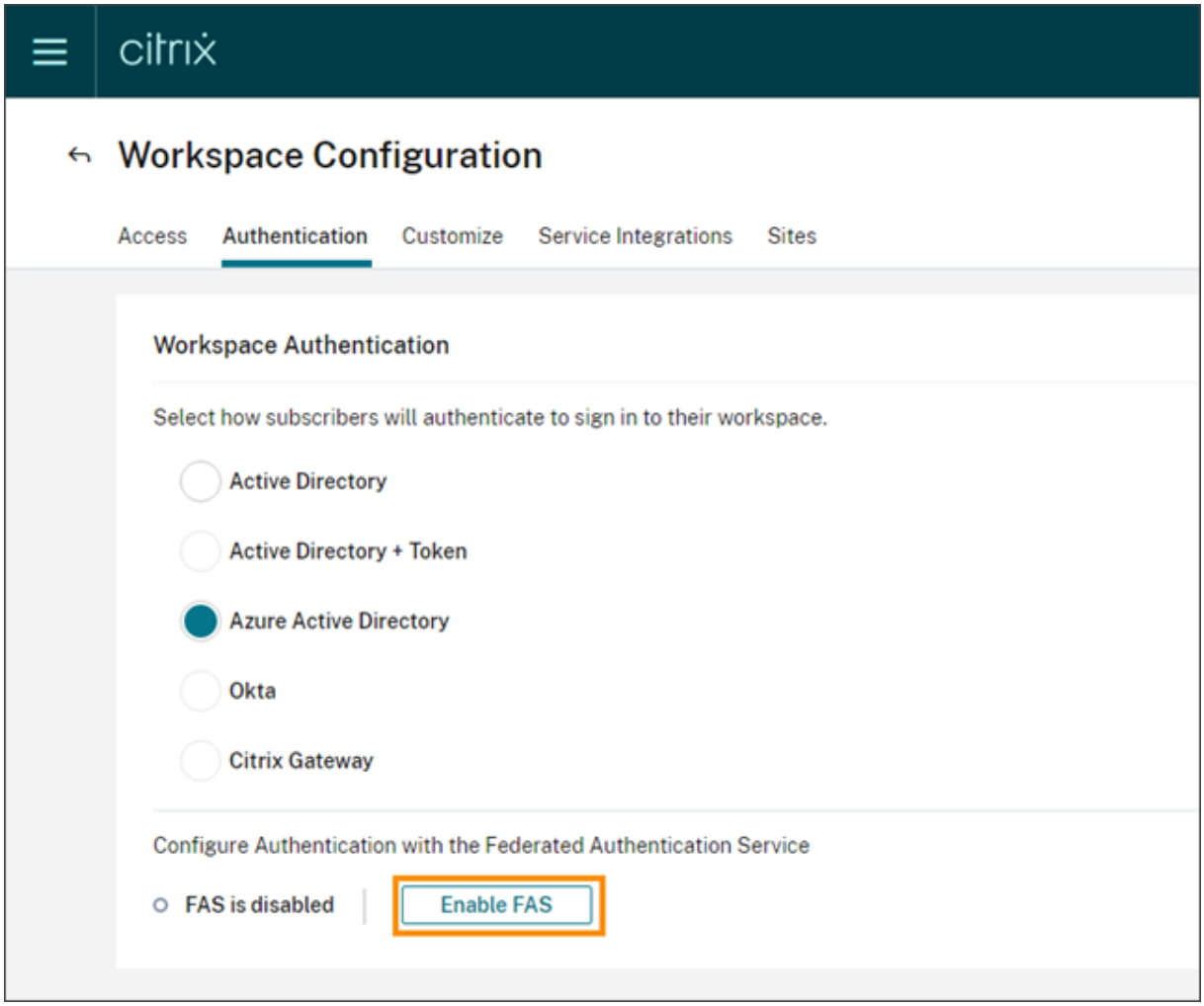
1. En la página **Ubicaciones de recursos**, seleccione el mosaico **Servidores de FAS** correspondiente a la ubicación de recursos que quiere administrar.
2. Seleccione la ficha **Servidores de FAS**.
3. Busque el servidor de FAS que quiere administrar, haga clic en los puntos suspensivos del lado derecho de la entrada y, a continuación, seleccione **Administrar servidor**.
4. Busque la ubicación de recursos con la prioridad que quiere cambiar y seleccione la nueva prioridad en la lista desplegable.



