Citrix Remote Browser Isolation

Machine translated content

Disclaimer

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

Contents

Remote Browser Isolation

July 2, 2024

Citrix Remote Browser Isolation Service (antes denominado Secure Browser Service) aísla la exploración en la web para proteger a la red corporativa de los ataques por explorador web. Remote Browser Isolation permite acceder de forma segura y consistente a las aplicaciones web alojadas en Internet en remoto, sin necesidad de configurar el dispositivo del usuario. Los administradores pueden abrir rápidamente exploradores aislados remotos, lo que ofrece una eficiencia instantánea. Al aislar la exploración en Internet, los administradores de TI pueden ofrecer a los usuarios finales acceso seguro a Internet sin comprometer la seguridad de la empresa.

Los usuarios inician sesión a través de Citrix Workspace (o Citrix Receiver) y pueden abrir aplicaciones web en el explorador web configurado. El sitio web no transfiere directamente ningún dato de navegación hacia o desde el dispositivo del usuario, por lo que la experiencia es segura.

Remote Browser Isolation Service puede publicar exploradores web aislados remotos para usarlos con:

- **Aplicaciones web externas con código de acceso compartido.** Si publica un explorador web con autenticación con código de acceso compartido, los usuarios deben introducir el código de acceso para iniciar una aplicación.
- **Aplicaciones web externas autenticadas.** Cuando publica aplicaciones web externas autenticadas e inicia las aplicaciones con Citrix Workspace, Remote Browser Isolation Service requiere una ubicación de recursos que contenga al menos un Cloud Connector (se recomiendan dos o más). Para obtener más información, consulte Citrix Cloud Connector. En el caso de las aplicaciones autenticadas, debe agregar a los usuarios con la Biblioteca de Citrix Cloud.
- **Aplicaciones web externas no autenticadas.** Cuando publica aplicaciones web externas sin autenticar e inicia las aplicaciones con Citrix Workspace, Remote Browser Isolation Service requiere una ubicación de recursos que contenga al menos un Cloud Connector (se recomiendan dos o más). Para obtener más información, consulte Citrix Cloud Connector.

  Aunque normalmente no se recomienda, se pueden usar aplicaciones web externas no autenticadas para una prueba de concepto simple.

Para obtener más información, consulte Publicar un explorador aislado remoto.

El servicio de Secure Browser Service también ofrece:

- Integración de aplicaciones publicadas con Citrix Workspace
- Integración de aplicaciones publicadas con la implementación local de StoreFront
- Funcionalidad sencilla de lista de direcciones URL permitidas a efectos de seguridad

- Supervisión de uso
- Controles para el uso del portapapeles, la impresión, el modo quiosco, la conmutación por error de región y la asignación de unidades del cliente

Servicio Remote Browser Isolation con Citrix Secure Private Access

Puede iniciar los exploradores publicados del servicio Remote Browser Isolation mediante la consola de Citrix Secure Private Access para acceder a las aplicaciones web empresariales, TCP y SaaS. También puede redirigir los sitios web no autorizados para que se abran en los exploradores publicados del servicio Remote Browser Isolation a través de Citrix Secure Private Access.

Para obtener más información sobre el acceso a los exploradores remotos aislados a través de Citrix Secure Private Access, consulte Configurar una directiva de acceso con varias reglas y sitios web no autorizados en la documentación de Citrix Secure Private Access.

Artículos de referencia

- Información general sobre la solución de servicio Secure Private Access
- Citrix Cloud
- Búsqueda de autoservicio para Remote Browser Isolation (Secure Browser)
- Citrix Enterprise Browser
- Información de seguridad y cumplimiento
- documentación para desarrolladores

Novedades en los productos relacionados

- Secure Private Access
- Citrix Enterprise Browser
- Citrix Analytics for Security

Novedades

October 14, 2022

Julio de 2022

- **Remote Browser Isolation admite la autenticación para todas las aplicaciones con Azure Active Directory.**

  - Ahora, los usuarios pueden iniciar sesión en cualquier aplicación de Remote Browser Isolation desde Citrix Workspace con credenciales de Azure Active Directory.
  - Cuando los usuarios de Remote Browser Isolation inician sesión, utilizan la página de inicio de sesión de Workspace que configuró para su sitio. Para obtener más información, consulte Integración con Citrix Workspace.

Septiembre de 2021

- **Remote Browser Isolation admite audio bidireccional**. El audio bidireccional está disponible en Remote Browser Isolation.
- **Los inicios de Remote Browser Isolation desde launch.cloud.com se autentican mediante la autenticación de Citrix Cloud**. Cuando los usuarios inician aplicaciones de Remote Browser Isolation desde la URL launch.cloud.com, la autenticación de Citrix Cloud gestiona sus credenciales. Esto mejora la seguridad sin alterar la experiencia del usuario.

Marzo de 2021

- **Remote Browser Isolation admite la autenticación con Azure Active Directory.** Ahora, los usuarios pueden iniciar sesión en aplicaciones de Remote Browser Isolation desde Citrix Workspace con credenciales de Azure Active Directory. Para obtener más información, consulte Integración con Citrix Workspace.
- **Remote Browser Isolation le permite supervisar y cerrar sesiones activas de los usuarios**. Remote Browser Isolation proporciona esta información sobre las sesiones activas de los usuarios: nombre de usuario, ID de sesión, IP de cliente, tipo de autenticación, nombre de aplicación, hora de inicio de sesión y duración de la sesión. Puede ver la información básica sobre cada sesión activa y desconectarla si es necesario. Para obtener más información, consulte Supervisar sesiones activas.

Publicaciones en 2020

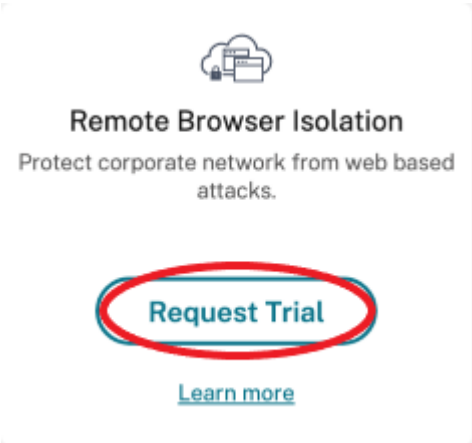
Todas las versiones de 2020 contienen mejoras que ayudan a mejorar el rendimiento y la estabilidad generales.

Introducción a Remote Browser Isolation

October 14, 2022

Aquí dispone de un vídeo sobre cómo empezar a utilizar Remote Browser Isolation Service (antes denominado Secure Browser Service).

