# Citrix Analytics for Security

**Machine translated content**

## Disclaimer

# Contents



# Novedades

June 18, 2024

Un objetivo de Citrix es ofrecer nuevas funciones y actualizaciones de productos a los clientes de Citrix Analytics cuando estén disponibles. Las nuevas versiones añaden valor al producto y no hay motivo para retrasar el momento de actualizar.

Para usted, como cliente, 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 de actualizaciones incrementalmente en ondas ayuda a garantizar la calidad del producto y a maximizar la disponibilidad.

## 15 de abril de 2024

### Nuevo informe resumen ejecutivo

Ahora tiene la opción de consolidar varios informes en un solo informe ejecutivo que se puede programar para el período de tiempo requerido. Con esta nueva función, solo está proporcionando a su audiencia la información gráfica necesaria. Para obtener más información, consulte Informe resumen ejecutivo.

## 29 de enero de 2024

### Actualizaciones del campo de estado de la aplicación Workspace

- **Búsqueda de autoservicio**: Ahora puede realizar consultas para averiguar el estado de compatibilidad de una versión de la aplicación Workspace mediante el campo de estado de la aplicación **Workspace** recientemente introducido para el origen de datos de **Citrix Apps and Desktops**.
- **Usuarios**: Se ha eliminado la columna **Estado de la aplicación Workspace**.

Para obtener más información, consulte Búsqueda de autoservicio de aplicaciones y escritorios.

## 25 de enero de 2024

### Se simplifican las inconsistencias en la interfaz de usuario de CAS

Se han resuelto los siguientes problemas en la función de **búsqueda de autoservicio** para el origen de datos de **Apps and Desktops**:

- Los eventos que antes se mostraban desordenados dentro de una sesión ahora aparecen correctamente.
- Se han actualizado las columnas predeterminadas.

## 24 de enero de 2024

### Eventos de perfil de usuario mejorados en entornos SIEM

Los eventos de perfil de usuario exportados a sus entornos de SIEM ahora incluyen:

- Información sobre direcciones IP
- Información sobre la ubicación de Citrix Virtual Apps and Desktops y Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service)

Estas nuevas mejoras le permiten identificar la dirección IP del cliente utilizada para acceder a los datos de su organización y recopilar información sobre la ubicación de los usuarios tanto de Citrix Virtual Apps and Desktops como de Citrix DaaS.

Para obtener más información, consulte Datos de información sobre riesgos para SIEM.

## 01 de diciembre de 2023

### Página de configuración de correo electrónico de administrador para alertas semanales de correo electrónico y SIEM

La nueva función de **configuración del correo electrónico del administrador** le permite configurar destinatarios de listas de distribución personalizadas para las alertas del sistema. Esta mejora garantiza que los administradores reciban solo las alertas del sistema que son relevantes para ellos.

Para obtener más información, consulta Configuración de correo electrónico de administrador.

### Panel de usuarios: nuevo filtro de tiempo de recuento de usuarios activos y actualización de la sección Descripción general

El nuevo filtro de tiempo del panel de **usuarios** le permite ver y modificar el número total de usuarios activos de su organización durante un período de tiempo específico, teniendo en cuenta las fuentes de datos para las que ha habilitado Citrix Analytics.

La sección **Descripción general** mejorada del panel de **usuarios** muestra el número total de usuarios de su organización, así como el número de usuarios activos e inactivos que han iniciado sesión actualmente.

Para obtener más información, consulte Panel de control de usuarios.

#### Informes personalizados mejorados

- Ahora puede crear y programar informes personalizados mediante los eventos y la información disponibles en Citrix Analytics for Security. Los informes personalizados le ayudan a extraer información de interés específico y a organizar los datos gráficamente.
- Ahora puede utilizar las funciones mejoradas de la plataforma de informes personalizados, que incluyen informes basados en consultas de búsqueda de autoservicio, plantillas, mejores visualizaciones, cobertura de todas las fuentes de datos y métricas, programación de informes y exportación de archivos PDF.

Para obtener más información, consulte Informes personalizados.

### 30 de noviembre de 2023

#### Eliminación de todas las capacidades de ShareFile en Citrix Analytics

Se eliminan las siguientes funciones de detección de ShareFile:

- Compartir enlaces
- Indicadores de riesgo asociados
- Directivas con sus ocurrencias
- Configuraciones de exportación de datos de Content Collaboration
- Informes de Content Collaboration
- Fuente de datos de Content Collaboration en Search
- Búsquedas guardadas de Content Collaboration
- Fuente de datos de Content Collaboration.

La eliminación de estas capacidades podría provocar una incoherencia temporal en la puntuación de riesgo y los plazos de los usuarios. Todas las demás capacidades de Citrix Analytics siguen siendo las mismas.

Descubra cómo ShareFile simplifica el acceso a los controles de seguridad directamente desde Sharefile.com.

### 22 de septiembre de 2023

#### Fuente de datos de Citrix Secure Browser en un indicador personalizado

Ahora puede crear indicadores de riesgo para la fuente de datos de Citrix Secure Browser para rastrear la actividad de un usuario en el navegador seguro. Para obtener más información, consulte Indicadores personalizados.

#### Mejora del correo electrónico semanal con la exportación de datos SIEM

El correo electrónico semanal se ha mejorado para proporcionar una visión más profunda de la postura de seguridad de su organización al permitir la exportación de datos SIEM. Ahora puede incorporar y activar más fuentes de datos para descubrir una amplia gama de eventos relacionados con sus usuarios. El correo electrónico semanal incluye las siguientes novedades:

- La sección de resumen de datos muestra el estado del consumo de datos en el entorno SIEM.
- Recomendaciones para la exportación de datos en función del estado de consumo de la exportación de datos.

Para obtener más información, consulte Notificación por correo electrónico semanal.

#### Consumo de las preferencias de notificación personalizadas del administrador en los correos electrónicos

Citrix Analytics for Security ahora respeta las preferencias de notificación establecidas por los administradores personalizados en Citrix Cloud. Esta mejora proporciona a los administradores personalizados una mayor flexibilidad a la hora de gestionar sus preferencias de notificación. Esta preferencia también se aprovecha al enviar correos electrónicos de notificación, como correos electrónicos semanales, correos electrónicos de acción de Notificar a los administradores y alertas para la exportación de datos.

Para obtener más información, consulte Administrar las funciones de administrador de Security Analytics.

### 04 de julio de 2023

#### Función para el operador OR en la búsqueda de autoservicio y el indicador personalizado

El operador **OR** ahora está disponible en las funciones de **búsqueda de autoservicio** e **indicador de riesgo personalizado**. Puede utilizar el operador **OR** en las vistas de búsqueda, como la búsqueda de autoservicio y las consultas de indicadores personalizados.

Para obtener más información, consulte Operadores compatibles en la consulta de búsqueda.

### 15 de junio de 2023

#### Habilitar la telemetría del portapapeles de VDA

Un evento denominado VDA.Clipboard se activa al iniciar cualquier operación de portapapeles en Citrix Apps and Desktops. Estos registros del portapapeles proporcionan información vital, como el

nombre del VDA, el tamaño del portapapeles, el tipo de formato del portapapeles, la IP del cliente, el funcionamiento del portapapeles, la dirección de operación del portapapeles y si la operación del portapapeles estaba permitida. Los atributos del evento del portapapeles de VDA también están disponibles en los flujos de trabajo de búsqueda automática y de indicadores de riesgo personalizados.

- **Búsqueda automática:**puede generar informes, guardar consultas y revisar los eventos de VDA.Clipboard junto con todos los detalles de sus atributos.
- **Indicadores de riesgo personalizados**: Los atributos de los eventos del portapapeles del VDA están disponibles con el flujo de trabajo de indicadores personalizados. Puede usar estos pares clave/valor del evento para configurar activadores de indicadores personalizados y configurar directivas automatizadas con acciones.

Puede utilizar la directiva **Recopilación de metadatos del portapapeles para la supervisión de seguridad** para habilitar la telemetría del portapapeles y la transmisión de los registros del portapapeles a Citrix Analytics for Security. De manera predeterminada, esta directiva está habilitada. Para inhabilitarla, vaya a la página de directivas e inhabilítela para detener la recopilación de datos de los VDA.

Para obtener más información, consulte Habilitar la telemetría del portapapeles para Citrix DaaS.

## 14 de junio de 2023

### Disponibilidad del ciclo de vida de la aplicación de grabación de sesiones y de los eventos de registro en Citrix Analytics for Security

Los siguientes eventos del **Registro** y del **Ciclo de vida de las aplicaciones** de **Grabación de sesiones** ya están disponibles en Citrix Analytics for Security:

- Citrix.EventMonitor.RegistryChange
- Citrix.EventMonitor.SessionLaunch
- Citrix.EventMonitor.SessionEnd
- Citrix.EventMonitor.Clipboard
- Citrix.EventMonitor.FileTransfer

Puede ver estos eventos, crear indicadores personalizados y exportarlos a sus entornos SIEM.

Para obtener más información, consulte Tipos de eventos y campos compatibles.

## 08 de junio de 2023

### Problemas resueltos

- Algunos eventos de inicio de sesión que se envían a Citrix Analytics for Security no tienen nombre de usuario. Esto hace que la columna de nombre de usuario aparezca como **NA** para algunos eventos de la página de inicio de sesión de usuario de Self-Service Search y Access Assurance. A veces, también da como resultado que el recuento de usuarios únicos sea cero, aunque el recuento total de inicios de sesión no es cero en el gráfico de organizaciones de registro de IP de Access Assurance cuando se ven los datos de un rango de tiempo reducido, como la **última hora** o **el último 1 día**. Este problema ya está solucionado. [CAS-70954]
- En la búsqueda de autoservicio para aplicaciones y escritorios, para los eventos Session.Logon y Session.End user, la dimensión App-Name de las consultas de búsqueda se rellena con nombres de grupos de entrega en lugar del nombre de la aplicación o el escritorio iniciados, lo que puede inducir a error a los administradores. La dimensión App-Name es más útil para consultas en eventos App.Start/App.End, ya que apunta a las aplicaciones que se están iniciando. Para obtener más información, consulte Búsqueda de autoservicio para aplicaciones y escritorios. Este problema ya está solucionado. [CAS-67968]
- Si su organización se incorpora a Citrix Cloud en la región de origen de **Asia Pacífico Sur**, los eventos de Content Collaboration no están visibles en sus arrendatarios de Citrix Analytics. Este problema ya está solucionado. [CAS-62317]
- Pocas versiones de la aplicación Citrix Workspace y del cliente Citrix Receiver no envían eventos específicos a Citrix Analytics. Por lo tanto, Citrix Analytics no puede proporcionar información ni generar indicadores de riesgo para estos eventos. Este problema ya está solucionado. Para obtener más información, consulte la Comprobación 6: ¿Se transmiten los eventos de escritorios y aplicaciones virtuales a Analytics?. [CAS-16151]

## 29 de mayo de 2023

### El complemento de Citrix Analytics para Splunk ya está disponible en la plataforma Splunk Cloud

La integración de Splunk para Citrix Analytics utiliza el complemento Citrix Analytics para Splunk para conectarse al entorno de análisis e incorporar datos empresariales críticos a su entorno de Splunk.

Anteriormente, Splunk solo examinaba el complemento para su instalación en la capa Splunk Enterprise y los clientes eran responsables de configurar el complemento en su entorno local de Splunk. Con la última versión de 2.1.2, el complemento tiene la compatibilidad adicional de la plataforma

Splunk con Splunk Cloud. Los clientes que utilicen instancias **clásicas** con instancias de IDM o **Victoria** pueden utilizar esta mejora de compatibilidad de plataformas. Ahora, los clientes tienen la flexibilidad de elegir entre Splunk Enterprise o Splunk Cloud y, al mismo tiempo, considerar la implementación de nuestro complemento para facilitar la integración con Splunk.

Para obtener más información, consulte Splunk Integration.

#### Grabación de eventos de sesión en SIEM

Los eventos de **grabación de sesiones** ahora se pueden exportar a SIEM en forma de eventos de **Risk Insight** y eventos de **fuente de datos** para aplicaciones y escritorios. Los tipos de eventos recién agregados se encuentran en la etapa Eventos de datos para exportación, en la página **Exportaciones de datos**.

Para obtener más información, consulte Directivas y acciones.

### 24 de mayo de 2023

#### Notificar la acción global del usuario final

La función **Directivas y acciones** de Citrix Analytics ahora admite la acción global **Notificar al usuario final**, que se puede combinar con activadores de indicadores de riesgo integrados o personalizados. Los administradores pueden crear directivas con la acción **Notificar al usuario final**, que genera notificaciones por correo electrónico únicamente para los usuarios finales. Esta acción se puede utilizar para varios casos de uso relacionados con el cumplimiento, como notificar a los usuarios el uso no autorizado de una aplicación o alertar sobre comportamientos sospechosos en sus cuentas de Citrix sin tomar ninguna medida perjudicial. Los administradores pueden personalizar el cuerpo y el asunto del mensaje de correo electrónico en función del caso específico.

Para obtener más información, consulte Notificar al usuario final.

### 04 de mayo de 2023

#### Generación de eventos de prueba

La función de **generación de eventos de prueba** se creó para ayudar a los clientes a probar rápidamente su proceso entre Citrix Analytics y SIEM. Antes, si el administrador tenía que probar esta integración, tenía que esperar a que se incorporaran las fuentes de datos y a la actividad de los usuarios para comprobar si Citrix Analytics generaba los eventos y, por lo tanto, los recibía su entorno SIEM. Esto ya no es una necesidad. Basta con hacer clic en el botón **Enviar datos de prueba** para enviar un evento ficticio al entorno SIEM y utilizar la consulta proporcionada para comprobar si la integración

SIEM de Citrix Analytics está configurada como se esperaba. Esto también puede funcionar para el administrador que intenta depurar el flujo de datos interrumpido, ya que puede ayudar a aislar el punto de error.

Para obtener más información, consulte Generación de eventos de prueba.

#### Generación de alertas de correo electrónico de SIEM

La capacidad de generación de alertas por correo electrónico de SIEM lleva la solución de problemas de la exportación de datos a un nuevo nivel de facilidad. Citrix Analytics envía alertas al sistema sobre las actividades que pueden provocar o indicar una interrupción del flujo de datos del SIEM. El correo electrónico se distribuye entre los administradores de Citrix Cloud, los administradores de seguridad completa, los administradores de solo lectura de seguridad y los administradores de solo lectura de seguridad y rendimiento. Los siguientes son los diferentes tipos de alertas que se envían:

1. **Alerta de exportación de datos SIEM: Se restableció la contraseña**

   Este correo electrónico se activa cada vez que se restablece la contraseña de la cuenta desde la página de exportación de datos. Si solo se hace en la GUI de Citrix Analytics for Security, puede provocar una interrupción en el flujo de datos. Esta alerta contiene la hora en la que se restableció la contraseña y, por lo tanto, facilita mucho el restablecimiento del flujo de datos correcto.

2. **Alerta de exportación de datos SIEM: Se detuvo el flujo de datos**

Este correo electrónico se activa cada vez que el cliente se enfrenta a una interrupción del flujo de datos

- **Más de 24 horas**: Tiempo crítico para volver rápidamente a un flujo de datos correcto utilizando los útiles consejos de solución de problemas de la alerta o utilizando la ficha **Resumen de exportación de datos** con la **Guía rápida**.
- **Más de 7 días**: La directiva de retención de Kakfa para cada tema de cliente es de siete días, lo que significa que existe la posibilidad de que algunos datos de seguridad hayan caducado. Es imperativo utilizar las herramientas de solución de problemas para restablecer el flujo de datos al SIEM.
- **Más de 30 días**: Esto significa que el cliente ha tenido problemas de seguridad en los datos y debe prestar atención inmediata a la restauración del flujo de datos de Citrix Analytics al entorno SIEM.

Para obtener más información, consulte Generación de alertas por correo electrónico de SIEM.

## 13 de abril de 2023

### Problema resuelto

La aplicación Citrix Workspace de Windows envía una propiedad de nombre, ruta y formato de archivo vacía desde la versión 2203 y versiones posteriores de la aplicación Citrix Workspace. Como resultado, la GUI de Citrix Analytics for Security muestra los valores NA para las columnas Nombre del archivo de descarga, Ruta del archivo de descarga y Formato de archivo de descarga. Este problema ya está solucionado. [CAS-73498]

## 31 de marzo de 2023

### Eventos de grabación de sesiones en Citrix Analytics for Security

En Citrix Apps and Desktops, se han agregado dos nuevos tipos de eventos para ayudar a identificar y evaluar los eventos basados en la grabación de sesiones.

- Citrix.EventMonitor.RDPConnection
- Citrix.EventMonitor.UserAccountModification

Los administradores ahora pueden identificar y evaluar fácilmente los posibles riesgos de seguridad. Pueden utilizar estos eventos para recopilar información sobre datos vitales, como los identificadores de procesos, las direcciones IP de destino y las descripciones de las operaciones de las cuentas de usuario. Además, estos eventos también se pueden encontrar en la página de **indicadores de riesgo personalizados** y en la página **de búsqueda por autoservicio**.

- **Búsqueda automática**: puede ver estos eventos junto con los detalles de sus atributos.
- **Indicadores de riesgo personalizados**: puede configurar cualquier indicador personalizado mediante estos tipos de eventos.
  Para obtener más información, consulte Tipos de eventos y campos compatibles.

### Eventos de protección de aplicaciones en la búsqueda de autoservicio

Un nuevo evento denominado **AppProtection.ScreenCapture se activa cuando intenta capturar** una captura de pantalla mientras se encuentra en una sesión protegida en la fuente de datos de Citrix Apps and Desktops. Los eventos **AppProtection.ScreenCapture** también están disponibles en las páginas **Búsqueda de autoservicio** y **Exportación de datos**.

- **Búsqueda de autoservicio:** Puede ver los resultados de **AppProtection.ScreenCapture** junto con todos los detalles de sus atributos.

- **Exportaciones de datos**: puede ver el tipo de evento **AppProtection.ScreenCapture** en la sección Exportaciones de datos. Vaya a **Configuración > Exportaciones de datos > Configuración > Eventos de datos para exportar >** seleccione **Aplicaciones y escritorios** en la categoría Eventos de fuentes de datos (opcional).

También puede ver un nuevo atributo denominado **Directivas de protección de aplicaciones** para el evento **Session.Logon**.

Para obtener más información, consulte Tipos de eventos y campos compatibles.

## 30 de marzo de 2023

### Soporte de roles personalizados

Se puede agregar un administrador para funciones personalizadas mediante grupos de Active Directory o Azure Active Directory o configurando una integración de Okta para Citrix Analytics for Security. Esta integración permite un enfoque simplificado para administrar los permisos de acceso a los servicios para todos los administradores de grupos.

Después de agregar correctamente un administrador a Active Directory o Azure Active Directory, el administrador puede crear grupos y asignar un rol personalizado a un grupo específico. Los permisos individuales tienen preferencia sobre los permisos de grupo si un administrador es miembro de ambos.

Para obtener más información, consulte Soporte de roles personalizados.

### Panel de solución de problemas para la interfaz de usuario de SIEM

La interfaz de usuario de exportación de datos se ha mejorado con los siguientes cambios:

- **Ficha de resumen**: la ficha Resumen describe las métricas de los eventos de SIEM, el estado de incorporación a la fuente de datos y el estado del consumo de datos en el siguiente escenario:
  - **Datos disponibles en Citrix Analytics**: proporciona el estado de incorporación de las diferentes fuentes de datos.
  - **Eventos disponibles para el consumo de SIEM**: proporciona la cantidad de información que se envía a su entorno de SIEM.
  - **Consumo de datos por SIEM**: proporciona el estado del consumo de datos.
- **Ficha Configuración**: La ficha **Configuración** contiene información sobre la configuración de la cuenta, la configuración del entorno SIEM y la selección de eventos de datos.
- **Guía rápida de exportación de datos**: los administradores ahora pueden utilizar la **Guía rápida**, que facilita la configuración y el mantenimiento de las integraciones de SIEM. Se puede

acceder al enlace **Guía rápida de exportación de datos** desde las fichas **Resumen** y **Configuración**.

Para obtener más información, consulte Solución de problemas de exportación de datos.

## 24 de marzo de 2023

### Cambio en la vista del perfil de usuario

**Los datos del perfil de los usuarios** relacionados con las aplicaciones, las ubicaciones, los dispositivos y el uso de datos de ShareFile no están disponibles en la página de **información del usuario** de la cronología del usuario. La siguiente información de usuario que proviene de Active Directory aún está disponible -

- Título del puesto
- Dirección
- Correo electrónico
- Teléfono
- Ubicación
- Organización

No hay cambios en los datos del perfil de usuario que se exportan a SIEM. Para obtener más información, consulte Perfil de usuario.

### Eliminación de las sugerencias automáticas dinámicas de todas las vistas de búsqueda

La función de sugerencia automática para dimensiones basadas en los datos históricos del arrendatario ahora está en desuso en las siguientes páginas:

- Búsqueda de autoservicio
- Indicador de riesgo personalizado

Sin embargo, las sugerencias estáticas para dimensiones como el **tipo de evento** y las **operaciones del portapapeles** siguen disponibles en el cuadro de búsqueda.

Para obtener más información, consulta Cómo utilizar la búsqueda automática.

## 21 de marzo de 2023

### Panel Recomendaciones para ayudar a integrar el origen de datos local de StoreFront

Se ha introducido el nuevo panel **Recomendaciones** en la página **Orígenes de datos**. El panel **Recomendaciones** de la página **Orígenes de datos** informa al usuario sobre la importancia de incorpo-

rar los orígenes de datos de StoreFront locales. Ayuda al usuario a incorporar fácilmente los orígenes de datos locales de StoreFront y también ofrece una opción para que el usuario revise y garantice la incorporación de todos los orígenes de datos disponibles.

Para obtener más información, consulte Conectarse a una implementación de StoreFront.

## 23 de febrero de 2023

### Problemas resueltos

Las acciones fallan para las implementaciones locales de Citrix Apps and Desktop en las que la versión de Citrix Apps and Desktop es superior a 1912. Este problema se ha visto tanto en las acciones manuales como en las basadas en directivas. Este problema ya está solucionado. [CAS-69098]

La página Búsqueda de aplicaciones y escritorios de autoservicio muestra varios eventos de inicio y finalización de aplicaciones cuando las aplicaciones virtuales se inician solo una vez. Este problema se produce en las versiones cliente de la aplicación Citrix Workspace para Linux. Este problema ya está solucionado. [CAS-36236]

Es posible que los eventos de usuario de Secure Private Access Service posteriores al 4 de abril de 2022 y hasta finales de mayo de 2022 no estén disponibles en sus arrendatarios de Citrix Analytics. Este problema ya está solucionado. [CAS-66897]

## 22 de febrero de 2023

### Mejora de las notificaciones semanales por correo electrónico

Citrix Analytics envía notificaciones semanales por correo electrónico que ayudan a resumir los riesgos de seguridad de su organización. La notificación semanal por correo electrónico se ha mejorado con las siguientes actualizaciones:

- Proporciona una vista de la distribución de riesgos de los usuarios: total de usuarios descubiertos, número de usuarios con riesgo y sin riesgo durante una semana
- Total de eventos procesados durante una semana
- Total de indicadores activados durante una semana
- Total de acciones realizadas durante una semana
- Total de fuentes de datos que están activadas para el procesamiento de datos

Para obtener más información, consulta Notificación semanal por correo electrónico.

#### Se agregó el campo de formato de archivo de descarga para el tipo de evento App.SaaS.File.Download

En la página de búsqueda automática de la fuente de datos de Apps and Desktops, se ha añadido un nuevo campo de **formato de archivo de descarga** para el tipo de evento App.SaaS.File.Download. Con este cambio, ahora puede configurar indicadores de riesgo personalizados para el campo **Formato de archivo de descarga** y también exportar el campo como parte del formato Exportar a CSV.

Para obtener más información, consulte Búsqueda de autoservicio de aplicaciones y escritorios.

#### Cambio en los campos derivados del navegador

Anteriormente, la página de búsqueda automática incluía los campos **Navegador**, **Versión principal delnavegador y Versión secundaria del navegador**para representar los nombres y las versiones del navegador. Sin embargo, para garantizar la claridad y la precisión, ahora estos tres campos están en desuso y se sustituyen por**Nombre**y**versión del navegador** en la búsqueda automática, plantilla de indicadores personalizados y descarga de CSV para la fuente de datos de aplicaciones y escritorios.

Para obtener más información, consulte Búsqueda de autoservicio de aplicaciones y escritorios.

### 16 de febrero de 2023

#### Problema resuelto

Los correos electrónicos semanales se ven afectados para algunos de los clientes de la UE y APS al obtener el estado de enmascaramiento de nombre de usuario de un arrendatario. Como resultado, los administradores reciben 10 correos electrónicos semanales idénticos debido a la excepción. Una vez que se produjo la excepción, los arrendatarios sucesivos no recibieron el correo electrónico semanal. Este problema ya se ha solucionado. [CAS-76138]

### 03 de febrero de 2023

#### Soporte analítico para el servicio Citrix Secure Private Access disponible en las regiones de la Unión Europea y Asia Pacífico Sur

Citrix Analytics for Security ahora procesa los eventos de los usuarios de Citrix Secure Private Access, disponible en la región de la Unión Europea y la región de Asia Pacífico Sur. Si su organización se ha incorporado a Citrix Cloud desde la región de la Unión Europea o la región de Asia Pacífico Sur, puede ver la información sobre los riesgos de los usuarios que utilizan el servicio Secure Private Access.

Para obtener más información, consulte Orígenes de datos.

## 11 de enero de 2023

### Eliminación de la capacidad de filtrado web de Secure Private Access

La capacidad de filtrado web se ha eliminado de la categoría Secure Private Access. Estas prestaciones de Citrix Analytics for Security se ven afectadas debido a que Secure Private Access ha dejado de utilizar el filtrado web basado en categorías:

1. Los campos de datos como el grupo de categorías, la categoría y la reputación de las URL ya no están disponibles en el panel de control de Citrix Analytics for Security.
2. El indicador de acceso a sitios web de riesgo, que se basa en los mismos datos, también se ha retirado y no se activa para los clientes.
3. Los indicadores de riesgo personalizados existentes que utilicen los campos de datos (categoría-grupo, categoría y reputación de las URL) y sus directivas asociadas ya no se activan.
4. Las fichas **Acceso de los usuarios** y **Acceso a las aplicaciones**.
5. Las exportaciones de SIEM seguirán teniendo los atributos urlcategory, urlcategorygroup y urlcategoryreputation durante algún tiempo con los siguientes valores ficticios:
   - 99999 para categoría y grupo de categorías
   - 0 por reputación

Para obtener más información, consulte Búsqueda de autoservicio de Secure Private Access.

## 27 de diciembre de 2022

### Menú desplegable de cambios en la fuente de datos para la búsqueda automática

La lista de fuentes de datos se cambia para reflejar **Sesiones** de forma predeterminada, en lugar de **Aplicaciones y escritorios**, en la página de búsqueda de autoservicio. Además, la sección Rendimiento se ha desplazado a la parte superior, seguida de la sección Seguridad, ya que los orígenes de datos de rendimiento no estaban visibles.

Para obtener más información, consulte Búsqueda de autoservicio.

## 13 de diciembre de 2022

### Mejora del panel de usuarios

El panel de usuarios se ha renovado con resúmenes y gráficos para ayudar a los administradores a supervisar la situación de seguridad de la organización. La vista no solo proporciona detalles de los

usuarios detectados, los indicadores de riesgo activados y las acciones aplicadas, sino que también proporciona una línea de tendencia basada en el tiempo de las métricas críticas para una mejor evaluación de los riesgos. Los administradores pueden analizar en detalle los datos de interés y acceder a los paneles pertinentes con el contexto adecuado para analizar los riesgos con mayor rapidez.

Para obtener más información, consulte Panel de control de usuarios.

## 05 de diciembre de 2022

### Panel de mandos de Access Assurance: Red de inicio de sesión

La sección Red de inicio de sesión se agregó recientemente y proporciona los siguientes detalles de usuario:

- Las organizaciones asociadas a las direcciones IP desde las que los usuarios han iniciado sesión.
- La subred pública única total y la subred privada desde las que los usuarios han iniciado sesión.
- Los detalles de que el usuario ha iniciado sesión mediante servidores proxy y servicios de VPN privadas.

Con estos detalles adicionales, un administrador puede validar los detalles de inicio de sesión del usuario y asegurarse de que el inicio de sesión del usuario cumple con las expectativas de seguridad de la organización.

Para obtener más información, consulte Panel de mandos de Access Assurance.

## 18 de noviembre de 2022

### Problema resuelto

- Se han corregido los indicadores de geocerca que se activaban por error sin tener ningún evento de origen. [CAS-73222]

## 08 de noviembre de 2022

### Cambiar el nombre de las acciones

Se cambia el nombre de algunas de las acciones que se utilizan en Citrix Analytics for Security para proporcionar más claridad. Esas acciones son las siguientes:

- **Notificar a los administradores**: Notifica a los administradores
- **Bloquear usuario**: Bloquea la cuenta de usuario

- **Cerrar sesión de usuario**: Cierra la sesión activa
- **Desbloquear usuario**: Desbloquea la cuenta de usuario
- **Inhabilitar usuario**: Inhabilita la cuenta de usuario

Para obtener más información, consulte ¿Cuáles son las acciones?

#### Problemas resueltos

- Si selecciona una opción del menú desplegable de acciones de la línea de tiempo, no podrá activar ninguna acción manual, ya que los botones Borrar y Aplicar no están visibles. Esta afección se produce en la última versión de Firefox. Este problema ya está solucionado. [CAS-72051]
- Las categorías **HardDrive**, **harddrive** y **HDD** se combinan en una sola categoría como **Hard Disk Drive** para el campo Tipo de dispositivo de descarga del origen de datos de aplicaciones y escritorios de la búsqueda de autoservicio de aplicaciones y escritorios. [CAS-67188]
- A veces, Microsoft Graph recibe notificaciones duplicadas con el mismo identificador de alerta, lo que provoca la creación de eventos de riesgo duplicados. Se implementa un mecanismo de desduplicación en las aplicaciones para evitar este problema. [CAS-66731]

### 19 de octubre de 2022

#### Fecha, origen, selección y exportación de eventos

Ahora puede aprovechar el nuevo flujo de trabajo de exportación de eventos de datos para exportar eventos de fuentes de datos, además de los eventos de información de riesgo generados por el aprendizaje automático y los datos asociados.

Esto permite a los administradores de operaciones de seguridad y seguridad (SOC):

- Correlacione los datos de Citrix Analytics con otros eventos de orígenes de datos agregados en la información de seguridad y la administración de eventos (SIEM)
- Controlar qué eventos de datos fluyen a los SIEM para optimizar los costes de almacenamiento

Los eventos de datos se envían a sus integraciones de SIEM y conectores de datos existentes y de forma similar a lo que está disponible en nuestra vista de búsqueda de eventos de autoservicio.

Para obtener más información, consulte Eventos de datos exportados de Citrix Analytics for Security a su servicio SIEM.

## 18 de octubre de 2022

### Permitir al administrador ejecutar una acción de grabación dinámica de sesiones en sitios de Citrix DaaS

Los administradores ahora pueden ejecutar acciones de grabación dinámica de sesiones en los sitios de Citrix DaaS y grabar dinámicamente las sesiones virtuales de los usuarios. Pueden configurar la acción con una directiva para iniciar automáticamente la grabación de las sesiones de los usuarios en caso de que Citrix Analytics for Security detecte una actividad arriesgada de un usuario determinado.

Para obtener más información, consulte ¿Cuáles son las acciones?

## 14 de octubre de 2022

### Proporcione comentarios sobre los indicadores de riesgo del usuario

Los administradores de Citrix Analytics for Security ahora pueden informar de que los indicadores de riesgo de los usuarios son útiles o no útiles proporcionando comentarios en el panel de detalles de los indicadores. Esta función permite a los administradores denunciar falsos positivos, reducir el ruido de los indicadores que se activan con frecuencia y compartir contexto adicional con otros administradores. Como resultado adicional, el indicador de riesgo poco útil se oculta en la cronología del usuario y se recalibra la puntuación de riesgo del usuario.

Para obtener más información, consulte Proporcionar comentarios sobre los indicadores de riesgo de los usuarios.

## 26 de septiembre de 2022

### Garantía de acceso para admitir la lista de geocercas bloqueados

Las fichas **Ubicación segura** y **Ubicaciones de riesgo** se agregan a los parámetros de geocercas.

- Las geocercas de Ubicación segura ayudan a identificar y restringir el acceso fuera del área de una geocerca definida.
- Las geocercas de ubicaciones de riesgos ayudan a detectar y restringir el acceso de los usuarios de riesgo según el comportamiento conocido de la organización.

Tanto las geocercas seguras como las de riesgo tienen sus propios indicadores de riesgo personalizados preconfigurados.

Para obtener más información, consulte Habilitar las geocercas.

#### Problemas resueltos

- API de Citrix Cloud para mostrar el **nombre del cliente** en el cuerpo del correo electrónico. Ahora, el correo electrónico usa el apodo para mostrar el **nombre del cliente** en el cuerpo del correo electrónico enviado a los administradores. [CAS-65350]
- La tarjeta de origen de datos de Citrix Gateway es común entre **Citrix Analytics para seguridad** y **Citrix Analytics para el rendimiento**. El procesamiento de datos invocaba constantemente el dispositivo de punto final de Citrix Analytics para seguridad y se interrumpió para los clientes que solo tenían derechos de **Citrix Analytics para el rendimiento**. [CAS-70817]
- Cuando se recibe más de un mensaje de autorización simultáneamente de Citrix Cloud, se produce una condición de carrera al actualizar la caché de Redis. En tal caso, se actualiza un mensaje de autorización en la memoria caché y el resto desaparece. Ahora se ha solucionado este problema para actualizar todos los mensajes de derechos de la caché. [CAS-70823]

### 13 de septiembre de 2022

#### Mejora del panel de control de Sharelink

El panel de control de Sharelink se ha renovado con una vista resumida y detallada. La vista de resumen consiste en las acciones más activas y las acciones con mayor riesgo. La vista detallada proporciona más información al administrador con la introducción de los atributos creados por, el recuento de actividades, el tipo de autenticación, el permiso, el tipo de recurso compartido y el contenido. El administrador puede profundizar y filtrar aún más según sea necesario y cambiar/proporcionar el marco de tiempo para ver los datos de interés.

Para obtener más información, consulte Panel de control Compartir vínculos.

### 9 de septiembre de 2022

#### Mejora de RI para trayectos imposibles

Los indicadores de riesgo de trayecto imposible se han mejorado para indicar la organización que registra y el tipo de ruta de las direcciones IP de los clientes. Estos nuevos campos están disponibles tanto en las vistas detalladas de los indicadores de la cronología del usuario como en los detalles de los indicadores enviados al SIEM.

Para obtener más información sobre las directivas predeterminadas, consulte los siguientes artículos:

- Evaluación continua de riesgos.
- Directivas y acciones

## 19 de agosto de 2022

### Habilitar telemetría de impresión de VDA

Un evento denominado VDA.Print se activa cuando se inicia un trabajo de impresión en Citrix Apps and Desktops. Los eventos de impresión del VDA también están disponibles en las páginas **Búsqueda de autoservicio** e **Indicadores de riesgo personalizados**.

- **Búsqueda de autoservicio**: Puede ver los resultados de VDA.Print junto con todos los detalles de sus atributos.
- **Indicadores de riesgo personalizados**: Se proporcionan nuevos eventos para la telemetría de impresión del VDA a través de EventHub y también están disponibles en Indicador personalizado. Puede usar estos pares clave/valor de eventos para configurar desencadenantes de indicadores personalizados.

Para habilitar la telemetría de impresión y la transmisión de registros de impresión a Citrix Analytics for Security, debe crear claves de registro y configurar el VDA. Estos registros de impresión proporcionan información vital sobre las actividades de impresión, como los nombres de las impresoras, los nombres de los archivos de impresión y el total de copias impresas. Como administrador de seguridad, puede usar estos registros para analizar el riesgo e investigar a sus usuarios.

Para obtener más información, consulte Habilitar la telemetría de impresión para Citrix DaaS.

## 18 de agosto de 2022

### Problema resuelto

- En la búsqueda de autoservicio de aplicaciones y escritorios y en la página Inicio de sesión de usuarios del panel de control de ubicación de la garantía de acceso, el valor de la versión de la aplicación Workspace se rellenó como **NA** (no disponible) en el archivo CSV descargado, mientras estaba disponible en la vista de páginas. Este problema ya se ha solucionado. [CAS-70361]

## 17 de agosto de 2022

### Personalización del correo electrónico del usuario final según la directiva

Ahora puede personalizar el contenido del correo electrónico enviado a los usuarios finales según la directiva. Específicamente, cuando se crea una directiva con la acción Solicitar respuesta del usuario final o una acción disruptiva en la cuenta del usuario (como Cerrar sesión del usuario y Bloquear usuario), el contenido del correo electrónico que se envía a los usuarios finales cuando se aplica la directiva se puede personalizar.

Para obtener más información sobre cómo personalizar el correo del usuario final por directiva, consulte Directivas y acciones.

## 11 de agosto de 2022

Se han agregado nuevas preguntas sobre la **garantía de acceso: geolocalización** en el artículo **Preguntas frecuentes**. Para obtener más información, consulte las preguntas frecuentes.

### Problema resuelto

- El botón **Ver todas las notificaciones** redirigía al administrador al enlace `https://citrix.cloud.com/notifications` del correo electrónico semanal que tenía un error tipográfico. [CAS-69236]

## 17 de junio de 2022

### El procesamiento de datos está habilitado de forma predeterminada para los nuevos derechos de pago

Anteriormente, los clientes con un nuevo derecho de pago a Citrix Analytics for Security tenían que activar el procesamiento de datos en la tarjeta de sitio de orígenes de datos específicas para comenzar a procesar los datos de esos orígenes de datos.

Con esta versión, cuando se aprovisiona el nuevo derecho de pago a Citrix Analytics for Security, el procesamiento de datos se activa de forma predeterminada para los siguientes servicios de Citrix Cloud:

- Citrix Secure Private Access
- Citrix Content Collaboration
- Citrix DaaS

Para obtener más información, consulte Introducción.

## 9 de junio de 2022

### Problema resuelto

- Los indicadores de riesgo de Microsoft Graph generados por la protección de identidad de Azure AD y Microsoft Defender for Endpoint pueden mostrarse varias veces en Security Analytics. Este problema ya se ha solucionado. [CAS-66593,CAS-66731]

## 2 de junio de 2022

### Problemas resueltos

- En la búsqueda de autoservicio de directivas, al seleccionar la dimensión **Nombre de directiva** en la consulta de búsqueda para filtrar eventos, se sugirió una lista de directivas no válidas junto con las directivas válidas para Security Analytics. [CAS-66838]
- El tamaño del archivo de descarga de los eventos **File.Download** de Windows Citrix Receiver no se mostraba correctamente en la búsqueda de autoservicio. Este problema surgió porque el valor real estaba en KB y la interfaz de usuario trataba el valor como bytes, lo que provocaba que se mostraran valores incorrectos a los usuarios. [CAS-67105]

## 24 de mayo de 2022

### Presentación de los indicadores de riesgo de trayecto imposibles para Content Collaboration, Citrix DaaS y Citrix Virtual Apps and Desktops, y orígenes de datos

Si el usuario inicia sesión desde dos ubicaciones que están demasiado separadas para viajar dentro del tiempo transcurrido, Citrix Analytics detecta esta actividad como un caso de trayecto imposible y activa el indicador de riesgo de **trayecto imposible**. Para obtener más información sobre los indicadores de riesgo de trayecto imposible, consulte los siguientes artículos:

- Indicadores de riesgo de Citrix Content Collaboration
- Indicadores de riesgo Citrix Gateway
- Indicadores de riesgo de Citrix Virtual Apps and Desktops y Citrix DaaS

## 17 de mayo de 2022

### El nombre de Virtual Apps and Desktops pasa a llamarse Aplicaciones y escritorios

En los paneles e informes de Security Analytics y en los datos enviados por Security Analytics a su servicio SIEM, todas las etiquetas de Virtual Apps and Desktops ahora se actualizan como aplicaciones y escritorios para alinearlas con el nombre del producto cambiado de marca.

Por ejemplo, en la página Orígenes de datos, las etiquetas Virtual Apps and Desktops pasan a llamarse Aplicaciones y escritorios.

La etiqueta Aplicaciones y escritorios representa tanto Citrix Virtual Apps and Desktops local como Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service) de su organización.

#### Problemas resueltos

Citrix Analytics no descubre automáticamente los sitios de Citrix DaaS Cloud Monitor o Director que están asociados a su cuenta de Citrix Cloud. [CAS-66801]

### 5 de abril de 2022

#### Novedades

#### Se cambia el nombre de Secure Workspace Access a Secure Private Access

En los paneles e informes de Analytics, todas las etiquetas de **Secure Workspace Access** ahora se actualizan como **Secure Private Access** para alinearse con el nombre del producto con el que se ha cambiado la marca.

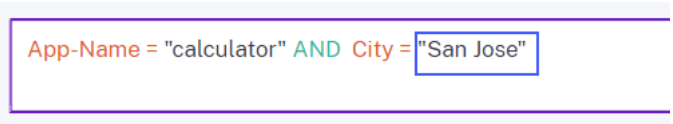
Por ejemplo, en la página **Orígenes de datos** y en la **página de búsqueda de autoservicio**, las etiquetas **Secure Workspace Access** se renombran como **Acceso privado seguro**.

### 21 de marzo de 2022

#### Problema resuelto

- En la página **Crear indicador de riesgo**, las sugerencias automáticas para dimensiones y operadores no funcionan si la condición anterior de la consulta de búsqueda contiene un valor de dimensión que está separado por un espacio.

  Por ejemplo, en la siguiente consulta, las sugerencias automáticas dejan de funcionar después de seleccionar la ciudad como `San Jose`. Este problema ya se ha solucionado. [CAS-64126]

### 10 de marzo de 2022

#### Novedades

#### Mejoras en el correo electrónico del administrador

- La notificación por correo electrónico para la acción **Notificar a los administradores** ahora proporciona los detalles de los múltiples indicadores de riesgo asociados con una directiva desencadenada.

- Puede ver el nombre, el nivel de gravedad y la fecha de activación de cada indicador de riesgo asociado a la directiva.
- Haga clic en **Ver detalles del riesgo** para abrir la página de línea de tiempo del usuario en Citrix Analytics y ver el indicador de riesgo más reciente que desencadenó la directiva. En la página de cronograma del usuario, también puede ver todos los indicadores de riesgo activados para el usuario.

citrix | Analytics

# Multiple risk indicators have been detected

Citrix Analytics has detected 4 risk indicators.

We have detected multiple risk indicators in your organization.

| | | |
|---|---|---|
| 1 | Risk indicator: | First time access from new device |
| | Severity: | MEDIUM |
| | Detected on: | 19 Jul, 2021 03:30 PDT (UTC-10:30) |
| 2 | Risk indicator: | Suspicious logon |
| | Severity: | MEDIUM |
| | Detected on: | 19 Jul, 2021 03:30 PDT (UTC-10:30) |
| 3 | Risk indicator: | Potential Data Exfiltration |
| | Severity: | MEDIUM |
| | Detected on: | 19 Jul, 2021 03:30 PDT (UTC-10:30) |
| | User: | wgerrish@smarttools.clm |
| | Customer name: | US-Production-Analytics |
| | Organization ID: | inte9ad836d |

View Risk Details

Para obtener más información sobre la acción **Notificar a los administradores**, consulte Directivas y acciones.

### Problema resuelto

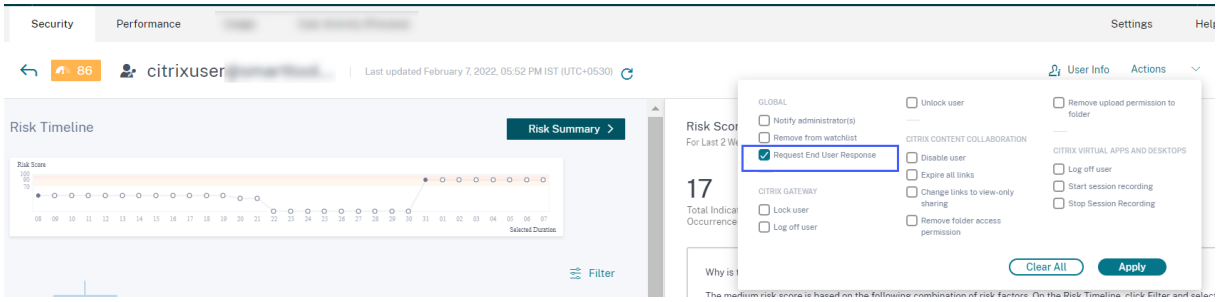
Citrix Analytics no recibe eventos de usuario del origen de datos de Secure Workspace Access. Por lo tanto, no verá los eventos del usuario en la página de búsqueda de autoservicio correspondiente. Además, no puede crear indicadores de riesgo personalizados para el origen de datos Secure Workspace Access. [CAS-64619]

## 3 de marzo de 2022

### Novedades

**Aplicar la respuesta del usuario final de solicitud manualmente** Anteriormente, solo podía aplicar la acción **Solicitar respuesta del usuario final** en una cuenta de usuario mediante la creación de una directiva.
Con esta versión, puede seleccionar la acción de la lista **Acciones** en la línea de tiempo del usuario y aplicar esta acción manualmente en un indicador de riesgo.

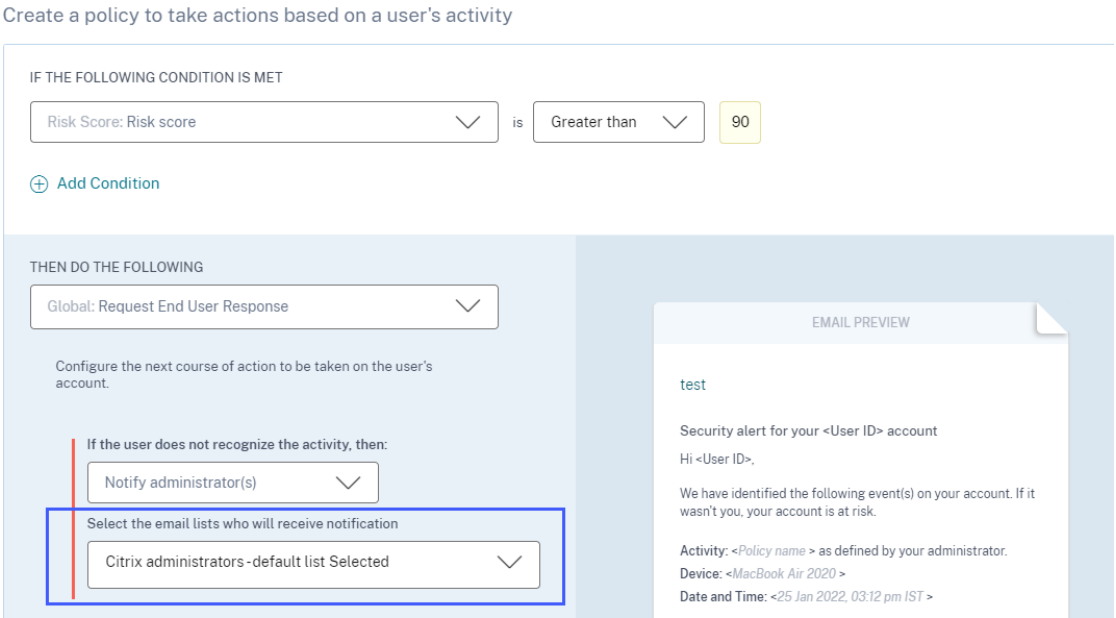
Para obtener más información sobre la acción y cómo aplicar acciones manualmente, consulte Directivas y acciones.



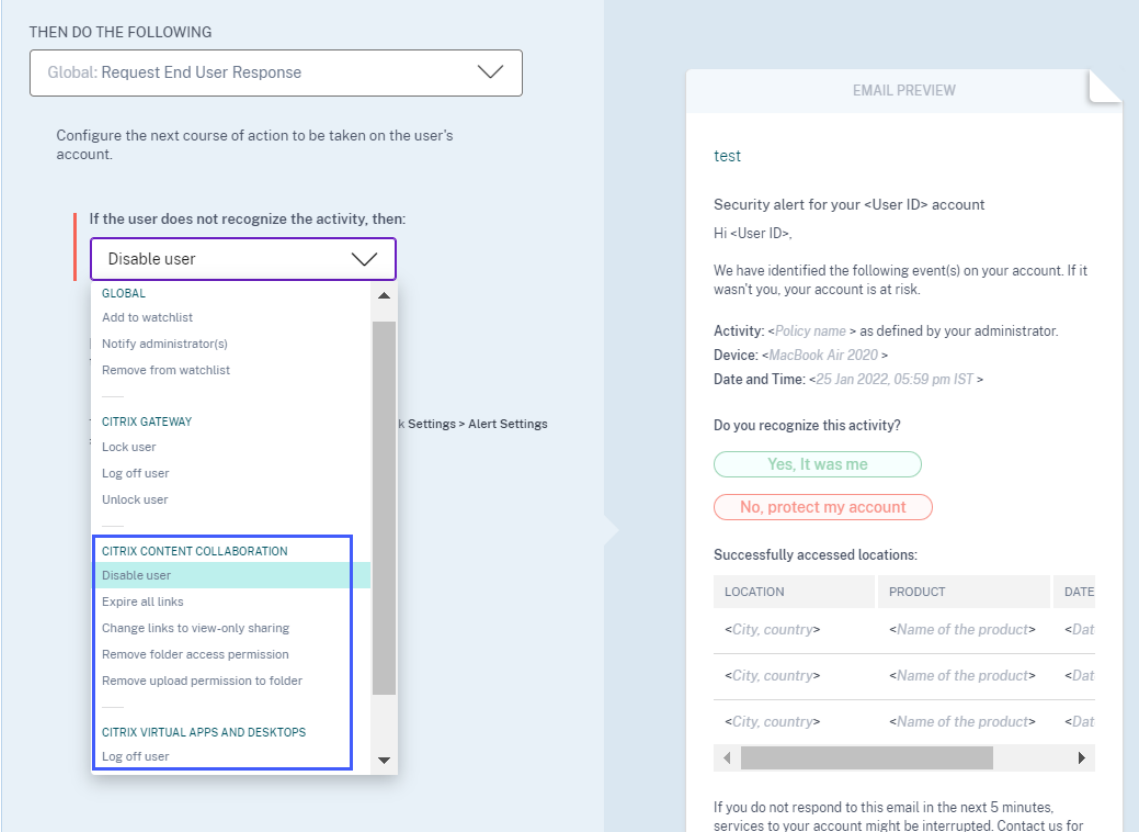

**Solicitar mejoras en la respuesta del usuario final para la directiva** Al crear una directiva con la acción **Solicitar respuesta del usuario final**, verá las siguientes mejoras:

- Después de seleccionar **Notificar a los administradores** como la siguiente acción, ahora puede ver las listas de distribución de correo electrónico predeterminadas y creadas entre las que puede elegir.




- Ahora puede seleccionar una de las acciones de Citrix Content Collaboration o Citrix Virtual Apps and Desktops y Citrix DaaS como acción siguiente. Anteriormente, solo podía seleccionar una de las acciones globales o las acciones de Citrix Gateway.




Para obtener más información sobre la acción, consulte Directivas y acciones.

## 23 de febrero de 2022

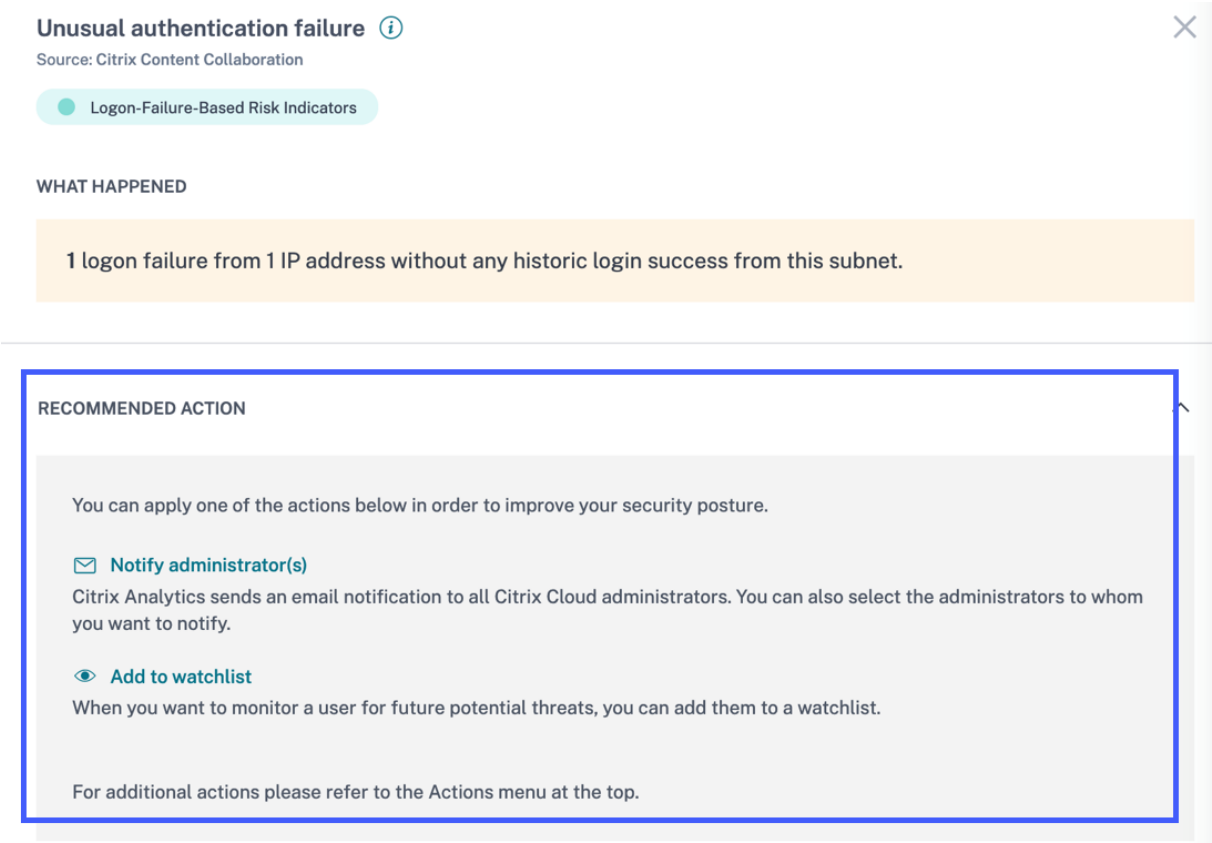
### Novedades

**Medidas recomendadas para un indicador de riesgo** Citrix Analytics le sugiere aplicar acciones como **Notificar a los administradores**, **Agregar a la lista de seguimiento**y **Crear una directiva** cuando se desencadenen los siguientes indicadores de riesgo para un usuario:

- Error de autenticación inusual (origen de datos de Content Collaboration)
- Fallo de autenticación inusual (origen de datos de gateway)
- Inicio de sesión sospechoso (origen de datos de Citrix Virtual Apps and Desktops y Citrix DaaS)

Cuando vaya a la línea de tiempo del usuario y seleccione el indicador de riesgo, puede ver todas las acciones sugeridas en la sección **ACCIÓN RECOMENDADA**.

Por ejemplo, en el indicador de riesgo de error de autenticación inusual, puede ver las siguientes acciones recomendadas:




Esta función proporciona orientación para elegir una acción que puede tomar en función de la gravedad del riesgo que presente el usuario. Sin embargo, también puede tomar una acción apropiada que esté fuera de la lista recomendada y en función de su análisis de riesgos.

**Problema resuelto**

- Si su organización se incorpora a Citrix Cloud en la región de origen de **Asia Pacífico Sur**, es posible que Citrix Analytics no reciba eventos de usuario del origen de datos de autenticación. Por lo tanto, es posible que no consulte los eventos de usuario en la página de búsqueda de autoservicio correspondiente. Este problema se ha solucionado. [CAS-62300]

## 17 de febrero de 2022

**Novedades**

**Recopilación de datos e informes mejorados para el origen de datos de Citrix Virtual Apps and Desktops y Citrix DaaS** En esta versión, verá los siguientes cambios:

- Mejoras en la recopilación de datos, la correlación y los informes de eventos de los clientes de la aplicación Citrix Workspace y el servicio Citrix Monitor.
- Mejoras en la calidad de los eventos recibidos de los usuarios y las versiones de los clientes, que se pueden utilizar para la búsqueda de autoservicio, los indicadores de riesgo personalizados y la detección general de riesgos.

**Compatibilidad con plantillas contextuales para los eventos de sesión y los eventos de aplicaciones en Content Collaboration** En la página de búsqueda de autoservicio, ahora puede ver los detalles de solo los campos relevantes asociados con el archivo, la carpeta, la sesión, el recurso compartido y los eventos del usuario. Se eliminan los campos no aplicables a los eventos.

Por ejemplo, puede ver los siguientes detalles de los eventos de `File.Copy`:

- ID de archivo
- ID de copia de archivo
- Ruta de archivo
- Ruta del archivo de destino
- ID de transmisión
- ID. de zona

Estos detalles lo ayudan durante la investigación y el análisis de riesgos de una cuenta de usuario asociada con un comportamiento de riesgo. Puede profundizar en los atributos específicos de un evento que parezca con riesgos.

Para obtener más información sobre los campos, consulte Búsqueda de autoservicio de Content Collaboration.

## 10 de febrero de 2022

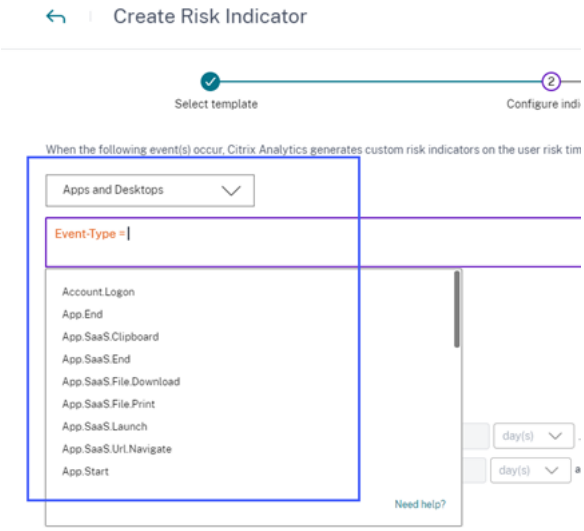
### Novedades

**Valores sugeridos automáticamente para las dimensiones en el indicador de riesgo personalizado** En la página del indicador de riesgo personalizado, cuando selecciona una dimensión y un operador válido en la barra de condiciones, los valores de la dimensión se muestran automáticamente. Seleccione un valor de la lista de sugerencias automáticas o introduzca un valor manualmente en función de sus casos de uso. Cuando escribe un valor, los valores coincidentes disponibles en los registros se sugieren automáticamente.

La lista de valores sugeridos para una dimensión está predefinida (valores conocidos) en la base de datos o se basa en eventos históricos.

Por ejemplo, cuando selecciona la dimensión `Event-Type` y el operador de asignación, los valores conocidos se sugieren automáticamente. Puede seleccionar un valor en función de sus requisitos.

Para obtener más información, consulte Indicadores de riesgo personalizados.




## 9 de febrero de 2022

### Novedades

**Nuevas funciones personalizadas para los administradores** Como administrador de Citrix Cloud con permiso de acceso completo, puede invitar a otros administradores a administrar Security Analytics en su organización. Ahora puede asignar las siguientes funciones personalizadas a los administradores invitados:

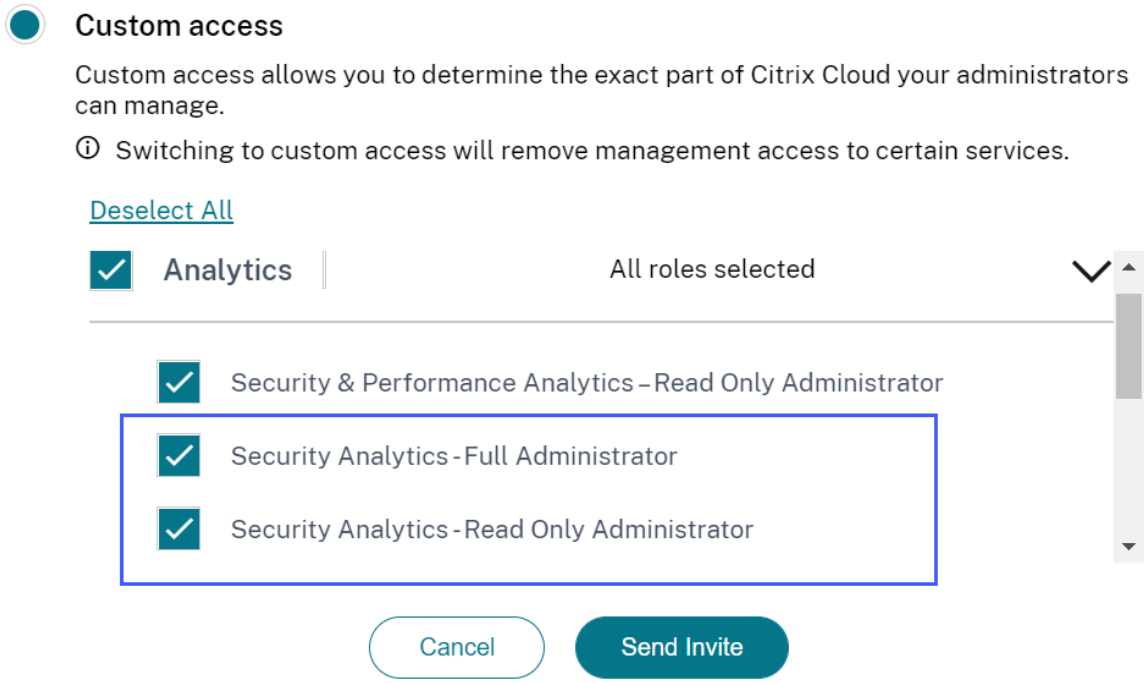
- Análisis de seguridad: administrador total

- Análisis de seguridad: administrador de solo lectura

Con el rol personalizado, puede proporcionar permisos de solo lectura o de acceso completo a sus administradores y permitirles administrar las diversas funciones de Security Analytics.

Para obtener más información sobre los permisos de acceso para estas funciones personalizadas, consulte Administrar funciones de administrador para Security Analytics.




**Soporte para notificaciones por correo electrónico para administradores de acceso personalizados** Si es administrador de Citrix Cloud con permisos de acceso personalizados (solo lectura o acceso completo) para administrar Security Analytics, ahora recibe las siguientes notificaciones:

- Notificaciones semanales sobre los riesgos de seguridad detectados en su organización. Para obtener más información, consulte Notificación por correo electrónico semanal.
- Notificaciones sobre los indicadores de riesgo cuando la acción **Notificar a los administradores** se aplica manualmente o se desencadena por una directiva. Para obtener más información, consulte Directivas y acción.

## 28 de enero de 2022

### Novedades

**Presentación de indicadores de riesgo de inicio de sesión sospechosos para orígenes de datos de Content Collaboration** Citrix Analytics for Security detecta ahora los inicios de sesión de usuario

sospechosos en función de varios factores contextuales, tales como:

- La ubicación se considera inusual con respecto al usuario y al historial de la organización
- El dispositivo se considera inusual con respecto al usuario y al historial de la organización
- La red se considera inusual con respecto al usuario y al historial de la organización.
- La dirección IP se considera sospechosa en función de las fuentes de inteligencia de amenazas IP

Cuando un usuario inicia sesión desde un contexto sospechoso en función de la combinación de estos factores, se activa el indicador de riesgo.

Este indicador de riesgo reemplaza el indicador de riesgo de acceso desde una ubicación inusual asociado a los orígenes de datos de Citrix Content Collaboration y Citrix Gateway. Todas las directivas existentes basadas en el indicador de riesgo de acceso desde una ubicación inusual se vinculan automáticamente al nuevo indicador de riesgo: inicio de sesión sospechoso.

Para obtener más información sobre los indicadores de riesgo, consulte Suspicious Logon- Content Collaboration y Suspicious logon- Gateway.