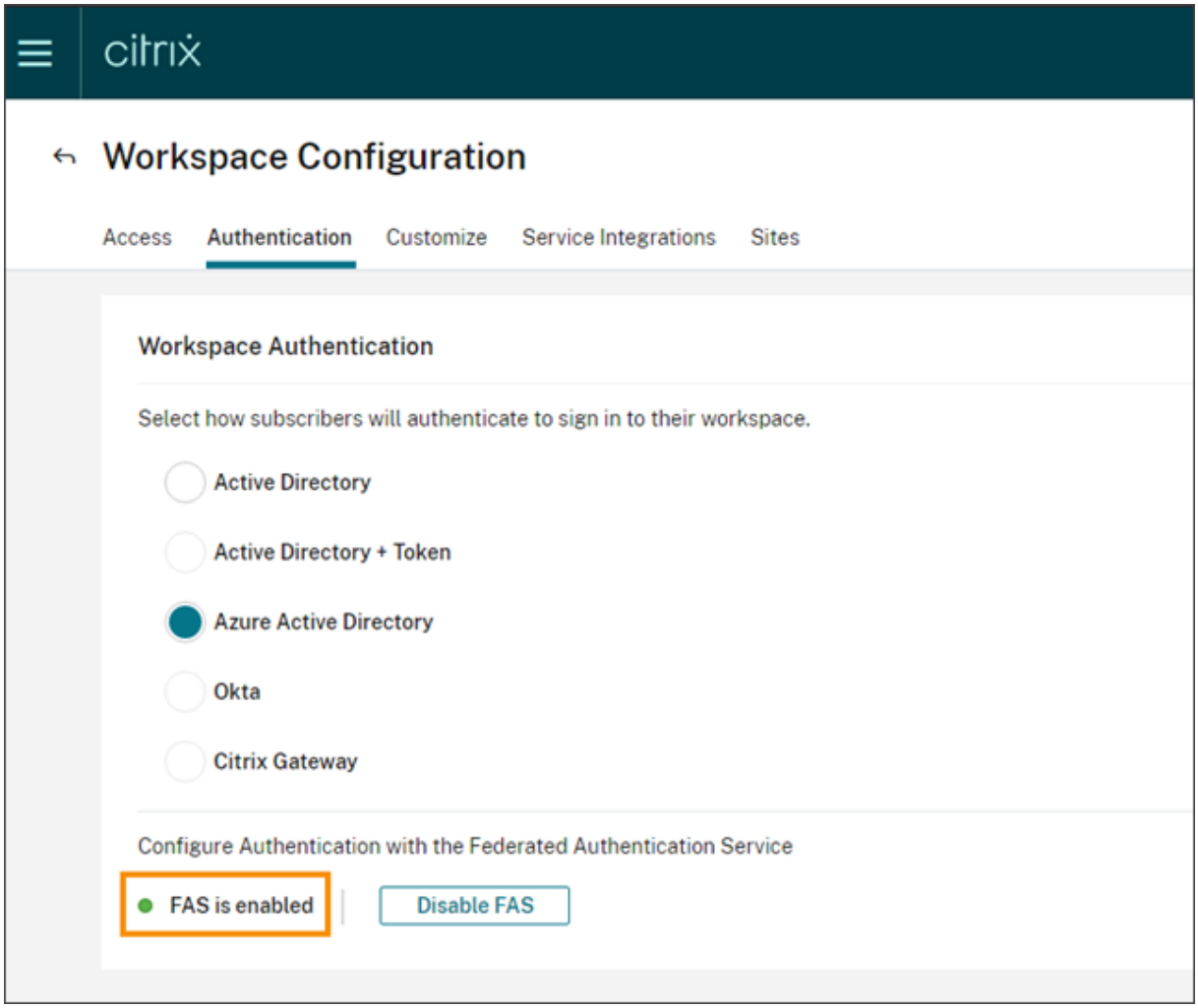
5. Seleccione **Guardar cambios**.