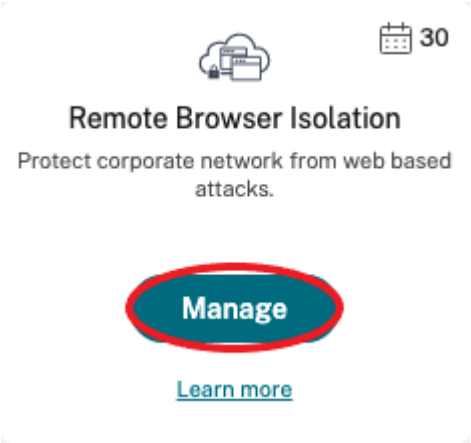
1. Inicie sesión en Citrix Cloud. Si no tiene cuenta, consulte Registrarse en Citrix Cloud. Puede solicitar una prueba de 30 días de Citrix Remote Browser Isolation.
2. En el mosaico de **Remote Browser Isolation**, haga clic en **Solicitar prueba**.



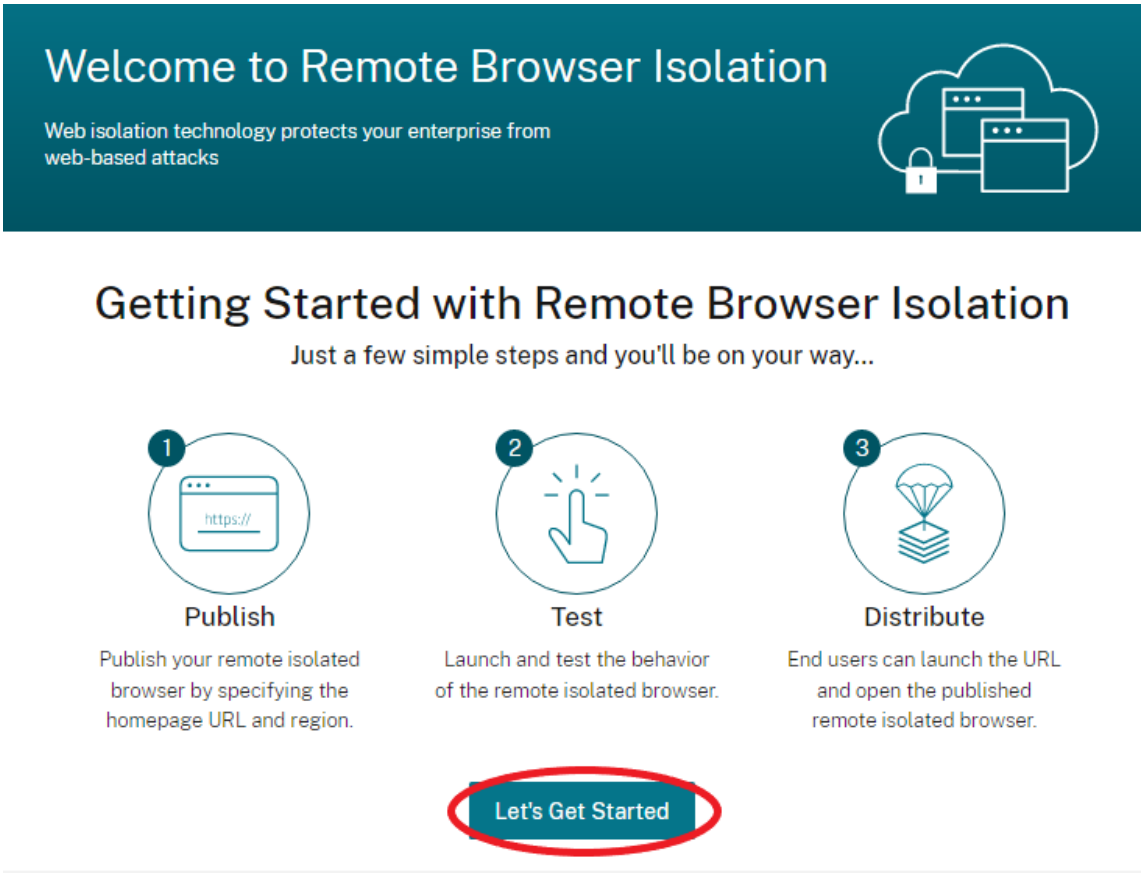
3. En breves instantes, recibirá un correo electrónico (al correo electrónico asociado con su cuenta

de Citrix Cloud). Haga clic en el enlace **Registrarse** en el correo electrónico.

4. Cuando haya vuelto a Citrix Cloud, haga clic en **Administrar** en el mosaico de **Remote Browser Isolation**.



5. En la página **Le damos la bienvenida a Remote Browser Isolation**, haga clic en **Vamos a empezar**.



6. Seleccione el tipo de explorador aislado remoto que quiere publicar: con código de acceso compartido, autenticado o no autenticado. Luego haga clic en **Continuar**.

De forma predeterminada, los usuarios deben iniciar las aplicaciones con autenticación con código de acceso compartido mediante launch.cloud.com. Ni Citrix Workspace ni la biblioteca de Citrix Cloud admiten aplicaciones con códigos de acceso compartidos.

Para usar Citrix Workspace, debe publicar aplicaciones autenticadas y asignar explícitamente suscriptores (usuarios) o grupos en la biblioteca de Citrix Cloud. Las aplicaciones no autenticadas están disponibles para todos los suscriptores de Workspace sin asignación de usuarios.

7. Configure los siguientes parámetros:

   - **Nombre:** Escriba el nombre de la aplicación que va a crear.
   - **URL de inicio:** Especifique la URL que se abre cuando los usuarios inician dicha aplicación.
   - **Región:** Seleccione la ubicación o región del servidor. Las regiones disponibles son: Oeste de los Estados Unidos, Este de los Estados Unidos, Sudeste Asiático, Este de Australia y Europa occidental.

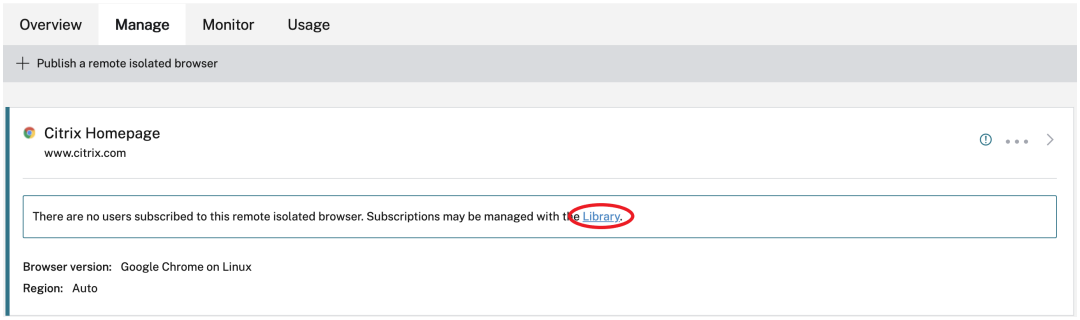
     Si selecciona **Automático**, su explorador web aislado le conecta a la región más cercana según su geolocalización.
   - **Código de acceso:** Si seleccionó un explorador con autenticación mediante código de acceso compartido, introdúzcalo para proporcionar acceso seguro mejorado a la aplicación. El código de acceso debe tener al menos 10 caracteres, y al menos 1 carácter numérico y 1 símbolo. Asegúrese de guardar el código de acceso y compartirlo con sus usuarios. Los usuarios deben introducir el código de acceso cuando inicien una aplicación mediante launch.cloud.com.
   - **Icono:** De manera predeterminada, se usa el icono del ejecutable de Google Chrome cuando publica un explorador web aislado. Ahora puede elegir su propio icono para representar un explorador publicado.