Para obtener más información sobre el esquema de los indicadores de riesgo, consulte Formato de datos de Citrix Analytics para SIEM.

## 20 de enero de 2022

### Novedades

**Integración de Microsoft Azure Active Directory** Ahora puede conectar su Azure Active Directory con Citrix Analytics for Security para:

- Importe los detalles de los usuarios y los grupos de usuarios del dominio de su organización a Citrix Analytics for Security.
- Enriquezca los perfiles de usuario con detalles adicionales, como el cargo, la organización, la ubicación de la oficina, el correo electrónico y los detalles de contacto, que lo ayudarán durante la investigación y el análisis de riesgos.

Para obtener más información, consulte Integración de Azure Active Directory.

## 18 de enero de 2022

### Novedades

**Soporte para las acciones de enlace compartido en todos los indicadores de riesgo de Content Collaboration** Anteriormente, puede aplicar las acciones de enlace compartido: **caducar todos los**

**enlaces** y **Cambiar enlace para compartir de solo lectura** en los siguientes indicadores de riesgo basados en enlaces compartidos asociados con el servicio Content Collaboration:

- Descarga de enlace compartido confidencial anónimo
- Descargas excesivas de enlaces compartidos
- Uso compartido excesivo de archivos

Con esta versión, ahora puede aplicar las acciones de enlace compartido en los siguientes indicadores de riesgo basados en el usuario asociados con el servicio de Content Collaboration:

- Acceso desde una ubicación inusual
- Acceso excesivo a archivos confidenciales
- Subidas excesivas de archivos
- Descargas excesivas de archivos
- Eliminación excesiva de archivos o carpetas
- Archivos de malware detectados
- Actividad de ransomware sospechosa
- Fallas de autenticación inusuales

También puede aplicar las acciones de enlace compartido en los indicadores de riesgo personalizados asociados con el servicio de Content Collaboration.

Para obtener más información sobre las acciones y los indicadores de riesgo, consulte los siguientes artículos:

- Directivas y acciones
- Indicadores de riesgo de Content Collaboration
- Indicadores de riesgo personalizados

**La integración con SIEM ya está disponible de forma general** Puede integrar Citrix Analytics for Security con sus servicios de administración de eventos e información de seguridad (SIEM) y exportar los datos de los usuarios desde el entorno de TI de Citrix a su SIEM. La integración le ayuda a correlacionar los datos recopilados de varias fuentes y a obtener una visión integral de la seguridad de su organización.

Actualmente, puede integrar Citrix Analytics for Security con los siguientes servicios:

- Splunk
- Microsoft Sentinel

- Elasticsearch
- Otros servicios SIEM mediante el uso de un conector de datos basado en Kafka o Logstash

Para obtener más información, consulte Integración de la información de seguridad y la gestión de eventos (SIEM).

## 23 de diciembre de 2021

### Novedades

**Mejoras en los indicadores de riesgo de enlaces** Se han realizado las siguientes mejoras:

- Ahora puede crear una directiva con el indicador de riesgo de **descarga de enlace compartido confidencial anónimo**.
- El indicador de riesgo de **descarga de acciones confidenciales anónimascambia su nombre a Descarga de enlace compartido confidencial anónimo** para distinguirlo como un indicador de riesgo de enlace compartido.
- El indicador de riesgo de **descargas excesivas** se renombra como **Descargas excesivas de enlaces compartidos** para distinguirlo como un indicador de riesgo de enlace compartido y diferenciarlo del indicador de riesgo de **descargas excesivas de archivos** basado en el usuario.

Para obtener más información, consulte Indicadores de riesgo de vínculos compartidos de Citrix.

## 21 de diciembre de 2021

### Novedades

**Envíe notificaciones sobre los indicadores de riesgo a los administradores que no sean de Citrix Cloud** Ahora puede notificar a los administradores de su organización que no son de Citrix Cloud con la acción **Notificar a los administradores**.

Para notificar a estos administradores, cree una lista de distribución de correo electrónico. Seleccione los administradores en la lista de distribución de correo electrónico de los dominios externos que están conectados a Citrix Cloud o mediante sus direcciones de correo electrónico directamente. Al aplicar la acción **Notificar a los administradores**, seleccione la lista de distribución de correo electrónico que contiene a los administradores que no son de Citrix Cloud.

Para obtener más información, consulte Lista de distribución de correo electrónico.

## 20 de diciembre de 2021

### Novedades

**Enviar notificaciones de respuesta del usuario a los usuarios de Content Collaboration** Además de los usuarios de Active Directory, ahora puede aplicar la acción **Solicitar respuesta del usuario final** a los usuarios de Content Collaboration.

Esta acción envía notificaciones por correo electrónico a los usuarios cuando Citrix Analytics detecta cualquier actividad inusual en sus cuentas de Citrix. Para obtener más información sobre la acción **Solicitar respuesta del usuario final**, consulte Directivas y acciones.

**El nombre de Control de acceso cambia a Secure Workspace Access** En los paneles e informes de **Security** Analytics, todas las etiquetas de **control de acceso** ahora se actualizan como **Secure Workspace Access** para alinearse con el nombre del producto con el que se ha cambiado la marca.

Por ejemplo, en la página **Orígenes de datos**, la página de **búsqueda de autoservicio** y la página **Directivas**, las etiquetas de Control de acceso se renombran como Secure Workspace Access.

### Problema resuelto

- Para el origen de datos de Apps and Desktops, cuando descarga el informe de búsqueda como archivo CSV, algunos valores de campo del archivo CSV se muestran como no disponibles (N/A), aunque sus valores sí están disponibles. Por ejemplo, los valores de los campos como `Download File Name`, `Session Launch Type` y `Workspace App Version` se muestran en la página de **búsqueda de autoservicio**, pero en el archivo CSV descargado, ve estos valores como no disponibles (N/A). Este problema ya se ha solucionado. [CAS-62299]

## 9 de diciembre de 2021

### Novedades

**Crear sus indicadores de riesgo personalizados fácilmente con plantillas** Ahora puede seleccionar una plantilla en función de su caso de uso y crear un indicador de riesgo personalizado. Las plantillas lo guían al proporcionarle consultas y parámetros predefinidos. Facilita su esfuerzo a la vez que crea un indicador de riesgo personalizado.

Para obtener más información, consulte Indicadores de riesgo personalizados.

## 7 de diciembre de 2021

### Problema resuelto

- En Citrix Analytics for Security, no recibe los eventos de los usuarios que utilizan Citrix Secure Browser que se publicó en septiembre de 2021. El problema existe porque la directiva de **seguimiento de nombres de host** no está visible en Citrix Secure Browser posterior a la versión de septiembre de 2021 y, por lo tanto, no se puede habilitar para integrarse con Citrix Analytics for Security. Este problema ya se ha solucionado. [CAS-62254]

## 2 de diciembre de 2021

### Novedades

**Indicador de riesgo detectado por archivos de malware** Ahora puede recibir una alerta cuando un usuario cargue un archivo infectado en Content Collaboration.

El indicador de riesgo detecta un archivo infectado por un malware como un troyano, un virus o cualquier otra amenaza maliciosa. Proporciona visibilidad de los detalles del archivo malicioso, como el propietario del archivo, el nombre del virus y la ubicación del archivo.

El factor de riesgo asociado con el indicador de riesgo de **archivos de malware detectados** es el indicador de riesgo basado en archivos.

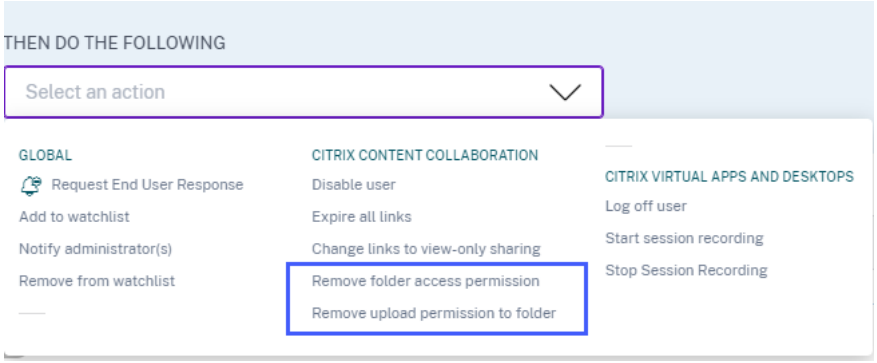
Para obtener más información sobre el indicador de riesgo y las acciones que puede aplicar, consulte el indicador de riesgo de archivos de malware detectados.

**Nuevas acciones para el origen de datos Content Collaboration** Puede aplicar las siguientes acciones cuando se activa el indicador de riesgo de **archivos de malware detectados** para un usuario:

- **Elimina el permiso de acceso a carpetas**. Puede bloquear el permiso de acceso del usuario que carga el archivo infectado. El usuario no puede acceder a la carpeta en la que se cargó el archivo infectado.
- **Elimina el permiso de carga en la carpeta**. Puede bloquear el permiso de carga del usuario que carga el archivo infectado. El usuario no puede cargar un archivo en la carpeta en la que se cargó el archivo infectado.

Para obtener más información sobre las acciones de Content Collaboration, consulte Directivas y acciones.



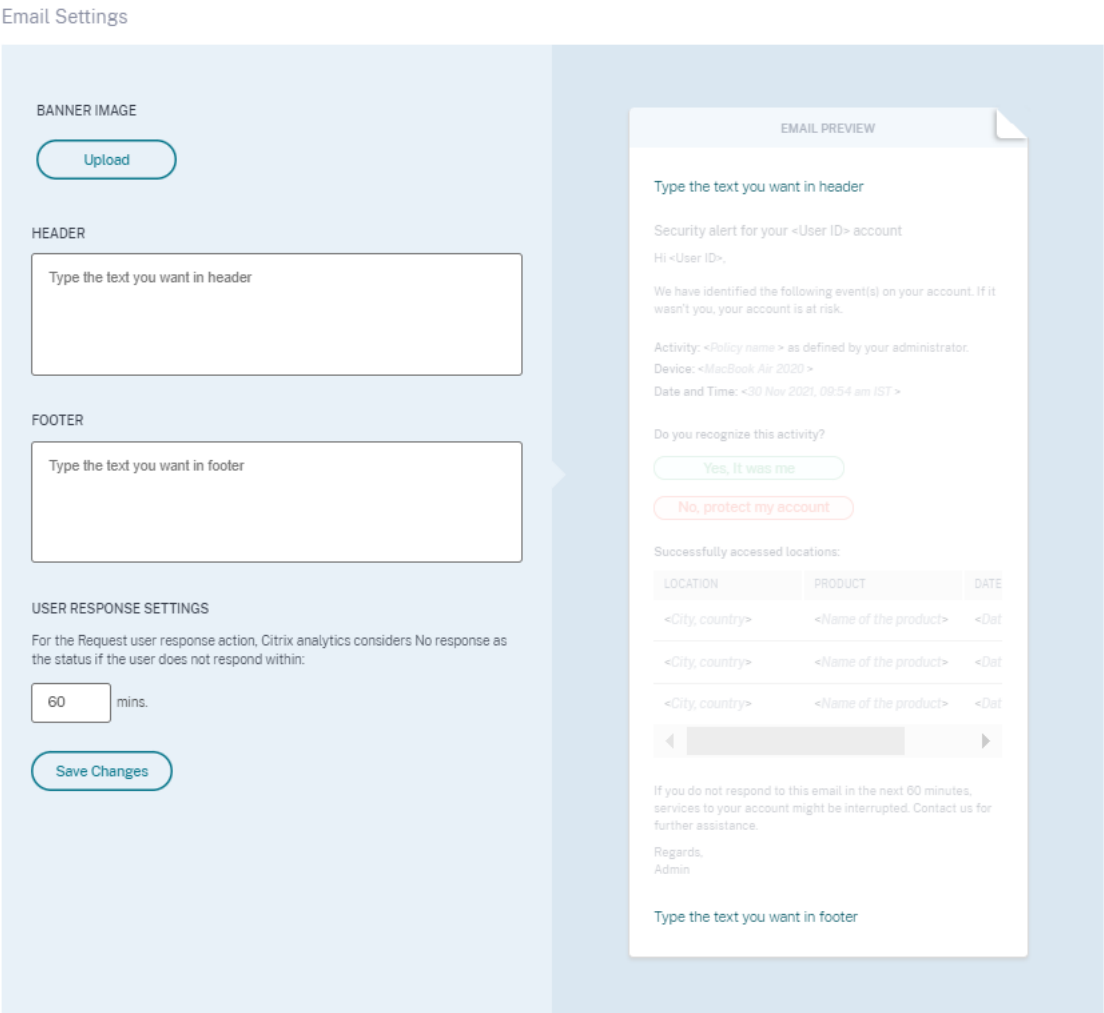

## 29 de noviembre de 2021

### Novedades

**Mejoras en la configuración del correo electrónico para las notificaciones a los usuarios** Como administrador, ahora puede agregar imagen de encabezado, texto de encabezado y pie de página en la plantilla de correo electrónico de respuesta del usuario. Estos campos mejoran la legitimidad de su correo electrónico, lo que aumenta la atención y las respuestas de los usuarios hacia su correo electrónico.

Para obtener más información, consulte Configuración del correo electrónico del usuario final.

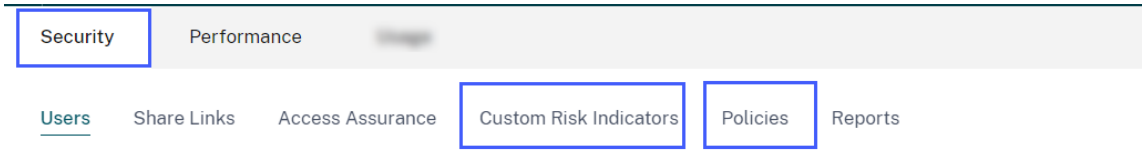



## 26 de noviembre de 2021

### Novedades

**Cambios en el menú de directivas e indicadores de riesgo** Se actualizan los enlaces de navegación de las siguientes funciones:

- Indicadores de riesgo personalizados: utilice esta función haciendo clic en **Seguridad > Indicadores de riesgo personalizados**.
- Directivas: utilice esta función haciendo clic en **Seguridad > Directivas**.



## 25 de noviembre de 2021

### Novedades

**Mejoras en la integración de la gestión de información y eventos de seguridad (SIEM)**

> **Nota**
>
> Esta integración está en versión preliminar.

Ahora puede integrar Citrix Analytics for Security con los siguientes servicios de SIEM:

- Microsoft Sentinel
- Elasticsearch con servicios de visualización como Kibana y servicio SIEM como LogRythm
- Cualquier otro servicio SIEM que utilice el motor de recopilación de datos Logstash

En función de sus necesidades empresariales, importe los datos de los usuarios de Citrix Analytics for Security a su servicio SIEM. Esta integración permite a sus equipos de operaciones de seguridad correlacionar, analizar y buscar datos de registros dispares dentro de los servicios de SIEM en su organización, lo que les ayuda a identificar y remediar rápidamente los riesgos de seguridad.

Para obtener más información, consulte Integración de la información de seguridad y la gestión de eventos (SIEM).

## 9 de noviembre de 2021

### Problema resuelto

- En algunos arrendatarios, las directivas de usuario no funcionan. Este problema se producía cuando las alertas de las aplicaciones virtuales tenían valores de cadena vacíos para los dominios. Este problema ya se ha solucionado. [CAS-60920]

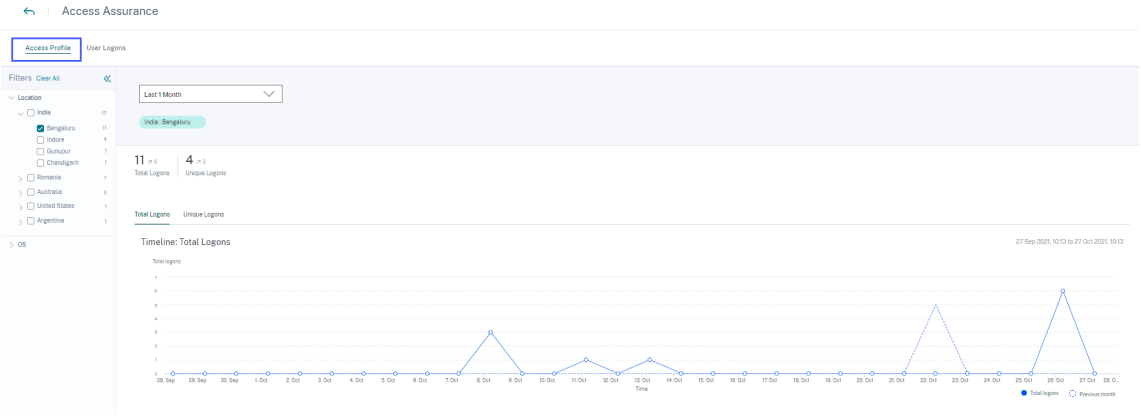
## 2 de noviembre de 2021

### Novedades

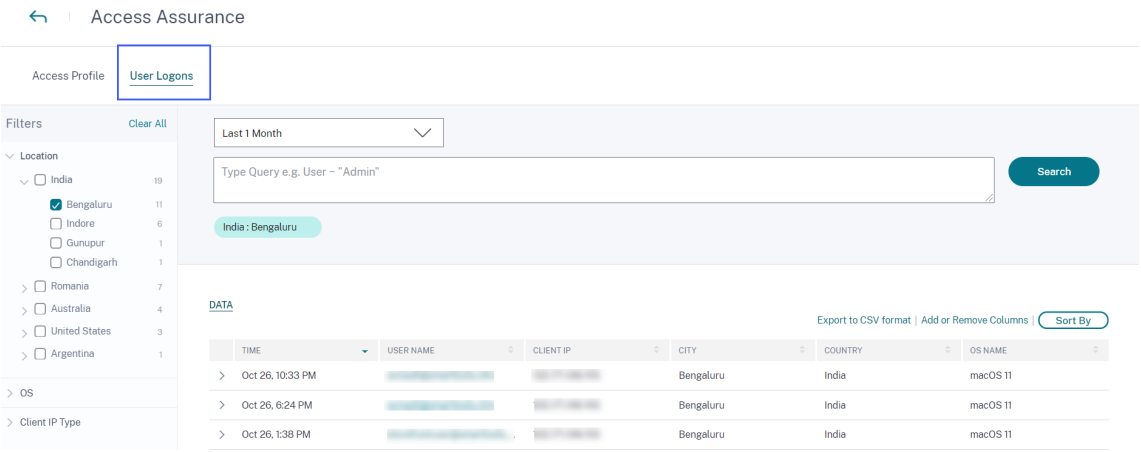
**Ver los perfiles de acceso y los detalles de inicio de sesión de los usuarios de Citrix Virtual Apps and Desktops y Citrix DaaS** En el panel **Ubicación de control de acceso**, puede ver los perfiles de acceso y los detalles de inicio de sesión de los usuarios que han iniciado sesión en aplicaciones virtuales y escritorios virtuales. Esta información le ayuda durante la investigación y el análisis de amenazas.

- La página **Perfil de acceso** proporciona el resumen de los accesos de los usuarios desde las ubicaciones seleccionadas. Puede ver el análisis de tendencias y los eventos de acceso superior del total de usuarios y los inicios de sesión de usuarios únicos.




- La página Inicios de **sesión de usuario** proporciona los detalles de los inicios de sesión de los usuarios en aplicaciones virtuales y escritorios virtuales desde las ubicaciones seleccionadas.



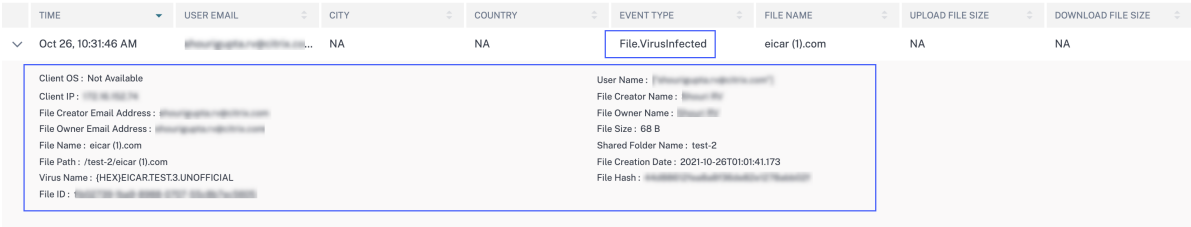

Para obtener más información, consulte el panel de control Ubicación de Access Assurance.

**Ver los registros de malware en la página de búsqueda de autoservicio de Content Collaboration**

En la página de autoservicio de Content Collaboration, ahora puede ver el evento de malware `File.VirusInfected` y sus registros asociados. Este evento se desencadena cuando un usuario de Content Collaboration carga un archivo que está infectado con un malware.

Para obtener más información, consulte Búsqueda de autoservicio de Content Collaboration




### Problema resuelto

- Algunos usuarios de Content Collaboration se configuran incorrectamente como no empleados al procesar los eventos en Citrix Analytics. Por lo tanto, los usuarios no se identifican como usuarios descubiertos. Este problema ya se ha solucionado. [CAS-59608]

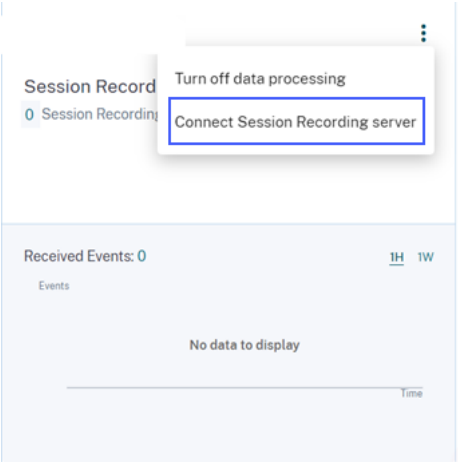
## 20 de octubre de 2021

### Novedades

**Integración del servidor de grabación de sesiones** Para su implementación de Citrix Virtual Apps and Desktops y Citrix DaaS, ahora puede configurar sus servidores de Grabación de sesiones para enviar los eventos de los usuarios a Citrix Analytics for Security. Estos eventos de los usuarios se procesan para proporcionar información útil sobre el comportamiento de los usuarios.

En la página **Orígenes de datos > Seguridad**, vaya a la tarjeta del sitio **Virtual Apps and Desktops**. En la tarjeta del sitio **Grabación de sesiones**, haga clic en puntos suspensivos verticales () y, a continuación, seleccione **Conectar servidor de grabación de sesiones**.

Para obtener más información, consulte Implementación de Conectarse a la grabación de sesiones.



## 19 de octubre de 2021

### Novedades

**Mejoras en la plantilla de correo electrónico de notificación al administrador** La notificación por correo electrónico que recibe un administrador después de aplicar la acción **Notificar a los administradores** se ha mejorado para proporcionar una mejor información sobre los eventos de riesgo del usuario.

- La notificación ahora proporciona información detallada sobre el indicador de riesgo desencadenado o la directiva aplicada. Por ejemplo, puede ver la gravedad y el tiempo de activación de los indicadores de riesgo predeterminados y personalizados. La estructura del contenido se ha mejorado para una mejor legibilidad.
- Los administradores ahora pueden acceder a la línea de tiempo del usuario directamente desde la notificación por correo electrónico y ver los detalles sobre los eventos de riesgo.
- Se agrega una opción de valoración en la notificación. Esta opción ayuda a recopilar las respuestas de los administradores y a mejorar continuamente el contenido de la notificación en función de las respuestas.

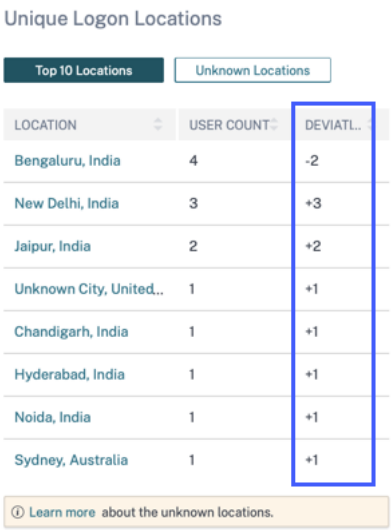
Para obtener más información sobre la acción **Notificar a los administradores**, consulte Directivas y acciones.

### Mejoras en el resumen de inicio de sesión del usuario

- Ahora puede ver la tendencia ascendente o descendente de los inicios de sesión de los usuarios para el total de inicios de sesión de usuarios en todo el mundo y los inicios de sesión de usuarios únicos en todo el mundo.


- La columna **DESVIACIÓN** de la tabla **Ubicaciones de inicio de sesión únicas** muestra el cambio hacia arriba o hacia abajo en los inicios de sesión de usuario únicos para una ubicación en particular.




Estas métricas le ayudan a entender cómo han cambiado los inicios de sesión de los usuarios (positivos o negativos) con respecto al período anterior. Proporciona visibilidad de las interacciones de los usuarios con sus implementaciones de Citrix Virtual Apps and Desktops y Citrix DaaS.

Para obtener más información, consulte Panel de control de ubicación de Access assurance.

### Problema resuelto

- En el panel de control **Ubicación de Access Assurance**, las tarjetas de **resumen de inicio de sesión de usuario** no muestran las métricas de inicio de sesión de los usuarios (total de inicios de sesión de usuarios en todo el mundo, inicios de sesión de usuario únicos en todo el mundo y los países tienen inicios de sesión de usuario) cuando ningún usuario inicia sesión desde fuera de las áreas de geocercas. Este problema ya se ha solucionado. [CAS-59595]

## 1 de octubre de 2021

### Novedades

**Ver los registros de auditoría en la búsqueda de autoservicio de Content Collaboration** En la búsqueda de autoservicio de Content Collaboration, ahora puede ver los registros de auditoría. Estos registros proporcionan información sobre los permisos y las acciones que los administradores de Content Collaboration aplican a las cuentas de usuario. Con estos datos, puede verificar si los administradores de Content Collaboration han tomado medidas válidas en sus cuentas de usuario. Como administrador de seguridad, le ayuda durante la investigación y el análisis de riesgos.

Para obtener más información sobre los registros de auditoría, consulte Búsqueda de autoservicio de Content Collaboration.

#### Problema resuelto

Los administradores que inician sesión en Citrix Cloud mediante Azure AD no pueden acceder al servicio Citrix Analytics cuando el identificador de sesión caducado anterior viene con el nuevo ID de sesión. Este problema ya se ha solucionado. [CAS-59385]

### 29 de septiembre de 2021

#### Novedades

**El panel de control de ubicación de garantía de acceso ahora está disponible de forma general**
El panel proporciona visibilidad de las ubicaciones de sus usuarios de Citrix Virtual Apps and Desktops y Citrix DaaS. Puede identificar a los usuarios cuyas ubicaciones son inusuales habilitando la geocerca y aplicando las acciones apropiadas para evitar cualquier amenaza.

Para ver el panel de control, haga clic en **Seguridad > Garantía de acceso**. Seleccione el período de tiempo para el que quiere ver los detalles de la ubicación.

Para obtener más información, consulte Panel de control de ubicación de Access assurance.

### 15 de septiembre de 2021

#### Novedades

**Mejoras en los indicadores de riesgo personalizados**

- Cuando se activa un indicador de riesgo personalizado, se muestra inmediatamente en la línea de tiempo del usuario. Sin embargo, el resumen de riesgos y la puntuación de riesgo del usuario se actualizan al cabo de unos minutos (aproximadamente 15-20 minutos).
- Si modifica los atributos como condición, categoría de riesgo, gravedad y nombre de un indicador de riesgo personalizado existente, en el cronograma del usuario, podrá ver las apariciones anteriores del indicador de riesgo personalizado (con los atributos antiguos) que se activaron para el usuario.
- Si elimina un indicador de riesgo personalizado, en el cronograma del usuario, podrá seguir viendo las apariciones anteriores del indicador de riesgo personalizado que se activaron para el usuario.

Para obtener más información, consulte Indicadores de riesgo personalizados.

## 14 de septiembre de 2021

### Novedades

**Introducción del indicador de riesgo de inicio de sesión sospechoso** Citrix Analytics for Security detecta ahora los inicios de sesión de usuario sospechosos en función de varios factores contextuales, tales como:

- La ubicación se considera inusual con respecto al usuario y al historial de la organización
- El dispositivo se considera inusual con respecto al usuario y al historial de la organización
- La red se considera inusual con respecto al usuario y al historial de la organización.
- La dirección IP se considera sospechosa en función de las fuentes de inteligencia de amenazas IP

Cuando un usuario de Citrix Virtual Apps and Desktops y Citrix DaaS inicia sesión desde un contexto sospechoso en función de la combinación de estos factores, se activa el indicador de riesgo.

Este indicador de riesgo reemplaza el indicador de riesgo **de acceso desde una ubicación inusual** asociado al origen de datos de Citrix Virtual Apps and Desktops. Todas las directivas existentes basadas en el indicador de riesgo **de acceso desde una ubicación inusual** se vinculan automáticamente al nuevo indicador de riesgo: inicio de **sesión sospechoso**.

Para obtener más información sobre el indicador de riesgo, consulte Indicadores de riesgo de Citrix Virtual Apps and Desktops y Citrix DaaS.

**Mejora de mensajes SIEM** Citrix Analytics for Security envía ahora los detalles del esquema del indicador de riesgo de inicio de **sesión sospechoso** al servicio SIEM. Puede ver el esquema del resumen del indicador y los detalles del evento del indicador de riesgo de inicio de **sesión sospechoso**. Para obtener más información, consulte Formato de datos de Citrix Analytics para SIEM.

### Problema resuelto

- Para la búsqueda de autoservicio de Apps and Desktops, falta el valor de la IP del cliente en el archivo CSV descargado. Este problema ya se ha solucionado. [CAS-58426]

## 19 de agosto de 2021

### Novedades

**Presentación de la aplicación Citrix Analytics para Splunk**

> **Nota**
>
> La aplicación se halla en Tech Preview.

La aplicación Citrix Analytics para Splunk le permite ver los datos recopilados de Citrix Analytics for Security en forma de paneles detallados en su Splunk. Los paneles proporcionan información sobre los eventos de riesgo de los usuarios. También puede correlacionar los datos de Citrix Analytics con los registros recopilados de otros orígenes de datos. La correlación le ayuda a encontrar relaciones entre los eventos y a tomar medidas oportunas para proteger su entorno de TI.

Para descargar la aplicación, vaya a Splunk base. Instala la aplicación en su buscador de Splunk.

Para obtener más información, consulte Aplicación Citrix Analytics para Splunk.

**Esquema indicador de riesgo personalizado para SIEM** En su servicio SIEM, ahora puede ver el esquema de los indicadores de riesgo personalizados creados para Citrix Virtual Apps and Desktops y Citrix DaaS. Estos datos le ayudan a obtener información sobre la postura de riesgo de seguridad de su organización.

Para obtener más información sobre el esquema de indicador de riesgo personalizado, consulte Formato de datos de Citrix Analytics para SIEM.

**Compatibilidad con Citrix Director como origen de datos** Ahora puede configurar sus sitios locales en Citrix Director para enviar eventos a Security Analytics. Estos eventos se utilizan para descubrir a los usuarios conectados a Security Analytics y determinar las versiones de la aplicación Workspace instaladas en los dispositivos de los usuarios.

De forma predeterminada, el procesamiento de datos está habilitado tras el descubrimiento de los sitios. En la tarjeta **Monitoring**, puede ver todos los sitios conectados.

Para obtener más información sobre cómo configurar sus sitios en Director, consulte Origen de datos de Citrix Virtual Apps and Desktops y Citrix DaaS.

**Compatibilidad con geocercas en el panel de control de ubicación de Access assurance** Ahora puede utilizar la **configuración de geocercas** del tablero de mandos para seleccionar y habilitar las áreas geocercadas. Tras habilitar la geocerca, el mapa muestra las áreas geocercadas (países) y el usuario inicia sesión desde el exterior y desde el interior de la geocerca. Esta función utiliza la **sesión de CVAD iniciada fuera del indicador de riesgo de geocerca** para supervisar los inicios de sesión de los usuarios.

Para obtener más información, consulte Panel de control de ubicación de Access assurance.

**Estado de la aplicación Workspace en la página Usuarios** En la página **Usuarios**, ahora puede ver el estado de los clientes de la aplicación Citrix Workspace admitidos por Citrix Analytics. La página muestra el siguiente estado:

- Compatible
- Compatible parcialmente
- No compatible
- No disponible
- Inactivo

El estado le ayuda a identificar cualquier versión de cliente no admitida utilizada por los usuarios y recomienda a los usuarios que actualicen sus clientes a una versión compatible. Una versión de cliente compatible envía los eventos de usuario a Citrix Analytics.

> **Nota**
>
> Para ver el estado de la aplicación Citrix Workspace, debe incluir el origen de datos de Citrix Director. De lo contrario, el estado de cada usuario de Citrix Virtual Apps and Desktops y Citrix DaaS se muestra como **Inactivo**.

Para obtener más información, consulte el panel Usuarios.

**Compatible con el operador IS EMPTY** Al crear un indicador de riesgo personalizado, ahora puede utilizar el operador **IS EMPTY** en su condición para comprobar si hay una dimensión nula o vacía.

> **Nota**
>
> El operador solo funciona para dimensiones de tipo cadena como Nombre de aplicación, Explorador y País.

Para obtener más información, consulte Indicadores de riesgo personalizados.

**Puntuación de riesgo mejorada** En la cronología del usuario, ahora puede ver el resumen de riesgos de un usuario. El resumen de riesgos proporciona información sobre los factores de riesgo asociados a los eventos de los usuarios. El factor de riesgo ayuda a identificar el tipo de anomalías en los eventos de usuario y también determina la puntuación de riesgo. Los factores de riesgo son los siguientes:

- Indicadores de riesgo basados en dispositivos
- Indicadores de riesgo basados en la ubicación
- Indicadores de riesgo basados en IP
- Indicadores de riesgo basados en fallos de inicio de sesión

- Indicadores de riesgo basados en datos
- Indicadores de riesgo basados en archivos
- Indicadores de riesgo personalizados
- Otros indicadores de riesgo

En la línea de tiempo del usuario, ahora puede aplicar el filtro para ver los eventos del usuario en función de los factores de riesgo.

Para obtener más información, consulte estos temas:

- Indicadores de riesgo de usuario de Citrix
- Cronología y perfil de riesgo del usuario

## 29 de julio de 2021

### Función obsoleta

**Acciones obsoletas asociadas a Citrix Endpoint Management** Las acciones siguientes se quitan del origen de datos de Citrix Endpoint Management. Ya no puede aplicar estas acciones en los indicadores de riesgo ni crear directivas con estas acciones.

- Bloquear dispositivo
- Notificar Endpoint Management
- Notificar al usuario
- Revocar dispositivo
- Borrar datos del dispositivo

En las directivas existentes, si estas acciones ya están en uso, se sustituyen automáticamente por la acción **Agregar a la lista de seguimiento**. Y puede supervisar a esos usuarios desde la lista de seguimiento.

## 14 de julio de 2021

### Novedades

**Compatible con el operador IS NOT EMPTY** Al crear un indicador de riesgo personalizado, ahora puede utilizar el operador **NO ESTÁ VACÍO** en su condición para comprobar si la dimensión no está vacía (ni en blanco).

> **Nota**
>
> El operador solo funciona para dimensiones de tipo cadena como Nombre de aplicación, Explorador y País.

Por ejemplo, la siguiente condición detecta sucesos de inicio de sesión de usuario de cualquier país en el que el valor del país no sea nulo. En otras palabras, se especifica el nombre del país.

```
Event-Type = "Session.logon" AND Country IS NOT EMPTY
```

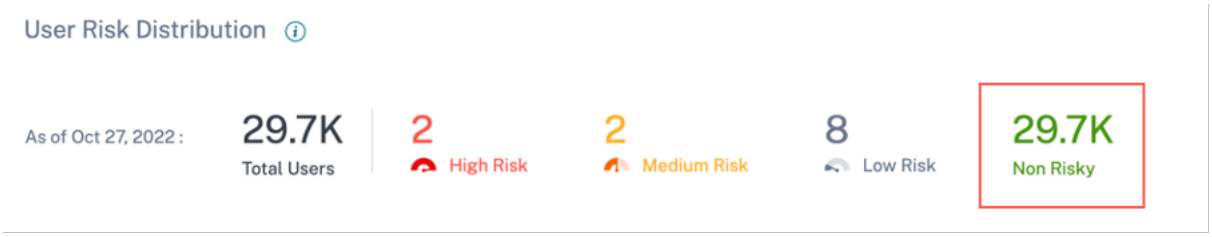
Para obtener más información, consulte Indicadores de riesgo personalizados.

## 6 de julio de 2021

### Novedades

**Ver usuarios no con riesgos en el panel Usuarios** En el panel **Usuarios**, ahora puede ver el número de usuarios sin riesgo durante el período de tiempo seleccionado. Estos usuarios descubiertos se identifican como no con riesgos en función de la puntuación de riesgo cero para el período seleccionado. Haga clic en la tarjeta **Usuarios sin riesgo** para ver todos los usuarios que tienen una puntuación de riesgo cero.

Para obtener más información, consulte Panel de control de usuarios.




## 1 de julio de 2021

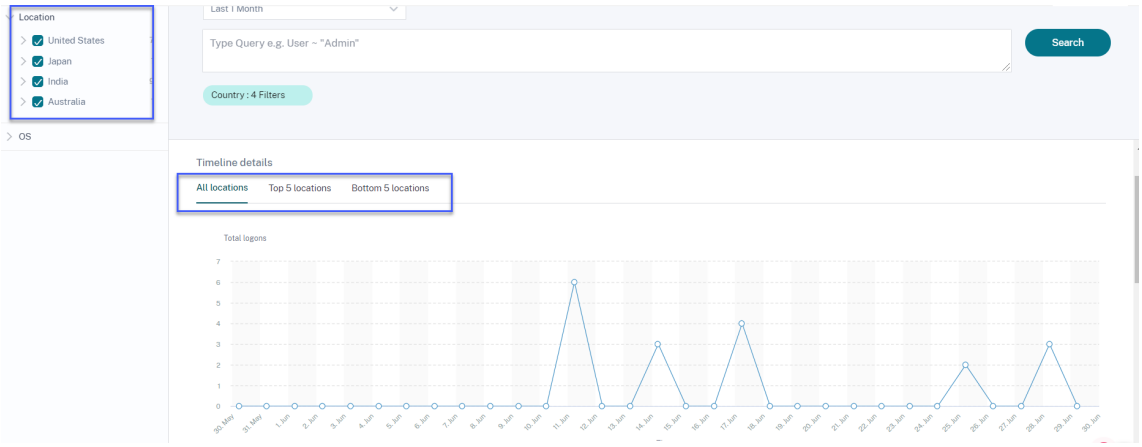
### Novedades

**Mejoras en el panel de control de ubicación de Access Assurance**

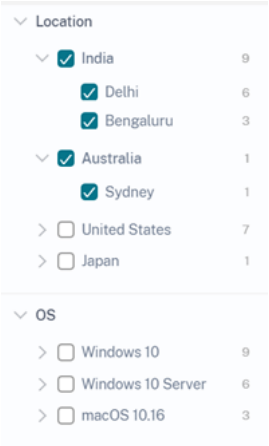
- En la tabla **Diez ubicaciones de inicio de sesión únicas principales**, puede ver el número de inicios de sesión de usuario únicos desde ubicaciones desconocidas. Esta lista es un subconjunto de las 10 ubicaciones de inicio de sesión únicas principales. También puede encontrar los motivos por los que se desconocen las ubicaciones y las posibles formas de obtener la ubicación de los usuarios.


- En la página **Ubicación de acceso**, si selecciona varias ubicaciones, puede ver y comparar los detalles del cronograma de los inicios de sesión de los usuarios de todas las ubicaciones, las cinco ubicaciones principales y las cinco ubicaciones inferiores.




- En la página **Ubicación de acceso**, puede utilizar las facetas anidadas como país y sus ciudades, sistemas operativos, versiones principales y secundarias. Estas facetas permiten filtrar los eventos de forma granular.

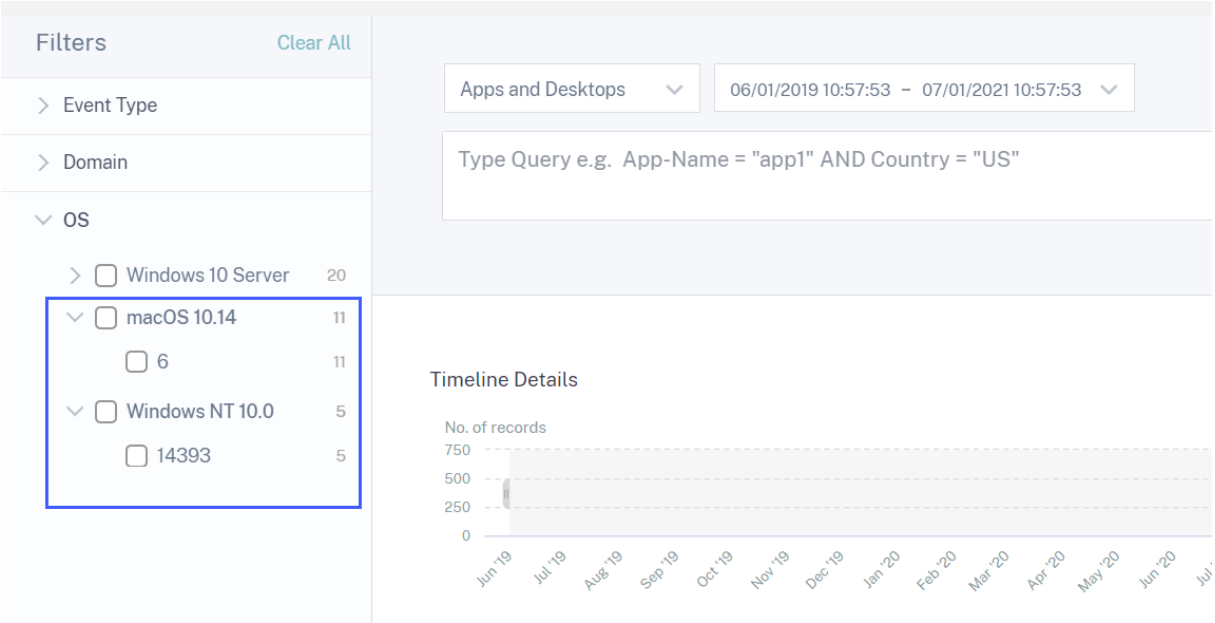



Para obtener más información, consulte Ubicación de Access Assurance.

**Actualización de la faceta del sistema operativo en la búsqueda de autoservicio de Virtual Apps and Desktops** Ahora puede filtrar los eventos de Apps and Desktops mediante la faceta

de SO anidada. Seleccione la versión principal y la versión secundaria asociadas a un sistema operativo y filtre los eventos de forma granular. Para obtener más información, consulte Búsqueda de autoservicio de aplicaciones y escritorios.




## 30 de junio de 2021

### Novedades

**Se agregó la versión de la aplicación Workspace en condición de indicador de riesgo personalizado para aplicaciones y escritorios** Para el origen de datos **Apps and Desktops**, ahora puede usar la dimensión **Workspace App-Version** para definir su condición y crear un indicador de riesgo personalizado. Para obtener más información sobre la dimensión, consulte Búsqueda de autoservicio de aplicaciones y escritorios.


## 23 de junio de 2021

### Novedades

**Mejoras en los mensajes SIEM** Los siguientes campos se agregan ahora al esquema de los indicadores de riesgo:

- `indicator_vector_name`- Indica el vector de riesgo asociado a un indicador de riesgo. Los vectores de riesgo son indicadores de riesgo basados en dispositivos, indicadores de riesgo basados en la ubicación, indicadores de riesgo basados en fallos de inicio de sesión, indicadores de riesgo basados en IP, indicadores de riesgo basados en datos, indicadores de riesgo basados en archivos y otros indicadores de riesgo.
- `indicator_vector_id`- Identificación asociada a un vector de riesgo. ID 1 = Indicadores de riesgo basados en dispositivos, ID 2 = Indicadores de riesgo basados en la ubicación, ID 3 = Indicadores de riesgo basados en fallos de inicio de sesión, ID 4 = Indicadores de riesgo basados en IP, ID 5 = Indicadores de riesgo basados en IP, ID 6 = Indicadores de riesgo basados en datos, ID 7 = Otros indicadores de riesgo e ID 999 = No disponible.

Para obtener más información, consulte Formato de datos de Citrix Analytics para SIEM.

## 7 de junio de 2021

### Novedades

**Mejoras en la acción notificar a los administradores** Al aplicar la acción **Notificar a los administradores** a un indicador de riesgo o crear una directiva con la acción, ahora puede seleccionar los

administradores que reciben una notificación sobre el comportamiento de riesgo del usuario. Para obtener más información sobre la acción, consulte Directivas y acciones.

**Se agregó compatibilidad con la acción de compartir de solo lectura** Si un usuario comparte archivos de forma excesiva, Citrix Analytics activa el indicador de riesgo de **uso compartido excesivo de archivos**. Desde el cronograma de riesgo del usuario, ahora puede aplicar la acción **Cambiar vínculos al uso compartido de solo lectura** al indicador **Riesgo excesivo de uso compartido de archivos**. También puede aplicar la acción en un enlace de recurso compartido concreto en el cronograma de riesgo del enlace de compartir. Esta acción impide que otros usuarios descarguen, copien o impriman los archivos asociados a los vínculos compartidos. Para obtener más información sobre la acción, consulte Directivas y acciones.

## 18 de mayo de 2021

### Novedades

**Migración de los indicadores de riesgo de incumplimiento a indicadores de riesgo personalizados** Los siguientes indicadores de riesgo por defecto se migran a indicadores de riesgo personalizados preconfigurados.

| Indicador de riesgo de impago | Origen de datos | Indicador de riesgo personalizado preconfigurado |
|---|---|---|
| Acceso por primera vez desde un dispositivo nuevo | Citrix Virtual Apps and Desktops y Citrix DaaS | Acceso por primera vez al CVAD desde un nuevo dispositivo |
| Acceso por primera vez desde una nueva IP | Citrix Gateway | Acceso por primera vez a la puerta de enlace desde una nueva IP |

Con esta migración a los indicadores de riesgo personalizados, los indicadores de riesgo predeterminados y los algoritmos de aprendizaje automático asociados quedan obsoletos.

Los indicadores de riesgo personalizados correspondientes se activan en función de las siguientes condiciones preconfiguradas:

- Cuando un usuario accede desde un dispositivo nuevo por primera vez o desde un dispositivo existente que no se ha utilizado durante un mínimo de 90 días.
- Cuando un usuario inicia sesión desde una nueva dirección IP por primera vez o desde una dirección IP existente que no se ha utilizado durante un mínimo de 90 días.

Junto con las condiciones preconfiguradas, ahora puede agregar sus propias condiciones para estos indicadores de riesgo personalizados para identificar las amenazas en su entorno Citrix. Esta opción le da flexibilidad para configurar el indicador de riesgo personalizado en función de sus necesidades de seguridad. También puede crear directivas para aplicar acciones en los eventos de riesgo detectados por estos indicadores de riesgo personalizados.

Sin embargo, en la línea temporal del usuario, todavía se pueden ver los indicadores de riesgo predeterminados activados anteriormente y sus eventos.

Las directivas asociadas a estos indicadores de riesgo de incumplimiento se vinculan automáticamente a los indicadores de riesgo personalizados preconfigurados correspondientes.

Para obtener más información, consulte Directivas e indicadores de riesgo personalizados preconfigurados.

#### Mejoras en la búsqueda de autoservicio para Gateway

- El filtro **Tipo de evento** se renombró ahora a **Tipo de registro**. Seleccione uno de los siguientes tipos de registro para filtrar sus eventos: VPN_AI, VPN_IF y VPN_ST.
- En la tabla **DATOS**, expanda una fila de un evento de usuario para ver el tipo de evento correspondiente. Los tipos de eventos pueden ser uno de los siguientes: autenticación, archivo ICA o cierre de sesión.

En la tabla siguiente se describe la correlación entre los tipos de registro y los tipos de sucesos.

| Tipo de registro | Tipo de evento |
|---|---|
| VPN_AI | Autenticación |
| VPN_IF | Archivo ICA |
| VN_ST | Cerrar sesión |

Para obtener más información, consulte Búsqueda de autoservicio de Gateway.

#### Problema resuelto

- El indicador de riesgo personalizado se activa en función de la sensibilidad entre mayúsculas y minúsculas de los valores condicionales. Por ejemplo, en los eventos de usuario que contienen ID de dispositivo de la lista de permitidos, se observa el siguiente comportamiento:
  - Si introduce el valor de la dimensión `Device-ID` en minúsculas, se activa el indicador personalizado.

```
Event-Type = Session.Logon AND Device-ID NOTIN ("1621d2cb-
f598-5ef7-a5bf-81747496ed2e")
```

- Si introduce el valor de la dimensión `Device-ID` en mayúsculas para el mismo dispositivo, el indicador personalizado no se activa.

```
Event-Type = Session.Logon AND Device-ID NOTIN ("1621D2CB-
F598-5EF7-A5BF-81747496ED2E")
```

Este problema ya se ha solucionado y el indicador de riesgo personalizado se activa independientemente de la sensibilidad entre mayúsculas y minúsculas de los valores condicionales.

[CAS-50153]

## 29 de abril de 2021

### Novedades

**Detalles de eventos para un indicador de riesgo personalizado** En la página del cronograma de riesgo del usuario, ahora puede ver los eventos que han desencadenado un indicador de riesgo personalizado. Anteriormente, solo podía ver las condiciones definidas, la descripción y la frecuencia de activación de un indicador de riesgo personalizado. Haga clic en **Búsqueda de eventos** para ver los detalles de los eventos asociados al usuario y el indicador de riesgo.
Para obtener más información, consulte Indicadores de riesgo personalizados.

### Problema resuelto

- Un administrador no puede crear indicadores de riesgo personalizados incluso después de cambiar su permiso de acceso de administrador de solo lectura a administrador completo. [CAS-49628]

## 16 de abril de 2021

### Novedades

**Mejoras en los mensajes SIEM** Puede ver las siguientes mejoras en el formato del esquema del indicador de riesgo:

- La dirección IP del cliente ya está disponible en el esquema de todos los indicadores de riesgo por lotes. Anteriormente, la dirección IP del cliente solo estaba disponible para unos pocos indicadores de riesgo por lotes:
  - Error en la exploración de la EPA

  - Fallos de autenticación excesivos
  - Inicio de sesión desde IP sospechosa
  - Acceso desde una ubicación inusual
  - Error de autenticación inusual
  - Descarga compartida confidencial anónima
  - Exfiltración potencial de datos

- Si un valor de campo de tipo de datos enteros no está disponible, el valor asignado es **-999**. Por ejemplo, `"latitide"= -999`.
- Si un valor de campo de tipo de datos de cadena de caracteres no está disponible, el valor asignado es **NA**. Por ejemplo, `"city"= "NA"`.

Para obtener más información, consulte Formato de datos de Citrix Analytics para SIEM.

## 26 de marzo de 2021

### Novedades

**Restricción de los mensajes SIEM** Citrix Analytics envía un máximo de 1000 detalles de eventos por cada aparición de indicador de riesgo a su servicio SIEM. Estos eventos se envían en orden cronológico de ocurrencia. Para obtener más información, consulte Formato de datos de Citrix Analytics para SIEM.

**Agregados los campos ID de origen de datos y ID de categoría de indicador en los mensajes SIEM** Los campos siguientes se agregan en el esquema de resumen del indicador y en el esquema de detalles de eventos del indicador.

| Campo | Descripción |
|---|---|
| `data_source_id` | Identificador asociado a un origen de datos. ID 0 = Citrix Content Collaboration, ID 1 = Citrix Gateway, ID 2 = Citrix Endpoint Management, ID 3 = Citrix Virtual Apps and Desktops, ID 4 = Citrix Access Control |
| `indicator_category_id` | ID asociado a una categoría de indicador de riesgo. ID 1 = Exfiltración de datos, ID 2 = Amenazas internas, ID 3 = Usuarios comprometidos |

Para obtener más información, consulte Formato de datos de Citrix Analytics para SIEM.

## 18 de marzo de 2021

### Novedades

#### Panel de control de ubicación de control de acceso

> **Nota**
>
> La función se halla en Tech Preview.

El panel **Ubicación de garantía de acceso** proporciona una descripción general de las ubicaciones desde las que los usuarios de Citrix Virtual Apps and Desktops y Citrix DaaS iniciaron sesión durante un período seleccionado. Citrix Analytics recibe estos eventos de inicio de sesión de usuario de la aplicación Citrix Workspace instalada en los dispositivos de los usuarios.

Para ver el panel de control, haga clic en **Seguridad > Garantía de acceso**.

Puede ver la siguiente información de un período seleccionado:

- Número total de inicios de sesión de usuarios desde una ubicación concreta y en todas las ubicaciones.
- Número total de inicios de sesión de usuario únicos en todas las ubicaciones.
- Número total de países desde los que los usuarios han iniciado sesión.
- Las 10 mejores ubicaciones con inicios de sesión de usuario únicos.

Para obtener más información, consulte Ubicación de Access Assurance.


**Compatibilidad con el operador NOT LIKE (!~)** Para la consulta de búsqueda de autoservicio y la condición del indicador de riesgo personalizado, ahora puede usar el comando NOT LIKE (!~) operador. El operador comprueba los eventos de usuario para el patrón coincidente que ha especificado.

Devuelve los eventos que no contienen el patrón especificado en ninguna parte de la cadena de eventos.

Por ejemplo, la consulta `User-Name !~ "John"` muestra los eventos de los usuarios excepto John, John Smith o cualquier otro usuario que contenga el nombre coincidente "John".

Para obtener más información, consulte Búsqueda de autoservicio.

**Versión traducida del sistema operativo** Para el origen de datos Citrix Virtual Apps and Desktops y Citrix DaaS, la dimensión **Plataforma** ahora se traduce como las dimensiones **OS-Major-Version**, **OS-Minor-Version** y **OS-Extra-Details**. Según los detalles del sistema operativo de un usuario, Citrix Analytics muestra estas dimensiones en la página de búsqueda de autoservicio.

Puede utilizar estas dimensiones para definir las condiciones de un indicador de riesgo personalizado.

Para los indicadores de riesgo personalizados creados anteriormente, si ha utilizado la dimensión **Plataforma** como condición, Citrix Analytics sustituye automáticamente la dimensión de **plataforma** por la versión **principal** del sistema operativo, la versión**menor**del sistema operativo y los **detalles adicionales** del sistema operativo. Esta actualización no afecta a la integridad de la condición definida.

Para obtener más información sobre las nuevas dimensiones, consulte Búsqueda de autoservicio de Virtual Apps and Desktops.

**Se actualizaron los campos de datos para aplicaciones y escritorios** En la búsqueda de autoservicio de aplicaciones y escritorios, consulte los campos de datos actualizados en función de la plantilla contextual.

Para obtener más información, consulte Búsqueda de autoservicio de aplicaciones y escritorios.

### Función obsoleta

**Se han eliminado los eventos VPN_AF y VPN_SU de la página de búsqueda de autoservicio** En la página de búsqueda de autoservicio del origen de datos de Citrix Gateway, se quitan los siguientes tipos de registro.

| Tipo de registro | Nombre del registro |
|---|---|
| VPN_SU | Registro de actualización de sesión |
| VPN_AF | Registro de error de inicio de la aplicación |

Por lo tanto, no puede filtrar ni ver sus eventos en función de estos tipos de registro. Cualquier indicador de riesgo personalizado basado en estos tipos de registro deja de funcionar.

Para obtener más información, consulte Búsqueda de autoservicio de Gateway.

## 11 de marzo de 2021

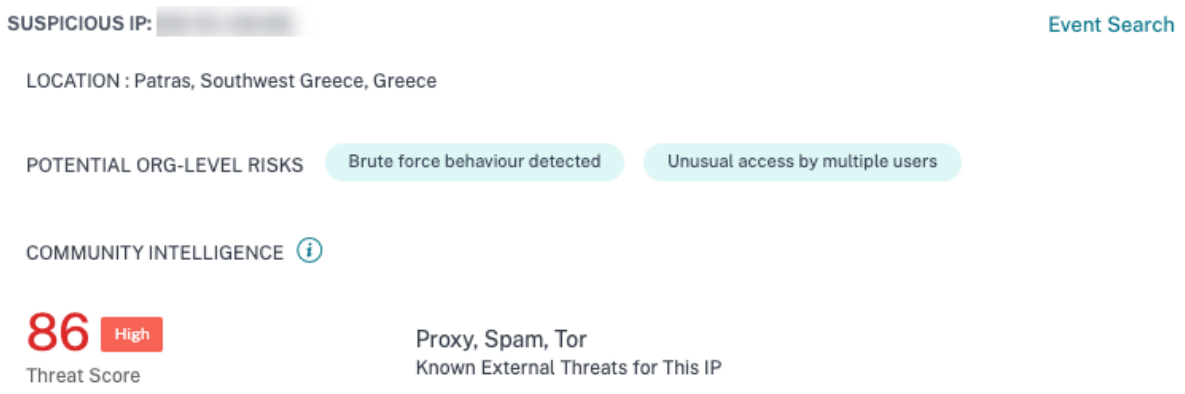
### Novedades

**Marca de tiempo actual del esquema de puntuación de riesgo del usuario** `last_update_timestamp` Se agrega un nuevo campo en el formato de esquema de puntuación de riesgo del usuario. Este campo indica el momento en que se actualizó por última vez la puntuación de riesgo. Para obtener más información sobre el formato del esquema, consulte Esquema de puntuación de riesgo del usuario.

## 3 de marzo de 2021

### Novedades

**Mejoras en el indicador de riesgo de inicio de sesión desde IP sospechosa** En la página de cronograma de riesgo del usuario, se muestra una nueva sección **IP sospechosa** para el indicador de riesgo de inicio de **sesión desde IP sospechosa**. En esta sección se proporciona la siguiente información:




- Dirección IP desde la que se detecta una actividad de inicio de sesión sospechosa.
- Ubicación del usuario.
- Cualquier patrón de actividad IP sospechosa que Citrix Analytics haya detectado recientemente en su organización.
- Fuente de inteligencia a nivel comunitario sobre la dirección IP.

Para obtener más información, consulte el indicador de riesgo de inicio de sesión desde IP sospechosa.

#### Mejoras en el indicador de riesgo de acceso desde una ubicación inusual

- En el indicador de riesgo de acceso desde una ubicación inusual de Citrix Content Collaboration, se agregó la columna **NOMBRE DE HERRAMIENTA** en la tabla de eventos. Se ha eliminado la columna **EXPLORADOR DE DISPOSITIVOS** de la tabla de eventos. Para obtener más información, consulte Indicadores de riesgo de Citrix Content Collaboration.
- En el indicador de riesgo Acceso desde una ubicación inusual para Citrix Virtual Apps and Desktops y Citrix DaaS, se agregaron las columnas **ID DE DISPOSITIVO** y **TIPO DE RECEIVER** a la tabla de eventos. Para obtener más información, consulte Indicadores de riesgo de Citrix Virtual Apps and Desktops.

**Formato de datos de Citrix Analytics para SIEM** En este artículo se describe el esquema de los datos procesados generados por Citrix Analytics para su servicio SIEM.

#### Problema resuelto

- Para un usuario de Content Collaboration, si el valor de `Is Employee` es nulo, el usuario no se muestra en la lista de usuarios detectados. [CAS-47815]

### 18 de febrero de 2021

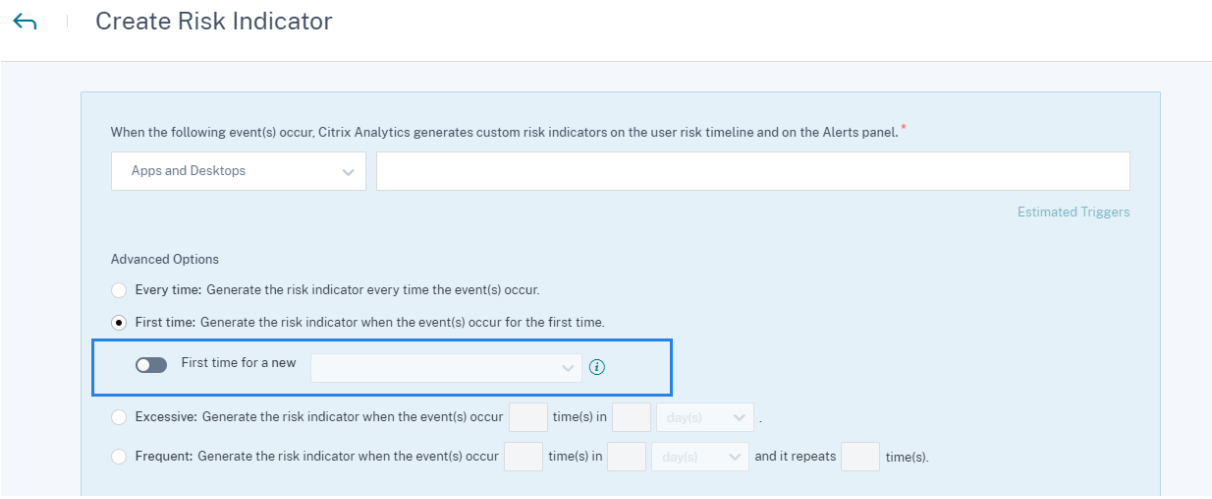
#### Novedades

**Compatibilidad con el acceso por primera vez desde una nueva entidad en el indicador de riesgo personalizado** Ahora puede crear un indicador de riesgo que se active cuando Citrix Analytics recibe eventos de una nueva entidad por primera vez. Algunos ejemplos de entidades son IP del cliente, ciudad y país.

En la página **Crear indicador**, haga clic en la opción **Primera vez**. Active el botón **Primera vez para un nuevo** y seleccione una entidad válida de la lista en función del origen de datos. No es necesario asignar ningún valor específico a la entidad. Por ejemplo, si selecciona **Ciudad** de la lista, Citrix Analytics activa un indicador de riesgo cada vez que los usuarios inician sesión desde una nueva ciudad por primera vez.

Para obtener más información, consulte Creación de un indicador de riesgo personalizado.



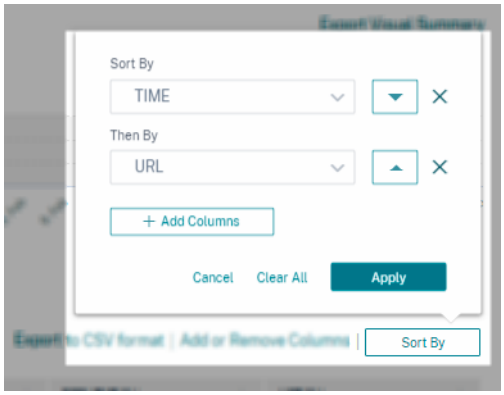

**Límite máximo para crear un indicador de riesgo personalizado** Ahora puede crear indicadores de riesgo personalizados hasta un límite máximo de 50. Si alcanza este límite máximo, debe eliminar o modificar cualquier indicador de riesgo personalizado existente para crear un indicador de riesgo personalizado.

Para obtener más información, consulte Indicadores de riesgo personalizados.

**Datos de ubicación de usuarios de Citrix Virtual Apps and Desktops y Citrix DaaS** En la página **Información del usuario**, Citrix Analytics ahora muestra la ubicación del usuario en el origen de datos de Citrix Virtual Apps and Desktops y Citrix DaaS.

Para obtener más información sobre la ubicación del usuario, consulte Perfil de usuario.

**Clasificación de varias columnas** En la página de búsqueda de autoservicio, ahora puede ordenar los eventos de usuario por más de una columna. Haga clic en **Ordenar por**, agregue las columnas y el orden de clasificación. Haga clic en **Aplicar** para ordenar los eventos de usuario. Puede agregar hasta seis columnas para ordenar varias columnas.



Para obtener más información, consulte Búsqueda de autoservicio.

#### Funciones retiradas

**Indicador de riesgo de fallo de autorización excesivo obsoleto** El indicador de riesgo de Citrix Gateway: **error de autorización excesivo** ha quedado obsoleto. Solo se pueden ver los datos históricos relacionados con este indicador.

Los siguientes cambios se aplican como parte de esta desuso:

- Citrix Analytics ya no genera estos indicadores de riesgo.
- Citrix Analytics ya no genera directivas con estos indicadores de riesgo como condiciones.
- Directivas de impago con estos indicadores de riesgo, ya que las condiciones ya no surten efecto.