Habilitar la autenticación federada para espacios de trabajo

1. En el menú de Citrix Cloud, seleccione **Configuración de Workspace** y, luego, **Autenticación**.
2. Haga clic en **Habilitar FAS**. Este cambio puede tardar hasta cinco minutos en aplicarse a las sesiones de los suscriptores.



Posteriormente, el Servicio de autenticación federada (FAS) se activa para todos los inicios de aplicaciones virtuales y escritorios de Citrix Workspace.



Cuando los suscriptores inician sesión en su espacio de trabajo e inician una aplicación virtual o un escritorio en la misma ubicación de recursos que el servidor FAS, la aplicación o el escritorio se inician sin solicitar credenciales.

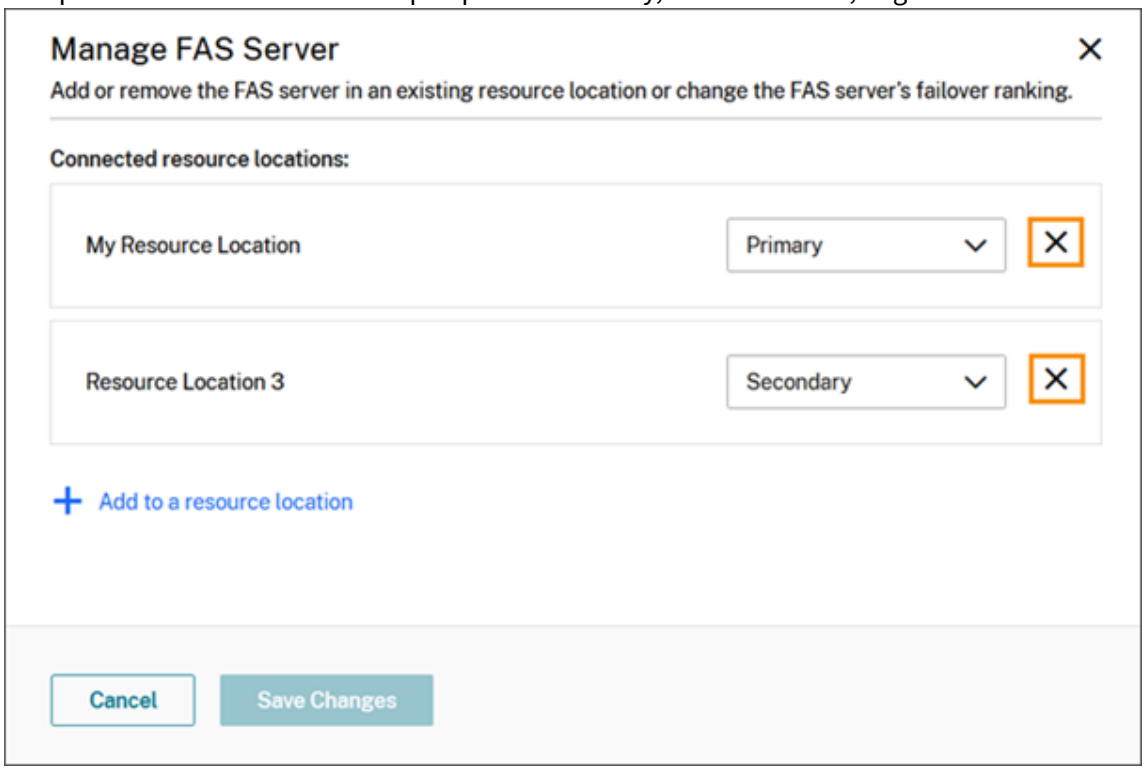
> **Nota:**
>
> Si todos los servidores de FAS de una ubicación de recursos están inactivos o están en modo de mantenimiento, los inicios de aplicación se ejecutan correctamente, pero Single Sign-On no está activo. Se solicita a los suscriptores sus credenciales de AD para acceder a cada aplicación o escritorio.