     Haga clic en **Cambiar icono> Seleccionar icono** para cargar un icono de su elección, o elija **Usar el icono predeterminado** para utilizar el icono de Google Chrome existente.

   Haga clic en **Publicar**.

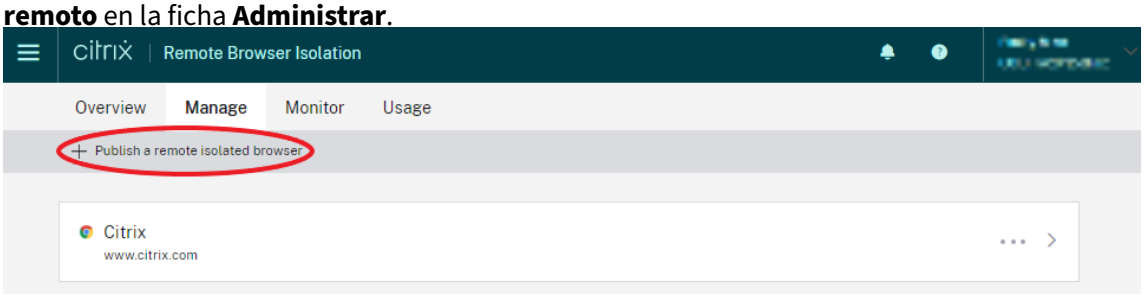
8. La ficha **Administrar** muestra el explorador web publicado. Para iniciar el explorador web que acaba de crear, haga clic en los puntos suspensivos del mosaico que contiene el explorador web aislado y, a continuación, haga clic en **Iniciar explorador publicado**.

   - Si ha publicado un explorador aislado autenticado, debe usar la biblioteca de Citrix Cloud para agregar usuarios o grupos. Haga clic en la flecha derecha al final de la fila para expandir el recuadro Detalles que contiene un enlace a la biblioteca.



Si hace clic en el enlace proporcionado, se le llevará a la pantalla de la Biblioteca que contiene su explorador aislado remoto. Haga clic en el menú de tres puntos del mosaico que contiene el explorador web aislado y haga clic en **Administrar suscriptores**. Para obtener información sobre cómo agregar suscriptores, consulte Asignar usuarios y grupos a ofertas de servicios desde la biblioteca.

Para publicar otro explorador aislado remoto, haga clic en **Publicar un explorador aislado remoto** en la ficha **Administrar**.



Para obtener información sobre la compra de Citrix Remote Browser Isolation Service (antes denominado Citrix Secure Browser Service), visite https://www.citrix.com/products/citrix-remote-browser-isolation/.

Integrar en Citrix Workspace

Remote Browser Isolation se puede integrar en Citrix Workspace. Para asegurarse de que está integrado:

1. Inicie sesión en Citrix Cloud.
2. En el menú superior izquierdo, seleccione **Configuración de Workspace**.
3. Seleccione la ficha **Integraciones de servicio**.
4. Confirme que la entrada de Remote Browser Isolation Service indica **Habilitado**. Si no es así, haga clic en el menú de tres puntos y seleccione **Habilitar**.

Si aún no lo ha hecho, configure la URL del espacio de trabajo, la conectividad externa y la autenticación del espacio de trabajo de su espacio de trabajo, tal y como se describe en Configurar la autenticación en espacios de trabajo.

Remote Browser Isolation admite la autenticación con Active Directory y Azure Active Directory. La autenticación con Active Directory está configurada de forma predeterminada. Para obtener información sobre cómo configurar la autenticación mediante Azure Active Directory, consulte Conectar Azure Active Directory a Citrix Cloud.

Si configura la autenticación mediante Azure Active Directory, el dominio local que contiene sus controladores de dominio de Active Directory debe contener un Cloud Connector (preferiblemente dos).

Integración de la implementación local de StoreFront

Los clientes de Citrix Virtual Apps and Desktops con una implementación local de StoreFront pueden integrarse fácilmente en Remote Browser Isolation Service para disfrutar de estas ventajas:

- Agrupe sus exploradores web aislados remotos con sus aplicaciones de Citrix Virtual Apps and Desktops existentes para una disfrutar de una experiencia de almacén unificada.
- Utilice los receptores nativos Citrix para una experiencia de usuario final óptima.
- Refuerce la seguridad al iniciar Remote Browser Isolation con su solución de autenticación existente de varios factores integrada con StoreFront.

Para obtener más información, consulte CTX230272 y la documentación de StoreFront.

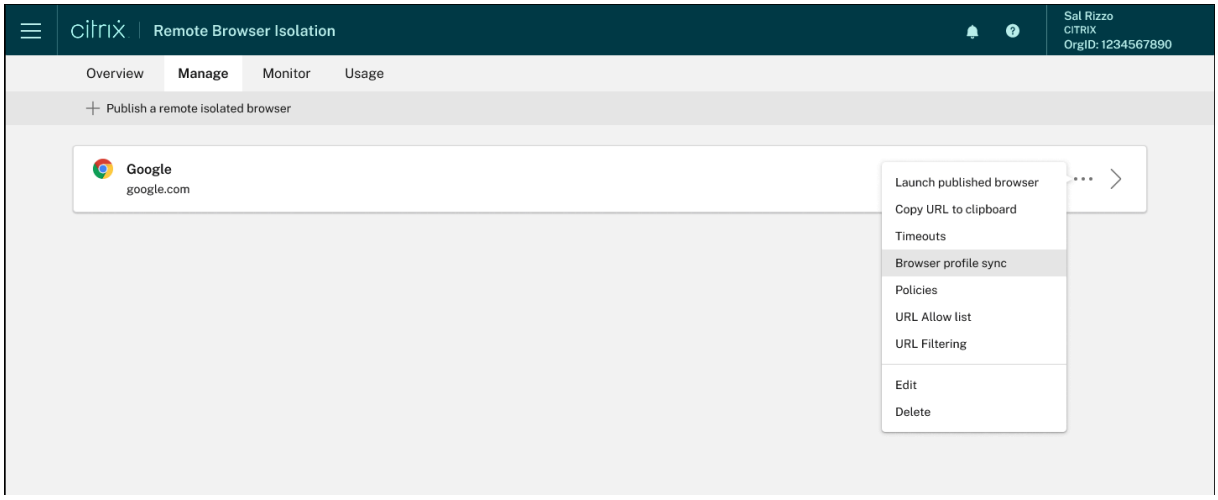
Administrar y supervisar exploradores web aislados remotos

April 5, 2024

Ahora puede administrar, supervisar y comprobar el uso de los exploradores web publicados en Remote Browser Isolation.