Para obtener más información, consulte Indicadores de riesgo de Citrix Gateway.

### 27 de enero de 2021

#### Novedades

**Mejoras en el indicador de riesgo de acceso desde una ubicación inusual** En Citrix Content Collaboration, Citrix Gateway y Citrix Virtual Apps and Desktops, el indicador de riesgo de **acceso desde una ubicación inusual** ahora se activa cuando el usuario inicia sesión desde una dirección IP asociada a un nuevo país o una nueva ciudad que se encuentre anómalamente lejos de cualquier inicio de sesión anterior ubicación. Otros factores incluyen el nivel general de movilidad del usuario y la frecuencia relativa de los inicios de sesión desde la ciudad en todos los usuarios de la organización. En todos los casos, el historial de ubicaciones de usuario se basa en los 30 días anteriores de actividad de inicio de sesión.

Para obtener más información sobre el indicador de riesgo, consulte los temas siguientes:

- Indicadores de riesgo de Citrix Content Collaboration
- Indicadores de riesgo Citrix Gateway
- Indicadores de riesgo de Citrix Virtual Apps and Desktops y Citrix DaaS

### 20 de enero de 2021

#### Problema resuelto

- Para el origen de datos de Apps and Desktops con StoreFront local, el procesamiento de datos falla aunque la implementación de StoreFront se haya conectado correctamente.

[CAS-46656]

## 19 de enero de 2021

### Problema resuelto

- En la página del indicador de riesgo personalizado, después de corregir una condición no válida en el campo de búsqueda, el enlace **Activador de estimación** no responde.

  Por ejemplo, escribe una condición no válida *Client-IP = 10.10.10.10*. Después de corregir esta condición y escribir como *IP de cliente = "10.10.10.10"*, el enlace **Desencadenador de estimación** no responde.

  **Solución alternativa**: actualice la página del indicador personalizado y, a continuación, cree el indicador personalizado con una condición válida.

  [CAS-46316]

## 13 de enero de 2021

### Novedades

**Ya está disponible una nueva versión del complemento Citrix Analytics para Splunk** El complemento Citrix Analytics versión 2.1.0 para Splunk ya está disponible. Vaya a la página de descargas para descargar el archivo.

**Se agregó compatibilidad con Splunk Cloud Inputs Data Manager (IDM) y Splunk 8.1 de 64 bits** Ahora puede integrar Citrix Analytics for Security con Splunk Cloud IDM y Splunk 8.1 de 64 bits. Para obtener más información, consulte Integración de Splunk.

### Compatibilidad retirada

**Se ha eliminado la compatibilidad con Splunk 7.1 de 64 bits** Ya no puede integrar Citrix Analytics for Security con Splunk 7.1 de 64 bits. Para obtener información sobre las versiones de Splunk compatibles, consulte Integración de Splunk.

## 11 de enero de 2021

### Problema resuelto

- En la tarjeta de sitio Virtual Apps and Desktops, la etiqueta **Usuarios cliente admitidos** pasa a llamarse **Eventos recibidos de los usuarios**. La etiqueta **Usuarios cliente no admitidos** pasa a llamarse **No se pueden recibir eventos de los usuarios**.

  [CAS-44773]

## 17 de diciembre de 2020

### Novedades

**Utilice indicadores de riesgo personalizados preconfigurados y una directiva para bloquear el acceso desde ubicaciones inusuales (geocercas)** Citrix proporciona una lista de indicadores de riesgo personalizados preconfigurados y una directiva que le ayudan a supervisar la seguridad de su infraestructura Citrix. Con estos indicadores y una directiva, puede bloquear el acceso de usuario originario de países que están fuera de su país operativo habitual. De forma predeterminada, el país se establece en "Estados Unidos". Puede establecer el país requerido para el geocercado.

A continuación se indican los indicadores de riesgo personalizados preconfigurados y una directiva:

- Sesión CVAD iniciada fuera de la geocerca
- Cruce de geocercas GW
- Cruce de geocerca CCC
- Inicio de sesión fuera de la geocerca

Para obtener más información, consulte Directivas e indicadores de riesgo personalizados preconfigurados.

**Ver ubicaciones accedidas en el correo electrónico de respuesta del usuario** En lugar de la dirección IP de un dispositivo de usuario, el correo electrónico de respuesta del usuario muestra ahora todas las ubicaciones a las que ha accedido el usuario en los últimos 15 minutos. La ubicación se muestra en el formato `<City>,<Country>`. Si la ciudad o el país no están disponibles, el valor correspondiente se muestra como "Desconocido".

Para obtener más información, consulte Solicitar respuesta del usuario.

**Indicador de riesgo de Content Collaboration renombrado: acceso por primera vez desde una nueva ubicación** El indicador de riesgo de Citrix Content Collaboration cambia el nombre del **primer acceso desde una nueva ubicación** como **Acceso desde una ubicación inusual**.

Para obtener más información, consulte Acceso desde una ubicación inusual.

#### Funciones retiradas

**Comentarios sobre los indicadores de riesgo** Se elimina el mecanismo de retroalimentación del indicador de riesgo. Si el indicador de riesgo de Content Collaboration (Acceso desde una ubicación inusual) se activa incorrectamente, ya no podrá denunciarlo como falso positivo ni proporcionar comentarios.

### 7 de diciembre de 2020

#### Novedades

**Mejoras en el indicador de riesgo potencial de exfiltración de datos** Se han realizado las siguientes mejoras en el indicador de riesgo:

- Se actualiza la información de la sección **QUÉ HA OCURRIDO**. El formato de hora se actualiza para mantener la coherencia.
- La información de ubicación del dispositivo aparece en la lista de eventos.

Para obtener más información sobre el indicador de riesgo, consulte Exfiltración potencial de datos.

**Mejoras en el indicador de riesgo de Content Collaboration: acceso por primera vez desde una nueva ubicación** En el cronograma de riesgo del usuario, seleccione **Acceso por primera vez desde una nueva ubicación** para ver la siguiente información:

- **Ubicaciones de inicio de sesión**: muestra una vista de mapa geográfico de las ubicaciones habituales e inusuales desde las que el usuario ha iniciado sesión.
- **Número de inicios de sesión desde ubicaciones habituales: últimos 30 días**: muestra una vista de gráfico circular de las 6 ubicaciones habituales principales desde las que el usuario ha iniciado sesión en los últimos 30 días. También muestra el número de eventos de inicio de sesión de estas ubicaciones.
- **Detalles de sucesos para ubicaciones inusuales**: proporciona la lista de los eventos de inicio de sesión de una ubicación inusual para el usuario.

Para obtener más información sobre el indicador de riesgo, consulte Acceso por primera vez desde una nueva ubicación.

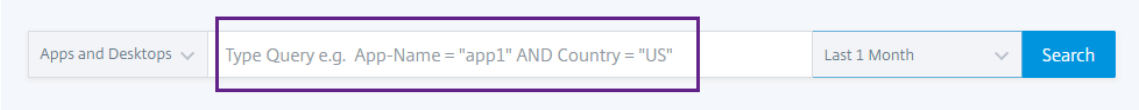
 

## 30 de noviembre de 2020

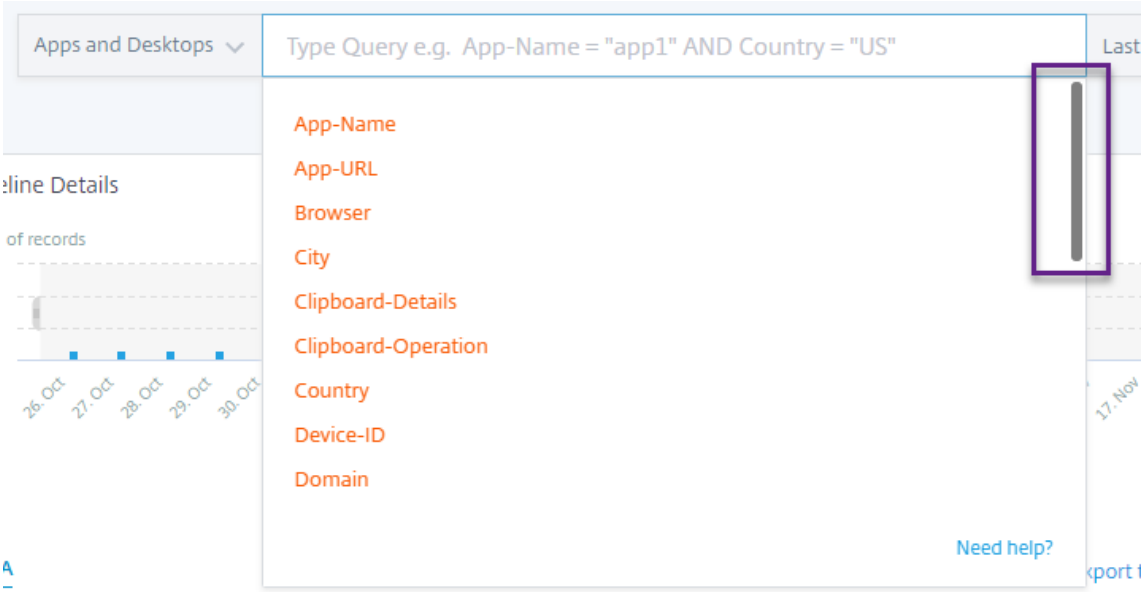
### Novedades

**Mejoras en la página de búsqueda autoservicio** Se han realizado las siguientes mejoras para mejorar la usabilidad de la página de búsqueda de autoservicio:

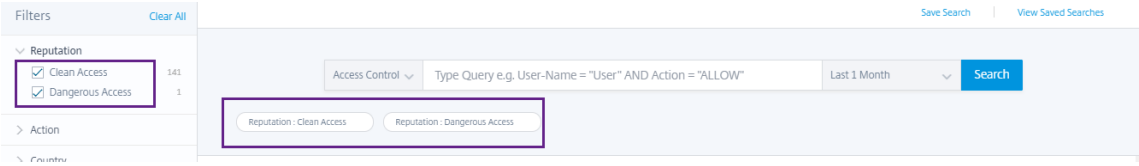
- El cuadro de búsqueda muestra un ejemplo de consulta para indicar cómo escribir su propia consulta.




- En macOS, la barra de desplazamiento de la lista de dimensiones aparece ahora de forma predeterminada.

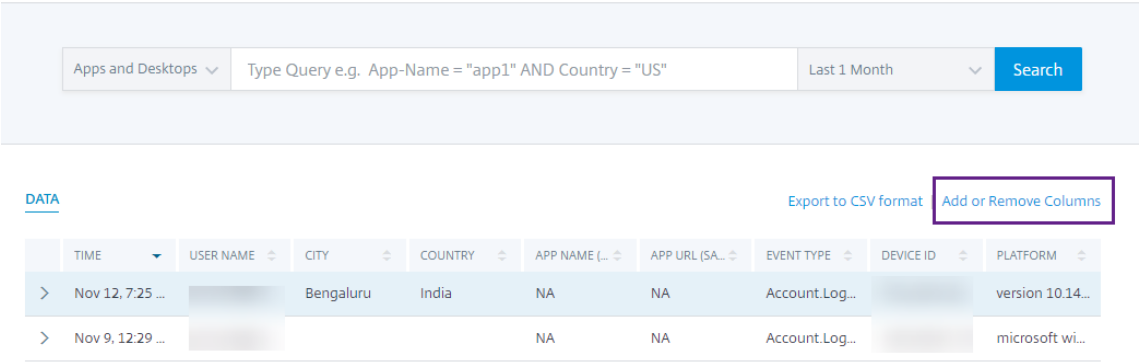



- Los filtros aplicados aparecen ahora como fichas.




- La etiqueta **Agregar o quitar columnas** sustituye al icono **+**.




Para obtener más información, consulte Búsqueda de autoservicio.

**Mejoras directivas** La página **Directivas** muestra ahora las directivas asociadas a los orígenes de datos que se han detectado correctamente y se han conectado a Citrix Analytics. En esta página no se muestran las directivas que tienen una condición definida para los orígenes de datos no detectadas. La desactivación del procesamiento de datos de un origen de datos ya conectada no afecta a las directivas existentes en la página **Directivas**.

Para obtener más información, consulte Configurar directivas y acciones.

## 4 de noviembre de 2020

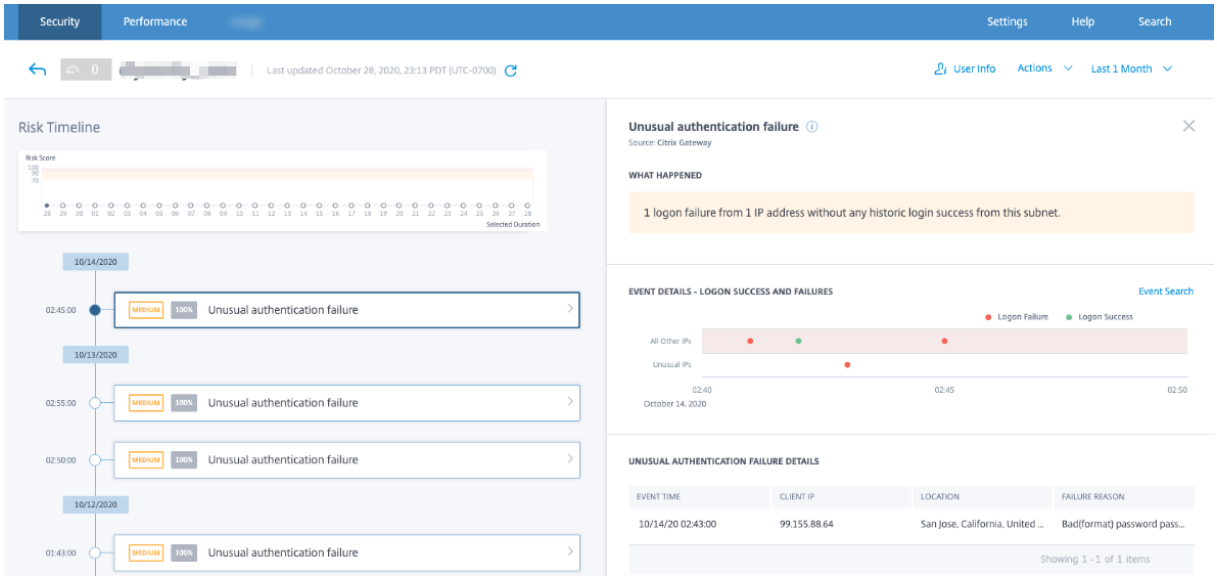
### Novedades

**Error de autenticación inusual: indicador de riesgo de Citrix Gateway** Citrix Analytics detecta amenazas basadas en el acceso cuando un usuario tiene errores de inicio de sesión desde una dirección IP inusual y activa el indicador de riesgo de **errores de autenticación inusuales**.

Este indicador de riesgo se activa cuando un usuario de su organización tiene errores de inicio de sesión desde una dirección IP inusual que es contraria a su comportamiento habitual.

Para obtener más información, consulte Indicadores de riesgo de Citrix Gateway.




## 20 de octubre de 2020

### Problema resuelto

- El indicador de riesgo **Acceso por primera vez desde un dispositivo nuevo** con la acción **Cerrar sesión del usuario** no funciona según lo esperado.

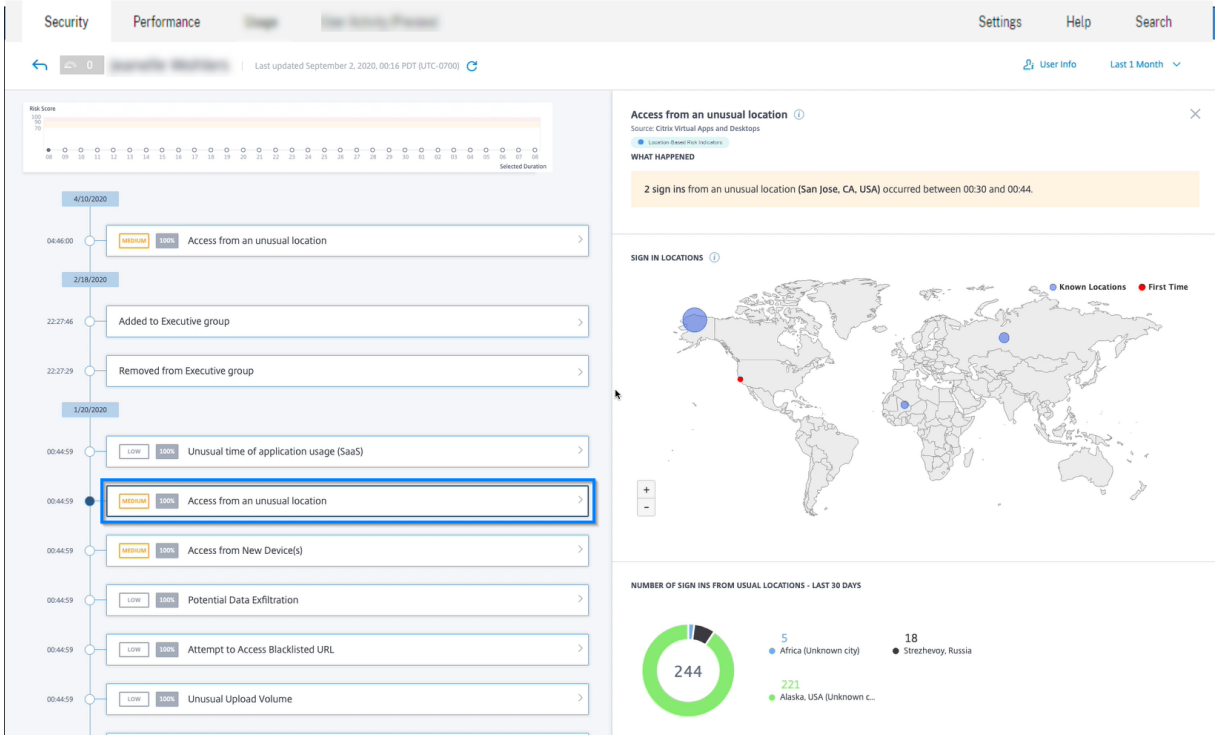
  [CAS-40743]

## 15 de octubre de 2020

### Funciones nuevas

**Acceso desde una ubicación inusual: indicador de riesgo de Citrix Virtual Apps and Desktops y Citrix DaaS** Citrix Analytics detecta las amenazas basadas en el acceso basándose en los accesos inusuales de Citrix Workspace y activa el indicador de riesgo correspondiente.




Para obtener más información, consulte Indicadores de riesgo de Citrix Virtual Apps and Desktops y Citrix DaaS.

### Mejoras en el panel Share Link

- La columna URL SHARE se sustituye ahora por la columna SHARE ID. Cada URL de recurso compartido se identifica ahora con un ID de recurso compartido.
- Se elimina la selección de tiempo en el tablero de mandos. Ahora, este panel muestra todos los enlaces de recursos compartidos desde el estado activo hasta el estado caducado en lugar de un período seleccionado.
- Todos los enlaces compartidos se ordenan primero según el orden de los enlaces activos y, a continuación, los enlaces caducados. De forma predeterminada, el enlace de compartir con el recuento de indicadores de riesgo más alto aparece en la parte superior de la lista.
- Los vínculos de riesgo muestran ahora los vínculos activos que tienen un comportamiento de riesgo. No muestra los enlaces caducados. De forma predeterminada, el vínculo de riesgo con el recuento de indicadores de riesgo más alto aparece en la parte superior de la lista.
- Se ha eliminado la vista de tendencias de la tarjeta Enlaces de recursos compartidos con riesgos y de la tarjeta Todos los vínculos a compartir.

Para obtener más información, consulte Panel de control Compartir vínculos.

**Mejoras en el cronograma de riesgo de Share Link** El cronograma de riesgo ahora muestra el ID del recurso compartido en lugar de la URL del recurso compartido. Para obtener más información, consulte Cronología de riesgo de Share Link.

#### Funciones retiradas

**El acceso desde un dispositivo con indicador de riesgo del sistema operativo (SO) no compatible está obsoleto** El indicador de riesgo de Citrix Virtual Apps and Desktops: El **acceso desde un dispositivo con sistema operativo (SO) no compatible** ha quedado obsoleto. Solo se pueden ver los datos históricos relacionados con este indicador.

Los siguientes cambios se aplican como parte de esta desuso:

- La analítica ya no genera estos indicadores de riesgo.
- Analytics ya no genera directivas con estos indicadores de riesgo como condiciones.
- Directivas de impago con estos indicadores de riesgo, ya que las condiciones ya no surten efecto.

Para obtener más información, consulte Indicadores de riesgo de Citrix Virtual Apps and Desktops y Citrix DaaS.

### 10 de septiembre de 2020

#### Funciones nuevas

**Lista de comprobación para StoreFront** Citrix Analytics muestra ahora una lista de los requisitos previos que debe cumplir antes de descargar el archivo de configuración de StoreFront. Revise la lista de comprobación y asegúrese de que se han seleccionado todos los requisitos mínimos. Si no se seleccionan los requisitos mínimos, no podrá descargar el archivo de configuración. Para obtener más información, consulte Origen de datos de Citrix Virtual Apps and Desktops.

**Búsqueda de autoservicio: Compatibilidad con el operador NOT EQUAL (!=)** Ahora puede usar el valor NOT EQUAL (! =) en su consulta en las siguientes funciones:

- Indicador de riesgo personalizado
- Búsqueda de autoservicio

Puede utilizar este operador para las siguientes condiciones:

| Origen de datos | Dimensiones |
|---|---|
| Content Collaboration | País, ciudad, SO cliente |
| Control de acceso | País, Ciudad, Acción, URL, Categoría de URL, Reputación, Explorador, SO, Dispositivo |
| Aplicaciones y escritorios | País, ciudad, nombre de la aplicación, operación del portapapeles, explorador, sistema operativo |
| Gateway | Etapa de autenticación, IP de cliente |

Con el operador, cree una expresión de indicador personalizada con un único valor como "¡País! = XYZ"y ver la lista de usuarios. A continuación, cree una directiva para aplicar acciones como Agregar a lista de seguimiento, Notificar al administrador o Inhabilitar usuario.
También puede utilizar el operador en la búsqueda de autoservicio de los orígenes de datos especificadas para filtrar los eventos de usuario.

Al introducir los valores de las dimensiones de la consulta, utilice los valores exactos que se muestran en la página de búsqueda de autoservicio de un origen de datos. Los valores de cota distinguen entre mayúsculas y minúsculas

## 8 de septiembre de 2020

### Funciones nuevas

**Correlación de usuarios** Analytics ahora correlaciona a los usuarios descubiertos de varios orígenes de datos. Este mecanismo elimina la mayoría de los usuarios duplicados de la lista de usuarios descubiertos. Los usuarios descubiertos en Analytics ahora muestran la lista de usuarios únicos junto con sus orígenes de datos y los indicadores de riesgo.

Por ejemplo, el usuario "Joe Smith"puede tener varios identificadores de usuario, JosephSm, joe.smith@citrix.com y joe.smith, según los orígenes de datos. Analytics ahora identifica a este usuario con un nombre de identificador único. Todos los demás identificadores de usuario están correlacionados y los eventos recibidos para Joe Smith de varios orígenes de datos están vinculados a este nombre único.
Para obtener más información, consulte Usuarios descubiertos

### Problema resuelto

En la lista **Acciones**, tras seleccionar las opciones de acción y hacer clic en **Aplicar**, aparece un mensaje de error.

[CAS-39914]

## 11 de agosto de 2020

### Problemas resueltos

- No puede integrar Microsoft Graph Security con Citrix Analytics. Este problema se produjo porque el portal de Microsoft no pudo redirigir a Citrix Analytics.

[CAS-38021]

## 31 de julio de 2020

### Problemas resueltos

- La opción **Desencadenadores estimados** del indicador de riesgo personalizado no predice las instancias del indicador de riesgo personalizado del último día.

[CAS-38129]

## 9 de julio de 2020

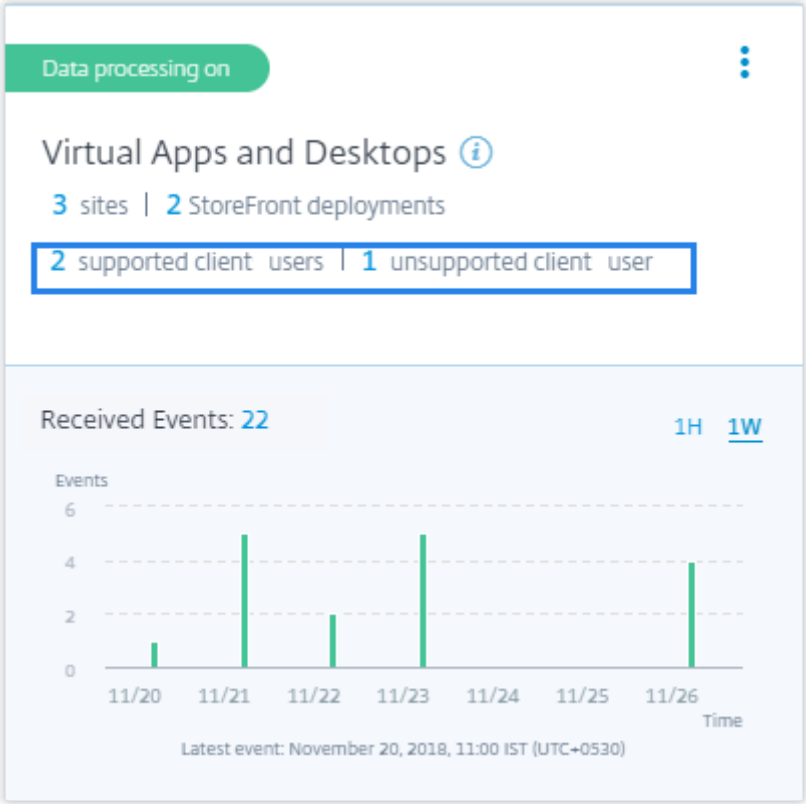
### Funciones nuevas

**La tarjeta de sitio de Virtual Apps and Desktops muestra a los usuarios clientes compatibles y no compatibles** En la tarjeta del sitio, ahora puede ver el número de usuarios que utilizan versiones compatibles y no compatibles de la aplicación Citrix Workspace o clientes de Citrix Receiver en sus dispositivos de punto final.

- Haga clic en el recuento de usuarios de los clientes admitidos para ver la página **Usuario** que muestra todos los usuarios detectados.
- Haga clic en el recuento de usuarios de los clientes no compatibles para descargar un archivo CSV. El archivo enumera los usuarios y sus versiones de cliente no compatibles. Analytics no recibe eventos de usuario de los clientes no admitidos y, por lo tanto, no agrega los usuarios como usuarios detectados. Con el archivo CSV, identifica a los usuarios que deben actualizar sus clientes a una versión compatible para que Analytics pueda proporcionar información de seguridad sobre su comportamiento.

Para ver la lista de clientes compatibles, consulte Origen de datos de Citrix Virtual Apps and Desktops y Citrix DaaS.




**Acceso desde un indicador de riesgo de ubicación inusual**

- El indicador de riesgo de Citrix Gateway El **primer acceso desde una nueva ubicación** pasa a llamarse **Acceso desde una ubicación inusual**.
- En la línea de tiempo de riesgo del usuario, se introducen un mapa geográfico y un gráfico circular en la sección de detalles del evento.
  - **Ubicaciones de inicio de sesión**: esta sección muestra una vista de mapa geográfico de las ubicaciones habituales e inusuales del usuario. Las ubicaciones habituales e inusuales se indican mediante un código de color en la sección superior derecha del mapa geográfico. Puede hacer zoom en el mapa geográfico para ver más de cerca la ubicación.

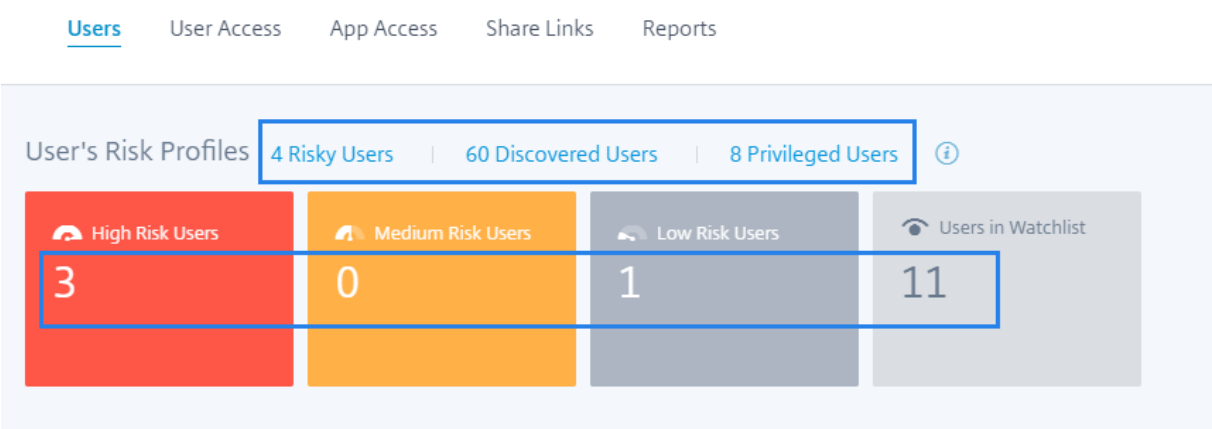

– **Ubicaciones habituales: últimos 30 días**: esta sección muestra un gráfico circular que ofrece una vista de las 6 ubicaciones habituales principales desde las que el usuario ha iniciado sesión. Cada ubicación está marcada con un código de color diferente. Puede ordenar la sección por ubicación para obtener una vista detallada de la ubicación seleccionada.


Para obtener más información, consulte Acceso desde una ubicación inusual.

**Datos del panel de usuarios** El número de usuarios de riesgo, usuarios descubiertos, usuarios privilegiados y usuarios de la lista de seguimiento se muestra durante los últimos 13 meses, independientemente del período de tiempo seleccionado en el panel de control **Usuarios** y en la página **Usuarios**. Al seleccionar el período de tiempo, las incidencias del indicador de riesgo cambian.

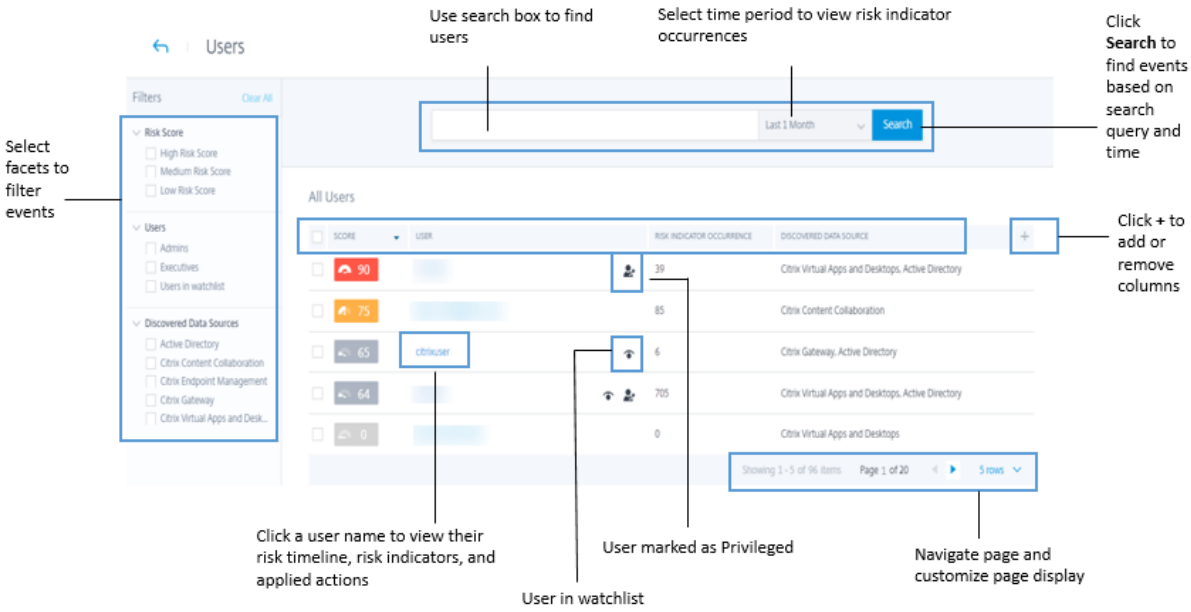
Para obtener más información, consulte Panel de control de usuarios.




**Página Usuarios rediseñada** La página **Usuarios** se ha mejorado para ofrecer una mejor experiencia de usuario. Proporciona un resumen consolidado de los eventos de usuario en función de las puntuaciones de riesgo del usuario, el origen de datos y el tipo de usuario.

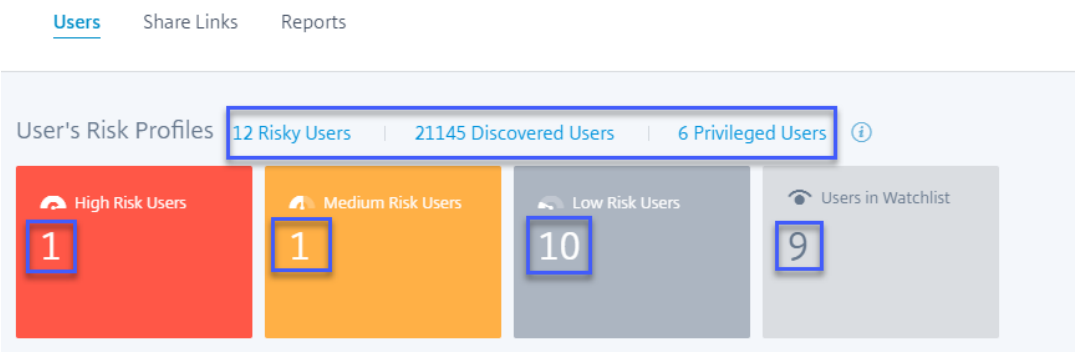
Para permitir una búsqueda más específica, la página **Usuarios** contiene la sección **Filtros** en el panel izquierdo y la barra de búsqueda en la parte superior. Puede buscar eventos de usuario para un tiempo preestablecido o un intervalo de tiempo personalizado.




Para ver la página **Usuarios**:

- Vaya a **Seguridad > Usuarios** para ver el panel **Usuarios** y haga lo siguiente:
  - Haga clic en uno de los siguientes enlaces o en las tarjetas.



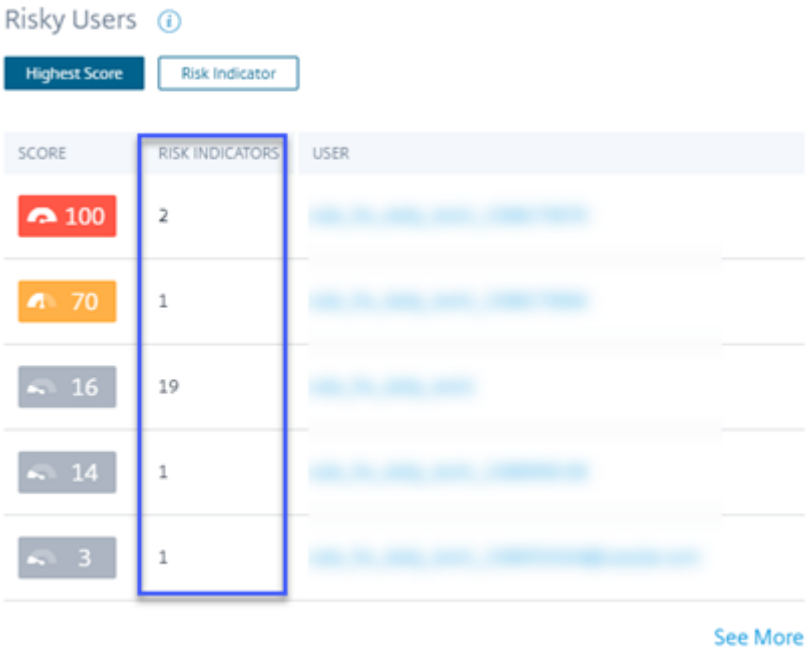

  - En el panel **Usuarios con riesgos**, haga clic en **Ver más**.
  - En el panel **Usuarios de lista de observación**, haga clic en **Ver más**.
  - En el panel **Usuarios con privilegios**, haga clic en **Ver más**.

- Vaya a **Configuración > Orígenes de datos > Seguridad**. Haga clic en el número de usuarios de cualquier tarjeta de sitio de origen de datos.

Para obtener más información, consulte Panel de control de usuarios.

**Mejoras en el panel Usuarios con riesgos** La columna **Cambio** se sustituye por la columna **Indicadores de riesgo**. En la columna **Indicadores** de riesgo se muestran las incidencias totales del indicador de riesgo de un usuario durante un período de tiempo específico.

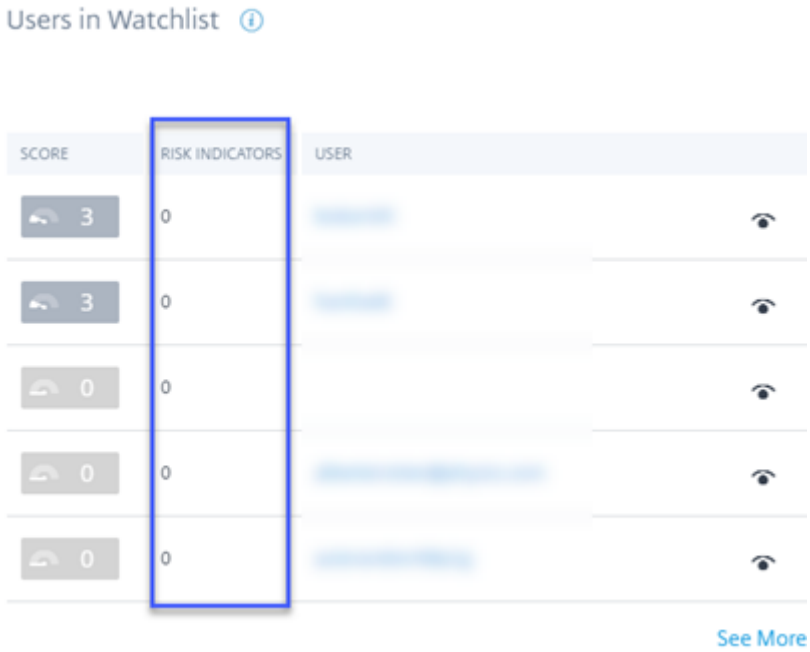
Para obtener más información, consulte Usuarios con riesgos.



**Mejoras en el panel Lista de observación de usuarios** La columna **Cambio** se sustituye por la columna **Indicadores de riesgo**. En la columna **Indicadores** de riesgo se muestran las incidencias totales del indicador de riesgo de un usuario durante un período de tiempo específico.

Para obtener más información, consulte Usuarios de la lista de seguimiento.

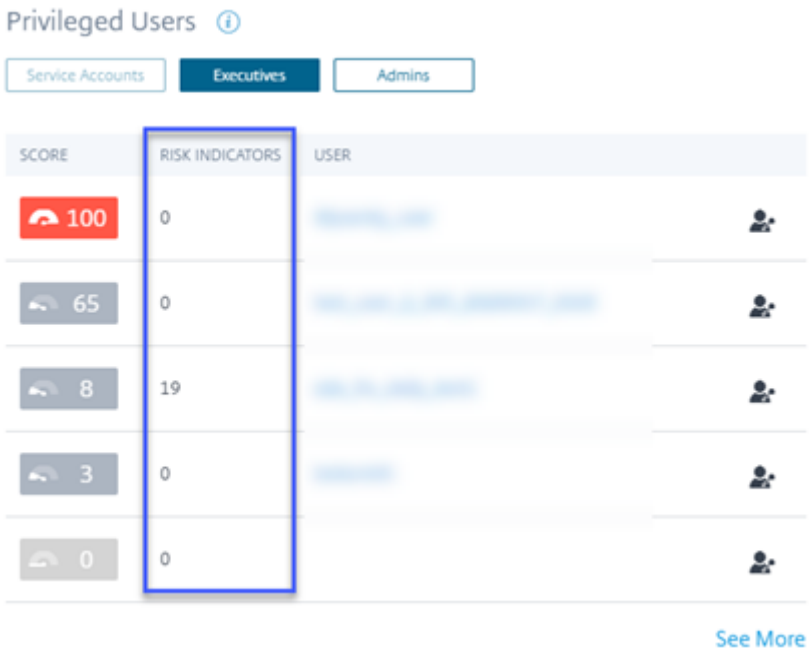



**Mejoras en el panel Usuarios privilegiados**

- La columna **Cambio** se sustituye por la columna **Indicadores de riesgo**. En la columna **Indicadores** de riesgo se muestran las incidencias totales del indicador de riesgo de un usuario durante un período de tiempo específico.
- Haga clic en **Ver más** para ver la página **Usuarios**. La página **Usuarios** que muestra la lista de usuarios con privilegios de administrador y ejecutivo. En esta página, puede agregar o quitar un usuario como usuario privilegiado.

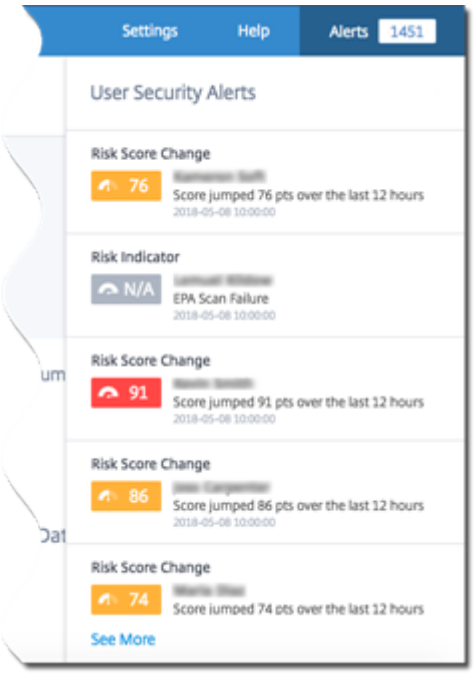
Para obtener más información, consulte Usuarios con privilegios.




**Funciones retiradas**

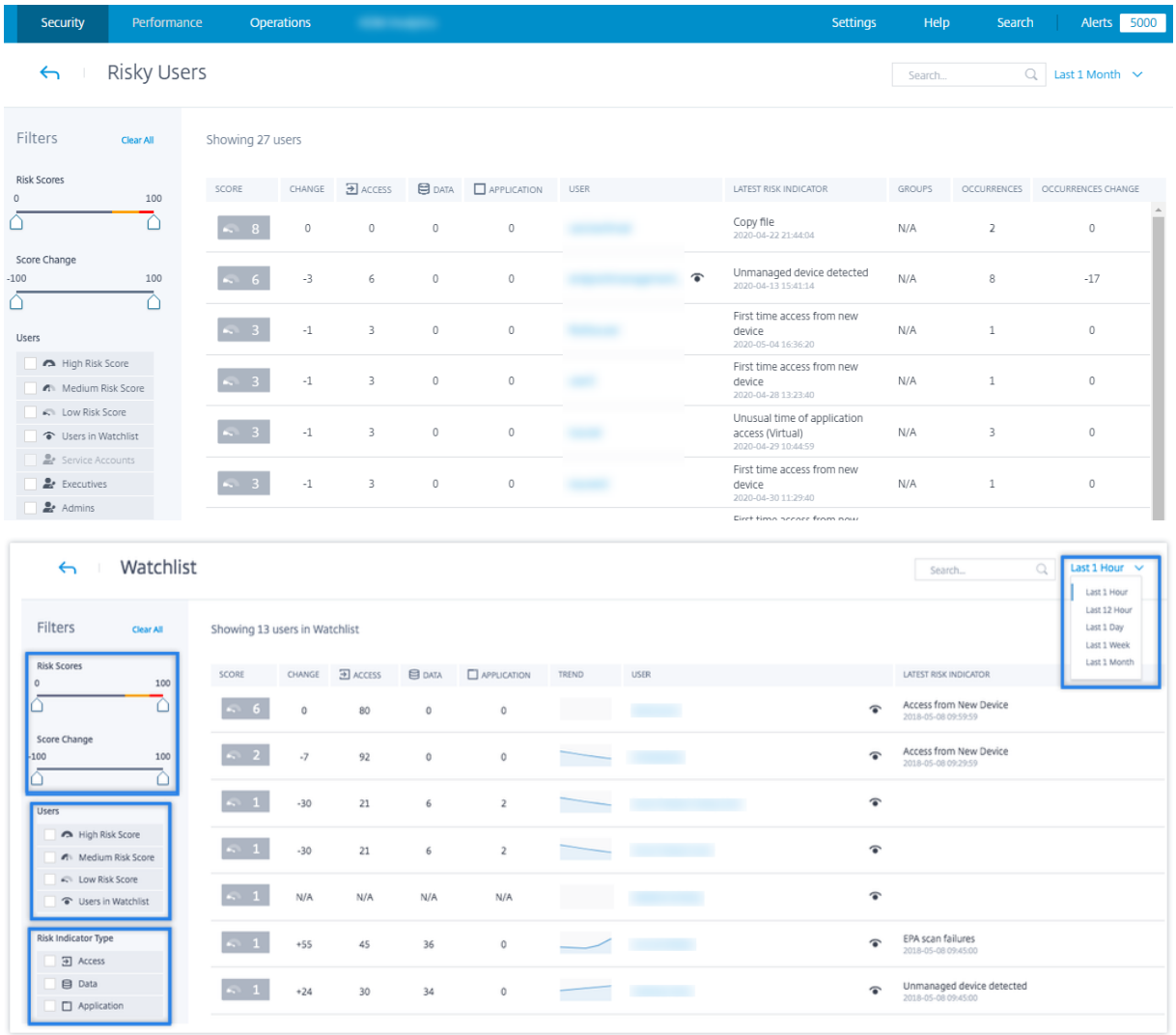
**Alertas** La función **Alertas** está obsoleta y ya no está disponible en la interfaz de usuario de Analytics.




**Página Usuarios con riesgos y lista de seguimiento** Las páginas **Usuarios con riesgos** y **Lista de observación** están obsoletas. Se sustituyen por la página **Usuarios** que resume todos los eventos de

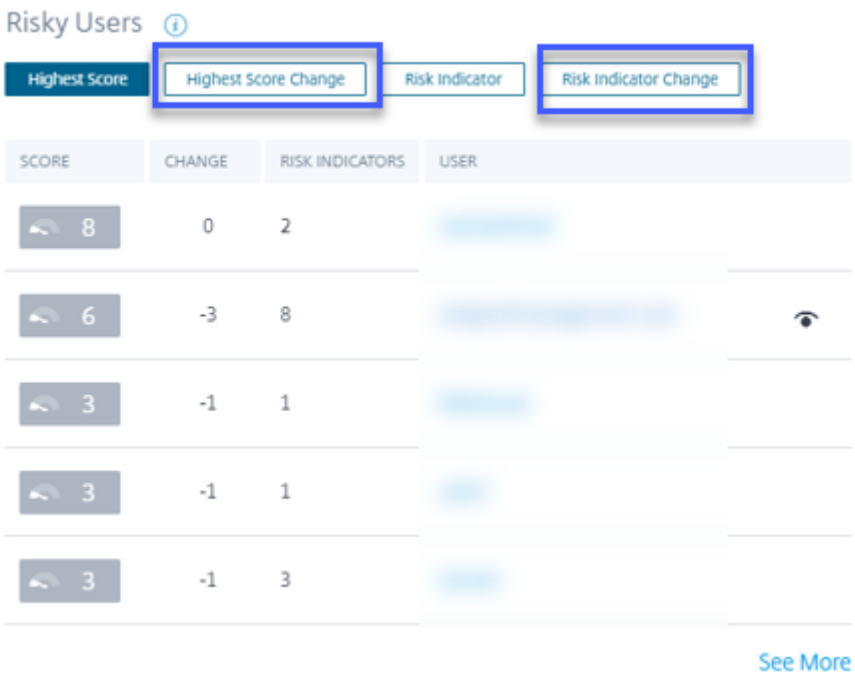
 

usuario de riesgo y los usuarios de la lista de seguimiento.



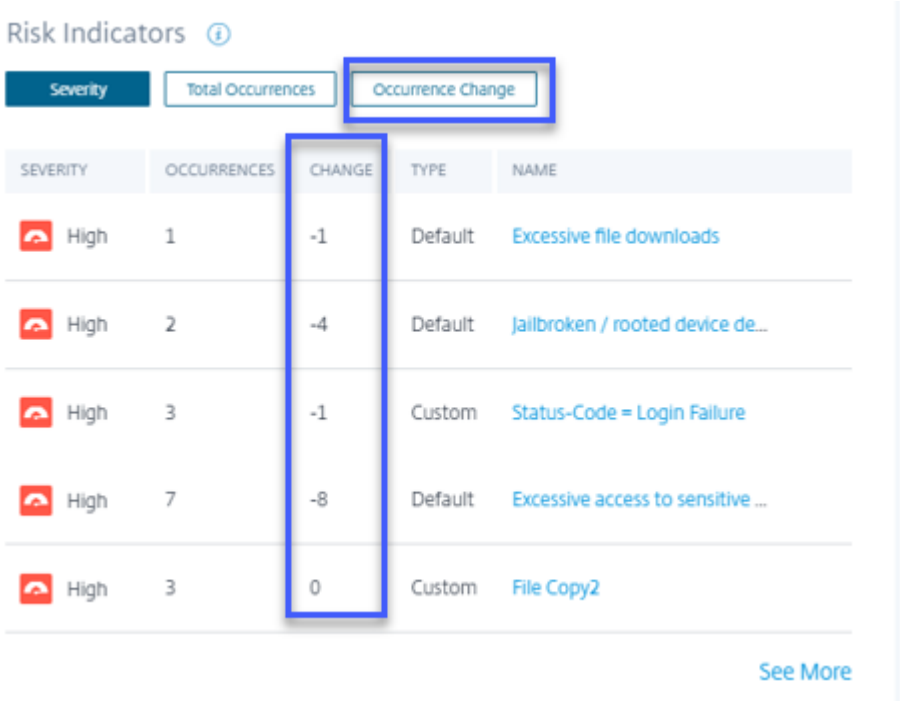

**Panel Usuarios con riesgos** Las fichas **Cambio de puntuación más alta** y **Cambio del indicador de riesgo** se eliminan del panel **Usuarios con riesgos**.




**Panel Indicador de riesgo**

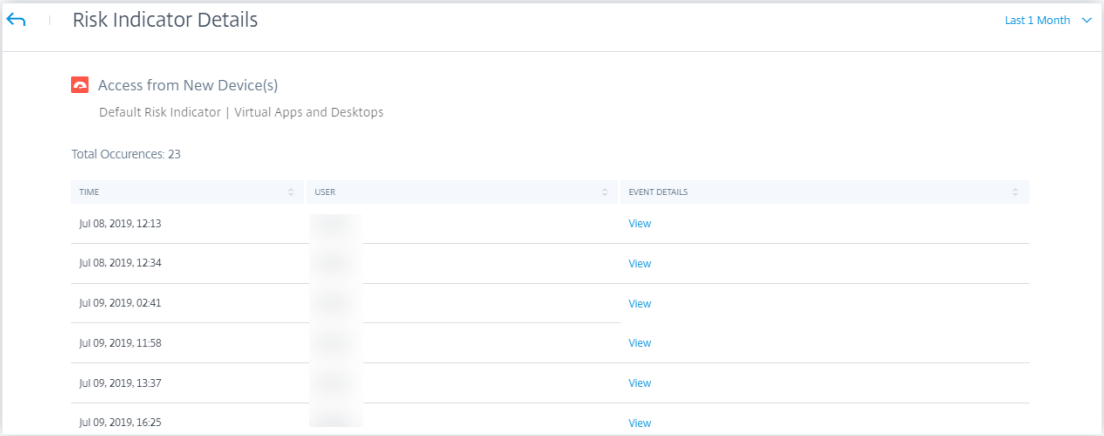
- Se quitan la ficha **Cambio de ocurrencia** y la columna **CAMBIAR**.



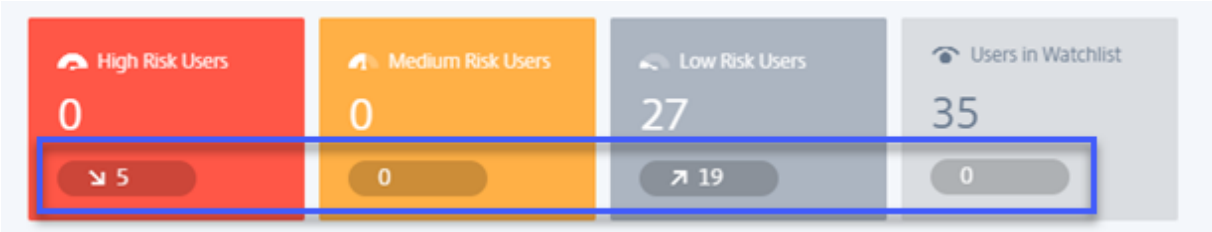

- La página **Detalles del indicador de riesgo** está obsoleta. Anteriormente, esta página se mostraba cuando se seleccionaba un indicador de riesgo en el panel **Indicadores de riesgo** o

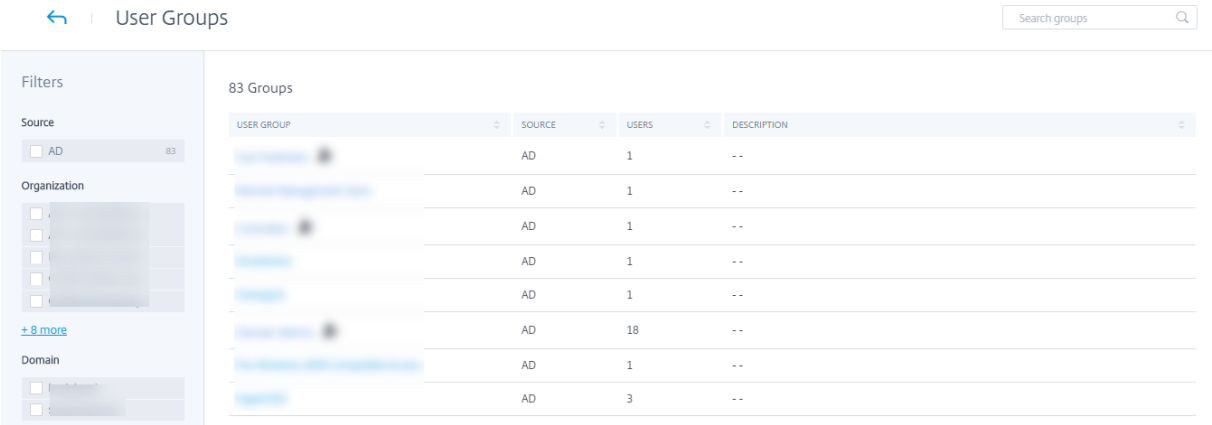
en la página **Visión general de indicadores de riesgo**.




**Vista de tendencias** En el panel **Usuarios**, la vista de tendencias del recuento de usuarios se elimina de las tarjetas **Usuarios de alto riesgo**, **Usuarios de riesgo medio**, **Usuarios de bajo riesgo** y **Usuarios de la lista de seguimiento**.




**Página Grupos de usuarios** La página **Grupos de usuarios** de la opción **Configuración** está obsoleta. Ya no se puede agregar ni quitar un grupo de usuarios como grupo privilegiado. Sin embargo, puede agregar o quitar usuarios individuales como usuarios privilegiados. Para obtener más información, consulte Usuarios con privilegios.



## 26 de junio de 2020

### Funciones retiradas

**Indicadores de riesgo de tiempo inusual de acceso a las aplicaciones (virtual/SaaS) obsoletos**
Los indicadores de riesgo de Citrix Virtual Apps and Desktops: **tiempo inusual de acceso a las aplicaciones (virtual)** y **tiempo inusual de acceso a las aplicaciones (SaaS)** han quedado obsoletos. Solo se pueden ver los datos históricos relacionados con estos indicadores.

Los siguientes cambios se aplican como parte de esta desuso:

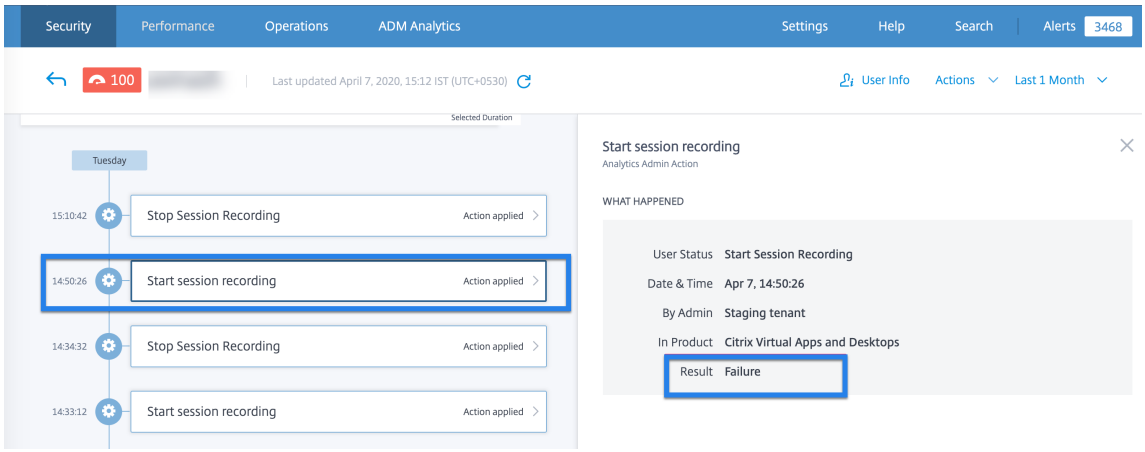
- La analítica ya no genera estos indicadores de riesgo.
- Analytics ya no genera directivas con estos indicadores de riesgo como condiciones.
- Directivas de impago con estos indicadores de riesgo, ya que las condiciones ya no surten efecto.

Para obtener más información, consulte Indicadores de riesgo de Citrix Virtual Apps and Desktops y Citrix DaaS.

## 2 de junio de 2020

### Problemas resueltos

- En el cronograma de riesgo del usuario, el estado de las acciones de Virtual Apps and Desktops (basadas en directivas o aplicadas manualmente) aparece como “Error”aunque las acciones se hayan aplicado correctamente en la cuenta de usuario. Por ejemplo, la acción **Iniciar grabación de sesiones** se aplica correctamente en la cuenta de usuario, pero el resultado se muestra como “Error”. [CAS-32773]



## 11 de mayo de 2020

### Problemas resueltos

- Para algunos usuarios, las acciones basadas en directivas no se desencadenan y no se puede aplicar el modo de aplicación de directivas. Este problema se produce cuando los ID de cliente no están en minúsculas.

  [CAS-34209], [CAS-34141]

- No se pueden crear indicadores de riesgo personalizados para algunos usuarios. Este problema se produce cuando los ID de cliente no están en minúsculas.

  [CAS-34139]

## 29 de abril de 2020

### Problemas resueltos

- Las acciones aplicadas en los indicadores de riesgo de Citrix Virtual Apps and Desktops no surten efecto, aunque Analytics muestra un mensaje indicando que las acciones se han aplicado correctamente. Este problema se observa en la versión 7 1912 de Citrix Virtual Apps and Desktops.

  [CAS-31544]

## 2 de abril de 2020

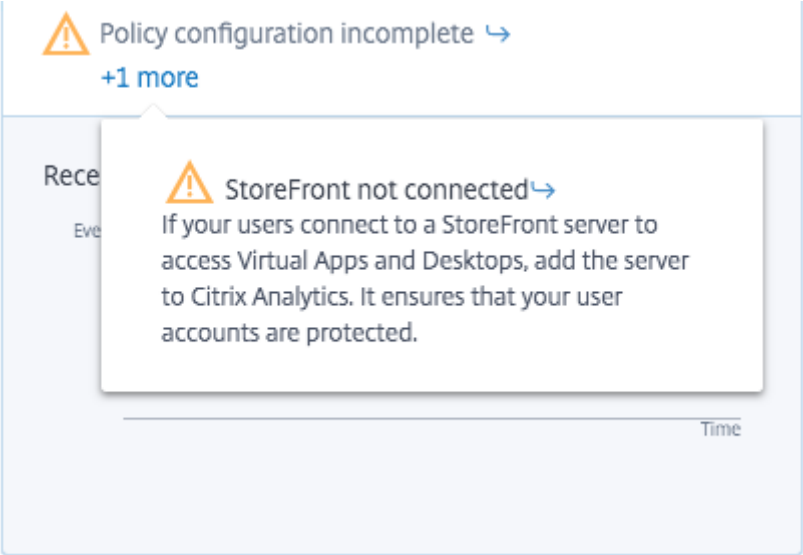
### Funciones nuevas

**Inhabilitar el procesamiento de datos cuando no se agrega StoreFront** En la tarjeta del sitio de origen de datos **Configuración** > **Orígenes de datos** > **Seguridad** > **Virtual Apps and Desktops**, el botón **Activar procesamiento de datos** no se activa si no ha integrado StoreFront. Aparece el mensaje de advertencia de **StoreFront no conectado** en la tarjeta del sitio. Si tiene un sitio local activo desde el que quiere que Analytics reciba datos, debe comprobar que ha incorporado StoreFront en Citrix Analytics. Garantiza que sus cuentas de usuario estén protegidas.

En la tarjeta del sitio **Virtual Apps and Desktops**, seleccione los puntos suspensivos verticales () y haga clic en **Conectar implementación de StoreFront**. En la pantalla que se muestra, siga las instrucciones y complete la configuración de StoreFront.

Para obtener más información, consulte Incorporar sitios locales de Citrix Virtual Apps and Desktops mediante StoreFront.




**Problemas resueltos**

- Para los usuarios de Citrix Content Collaboration, las acciones basadas en directivas no surten efecto en las siguientes condiciones:
  - Cuando se definen las condiciones del indicador de riesgo personalizado
  - Hasta que se genere un indicador de riesgo para un usuario

  [CAS-29226]

## 4 de marzo de 2020

**Problemas resueltos**

- Cuando los usuarios de Gateway se incorporan a Analytics por primera vez, ven el error **Citrix ADC no responde o las credenciales son incorrectas**. Al volver a intentarlo, ven el error El **dispositivo con esta dirección IP ya existe**.

[CAS-31180]

## 20 de febrero de 2020

**Funciones nuevas**

**Oferta de Citrix Analytics para seguridad** Citrix Analytics for Security ya está disponible para suscripciones individuales.

Puede suscribirse a Citrix Analytics for Security y obtener información específica de esta oferta. Para obtener más información, consulte Introducción.

**Panel de control Categorías de riesgo** Citrix Analytics introduce la categorización de los indicadores de riesgo en función de los riesgos que tienen un impacto similar en el aspecto de seguridad de la organización. Este panel proporciona una visión completa de las exposiciones al riesgo y los riesgos críticos que requieren atención inmediata. Para los indicadores de riesgo de impago, Analytics asigna automáticamente una categoría de riesgo en función de la exposición al riesgo. Para los indicadores de riesgo personalizados, debe seleccionar una categoría de riesgo adecuada en función de la exposición al riesgo.