Quitar un servidor de FAS

Para quitar un servidor de FAS de una sola ubicación de recursos:

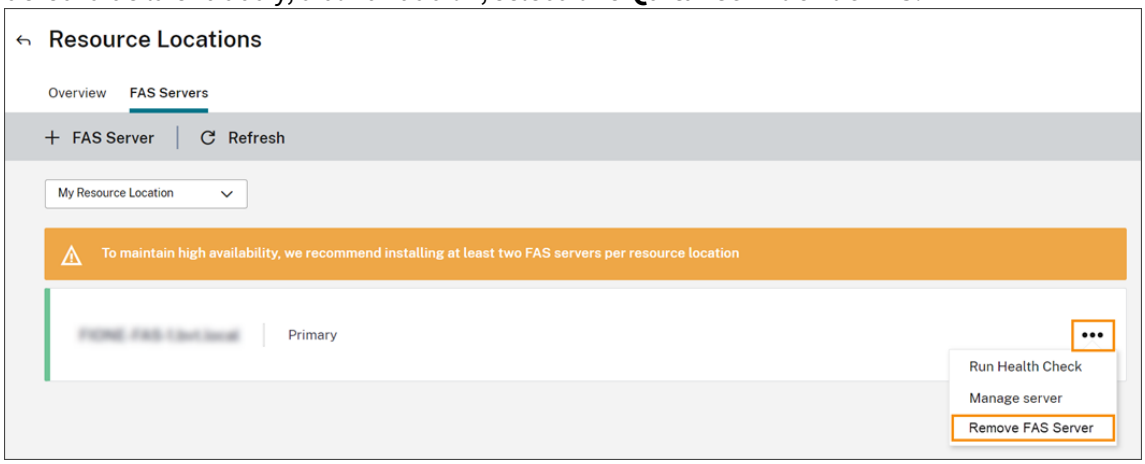
1. En la página **Ubicaciones de recursos**, seleccione el mosaico **Servidores de FAS** correspondiente a la ubicación de recursos que quiere administrar.

2. Seleccione la ficha **Servidores de FAS**.
3. Busque el servidor de FAS que quiere administrar, haga clic en los puntos suspensivos del lado derecho de la entrada y, a continuación, seleccione **Administrar servidor**.
4. Busque la ubicación de recursos que quiere eliminar y, a continuación, haga clic en el icono **X**.