Administrar

La ficha **Administrar** muestra los exploradores publicados. Para acceder a las tareas de administración, haga clic en el menú de tres puntos situado en el extremo derecho del explorador publicado y después seleccione la tarea requerida.



Si selecciona una entrada de menú y luego decide no cambiar nada, cancele la selección haciendo clic en la **X** que hay fuera del cuadro de diálogo.

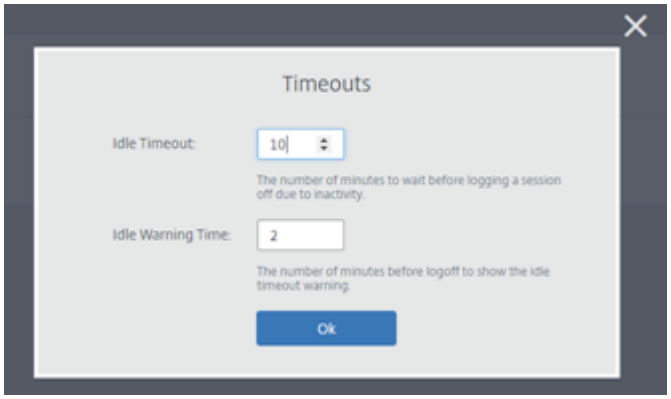
Puede administrar el explorador aislado publicado mediante las siguientes tareas:

- **Iniciar el explorador publicado:** abre la sesión del explorador publicado. Tras publicar el explorador, puede seleccionar esta tarea para verificar el inicio de la sesión de explorador publicada.
- **Copiar URL al portapapeles:** copia la URL del explorador publicado. Puede compartir esta URL con los usuarios finales para acceder a los exploradores publicados.
- **Tiempos de espera:** puede establecer el **Tiempo límite de inactividad** y el **Tiempo límite de advertencia de inactividad** seleccionando la tarea **Tiempos de espera**.
  - **Tiempo límite de inactividad:** la cantidad de minutos de inactividad que se permite en una sesión antes de cerrarla por inactividad.
  - **Tiempo límite de advertencia de inactividad:** la cantidad de minutos que transcurre tras el envío de un mensaje de advertencia antes de cerrar la sesión por inactividad.

  Por ejemplo, si establece el tiempo límite de inactividad en 20 y el tiempo límite de advertencia de inactividad en 5, el sistema mostrará un mensaje de advertencia si no hay actividad en la

sesión durante 15 minutos. Si el usuario no responde, la sesión termina cinco minutos después.

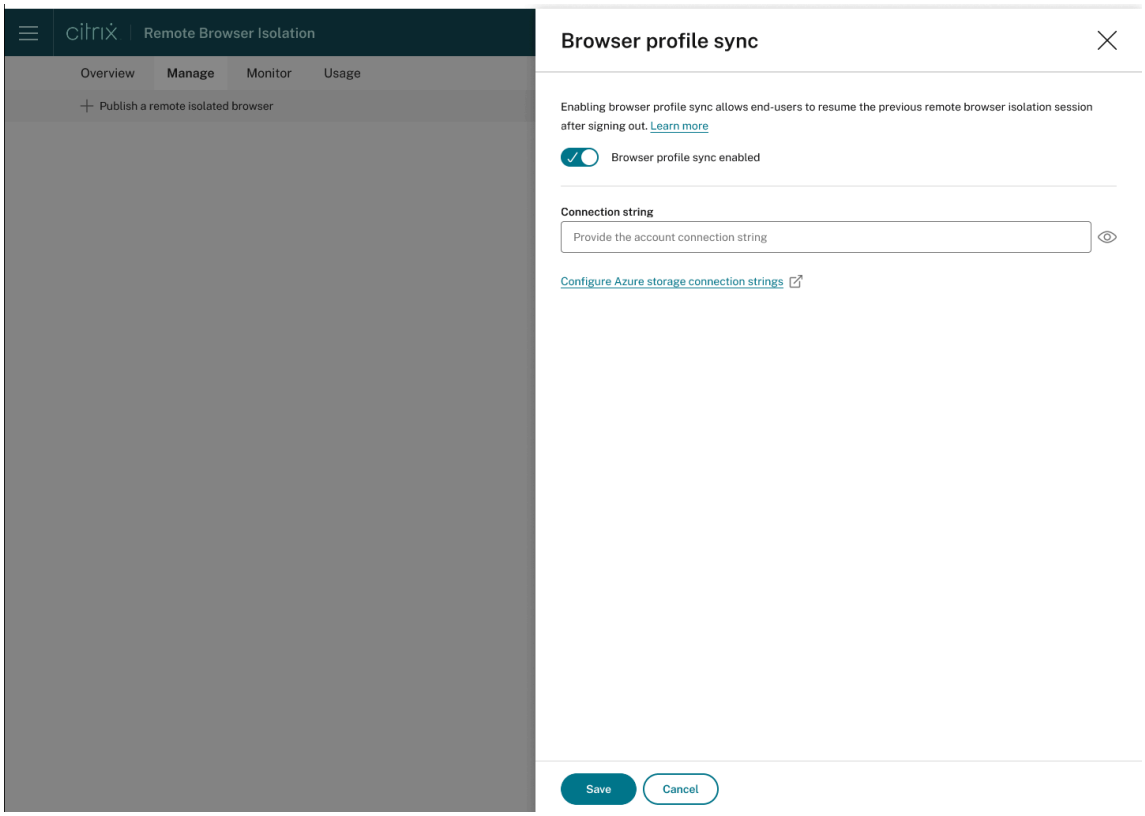
Para establecer el **Tiempo límite de inactividad** y el **Tiempo límite de advertencia de inactividad** del explorador aislado publicado, seleccione la tarea **Tiempos de espera** y establezca la duración de **Tiempo límite de inactividad** y **Tiempo límite de advertencia de inactividad** en el cuadro de diálogo **Tiempos de espera**. A continuación, haga clic en **Aceptar** para guardar los cambios.