Analytics admite las siguientes categorías de riesgo:

- Exfiltración de datos
- Amenazas internas
- Usuarios comprometidos
- Dispositivos de punto final comprometidos

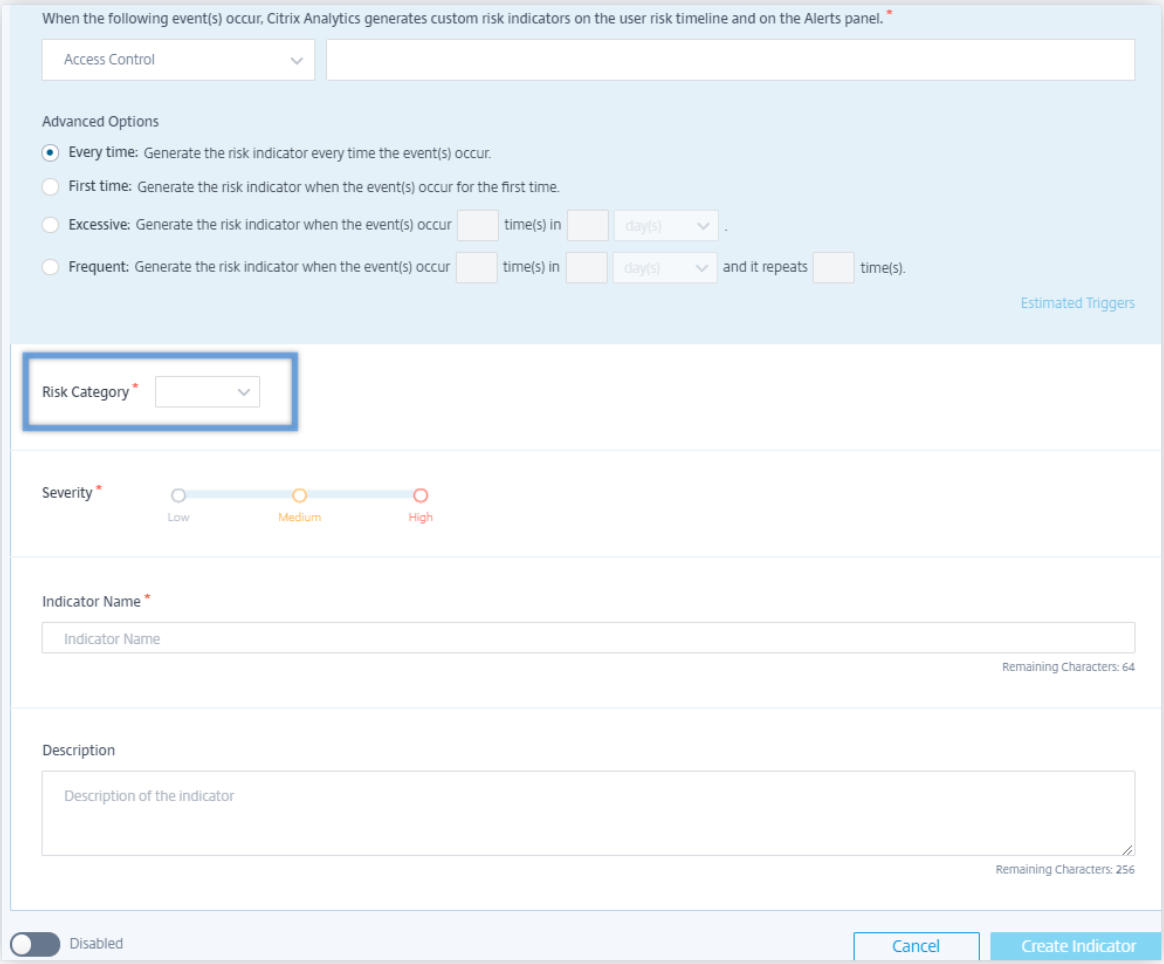
Para obtener más información, consulte Categorías de riesgo.


**Columna Categoría de riesgo de la página Indicadores personalizados** La columna **Categoría de riesgo** se introduce en la página Indicador de riesgo personalizado. Según el tipo de exposición al riesgo, puede seleccionar una categoría de riesgo para su indicador de riesgo personalizado. Los

indicadores de riesgo personalizados creados anteriormente se muestran en el panel de control Categorías de riesgo si los modifica seleccionando una categoría de riesgo.

Para obtener más información, consulte Indicadores de riesgo personalizados.




**Cambio en los nombres de los indicadores de riesgo** Se han cambiado los nombres de los indicadores de riesgo siguientes:

| Origen de datos | Nombre antiguo | Nuevo nombre |
|---|---|---|
| Citrix Virtual Apps and Desktops y Citrix DaaS | Uso inusual de aplicaciones (virtual) | Tiempo inusual de acceso a las aplicaciones (virtual) |
| Citrix Virtual Apps and Desktops y Citrix DaaS | Uso inusual de aplicaciones (SaaS) | Tiempo inusual de acceso a las aplicaciones (SaaS) |
| Citrix Content Collaboration | Errores de inicio de sesión excesivos | Fallos de autenticación excesivos |

| Origen de datos | Nombre antiguo | Nuevo nombre |
|---|---|---|
| Citrix Content Collaboration | Acceso de inicio de sesión inusual | Acceso por primera vez desde una nueva ubicación |
| Citrix Access Control | Volumen de descarga inusual | Descarga excesiva de datos |
| Citrix Gateway | Errores de inicio de sesión | Fallos de autenticación excesivos |
| Citrix Gateway | Errores de autorización | Fallos excesivos de autorización |
| Citrix Gateway | Acceso de inicio de sesión inusual | Acceso por primera vez desde una nueva ubicación |

Para obtener más información, consulte Indicadores de riesgo.

**Problemas resueltos**

- Para algunos usuarios, Citrix Analytics no puede recibir datos de Virtual Apps and Desktops aunque el origen de datos se haya integrado correctamente y StoreFront esté habilitado. [CAS-24134]
- Citrix Analytics no puede recibir eventos de descarga de Citrix Content Collaboration. Por lo tanto, no se activan los siguientes indicadores de riesgo:
  - Descarga compartida confidencial anónima
  - Descargas excesivas de enlaces compartidos
  - Acceso excesivo a archivos confidenciales
  - Descargas excesivas de archivos

  [CAS-29207]
- Para los usuarios recién incorporados, las acciones manuales y basadas en directivas aplicadas en los indicadores de riesgo de Citrix Gateway no surten efecto alguno. [CAS-29029]
- Algunos usuarios no pueden ver las tarjetas de sitio en la página Orígenes de datos. Este problema se resuelve rellenando de nuevo la caché. [CAS-28781]

## 9 de enero de 2020

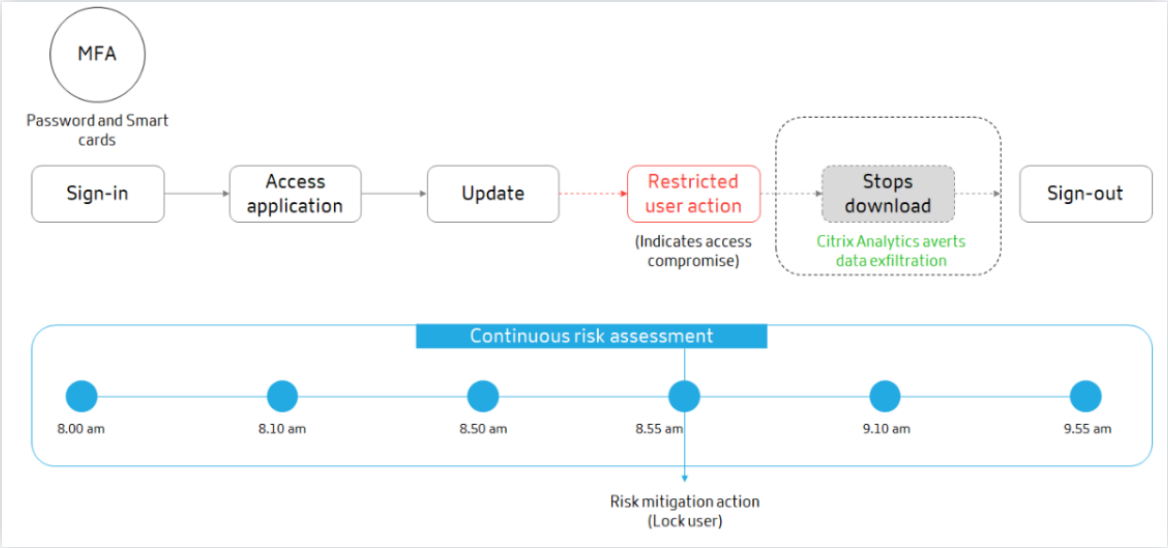
### Funciones nuevas

**Evaluación continua del riesgo** Algunos desafíos a los que se enfrentan los usuarios de Citrix Workspace son que el acceso remoto expone los datos confidenciales a riesgos de seguridad a través de actividades cibernéticas como la exfiltración de datos, el robo, el vandalismo y las interrupciones del servicio. También es probable que los empleados de las organizaciones contribuyan a este daño.

Algunas formas de abordar estos riesgos son implementar la autenticación multifactor, aplicar tiempos de espera de inicio de sesión cortos, etc. Aunque estos métodos de evaluación de riesgos garantizan un mayor nivel de seguridad, no proporcionan una seguridad completa tras la validación inicial.

Para mejorar el aspecto de la seguridad y garantizar una mejor experiencia de usuario, Citrix Analytics presenta la solución de evaluación continua de riesgos. Esta solución le ayuda a supervisar continuamente los perfiles de usuario y a realizar diversas acciones cuando se detectan eventos de riesgo.

Para obtener más información, consulte Evaluación continua de riesgos.



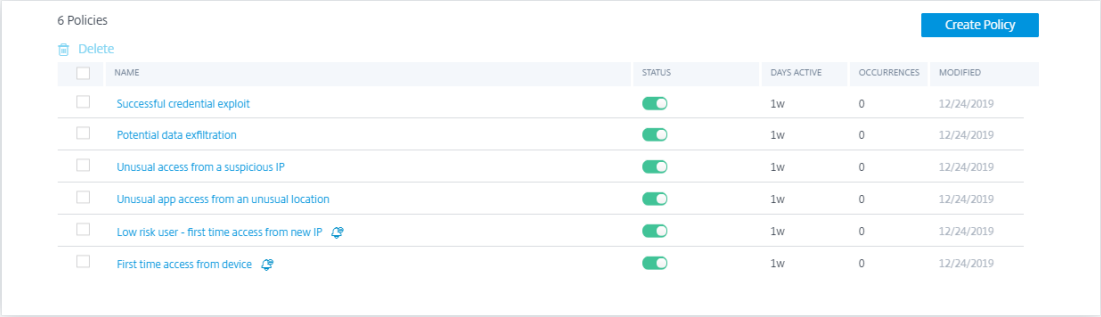

**Configuración de directivas** Citrix Analytics le ayuda a administrar las configuraciones de directivas de forma más eficaz. Puede proteger las cuentas de usuario de ataques maliciosos con la ayuda de las siguientes capacidades:

- **Directivas predeterminadas**: Citrix Analytics admite las siguientes directivas predeterminadas:
  - Explotación de credenciales correcta
  - Exfiltración potencial de datos

- Acceso inusual desde una IP sospechosa
- Acceso inusual a aplicaciones desde una ubicación inusual
- Usuario de bajo riesgo: acceso por primera vez desde una nueva IP
- Acceso por primera vez desde el dispositivo

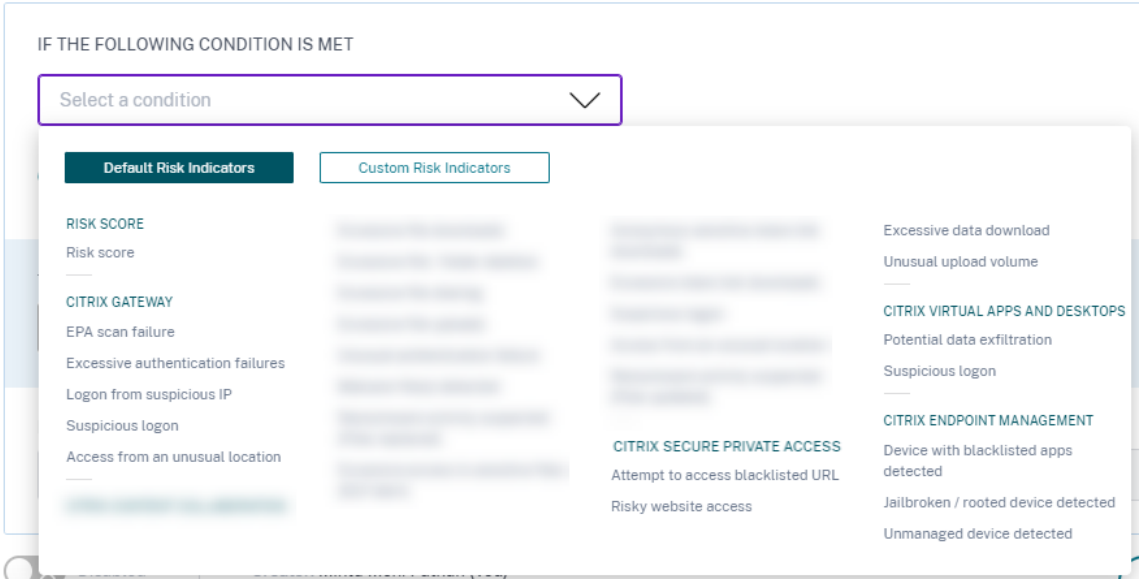
Puede modificar las directivas predeterminadas según sus requisitos.



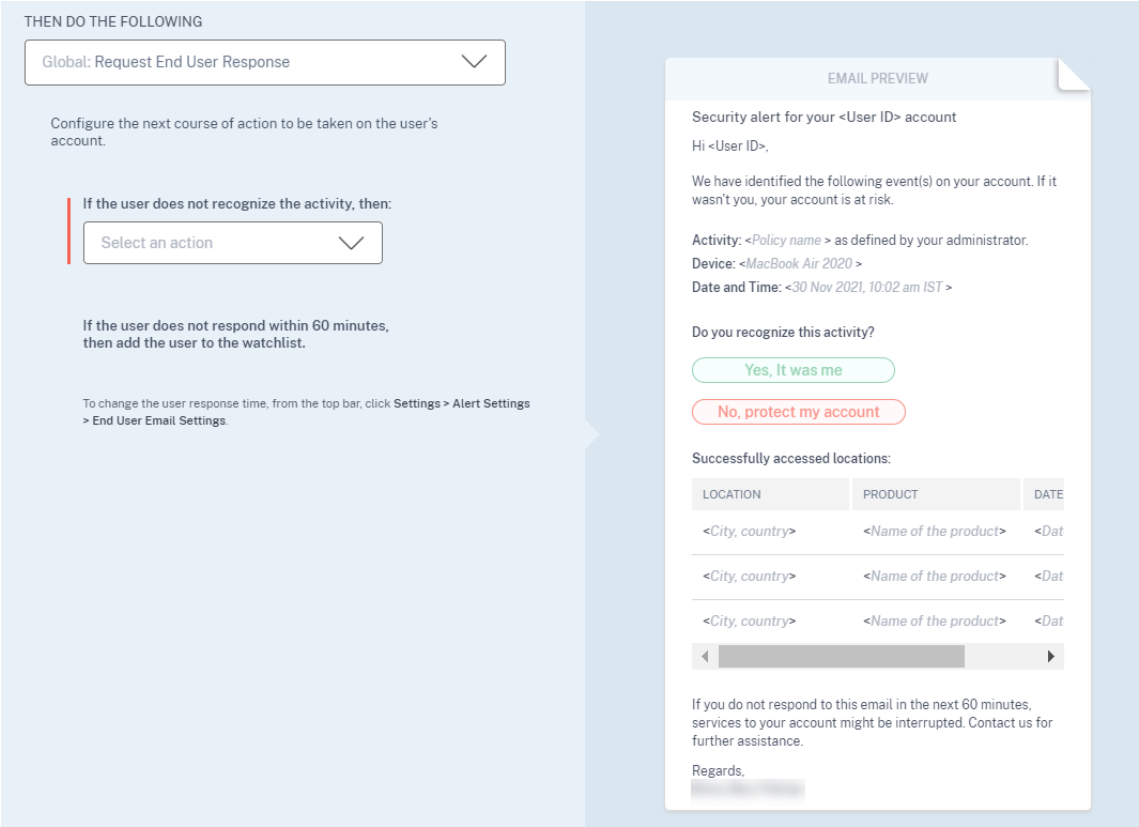

- **Múltiples condiciones**: una directiva puede contener hasta cuatro condiciones. Las condiciones se pueden establecer con combinaciones de puntuaciones de riesgo e indicadores de riesgo, o ambos.


- **Indicadores de riesgo predeterminados y personalizados**: El menú de condiciones de la página **Crear Directiva** ahora está segregado en función de los indicadores de riesgo predeterminados y personalizados. Al crear una directiva, puede cambiar entre las fichas de indicadores de riesgo predeterminados y personalizados, y establecer las condiciones del indicador de riesgo.

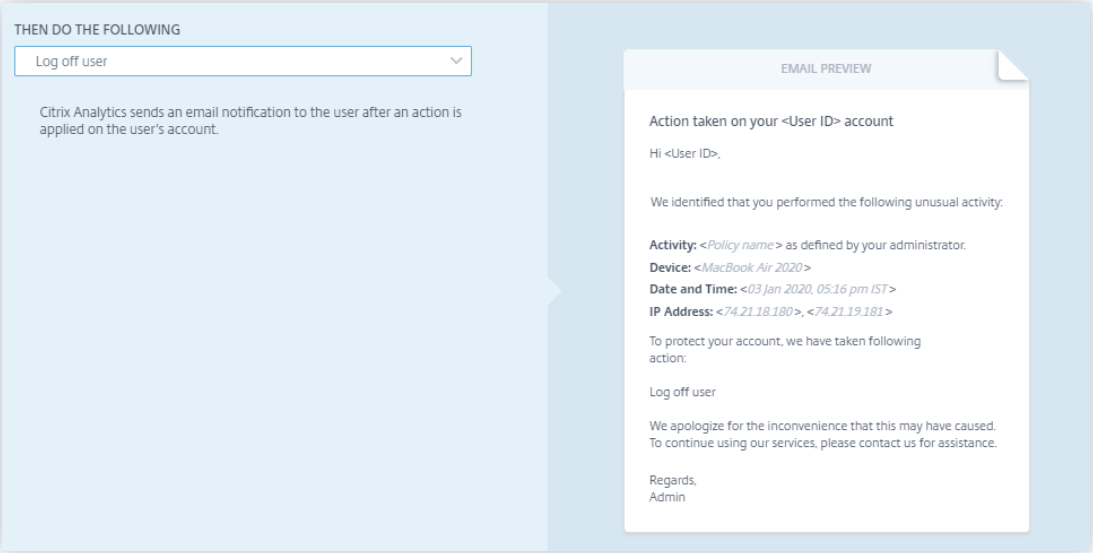



- **Solicitar respuesta del usuario final**: Citrix Analytics presenta la acción **Solicitar respuesta del usuario final**. Con esta acción, puede enviar una notificación por correo electrónico al usuario sobre la actividad de riesgo detectada. Una vez que el usuario responda sobre la actividad, puede determinar el siguiente curso de acción que se tomará en su cuenta. También puede configurar el tiempo de respuesta del usuario. Si no se recibe ninguna respuesta, Citrix Analytics considera el estado **Sin respuesta**.

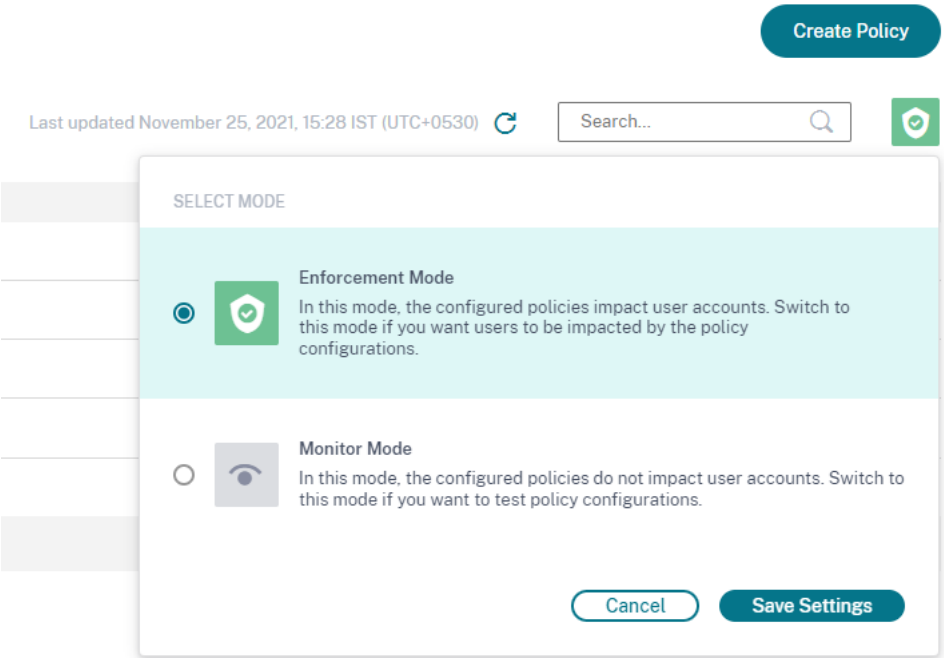


- **Aplicar acciones disruptivas**: puede notificar a los usuarios cuando se aplica una acción disruptiva, como **Cerrar sesión** o **Bloquear usuario**. Se envía una notificación al usuario con detalles de la actividad y la acción aplicada. Esta acción interrumpe temporalmente los servicios de la cuenta del usuario para evitar un uso indebido posterior. Para continuar accediendo a la cuenta, el usuario debe ponerse en contacto con el administrador para obtener ayuda.




- **Modos de cumplimiento y supervisión**: Puede establecer modos de cumplimiento o supervisión para sus directivas.




Para obtener más información sobre las mejoras de directivas, consulte Directivas y acciones.

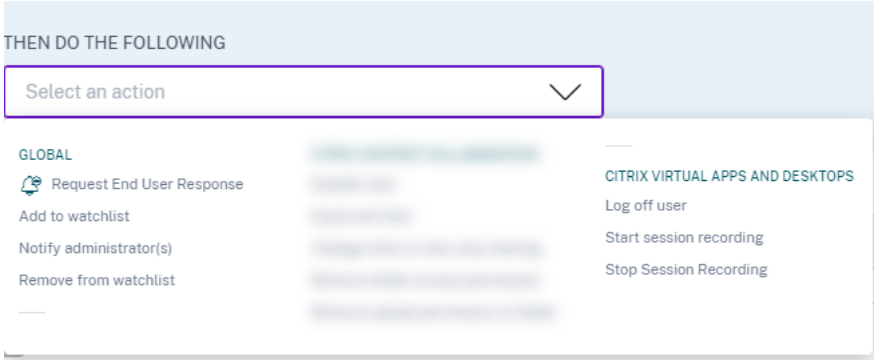
 

**Bloquear acciones de usuario y desbloquear usuario** Citrix Analytics presenta las siguientes acciones de puerta de enlace:

- Bloquear usuario
- Desbloquear usuario

Puede aplicar estas acciones de forma manual o al configurar directivas.

Para obtener más información, consulte Qué son las acciones.



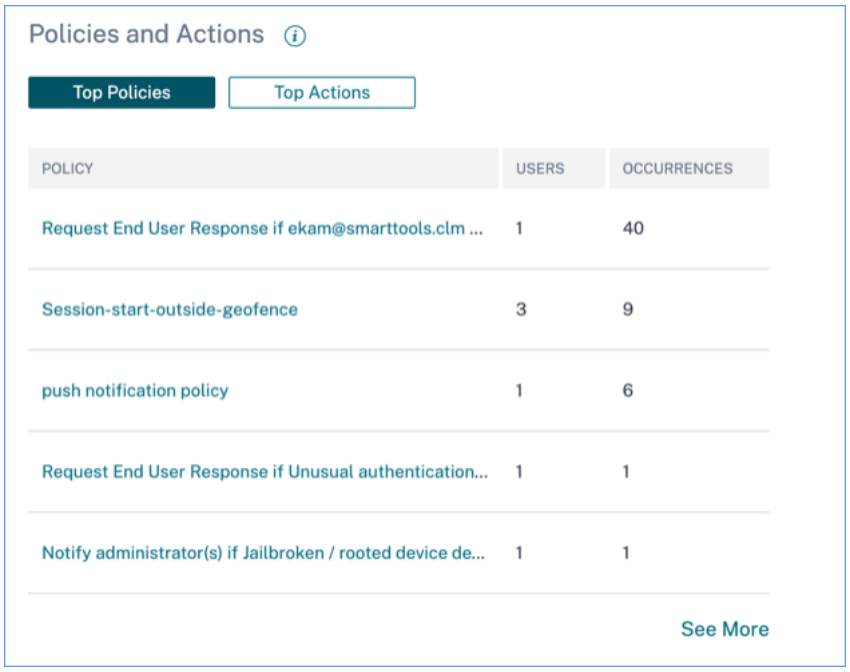

**Panel de resumen de acceso** Citrix Analytics presenta el panel **Resumen de acceso** en el panel **Usuarios**. Resume el número total de intentos que han realizado los usuarios para acceder a los recursos de una organización.

Para obtener más información, consulte Resumen de Access.

**Panel de directivas y acciones** Citrix Analytics presenta el panel **Directivas y acciones** en el panel **Usuarios**. Muestra las cinco directivas y acciones principales aplicadas en los perfiles de usuario. Puede ordenar los datos según las directivas principales y las acciones principales durante un período de tiempo seleccionado.

Para obtener más información, consulte Directivas y acciones.




**Búsqueda de directivas de autoservicio** Utilice la búsqueda de autoservicio para ver los eventos de usuario que cumplen las directivas definidas. También puede ver las acciones que Analytics ha aplicado para estos eventos anómalos. Utilice las facetas y el cuadro de búsqueda para buscar los eventos necesarios.

Para ver los eventos, en el cuadro de búsqueda, seleccione **Directivas** de la lista, seleccione el período de tiempo y, a continuación, haga clic en **Buscar**.

Para obtener más información, consulte Búsqueda de autoservicio de directivas.

### Funciones retiradas

**Se eliminó la condición basada en directivas de cambio de puntuación de riesgo** Al configurar directivas, ya no puede utilizar la condición basada en directivas de **cambio de puntuación de riesgo**. Citrix Analytics no admite esta condición.

Para obtener más información, consulte Directivas y acciones.

**Se han eliminado varias acciones basadas en directivas** Al configurar directivas, ya no se pueden aplicar varias acciones. Citrix Analytics admite solo una acción para cada directiva.

Para obtener más información, consulte Directivas y acciones.

#### Problemas resueltos

- Los administradores delegados de solo lectura encuentran un error al acceder a los paneles de control **Acceso de usuario** y **Acceso a aplicaciones**. [CAS-16297]

### 12 de diciembre de 2019

#### Funciones nuevas

**Compatibilidad con la versión de Splunk** Citrix Analytics admite las siguientes versiones de Splunk:

- **Splunk 8.0 de 64 bits**
- **Splunk 7.3 de 64 bits**

Para obtener los máximos beneficios de seguridad de la integración de Splunk, actualice a la última versión de la aplicación complementaria de Splunk desde la página de descargas.

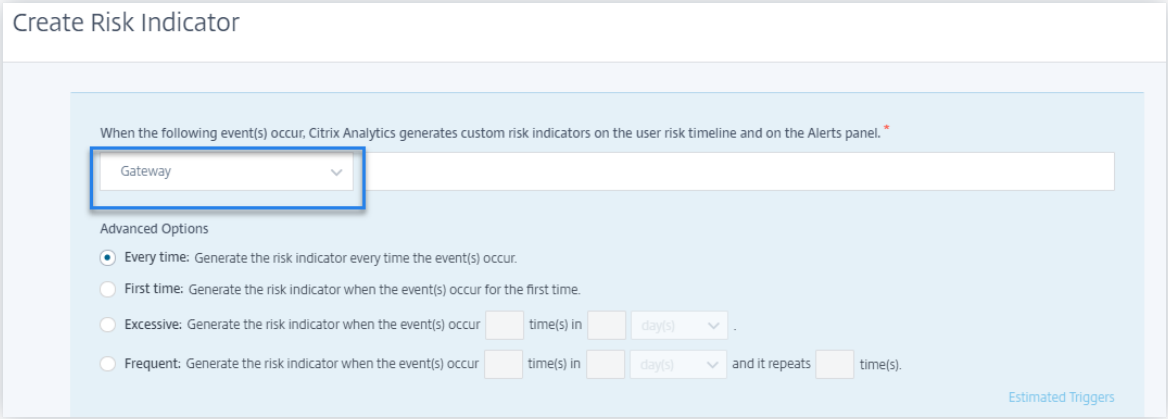
Para obtener más información sobre las versiones de Splunk compatibles, consulte Versiones compatibles.

### 04 diciembre 2019

#### Funciones nuevas

**Indicador de riesgo personalizado para Citrix Gateway** Con los indicadores de riesgo personalizados, ahora puede definir las condiciones y la frecuencia de activación de los indicadores de riesgo de los eventos de Citrix Gateway. Cuando un evento de usuario cumple las condiciones, Analytics activa los indicadores de riesgo. Para obtener más información sobre cómo crear un indicador de riesgo personalizado, consulte Indicadores de riesgo personalizados.

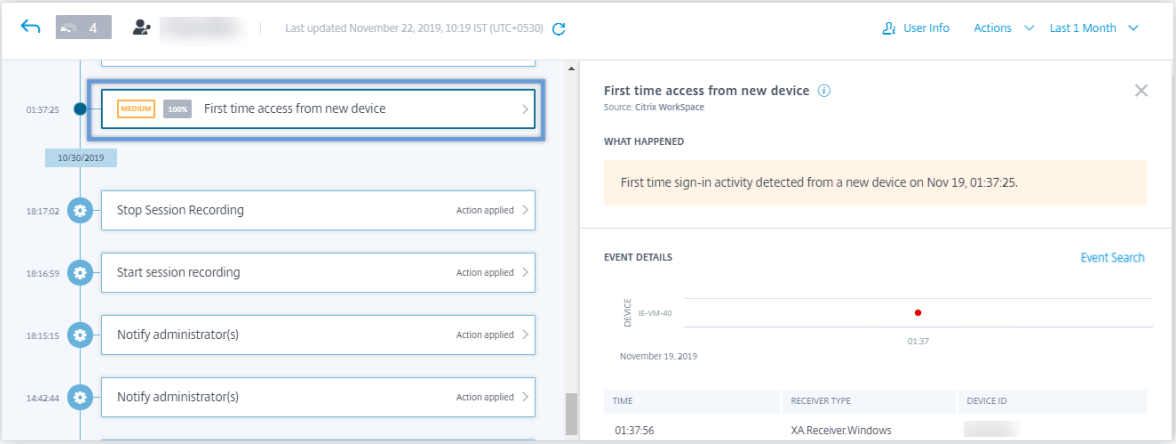



## 22 noviembre 2019

### Funciones nuevas

**Acceso por primera vez desde un dispositivo nuevo: indicador de riesgo de Citrix Virtual Apps and Desktops** Citrix Analytics detecta las amenazas de acceso en función del acceso desde un nuevo dispositivo y activa el indicador de riesgo correspondiente.

El indicador de riesgo **de acceso por primera vez desde un dispositivo nuevo** se activa cuando un usuario inicia sesión desde un dispositivo después de 90 días. Este evento se desencadena porque Citrix Receiver no tiene registros de inicio de sesión de este dispositivo nuevo o desconocido durante los últimos 90 días. Para obtener más información, consulte Indicadores de riesgo de Citrix Virtual Apps and Desktops y Citrix DaaS.



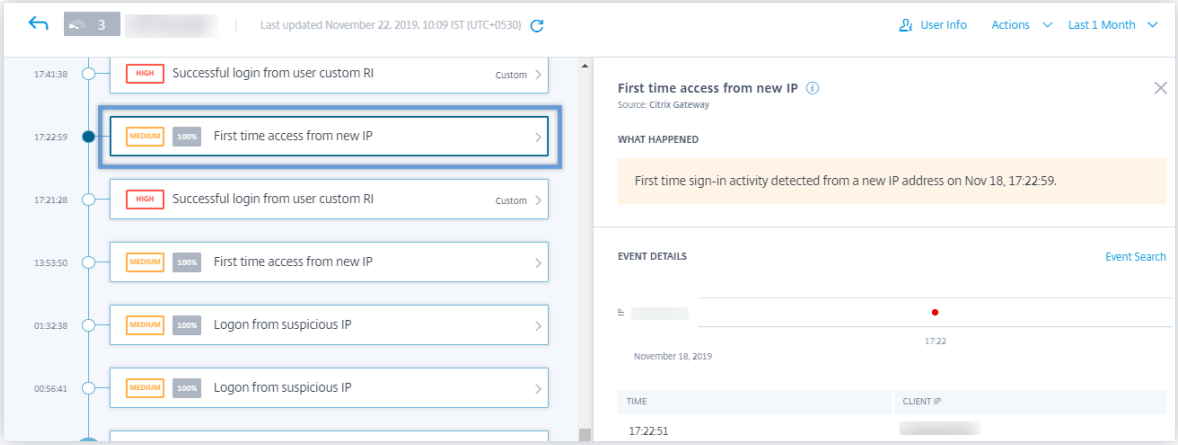

**Acceso por primera vez desde una nueva IP - Indicador de riesgo de Citrix Gateway** Citrix Analytics detecta las amenazas de acceso en función del acceso desde una nueva dirección IP y activa el

indicador de riesgo correspondiente.

El indicador de riesgo **de acceso por primera vez desde una nueva IP** se activa cuando un usuario inicia sesión desde una dirección IP después de 90 días. Este evento se desencadena porque Citrix Receiver no tiene registros de inicio de sesión de la dirección IP nueva o desconocida durante los últimos 90 días.

Para obtener más información, consulte Indicadores de riesgo de Citrix Gateway.



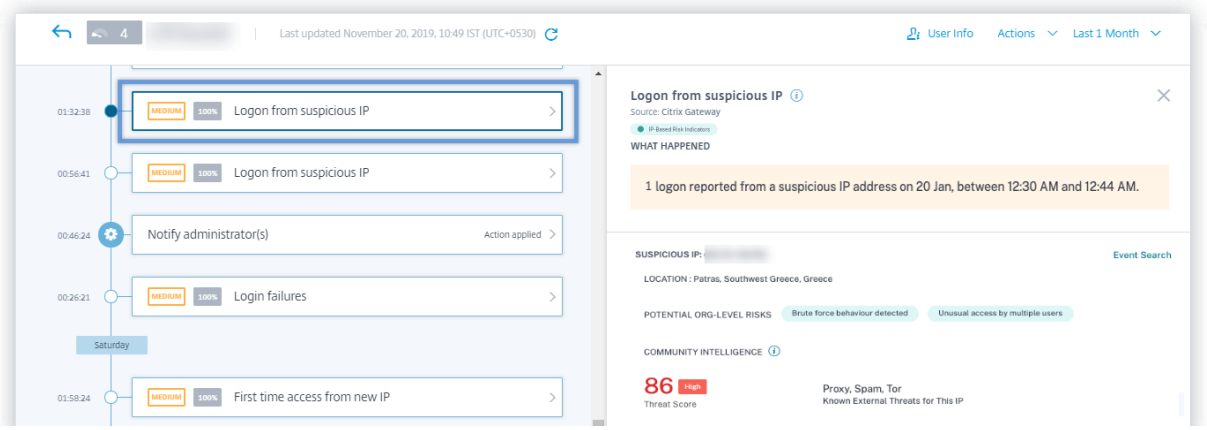

**Inicio de sesión desde una IP sospechosa: indicador de riesgo de Citrix Gateway** Citrix Analytics detecta las amenazas de acceso de los usuarios en función de la actividad de inicio de sesión de IP sospechosa y activa el indicador de riesgo de inicio de **sesión desde IP sospechosa**.

Este indicador de riesgo se activa cuando un usuario intenta acceder a la red desde una dirección IP sospechosa. Analytics considera que una dirección IP es sospechosa en función de cualquiera de las siguientes condiciones:

- Aparece en la fuente externa de inteligencia de amenazas IP
- Tiene varios registros de inicio de sesión de usuarios desde una ubicación inusual
- Tiene intentos de inicio de sesión fallidos excesivos que podrían indicar un ataque de fuerza bruta

Para obtener más información, consulte Indicadores de riesgo de Citrix Gateway.




**Búsqueda de autoservicio de eventos de Citrix Gateway** Utilice la función de búsqueda de autoservicio para obtener información sobre los eventos de usuario recibidos del origen de datos de Citrix Gateway. Citrix Analytics recibe eventos como la etapa de autenticación, el tipo de autorización, el código de sesión VPN y el estado de la sesión VPN para los usuarios de Citrix Gateway. Utilice las facetas y el cuadro de búsqueda para buscar los eventos necesarios y explorar los datos subyacentes.

Para ver los eventos, en el cuadro de búsqueda, seleccione **Puerta de enlace** en la lista, seleccione el período de tiempo y, a continuación, haga clic en **Buscar**.

Para obtener más información, consulte Búsqueda de autoservicio de Gateway.

**Búsqueda de autoservicio de eventos de Citrix Remote Browser Isolation** Utilice la función de búsqueda de autoservicio para obtener información sobre los eventos de navegación recibidos de Citrix Remote Browser Isolation Service. Citrix Analytics recibe eventos como conexión de sesión, inicio de sesión, aplicaciones publicadas y aplicaciones eliminadas para cada conexión de usuario. Utilice el cuadro de búsqueda para buscar los eventos necesarios y explorar los datos subyacentes.

Para ver los eventos, en el cuadro de búsqueda, seleccione **Remote Browser Isolation** en la lista, seleccione el período de tiempo y, a continuación, haga clic en **Buscar**.

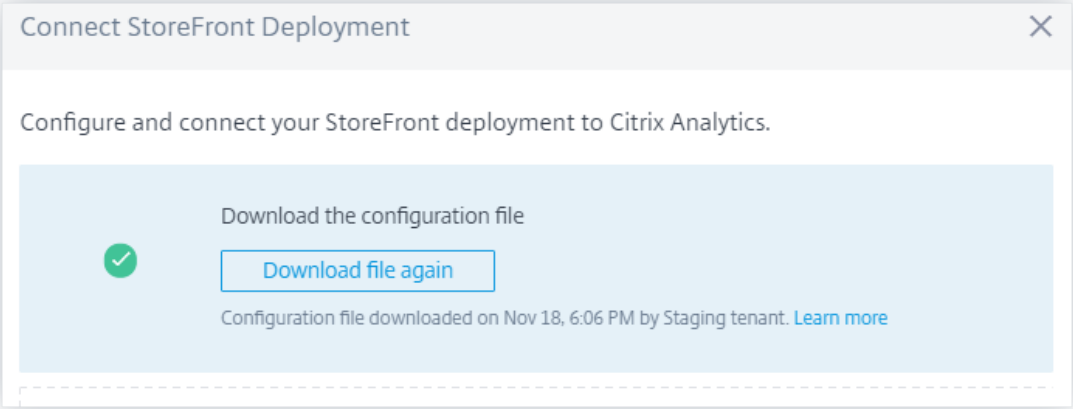
Para obtener más información, consulte Búsqueda de autoservicio para Remote Browser Isolation.

**Acción Eliminar de la lista de observación** Puede quitar a un usuario de la lista de seguimiento aplicando el método manual o aplicando un método basado en directivas. Para obtener más información, consulte Lista de seguimiento.

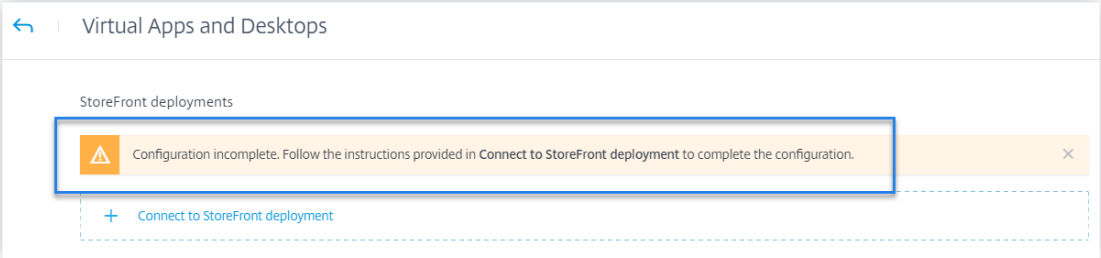
**Mensajes de incorporación mejorados al configurar una implementación de StoreFront** Citrix Analytics ahora proporciona los siguientes mensajes para ayudarle a configurar las implementaciones de StoreFront:

- Tras descargar el archivo de configuración, puede ver un mensaje que indica la fecha y hora de la descarga y el nombre de usuario. Al actualizar esta página, el botón **Descargar archivo** cambia de **nuevo a Descargar archivo**.




- Si la configuración de StoreFront está incompleta, aparece un mensaje de advertencia en el que se le indica que debe seguir los pasos de configuración y conectar la implementación de StoreFront con Analytics.




Para obtener más información sobre cómo configurar la implementación de StoreFront, consulte Incorporar sitios locales de Citrix Virtual Apps and Desktops mediante StoreFront.

### Funciones retiradas

**Indicador de riesgo: eliminar el acceso desde un dispositivo nuevo** Citrix Analytics ya no activa el indicador de riesgo **Acceso desde un nuevo dispositivo**. Sin embargo, en el panel de control del usuario, el cronograma del usuario y el panel de directivas, puede ver los datos históricos relacionados con este indicador de riesgo.

Para las directivas creadas anteriormente basadas en **Acceso desde un nuevo dispositivo**, debe modificar la directiva o crear una directiva con el nuevo indicador de riesgo **Acceso por primera vez desde un dispositivo nuevo**.

### Problemas resueltos

- La búsqueda autoservicio de autenticación no muestra los eventos. [CAS-24959]

## 08 noviembre 2019

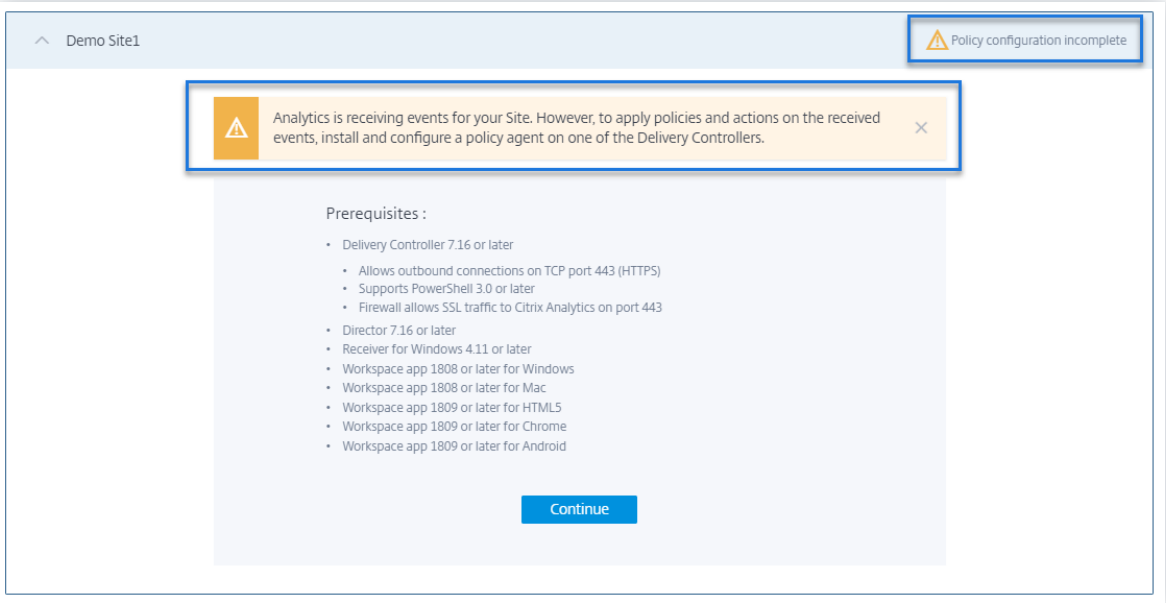
### Problemas resueltos

- Para los indicadores de riesgo de Citrix Content Collaboration, los usuarios no pueden aplicar acciones en el cronograma de riesgos. [CAS-24844]
- La aplicación Citrix Workspace para Chrome anterior a la versión 1911 no envía los detalles del evento a Citrix Analytics. [CAS-24938]

## 21 de octubre de 2019

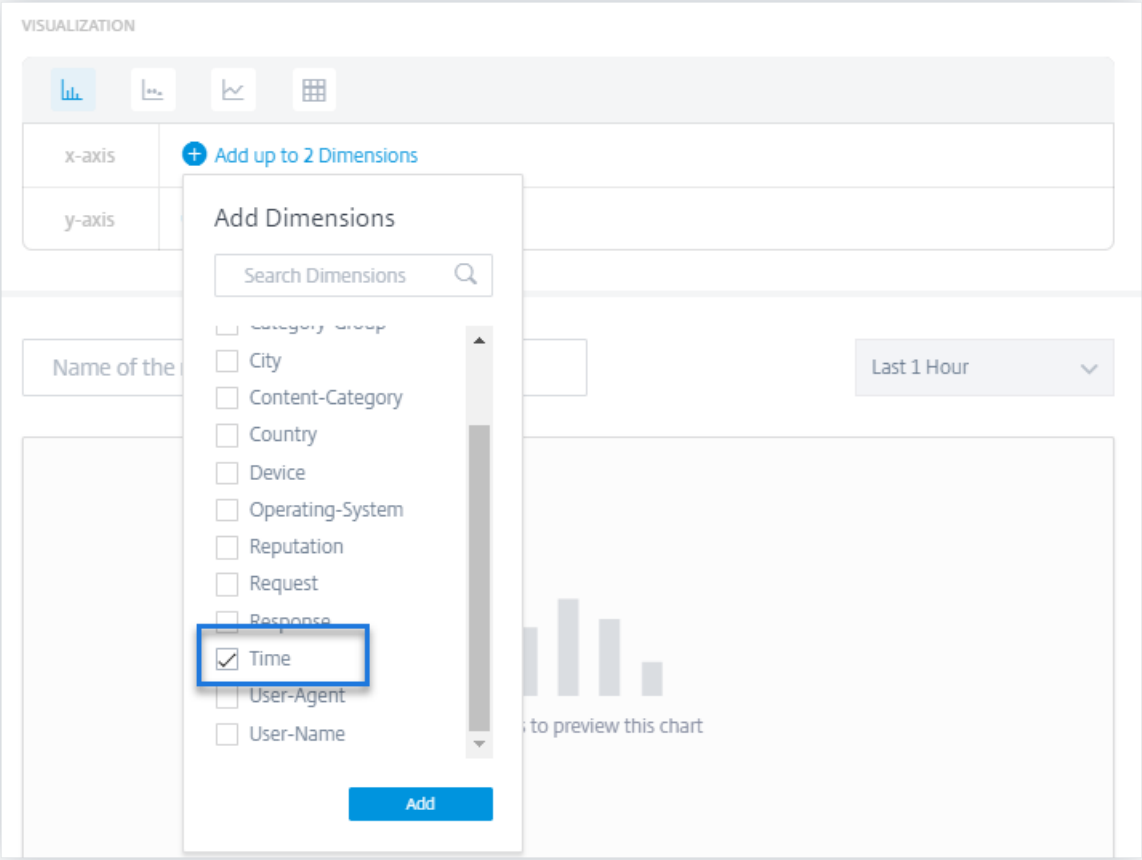
### Funciones nuevas

**Nombre modificado del agente de análisis** El nombre del agente se menciona ahora como **agente de directivas de Analytics** en las interfaces de usuario para indicar su función. Al incorporar los orígenes de datos de Citrix Virtual Apps and Desktops locales, Citrix Analytics notifica claramente que solo se necesita un agente de directivas para configurar directivas y acciones para su sitio. Este agente no tiene ninguna función en la transmisión de datos desde el origen de datos. Para obtener más información, consulte Origen de datos de Citrix Virtual Apps and Desktops y Citrix DaaS.



**Compatibilidad con la dimensión temporal para informes personalizados** Ahora puede agrupar los eventos en función del tiempo seleccionando la dimensión de **tiempo** para el eje x. El informe muestra el total de eventos recibidos en función de los intervalos de tiempo del período seleccionado. Para obtener más información sobre cómo crear informes, consulte Informes personalizados.

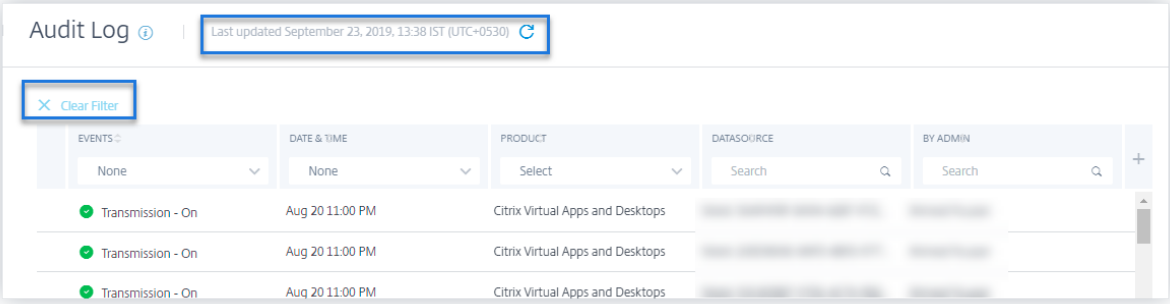



**Mejoras en los registros de auditoría** Se ha mejorado la experiencia del usuario de la página **Registro de auditoría**.

- Puede ver los detalles de fecha y hora de la última actualización de la página **Registro de auditoría** y actualizar la página para ver los registros de auditoría más recientes.
- Puede borrar todos los filtros aplicados en los registros de auditoría.

Para obtener más información sobre los datos de auditoría, consulte Registros de auditoría.




### Problemas resueltos

- Citrix Analytics no puede generar el indicador de riesgo de **direcciones IP anónimas** aunque Microsoft Graph Security se haya incorporado correctamente. [CAS-21329]
- La aplicación Citrix Workspace para HTML5 anterior a la versión 1910 no envía los detalles del evento a Citrix Analytics. [CAS-24938]

## 23 de septiembre de 2019

### Problemas resueltos

- En las tarjetas de sitio de orígenes de datos, el campo **Último evento** muestra información de fecha y hora incorrecta. [CAS-24087]

## 30 de agosto de 2019

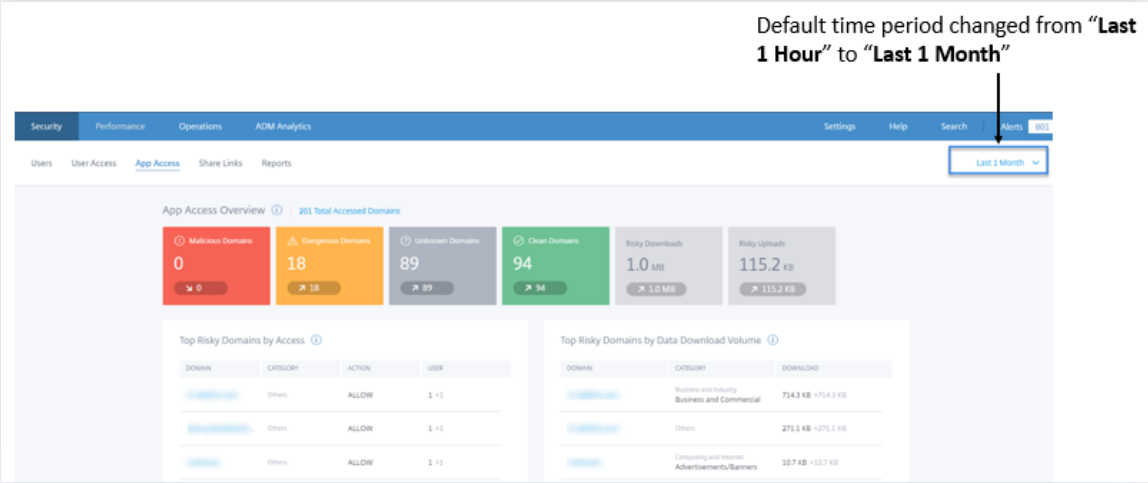
### Funciones nuevas

**Cambio en el período de tiempo predeterminado en todos los paneles** El período de tiempo predeterminado de los paneles siguientes cambia de **Última hora** a **Último mes**:

- Usuarios
- Cronología del riesgo
- Acceso de usuarios
- Acceso a aplicaciones
- Compartir enlaces
- Historial de alertas

Ahora los paneles muestran los eventos del último mes de forma predeterminada. Obtendrá una experiencia más atractiva al utilizar estos paneles. Por ejemplo, al abrir el panel de control **Acceso a aplicaciones**, el panel muestra los eventos de acceso a aplicaciones del último mes de forma predeterminada.




### Problemas resueltos

- Para los indicadores de riesgo de Content Collaboration, la acción **Inhabilitar basada en directivas de usuario** no se puede aplicar correctamente. [CAS-17304]
- Citrix Analytics no puede procesar eventos de Citrix Gateway 13.0. Este problema se produce porque Citrix Gateway 13.0 no proporciona nombres de usuario en los eventos de inicio de sesión enviados a Citrix Analytics. [CAS-21339]

## 20 de agosto de 2019

### Funciones nuevas

#### Mejoras en la búsqueda de autoservicio

- Se ha mejorado la experiencia del usuario de la página de autoservicio. Ahora puede cambiar sin problemas entre el cronograma de riesgo del usuario y la página de búsqueda de autoservicio.
- Ahora puede ordenar sus eventos por tiempo. De forma predeterminada, los últimos eventos aparecen en primer lugar en la tabla de eventos. Haga clic en el icono de ordenación de la columna **TIEMPO** para ordenar los eventos según la última hora o la hora más temprana.

Para obtener más información sobre cómo utilizar la búsqueda de autoservicio, consulte Búsqueda de autoservicio.

**Mejoras en los informes personalizados**

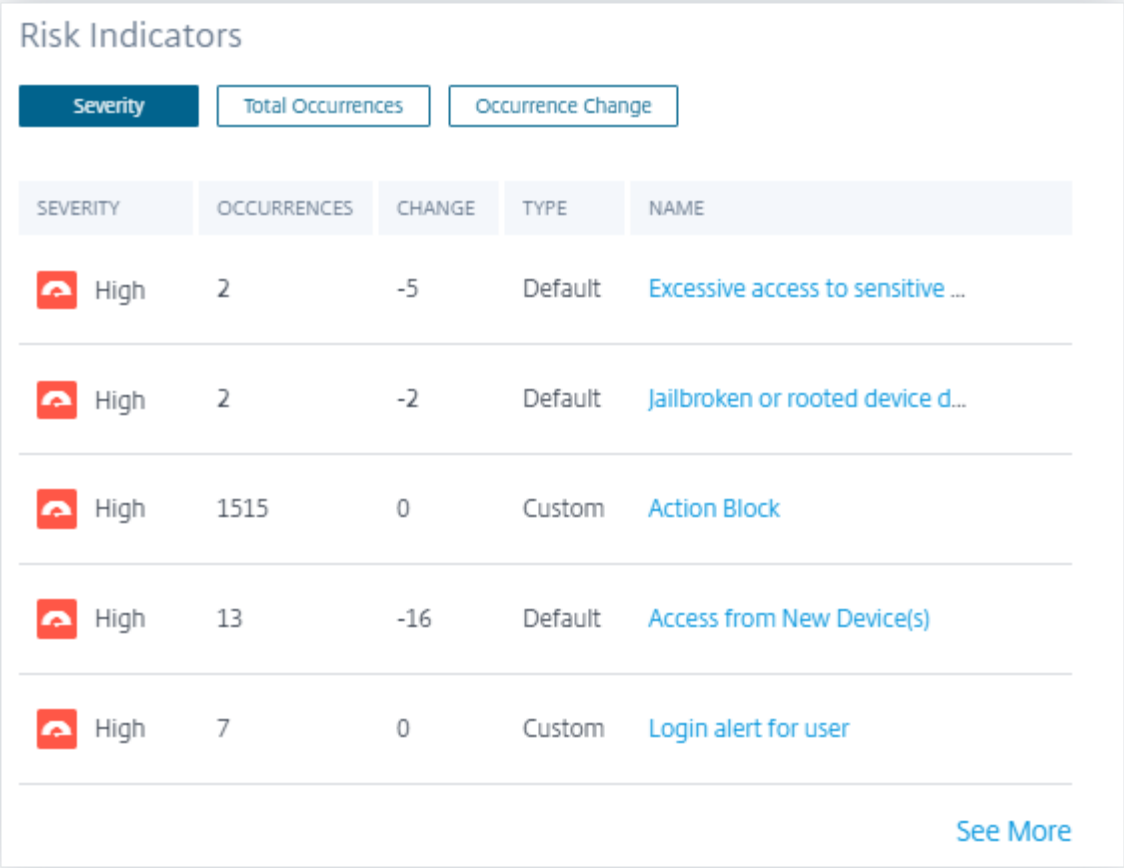
- Se agregan nuevas dimensiones para los orígenes de datos de Control de acceso, Content Collaboration y Apps and Desktops. Puede elegir estas dimensiones para crear informes. Se agregan las siguientes dimensiones para los orígenes de datos:
  - **Access Control**: Agente de usuario, nombre de usuario
  - **Content Collaboration contenido**: Correo electrónico de usuario, nombre de usuario, creado por, ID de cuenta, ID de cliente de OAuth, ID de evento, ID de carpeta, nombre de carpeta, ID de recurso, ID de formulario, IP de cliente
  - **Aplicaciones y escritorios**: nombre de usuario, dirección IP, identificador de dispositivo, jaula rota, tipo de inicio de sesión, nombre del servidor de sesión, nombre de usuario de la sesión, nombre del archivo de descarga, ruta del archivo de descarga, nombre de la impresora de impresión, nombre de archivo de detalles del trabajo de impresión, dirección URL de inicio de la aplicación SaaS, operación del portapapeles, resultado de detalles
- La interfaz de usuario de informes personalizados se ha mejorado con la compatibilidad con la paginación y la opción **Borrar todo** para los filtros.

Para obtener más información sobre cómo crear un informe personalizado con estas dimensiones, consulte Informes personalizados.

**Panel de indicadores de riesgo** El panel de **indicadores de riesgo** se introduce en la página **Usuarios**. Resume los cinco principales indicadores de riesgo por defecto y personalizados para un usuario. Un enlace Ver más le redirige a la página **Visión general del indicador de riesgo**. Esta página proporciona información detallada sobre los indicadores de riesgo generados durante un período de tiempo seleccionado.

Para obtener más información, consulte Panel de control de usuarios.

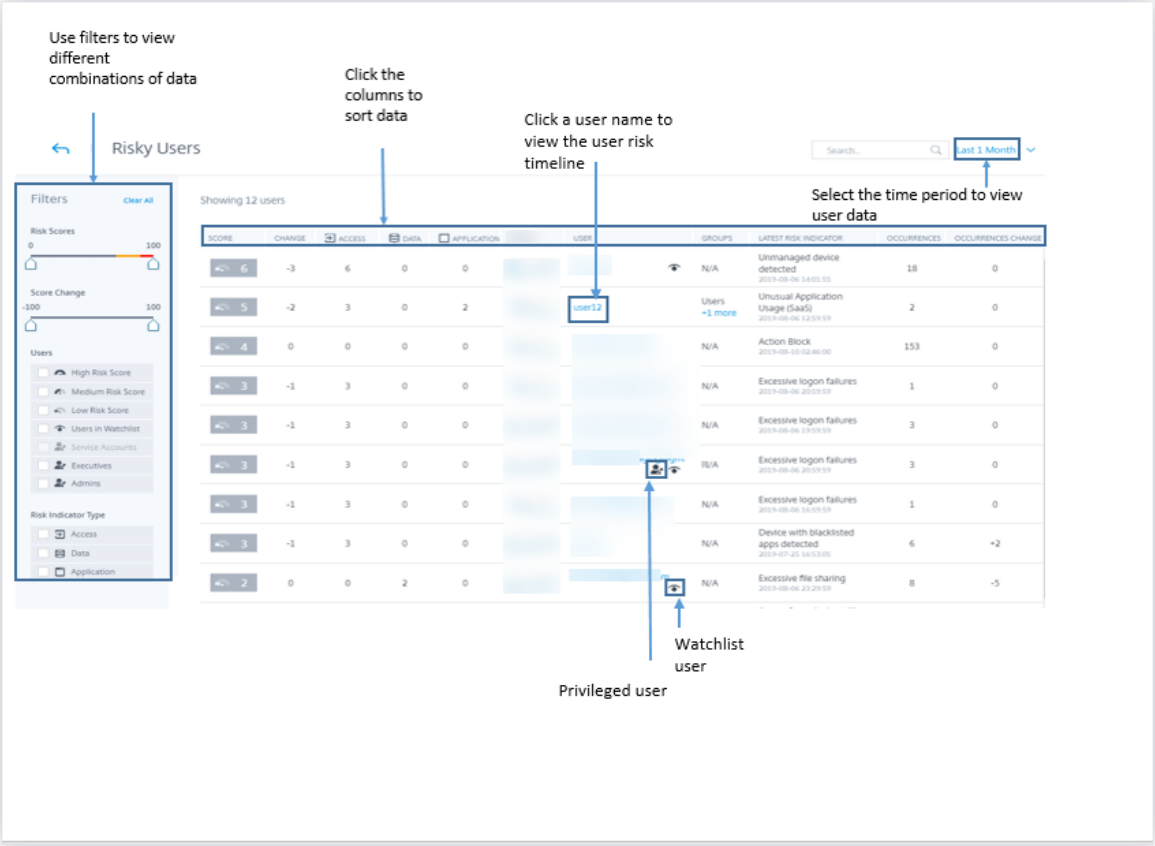



**Mejoras en el panel de usuarios con riesgos** Citrix Analytics presenta las fichas **Cambio de indicadores de riesgo** e **Indicadores de riesgo** en el panel **Usuarios con riesgos**. Puede ver los cinco usuarios más con riesgos basándose en estas fichas. El panel también introduce la columna **Indicadores de riesgo**. Muestra el número de indicadores de riesgo de un usuario.

La página **Usuarios con riesgos** introduce las columnas **Cambio de ocurrencias** y **ocurrencias**. En estas columnas se resumen el total de ocurrencias y el cambio en las apariciones de los indicadores de riesgo personalizados y predeterminados.

Para obtener más información, consulte Panel de control de usuarios.




**Indicador de riesgo de enlace compartido - Descargas excesivas** Citrix Analytics detecta amenazas de acceso en función de descargas excesivas en un enlace compartido y activa el indicador de riesgo de **descargas excesivas**. Al identificar los enlaces compartidos con descargas excesivas, en función del comportamiento anterior, puede supervisar el enlace para compartir en busca de posibles ataques. Este indicador de riesgo ayuda a identificar una actividad excesiva de descarga de archivos.

Para obtener más información, consulte Descargas excesivas.

**Búsqueda de autoservicio de los datos de autenticación** Utilice la búsqueda de autoservicio para obtener información sobre los eventos de autenticación. Citrix Analytics recibe los eventos de autenticación como inicio de sesión de usuario, cierre de sesión de usuario y actualización de clientes del servicio de administración de identidades y accesos de Citrix Cloud. La búsqueda proporciona un informe detallado sobre los eventos de autenticación, ayuda a identificar cualquier problema de autenticación y a solucionarlo. También puede definir una consulta de búsqueda para recuperar eventos que coincidan con los criterios definidos.

Para ver los eventos, seleccione **Autenticación** en la lista, seleccione el período de tiempo y, a continuación, haga clic en **Buscar**.

Para obtener más información, consulte Búsqueda de autoservicio de autenticación.

## 11 de julio de 2019

### Funciones nuevas

**Indicadores de riesgo personalizados** Los indicadores de riesgo predeterminados que genera Citrix Analytics se basan en algoritmos de aprendizaje automático. Citrix Analytics ahora permite crear indicadores de riesgo personalizados. En función de los eventos de usuario, puede definir las condiciones y crear indicadores de riesgo personalizados.

Cuando se cumplen las condiciones definidas, Citrix Analytics genera indicadores de riesgo personalizados similares a los indicadores de riesgo predeterminados y los muestra en el cronograma de riesgo del usuario. Los indicadores de riesgo personalizados se indican con una etiqueta en la línea de tiempo de riesgo del usuario.

Para obtener más información, consulte Indicadores de riesgo personalizados.

### Estado privilegiado en el cronograma de riesgo

El cronograma de riesgo del usuario muestra los siguientes eventos siempre que se produzca un cambio en el estado de privilegios de administrador o ejecutivo de un usuario:

- Agregado al grupo ejecutivo
- Eliminado del grupo ejecutivo
- Privilegio elevado a administrador
- Privilegio de administrador eliminado

Cuando se activa un indicador de riesgo para un usuario, puede correlacionarlo con el evento de cambio de estado de privilegios especificado. Si es necesario, puede aplicar las acciones apropiadas en el perfil de usuario.

Para obtener más información, consulte Cronología de riesgos del usuario.

### Acción de enlace de recurso compartido caducar

Citrix Analytics le permite aplicar acciones en indicadores de riesgo de vínculos compartidos. En la actualidad, la acción admitida es **Vencimiento del enlace de recurso compartido**.