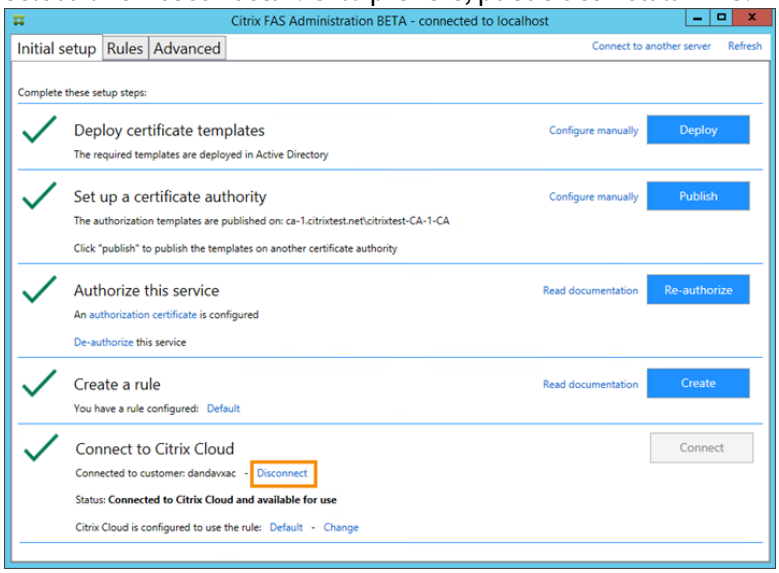


Para quitar un servidor de FAS de todas las ubicaciones de recursos conectadas:

1. En el menú de Citrix Cloud, seleccione **Ubicaciones de recursos**.
2. Busque la ubicación de recursos que quiere administrar y, a continuación, seleccione el icono **Servidores de FAS**.
3. Busque el servidor de FAS que quiere quitar, haga clic en los puntos suspensivos de la parte derecha de la entrada y, a continuación, seleccione **Quitar servidor de FAS**.

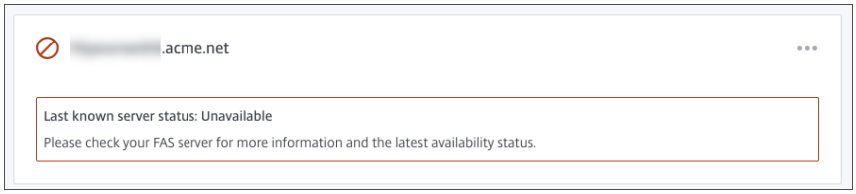


4. En la consola de administración de FAS (en el servidor FAS local), en **Conectarse a Citrix Cloud**, seleccione **Desconectar**. Si lo prefiere, puede desinstalar FAS.

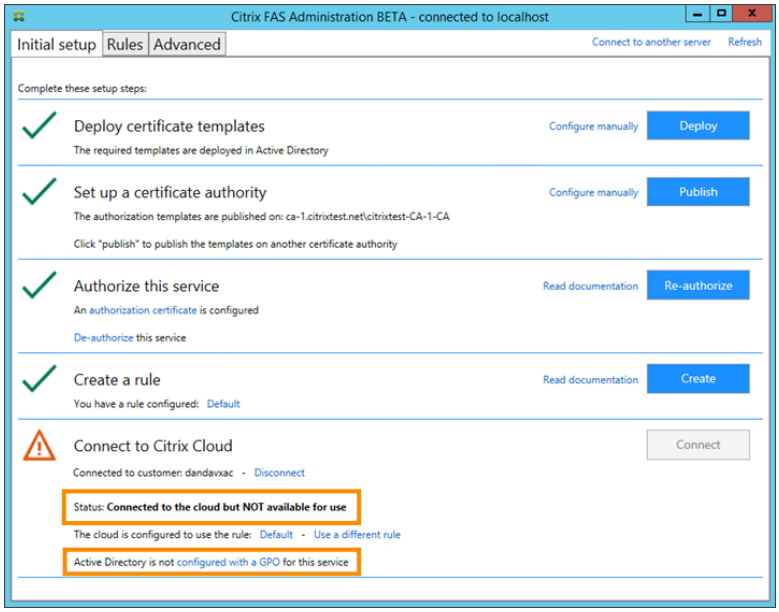


Solución de problemas

Si el servidor FAS no está disponible, aparecerá un mensaje de advertencia en la página Servidores de FAS.



Para diagnosticar el problema, abra la consola de administración de FAS en el servidor FAS local e inspeccione el estado. Por ejemplo, el servidor FAS no está presente en el objeto de directiva de grupo (GPO) del servidor FAS:



Si la consola de administración de FAS indica que el servidor está funcionando correctamente, pero sigue habiendo problemas de inicio de sesión con el agente VDA, consulte la Guía de solución de problemas FAS.

Más información

Configurar Single Sign-On en la aplicación Workspace