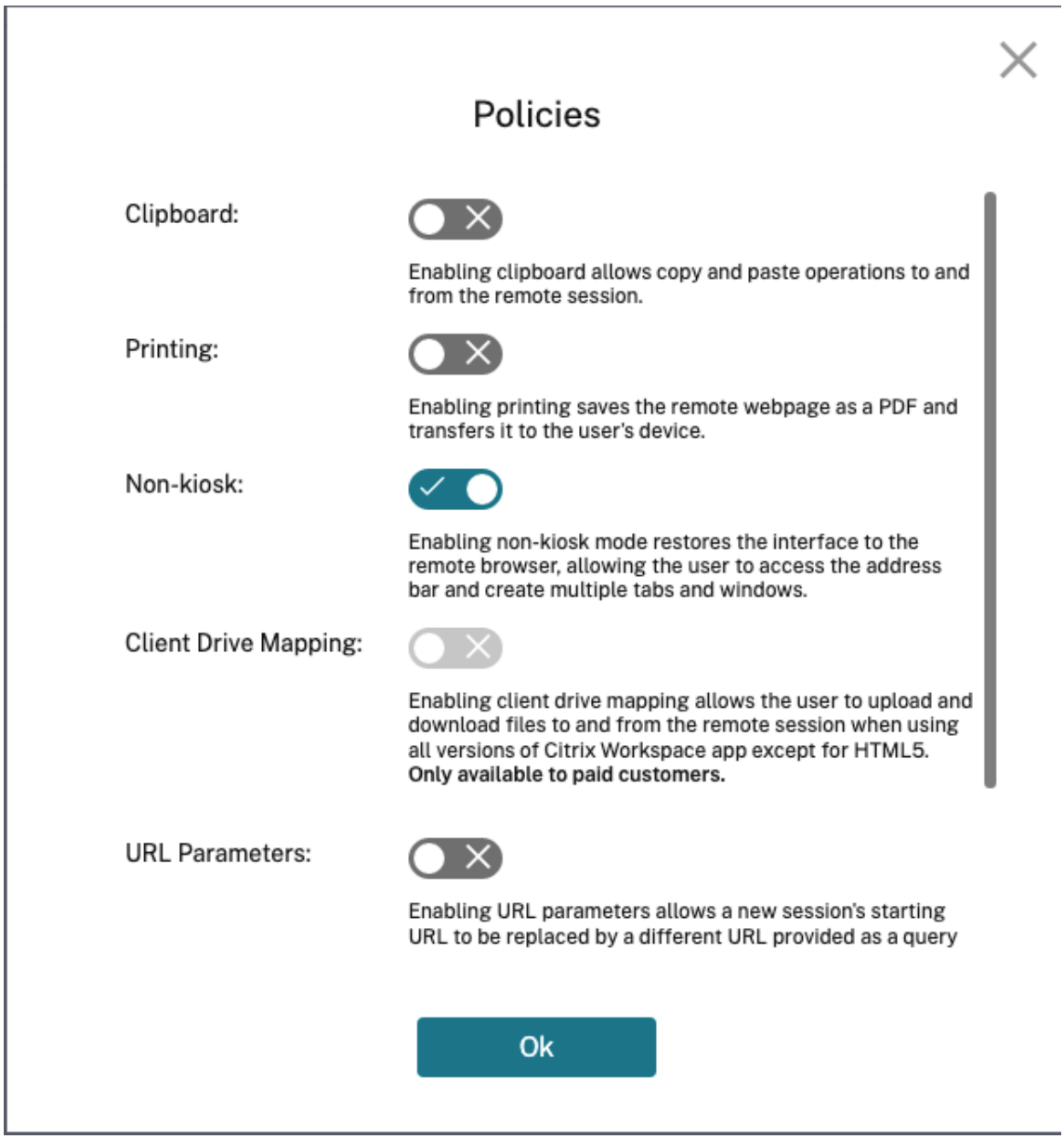
- **Sincronización del perfil del explorador**: permite a los usuarios finales reanudar la sesión anterior del explorador después de cerrar sesión. Los administradores pueden especificar una cadena de conexión para su almacenamiento de Azure a fin de habilitar el almacenamiento del perfil del explorador. Cuando el usuario abre otra sesión de explorador con el mismo perfil, se restaura la sesión de explorador anterior donde la dejó el usuario. Si el usuario ha iniciado sesión en algún sitio web, esos sitios web se encargan de la autenticación. Aunque esta función puede guardar sesiones, cookies y otra información, es posible que el sitio web requiera que el usuario inicie sesión de nuevo. Actualmente, esta función solo admite la restauración de fichas.

  Para habilitar la función **Sincronización del perfil del explorador**, siga estos pasos:

  1. Seleccione la tarea **Sincronización del perfil del explorador** para el explorador publicado requerido.
  2. En el cuadro de diálogo **Sincronización del perfil del explorador**, habilite **Sincronización del perfil del explorador** e introduzca la **Cadena de conexión**. Para obtener más información sobre la configuración de la cadena de conexión, consulte Configurar cadenas de conexión de Azure Storage en la documentación de Azure Blob Storage.
  3. Haga clic en **Guardar**.



- **Directivas:** puede establecer directivas para los exploradores publicados.

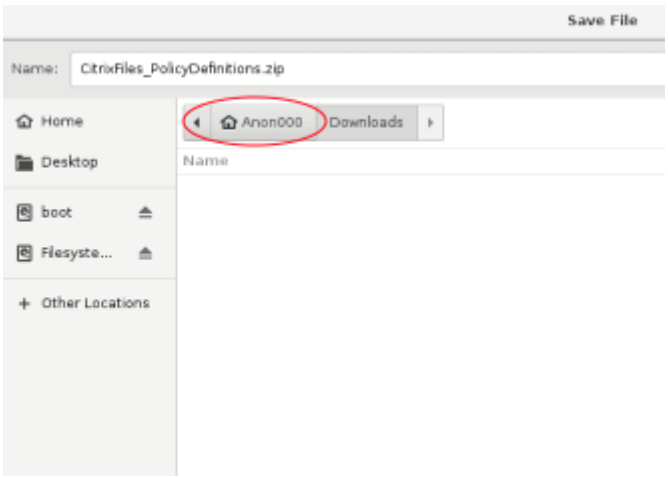


Los parámetros en la página de directivas controlan lo siguiente:

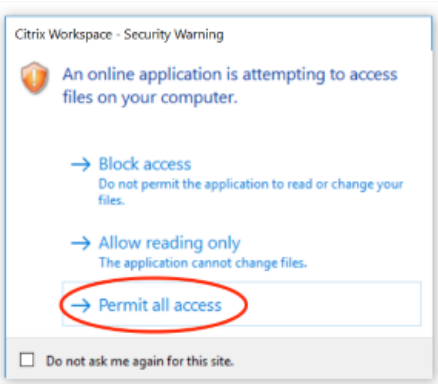
- **Portapapeles:** Al habilitar la directiva de portapapeles se permiten las operaciones de copiar y pegar desde y hacia la sesión remota. (Al inhabilitar la directiva del portapapeles, se quita el botón Portapapeles de la barra de herramientas de la aplicación Citrix Workspace) De forma predeterminada, este parámetro está inhabilitado.
- **Impresión:** Habilitar la impresión guarda la página web remota como PDF y la transfiere al dispositivo del usuario. A continuación, el usuario puede presionar Ctrl-P y seleccionar la impresora Citrix PDF Printer. De forma predeterminada, esta configuración está inhabilitada.
- **No quiosco:** Al habilitar el modo no quiosco, se restaura la interfaz al explorador remoto.