Para obtener más información, consulte Indicadores de riesgo de vínculos compartidos de Citrix.

### Mejoras en la búsqueda de autoservicio

- **Compatibilidad con el carácter comodín * en la consulta de búsqueda**: Utilice el carácter asterisco (*) en su consulta de búsqueda para que coincida con cualquier carácter cero o más veces. Por ejemplo, la consulta de búsqueda Nombre de usuario = "John*"muestra los eventos de todos los nombres de usuario que comienzan por John.
- **Se ha agregado la opción Borrar todo para las facetas**: haga clic en **Borrar todo**para eliminar todas las facetas seleccionadas a la vez.
- **Ver datos de columnas ocultas en la lista de eventos**: tras quitar una columna de la tabla de eventos, puede ver los datos correspondientes en la lista de eventos de usuario. Expanda la fila de eventos de un usuario y visualice los datos.

Para obtener más información, consulte Búsqueda de autoservicio.

### Estado de error de datos en las tarjetas de sitio

Las tarjetas de sitio muestran la etiqueta **No se han recibido datos** en rojo cuando Citrix Analytics no recibe eventos durante la última hora del origen de datos. También muestra el número de eventos recibidos y está vinculado a la página de búsqueda de autoservicio correspondiente. Esta función le ayuda a ver los eventos correspondientes en la página de búsqueda de autoservicio y a comprobar si hay problemas de transmisión de datos.

> **Nota**
>
> Actualmente, la búsqueda de autoservicio solo está disponible para los orígenes de datos de Access, Content Collaboration y Apps and Desktop.

Para obtener más información, consulte Habilitar Analytics en orígenes de datos de Citrix.

### Problemas resueltos

- En el origen de datos de Control de acceso, el número de eventos de la tarjeta del sitio no coincide con los resultados de la búsqueda de autoservicio. [CAS-18286]

## 19 de junio de 2019

### Problemas resueltos

- La página **Registro de auditoría** muestra el estado activado o desactivado de la transmisión de datos cada vez que se detecta el origen de datos de Active Directory. [CAS-17575]

- El menú de períodos de tiempo del panel **Usuarios** no se carga correctamente. Muestra un mensaje de error de tiempo de espera. [CAS-19467]
- Los usuarios reciben un mensaje de error en Citrix Analytics mientras se conectan a un arrendatario desde Splunk. En ocasiones, se produce un error en la incorporación de nuevos orígenes de datos. [CAS-19429]

## 17 de junio de 2019

### Funciones nuevas

#### Configurar StoreFront

Si su organización utiliza StoreFront local, ahora puede configurar StoreFront para que se conecte a Citrix Analytics. La configuración se realiza mediante un archivo de configuración importado de Citrix Analytics. Una vez que la configuración se ha realizado correctamente, la aplicación Citrix Workspace envía eventos de usuario a Citrix Analytics para generar información útil sobre los comportamientos de los usuarios. La información le ayuda a detectar cualquier comportamiento anómalo de los usuarios y a gestionar de forma proactiva las amenazas a la seguridad de su organización. Para obtener más información, consulte Incorporar sitios locales de Citrix Virtual Apps and Desktops mediante StoreFront.

## 30 de mayo de 2019

### Funciones nuevas

#### Errores de inicio de sesión excesivos

Citrix Analytics detecta las amenazas de acceso en función de una actividad de inicio de sesión excesiva y activa el indicador de riesgo de errores de inicio de sesión excesivos. Este indicador de riesgo se activa cuando un usuario experimenta varios intentos fallidos de inicio de sesión para acceder a Content Collaboration. Al identificar a los usuarios con errores de inicio de sesión excesivos, según el comportamiento anterior, los administradores pueden supervisar la cuenta del usuario en busca de ataques de fuerza bruta.

> **Nota**
>
> Los**errores de inicio de sesión excesivos** ahora se denominan **Errores de autenticación excesivos**.

### Problemas resueltos

- En el caso de algunos eventos de usuario transmitidos por las aplicaciones Citrix Workspace, el origen de datos se identifica incorrectamente como Endpoint Management en lugar de Citrix Virtual Apps and Desktops.

  [CAS-17323]

- El panel **Usuarios** tarda mucho en cargarse durante el período de **Último mes**. Este problema se produce cuando el número de usuarios es elevado. En algunos casos, es posible que incluso se produzcan errores 601.

  [CAS-16300]

- Citrix Content Collaboration no se descubre como origen de datos, aunque algunos usuarios se suscriben al servicio en Citrix Cloud.

  [CAS-16299]

## 09 de mayo de 2019

### Funciones nuevas

#### Creación de informes personalizados

Ahora puede crear informes personalizados en función de sus requisitos operativos. Citrix Analytics proporciona una lista de dimensiones y métricas según el origen de datos seleccionado. Elija los parámetros necesarios y los tipos de visualización, como gráfico de barras, gráfico de eventos, gráfico de líneas o tabla, para crear sus informes. La creación de informes le ayuda a organizar y analizar sus datos de forma gráfica.

Para crear un informe personalizado, en la ficha **Seguridad**, haga clic en **Informes** > **Crear informe**. Para ver los informes creados anteriormente, en la ficha **Seguridad**, haga clic en **Informes**. Para obtener más información, consulte Informes personalizados.

#### Supervisión de usuarios privilegiados

Citrix Analytics le permite supervisar de cerca las anomalías de comportamiento de los usuarios con privilegios de una organización. Dado que los usuarios privilegiados son muy vulnerables a las amenazas de seguridad, resulta difícil distinguir sus actividades diarias de las maliciosas. Por lo tanto, las actividades maliciosas de los usuarios privilegiados permanecen desapercibidas durante mucho tiempo. Esta función le permite supervisar de forma proactiva dichas actividades y tomar las medidas adecuadas en las cuentas de usuario adecuadas. Los usuarios con privilegios se representan con un icono en el panel **Usuarios**.

Citrix Analytics admite la supervisión de los siguientes tipos de usuarios con privilegios:

- **Administradores**: Usuarios a los que el servicio Citrix respectivo asigna privilegios de administrador. En la actualidad, Citrix Analytics admite la supervisión de usuarios con privilegios de usuario con privilegios de administrador en el servicio Content Collaboration.
- **Ejecutivos**: En Citrix Analytics, puede marcar un grupo de AD como grupo de ejecutivos. Marcar un grupo de AD como grupo ejecutivo convierte a todos los usuarios del grupo en usuarios privilegiados. Si no es necesario seguir atendiendo las anomalías de comportamiento de los usuarios de un grupo de AD, puede quitar el grupo como grupo ejecutivo.

Para obtener más información, consulte Usuarios con privilegios.

#### Resumen semanal del correo electrónico

Citrix Analytics envía un correo electrónico semanal a los administradores en el que se resumen los riesgos de seguridad en el entorno de TI de su organización. La notificación por correo electrónico se envía todos los martes a los administradores y resalta los eventos de seguridad que se han producido en la semana anterior. Este correo electrónico garantiza que los administradores estén informados sobre los riesgos de seguridad sin iniciar sesión en Citrix Analytics. Para obtener más información, consulte Resumen semanal por correo electrónico.

### 26 de abril de 2019

#### Funciones nuevas

#### Administradores delegados

Citrix Analytics ahora admite funciones de administrador delegadas. Esta funcionalidad le permite invitar a otros administradores a su cuenta de Citrix Cloud para administrar Citrix Analytics para su organización. Si es administrador de Citrix Analytics con permiso de acceso completo, puede agregar otros administradores a su cuenta de Citrix Cloud. Estos administradores adicionales se denominan administradores delegados. En este momento, puede asignar acceso de solo lectura a los administradores delegados. Para obtener más información, consulte Administradores delegados.

#### Problemas resueltos

Pocos indicadores de riesgo para los orígenes de datos que utilizan la transmisión de datos no generan alertas. No recibe ninguna notificación de alerta y las acciones basadas en directivas no se aplican automáticamente si se activa alguno de los siguientes indicadores de riesgo:

- **Indicadores de riesgo de Citrix Endpoint Management**: Dispositivo no administrado, dispositivo con jailbreak o rooteado y dispositivo con aplicaciones incluidas en la lista de bloqueados.
- **Indicador de riesgo de Citrix Virtual Apps and Desktops**: Acceso desde un dispositivo con sistema operativo (SO) no compatible.
- **Indicador de riesgo de Citrix Content Collaboration**: Acceso excesivo a archivos confidenciales.

[CAS-14590]

## 19 febrero 2019

### Funciones nuevas

#### Integración de Splunk

Citrix Analytics se integra con Splunk para mejorar sus experiencias de supervisión de incidentes de seguridad y solución de problemas. Esta integración aumenta los orígenes de datos existentes con las capacidades de análisis de riesgos y la inteligencia de Citrix Analytics for Security, como indicadores de riesgo, puntuaciones de riesgo y perfiles de usuario. Citrix Analytics exporta información de análisis de riesgos a un canal. Splunk saca lo mismo de este canal.

La integración de Splunk implica la configuración en Citrix Analytics, la instalación del **complemento Citrix Analytics para la aplicación Splunk** y la configuración de la aplicación. Asegúrese de activar el procesamiento de datos para al menos un origen de datos. Ayuda a Citrix Analytics a iniciar el proceso de integración de Splunk.

Para obtener más información, consulte Integración de Splunk.

**Grabación dinámica de sesiones** Citrix Analytics introduce la capacidad de activar la grabación de sesiones de forma dinámica en las sesiones actuales de Virtual Apps and Desktops de los usuarios. Ayuda a capturar las evidencias necesarias para el análisis de riesgos y tomar las acciones adecuadas de respuesta a incidentes, como sesiones de desconexión y bloquear usuarios.

Para obtener más información, consulte Directivas y acciones.

**Panel e indicador de riesgo de Share Links** Citrix Analytics introduce la visibilidad del riesgo de Share Links en función de los datos recopilados de Citrix Content Collaboration. Le ayuda a comprender la exposición al riesgo de los enlaces de acciones a través de los indicadores de riesgo que activan los enlaces de acciones.

Para obtener más información, consulte Panel de control Compartir vínculos.

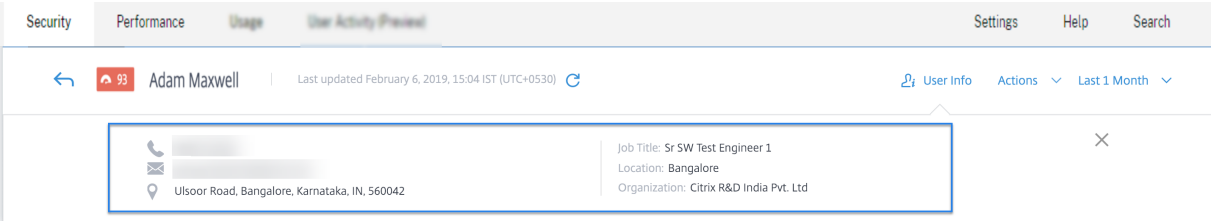
 

Actualmente, el indicador de riesgo de descarga de acciones confidenciales anónimas se activa para un enlace para compartir. Cuando Content Collaboration detecta este comportamiento de riesgo, Citrix Analytics recibe los eventos. Se le notifica en el panel **Alertas** y el indicador de riesgo de descarga de acciones confidenciales anónimas se agrega a la línea de tiempo de riesgo del enlace compartido.

Para obtener más información, consulte Cronología de riesgo de Share Link e indicadores de riesgo de Citrix Share Link.

**Integración Microsoft Active Directory** Ahora puede integrar Microsoft Active Directory con Citrix Analytics. Esta integración mejora el contexto de los usuarios de riesgo con información adicional, como el cargo, la organización, la ubicación de la oficina, el correo electrónico y los datos de contacto. Puede obtener una mejor visibilidad de un usuario en la página de perfil de usuario de Citrix Analytics.

Para obtener más información, consulte Integración de Analytics con Microsoft Active Directory.




## 04 de enero de 2019

### Funciones nuevas

**Adición de la columna SOURCE para los indicadores de riesgo existentes** La columna **ORIGEN** se ha introducido en la sección **DETALLES DEL EVENTO** para los siguientes indicadores de riesgo:

- Subidas excesivas de archivos
- Descargas excesivas de archivos
- Uso compartido excesivo de archivos
- Eliminación excesiva de archivos o carpetas

Para obtener más información, consulte Indicadores de riesgo de Citrix Content Collaboration.

**Perfil de usuario avanzado** Se ha mejorado la vista **Información** del usuario en el perfil de usuario. El enlace **Vista de tendencias** se ha introducido en la esquina superior derecha de las secciones **Aplicación**, **Dispositivos** y **Uso de datos**. El vínculo **Vista de mapa** se ha introducido en la esquina superior derecha de la sección **Ubicaciones**. Estos enlaces proporcionan una representación gráfica del

comportamiento histórico del usuario durante un período de tiempo específico. Puede navegar a **Información de usuario** desde la línea de tiempo de riesgo del usuario o desde la página **Orígenes de datos**.

> **Nota**
>
> Los datos **Autenticación** y **Dominios** no están disponibles actualmente en el perfil Información de usuario.

Para obtener más información, consulte Cronología y perfil de riesgos del usuario.

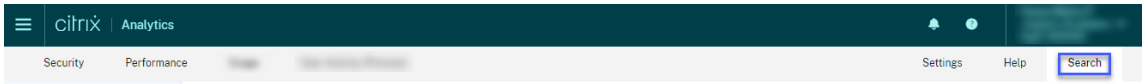

**Indicadores de riesgo para Microsoft Graph Security** Microsoft Graph Security incorporada puede recibir detalles del indicador de riesgo de uno de los siguientes proveedores de seguridad y reenviarlos a Citrix Analytics:

- Protección de identidad de Azure AD
- Microsoft Defender para dispositivos de punto final

Para obtener más información, consulte Indicadores de riesgo para Microsoft Graph Security.

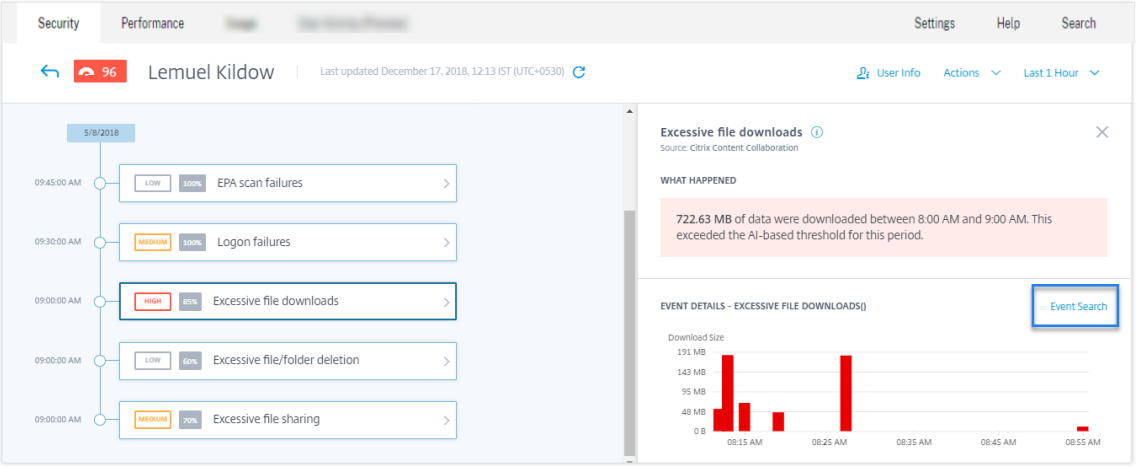
**Formas de entrar en la página de búsqueda de autoservicio** Ahora puede acceder a la página de búsqueda de autoservicio mediante las siguientes opciones:

- **Barra superior**: haga clic en **Buscar** en la barra superior para acceder directamente a la página de búsqueda.




- **Cronología de riesgos en la página de perfil del usuario**: haga clic en **Búsqueda de eventos** para acceder a la página de búsqueda y ver los eventos correspondientes al indicador de riesgo de un usuario específico y a el origen de datos. Para obtener más información, consulte Búsqueda de autoservicio.




**Búsqueda de autoservicio de Content Collaboration** Utilice la búsqueda de autoservicio para obtener información sobre los eventos asociados a el origen de datos de Content Collaboration. Para ver los eventos, seleccione **Content Collaboration** de la lista, seleccione el período de tiempo y, a continuación, haga clic en **Buscar**.
Para obtener más información, consulte Búsqueda de autoservicio para Content Collaboration.

**Búsqueda de autoservicio de aplicaciones y escritorios** Use la búsqueda de autoservicio para obtener información sobre los eventos asociados con el origen de datos de Apps and Desktops. Para ver los eventos, selecciona **Aplicaciones y escritorios** en la lista, selecciona el período de tiempo y, a continuación, haga clic en **Buscar**. Para obtener más información, consulte Búsqueda de autoservicio de aplicaciones y escritorios.

**Exportar eventos de búsqueda de autoservicio a un archivo CSV** Ahora puede exportar los eventos de búsqueda de autoservicio a un archivo CSV y descargarlo para utilizarlo en el futuro. Para obtener más información, consulte Búsqueda de autoservicio.

**Integración mejorada para Citrix Virtual Apps and Desktops** El proceso de incorporación de la fuente de datos de Citrix Virtual Apps and Desktops ahora se ha mejorado para ofrecer una mejor experiencia de usuario. Se han modificado las fichas del sitio y los pasos de embarque. Para obtener más información, consulte Origen de datos de Citrix Virtual Apps and Desktops y Citrix DaaS.

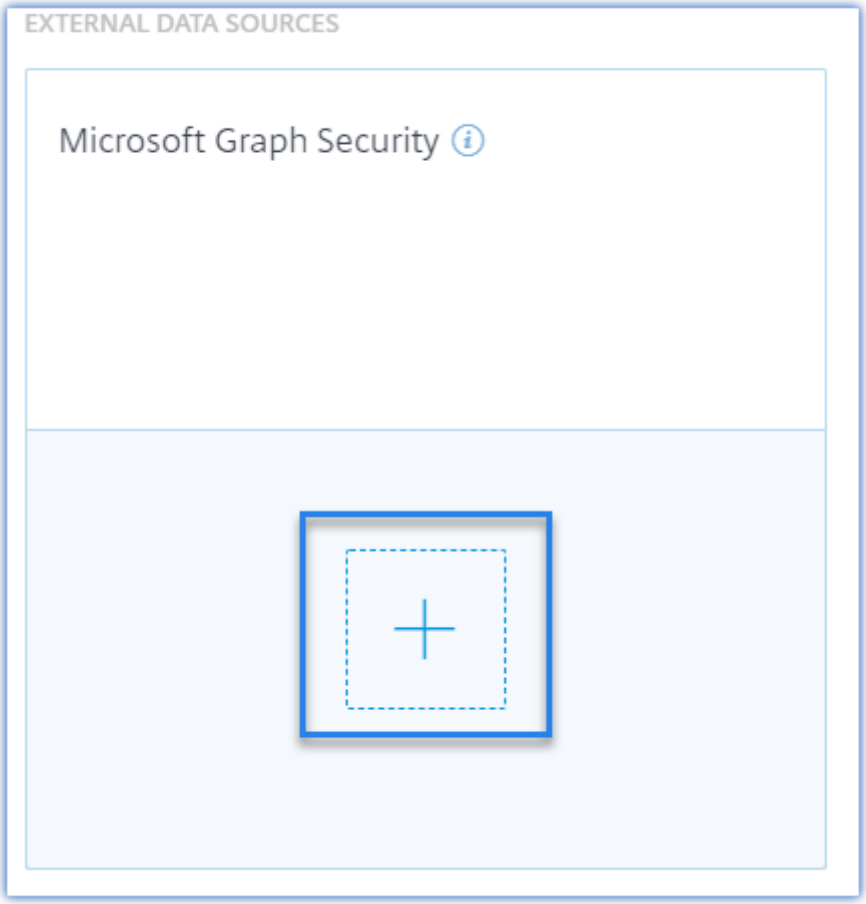
## 29 de noviembre de 2018

### Funciones nuevas

**Origen de datos Microsoft Security Graph** Microsoft Graph Security es un origen de datos externa que agrega datos de varios proveedores de seguridad. También proporciona acceso a los datos del inventario de usuarios.

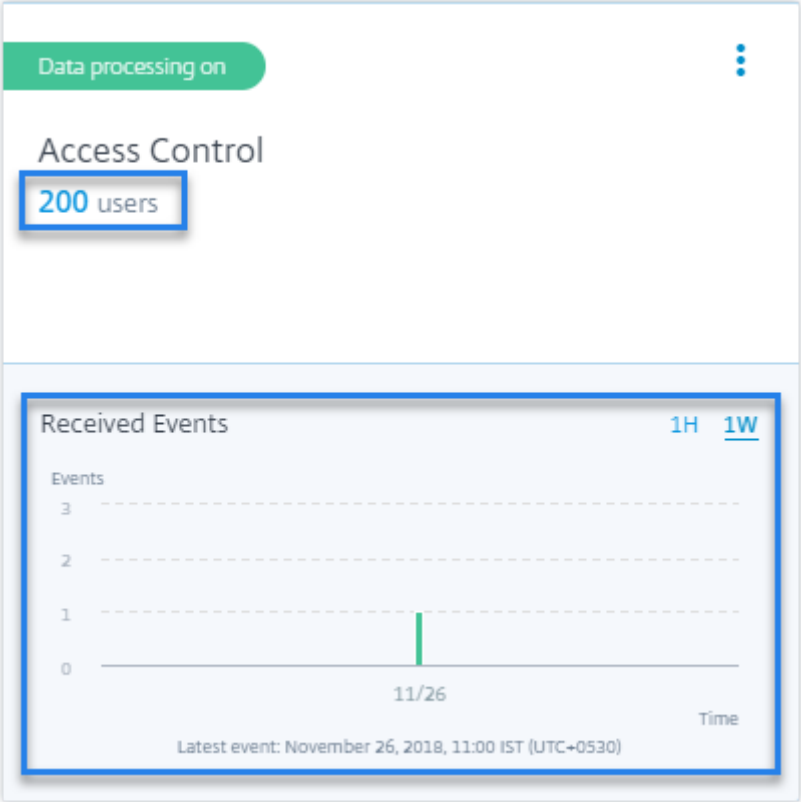
Actualmente, Citrix Analytics admite los proveedores de seguridad de **protección de identidad de Azure AD** y **Microsoft Defender for Endpoint** asociados a este origen de datos.

Para integrar este origen de datos, debe obtener permisos de la plataforma de identidad de Microsoft. Para obtener más información, consulte Microsoft Graph Security.




**Ver detalles de eventos y usuarios detectados en las tarjetas de sitio para orígenes de datos** Las tarjetas de sitio de los orígenes de datos muestran ahora los detalles de los eventos y el número de usuarios. Por ejemplo, puede ver los detalles del evento y los usuarios de Control de acceso en la tarjeta del sitio. Para obtener más información, consulte Habilitar análisis en orígenes de datos.




## 16 de noviembre de 2018

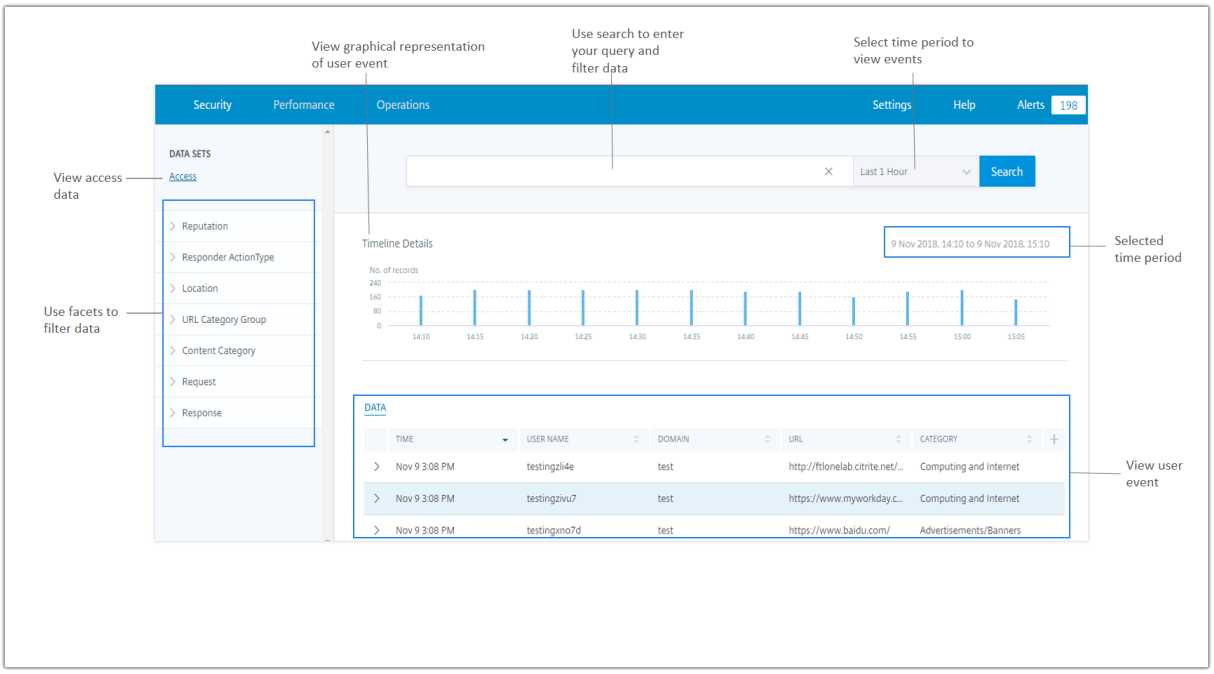
### Funciones nuevas

**Búsqueda de autoservicio de datos de acceso** Puede utilizar la búsqueda de autoservicio para obtener información sobre los detalles de acceso de los usuarios de su empresa. Citrix Analytics recopila los detalles de acceso de los usuarios del servicio Citrix Access Control. Utilice las facetas y la consulta de búsqueda para reducir los resultados de búsqueda.

Para utilizar la página de búsqueda de autoservicio, en la ficha **Seguridad**, haga clic en **Búsqueda de eventos**.

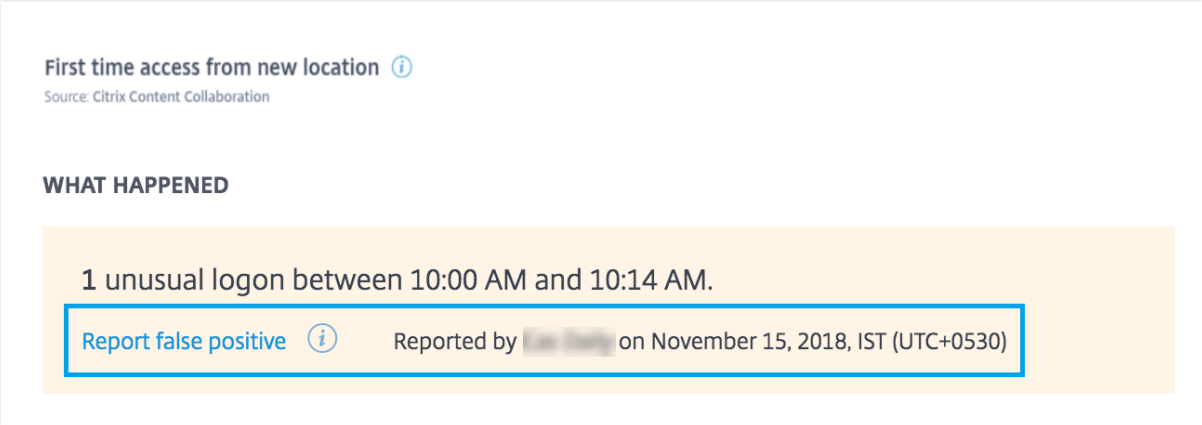
Para obtener más información, consulte Búsqueda de autoservicio de Access.




**Comentarios sobre los indicadores de riesgo** Con la función de comentarios sobre indicadores de riesgo de Citrix Analytics, puede proporcionar comentarios sobre un indicador de riesgo. Sus comentarios ayudan a confirmar si el incidente de seguridad denunciado es correcto o no.

Actualmente, esta función se admite en el indicador Riesgo de **acceso de inicio de sesión inusual** activado por el origen de datos de Content Collaboration. Si este indicador de riesgo activado es incorrecto, puede denunciarlo como un falso positivo y proporcionar comentarios. También puede modificar los comentarios que haya enviado anteriormente. Citrix Analytics captura sus comentarios y valida la información prevista para optimizar la detección de comportamientos anómalos.



**Problemas resueltos**

- No puede modificar ni guardar una directiva si accede a Citrix Analytics mediante Internet Explorer 11.0.

## Problemas conocidos

December 7, 2023

Citrix Analytics for Security presenta los siguientes problemas conocidos:

- La aplicación Citrix Workspace para Linux no envía eventos de impresión a Citrix Analytics cuando las aplicaciones y los escritorios se abren mediante un explorador web y se inician desde ICA en el cliente nativo. [CAS-36238]

> **Nota**
>
> Para obtener más información sobre las fechas del ciclo de vida y las fases del ciclo de vida (disponibilidad general, fin del mantenimiento y fin del ciclo de vida) de la aplicación Citrix Workspace y Citrix Receiver en todas las plataformas, consulte Hitos del ciclo de vida de la aplicación Citrix Workspace y Citrix Receiver.

## Ofertas de Citrix Analytics

December 7, 2023

### Citrix Analytics for Security

Recopila y proporciona visibilidad del comportamiento de los usuarios y las aplicaciones, recopilado de las fuentes de datos conectadas de los clientes, como Secure Private Access, Citrix Virtual Apps and Desktops, Citrix DaaS Site o NetScaler Gateway. Puede realizar un seguimiento de todos los aspectos del comportamiento y, al aprovechar los algoritmos avanzados de aprendizaje automático, puede distinguir entre el comportamiento normal y un atacante malintencionado. Por lo tanto, le permite identificar y gestionar de manera proactiva las amenazas internas y externas.

**Más información**: Citrix Analytics for Security

### Citrix Analytics for Performance

Proporciona una visibilidad integral de extremo a extremo en las implementaciones híbridas de Citrix Virtual Apps and Desktops y sitios de Citrix DaaS. El rendimiento se indica mediante la puntuación de experiencia del usuario, que cuantifica los factores históricos y las métricas que definen la experiencia que tiene un usuario al utilizar una aplicación publicada, un escritorio publicado o un PC remoto proporcionados por Citrix.

**Más información**: Citrix Analytics for Performance

### Citrix Analytics: uso (fin de la vida útil)

> **Nota**
>
> **:**Citrix Usage Analytics ha llegado al final de su vida útil y ya no está disponible para los usuarios.

## Orígenes de datos

April 12, 2024

Los orígenes de datos son los servicios en la nube y los productos locales que envían datos a Citrix Analytics.

### Orígenes de datos de Citrix

En la siguiente tabla se enumeran varios orígenes de datos de Citrix compatibles con Citrix Analytics for Security. Para obtener más información, consulte Introducción.

| Origen de datos | Tipo de implementación | Agentes requeridos | Componente y versión del producto |
|---|---|---|---|
| Citrix Endpoint Management | Servicio | N/D | Citrix Endpoint Management |
| Gateway | Local | Agente de administración de entrega de aplicaciones | Citrix Gateway 12.0.56.16 o posterior |

| Origen de datos | Tipo de implementación | Agentes requeridos | Componente y versión del producto |
|---|---|---|---|
| Proveedor de identidades Citrix | Servicio | N/D | Administración de acceso e identidad de Citrix |
| Citrix Secure Private Access | Servicio | (No aplica) N/A | Citrix Secure Private Access |
| Citrix Remote Browser Isolation | Servicio | N/D | Citrix Remote Browser Isolation |
| Citrix DaaS (antes denominado Virtual Apps and Desktops Service) | Servicio | N/D | Aplicación Citrix Workspace para Windows 1907 o posterior, aplicación Citrix Workspace para Mac 1910.2 o posterior, aplicación Citrix Workspace para HTML5 2007 o posterior, aplicación Citrix Workspace para Chrome, la última versión disponible en Chrome Web Store, aplicación Citrix Workspace para Android: la última versión disponible en Google Play, la aplicación Citrix Workspace para iOS: la última versión disponible en Apple App Store, la aplicación Citrix Workspace para Linux 2006 o posterior |

| Origen de datos | Tipo de implementación | Agentes requeridos | Componente y versión del producto |
|---|---|---|---|
| Citrix Virtual Apps and Desktops | Local | Agente de Virtual Apps and Desktops<br><br>El agente es necesario para funciones avanzadas como Acciones. | Citrix Virtual Apps and Desktops 7 1808, Citrix XenApp y XenDesktop 7.16 y posteriores<br>Aplicación Citrix Workspace para Windows 1907 o posterior, aplicación Citrix Workspace para Mac 1910.2 o posterior, aplicación Citrix Workspace para HTML5 2007 o posterior, aplicación Citrix Workspace para Chrome, la última versión disponible en Chrome Web Store, aplicación Citrix Workspace para Android: la última versión disponible en Google Play, la aplicación Citrix Workspace para iOS: la última versión disponible en Apple App Store, la aplicación Citrix Workspace para Linux 2006 o posterior<br>Citrix Director 7.16 o posterior |

| Origen de datos | Tipo de implementación | Agentes requeridos | Componente y versión del producto |
|---|---|---|---|
| | | | **Para los usuarios de Workspace: Los**sitios locales de Virtual Apps and Desktops deben agregarse a Workspace mediante la agregación de sitios.<br><br>**Para los usuarios de StoreFront**: La versión de implementación de StoreFront debe ser StoreFront 1906 o posterior. Se debe acceder a StoreFront mediante uno de los clientes: sitios de Citrix Receiver para Web en exploradores compatibles con HTML5, aplicación Citrix Workspace 1907 para Windows o posterior, aplicación Citrix Workspace 2006 para Linux o posterior, aplicación Citrix Workspace 2006 para Mac o posterior.<br><br>**Compatibilidad con LTSR**: para Citrix Virtual Apps and Desktops 7 1912 LTSR, la versión compatible de StoreFront es 1912. |

> **Nota**
>
> Consulte los servicios de Citrix Cloud para conocer los productos Citrix y sus suscripciones.

### Orígenes de datos externas

En la siguiente tabla se enumeran los orígenes de datos externas (productos de terceros) que admite Citrix Analytics for Security.

| Origen de datos | Tipo de implementación | Agentes requeridos |
|---|---|---|
| Microsoft Graph Security | Servicio | N/D |
| Microsoft Active Directory | Local | Citrix Cloud Connector |

### Regiones de origen admitidas

Citrix Analytics for Security se admite en las siguientes regiones de origen:

- Estados Unidos (EE. UU.)
- Unión Europea (UE)
- Sur de Asia Pacífico (APS)

Según la ubicación de su organización, puede incorporarse a Citrix Cloud en una de las regiones de origen.

Si su organización se incorpora a Citrix Cloud en una región de origen donde no se admite una fuente de datos, no obtendrá eventos de usuario de la fuente de datos.

Use la siguiente tabla para ver los orígenes de datos y las regiones en las que se admiten.

| Origen de datos | Apoyado en la región de EE. UU. | Apoyado en la región de la UE | Se admite en la región APS |
|---|---|---|---|
| Citrix Endpoint Management | Sí | Sí | Sí |
| Citrix Gateway (local) | Sí | Sí | Sí |
| Proveedor de identidades Citrix | Sí | Sí | Sí |
| Citrix Secure Private Access | Sí | Sí | Sí |

| Origen de datos | Apoyado en la región de EE. UU. | Apoyado en la región de la UE | Se admite en la región APS |
|---|---|---|---|
| Citrix Remote Browser Isolation | Sí | Sí | Sí |
| Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service) | Sí | Sí | Sí |
| Citrix Virtual Apps and Desktops local | Sí | Sí | Sí |
| Microsoft Active Directory | Sí | Sí | Sí |
| Microsoft Graph Security | Sí | Sí | Sí |

### Matriz de versiones de la aplicación Citrix Workspace

En esta sección se muestran las versiones compatibles de la aplicación Citrix Workspace, que envía toda la telemetría y contiene todas las correcciones de errores críticas necesarias.

En la siguiente tabla se enumeran las versiones compatibles y no compatibles de la aplicación Citrix Workspace.

| Plataforma | Versión compatible |
|---|---|
| Windows | Todas las versiones de LTSR 2203 posteriores a CU3<br>23.0.3.0 o posterior |
| HTML5 | 21.5.0.0 o posterior |
| Macintosh | 21.0.4.0 o posterior |
| Linux | 21.4.0.0 o posterior |
| Chrome | 21.5.0.0 o posterior |
| iOS | 21.4.0.0 o posterior |
| Android | 21.5.0.0 o posterior |

En la siguiente tabla se muestra la versión mínima de la aplicación Citrix Workspace requerida para que el sistema operativo reciba los siguientes atributos de eventos de usuario en Citrix Analytics for

Security.

| Atributos de eventos | Funciones asociadas | Windows | Mac | Linux | HTML5 | Chrome | iOS | Android |
|---|---|---|---|---|---|---|---|---|
| Ciudad, país | Ubicación de garantía de acceso, búsqueda de autoservicio: aplicaciones y escritorios | 2008 o superior | 2006 o superior | 2104 o superior | 2007 o superior | Última versión disponible en Chrome Web Store | Última versión disponible en la App Store de Apple | Última versión disponible en Google Play |
| Client IP | Búsqueda de autoservicio: aplicaciones y escritorios | 2008 o superior | 2006 o superior | 2104 o superior | 2007 o superior | Última versión disponible en Chrome Web Store | Última versión disponible en la App Store de Apple | Última versión disponible en Google Play |

| Atributos de eventos | Funciones asociadas | Windows | Mac | Linux | HTML5 | Chrome | iOS | Android |
|---|---|---|---|---|---|---|---|---|
| Nombre del sistema operativo, versión del sistema operativo, información adicional del sistema operativo | Búsqueda de autoservicio: aplicaciones y escritorios | 2109 o superior | 2108 o superior | 2104 o superior | 2007 o superior | Última versión disponible en Chrome Web Store | Última versión disponible en la App Store de Apple | Última versión disponible en Google Play |
| Nombre de impresora | Búsqueda de autoservicio: aplicaciones y escritorios | 2106 o posterior | 1809 o posterior | 2006 o posterior | 1911 o posterior | Última versión disponible en Chrome Web Store | Última versión disponible en la App Store de Apple | Última versión disponible en Google Play |
| Todos los eventos de usuarios para lanzamiento web | Búsqueda de autoservicio: aplicaciones y escritorios | 2008 o posterior | 2006 o posterior | 2006 o posterior | No aplicable | No compatible | Última versión disponible en la App Store de Apple | Última versión disponible en Google Play |

# Reglamentación de datos

September 11, 2024

En esta sección se proporciona información sobre la recopilación, el almacenamiento y la retención de registros por parte del servicio Citrix Analytics. Todos los términos en mayúsculas que no estén definidos en la sección Definiciones tienen el significado especificado en el Acuerdo de servicios de usuario final de Citrix.

Citrix Analytics está diseñado para proporcionar a los clientes información sobre las actividades de su entorno informático Citrix. Citrix Analytics permite a los administradores de seguridad elegir los registros que desean supervisar y tomar medidas directas en función de la actividad registrada. Esta información ayuda a los administradores de seguridad a administrar el acceso a sus entornos informáticos y a proteger el contenido del cliente en el entorno informático del cliente.

## Residencia de datos

Los registros de Citrix Analytics se mantienen por separado de los orígenes de datos y se agregan en varios entornos de Microsoft Azure Cloud, que se encuentran en las regiones de Estados Unidos, la Unión Europea y Asia Pacífico Sur. El almacenamiento de los registros depende de la región de origen seleccionada por los administradores de Citrix Cloud al incorporar sus organizaciones a Citrix Cloud. Por ejemplo, si elige la **región europea** al incorporar su organización a Citrix Cloud, los registros de Citrix Analytics se almacenan en entornos Microsoft Azure de la Unión Europea.

Para obtener más información, consulte Administración de registros y contenido de clientes de Citrix Cloud Services y consideraciones geográficas.

## Recopilación de datos

Los servicios de Citrix Cloud están instrumentados para transmitir registros a Citrix Analytics. Los registros se recopilan de estos orígenes de datos:

- Citrix ADC (local) junto con la suscripción a Citrix Application Delivery Management
- Citrix Endpoint Management
- Citrix Gateway (local)
- Proveedor de identidades Citrix
- Citrix Secure Browser
- Citrix Secure Private Access

- Citrix Virtual Apps and Desktops
- Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service)
- Microsoft Active Directory
- Microsoft Graph Security

### Transmisión de datos

Los registros de Citrix Cloud se transmiten de forma segura a Citrix Analytics. Cuando el administrador del entorno del cliente habilita explícitamente Citrix Analytics, estos registros se analizan y almacenan en una base de datos de clientes. Lo mismo se aplica a Citrix Virtual Apps and Desktops los orígenes de datos con Citrix Workspace configurado.

En el caso de los orígenes de datos de Citrix ADC, la transmisión de registros se inicia únicamente cuando el administrador habilita explícitamente Citrix Analytics para el origen de datos específica.

### Control de datos

El administrador puede activar o desactivar los registros enviados a Citrix Analytics en cualquier momento.

Cuando se desactiva para los orígenes de datos locales de Citrix ADC, se detiene la comunicación entre el origen de datos ADC concreta y Citrix Analytics.

Cuando se desactiva todo para otros orígenes de datos, los registros del origen de datos concreta ya no se analizan ni se almacenan en Citrix Analytics.

### Retención de datos

Los registros de Citrix Analytics se conservan de forma identificable durante un máximo de 13 meses o 396 días. Todos los registros y datos analíticos asociados, como perfiles de riesgo de usuario, detalles de puntuación de riesgo de usuario, detalles de eventos de riesgo de usuario, lista de seguimiento de usuarios, acciones de usuario y perfil de usuario, se conservan durante este período.

Por ejemplo, si ha habilitado Analytics en un origen de datos el 1 de enero de 2021, de forma predeterminada, los datos recopilados el 1 de enero de 2021 se conservarán en Citrix Analytics hasta el 31 de enero de 2022. Del mismo modo, los datos recopilados el 15 de enero de 2021 se conservarán hasta el 15 de febrero de 2022, etc.

Estos datos se almacenan durante el período de retención de datos predeterminado incluso después de haber desactivado el procesamiento de datos para el origen de datos o después de haber eliminado el origen de datos de Citrix Analytics.

Citrix Analytics elimina todo el contenido del cliente 90 días después del vencimiento de la suscripción o del período de prueba.

## Exportación de datos

En esta sección se explican los datos exportados desde Citrix Analytics for Security y Citrix Analytics for Performance.

Citrix Analytics for Performance recopila y analiza las métricas de rendimiento de los orígenes de datos.

Puede descargar los datos de la página de búsqueda de autoservicio como un archivo CSV.

Citrix Analytics for Security recopila eventos de usuarios de varios productos (orígenes de datos). Estos eventos se procesan para proporcionar visibilidad del comportamiento con riesgos e inusual de los usuarios. Puede exportar estos datos procesados relacionados con las perspectivas de riesgo de los usuarios y los eventos de los usuarios a su servicio de Administración de eventos e información del sistema (SIEM).

Actualmente, los datos se pueden exportar de dos maneras desde Citrix Analytics for Security:

- Integración de Citrix Analytics for Security con su servicio SIEM
- Descargar los datos de la página de búsqueda de autoservicio como un archivo CSV.

Cuando integra Citrix Analytics for Security con su servicio SIEM, los datos se envían a su servicio SIEM mediante el tema Kafka en dirección norte o un conector de datos basado en Logstash.

Actualmente, puede integrarse con los siguientes servicios SIEM:

- Splunk (conectándose a través del complemento Citrix Analytics)
- Cualquier servicio SIEM que admita conectores de datos basados en temas de Kafka o Logstash, como Elasticsearch y Microsoft Azure Sentinel

También puede exportar los datos a su servicio SIEM mediante un archivo CSV. En la página de búsqueda de autoservicio, puede ver los datos (eventos de usuario) de una fuente de datos y descargar estos datos como un archivo CSV. Para obtener más información sobre el archivo CSV, consulte Búsqueda de autoservicio.

> **Importante**
>
> Después de exportar los datos a su servicio SIEM, Citrix no es responsable de la seguridad, el almacenamiento, la administración y el uso de los datos exportados en su entorno SIEM.

Puede activar o desactivar la transmisión de datos desde Citrix Analytics for Security a su servicio SIEM.

Para obtener información sobre los datos procesados y la integración de SIEM, consulte Integración de administración de eventos e información de seguridad (SIEM) y Formato de datos de Citrix Analytics para SIEM.

## anexo de seguridad de Citrix Services

En la exposición de seguridad de Citrix Services se incluye información detallada sobre los controles de seguridad aplicados a Citrix Analytics, incluidos el acceso y la autenticación, la administración de programas de seguridad, la continuidad del negocio y la administración de incidentes.

## Definiciones

Por**contenido del cliente** se entiende cualquier dato cargado en una cuenta de cliente para su almacenamiento o datos en un entorno de cliente al que Citrix tenga acceso para prestar los Servicios.

**Registro** significa un registro de eventos relacionados con los servicios mencionados, incluidos los registros que miden el rendimiento, la estabilidad, el uso, la seguridad y la asistencia.

**Servicios** significa los Citrix Cloud Services descritos anteriormente para los fines de Citrix Analytics.

## Acuerdo de recopilación de datos

Al cargar sus datos en Citrix Analytics y utilizar las funciones de Citrix Analytics, acepta y acepta que Citrix recopile, almacene, transmita, mantenga, procese y use información técnica, de usuario o relacionada sobre sus productos y servicios Citrix.

Citrix siempre trata la información recibida de acuerdo con la Directiva de privacidad de Citrix.

## Apéndice: registros recopilados

- Registros de Citrix Analytics para seguridad
- Registros de Citrix Analytics para rendimiento

## Registros de Citrix Analytics para seguridad

### Registros generales

En general, los registros de Citrix Analytics contienen los siguientes puntos de datos de identificación de encabezados:

- Claves de encabezado
- Identificación de dispositivos
- Identificación
- Dirección IP
- Organización
- Producto
- Versión del producto
- Hora del sistema
- Identificación del arrendatario
- Tipo
- Usuario: correo electrónico, ID, nombre de cuenta SAM, dominio, UPN
- Versión

**Registros del servicio Citrix Endpoint Management**

Los registros del servicio Citrix Endpoint Management contienen los siguientes puntos de datos:

- Cumplimiento de normativas
- Propiedad corporativa
- ID de dispositivo
- Modelo de dispositivo
- Tipo de dispositivo
- Latitud geográfica
- Longitud geográfica
- Nombre de host
- IMEI
- Dirección IP
- Prisión rota
- Última actividad
- Modo de gestión
- Sistema operativo

- Versión del sistema operativo
- Información de la plataforma
- Motivo
- Número de serie
- Supervisado

**Registros de Citrix Secure Private Access**

- AAA User Name
- Auth Policy Action Name
- Authentication Session ID
- Request URL
- URL Category Policy Name
- VPN Session ID
- Vserver IP
- AAA User Email ID
- Actual Template Code
- App FQDN
- Nombre de la aplicación
- App Name Vserver LS
- Application Flags
- Authentication Type
- Authentication Stage
- Authentication Status Code
- Dirección IPv4 Dst del servidor back-end
- Dirección IPv4 del servidor back-end
- Dirección IPv6 del servidor back-end
- Category Domain Name
- Category Domain Source
- IP de cliente

- Client MSS
- Client Fast Retx Count
- Client TCP Jitter
- Client TCP Packets Retransmited
- Client TCP RTO Count
- Client TCP Zero Window Count
- Clt Flow Flags Rx
- Clt Flow Flags Tx
- Clt TCP Flags Rx
- Clt TCP Flags Tx
- Connection Chain Hop Count
- Connection Chain ID
- Egress Interface
- Exporting Process ID
- Flow Flags Rx
- Flow Flags Tx
- HTTP Content Type
- HTTP Domain Name
- HTTP Req Authorization
- HTTP Req Cookie
- HTTP Req Forw FB
- HTTP Req Forw LB
- HTTP Req Host
- HTTP Req Method
- HTTP Req Rcv FB
- HTTP Req Rcv LB
- HTTP Req Referer
- HTTP Req URL
- HTTP Req XForwarded For

- HTTP Res Forw FB
- HTTP Res Forw LB
- HTTP Res Location
- HTTP Res Rcv FB
- HTTP Res Rcv LB
- HTTP Res Set Cookie
- HTTP Rsp Len
- HTTP Rsp Status
- HTTP Transaction End Time
- HTTP Transaction ID
- IC Cont Grp Name
- IC Flags
- IC No Store Flags
- IC Policy Name
- Ingress Interface Client
- ID de aplicación del NetScaler Gateway Service
- Nombre de aplicación del NetScaler Gateway Service
- Tipo de aplicación del NetScaler Gateway Service
- ID de partición de NetScaler
- Observation Domain ID
- Observation Point ID
- Origin Res Status
- Origin Rsp Len
- Protocol Identifier
- Rate Limit Identifier Name
- Tipo de registro
- Responder Action Type
- Response Media Type
- Srv Flow Flags Rx

- Srv Flow Flags Tx
- Srvr Fast Retx Count
- Fluctuación del servidor TCP
- Paquetes TCP de Srvr retransmitidos
- Recuento Rto de TCP de servidor
- Recuento cero de ventanas Srvr TCP
- SSL Cipher Value BE
- SSL Cipher Value FE
- SSL Client Cert Size BE
- SSL Client Cert Size FE
- SSL Clnt Cert Sig Hash BE
- SSL Clnt Cert Sig Hash FE
- SSL Err App Name
- SSL Err Flag
- SSL Flags BE
- SSL Flags FE
- SSL Handshake Error Msg
- SSL Server Cert Size BE
- SSL Server Cert Size FE
- SSL Session ID BE
- SSL Session ID FE
- SSL Sig Hash Alg BE
- SSL Sig Hash Alg FE
- SSL Srvr Cert Sig Hash BE
- SSL Srvr Cert Sig Hash FE
- SSL iDomain Category
- SSL iDomain Category Group
- SSL iDomain Name
- SSL iDomain Reputation

- SSL iExecuted Action
- SSL iPolicy Action
- SSL iReason For Action
- SSL iURL Set Matched
- SSL iURL Set Private
- Subscriber Identifier
- Svr Tcp Flags Rx
- Svr Tcp Flags Tx
- Tenant Name
- Tracing Req Parent Span ID
- Tracing Req Span ID
- Tracing Trace ID
- Trans Clt Dst IPv4 Address
- Trans Clt Dst IPv6 Address
- Trans Clt Dst Port
- Trans Clt Flow End Usec Rx
- Trans Clt Flow End Usec Tx
- Trans Clt Flow Start Usec Rx
- Trans Clt Flow Start Usec Tx
- Trans Clt IPv4 Address
- Trans Clt IPv6 Address
- Trans Clt Packet Tot Cnt Rx
- Trans Clt Packet Tot Cnt Tx
- Trans Clt RTT
- Trans Clt Src Port
- Trans Clt Tot Rx Oct Cnt
- Trans Clt Tot Tx Oct Cnt
- Trans Info
- Trans Srv Dst Port

- Trans Srv Packet Tot Cnt Rx
- Trans Srv Packet Tot Cnt Tx
- Trans Srv Src Port
- Trans Svr Flow End Usec Rx
- Trans Svr Flow End Usec Tx
- Trans Svr Flow Start Usec Rx
- Trans Svr Flow Start Usec Tx
- Trans Svr RTT
- Trans Svr Tot Rx Oct Cnt
- Trans Svr Tot Tx Oct Cnt
- ID de la transacción
- URL Category
- URL Category Group
- URL Category Reputation
- URL Category Action Reason
- URL Set Matched
- URL set Private
- URL Object ID
- VLAN Number

**Registros de Citrix Virtual Apps and Desktops y Citrix DaaS**

Los registros de Citrix Virtual Apps and Desktops y Citrix DaaS contienen los siguientes puntos de datos:

- Nombre de la aplicación
- Explorador web
- ID de cliente
- Detalles: Tamaño de formato, Tipo de formato, Iniciador, Resultado
- ID de dispositivo
- Tipo de dispositivo

- Comentarios
- ID de comentario
- Nombre del archivo
- Ruta de archivo
- Tamaño de archivo
- Es como
- Prisión rota
- Detalles del trabajo: nombre de archivo, formato, tamaño
- Ubicación: estimación, latitud, longitud

> **Nota**
>
> La información de ubicación se proporciona a nivel de ciudad y país y no representa una geolocalización precisa.

- Línea CMD larga
- Ruta del archivo del módulo
- Operación
- Sistema operativo
- Información adicional sobre la plataforma
- Nombre de impresora
- Pregunta
- ID de pregunta
- Nombre de la aplicación SaaS
- Dominio de sesión
- Nombre del servidor de sesión
- Nombre de usuario de sesión
- GUID de sesión
- Timestamp
- Zona horaria: sesgo, horario de verano, nombre
- Total de copias impresas
- Total de páginas impresas

- Tipo
- URL
- Agente de usuario

**Registros de Citrix ADC**

Los registros de Citrix ADC contienen los siguientes puntos de datos:

- Contenedor
- Archivos
- Formato
- Tipo

**Registros de Citrix DaaS Standard for Azure**

Los registros de Citrix DaaS Standard for Azure contienen los siguientes puntos de datos:

- Nombre de la aplicación
- Explorador web
- Detalles: Tamaño de formato, Tipo de formato, Iniciador, Resultado
- ID de dispositivo
- Tipo de dispositivo
- Nombre del archivo
- Ruta de archivo
- Tamaño de archivo
- Prisión rota
- Detalles del trabajo: nombre de archivo, formato, tamaño
- Ubicación: estimación, latitud, longitud

  > **Nota**
  >
  > La información de ubicación se proporciona a nivel de ciudad y país y no representa una geolocalización precisa.

- Línea CMD larga
- Ruta del archivo del módulo

- Operación
- Sistema operativo
- Información adicional sobre la plataforma
- Nombre de impresora
- Nombre de la aplicación SaaS
- Dominio de sesión
- Nombre del servidor de sesión
- Nombre de usuario de sesión
- GUID de sesión
- Timestamp
- Zona horaria: sesgo, horario de verano, nombre
- Tipo
- URL
- Agente de usuario

**Registros del proveedor de identidad de Citrix**

- Inicio de sesión de usuario:
  - Dominios de autenticación: nombre, producto, tipo de proveedor de identidad, nombre para mostrar del proveedor de identidad
    - Propiedades del IdP: aplicación, tipo de autenticación, ID de cliente, ID de cliente, directorio, emisor, logotipo, recursos, TID
    - Extensiones:
      - Espacio de trabajo: color de fondo, logotipo de encabezado, logotipo de inicio de sesión, color de enlace, color de texto, dominios de StoreFront
      - ShareFile: ID de cliente, geometría del cliente
      - Token de larga duración: habilitado, tipo de caducidad, segundos de caducidad absoluta, segundos de caducidad deslizantes
  - Resultado de autenticación: nombre de usuario, mensaje de error
  - Mensaje de inicio de sesión: ID de cliente, nombre del cliente

  - Reclamación de usuario: AMR, hash de token de acceso, Aud, tiempo de autenticación, credo CIP, alias de autenticación, dominios de autenticación, grupos, producto, alias del sistema, correo electrónico, correo electrónico
    verificado, Exp, apellido, nombre de pila, IAT, IdP, ISS, configuración regional, nombre, NBF, SID, sub
    * Reclamaciones de alias de autenticación: nombre, valor
    * Contexto de directorio: dominio, Forrest, proveedor de identidad, ID de arrendatario
    * Usuario: Clientes, correo electrónico, OID, SID, UPN
    * Campos adicionales del proveedor de identidades: Azure AD OID, Azure AD TID
- Cierre de sesión de usuario: ID de cliente, nombre de cliente, nombre de usuario, sub
- Actualización del cliente: acción, ID de cliente, nombre del cliente

**registros de Citrix Gateway**

- Eventos de transacción:
  - Aplicación ICA: Record Type, Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, ICA Session Guid, MSI Client Cookie, Flow Id Rx, ICA Flags, Connection Id, Padding Octets Two, ICA Device Serial Number, IP Version 4, Protocol Identifier, Source IPv4 Address Rx, Destination IPv4 Address Rx, Source Transport Port Rx, Destination Transport Port Rx, ICA Application Start up Duration, ICA Launch Mechanism, ICA Application Start up Time, ICA Process ID Launch, ICA Application Name, ICA App Module Path, ICA Application Termination Type, ICA Application Termination Time, Application Name App Id, ICA App Process ID Terminate, ICA App
  - Evento ICA: Record Type, Actual Template Code, Source IPv4 Address Rx, Destination IPv4 Address Rx, ICA Session Guid, MSI Client Cookie, Connection Chain ID, ICA Client Version, ICA Client Host Name, ICA User Name, ICA Domain Name, Logon Ticket Setup, Server Name, Server Version, Flow Id Rx, ICA Flags, Observation Point Id, Exporting Process Id, Observation Domain Id, Connection Id, ICA Device Serial Number, ICA Session Setup Time, ICA Client IP, NS ICA Session Status Setup, Source Transport Port Rx, Destination Transport Port Rx, ICA Client Launcher, ICA Client Type, ICA Connection Priority Setup, NS ICA Session Server Port, NS ICA Session Server IP Address, IPv4, Protocol Identifier,Connection Chain Hop Count, Access Type
  - Actualización de ICA: Record Type, Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, ICA Session Guid, MSI Client Cookie, Flow Id Rx,ICA Flags, Connection Id, ICA Device Serial Number, IPv4, Protocol Identifier, Padding Octets

Two, ICA RTT, Client Side RX Bytes, Client Side Packets Retransmit, Server Side Packets Retransmit, Client Side RTT, Client Side Jitter, Server Side Jitter, ICA Network Update Start Time, ICA Network Update End Time, Client Side SRTT, Server Side SRTT,Client Side Delay, Server Side Delay, Host Delay, Client Side Zero Window Count, Server Side Zero Window Count, Client Side RTO Count, Server Side RTO Count, L7 Client Latency, L7 Server Latency, App Name App Id, Tenant Name, ICA Session Update Begin Sec, ICA Session Update End Sec, ICA Channel Id 1, ICA Channel Id 2, ICA Channel Id 2 Bytes, ICA Channel Id 3, ICA Channel Id 3 Bytes, ICA Channel Id 4, ICA Channel Id 4 Bytes, ICA Channel Id 5, ICA Channel Id 5 Bytes

- Configuración de AppFlow: Record Type, Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, System Rule Flag 1, System Safety Index, AppFlow Profile Relaxed Flags, AppFlow Profile Block Flags, AppFlow Profile Log Flags, AppFlow Profile Learn Flags, AppFlow Profile Stats Flags, AppFlow Profile None Flags, AppFlow App Name Id, AppFlow Profile Sign Disabled, AppFlow Profile Sign Block Count, AppFlow Profile Sign Log Count, AppFlow Profile Sign Stat Count, AppFlow Incarnation Number,AppFlow Sequence Number, AppFlow Profile Sign Auto Update, AppFlow Safety Index, AppFlow App Safety Index, AppFlow Profile Sec Checks Safety Index, AppFlow Profile Type, Iprep App Safety Index, AppFlow Profile Name, AppFlow Sig Name, AppFlow App Name Ls, AppFlow Sig Rule ID1, AppFlow Sig Rule ID2, AppFlow Sig Rule ID3, AppFlow Sig Rule ID4, AppFlow Sig Rule ID5, AppFlow Sig Rule Enabled Flags, AppFlow Sig Rule Block Flags, AppFlow Sig Rule Log Flags, AppFlow Sig Rule File Name, AppFlow Sig Rule Category1, AppFlow Sig Rule Logstring1, AppFlow Sig Rule Category2, AppFlow Sig Rule Logstring2, AppFlow Sig Rule Category3, AppFlow Sig Rule Category4, AppFlow Sig Rule Logstring4, AppFlow Sig Rule Category5, AppFlow Sig Rule LogString5
- AppFlow: Actual Template Code, Observation Domain Id, Observation Point Id, Exporting Process Id, Transaction Id, Appfw Violation Occurred Time, App Name App Id, Appfw Violation Severity, Appfw Violation Type, Appfw Violation Location, Appfw Violation Threat Index, Appfw NS Longitude, Appfw NS Latitude, Source IPv4 Address Rx, Appfw Http Method, Appfw App Threat Index, Appfw Block Flags, Appfw Transform Flags, Appfw Violation Profile Name, Appfw Session Id, Appfw Req Url, Appfw Geo Location, Appfw Violation Type Name 1, Appfw Violation Name Value 1, Appfw Sig Category 1, Appfw Violation Type Name 2, Appfw Violation Name Value 2, Appfw Sig Category 2, Appfw Violation Type Name 3, Appfw Violation Name Value 3, Appfw Sig Category3, Appfw Req X Forwarded For, Appfw App Name Ls,App Name Ls, Iprep Category, Iprep Attack Time, Iprep Reputation Score, Iprep NS Longitude, Iprep NS Latitude, Iprep Severity, Iprep HTTP Method, Iprep App Threat Index, Iprep Geo Location, Tcp Syn Attack Cntr, Tcp Slow Ris Cntr, Tcp Zero Window Cntr, Appfw Log Expr Name, Appfw Log Expr Value, Appfw Log Expr Comment
- VPN: Actual Template Code, Observation Domain Id, Access Insight Flags, Observation

Point Id, Exporting Process Id, Access Insight Status Code, Access Insight Timestamp, Authentication Duration, Device Type, Device ID, Device Location, App Name App Id, App Name App Id1, Source Transport Port Rx, Destination Transport Port Rx, Authentication Stage, Authentication Type, VPN Session ID, EPA Id, AAA User Name, Policy Name, Auth Agent Name, Group Name, Virtual Server FQDN, cSec Expression, Source IPv4 Address Rx, Destination IPv4 Address Rx, Cur Factor Policy Label, Next Factor Policy Label, App Name Ls, App Name 1 Ls,AAA User Email Id, Gateway IP, Gateway Port, Application Byte Count, VPN Session State, VPN Session Mode, SSO Auth Method, IIP Address, VPN Request URL, SSO Request URL, Backend Server Name, VPN Session Logout Mode, Logon Ticket File Info, STA Ticket, Session Sharing Key, Resource Name, SNIP Address, Temp VPN Session ID

- HTTP: Actual Template Code, Http Req Method, Http Req Url, Http Req User Agent, Http Content Type, Http Req Host, Http Req Authorization, Http Req Cookie, Http Req Referer, Http Res Set Cookie, Ic Cont Grp Name, Ic Flags, Ic Nostore Flags, Ic Policy Name, Response Media Type, Ingress Interface Client, Origin Res Status, Origin Rsp Len, Srv Flow Flags Rx, Srv Flow Flags Tx, Flow Flags Rx, Flow Flags Tx, App Name, Observation Point Id, Exporting Process Id, Observation Domain Id, Http Trans End Time, Transaction Id, Http Rsp Status, Trans Clt Ipv4 Address, Trans Clt Dst Ipv4 Address, Backend Svr Dst Ipv4 Address, Backend Svr Ipv4 Address, Http Rsp Len, Trans Svr RTT, Trans Clt RTT, Http Req Rcv FB, Http Req Rcv LB, Http Res Rcv FB, Http Res Rcv LB, Http Req Forw FB, Http Req Forw LB, Http Res Forw FB, Http Res Forw LB, Http Req X Forwarded For, Http Domain Name, Http Res Location, Protocol Identifier, Egress Interface, Backend Svr Ipv6 Address, SSL Flags BE, SSL Flags FE, SSL Session IDFE, SSL Session IDBE, SSL Cipher Value FE, SSL Cipher Value BE, SSL Sig Hash Alg BE, SSL Sig Hash Alg FE, SSL Srvr Cert Sig Hash BE, SSL Srvr Cert Sig Hash FE, SSL Clnt Cert Sig Hash FE, SSL Clnt Cert Sig Hash BE, SSL Server Cert Size FE, SSL Server Cert Size BE, SSL Client Cert Size FE, SSL Client Cert Size BE, SSL Err App Name, SSL Err Flag, SSL Handshake Error Msg, Client IP, Virtual Server IP, Connection Chain Id, Connection Chain Hop Count, Trans Clt Tot Rx Oct Cnt, Trans Clt TotTx Oct Cnt, Trans Clt Src Port, Trans Clt Dst Port, Trans Srv Src Port, Trans Srv Dst Port, VLAN Number, Client Mss, Trans Info, Trans Clt Flow End Usec Rx, Trans Clt Flow End Usec Tx, Trans Clt Flow Start Usec Rx, Trans Clt Flow Start Usec Tx, Trans Svr Flow End Usec Rx, Trans Svr Flow End Usec Tx, Trans Svr Flow Start Usec Rx, Trans Svr Flow Start Usec Tx, Trans Svr Tot Rx Oct Cnt, Trans Svr Tot Tx Oct Cnt, Clt Flow Flags Tx, Clt Flow Flags Rx, Trans Clt Ipv6 Address, Trans Clt Dst Ipv6 Address, Subscriber Identifier, SSLi Domain Name, SSLi Domain Category, SSLi Domain Category Group, SSLi Domain Reputation, SSLi Policy Action, SSLi Executed Action, SSLi Reason For Action, SSLi URL Set Matched, SSLi URL Set Private, URL Category, URL Category Group, URL Category Reputation, Responder Action Type, URL Set Matched, URL Set Private, Category Domain Name, Category Domain Source, AAA User Name, VPN Session ID, Tenant Name

- Eventos métricos:

- Equilibrio de carga de vServer: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, CPU, GSLB Server, GSLB VServer, Interface, Memory Pool, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer LB: RATE Si Tot Request Bytes, RATE Si Tot Requests, RATE Si Tot Response Bytes, RATE Si Tot Responses, RATE Si Tot Clt Ttlb Transactions, RATE Si Tot Clt Ttlb Pkt Rcvd, RATE Si Tot Clt Ttlb Pkt Sent, RATE Vsvr Tot Hits, Si Cur Clients, Si Cur Conn Established, Si Cur Servers, Si Cur State, Si Tot Request Bytes, Si Tot Responses, Si Tot Clt Ttlb, Si Tot Clt Ttlb Transactions, Si Tot Pkt Rcvd, Si Tot Pkt Sent, Si Tot Ttlb Frustrating Transactions, Si Tot Ttlb Tolerating Transactions, Vsvr Active Svcs, Vsvr Tot Hits, Vsvr tot Req Resp Invalid, Vsvr Tot Req Resp Invalid Dropped
- CPU: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, Cc CPU Use GSLB Server, GSLB Vserver, Interface, Memory Pool, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User
- Grupo de servicios del servidor: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, Cc CPU Use, GSLB Server, GSLB Vserver, Interface, Memory Pool, NetScaler, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User, Server Service Group: RATE Si Tot Request Bytes, RATE Si Tot Requests, RATE Si Tot_Response Bytes, RATE Si Tot Responses, RATE Si Tot Clt Ttlb, RATE Si Tot Clt Ttlb Transactions, RATE Si Tot Svr Ttfb, RATE Si Tot Svr Ttfb Transactions, RATE Si Tot Svr Ttlb, RATE Si Tot Svr Ttlb Transactions, RATE Si Tot Ttlb Frustrating Transactions, RATE Si Tot Ttlb Tolerating Transactions, Si Cur State, Si Tot Request Bytes, Si Tot Requests, Si Tot Response Bytes, Si Tot Responses, Si Tot Clt Ttlb, Si Tot Clt Ttlb Transactions, Si Tot Svr Ttfb, Si Tot Svr Ttfb Transactions,Si Tot Svr Tlb, Si Tot Svr Ttlb Transactions, Si Tot Ttlb Frustrating Transactions, Si Tot Ttlb Tolerating Transactions
- CFG del SVC de servidor: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Representation, Schema Type, Time, CPU Use, GSLB Server, GSLB Vserver, Interface, Memory Pool, NetScaler, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User, Server Svc Cfg: RATE Si Tot Request Bytes, RATE Si Tot Requests, RATE Si Tot Response Bytes, RATE Si Tot Responses, Si Tot Clt Ttlb, RATE Si Tot Clt Ttlb Transactions, RATE Si Tot Pkt Rcvd, RATE Si Tot Pkt Sent, RATE Si Tot Svr Busy Err, RATE Si Tot Svr Ttfb, RATE Si Tot Svr Ttfb Transactions, RATE Si Tot Svr Ttlb, RATE Si Tot Svr Ttlb Transactions, RATE Si Tot Ttlb Frustrating Transactions, RATE Si Tot Ttlb Tolerating Transactions, Si Cur State, Si Cur Transport, Si Tot Request Bytes, Si Tot Requests, Si Tot Response Bytes, Si Tot Responses, Si Tot Clt Ttlb, Si Tot Clt Ttlb Transactions, Si Tot Pkt Rcvd, Si Tot Pkt Sent, Si Tot Svr Busy Err, Si Tot Svr Ttfb, Si Tot Svr Ttfb Transactions, Si Tot Svr Ttlb, Si Tot Svr Ttlb Transactions, Si Tot Ttlb Frustrating Transactions, Si Tot Ttlb Tolerating Transactions
- NetScaler: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Represen-

tation, Schema Type, Time, GSLB Server, GSLB VServer, Interface, Memory Pool, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User, NetScaler: RATE All Nic Tot Rx Mbits, RATE All Nic Tot Rx Mbits, RATE Dns Tot Queries, RATE Dns Tot Neg Nxdmn Entries,RATE Http Tot Gets, RATE Http Tot Others, RATE Http Tot Posts, RATE Http Tot Requests, RATE Http Tot Requests 1.0, RATE Http Tot Requests 1.1, RATE Http Tot Responses, RATE Http Tot Rx Request Bytes, RATE Http Tot Rx Response Bytes, RATE Ip Tot Rx Mbits, RATE Ip Tot Rx Bytes, RATE Ip Tot Rx Pkts, RATE Ip Tot Tx Mbits, RATE Ip Tot Tx Bytes, RATE Ip Tot Tx Pkts, RATE SSL Tot Dec Bytes, RATE SSL Tot Enc Bytes,RATE SSL Tot SSL Info Session Hits, RATE SSL Tot SSL Info Total Tx Count, RATE Tcp Err Rst, RATE Tcp Tot Client Open, RATE Tcp Tot Server Open, RATE Tcp Tot Rx Bytes, RATE Tcp Tot Rx Pkts, RATE Tcp Tot Syn, RATE Tcp Tot Tx Bytes, RATE Tcp Tot Tx Pkts, RATE Udp Tot Rx Bytes, RATE Udp Tot Rx Pkts, RATE Udp Tot Tx Bytes, RATE Udp Tot Tx Pkts, All Nic Tot Rx Mbits, All Nic Tot Tx Mbits, Cpu Use, Dns Tot Queries, Dns Tot Neg Nxdmn Entries, Http Tot Gets, Http Tot Others, Http Tot Posts, Http Tot Requests, Http Tot Requests1.0, Http Tot Requests1.1, Http Tot Responses, Http Tot Rx Request Bytes, Http Tot Rx Response Bytes, Ip Tot Rx Mbits, Ip Tot Rx Bytes, Ip Tot Rx Pkts, Ip Tot Tx Mbits, Ip Tot Tx Bytes, Ip Tot Tx Pkts, Mem Cur Free size, Mem Cur Free size Actual, Mem Cur Used size, Mem Tot Available, Mgmt Additional Cpu Use, Mgmt Cpu 0 Use, Mgmt Cpu Use, SSL Tot Dec Bytes, SSL Tot Enc Bytes, SSL Tot SSL Info Session Hits, SSL Tot SSL Info Total Tx Count, Sys Cpus, Tcp Cur Client Conn, Tcp Cur Client Conn Closing, Tcp Cur Client Conn Est, Tcp Cur Server Conn, Tcp Cur Server Conn Closing, Tcp Cur Server Conn Est, Tcp Err Rst, Tcp Tot Client Open, Tcp Tot Server Open, Tcp Tot Rx Bytes, Tcp Tot Rx Pkts, Tcp Tot Syn, Tcp Tot Tx Bytes, Tcp Tot Tx Pkts, Udp Tot Rx Bytes, Udp Tot Rx Pkts, Udp Tot Tx Bytes, Udp Tot Tx Pkts

- Grupo de memoria: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Schema Type, Time, CPU, Gslb Server, Gslb VServer, Interface, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, VServer Lb, VServer SSL, VServer User, Memory Pool: Mem Cur Alloc Size, Mem Err Alloc Failed, Mem Tot Available
- Enlace del servicio de supervisión: Bind Entity Name, Entity Name, NetScalerId, SchemaType, Time, CPU, Gslb Server, Gslb VServer, Interface, Memory Pool, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, Vserver Lb, VServer SSL, VServer User, Mon Service Binding: RATE Mon Tot Probes, Mon Tot Probes
- Interfaz: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Schema Type, Time, CPU, Gslb Server, Gslb VServer, Memory Pool, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, Vserver Lb, VServer SSL, VServer User, Interface: RATE NIC Tot Rx Bytes, RATE NIC Tot Rx Packets, RATE NIC Tot Tx Bytes, RATE NIC Tot Tx Packets, NIC Tot Rx Bytes, NIC Tot Rx Packets, NIC Tot Tx Bytes, NIC Tot Tx Packets

  - CS de vServer: Bind Entity Name, Entity Name, Mon Service Binding, NetScaler Id, Schema Type, Time, CPU, Gslb Server, Gslb VServer, Memory Pool, NetScaler, Server Service Group, Server Svc Cfg, VServer Authn, VServer Cr, VServer Cs, Vserver Lb, VServer SSL, VServer User, VServer Cs: RATE Si Tot Request Bytes, RATE Si Tot Requests, RATE Si Tot Response Bytes, RATE Si Tot Responses, RATE Si Tot Clt Ttlb,RATE Si Tot Clt Ttlb Transactions, RATE Si Tot Pkt Rcvd, RATE Si Tot Pkt Sent, RATE Si Tot Ttlb Frustrating Transactions, RATE Si Tot Ttlb Tolerating Transactions, RATE Vsvr Tot Hits, Si Cur State, Si Tot Request Bytes, Si Tot Requests, Si Tot Response Bytes, Si Tot Responses, Si Tot Clt Ttlb, Si Tot Clt Ttlb Transactions, Si Tot Pkt Rvd, Si Tot Pkt Sent, Si Tot Ttlb Frustrating Transactions, Si Tot Tlb Tolerating Transactions, Vsvr Tot Hits, Vsvr Tot Req Resp Invalid, Vsvr Tot Req Resp Invalid Dropped

**Registros del explorador seguro**

- Publicación de aplicación:
  - Registros antes de la aplicación publicada: Authentication, Browser, Change Id, Created, Customer Name, Destination URL, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External, Whitelist Internal, Whitelist Redirect
  - Registros después de la aplicación publicada: Authentication, Browser, Change Id, Created, Customer Name, Destination, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External URL, Whitelist Internal URL, Whitelist Redirect URL
- Eliminación de aplicaciones:
  - Registros antes de la aplicación publicada: Authentication, Browser, Change Id, Created, Customer Name, Destination URL, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External, Whitelist Internal, Whitelist Redirect
  - Registros después de la aplicación publicada: Authentication, Browser, Change Id, Created, Customer Name, Destination, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External URL, Whitelist Internal URL, Whitelist Redirect URL
- Actualización de aplicaciones:

  - Registros antes de la aplicación publicada: Authentication, Browser, Change Id, Created, Customer Name, Destination URL, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External, Whitelist Internal, Whitelist Redirect
  - Registros después de la aplicación publicada: Authentication, Browser, Change Id, Created, Customer Name, Destination, E-Tag, Gateway Service Product Id, Session Id, Legacy Icon, Application Name, Policies, Published Application Id, Region, Resource Zone, Resource Zone Id, Subscription, Session Idle Timeout, Session Idle Timeout Warning, Watermark, Whitelist External URL, Whitelist Internal URL, Whitelist Redirect URL

- Creación de derechos:
  - Registros anteriores a la creación del derecho: aprobado, identificador de cliente, días de retención de datos, fecha de finalización, identificador de sesión, SKU del producto, cantidad, números de serie, fecha de inicio, estado, tipo
  - Registros posteriores a la creación del derecho: aprobado, identificador de cliente, días de retención de datos, fecha de finalización, identificador de sesión, SKU del producto, cantidad, números de serie, fecha de inicio, estado, tipo
- Actualización de derechos:
  - Registros anteriores a la actualización del derecho: aprobado, identificador de cliente, días de retención de datos, fecha de finalización, identificador de sesión, SKU del producto, cantidad, números de serie, fecha de inicio, estado, tipo
  - Registros posteriores a la actualización del derecho: aprobado, identificador de cliente, días de retención de datos, fecha de finalización, identificador de sesión, SKU del producto, cantidad, números de serie, fecha de inicio, estado, tipo
- Host de acceso a sesiones: Accept Host, Client IP, Date Time, Host, Session, User Name
- Conexión de sesión:
  - Registros antes de la conexión de la sesión: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
  - Registros después de la conexión de la sesión: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
- Inicio de sesión:

  - Registros antes del inicio de la sesión: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
  - Registros después del inicio de la sesión: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
- Marca de sesión:
  - Registros antes de la marca de la sesión: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name
  - Registros después de la marca de la sesión: Application Id, Application Name, Browser, Created, Customer Id, Duration, Session Id, IP Address, Last Updated, Launch Source, User Name

**Registros de Microsoft Graph Security**

- ID de arrendatario
- ID de usuario
- ID del indicador
- Indicador UUID
- Hora del evento
- Crear tiempo
- Categoría de alerta
- Ubicación de inicio de sesión
- IP de inicio de sesión
- Tipo de inicio de sesión
- Tipo de cuenta de usuario
- Información del proveedor
- Información de proveedor del vendedor
- Estados de vulnerabilidad
- Gravedad de vulnerabilidad

**Registros de Microsoft Active Directory**

- ID de arrendatario
- Recoger tiempo
- Tipo
- Contexto de directorio
- Grupos
- Identidad
- Tipo de usuario
- Nombre de cuenta
- Recuento de contraseña incorrecta
- City
- Nombre común
- Empresa
- País
- Días hasta el vencimiento de la contraseña
- Departamento
- Descripción
- Display Name
- Nombre distinguido
- Correo electrónico
- Número de fax
- Nombre
- Categoría de grupo
- Ámbito de grupo
- Teléfono de casa
- Iniciales
- Teléfono IP
- ¿Está habilitada la cuenta
- Está bloqueada la cuenta

- Es un grupo de seguridad
- Apellido
- Gestor
- Miembro de
- Teléfono móvil
- Buscapersonas
- La contraseña nunca caduca
- Nombre de la oficina de entrega física
- Oficina de correos
- Código postal
- ID de grupo principal
- Estado
- Dirección
- Título
- Control de cuentas de usuario
- Lista de grupos de usuarios
- Nombre principal del usuario
- Teléfono de trabajo

### Registros de Citrix Analytics para rendimiento

- actionid
- actionreason
- actiontype
- adminfolder
- agentversion
- allocationtype
- applicationid
- applicationname
- applicationpath

- applicationtype
- applicationversion
- associateduserfullnames
- associatedusername
- associatedusernames
- associateduserupns
- authenticationduration
- autoreconnectcount
- autoreconnecttype
- AvgEndpointThroughputBytesReceived
- AvgEndpointThroughputBytesSent
- blobcontainer
- blobendpoint
- blobpath
- brokerapplicationchanged
- brokerapplicationcreated
- brokerapplicationdeleted
- brokeringdate
- brokeringduration
- brokerloadindex
- brokerregistrationstarted
- browsername
- catalogchangeevent
- catalogcreatedevent
- catalogdeletedevent
- catalogid
- catalogname
- catalogsync
- clientaddress

- nombre_cliente
- clientplatform
- clientsessionvalidatedate
- clientversion
- collecteddate
- connectedviahostname
- connectedviaipaddress
- connectionid
- connectioninfo
- connectionstate
- connectiontype
- controllerdnsname
- cpu
- cpuindex
- createddate
- currentloadindexid
- currentpowerstate
- currentregistrationstate
- currentsessioncount
- datetime
- deliverygroupadded
- deliverygroupchanged
- deliverygroupdeleted
- deliverygroupid
- deliverygroupmaintenancemodechanged
- deliverygroupname
- deliverygroupsync
- deliverytype
- deregistrationreason

- desktopgroupdeletedevent
- desktopgroupid
- desktopgroupname
- desktopkind
- disconnectcode
- disconnectreason
- disk
- diskindex
- dnsname
- domainname
- effectiveloadindex
- enddate
- errormessage
- establishmentdate
- eventreporteddate
- eventtime
- exitcode
- failurecategory
- failurecode
- failuredata
- failuredate
- failurereason
- failuretype
- faultstate
- functionallevel
- gpoenddate
- gpostartdate
- hdxenddate
- hdxstartdate

- host
- hostedmachineid
- hostedmachinename
- hostingservername
- hypervisorconnectionchangedevent
- hypervisorconnectioncreatedevent
- hypervisorid
- hypervisorname
- hypervisorsync
- icartt
- icarttms
- id
- idletime
- inputbandwidthavailable
- inputbandwidthused
- instancecount
- interactiveenddate
- interactivestartdate
- ipaddress
- isassigned
- isinmaintenancemode
- ismachinephysical
- ispendingupdate
- ispreparing
- isremotepc
- issecureica
- lastderegisteredcode
- launchedviahostname
- launchedviaipaddress

- lifecyclestate
- LinkSpeed
- logonduration
- logonenddate
- logonscriptsenddate
- logonscriptsstartdate
- logonstartdate
- long
- machineaddedtodesktopgroupevent
- machineassignedchanged
- machinecatalogchangedevent
- machinecreatedevent
- machinedeletedevent
- machinederegistrationevent
- machinednsname
- machinefaultstatechangeevent
- machinehardregistrationevent
- machineid
- machinemaintenancemodechangeevent
- machinename
- machinepvdstatechanged
- machineregistrationendedevent
- machineremovedfromdesktopgroupevent
- machinerole
- machinesid
- machineupdatedevent
- machinewindowsconnectionsettingchanged
- memory
- memoryindex

- modifieddate
- NGSConnector.ICAConnection.Start
- NGSConnector.NGSSyntheticMetrics
- NGSConnector.NGSPassiveMetrics
- NGSConnector.NGSSystemMetrics
- network
- networkindex
- networklatency
- networkinfoperiodic
- NetworkInterfaceType
- ostype
- outputbandwidthavailable
- outputbandwidthused
- path
- percentcpu
- persistentuserchanges
- powerstate
- processname
- profileloadenddate
- profileloadstartdate
- protocolo
- provisioningschemeid
- provisioningtype
- publishedname
- registrationstate
- serversessionvalidatedate
- sessioncount
- sessionend
- sessionfailure

- sessionid
- sessionidlesince
- sessionindex
- sessionkey
- sessionstart
- sessionstate
- sessionsupport
- sessiontermination
- sessiontype
- sid
- SignalStrength
- siteid
- sitename
- startdate
- totalmemory
- triggerinterval
- triggerlevel
- triggerperiod
- triggervalue
- usedmemory
- userid
- userinputdelay
- username
- usersid
- vdalogonduration
- vdaprocessdata
- vdaresourcedata
- version
- vmstartenddate

- vmstartstartdate
- windowsconnectionsetting
- xd.SessionStart

## Requisitos del sistema

September 11, 2024

Antes de empezar a usar Citrix Analytics for Security, revise los siguientes requisitos.

### Suscripción a Citrix Analytics for Security

Este producto de Analytics es una oferta basada en suscripción. Debe tener una suscripción válida para usar Security Analytics. Para obtener más información, consulte la página de descripción general del producto .

### Requisitos de orígenes de datos

Citrix Analytics for Security recibe eventos de varios orígenes de datos. Para que Analytics funcione correctamente, debe tener una suscripción válida para usar al menos uno de los siguientes productos, que actúan como orígenes de datos para Analytics:

- Citrix ADC (local) junto con la suscripción a Citrix Application Delivery Management
- Servicio Citrix Endpoint Management
- Citrix Gateway (local)
- Proveedor de identidades Citrix
- Citrix Remote Browser Isolation
- Servicio Citrix Secure Private Access
- Citrix Virtual Apps and Desktops o Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service)
- Microsoft Active Directory
- Microsoft Graph Security

### Exploradores web compatibles

Para acceder a Analytics, su estación de trabajo debe tener el siguiente navegador web compatible:

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

## Gestionar las funciones de administrador para Security

September 11, 2024

> **Nota:**
>
> Desde julio de 2023, Microsoft cambió el nombre de Azure Active Directory (Azure AD) a Microsoft Entra ID. En este documento, cualquier referencia a Azure Active Directory, Azure AD o AAD ahora se refiere a Microsoft Entra ID.

Como administrador de Citrix Cloud con permisos de acceso total, puede invitar a otros administradores a administrar la oferta de Security Analytics y asignarles una de las siguientes funciones personalizadas:

- **Análisis de seguridad: administrador total**
- **Análisis de seguridad: administrador de solo lectura**

Puede agregar nuevos administradores de dos maneras: individualmente como usuarios o mediante grupos de Azure Active Directory. Para obtener más información sobre cómo agregar nuevos administradores, consulte Administrar funciones de administrador.

> **Nota:**
> Si a un usuario se le concede acceso directamente como usuario y a través de un grupo de Azure Active Directory, el acceso otorgado individualmente al usuario surtirá efecto.

### Permisos para las funciones personalizadas

Los administradores con la función **Security Analytics: administrador total** pueden acceder a todas las características y funcionalidades de la oferta de Security Analytics. Pueden usar y modificar las funciones de acuerdo con sus requisitos organizativos. Por ejemplo, un administrador completo puede crear indicadores de riesgo personalizados, habilitar geocercas y crear directivas.

Los administradores con la función de **administrador de solo lectura de Security Analytics** solo pueden acceder y ver los paneles de seguridad: usuarios, acceso de usuarios, acceso a aplicaciones, garantía de acceso e informes. Pueden supervisar el comportamiento de los usuarios y ver los eventos de los usuarios en estos paneles. Sin embargo, no se les permite realizar ninguna tarea crítica, como:

- Activar o desactivar el procesamiento de datos para los orígenes de datos
- Crear o eliminar directivas y acciones
- Aplicar acciones manualmente en los indicadores de riesgo que se muestran en el cronograma de riesgo del usuario
- Crear, modificar o eliminar indicadores de riesgo personalizados
- Crear informes personalizados
- Agregar, modificar o eliminar otro usuario administrador
- Agregue o modifique la cerca geográfica para la ubicación de garantía de acceso

### Notificaciones de alertas de seguridad para los administradores

Al igual que los administradores de Citrix Cloud con permisos de acceso total, los administradores con roles personalizados (acceso completo y acceso de solo lectura) reciben notificaciones por correo electrónico de Security Analytics.

Los administradores reciben dos tipos de notificaciones por correo electrónico:

- Notificación semanal sobre las perspectivas de seguridad en su organización. Para obtener más información, consulte Notificación por correo electrónico semanal.
- Notificaciones basadas en la acción Notificar a los administradores. Para obtener más información, consulte Directivas y acciones.

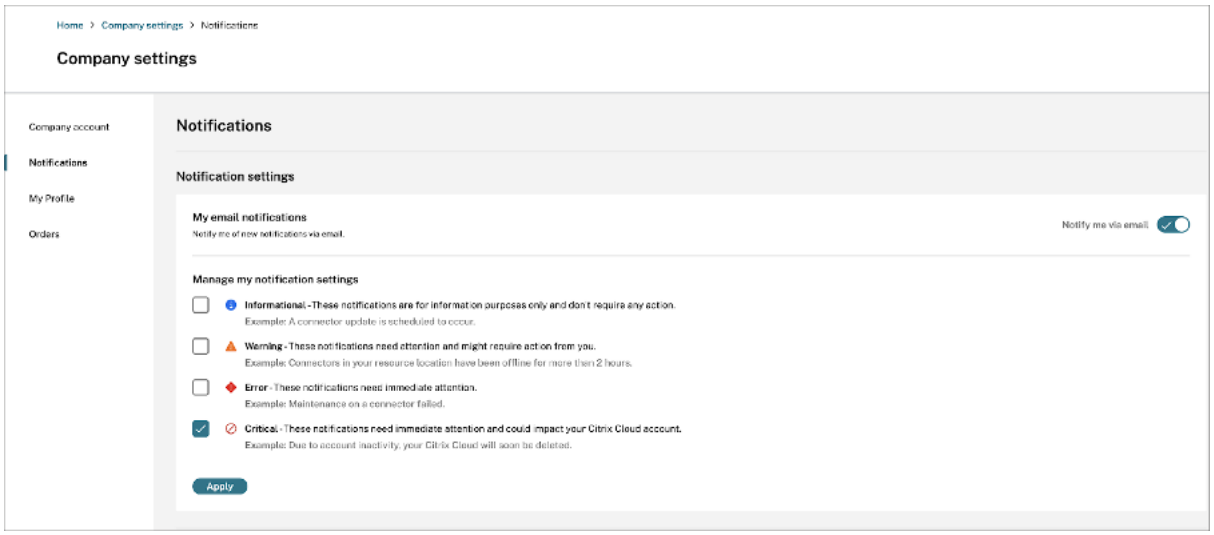
Si es administrador de Citrix Cloud con permiso de acceso completo o personalizado, las notificaciones por correo electrónico están inhabilitadas de forma predeterminada en su cuenta de Citrix Cloud. Para recibir notificaciones por correo electrónico de cualquier servicio de Citrix Cloud, como Citrix Analytics, habilite la opción de notificación en su Citrix Cloud. Para obtener más información, consulte Notificaciones por correo electrónico recibidas. Las preferencias de notificación no están disponibles para los administradores que se agregan a través de Active Directory/Azure AD Groups.

La preferencia de notificación se aprovecha al enviar notificaciones, como correos electrónicos semanales, correos electrónicos de acción de Notificar a los administradores y alertas para la exportación de datos. En cuanto a las notificaciones por correo electrónico, si quiere dejar de recibir correos electrónicos, un administrador con acceso total a Security Analytics debe eliminarlo de la lista de distribu-

ción. Para obtener más información sobre la lista de distribución, consulte Lista de distribución de correo electrónico.

> **Tenga en cuenta**
>
> que los administradores de Citrix Cloud (con permiso de acceso completo o personalizado) no reciben ninguna notificación de otros servicios de Citrix Cloud que aprovechen **las preferencias de notificación**.




Para obtener más información, consulte Administrar administradores de Citrix Analytics.

## Introducción

December 7, 2023

En este documento se describe cómo empezar a utilizar Citrix Analytics for Security por primera vez.

### Paso 1: Inicie sesión en Citrix Cloud

Para usar Citrix Analytics for Security, debe tener una cuenta de Citrix Cloud. Vaya a https://citrix.cloud.com e inicie sesión con su cuenta de Citrix Cloud existente.

Si no tiene una cuenta de Citrix Cloud, primero debe crear una cuenta de Citrix Cloud o unirse a una cuenta existente creada por otra persona de su organización. Para obtener información detallada sobre los procesos e instrucciones sobre cómo proceder, consulte Inscribirse en Citrix Cloud.

### Paso 2: Obtenga acceso a Security Analytics

Puede acceder a Citrix Analytics for Security de una de las siguientes maneras:

- **Solicite una prueba de Citrix Analytics for Security**. Después de iniciar sesión en Citrix Cloud, haga lo siguiente:
  1. En la sección **Servicios disponibles**, haga clic en **Administrar** en el mosaico **Análisis**. Se le redirigirá a la página de descripción general de Analytics.
  2. En el icono **de seguridad**, haga clic en **Solicitar prueba** o póngase en contacto directamente con su cuenta de Citrix o Citrix Partner.
- **Suscríbase a Citrix Analytics for Security**. Para comprar una suscripción a Citrix Analytics for Security, visite https://www.citrix.com/en-in/products/citrix-analytics/form/inquiry/ y póngase en contacto con un experto de Citrix Analytics que pueda ayudarlo.

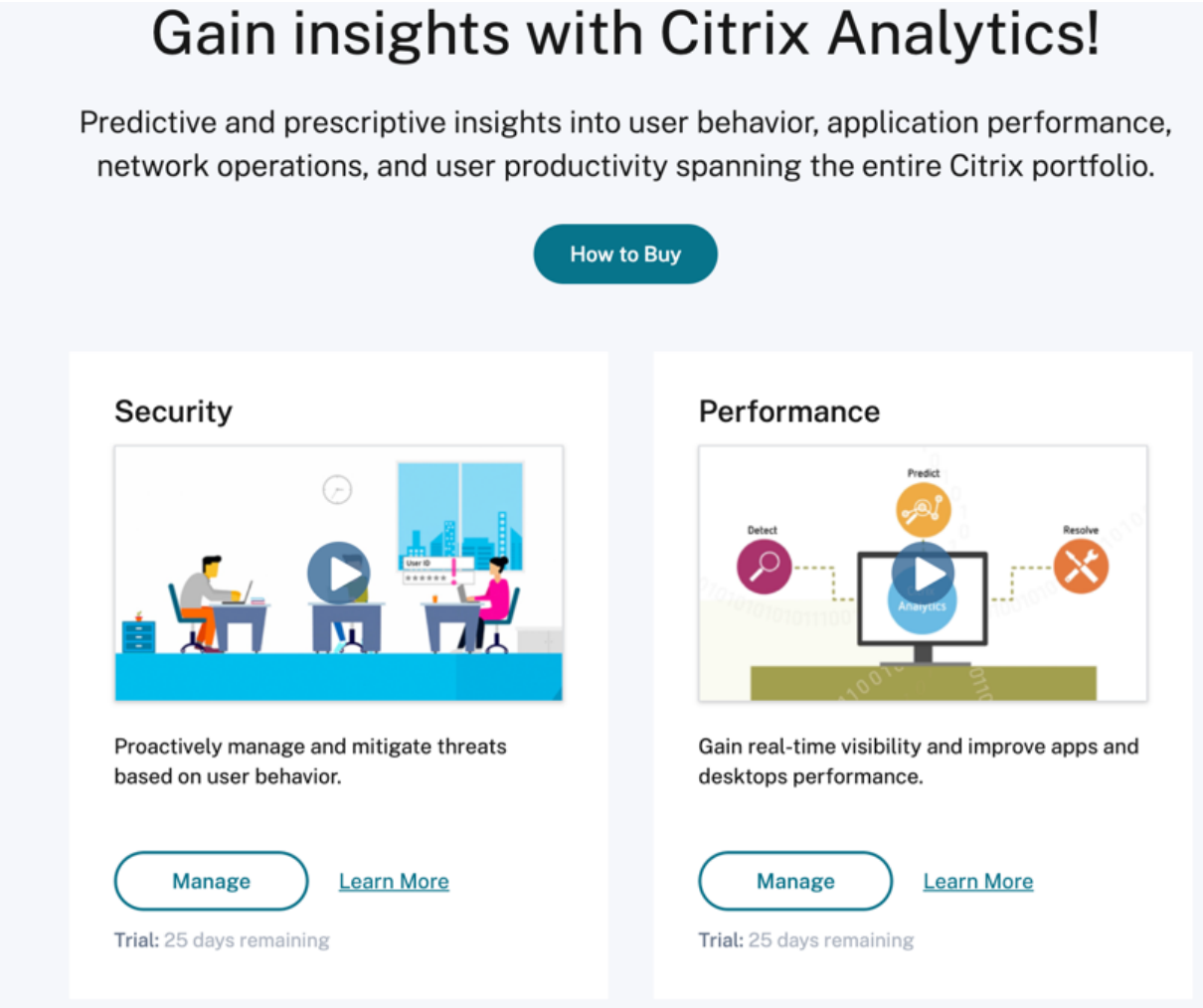
> **Nota**
>
> - A partir del 8 de marzo de 2023, Citrix Analytics for Security dejará de estar disponible como oferta independiente con ShareFile/Citrix Content Collaboration. Anunciamos el complemento independiente de fin de ventas (EOS) y fin de renovaciones (EOR) de Citrix Analytics Service para ShareFile/Citrix Content Collaboration. Los derechos actuales de los clientes para Citrix Analytics for Security siguen siendo válidos hasta que caduque su suscripción. Sin embargo, las integraciones de ShareFile/Citrix Content Collaboration no admitirán las versiones de prueba, las renovaciones ni las nuevas compras. Las integraciones de Citrix Analytics Service para otros productos Citrix se siguen ofreciendo como ofertas independientes o en paquetes con los planes Citrix DaaS existentes, las implementaciones de Citrix Virtual Apps and Desktops y las implementaciones de Citrix Workspace.
> - A partir del 3 de febrero de 2020, Citrix Analytics for Security ya no se incluye en las suscripciones de Workspace Premium y Workspace Premium Plus. Los clientes que hayan adquirido la suscripción a Workspace Premium o Workspace Premium Plus antes del 3 de febrero de 2020 pueden acceder a Citrix Analytics for Security como parte de la suscripción

> a Workspace hasta que caduque su suscripción. Citrix Analytics for Security ahora se ofrece como un servicio adicional con los paquetes de Citrix Workspace: Workspace Standard, Workspace Premium y Workspace Premium Plus. Para obtener más información, consulte Servicios de Citrix Cloud.

### Paso 3: Administrar Security Analytics

Una vez que tenga la suscripción necesaria o haya sido autorizado a acceder a la prueba, en la página de información general de Analytics, el botón **Solicitar prueba** de la oferta de seguridad cambia a **Administrar**. Haga clic en **Administrar** para ver el panel del usuario.




Analytics admite orígenes de datos de Citrix y orígenes de datos externos. Descubre automáticamente los orígenes de datos de Citrix asociadas a su cuenta de Citrix Cloud. Para recibir datos de orígenes de datos externos, debe integrar los orígenes de datos externos con Analytics. Para ver los orígenes de datos detectadas, haga clic en **Configuración > Orígenes de datos > Seguridad**.

## A continuación

- El procesamiento de datos se activa para los siguientes servicios en la nube cuando se aprueba su autorización de Citrix Analytics for Security:
  - Orígenes de datos de Citrix
    - Citrix Secure Private Access
    - Citrix Virtual Apps and Desktops y Citrix DaaS
- Para verificar el estado del procesamiento de datos o saber cómo activarlo manualmente, consulte los siguientes artículos:
  - Orígenes de datos de Citrix:
    - Citrix Endpoint Management
    - Citrix Gateway
  - Orígenes de datos externos:
    - Microsoft Graph Security
    - Microsoft Active Directory
- Exporte los datos procesados de Analytics a los siguientes productos:
  - Splunk
  - Centinela de Microsoft Azure
  - Elasticsearch
  - Otros SIEM que utilizan un conector de datos basado en Kafka o Logstash
- Utilice el panel Usuarios para ver los usuarios descubiertos y sus perfiles de riesgo de seguridad. El panel de **usuarios** es el punto de partida para el análisis del comportamiento de los usuarios y la prevención de amenazas.

  > **Nota**
  >
  > Si utiliza Analytics por primera vez, los perfiles de riesgo de usuario tardan algún tiempo en aparecer en el panel de control. Analytics utiliza el aprendizaje automático para determinar el patrón de riesgo o las anomalías en los eventos de usuario e identifica los perfiles de usuario como de alto riesgo, riesgo medio y riesgo bajo según la gravedad de los riesgos.

- Utilice la función de búsqueda de autoservicio para ver y filtrar los eventos de usuario (datos sin procesar) recibidos de los orígenes de datos.

# Origen de datos de Citrix Endpoint Management

December 6, 2021

La fuente de datos **de Endpoint Management** representa el servicio Citrix Endpoint Management asociado a su cuenta de Citrix Cloud. Cuando los usuarios utilizan este servicio, Citrix Analytics recibe los eventos de usuario relacionados con los puntos de enlace de los usuarios y sus actividades en tiempo real. Los eventos del usuario se procesan para detectar cualquier amenaza de seguridad.

## Requisitos previos

- Suscríbase a Citrix Endpoint Management que ofrece Citrix Cloud. Para obtener información sobre cómo configurar su servicio de Endpoint Management, consulte Configuración de recursos e incorporación.
- **Configuración de Cloud Site y Enterprise Directory**. Asegúrese de que tiene dos máquinas que ejecutan Windows 2012 R2 o Windows 2016 server para instalar Cloud Connector.
- **Cloud Connector instalado**. Descargue e instale Cloud Connector en una máquina virtual que forme parte de Active Directory.
- Revise los requisitos del sistema y asegúrese de que su entorno cumpla con los requisitos.

## Ver la fuente de datos y activar el procesamiento de datos

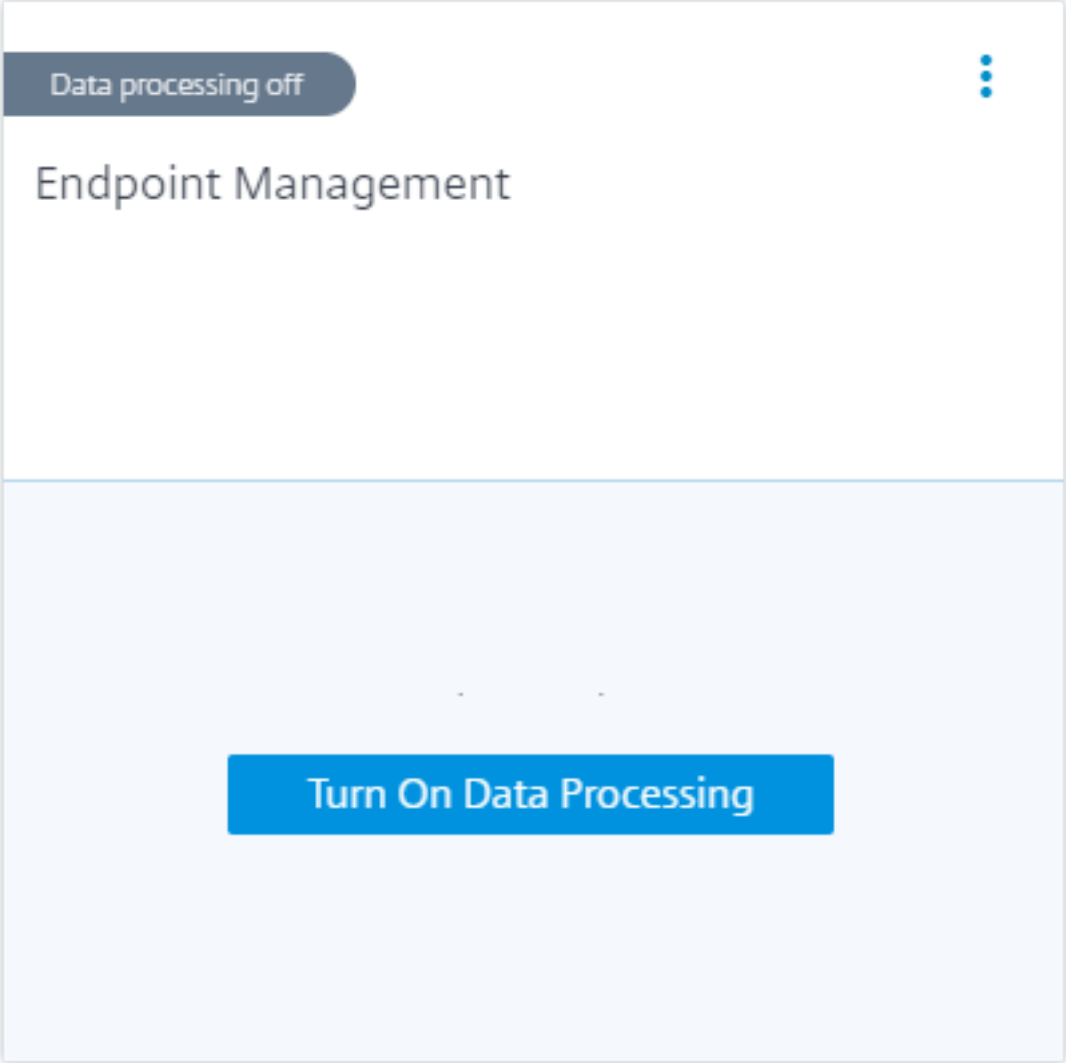
Citrix Analytics descubre automáticamente todas los orígenes de datos de Endpoint Management asociadas a su cuenta de Citrix Cloud.

**Para ver la fuente de datos**:

En la barra superior, haga clic en **Configuración** > **Orígenes de datos** > **Seguridad**.

En la página **Orígenes de datos aparece una tarjeta del sitio para la fuente de datos** de Endpoint Management. Haga clic **en Activar procesamiento de datos** para permitir que Citrix Analytics comience a procesar los datos de esta fuente de datos.

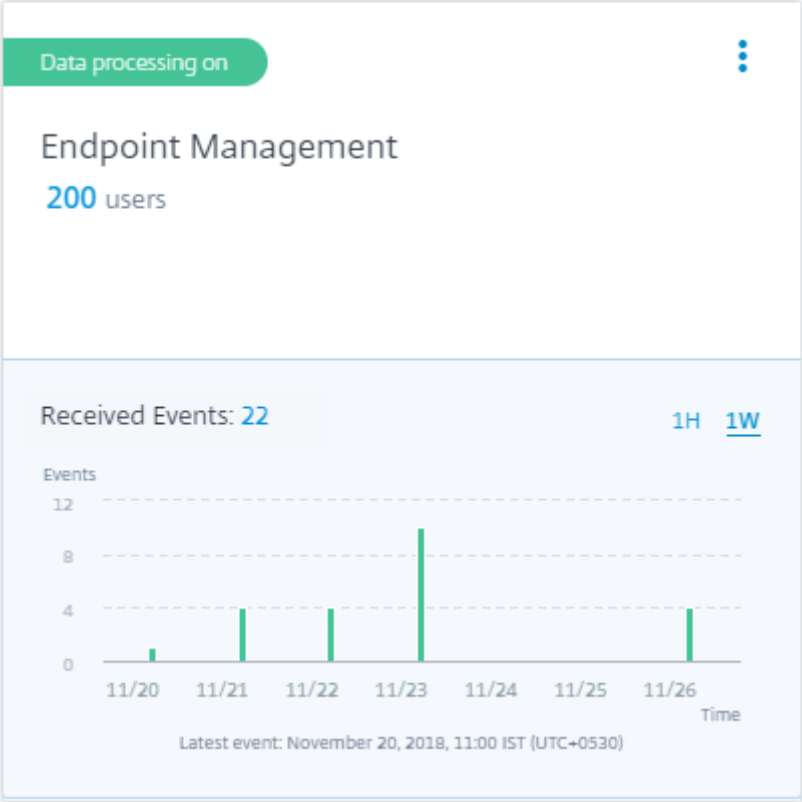



### Ver usuarios y eventos recibidos

La tarjeta del sitio muestra el número de usuarios, dispositivos y eventos recibidos de Endpoint Management durante la última hora, que es la selección de tiempo predeterminada. También puede seleccionar 1 semana (**1W**) y ver los datos.

Haga clic en el número de usuarios para ver los detalles del usuario en la página **Usuarios**.

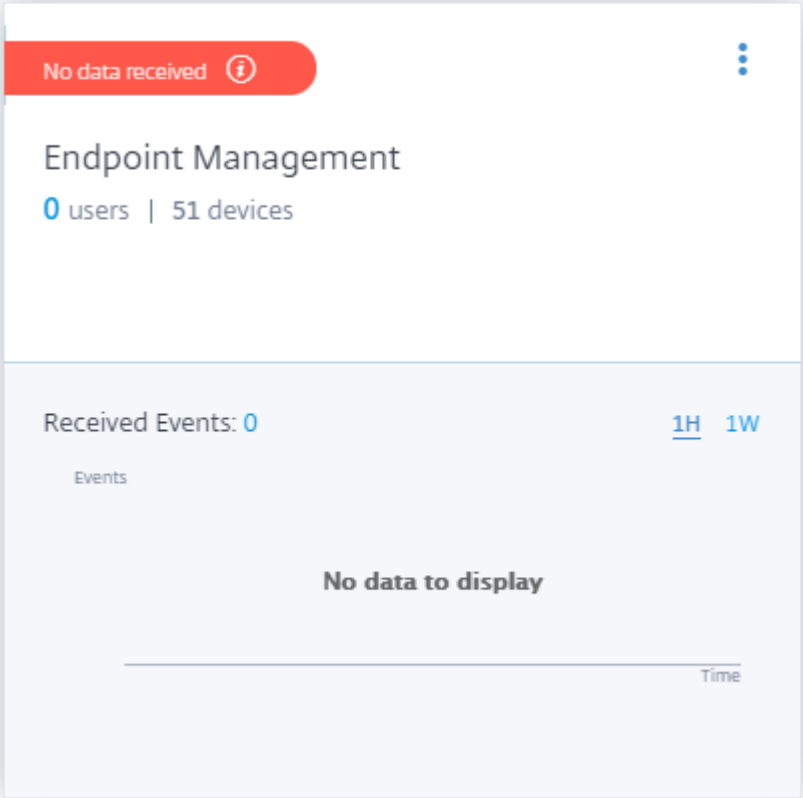
 




Una vez habilitado el procesamiento de datos, es posible que la tarjeta de sitio muestre el estado **No se han recibido datos**. Este estado aparece por dos motivos:

1. Si ha activado el procesamiento de datos por primera vez, los eventos tardan algún tiempo en llegar al centro de eventos de Citrix Analytics. Cuando Citrix Analytics recibe los eventos, el estado cambia a **Procesamiento de datos activado**. Si el estado no cambia después de un tiempo, actualice la página **Fuentes de datos**.
2. Analytics no ha recibido ningún evento de la fuente de datos en la última hora.

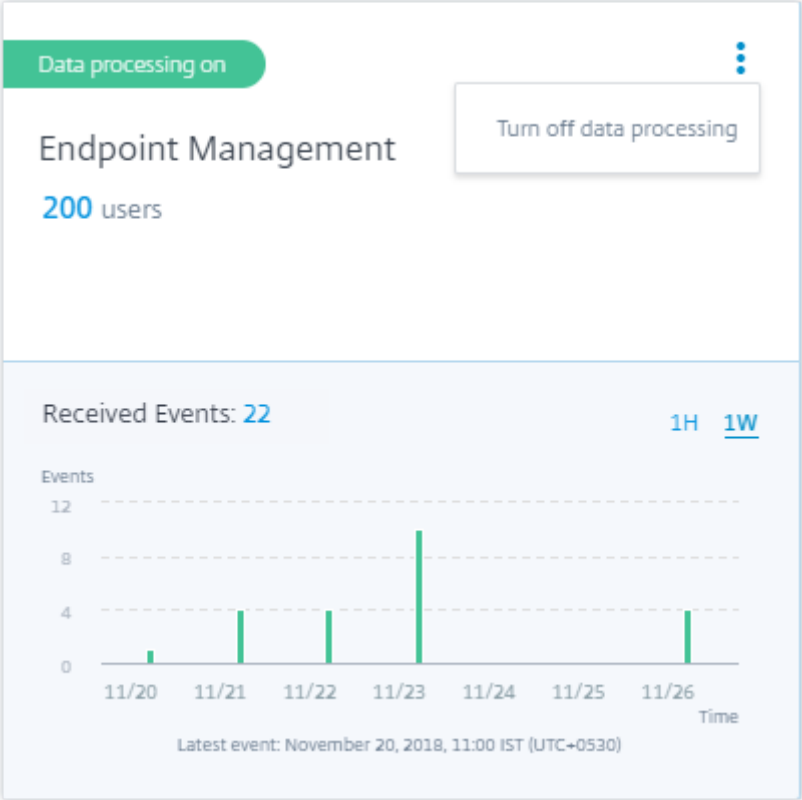
 




### Activar o desactivar el procesamiento de datos

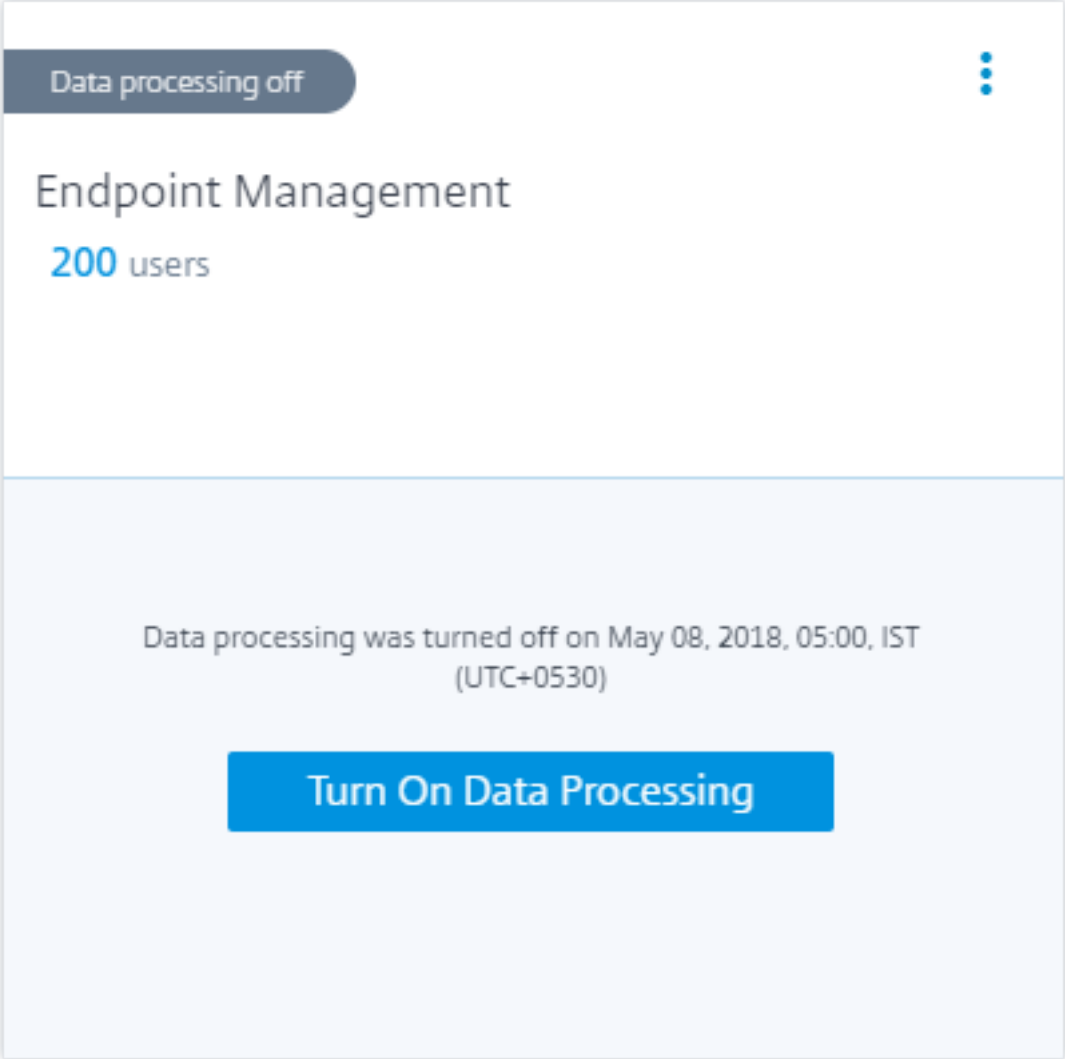
Para detener el procesamiento de datos, haga clic en los puntos suspensivos verticales () en la tarjeta del sitio y, a continuación, haga clic en **Desactivar el procesamiento de datos**. Citrix Analytics deja de procesar datos para este origen de datos.




Para volver a habilitar el procesamiento de datos, haga clic **en Activar procesamiento de datos**.




## Origen de datos de Citrix Gateway (local)

September 11, 2024

La fuente de datos de **Gateway** representa las instancias de Citrix Gateway locales en su entorno. Citrix Analytics detecta automáticamente los agentes de Citrix Application Delivery Management (ADM) y las instancias de Gateway agregadas al servicio Citrix ADM.

Cuando los usuarios acceden a cualquier servicio o aplicación a través de Gateway, Citrix Analytics recibe los eventos de acceso de los usuarios en tiempo real. Los eventos del usuario se procesan para detectar cualquier amenaza de seguridad.

Para obtener información sobre los requisitos previos y los pasos de incorporación, consulte el

artículo Fuente de datos de Citrix Gateway en la documentación de la plataforma Citrix Analytics.

## Origen de datos de Citrix Remote Browser Isolation

March 23, 2023

Citrix Remote Browser Isolation Service aísla la navegación web para proteger la red corporativa de los ataques basados en explorador web. Permite acceder de forma segura y consistente a las aplicaciones web alojadas en Internet en remoto, sin necesidad de configurar el dispositivo del usuario.

En Citrix Analytics for Security, puede ver los eventos de usuario de una sesión publicada de Remote Browser Isolation. Para obtener más información sobre los eventos de usuario, consulte Búsqueda de autoservicio para Remote Browser Isolation.

Para recibir los eventos de usuario de una sesión de Remote Browser Isolation publicada, habilite la directiva **Seguimiento de nombres de host** en Remote Browser Isolation. De forma predeterminada, la política está deshabilitada.

Al habilitar la directiva **Seguimiento de nombres de host**, Remote Browser Isolation puede enviar los nombres de host utilizados durante la sesión del usuario a Citrix Analytics for Security.
Para obtener más información, consulte Administrar sesiones de Remote Browser Isolation publicadas.

## Fuente de datos de Citrix Secure Private Access

April 12, 2024

El origen de datos **Secure Private Access** representa el servicio Citrix Secure Private Access que está asociado a su cuenta de Citrix Cloud. Cuando los usuarios utilizan este servicio, Citrix Analytics recibe los eventos de acceso de los usuarios (registros) en tiempo real. Los eventos del usuario se procesan para detectar cualquier amenaza de seguridad.

### Requisitos previos

- Suscríbase al servicio Citrix Secure Private Access que se ofrece en Citrix Cloud. Para saber cómo empezar, consulte Servicio de acceso privado seguro.
- Revise los requisitos del sistema y asegúrese de que su entorno cumpla con los requisitos.

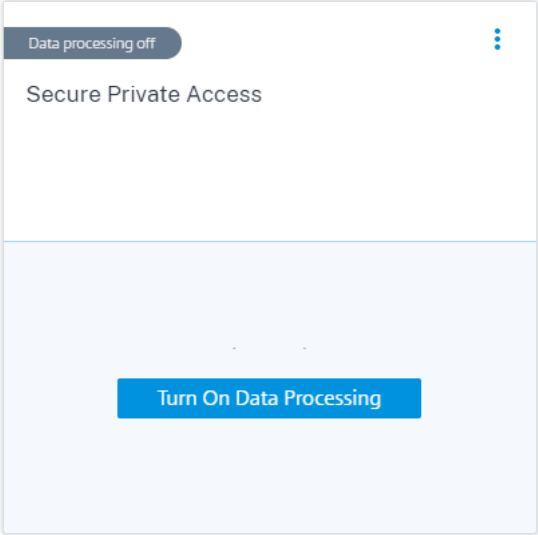
### Ver la fuente de datos y activar el procesamiento de datos

Citrix Analytics descubre automáticamente la fuente de datos de acceso privado seguro asociada a su cuenta de Citrix Cloud.

**Para ver la fuente de datos**:

En la barra superior, haga clic en **Configuración** > **Orígenes de datos** > **Seguridad**.

Aparece una tarjeta de sitio para la fuente de datos **Secure Private Access** en la página **Orígenes de datos** . Haga clic **en Activar procesamiento de datos** para permitir que Citrix Analytics comience a procesar los datos de esta fuente de datos.

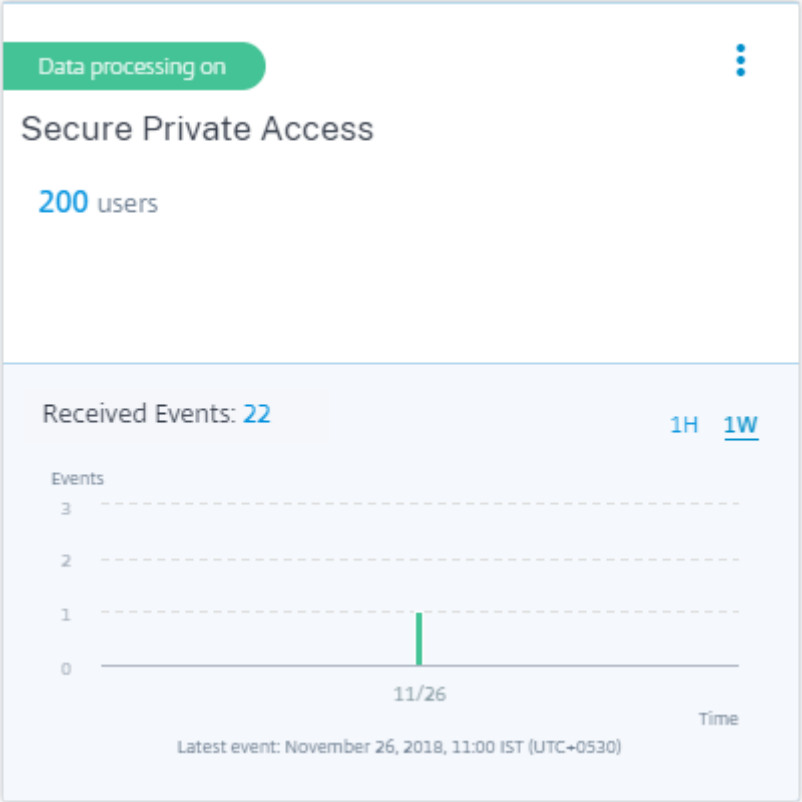



### Ver usuarios y eventos recibidos

La tarjeta del sitio muestra el número de usuarios activos y los eventos recibidos de la fuente de datos durante la última hora, que es la selección de tiempo predeterminada. También puede seleccionar 1 semana (1 W) y ver los datos.

Haga clic en el número de usuarios para ver los detalles del usuario en la página **Usuarios**. Haga clic en el número de eventos recibidos para ver los detalles del evento en la página de búsqueda de autoservicio.

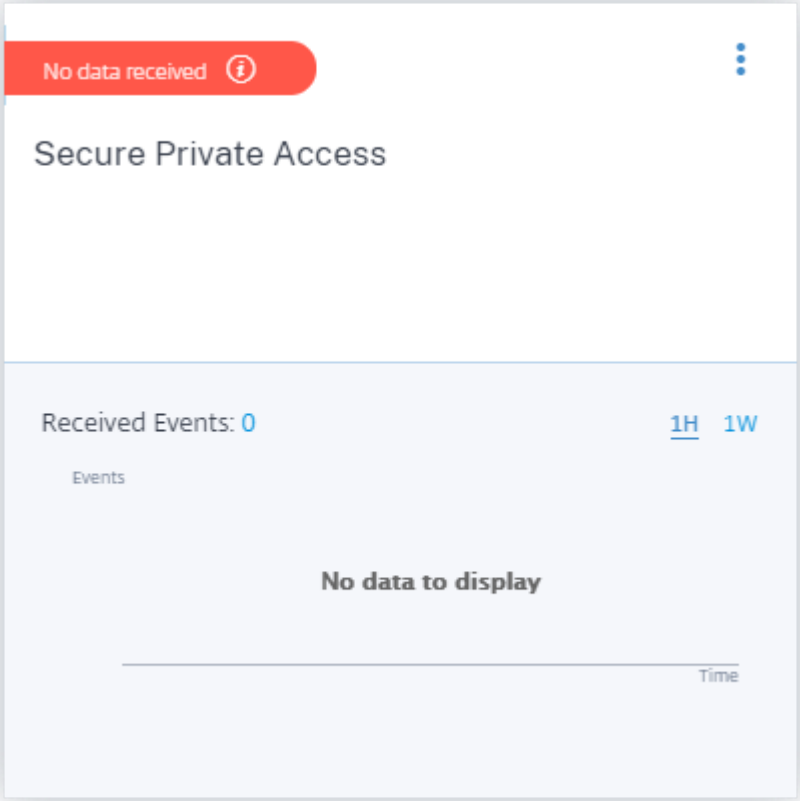
 




Una vez habilitado el procesamiento de datos, es posible que la tarjeta de sitio muestre el estado **No se han recibido datos**. Este estado aparece por dos motivos:

1. Si activó el procesamiento de datos por primera vez, los eventos tardan un tiempo en llegar al centro de eventos de Citrix Analytics. Cuando Citrix Analytics recibe los eventos, el estado cambia a **Data processing on**. Si el estado no cambia después de algún tiempo, actualice la página **Orígenes de datos** .
2. Analytics no ha recibido ningún evento de la fuente de datos en la última hora.

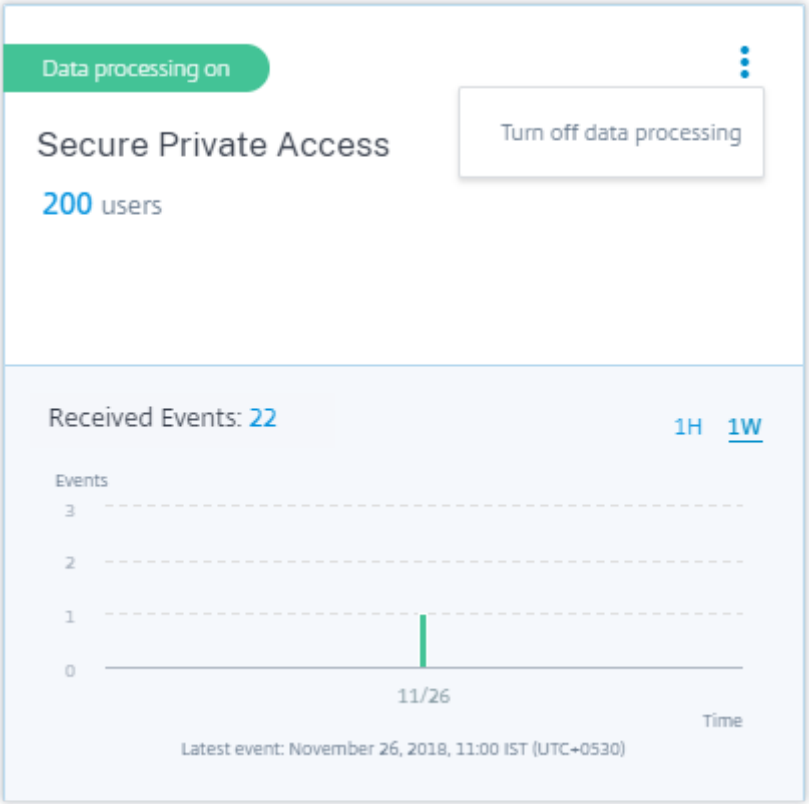
 



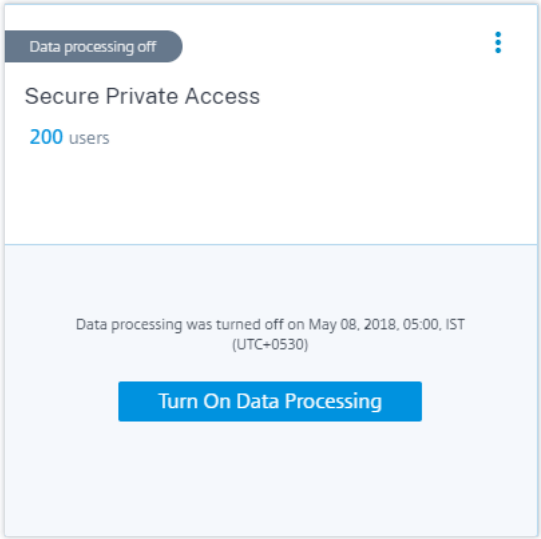

### Activar o desactivar el procesamiento de datos

Para detener el procesamiento de datos, haga clic en los puntos suspensivos verticales () en la tarjeta del sitio y, a continuación, haga clic en **Desactivar el procesamiento de datos**. Citrix Analytics deja de procesar datos para este origen de datos.




Para volver a habilitar el procesamiento de datos, haga clic **en Activar procesamiento de datos**.




## Origen de datos de Citrix Virtual Apps and Desktops y Citrix DaaS

April 12, 2024

El origen de datos de **Apps and Desktops** representa Citrix Virtual Apps and Desktops y Citrix DaaS (anteriormente el Citrix Virtual Apps and Desktops Service) locales de su organización.

Citrix Analytics for Security admite las ofertas y recibe eventos de usuario del origen de datos. En este artículo se explican los requisitos previos y los procedimientos para habilitar Analytics en ambas ofertas.