El usuario puede acceder a la barra de direcciones y crear múltiples fichas y ventanas. (Al inhabilitar el modo no quiosco, se eliminan los controles de navegación y la barra de direcciones del explorador remoto). De manera predeterminada, este parámetro está habilitado (el modo no quiosco está activado).

- **Conmutación por error de región:** La directiva de conmutación por error de región transfiere automáticamente el explorador publicado a otra región si la región actual tiene algún problema. Si no quiere utilizar esta función, inhabilite la directiva de conmutación por error de región. Si ha publicado el explorador mediante la selección de región **automática**, su explorador web aislado seguirá inscrito en la directiva. De manera predeterminada, esta configuración está habilitada.
- **Asignación de unidades del cliente:** Puede habilitar la directiva de asignación de unidades del cliente para permitir al usuario cargar y descargar los archivos desde y hacia la sesión remota. Esta función solo está disponible para las sesiones iniciadas con la aplicación Citrix Workspace. De forma predeterminada, este parámetro está inhabilitado.
  * Los usuarios deben guardar los archivos descargados solo en el disco `ctxmnt` del directorio `Anonxxx`. Para ello, los usuarios deben ir hasta la ubicación deseada para almacenar el archivo. Por ejemplo, **Anonxxx > ctxmnt > C > Usuarios > Nombre de usuario > Documentos**.



  * El cuadro de diálogo puede solicitar al usuario que acepte los permisos **Permitir todo el acceso** o **Leer y escribir** para acceder a la carpeta de `ctxmnt`.



  - **Parámetros de URL:** Habilitar los parámetros de URL le permite cambiar la URL de inicio de una nueva sesión cuando los usuarios inician una aplicación. Para que esta directiva se aplique, configure un servidor proxy local para identificar sitios web sospechosos y, así, redirigirlos a Remote Browser Isolation. De forma predeterminada, esta configuración está inhabilitada. Para obtener más información, consulte Proof of Concept Guide: URL Redirection to Remote Browser Isolation with Citrix ADC in Azure.
  - **Seguimiento de nombres de host:** Utilice el seguimiento de nombres de host para que Remote Browser Isolation registre los nombres de host durante una sesión de usuario. Esta directiva está inhabilitada de manera predeterminada. Esta información se comparte con Citrix Analytics. Para obtener más información, consulte Citrix Analytics.

  Cuando haya terminado, haga clic en **Aceptar**.

- **Listas de Direcciones URL permitidas:** use la tarea **Listas de permitidos** para restringir a los usuarios a visitar solo las URL incluidas en la lista de permitidos dentro de su sesión publicada de Remote Browser Isolation. Esta función está disponible para aplicaciones web externas autenticadas.

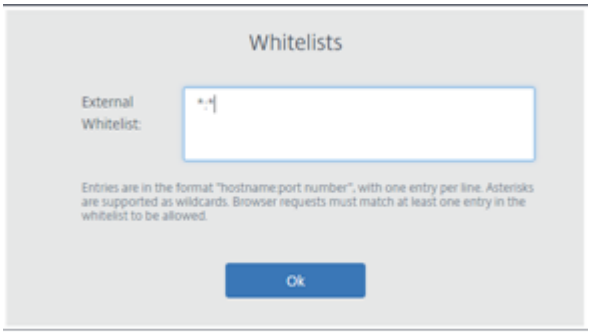
  Introduzca las entradas de la lista de permitidos en el formato `hostname:port number`. Especifique cada entrada en una nueva línea. Se admiten los asteriscos como comodines. Las solicitudes del explorador deben coincidir con, al menos, una entrada de la lista de permitidas.

  Por ejemplo, para establecer `https://example.com` como URL permitida:

  - `example.com:*` permite la conexión a esta URL desde cualquier puerto.
  - `example.com:80` permite la conexión a esta URL solo desde el puerto 80.
  - `*:*` permite el acceso a esta URL desde cualquier puerto y desde cualquier enlace a otras URL y puertos. El formato `*.*` permite el acceso a todas las aplicaciones web externas desde la aplicación publicada. Este formato es el valor predeterminado para el campo **Lista externa de permitidos** de las aplicaciones web.

  Cuando haya terminado, haga clic en **Aceptar**.

Las capacidades avanzadas de filtrado web están disponibles a través de la integración de Control Access Service. Más información en Caso de uso: acceso selectivo a aplicaciones.



- **Filtrado de URL:** puede configurar el filtrado de URL para controlar los métodos de acceso basados en categorías predefinidas asociadas a modelos de riesgo. Las opciones de filtrado de URL incluyen:
  - **Ninguno**: Se permiten todas las categorías.
  - **Flexible**: Se maximiza el acceso, aunque se sigue controlando el riesgo desde sitios web ilegales o malintencionados. Incluye las siguientes categorías:
    - **Adultos:** Grotesco, educación sexual, pornografía, desnudez, servicios sexuales, búsqueda y enlaces para público adulto, trajes de baño y lencería, revistas y noticias para adultos, expresión sexual (texto), fetichismo y citas.
    - **Informática e Internet:** Proxies remotos, direcciones IP privadas, intercambio de archivos punto a punto y archivos torrent.
    - **Apuestas:** Sorteos, premios, loterías y juegos de azar en general.
    - **Ilegal y dañino:** Terrorismo, extremismo, odio, calumnias, armas, violencia, suicidio, drogas ilegales, medicamentos, actividades ilegales, marihuana y defensa en general.
    - **Malware y spam:** Pirateo, malware, spam, spyware, botnets, sitios infectados, sitios de phishing, registradores de pulsaciones de teclas, malware para móviles, bots telefónicos, sitios web maliciosos y peligrosos.
  - **Moderado**: Se minimiza el riesgo, al tiempo que se permite el acceso a categorías adicionales con una baja probabilidad de exposición desde sitios no seguros o malintencionados. Incluye las siguientes categorías:
    - **Adultos:** Grotesco, educación sexual, pornografía, desnudez, servicios sexuales, búsqueda y enlaces para público adulto, trajes de baño y lencería, revistas y noticias para adultos, expresión sexual (texto), fetichismo y citas.
    - **Negocios e industria:** Subastas.
    - **Informática e Internet:** Anuncios, pancartas, proxies remotos, direcciones IP privadas, intercambio de archivos punto a punto y archivos torrent.

    * **Descargas:** Tiendas de aplicaciones móviles, servicios de almacenamiento, descargas y descargas de programas.
    * **Correo electrónico:** Suscripciones de correo y correo electrónico basadas en la web.
    * **Finanzas:** Criptomonedas.
    * **Apuestas:** Sorteos, premios, loterías y juegos de azar en general.
    * **Malware y spam:** Pirateo, malware, spam, spyware, botnets, sitios infectados, sitios de phishing, registradores de pulsaciones de teclas, malware para móviles, bots telefónicos, sitios web maliciosos y peligrosos.
    * **Mensajería, chat y telefonía:** Mensajes instantáneos y chat basado en la Web.
    * **Noticias, entretenimiento y sociedad:** WordPress (mensajes y cargas), URL no admitidas, oculto, sin contenido, miscelánea, horóscopo, astrología, adivinación, bebidas, religiones, páginas web personales, blogs y juegos en línea.
    * **Redes sociales:** Sitios de búsqueda y uso compartido de fotos, tablones de anuncios de TI y tablones de anuncios.