Citrix Analytics for Security recibe eventos de usuario de los siguientes componentes del origen de datos Citrix Virtual Apps and Desktops y Citrix DaaS:

- Aplicación Citrix Workspace instalada en los dispositivos de usuario
- Citrix Director para implementación local
- Servicio Citrix Monitor
- Servidores de grabación de sesiones

Los eventos de los usuarios se reciben en tiempo real en Citrix Analytics for Security cuando los usuarios usan aplicaciones virtuales o escritorios virtuales.

## Versiones de cliente compatibles

Citrix Analytics recibe eventos de usuario cuando se utiliza una versión de cliente compatible en los dispositivos de punto final de usuario. Si los usuarios utilizan versiones de cliente no compatibles, deben actualizar sus clientes a una de las siguientes versiones:

- Aplicación Citrix Workspace para Windows 1907 o posterior
- Aplicación Citrix Workspace para Mac 1910.2 o posterior
- Aplicación Citrix Workspace para HTML5 2007 o posterior
- Aplicación Citrix Workspace para Chrome-Última versión disponible en Chrome Web Store
- Aplicación Citrix Workspace para Android: última versión disponible en Google Play
- Aplicación Citrix Workspace para iOS: la última versión disponible en la App Store de Apple
- Aplicación Citrix Workspace para Linux 2006 o posterior

## Habilite el análisis en Citrix DaaS

### Requisitos previos

- Suscríbase a Citrix DaaS que se ofrece en Citrix Cloud. Para obtener información sobre cómo empezar a usar Citrix DaaS, consulte Instalación y configuración.
- Revise la sección **Requisitos del sistema** y asegúrese de que cumple los requisitos.

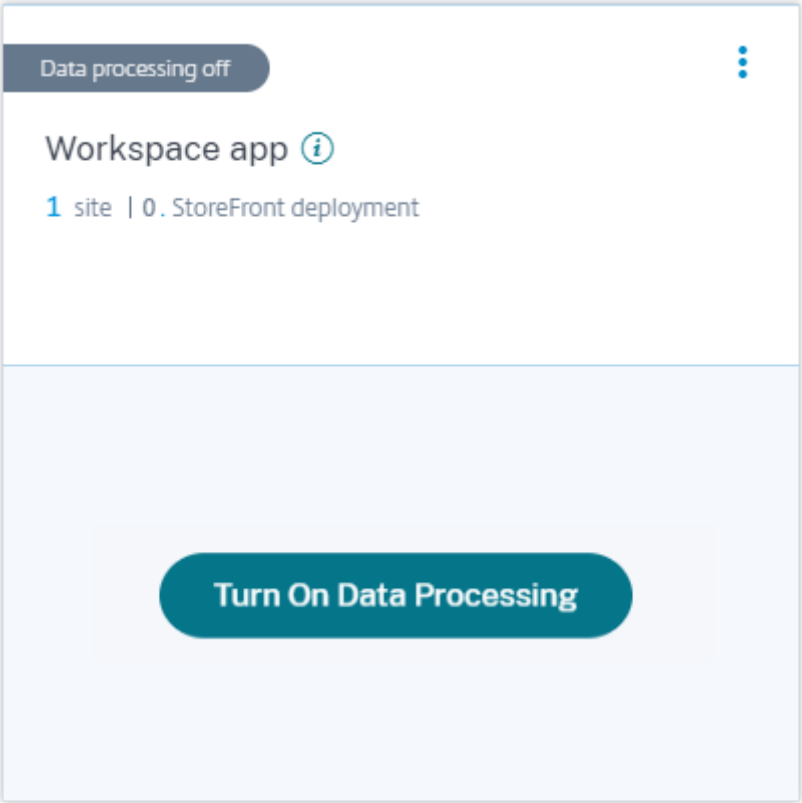
### Ver el origen de datos y activar el procesamiento de datos

Citrix Analytics descubre automáticamente los Citrix DaaS asociados a su cuenta de Citrix Cloud.

**Para ver la fuente de datos**:

En la barra superior, haga clic en **Configuración** > **Orígenes de datos** > **Seguridad**.

La tarjeta del sitio **Aplicaciones y escritorios: Aplicación Workspace** aparece en la página **Orígenes de datos**. Haga clic **en Activar procesamiento de datos** para permitir que Citrix Analytics comience a procesar los datos de esta fuente de datos.

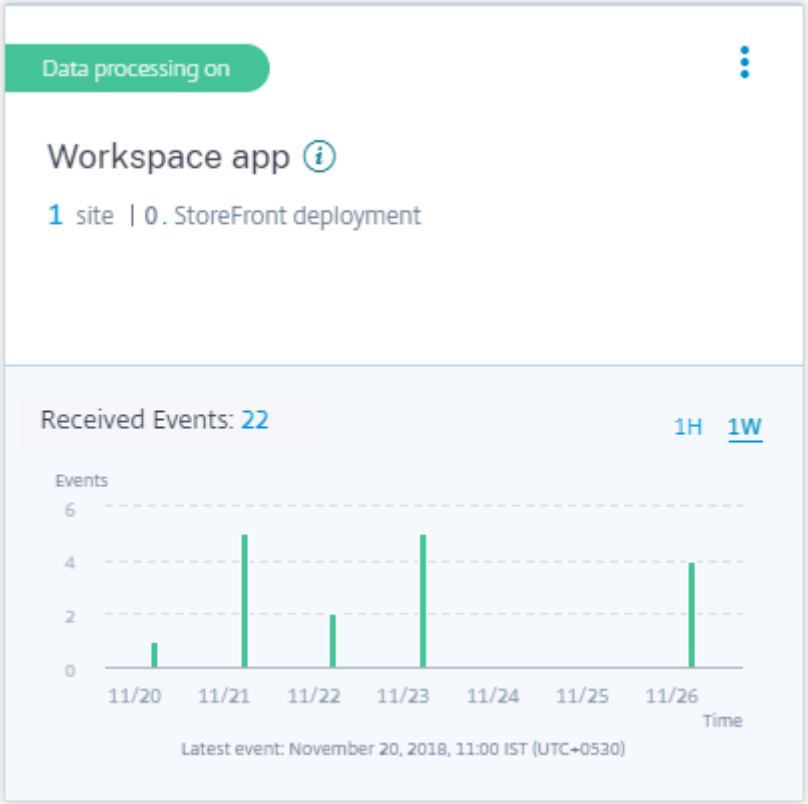



### Ver el sitio en la nube, los usuarios y los eventos recibidos

La tarjeta del sitio muestra la cantidad de usuarios de Apps y escritorios, el sitio en la nube descubierto y los eventos recibidos durante la última hora, que es la selección de hora predeterminada. También puede seleccionar 1 semana (1 W) y ver los datos.

Haga clic en el número de eventos recibidos para verlos en la página de búsqueda de autoservicio.

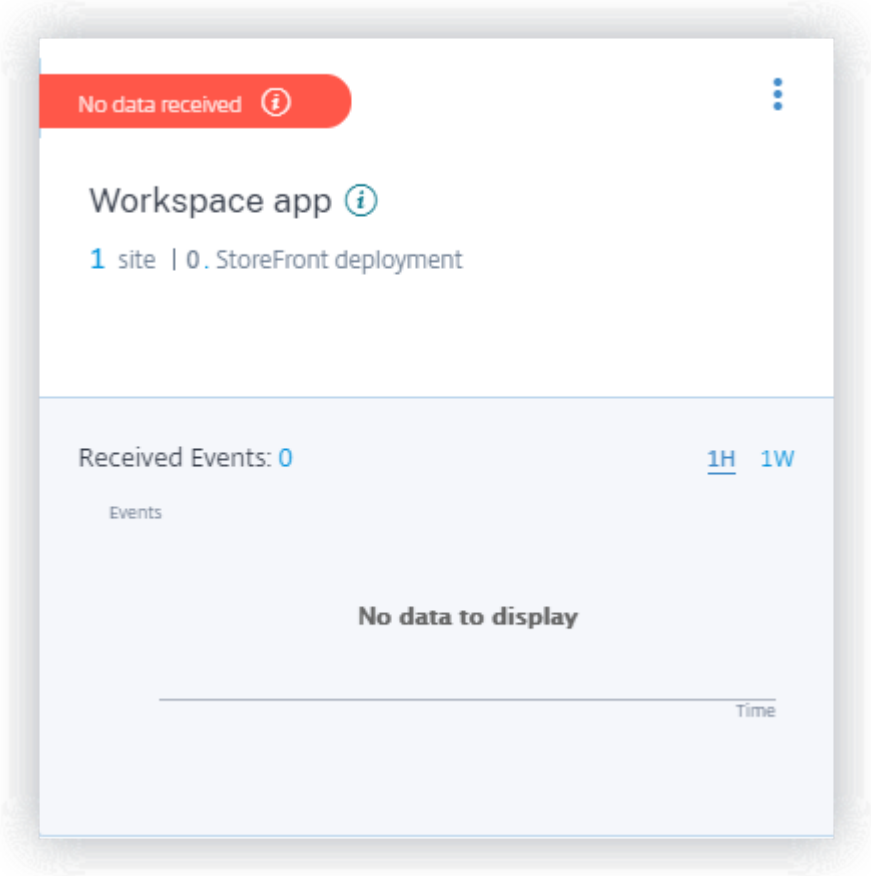
 




Después de habilitar el procesamiento de datos, es posible que la tarjeta del sitio muestre el estado **Sin datos recibidos**. Este estado aparece por dos motivos:

1. Si activó el procesamiento de datos por primera vez, los eventos tardan un tiempo en llegar al centro de eventos de Citrix Analytics. Cuando Citrix Analytics recibe los eventos, el estado cambia a **Data processing on**. Si el estado no cambia después de algún tiempo, actualice la página **Orígenes de datos**.
2. Analytics no ha recibido ningún evento del origen de datos en la última hora.




### Habilitar el análisis en Citrix Virtual Apps and Desktops locales

Citrix Analytics recibe eventos de usuario de sitios locales agregados a Workspace y de sitios a los que se accede a través de implementaciones de StoreFront.

Si su organización utiliza sitios locales, debe utilizar uno de los siguientes métodos para incorporar sus sitios, de modo que Analytics descubra los sitios:

- Incorpore sus sitios locales mediante StoreFront
- Incorporar sus sitios locales mediante Workspace

#### Requisitos previos

- Debe tener una licencia para usar la solución local de Citrix Virtual Apps and Desktops. Para obtener información sobre cómo empezar a utilizar Citrix Virtual Apps and Desktops en las instalaciones, consulte Instalación y configuración.
- Revise la sección **Requisitos del sistema** y asegúrese de que cumple los requisitos.

- Su Director tiene la versión 1912 CU2 o posterior. Para obtener más información, consulte la tabla de compatibilidad de funciones.
- **Suscripción a Citrix Workspace**. Si quiere agregar sus sitios a Citrix Workspace, debe requerir una suscripción a Workspace.

  Para comprar una suscripción a Citrix Workspace, visite https://www.citrix.com/products/citrix-workspace/get-started.html y póngase en contacto con un experto de Citrix Workspace que le puede ayudar.
- **Sitios agregados al espacio de trabajo**. Citrix Analytics descubre automáticamente los sitios agregados a Citrix Workspace. Agregue sus sitios a Citrix Workspace antes de continuar con la incorporación en Citrix Analytics. Este proceso se conoce como **agregación de sitios**.

  La agregación de sitios requiere que instale Cloud Connector, configure los servidores STA de NetScaler Gateway para la conectividad interna y externa a los recursos de Workspace y, a continuación, agregue los sitios a Workspace. Para obtener instrucciones detalladas sobre la agregación de sitios, consulte Agregar aplicaciones y escritorios virtuales locales en espacios de trabajo.
- **Versión StoreFront**. Si utiliza una implementación de StoreFront para sus sitios, asegúrese de que la versión de StoreFront sea 1906 o posterior.

#### Incorporar sitios locales de Citrix Virtual Apps and Desktops mediante StoreFront

Para obtener información sobre los requisitos previos y los pasos de incorporación, consulte el artículo Fuente de datos de Citrix Virtual Apps and Desktops en la documentación de la plataforma Citrix Analytics.

#### Incorporar sitios locales de Citrix Virtual Apps and Desktops mediante Workspace

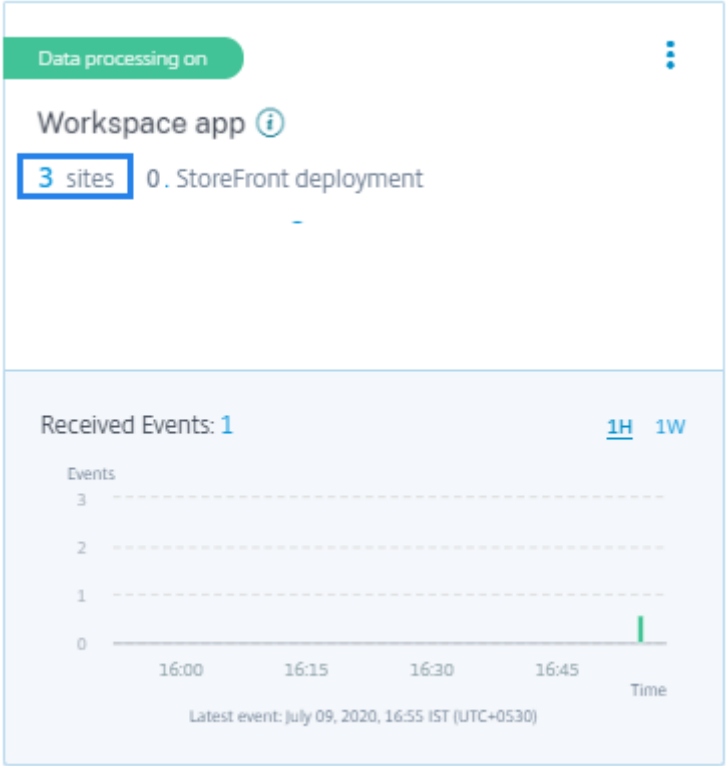
**Sitios ya agregados a Citrix Workspace** Citrix Analytics descubre automáticamente los sitios locales que ya se han agregado a Citrix Workspace y los muestra en la tarjeta del sitio de origen de datos.

**Para ver la fuente de datos:**

En la barra superior, haga clic en **Configuración** > **Orígenes de datos** > **Seguridad**.

La tarjeta del sitio **Aplicaciones y escritorios** muestra el número de sitios que se agregaron a Workspace y los usuarios conectados a estos sitios. Haga clic en el recuento de sitios para ver los sitios descubiertos. Haga clic en el recuento de usuarios para ver los usuarios detectados en la página **Usuarios**.

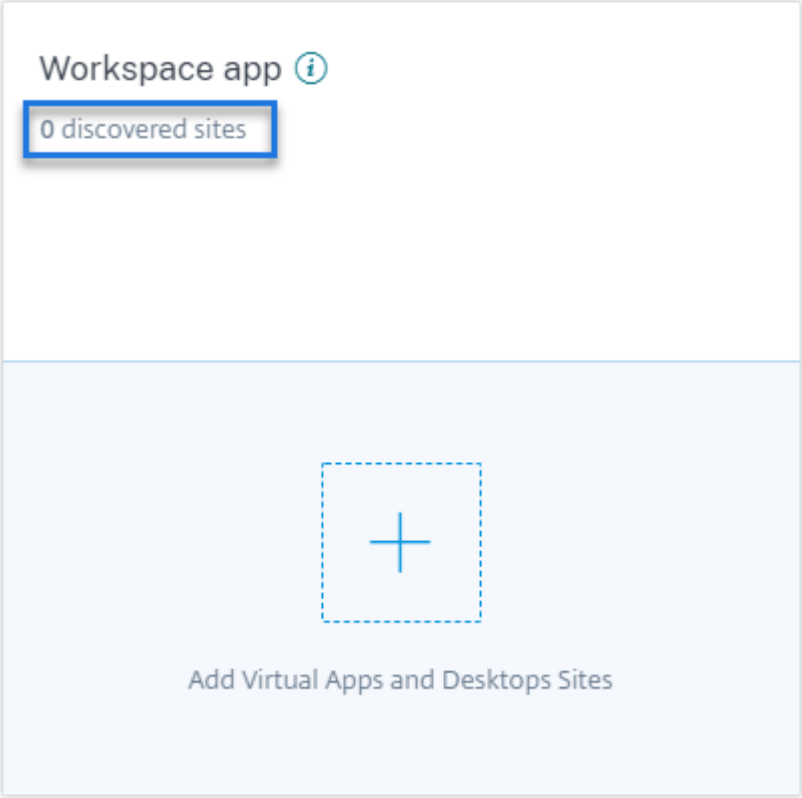



**Sitios no agregados a Citrix Workspace** Si aún no ha agregado sus sitios locales a Workspace, Analytics no podrá descubrir sus sitios. La tarjeta de sitio muestra **0 sitios descubiertos**.

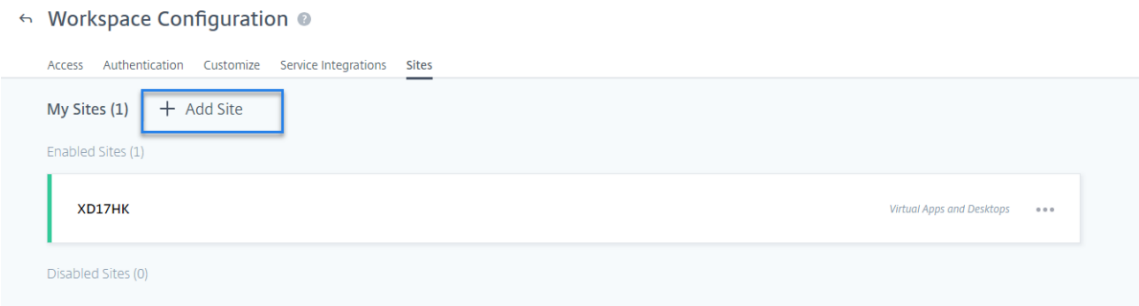
**Para agregar un sitio a Workspace:**

1. Haga clic en + en la tarjeta del sitio.




2. En la página **Configuración de Workspace**, haga clic en **+Agregar sitio**.



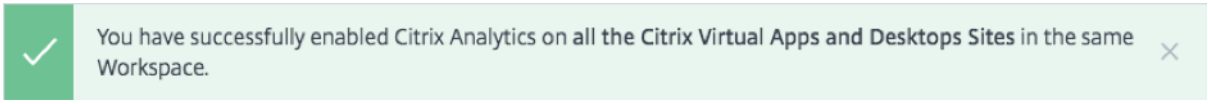

3. Siga las instrucciones que aparecen en pantalla para agregar un sitio. Para obtener más información, consulte Agregación de escritorios y aplicaciones virtuales locales en espacios de trabajo.
4. Después de agregar el sitio, vuelva a iniciar sesión en Citrix Analytics y actualice la página **Orígenes de datos** para ver el sitio agregado recientemente en la tarjeta del sitio.

**Activar el procesamiento de datos y ver los eventos recibidos** Para permitir que Analytics comience a procesar datos para los sitios descubiertos, haga clic **en Activar procesamiento de datos** en la tarjeta del sitio y siga las instrucciones en pantalla.

Si tiene varios sitios agregados al mismo espacio de trabajo, Analytics procesa y almacena los datos de todos los sitios del espacio de trabajo. Recibirá un mensaje de éxito cuando Analytics se haya

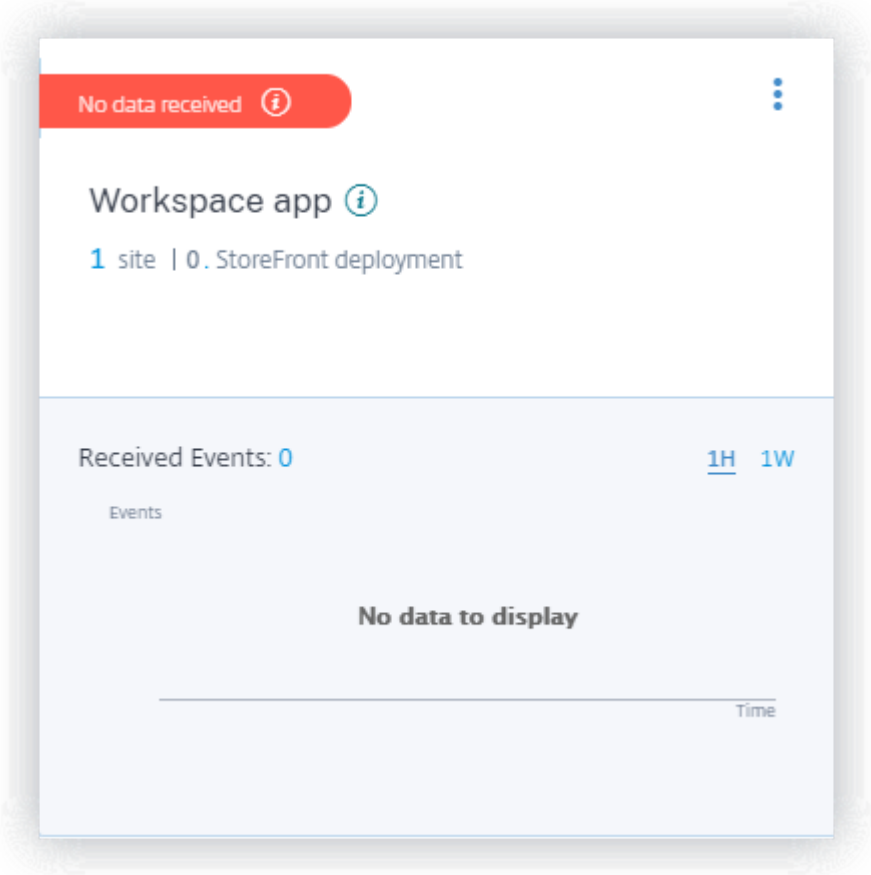
habilitado correctamente en todos sus sitios.




La tarjeta del sitio muestra los eventos recibidos durante la última hora, que es la selección de tiempo predeterminada. También puede seleccionar 1 semana (1 W) y ver los datos. Haga clic en el número de eventos recibidos para verlos en la página de búsqueda de autoservicio correspondiente.

Después de habilitar el procesamiento de datos, es posible que la tarjeta del sitio muestre el estado **Sin datos recibidos**. Este estado aparece por dos motivos:

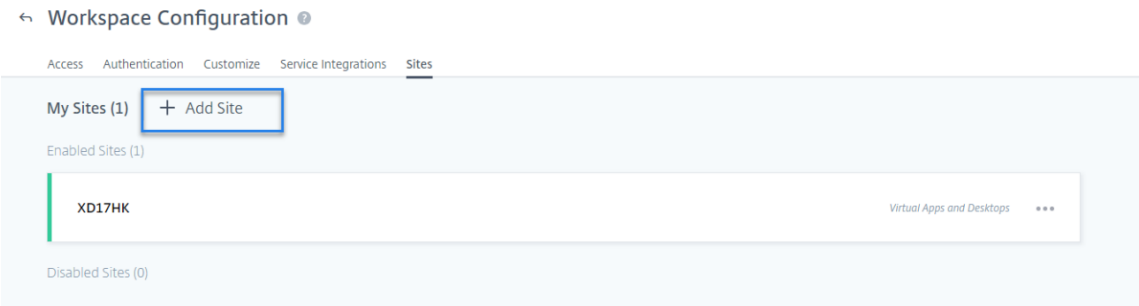
1. Si activó el procesamiento de datos por primera vez, los eventos tardan un tiempo en llegar al centro de eventos de Citrix Analytics. Cuando Citrix Analytics recibe los eventos, el estado cambia a **Data processing on**. Si el estado no cambia después de algún tiempo, actualice la página **Orígenes de datos**.
2. Analytics no ha recibido ningún evento del origen de datos en la última hora.




**Agregar un sitio** Si quiere agregar otro sitio local a Workspace, puede agregarlo desde Analytics:

1. En la página Configuración de Workspace, haga clic en **+Agregar sitio**.




2. Siga las instrucciones que aparecen en pantalla para agregar un sitio. Para obtener más información, consulte Agregación de escritorios y aplicaciones virtuales locales en espacios de trabajo.
3. Después de agregar el sitio, vaya a Citrix Analytics y actualice la página **Orígenes de datos** para ver el sitio agregado recientemente en la tarjeta del sitio.

## Conectarse a Citrix Director para sitios locales

Citrix Director es una consola de supervisión y solución de problemas para Citrix Virtual Apps and Desktops. Puede utilizar Director para configurar los sitios locales de Citrix Analytics for Security (Security Analytics). Una vez configurados los sitios, Director envía los eventos de supervisión a Security Analytics.

Si utiliza Citrix DaaS, el servicio Supervisar de Citrix envía eventos desde su sitio en la nube a Security Analytics.

En un entorno híbrido en el que tiene implementaciones tanto en la nube como en las instalaciones, Security Analytics recibe eventos del servicio Citrix Monitor y de los sitios incorporados en Citrix Director.

### Requisitos previos y pasos de configuración

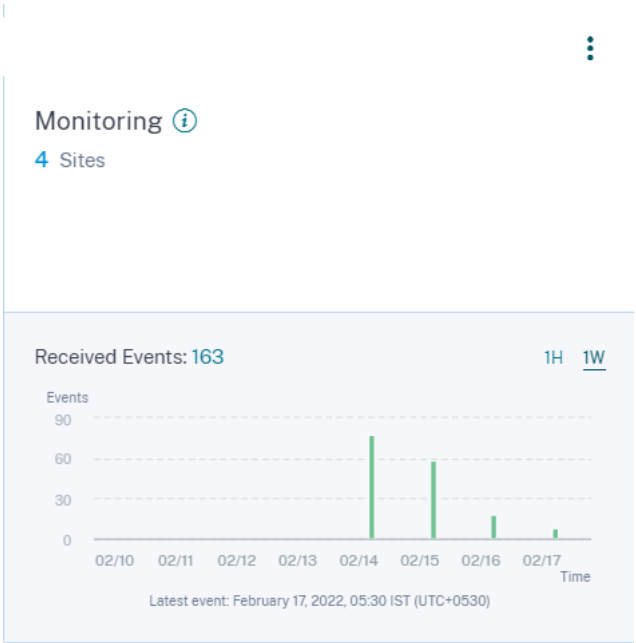
> **Notas**
>
> - Actualmente, la interfaz de usuario de Director muestra los pasos de configuración relacionados con Citrix Analytics para el rendimiento (Performance Analytics). Estos pasos de configuración también se aplican a Citrix Analytics for Security (Security Analytics). Si tiene un derecho activo de Citrix Cloud para Security Analytics, puede conectarse a Citrix Director siguiendo estos pasos.
> - Si su cuenta de Citrix Cloud tiene derechos activos tanto para Security Analytics como para Performance Analytics y ya ha configurado su sitio para Performance Analytics, no necesita volver a configurar Director para Security Analytics.

Para obtener información sobre los requisitos previos y los pasos de configuración, consulte la documentación de Citrix Analytics for Performance.

**Ver los sitios conectados y los eventos recibidos**

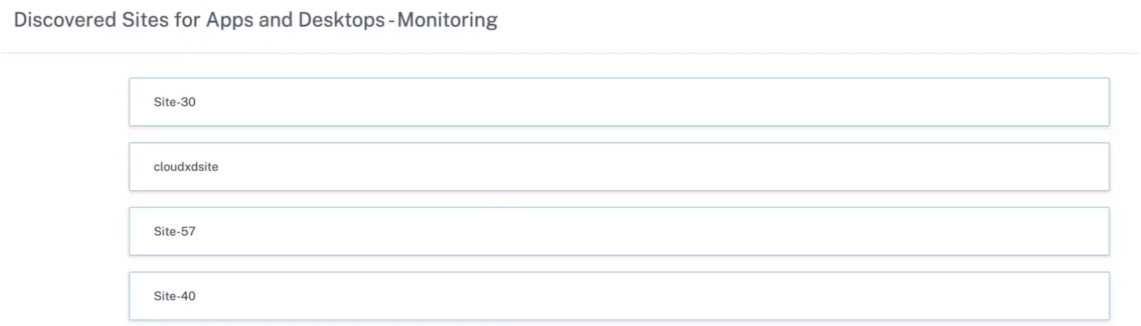
1. En Citrix Analytics, vaya a la página **Orígenes de datos**.
2. Haga clic en la ficha **Seguridad**.
3. En la tarjeta del sitio **Aplicaciones y escritorios: Supervisión**, puede ver sus sitios locales o el sitio en la nube (lo que corresponda). También puede ver los eventos recibidos de los sitios.




> **Notas**
>
> - La primera vez que configure un sitio local en Director, los eventos del sitio pueden tardar algún tiempo (aproximadamente una hora) en procesarse, lo que provoca un retraso en la visualización del sitio conectado en la tarjeta del sitio **Aplicaciones y escritorios: Supervisión**.
> - En la tarjeta del sitio de Monitoring, el procesamiento de datos para el servicio Monitor o el origen de datos de Director está habilitado de forma predeterminada. También puede desactivar el procesamiento de datos según sus requisitos. Sin embargo, se recomienda mantener el procesamiento de datos para obtener los máximos beneficios de Security Analytics.

4. Haga clic en el sitio para ver los detalles.




## Implementación de Conectarse a grabación de sesiones

Grabación de sesiones le permite grabar la actividad en pantalla de cualquier sesión de usuario en Citrix Virtual Apps and Desktops y Citrix DaaS. Puede configurar los servidores de grabación de sesiones para que envíen los eventos de usuario a Citrix Analytics for Security. Los eventos de los usuarios se procesan para proporcionar información útil sobre los comportamientos de riesgo de los usuarios.

### Requisitos previos

Antes de empezar, asegúrate de lo siguiente:

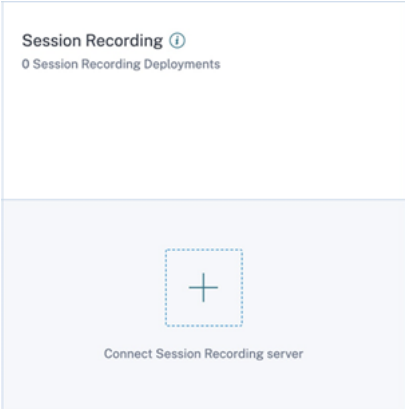
- El servidor de grabación de sesiones y el agente de VDA deben ser 2103 o posterior.
- El servidor de grabación de sesiones debe poder conectarse a las direcciones necesarias. Para obtener más información sobre las URL, consulte Requisitos de red.
- La implementación de Grabación de sesiones debe tener el puerto 443 abierto para las conexiones a Internet salientes. Todos los servidores proxy de la red deben permitir esta comunicación con Citrix Analytics para seguridad.
- Si utiliza Citrix Virtual Apps and Desktops 7 1912 LTSR, la versión de Grabación de sesiones admitida es 2103 o una posterior.

> **Nota**
>
> Asegúrese de comprobar los requisitos de conectividad adicionales al utilizar el servicio de **Grabación de sesiones**.

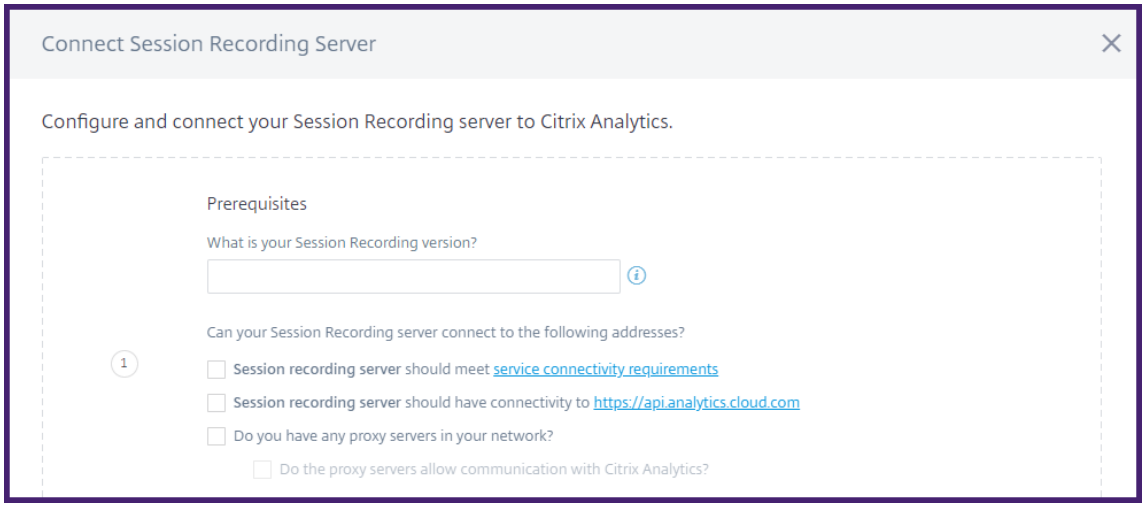
### Configure su servidor de grabación de sesiones

1. En la tarjeta del sitio **Aplicaciones y escritorios: Grabación de sesiones**, haga clic en **Conectar el servidor de grabación de sesiones**.




2. En la página **Connect Session Recording Server**, revise la lista de verificación y seleccione todos los requisitos obligatorios. Si no selecciona un requisito obligatorio, la opción Download File está inhabilitada.




3. Si tiene servidores proxy en su red, introduzca la dirección proxy en el archivo *SsRecStorageManager.exe.config* en el servidor de Grabación de sesiones.

   El archivo de configuración se encuentra en `<Session Recording Server installation path>\bin\SsRecStorageManager.exe.config`

   Por ejemplo: `C:\Program Files\Citrix\SessionRecording\Server\Bin\SsRecStorageManager.exe.config`


4. Haga clic en **Descargar archivo** para descargar el archivo *SessionRecordingConfigurationFile.json*.

> **Nota**
>
> El archivo contiene información confidencial. Guarde el archivo en un lugar seguro y protegido.

5. Copie el archivo en el servidor de Grabación de sesiones que quiere conectar a Citrix Analytics para seguridad.
6. Si tiene varios Servidores de grabación de sesiones en su implementación, debe copiar el archivo en cada servidor que quiera conectar y seguir los pasos para configurar cada servidor.
7. En el servidor de Grabación de sesiones, ejecute este comando para importar los parámetros:

```
<Session Recording Server installation path>\bin\SsRecUtils.exe -
    Import_SRCasConfigurations <configuration file path>
```

   Por ejemplo:

   `C:\Program Files\Citrix\SessionRecording\Server\bin\ SsRecUtils.exe -Import_SRCasConfigurations C:\Users\administrator \Downloads \SessionRecordingConfigurationFile.json`

8. Reinicie estos servicios:
   - Servicio Citrix Session Recording Analytics
   - Administrador de almacenamiento de grabación de sesiones de Citrix
9. Una vez que la configuración se haya realizado correctamente, vaya a Citrix Analytics para seguridad para ver el servidor de Grabación de sesiones conectado. Haga clic **en Activar procesamiento de datos** para permitir que Citrix Analytics for Security procese los datos.

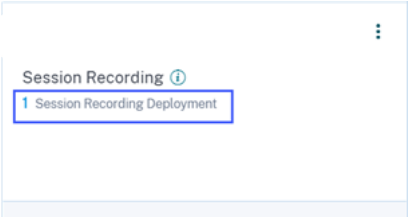
 

> **Nota**
>
> Si utiliza el servidor de grabación de sesiones de la versión 2103 o 2104, primero debe iniciar una sesión de Apps and Desktops para ver el servidor de grabación de sesiones conectado en Citrix Analytics for Security. De lo contrario, el servidor de Grabación de sesiones conectado no se muestra. Este requisito no se aplica a la versión 2106 del servidor de Grabación de sesiones ni a posteriores.

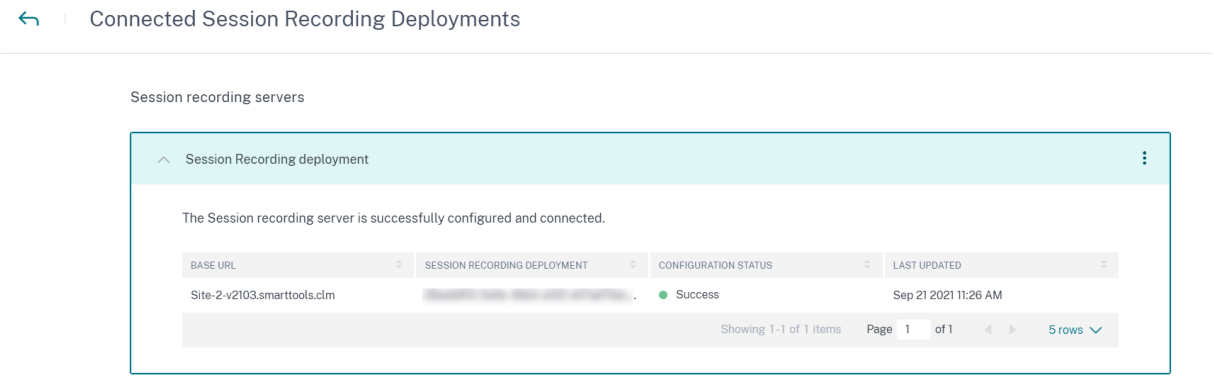
### Ver las implementaciones conectadas

Las implementaciones de servidores aparecen en la tarjeta del sitio Session Recording solo si la configuración se realiza correctamente. La tarjeta del sitio muestra el número de servidores configurados que han establecido conexiones con Citrix Analytics for Security.

Si no vaya los servidores de grabación de sesiones incluso después de que la configuración se haya realizado correctamente, consulte el artículo Solución deproblemas.




En la tarjeta del sitio, haga clic en el número de implementaciones para ver los grupos de servidores conectados con Citrix Analytics for Security. Por ejemplo, haga clic en **1 Session Recording Deployment** para ver el servidor o los grupos de servidores conectados. Cada servidor de Grabación de sesiones está representado por una URL base y un ServerGroupID.




### Ver eventos recibidos

La tarjeta del sitio muestra las implementaciones de Grabación de sesiones conectadas y los eventos recibidos de estas implementaciones durante la última hora, que es la selección de tiempo prede-

terminada. También puede seleccionar 1 semana (1 W) y ver los datos. Haga clic en la cantidad de eventos recibidos para verlos en la página de búsqueda de autoservicio.

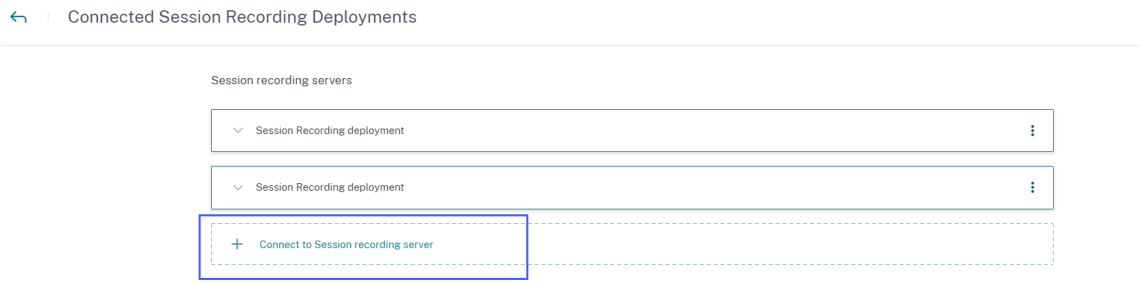
Después de habilitar el procesamiento de datos, es posible que la tarjeta del sitio muestre el estado **No data received**. Este estado aparece por dos motivos:

1. Si activó el procesamiento de datos por primera vez, los eventos tardan un tiempo en llegar al centro de eventos de Citrix Analytics. Cuando Citrix Analytics recibe los eventos, el estado cambia a **Data processing on**. Si el estado no cambia después de algún tiempo, actualice la página Data Sources.
2. Citrix Analytics no recibió ningún evento del origen de datos en la última hora.

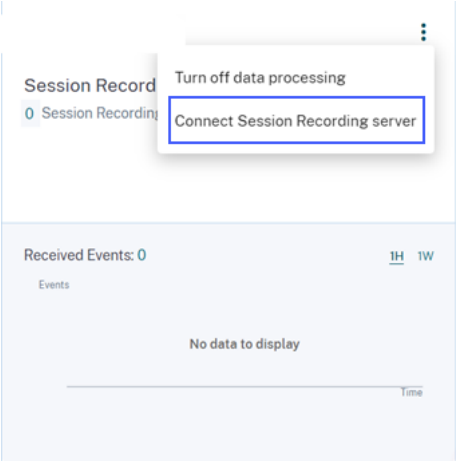
### Agregar Servidores de grabación de sesiones

Para agregar un servidor de Grabación de sesiones, siga uno de estos procedimientos:

- En la página **Connected Session Recording Deployments**, haga clic en **Connect to Session Recording server**.




- En la tarjeta del sitio **Aplicaciones y escritorios: Grabación de sesiones**, haga clic en los puntos suspensivos verticales (⋮) y, a continuación, seleccione **Conectar servidor de grabación de sesiones**.



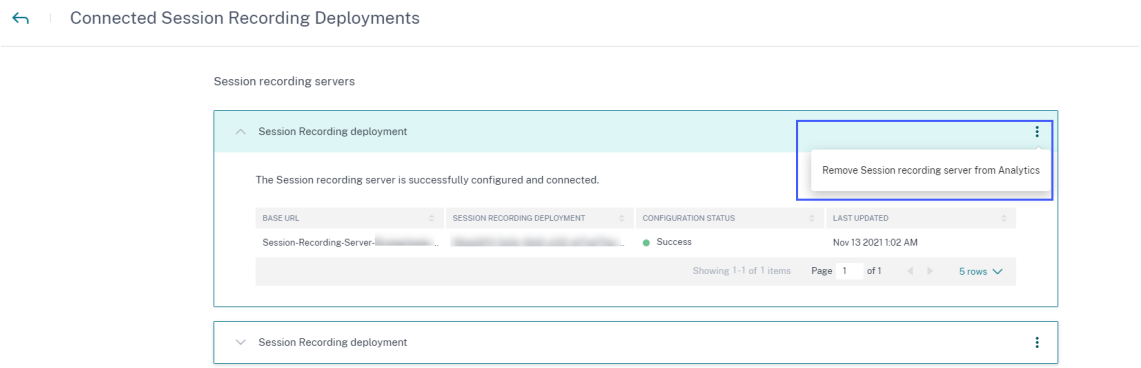

 

Siga los pasos para descargar el archivo de configuración y configurar un servidor de Grabación de sesiones.

### Quitar Servidores de grabación de sesiones

Para quitar un servidor de Grabación de sesiones:

1. En Citrix Analytics para seguridad, vaya a la página **Connected Session Recording Deployments** y seleccione la implementación del servidor que quiere quitar.
2. Haga clic en los puntos suspensivos verticales (⋮) y seleccione **Remove Session Recording server from Analytics**.




3. En el servidor de Grabación de sesiones que quitó de Citrix Analytics, ejecute este comando:

```
<Session Recording Server installation path>\bin\SsRecUtils.exe -
    Remove_SRCasConfigurations
```

Por ejemplo:

```
C:\Program Files\Citrix\SessionRecording\Server\bin\ SsRecUtils.
exe -Remove_SRCasConfigurations
```

### Habilitar la telemetría de impresión para Citrix DaaS

Cuando los usuarios realizan trabajos de impresión en Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service), puede ver los registros relacionados con estos trabajos de impresión en Citrix Analytics for Security. Estos registros de impresión proporcionan información vital sobre las actividades de impresión, como los nombres de las impresoras, los nombres de los archivos de impresión y el total de copias impresas.

> **Nota**
>
> Esta función solo es compatible con Citrix DaaS.

En Citrix Analytics for Security, en la página **Buscar**, puede seleccionar el origen de datos **Aplicaciones y escritorios** para ver los registros de impresión. Como administrador de seguridad, puede usar estos registros para analizar e investigar los riesgos de sus usuarios.

De forma predeterminada, la función de telemetría de impresión, que es la recopilación y transmisión de estos registros de impresión, está inhabilitada en los Virtual Delivery Agents (VDA).

Para habilitar la telemetría de impresión y la transmisión de registros de impresión a Citrix Analytics for Security, debe crear claves de registro y configurar el VDA.

> **Importante**
>
> Esta configuración solo se aplica a los VDA de Windows.

### Requisitos previos

- La versión de su VDA debe ser la misma que la versión básica de Citrix Virtual Apps and Desktops 7 2203 LTSR o una versión posterior. Para obtener más información, consulte Componentes básicos de Citrix Virtual Apps and Desktops 7 2203.
- Debe tener permisos de acceso total para realizar las actualizaciones de la clave de registro.

### Habilitar la telemetría de impresión en máquinas con administración de energía

Las máquinas con administración de energía incluyen máquinas virtuales o PC blade con los siguientes escenarios:

- Imagen maestra existente
- Nueva imagen maestra

### Habilitar la telemetría de impresión para una imagen maestra existente en la que la versión del VDA sea inferior a la de Citrix Virtual Apps and Desktops 7 2203 LTSR

1. Inicie sesión en la máquina VDA maestra y cree una instantánea del estado actual.
2. Para habilitar los registros del servicio de impresión, agregue las siguientes claves de registro:
   - Microsoft-Windows-PrintService/Operational
   - ShowJobTitleInEventLogs

   Para obtener más información sobre las claves de registro, consulte Crear claves de registro.
3. Actualice el VDA a una versión básica para Citrix Virtual Apps and Desktops 7 2203 LTSR o posterior. Para obtener más información, consulte Componentes básicos de Citrix Virtual Apps and Desktops 7 2203.

4. Apague la máquina y tome una instantánea del estado más reciente.
5. Inicie sesión en Citrix Cloud. Seleccione el catálogo de máquinas, haga clic en **Actualizar máquinas**y siga las instrucciones que aparecen en pantalla. Para obtener más información, consulte Crear catálogos de máquinas.
6. Espere 24 horas. La configuración se envía automáticamente en 24 horas. Si la configuración ya se ha completado, no necesita esperar.
7. Inicie una sesión de escritorio con la aplicación Citrix Workspace. Todos los eventos de impresión activados mediante la impresora del cliente están visibles en la página de **búsqueda** de Citrix Analytics for Security.

**Habilitar la telemetría de impresión para una imagen maestra existente en la que la versión del VDA sea la misma que la de Citrix Virtual Apps and Desktops 7 2203 LTSR o posterior** **Opción 1**: agregue las claves de registro de impresión en el VDA maestro y actualice los escritorios virtuales.

1. Inicie sesión en la máquina VDA maestra y cree una instantánea del estado actual.
2. Para habilitar los registros del servicio de impresión, agregue las siguientes claves de registro:
   - Microsoft-Windows-PrintService/Operational
   - ShowJobTitleInEventLogs

   Para obtener más información sobre las claves de registro, consulte Crear claves de registro.
3. Apague la máquina VDA y tome una instantánea del estado más reciente.
4. Inicie sesión en Citrix Cloud, seleccione el catálogo de máquinas, haga clic en **Actualizar máquinas** y siga las instrucciones que aparecen en pantalla.
5. Inicie una sesión de escritorio con la aplicación Citrix Workspace. Todos los eventos de impresión activados mediante la impresora del cliente están visibles en la página de **búsqueda** de Citrix Analytics for Security.

**Opción 2**: mover el escritorio virtual a la unidad organizativa (OU) y crear claves de registro mediante GPO

> **Nota**
>
> El método de la opción 2 solo funciona para máquinas estáticas. Para máquinas aleatorias, debe seguir el método de la opción 1 (como se mencionó anteriormente).

1. Inicie sesión en la máquina controladora de dominio.
2. Para habilitar los registros del servicio de impresión, agregue las siguientes claves de registro:
   - Microsoft-Windows-PrintService/Operational

- ShowJobTitleInEventLogs

Para obtener más información sobre las claves de registro, consulte Crear claves de registro.

> **Nota**
>
> En cualquier controlador de dominio, la creación de las claves de registro es una tarea que se realiza una sola vez.

1. Reinicie la máquina VDA desde Citrix Cloud.
2. Inicie una sesión de escritorio con la aplicación Citrix Workspace. Todos los eventos de impresión activados mediante la impresora del cliente están visibles en la página de **búsqueda** de Citrix Analytics for Security.

### Habilitar la telemetría de impresión en una nueva imagen maestra

1. Cree una máquina virtual (VM) mediante la herramienta de administración del hipervisor. Esta máquina virtual se trata como un VDA principal.
2. Asegúrese de que el VDA maestro esté agregado al dominio requerido.
3. Inicie sesión en el VDA maestro y habilite los registros del servicio de impresión agregando las siguientes claves de registro:

   - Microsoft-Windows-PrintService/Operational
   - ShowJobTitleInEventLogs

   Para obtener más información, consulte Crear claves de registro.
4. Instale la versión de VDA para Citrix Virtual Apps and Desktops 7 2203 LTSR o posterior. Al instalar el VDA, seleccione la opción **Imagen maestra**. Para obtener más información, consulte Componentes básicos de Citrix Virtual Apps and Desktops 7 2203.
5. Asegúrese de que la conexión de alojamiento esté agregada a Citrix Cloud. Para obtener más información, consulte Crear catálogos de máquinas.
6. Cree un catálogo de máquinas con la imagen maestra. Para obtener más información, consulte Crear catálogos de máquinas.
7. Cree un grupo de entrega y agregue el catálogo de máquinas. Para obtener más información, consulte Crear grupos de entrega.
8. Espere 24 horas. El motor de directivas de grupo envía automáticamente la configuración en un plazo de 24 horas.
9. Inicie una sesión de escritorio con la aplicación Citrix Workspace. Todos los eventos de impresión activados mediante la impresora del cliente están visibles en la página de **búsqueda** de Citrix Analytics for Security.

### Habilitar la telemetría de impresión en máquinas que no tienen administración de energía

Las máquinas sin administración de energía incluyen los equipos físicos con los siguientes escenarios:

- VDA físico existente
- Nuevo VDA físico

#### Habilitar la telemetría de impresión para un VDA físico existente en el que la versión del VDA sea inferior a la de Citrix Virtual Apps and Desktops 7 2203 LTSR

1. Para habilitar los registros del servicio de impresión, agregue las siguientes claves de registro:

   - Microsoft-Windows-PrintService/Operational
   - ShowJobTitleInEventLogs

   Para obtener más información, consulte Crear claves de registro.

2. Actualice el VDA a una versión básica para Citrix Virtual Apps and Desktops 7 2203 LTSR o posterior. Para obtener más información, consulte Componentes básicos de Citrix Virtual Apps and Desktops 7 2203.

3. Espere 24 horas. La configuración se envía automáticamente en 24 horas. Si la configuración ya está completa, no necesita esperar.

4. Inicie una sesión de escritorio con la aplicación Citrix Workspace. Todos los eventos de impresión activados mediante la impresora del cliente están visibles en la página de **búsqueda** de Citrix Analytics for Security.

#### Habilitar la telemetría de impresión para un nuevo VDA físico

1. Cree una máquina virtual física y cambie el dominio por el nombre de dominio requerido.

2. Inicie sesión en la máquina virtual y habilite los registros del servicio de impresión agregando las siguientes claves de registro:

   - Microsoft-Windows-PrintService/Operational
   - ShowJobTitleInEventLogs

   Para obtener más información, consulte Crear claves de registro.

3. Instale la versión de VDA para Citrix Virtual Apps and Desktops 7 2203 LTSR o posterior. Al instalar el VDA, seleccione la opción Acceso con Remote PC.

4. Cree un catálogo de máquinas. Para obtener más información, consulte Crear catálogos de máquinas.

> **Nota**
>
> La administración de máquinas debe seleccionarse como **Máquinas que no están administradas por energía (por ejemplo, máquinas físicas)**.

5. Cree un grupo de entrega y agregue el catálogo de máquinas. Para obtener más información, consulte Crear grupos de entrega.
6. Espere 24 horas. El motor de directivas de grupo envía automáticamente la configuración en un plazo de 24 horas.
7. Inicie una sesión de escritorio con la aplicación Citrix Workspace. Todos los eventos de impresión activados mediante la impresora del cliente están visibles en la página de **búsqueda** de Citrix Analytics for Security.

### Crear claves de registro

En el VDA, realice una de las siguientes opciones:

- Cree las claves de registro manualmente. Utilice este método para los VDA maestros y para tener una cantidad menor de VDA físicos en la implementación.
- Cree claves de registro mediante un objeto de directiva de grupo (GPO). Use este método cuando la implementación tenga un número mayor de máquinas VDA físicas y deba habilitar la telemetría de impresión en todas ellas.

### Detalles de claves del Registro

| SL | Nombre de clave del Registro | Propósito de la clave | Detalles del Registro |
|---|---|---|---|
| 1 | Microsoft-Windows-PrintService/Operational | Habilita los registros del servicio de impresión en el visor de eventos. | **Ruta del Registro**: HKLM:\SYSTEM\CurrentControlSet\ |

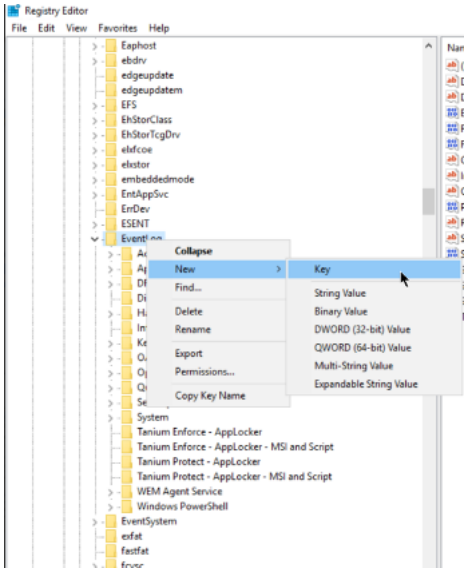
 

| SL | Nombre de clave del Registro | Propósito de la clave | Detalles del Registro |
|---|---|---|---|
| 2 | ShowJobTitleInEventLogs | Controla si el nombre del trabajo de impresión se incluye en los registros de eventos de impresión; de lo contrario, considera el nombre genérico del trabajo "Imprimir documento" . | **Subárbol del Registro**: HKEY_LOCAL_MACHINE<br>**Ruta del Registro**: Software\Policies\Microsoft\Windows NT\Printers<br>**Nombre del valor**: ShowJobTitleInEventLogs<br>**Tipo de valor**: REG_DWORD<br>**Valor**: 1 |

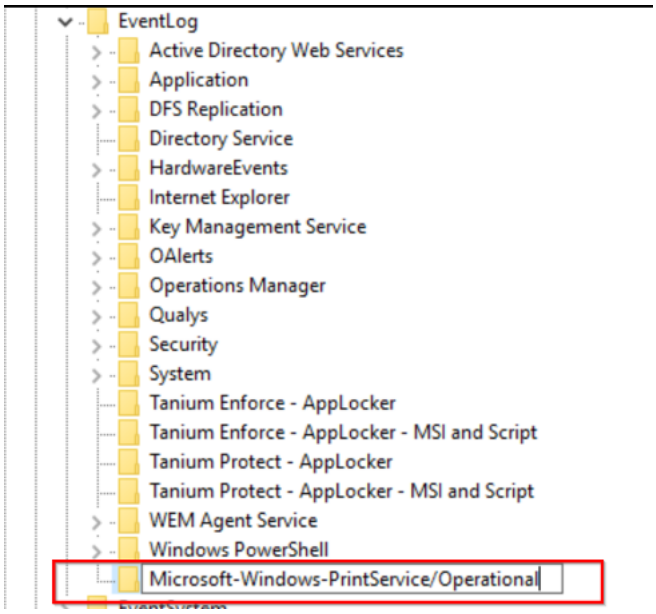
**Crear claves de registro manualmente en una máquina VDA** Utilice este método para crear la clave de registro en la imagen maestra del VDA. Agregar claves a la imagen maestra ayuda a mantener las claves persistentes para todos los tipos de VDA que se crean con la imagen maestra.

1. Inicie sesión en la máquina maestra del VDA.
2. Abra Ejecutar y escriba Regedit para abrir el registro de Windows.
3. Vaya a la ubicación HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog
4. Haga clic con el botón secundario en **EventLog** y seleccione **Nuevo > Clave**.



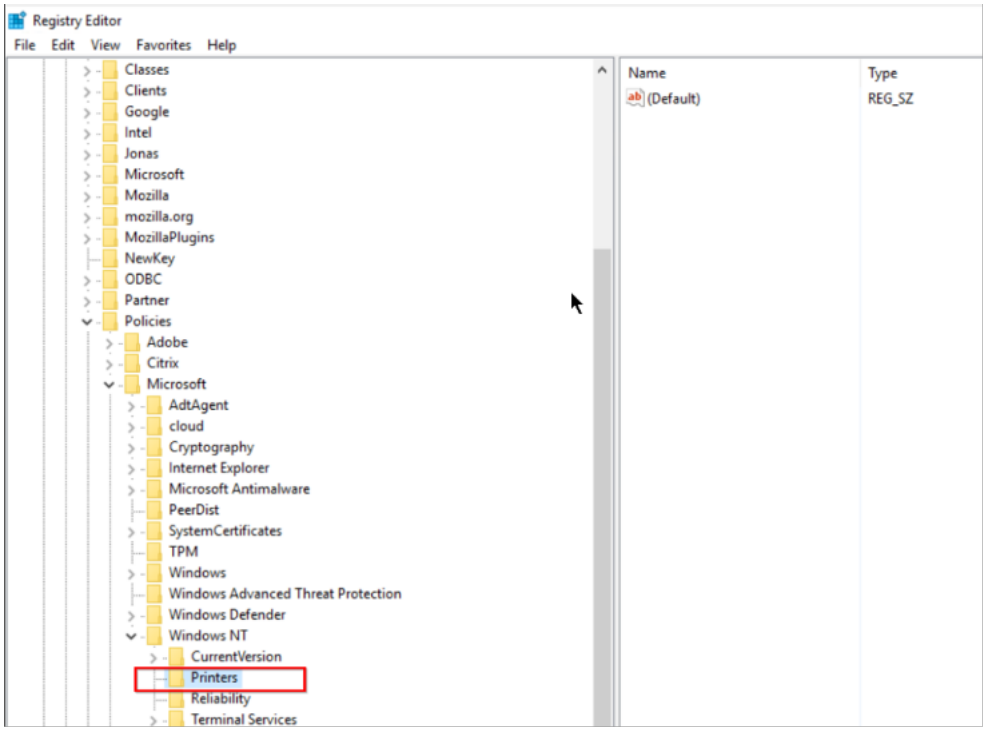

5. Cree una clave con el nombre **Microsoft-Windows-PrintService/Operational**. Esta clave habilita los registros del servicio de impresión.



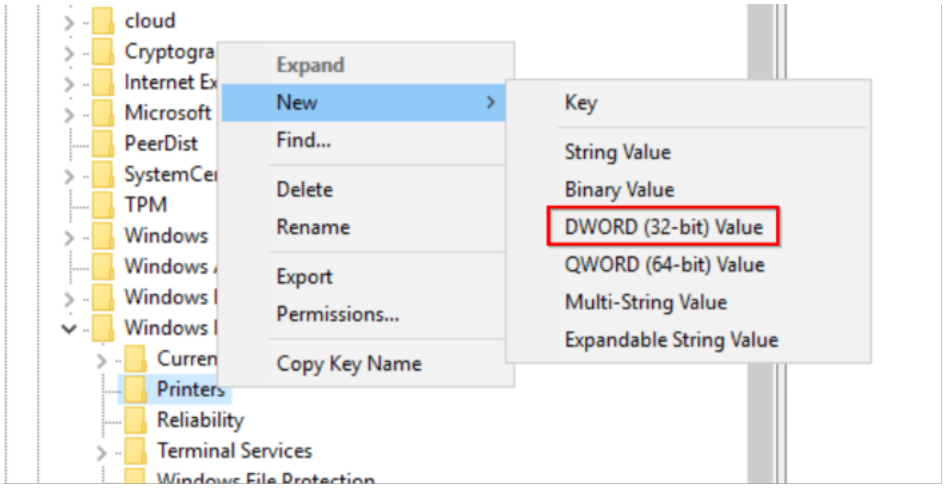

6. Vaya a **HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows NT\Printers**.

> **Nota**
>
> Si la carpeta Impresoras no está disponible, cree una clave con el nombre Impresoras en la carpeta Windows NT.

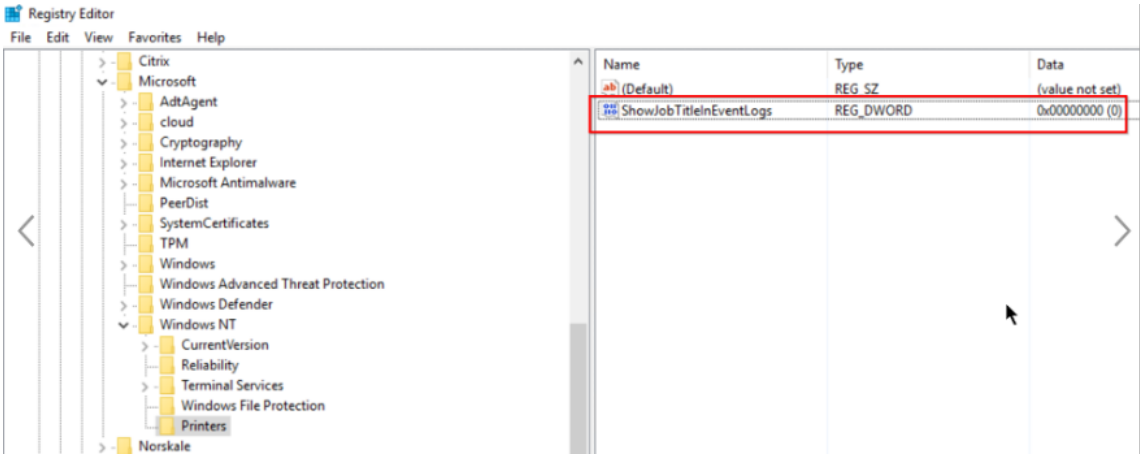



7. Haga clic con el botón secundario del mouse en la carpeta **Impresoras** y seleccione **Nuevo > Valor de DWORD (32 bits)**

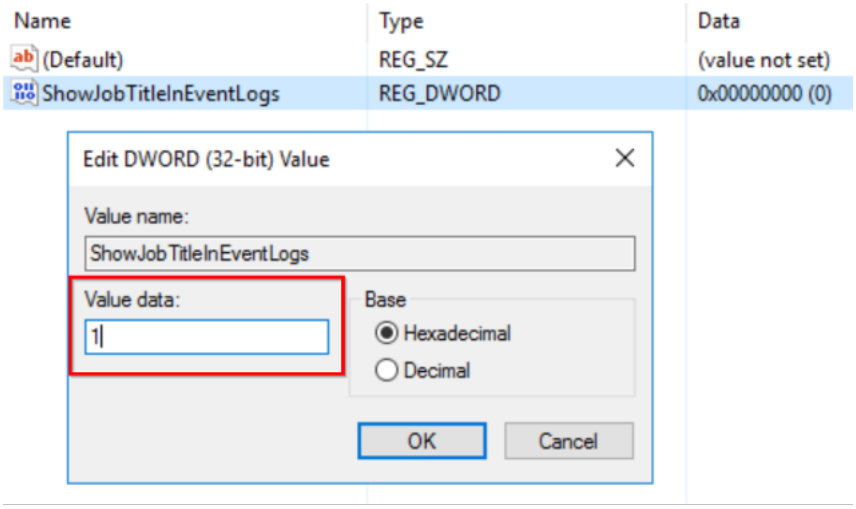



8. Cree un valor con el nombre **ShowJobTitleInEventLogs**.




9. Haga clic con el botón secundario en **ShowJobTitleInEventLogs** y seleccione **Modificar**. Introduzca 1 en **Datos del valor** y haga clic en **Aceptar**.