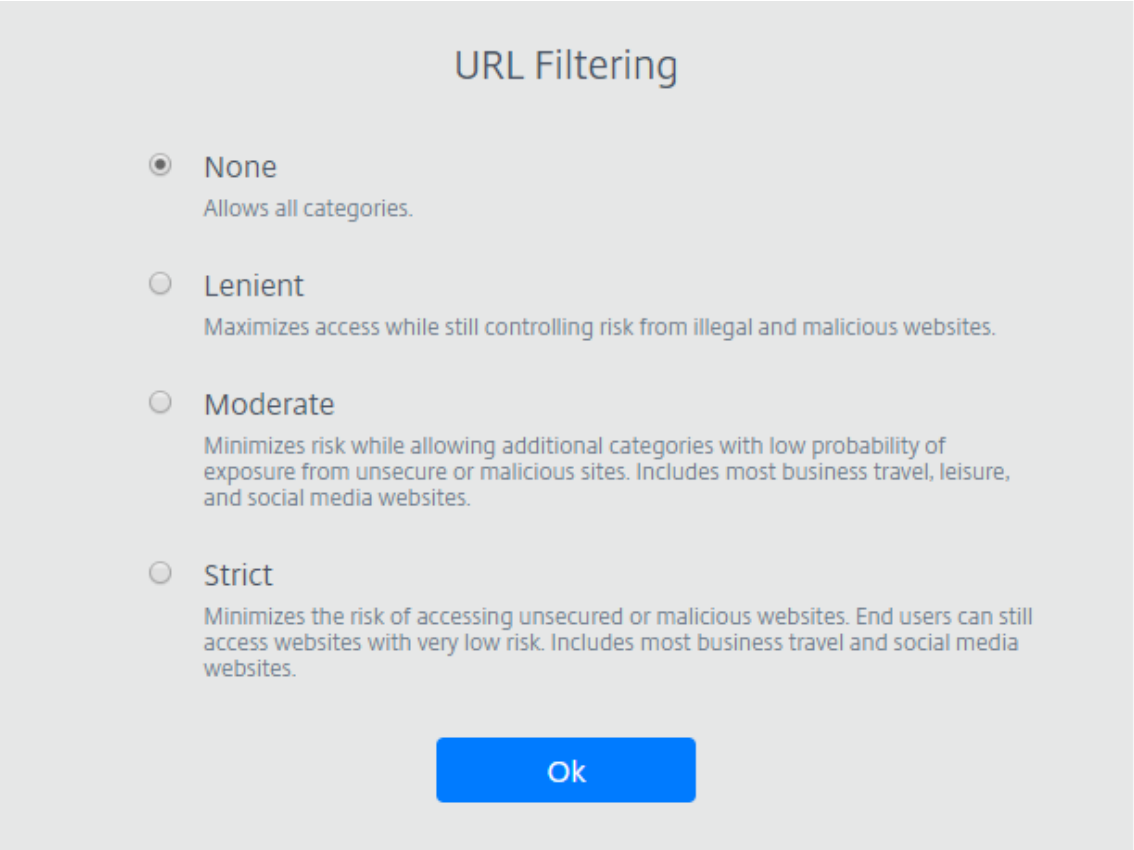
  – **Estricto**: Se minimiza el riesgo de acceso a sitios web malintencionados o no seguros. Los usuarios finales no pierden el acceso a sitios web que presenten un riesgo bajo. Incluye las siguientes categorías:

    * **Adultos:** Grotesco, educación sexual, pornografía, desnudez, servicios sexuales, búsqueda y enlaces para público adulto, trajes de baño y lencería, revistas y noticias para adultos, expresión sexual (texto), fetichismo y citas.
    * **Negocios e industria:** Subastas.
    * **Informática e Internet:** Anuncios, pancartas, DNS dinámico, aplicaciones móviles, editores, dominios estacionados, proxies remotos, direcciones IP privadas, intercambio de archivos punto a punto y archivos torrent.
    * **Descargas:** Tiendas de aplicaciones móviles, servicios de almacenamiento, descargas y descargas de programas.
    * **Correo electrónico:** Suscripciones de correo y correo electrónico basadas en la web.
    * **Finanzas:** Criptomonedas y productos financieros.
    * **Apuestas:** Sorteos, premios, loterías y juegos de azar en general.
    * **Ilegal y dañino:** Terrorismo, extremismo, odio, calumnias, armas, violencia, suicidio, drogas ilegales, medicamentos, actividades ilegales, marihuana y defensa en general.
    * **Empleos y currículos:** Empleo, promoción profesional y LinkedIn (actualizaciones, correo, conexiones y trabajos).
    * **Malware y spam:** Pirateo, malware, spam, spyware, botnets, sitios infectados, sitios de phishing, registradores de pulsaciones de teclas, malware para móviles, bots telefónicos, sitios web maliciosos y peligrosos.
    * **Mensajería, chat y telefonía:** Mensajes instantáneos y chat basado en la Web.
    * **Noticias, entretenimiento y sociedad:** WordPress (mensajes y cargas), alojamiento, viajes y turismo, URL no admitidas, política, moda y belleza, artes y eventos culturales,

referencia, ocio y pasatiempos, comunidades locales, miscelánea, bebidas, temas populares, eventos especiales, noticias, sociedad y cultura, revistas en línea, juegos en línea, eventos de la vida, ocultismo, sin contenido, horóscopo, astrología, adivinación, celebridades, medios de streaming, entretenimiento, lugares, actividades, páginas web personales y blogs, y religiones.

* **Redes sociales:** Redes sociales en general, YikYak (publicaciones), Twitter (publicaciones, correo y seguimiento), Vine (cargas, comentarios y mensajes), Google+ (carga de fotos y vídeos, publicaciones, chat de vídeo y comentarios), Instagram (cargas y comentarios), YouTube (acciones y comentarios), Facebook (grupos, juegos, preguntas, carga de vídeo, carga de fotos, eventos, chat, aplicaciones, publicaciones, comentarios y amigos), Tumblr (publicaciones, comentarios, fotos y vídeos), Pinterest (pines y comentarios), tablones de anuncios de TI y tablones de anuncios.

Cuando haya terminado, haga clic en **Aceptar**.



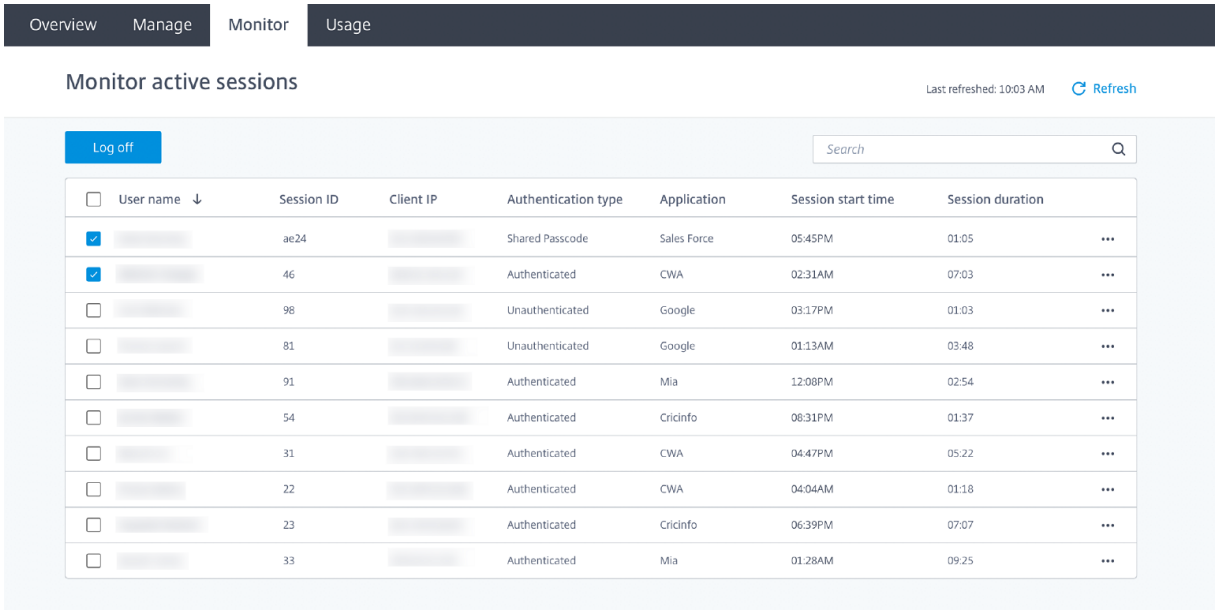
- **Modificar:** puede usar la tarea **Modificar** para cambiar el nombre, la URL de inicio o la región de un explorador publicado, o bien el código de acceso. Cuando termine, haga clic en **Publicar**.
- **Eliminar:** puede usar la tarea **Eliminar** para quitar un explorador aislado publicado. Cuando selecciona esta tarea, se le solicita que confirme la eliminación.

Supervisar

La ficha **Supervisar** proporciona información en tiempo real sobre las sesiones de los usuarios. Se pueden supervisar y desconectar una o varias sesiones activas.

Para detener una sola sesión, selecciónela y haga clic en el menú de puntos suspensivos al final de la fila de una entrada. Haga clic en **Cerrar sesión** y confirme los cambios.

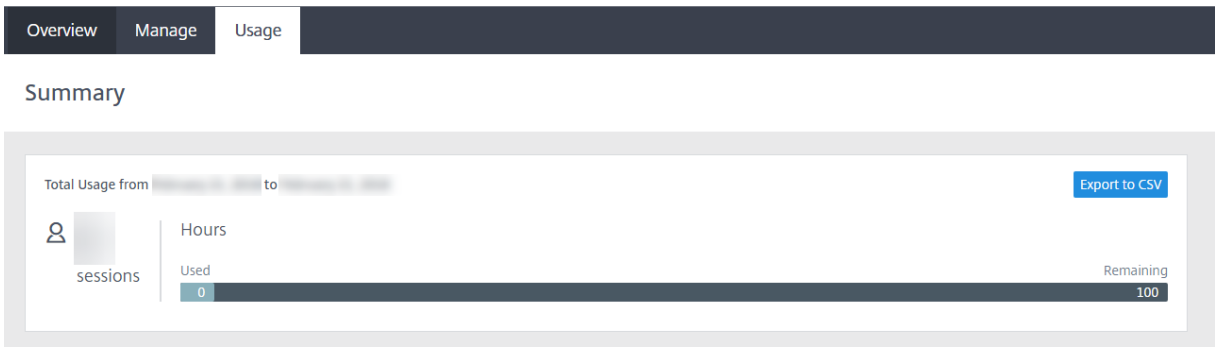
Para desconectar varias sesiones, seleccione las sesiones activas en la lista y haga clic en el botón **Cerrar sesión** en la parte superior de la página. Después de confirmar los cambios, Remote Browser Isolation desconecta inmediatamente todas las sesiones seleccionadas.



Uso

La ficha **Uso** muestra el número de sesiones iniciadas y el número de horas utilizadas.

Para crear una hoja de cálculo que contenga los detalles de uso, haga clic en **Exportar a CSV** y seleccione un período de tiempo.



Información técnica general sobre la seguridad de Remote Browser Isolation

October 14, 2022

Remote Browser Isolation (antes denominado Secure Browser Service) es un producto SaaS administrado y operado por Citrix. Permite el acceso a aplicaciones web a través de un explorador web intermedio cuyo host está en la nube.

Servicio Cloud

Citrix Remote Browser Isolation Service consta de exploradores web en los agentes Virtual Delivery Agent (VDA) junto con la consola de administración utilizada para administrar y conectar a los usuarios a estos VDA. Citrix Cloud administra el funcionamiento de estos componentes, incluida la seguridad y la aplicación de parches a los sistemas operativos, los exploradores web y los componentes de Citrix.

Mientras utiliza Remote Browser Isolation Service, los exploradores web alojados rastrean el historial de navegación del usuario y almacenan en caché las solicitudes HTTP. Citrix utiliza perfiles obligatorios y garantiza que estos datos se eliminen cuando finalice la sesión de navegación.

Se puede acceder a Remote Browser Isolation Service desde un explorador web compatible con HTML5. El servicio no proporciona ningún cliente descargable. Todo el tráfico que tenga lugar entre el explorador que se usa y el servicio en la nube se cifra mediante el cifrado estándar TLS. Remote Browser Isolation solo admite TLS 1.2.

El tráfico de salida para Remote Browser Isolation utiliza direcciones IP específicas para proteger la red interna. Para obtener la lista de direcciones IP aceptadas, consulte el artículo CTX286379 de Knowledge Center.

Aplicaciones web

Citrix Remote Browser Isolation Service se utiliza para entregar aplicaciones web que son propiedad del cliente o de un tercero. El propietario de la aplicación web es responsable de su seguridad, lo que incluye aplicar parches al servidor web y a la aplicación para protegerlos de vulnerabilidades.

La seguridad del tráfico entre Remote Browser Isolation y la aplicación web depende de los parámetros de cifrado del servidor web. Para proteger este tráfico según fluye por Internet, los administradores publican las URL de HTTPS.

Más información

Consulte los siguientes recursos para obtener más información acerca de la seguridad:

- Sitio de seguridad de Citrix: https://www.citrix.com/security
- Documentación de Citrix Cloud: Guía de implementación segura para la plataforma Citrix Cloud