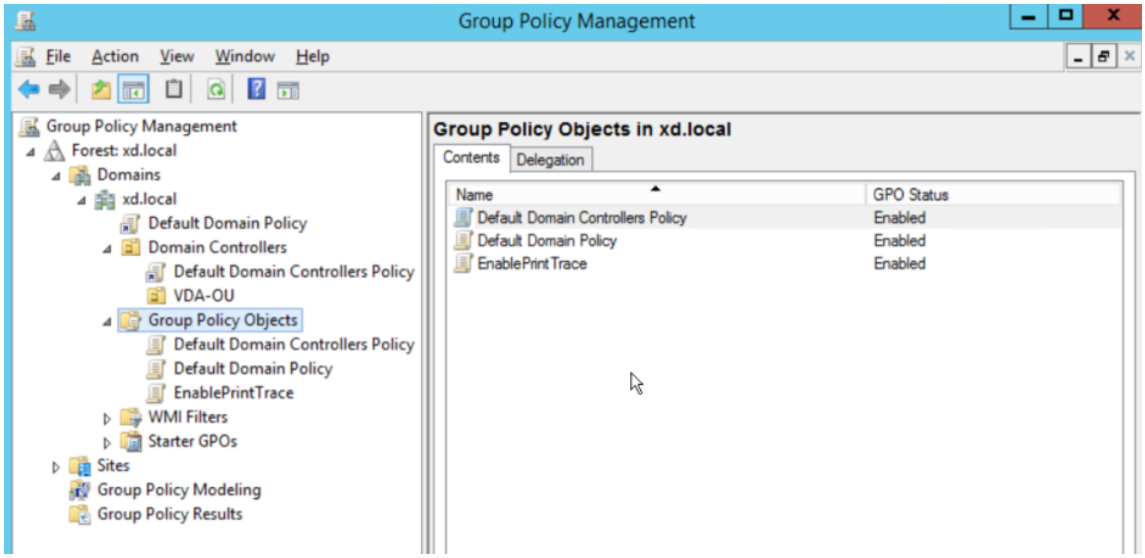



**Crear claves de registro en varios VDA mediante GPO** Este enfoque solo funciona para los VDA persistentes y requiere el reinicio de los VDA tras la creación de las claves de registro. Un VDA persistente es una máquina que mantiene su estado tras un reinicio. Los datos de los usuarios no se pierden tras el reinicio.

### Crear un GPO de registro con las claves de registro

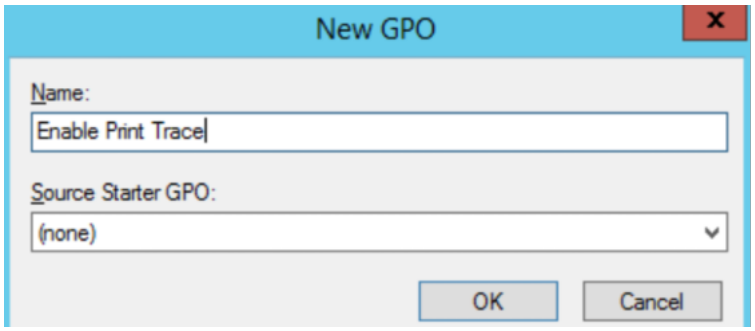
1. Abra la Administración de directivas de **grupo y haga clic con el botón**derecho en




2. En la ventana **Nuevo GPO**, introduzca los valores en los siguientes campos:

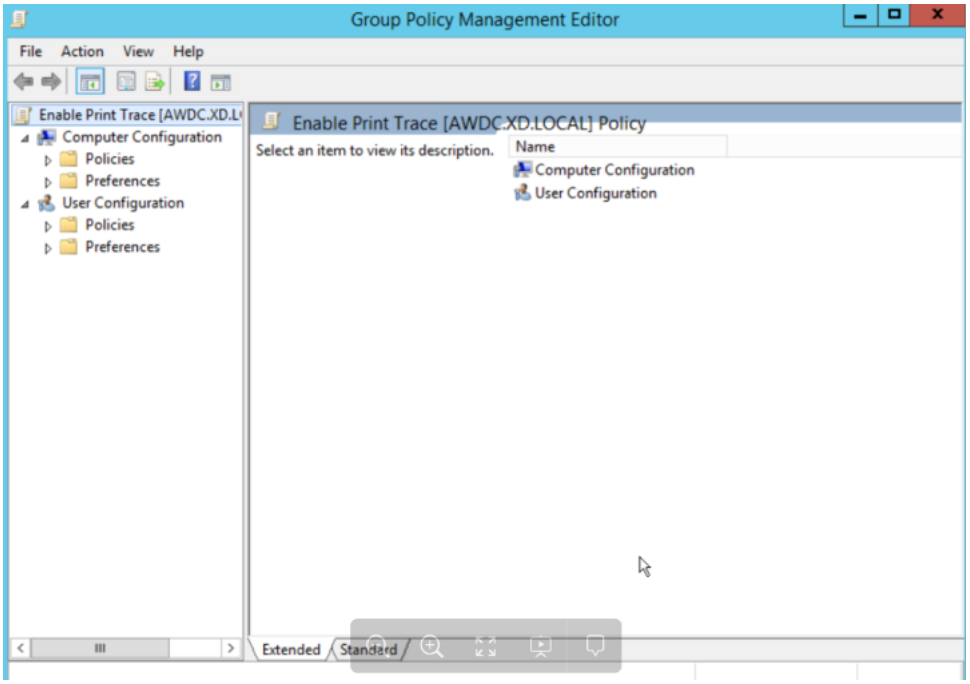
   - Nombre: Habilitar trazado de impresión
   - GPO de inicio de origen: (ninguno)



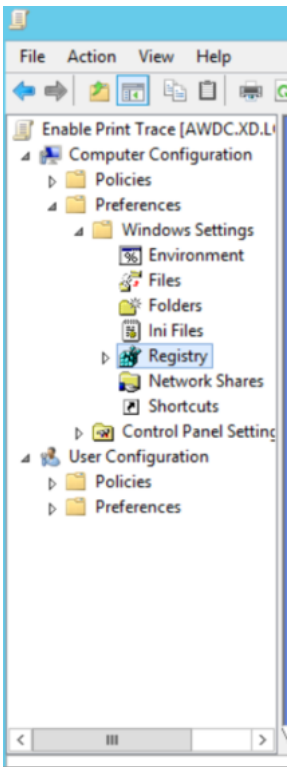

3. Seleccione **OK**.

4. Haga clic con el botón secundario en el objeto **Activar trazado de impresión** que creó y seleccione **Modificar**




5. En la lista **Configuración del equipo**, seleccione **Preferencias > Configuración de Windows**.

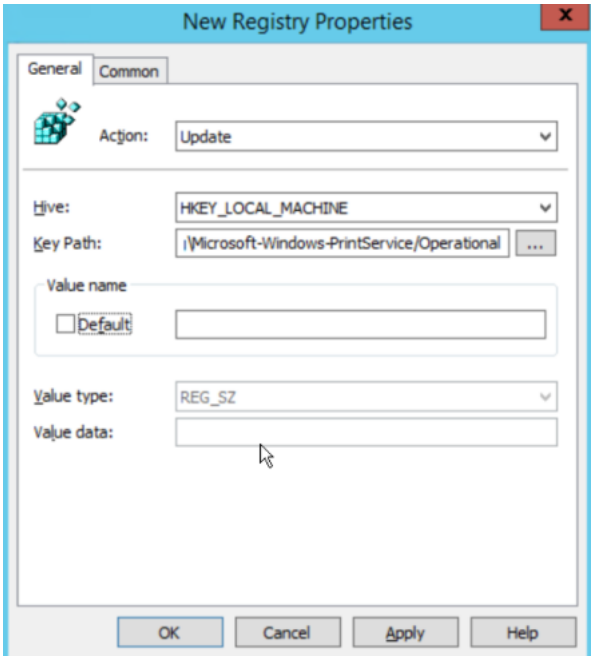



6. Haga clic con **el**botón secundario en **Registro y seleccione Nuevo > Elemento** Introduzca las siguientes propiedades para habilitar los registros de impresión:

   - Acción: actualizar

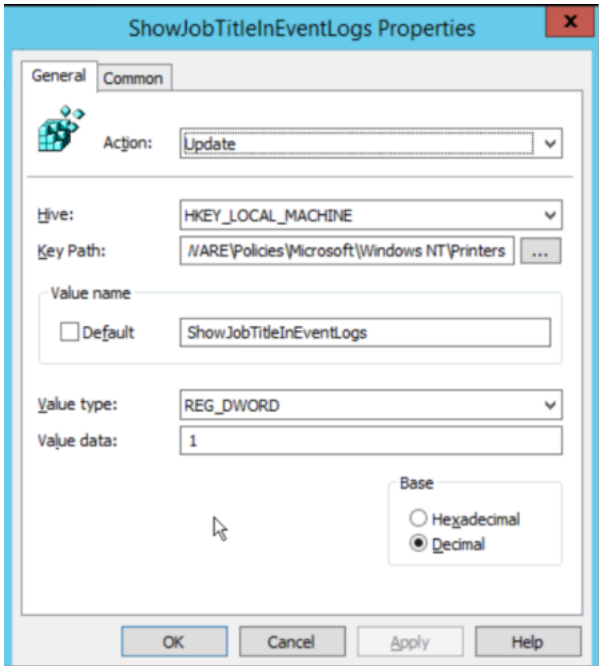
- Colmena: HKEY_LOCAL_MACHINE
- Ruta de la clave: SYSTEM\CurrentControlSet\Services\EventLog\Microsoft-Windows-PrintService/Operational




7. Selecciona **Aplicar** y, a continuación, **Aceptar**.
8. De nuevo, haga clic con el botón secundario en **Registro** y seleccione **Nuevo > Elemento del Registro**. Introduzca las siguientes propiedades para habilitar los nombres de los trabajos de impresión:

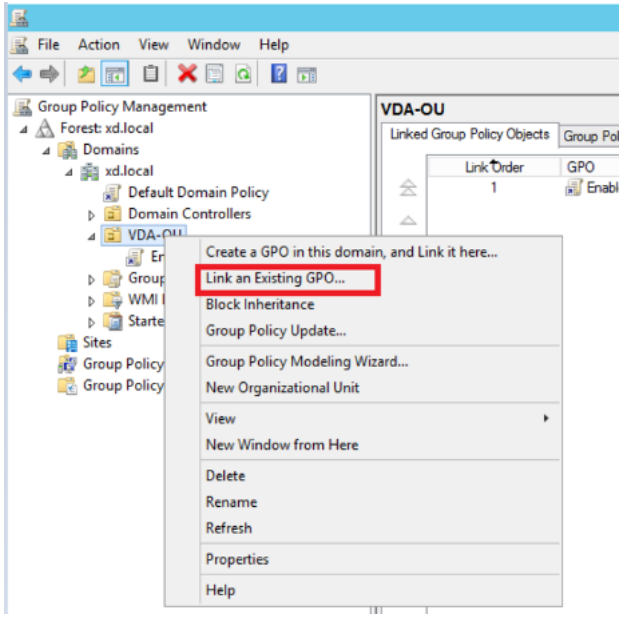
   - Acción: actualizar
   - Colmena: HKEY_LOCAL_MACHINE
   - Ruta de la clave: SOFTWARE\Policies\Microsoft\Windows NT\Printers
   - Nombre del valor: ShowJobTitleInEventLogs
   - Tipo de valor: REG_DWORD
   - Datos de valor: 1
   - Base: decimal



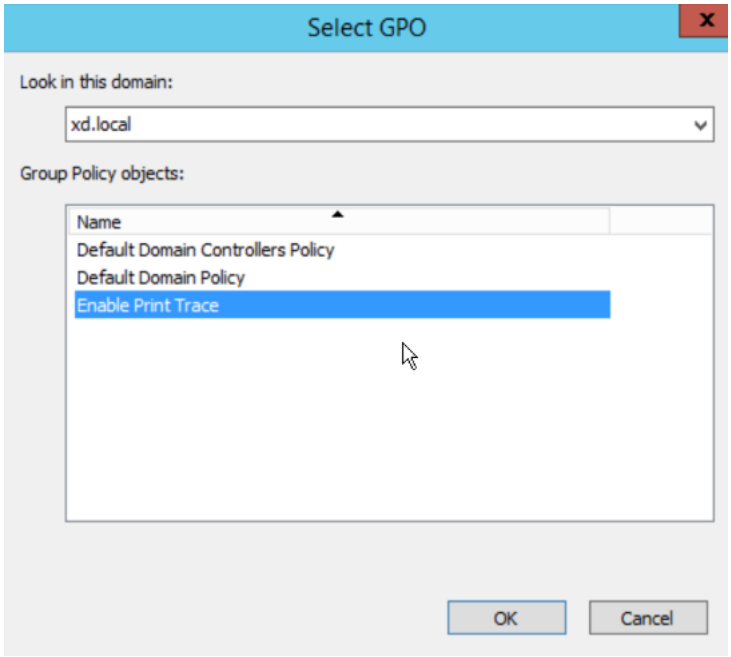

**Habilitar el seguimiento de impresión para la unidad organizativa**

1. Abra **Group Policy Management** y seleccione el dominio (por ejemplo, xd.local) o la OU si los VDA forman parte de ella (por ejemplo, VDA-OU).
2. Haga clic con el botón secundario en el dominio (xd.local) o la OU (VDA-OU) y seleccione **Vincular un GPO existente**.

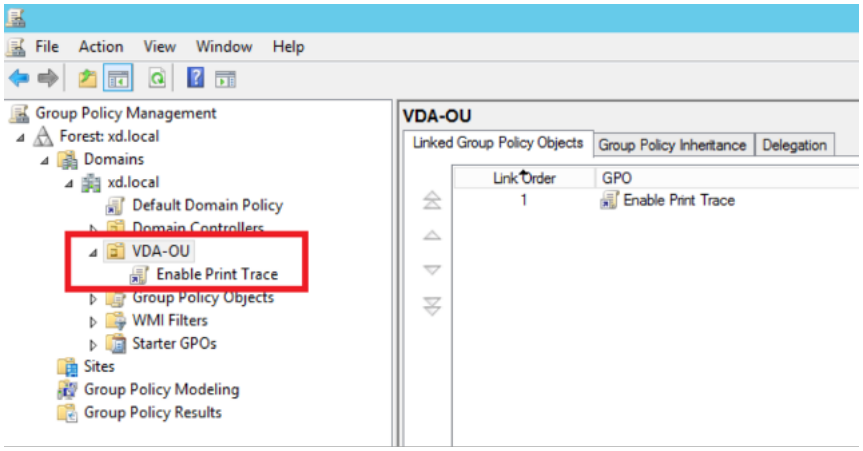



3. En el cuadro de diálogo **Seleccionar GPO**, seleccione Habilitar trazado de impresión y seleccione **Aceptar**.




4. Compruebe que el **GPO Habilitar seguimiento de impresión** esté vinculado a la OU.




**Nota**

- Cuando reinicia un VDA, se pierden todos los eventos de la cola y no estarán disponibles en Citrix Analytics.
- Este reinicio tiene poco impacto en un VDA de sesión única, ya que solo puede haber una sesión activa en un momento dado, por lo que la cantidad de eventos es menor.
- Este reinicio tiene un gran impacto en un VDA multisesión, ya que todas las sesiones activas se terminan durante el reinicio y se pierden los eventos que están en la cola.

### Habilitar la telemetría del portapapeles para Citrix DaaS

El Citrix DaaS (anteriormente conocido como Citrix Virtual Apps and Desktops Service) permite a los usuarios realizar operaciones con el portapapeles y los registros relacionados se pueden ver en Citrix Analytics for Security. Estos registros del portapapeles proporcionan información valiosa, como el nombre del VDA, el tamaño del portapapeles, el tipo de formato del portapapeles, la IP del cliente, el funcionamiento del portapapeles, la dirección de operación del portapapeles y si la operación del portapapeles estaba permitida.

Como administrador de seguridad, puede utilizar estos registros para analizar e investigar los riesgos seleccionando la fuente de datos de **aplicaciones y escritorios** en la página de **búsqueda** de Citrix Analytics for Security.

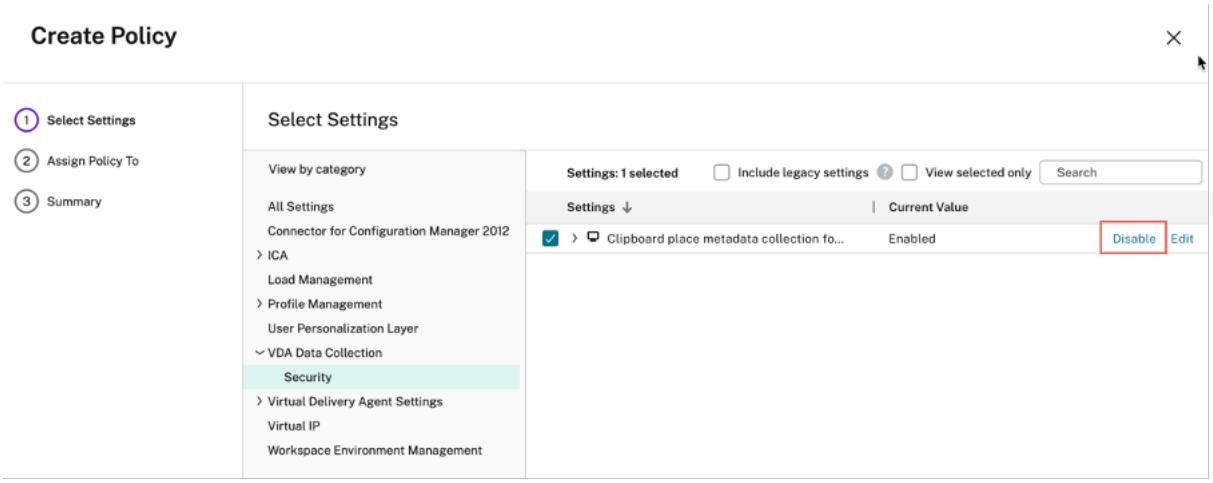
> **Nota**
>
> - De forma predeterminada, la recopilación y la transmisión de estos registros del portapapeles están habilitadas en los Virtual Delivery Agents (VDA).
> - Esta configuración solo se aplica a los VDA de Windows.

#### Requisitos previos

- La versión de su VDA debe ser la misma que la versión básica de Citrix Virtual Apps and Desktops 7 2305 o una versión posterior. Para obtener más información, consulte Citrix Virtual Apps and Desktops 7 2305.
- Asegúrese de que la configuración **Redirección del portapapeles del cliente** en la página **Directivas de Web Studio** no esté configurada en un estado prohibido. Para obtener más información, consulte Redirección del portapapeles del cliente.

Puede utilizar la **colección de metadatos del portapapeles para la directiva de supervisión de seguridad para** habilitar o inhabilitar la telemetría del portapapeles. De manera predeterminada, esta directiva está habilitada. Para inhabilitarla, debe ir a la página de **directivas** > seleccionar **Seguridad** en la **recopilación de datos del VDA** > comprobar la directiva > hacer clic en **Inhabilitar**.




Para obtener más información, consulte la colección de metadatos de Clipboard Place para la supervisión de la seguridad.

### Activar o desactivar el procesamiento de datos en el origen de datos

Puede detener el procesamiento de datos en cualquier momento para un origen de datos concreta: la aplicación Director y Workspace. En la tarjeta del sitio de origen de datos, haga clic en los puntos **suspensivos verticales () > Desactivar el procesamiento de datos**. Citrix Analytics deja de procesar los datos de esa fuente de datos. También puede detener el procesamiento de datos desde la tarjeta del sitio Aplicaciones y escritorios. Esta opción se aplica a los dos orígenes de datos: Director y la aplicación Workspace.

Para volver a habilitar el procesamiento de datos, haga clic **en Activar procesamiento de datos**.

## Integración de Microsoft Active Directory y Azure Active Directory

September 11, 2024

> **Nota:**
>
> Desde julio de 2023, Microsoft cambió el nombre de Azure Active Directory (Azure AD) a Microsoft Entra ID. En este documento, cualquier referencia a Azure Active Directory, Azure AD o AAD ahora se refiere a Microsoft Entra ID.

Conecte su Active Directory o Azure Active Directory e importe los detalles del usuario y los grupos de usuarios del dominio de su organización a Citrix Analytics for Security.

Esta integración mejora los perfiles de usuario en Citrix Analytics for Security con detalles de identidad del usuario, como el cargo, la organización, la ubicación de la oficina, el correo electrónico y los datos

de contacto. En la página Perfil de usuario, puede ver estos detalles del usuario, que le ayudan durante la investigación y el análisis de riesgos.

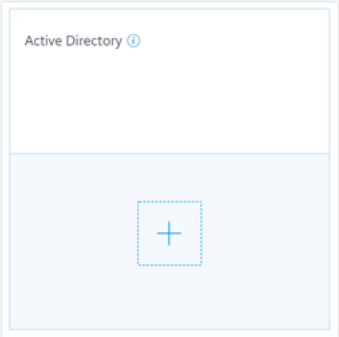
### Requisitos previos

- Si desea conectar Active Directory con Citrix Analytics for Security, asegúrese de que Active Directory esté conectado primero a su cuenta de Citrix Cloud. Para obtener más información, consulte Conectar Active Directory a Citrix Cloud.
- Si desea conectar Azure Active Directory con Citrix Analytics for Security, asegúrese de que su Azure Active Directory esté conectado primero a su cuenta de Citrix Cloud. Para obtener más información, consulte Conectar Azure Active Directory a Citrix Cloud.

### Conectar Microsoft Active Directory

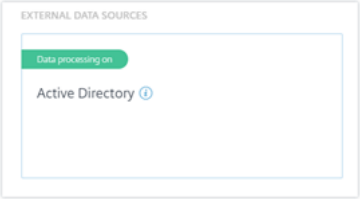
Para conectar su Active Directory a Citrix Analytics for Security, haga lo siguiente:

1. Vaya a **Parámetros** > **Orígenes de datos** > **Seguridad** y después vaya a la sección **ORÍGENES DE DATOS EXTERNOS**.
2. En la tarjeta del sitio de **Active Directory**, haga clic en el signo más **+**.




3. Citrix Analytics le pide que conecte Active Directory a su cuenta de Citrix Cloud. Para obtener más información, consulte Requisitos previos.

Después de conectar su Active Directory a su cuenta de Citrix Cloud, Citrix Analytics descubre automáticamente esta nueva fuente de datos. En la página **Orígenes de datos**, la tarjeta del sitio de Active Directory muestra **Procesamiento de datos en**.



El estado **Procesamiento de datos en** indica que se ha descubierto Active Directory y que la información del usuario se está obteniendo de Active Directory.

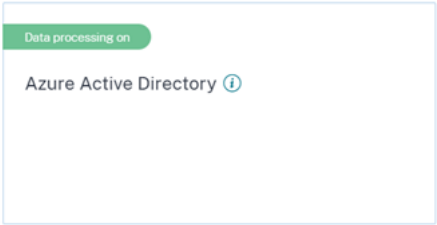
### Conectar Microsoft Azure Active Directory

Para conectar su Azure Active Directory a Citrix Analytics, haga lo siguiente:

1. Vaya a **Configuración > Orígenes de datos > Seguridad** y, a continuación, vaya a la sección **ORÍGENES DE DATOS EXTERNOS**.
2. En la tarjeta del sitio de **Azure Active Directory**, haga clic en el signo más +.


3. Citrix Analytics le pide que conecte Azure Active Directory a su cuenta de Citrix Cloud. Para obtener más información, consulte Conectar Azure Active Directory a Citrix Cloud.

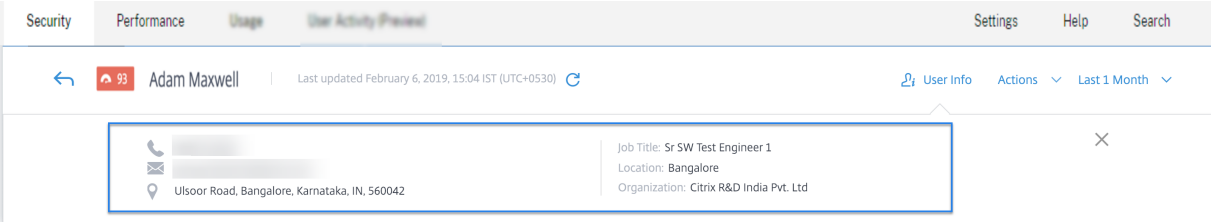
Después de conectar su Azure Active Directory a su cuenta de Citrix Cloud, Citrix Analytics descubre automáticamente esta nueva fuente de datos. En la página **Orígenes de datos**, la tarjeta de sitio de **Azure Active Directory** muestra el **procesamiento de datos en**. Este estado indica que se ha descubierto Azure Active Directory y que la información del usuario se está recuperando de Azure Active Directory.




### Ver la información del usuario

En la pestaña **Seguridad**, haga clic en un usuario con riesgos para ver la página de perfil de usuario. Si el usuario está disponible en Active Directory o Azure Active Directory, puede ver el puesto, la organización, el correo electrónico y el número de contacto en la página de perfil del usuario.




# Integración de Microsoft Graph Security

June 17, 2021

Microsoft Graph Security es una fuente de datos externa que agrega datos de varios proveedores de seguridad. También proporciona acceso a los datos de inventario del usuario.

Citrix Analytics admite actualmente los siguientes proveedores de seguridad de Microsoft Graph Security:

- Protección de identidad de Azure AD
- Microsoft Defender for Endpoint

Para obtener más información sobre los proveedores de seguridad, consulte los siguientes vínculos:

- Para **Azure AD Identity Protection**: https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/concept-risk-events
- Para **Microsoft Defender for Endpoint**: https://docs.microsoft.com/en-us/mem/configmgr/protect/deploy-use/defender-advanced-threat-protection

Para agregar el origen de datos de Microsoft Graph Security, debe obtener los permisos necesarios en nombre de un arrendatario desde la plataforma de identidades de Microsoft.

## Requisitos previos

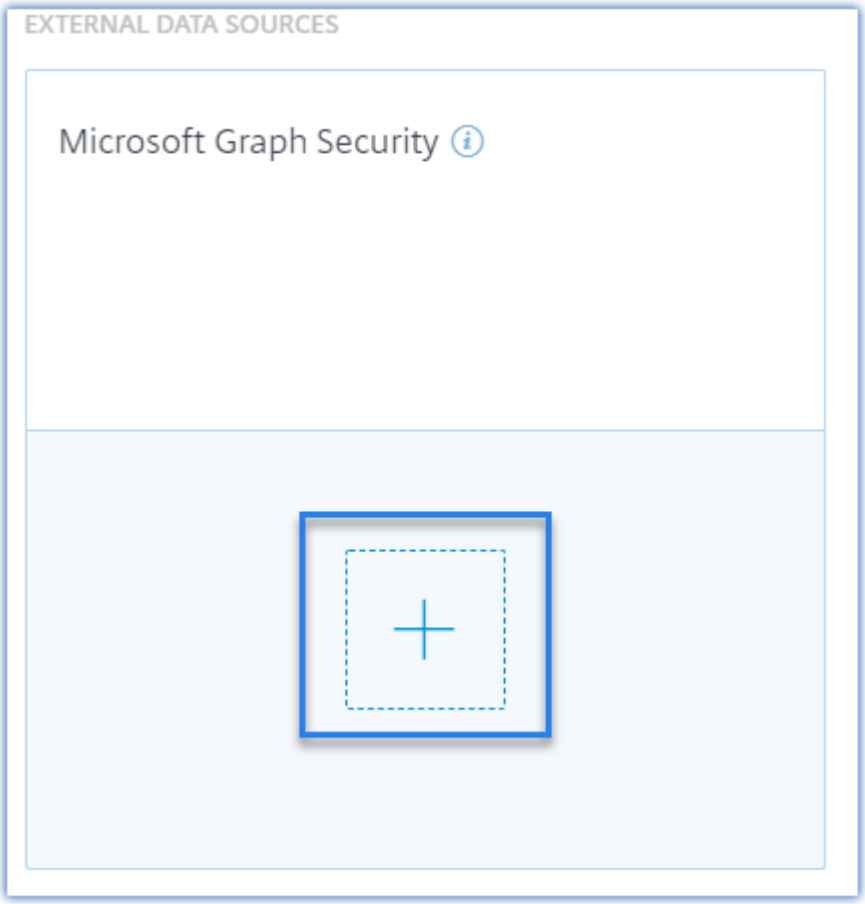
Antes de comenzar a incorporar el origen de datos de Microsoft Graph Security, asegúrese de que:

- El administrador está utilizando el proveedor de seguridad de Azure AD Identity Protection (parte del proveedor de seguridad de Azure AD Premium P2).
- El usuario final ha iniciado sesión en Microsoft Store con cuentas de Work o School.

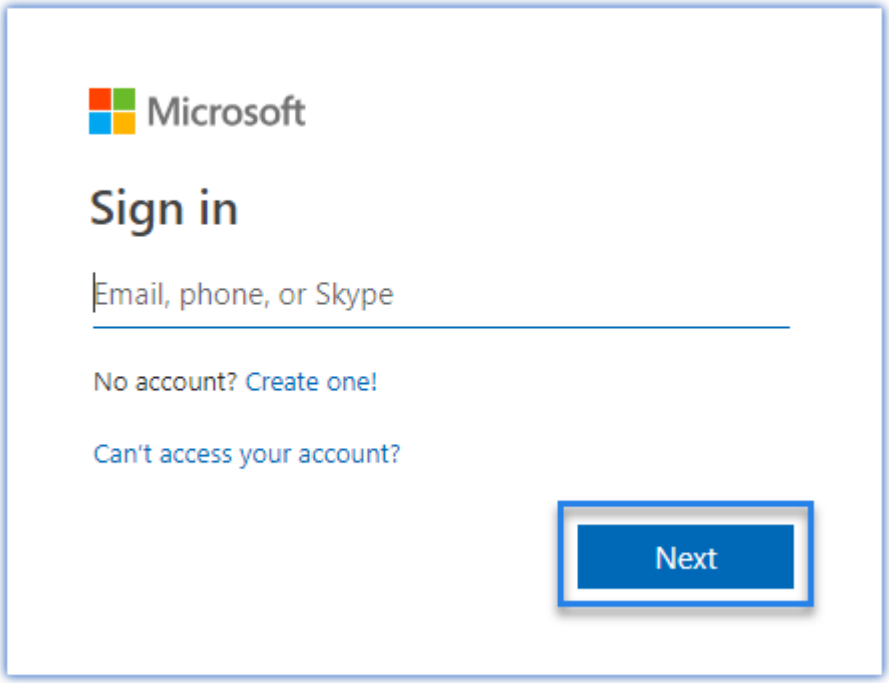
### Incorporación de instancias de Microsoft Graph Security

1. Vaya a **Configuración** > **Orígenes de datos** > **Seguridad** y, a continuación, vaya a la sección **FUENTES DE DATOS EXTERNAS**.
2. Haga clic en el signo más (**+**) de la tarjeta de sitio de Microsoft Graph Security. Se redirige al extremo de autorización.



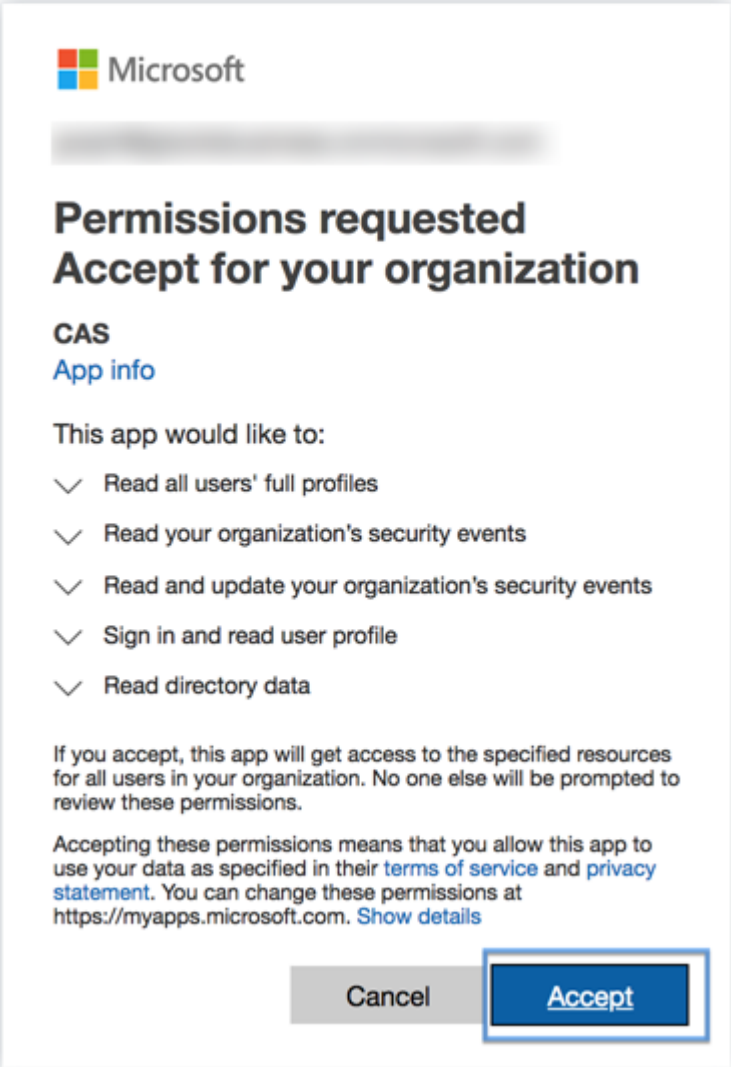

3. En la ventana de **Microsoft**, inicie sesión con sus credenciales de inicio de sesión de Azure para registrar una cuenta. O bien, seleccione una cuenta existente.
4. Haga clic en **Siguiente**.




5. Haga clic en **Aceptar**. Se redirige a la página Orígenes de datos. El origen de datos de Microsoft Graph Security ahora está vinculado a su cuenta de Citrix Cloud.

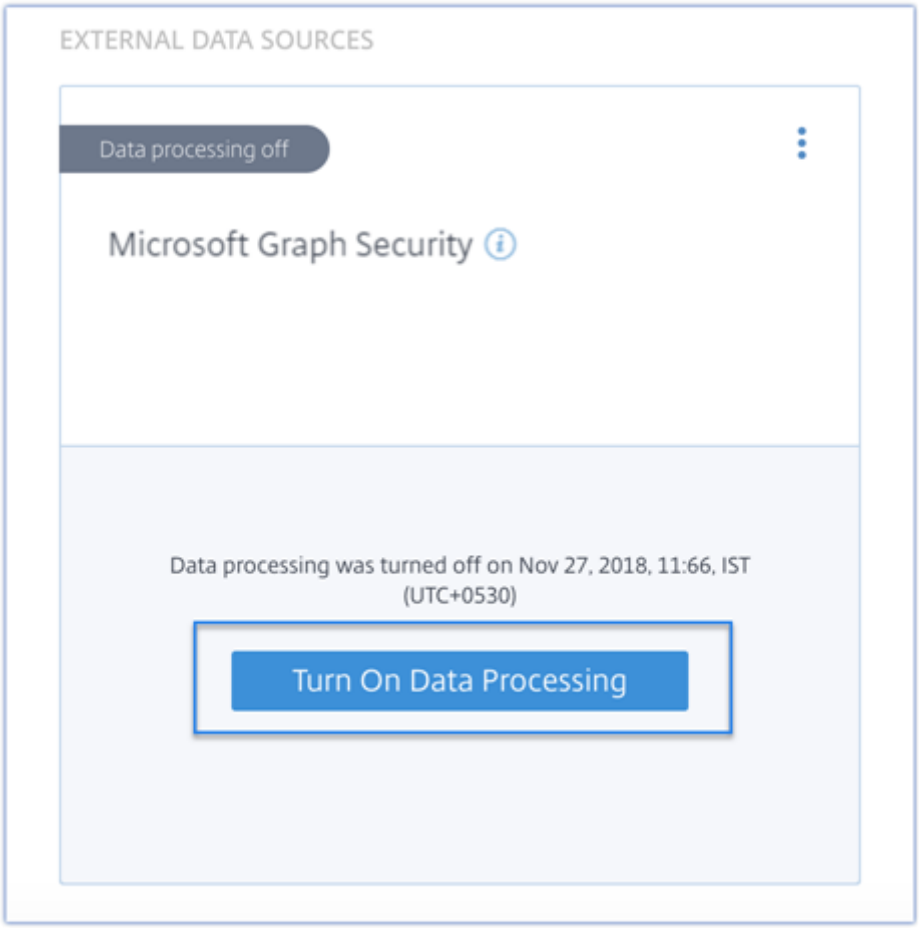



### Activar o desactivar el procesamiento de datos

Para inhabilitar el procesamiento de datos, haga clic en los puntos suspensivos verticales () de la tarjeta de sitio y seleccione **Desactivar el procesamiento de datos**. Impide que Citrix Analytics procese datos para esta fuente de datos.

Puede volver a activar el procesamiento de datos seleccionando **Activar procesamiento de datos** en la tarjeta del sitio.




Para obtener información sobre los indicadores de riesgo de Microsoft Graph Security, consulte Indicadores de riesgo de Microsoft Graph Security.

## Integración de gestión de información y eventos de seguridad (SIEM)

December 7, 2023

> **Nota**
>
> Contacte con CAS-PM-Ext@cloud.com para solicitar asistencia para la integración de SIEM, la exportación de datos a SIEM y proporcionar comentarios.

Integre Citrix Analytics for Security con sus servicios de SIEM y exporte los datos de los usuarios del entorno de TI de Citrix a su SIEM. Correlacione los datos exportados con los datos disponibles en su SIEM para obtener información más profunda sobre la postura de seguridad de su organización.

Esta integración mejora el valor tanto de su Citrix Analytics for Security como de su SIEM.

### Ventajas

- Permite a los equipos de operaciones de seguridad correlacionar, analizar y buscar datos de registros dispares.
- Ayuda a sus equipos de operaciones de seguridad a identificar y remediar rápidamente los riesgos de seguridad.
- Visibilidad de las alertas de seguridad en un lugar centralizado.
- Enfoque centralizado para detectar posibles amenazas a la seguridad de las capacidades de análisis de riesgos de la organización, como indicadores de riesgo, perfiles de usuario y puntuaciones de riesgo.
- Capacidad para combinar y correlacionar la información de inteligencia de riesgos de Citrix Analytics de una cuenta de usuario con los orígenes de datos externas conectadas dentro de su SIEM.

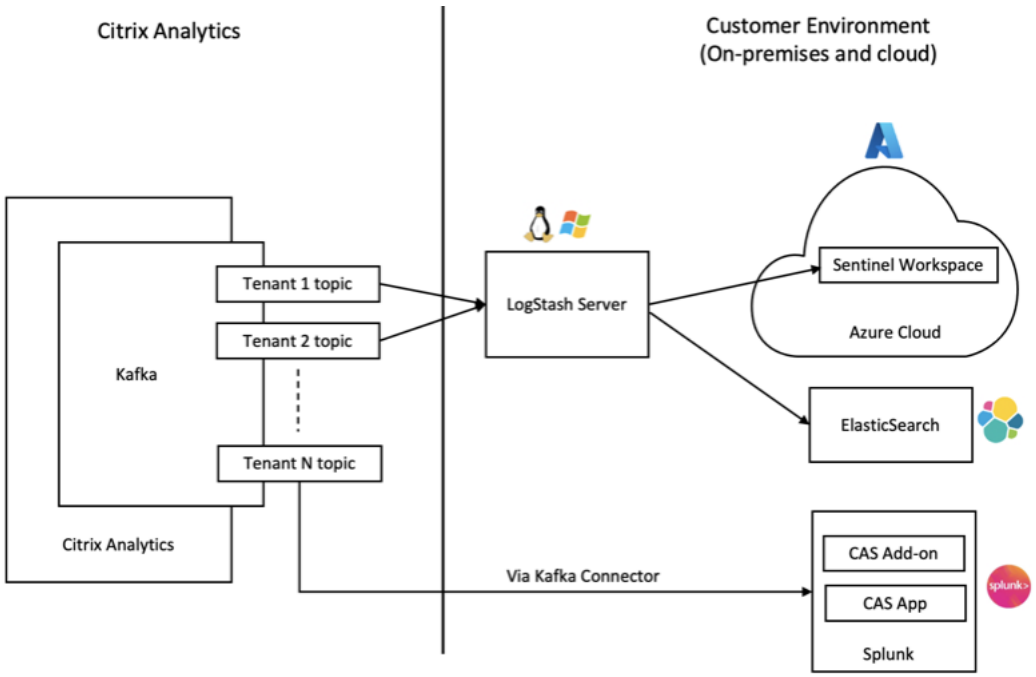
### Arquitectura de integración de SIEM

Su integración de SIEM se conecta con el Kafka en dirección norte implementado en la nube de Citrix Analytics for Security. Esto se puede lograr de las dos formas siguientes:

- **Dispositivos de punto final de Kafka**: Si su SIEM admite los dispositivos de punto final de Kafka, utilice los parámetros proporcionados en el archivo de configuración de Logstash y los detalles del certificado del archivo JKS o el archivo PEM para integrar su SIEM con Citrix Analytics for Security. Con los terminales de Kafka, puede conectar y extraer los datos al SIEM de su elección.
- **Motor Logstash**: Si su SIEM no admite los dispositivos de punto final de Kafka, puede utilizar el motor de recopilación de datos de Logstash. Puede enviar los datos de información sobre riesgos de Citrix Analytics for Security a uno de los complementos de salida compatibles con Logstash.

Consulte el siguiente diagrama de arquitectura de soluciones SIEM para comprender cómo fluyen los datos desde Citrix Analytics for Security a su servicio SIEM:

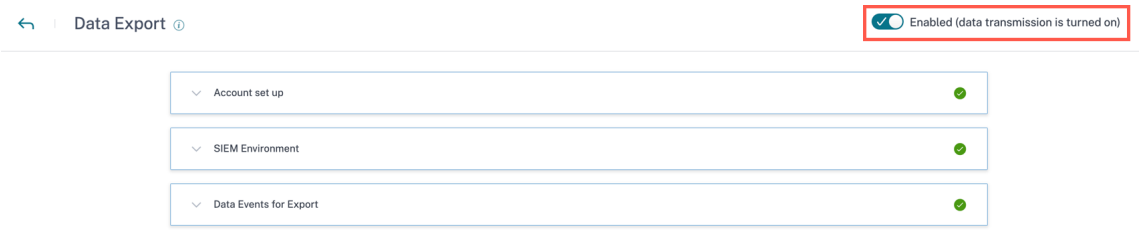



## Activar o desactivar la transmisión de datos

Para dejar de transmitir datos de Citrix Analytics for Security:

1. Ve a **Configuración > Exportaciones de datos**.
2. Apague el botón para desactivar la **transmisión de datos**.

> **Nota**
> De forma predeterminada, la transmisión de datos siempre está activada/habilitada para SIEM.




Para habilitar de nuevo la transmisión de datos, active el botón.

## Configuración del entorno SIEM

Para exportar datos a SIEM, debe realizar las siguientes acciones:

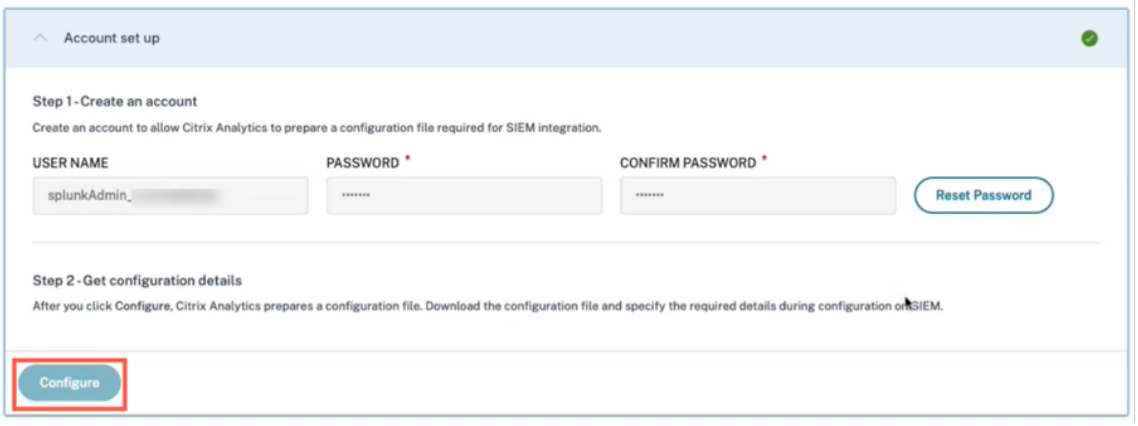
- Configure su cuenta de Kafka y sus credenciales de autenticación

- Descargue la configuración rellenada previamente y configure el entorno SIEM
- Eventos de datos para exportar

## Configuración de la cuenta de exportación SIEM

1. Para configurar su cuenta, vaya a **Configuración > Exportación de datos > expanda Configuración de cuenta**. Cree una cuenta especificando el nombre de usuario y la contraseña. Una vez que haya configurado su cuenta, se generarán sus datos de Kafka. Estos detalles se incrustan automáticamente al generar el archivo de configuración.



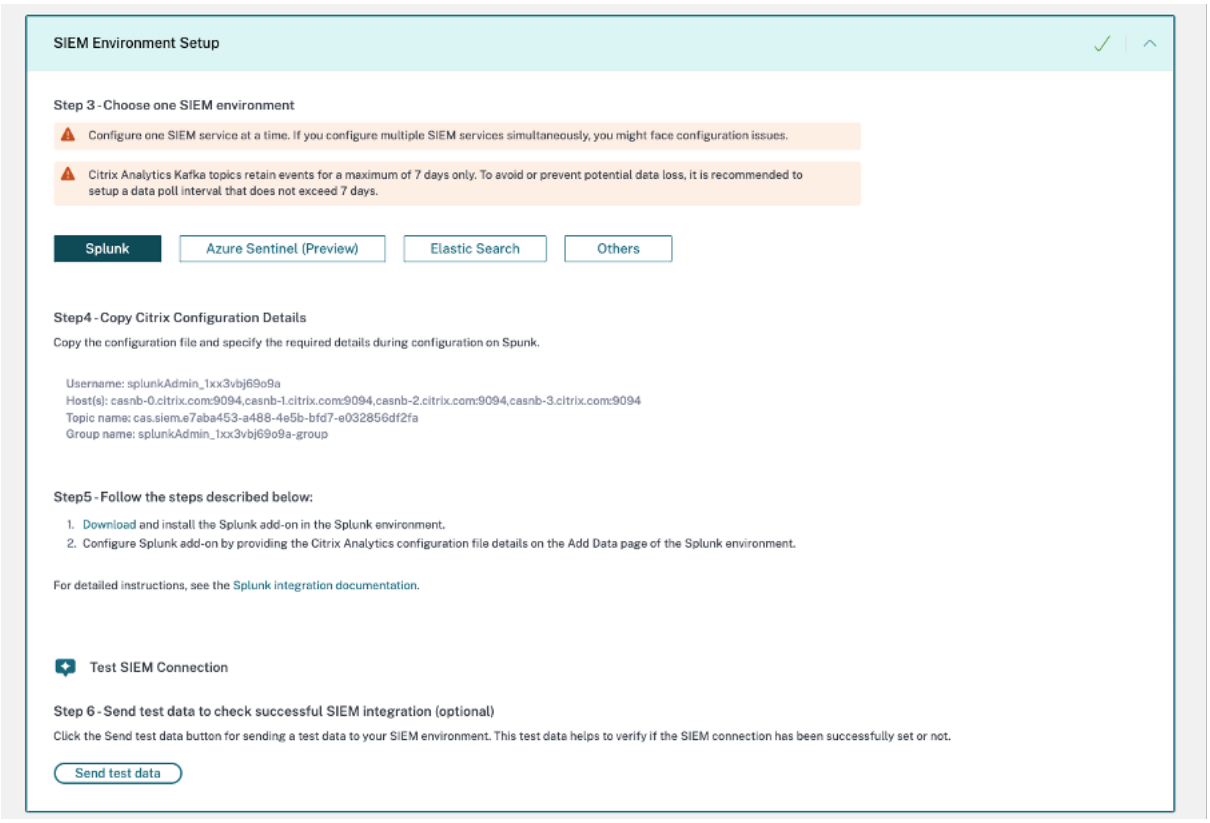

2. Haga clic en **Configurar** para generar el archivo de configuración. El archivo de configuración contiene detalles como los puntos finales de Kafka, los temas de suscripción específicos y los ID de grupo. Además, preconfigura los atributos Kafka y SSL que se requieren para completar la autenticación y el flujo de datos.

## Configuración de SIEM y configuración del entorno

Elija el entorno SIEM según sea necesario. Puede integrar Citrix Analytics for Security con los siguientes servicios. Consulte los siguientes enlaces para obtener información detallada y configuraciones específicas de SIEM:

- Splunk
- Microsoft Sentinel
- Elasticsearch
- Otros SIEM que utilizan un conector de datos basado en Kafka o Logstash




## Eventos de datos exportados de Citrix Analytics for Security a su servicio SIEM

Como parte de las exportaciones de SIEM, hay dos tipos de conjuntos de datos:

1. **Eventos de información de riesgos (exportaciones predeterminadas)**: Una vez que haya completado la configuración de la cuenta y la configuración de SIEM, los datos predeterminados (eventos de información de riesgo) comienzan a fluir a su implementación de SIEM. Los datos de información sobre riesgos contienen alertas de puntuación de riesgo, perfil de usuario e indicadores de riesgo del usuario. Se generan mediante el algoritmo de aprendizaje automático de Citrix Analytics, el análisis del comportamiento de los usuarios y se basan en los eventos de los usuarios. Para obtener información sobre los tipos de eventos, los metadatos y los esquemas disponibles, consulte Datos de información sobre riesgos para SIEM.

2. **Eventos de fuentes de datos (exportaciones opcionales)**: Además, puede configurar la función de exportación de datos para exportar eventos de usuario desde orígenes de datos de productos compatibles con Citrix Analytics for Security. Al realizar cualquier actividad en el entorno Citrix, se generan los eventos del origen de datos. Los eventos exportados son datos de uso de usuarios y productos en tiempo real sin procesar, tal como están disponibles en la vista de autoservicio. Los metadatos contenidos en estos eventos también se pueden utilizar para analizar las amenazas en profundidad, crear nuevos paneles y relacionarlos con otros eventos

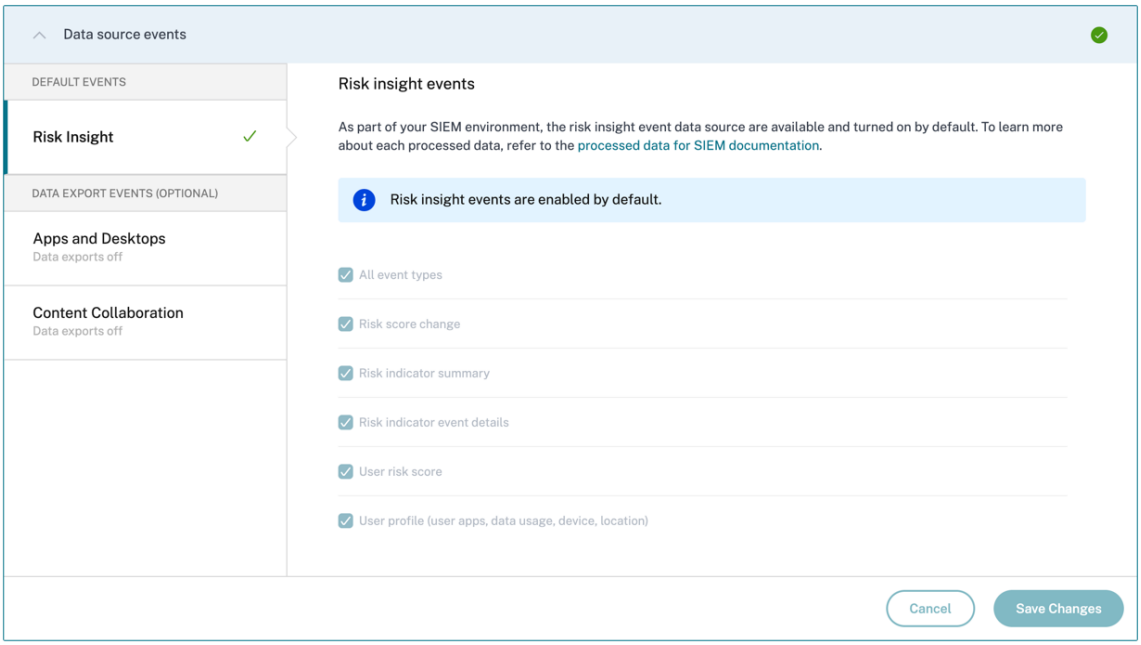
 

de fuentes de datos que no son de Citrix en su infraestructura de seguridad y TI.

Actualmente, Citrix Analytics for Security envía eventos de usuario a su SIEM para la fuente de datos de Citrix Virtual Apps and Desktops.

Para obtener información sobre los tipos de eventos, los metadatos y el esquema disponibles, consulte Eventos de fuentes de datos.

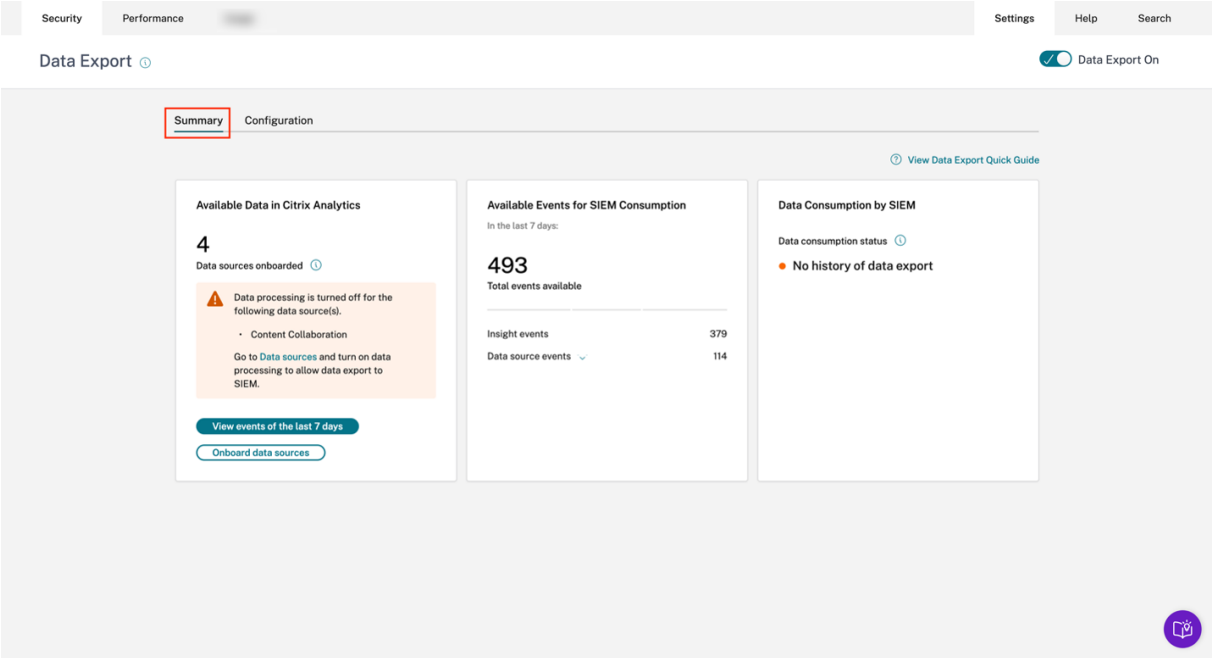
> **Nota**
>
> Para los clientes que utilicen un intermediario de datos Logstash, se recomienda descargar el archivo de configuración más reciente del portal Citrix Analytics for Security y actualizarlo al implementar el servicio Logstash. Esto garantiza que se creen las tablas de eventos del origen de datos correctas y que los eventos ahora estén disponibles en los índices de SIEM.




## Solución de problemas de integración con SIEM

La vista Exportaciones de datos por motivos de seguridad incluye una ficha de **resumen** para ayudar a los administradores a solucionar problemas de integración de SIEM con Citrix Analytics. El panel de **resumen** proporciona visibilidad sobre el estado y el flujo de los datos al guiarlos por los puntos de control que ayudan al proceso de solución de problemas.




Para obtener más información sobre esta función, consulte Solución de problemas de exportación de datos.

## Integración de Splunk

November 17, 2023

Integre Citrix Analytics for Security con Splunk para exportar y correlacionar los datos de los usuarios de su entorno de TI de Citrix con Splunk y obtener información más detallada sobre la postura de seguridad de su organización.

Para obtener más información sobre los beneficios de la integración y el tipo de datos procesados que se envían a su SIEM, consulte Integración de la información de seguridad y la gestión de eventos.

Para desarrollar una comprensión completa de la metodología de implementación de Splunk y adoptar las estrategias para una planificación eficaz, consulte la documentación de Arquitectura de Splunk con las aplicaciones de Citrix
Analytics alojadas en Splunk.

### Integre Citrix Analytics para la seguridad Splunk

Siga las directrices mencionadas para integrar Citrix Analytics for Security con Splunk:

- Exportación de datos. Citrix Analytics for Security crea un canal de Kafka y exporta información sobre riesgos y eventos de orígenes de datos. Splunk recupera esta inteligencia de riesgo del canal.
- Obtenga la configuración de Citrix Analytics. Cree una contraseña para su cuenta predefinida para la autenticación. Citrix Analytics for Security prepara un archivo de configuración necesario para configurar el complemento Citrix Analytics para Splunk.
- Descargue e instale el complemento Citrix Analytics para Splunk. Descargue el **complemento Citrix Analytics para Splunk mediante Splunk** o Splunk Cloud para completar el proceso de instalación.
- Configure el complemento Citrix Analytics para Splunk. Configure una entrada de datos mediante los detalles de configuración proporcionados por Citrix Analytics for Security y configure el complemento Citrix Analytics para Splunk.

Después de preparar el archivo de configuración de Citrix Analytics, consulte:

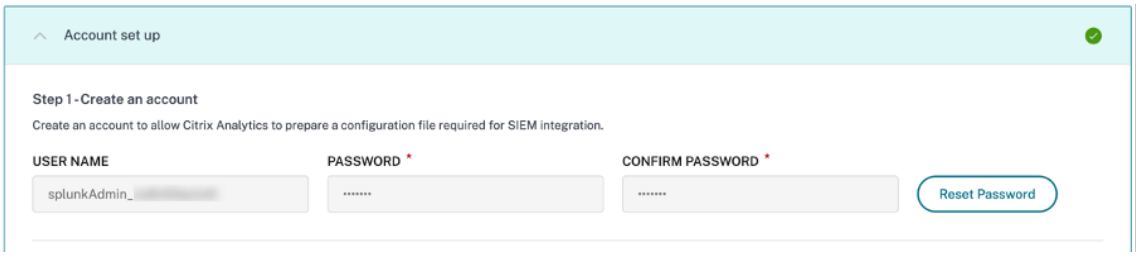
- Capacidad de restablecimiento de contraseña
- Activar o desactivar la transmisión de datos

Una vez configurado el complemento de Citrix Analytics para Splunk, consulte:

- Cómo consumir eventos en Splunk Environment
- Cómo configurar la aplicación Citrix Analytics para Splunk

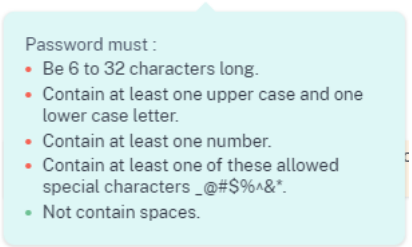
### Exportación de datos

1. Ve a **Configuración** > **Exportaciones de datos**.
2. En la sección **Configuración de la cuenta**, cree una cuenta especificando el nombre de usuario y la contraseña. Esta cuenta se usa para preparar un archivo de configuración, que se requiere para la integración.



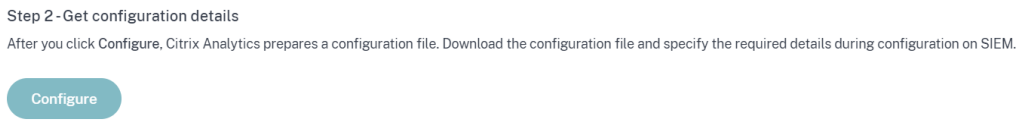

3. Asegúrese de que la contraseña cumpla con las siguientes condiciones:




4. Seleccione **Configurar**.

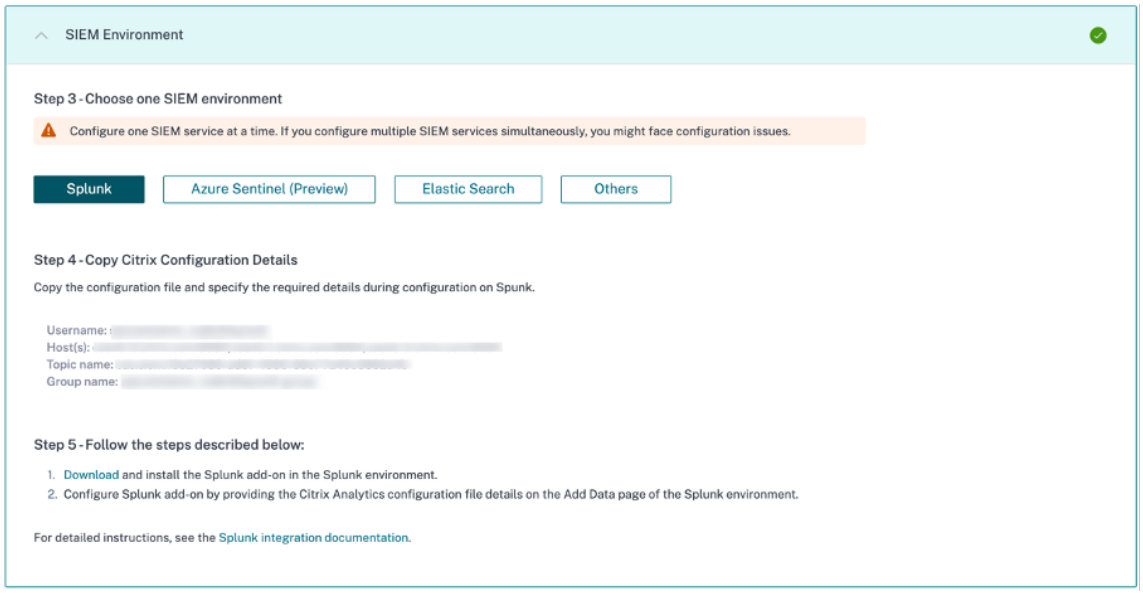
   Citrix Analytics for Security prepara los detalles de configuración necesarios para la integración de Splunk.




5. Seleccione **Splunk**.
6. Copie los detalles de configuración, que incluyen el nombre de usuario, los hosts, el nombre del tema de Kafka y el nombre del grupo.

   Necesita estos detalles para configurar el complemento de Citrix Analytics para Splunk en los pasos siguientes.

   > **IMPORTANTE**
   >
   > Estos detalles son confidenciales y debe guardarlos en un lugar seguro.




Para generar datos candidatos para Splunk Integration, active el procesamiento de datos para al menos una fuente de datos o utilice la capacidad de generación de eventos de prueba. Ayuda a

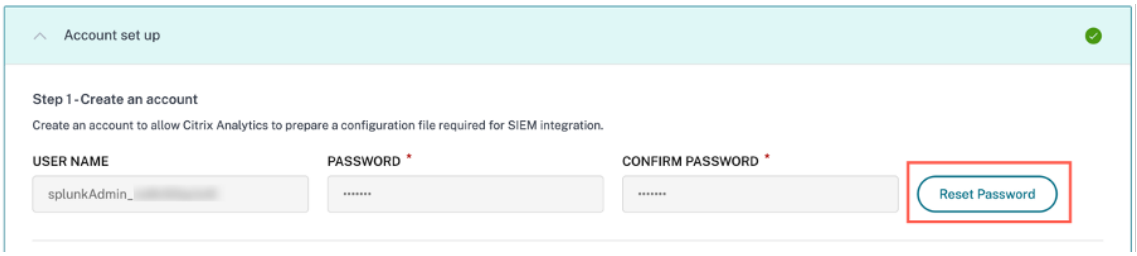
 

Citrix Analytics
for Security a iniciar el proceso de integración de Splunk.

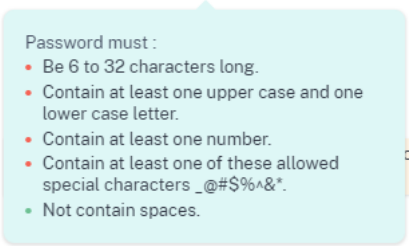
### Capacidad de restablecimiento de contraseña

Si quiere restablecer la contraseña de configuración en Citrix Analytics for Security, siga los pasos siguientes:

1. En la página **Configuración de la cuenta**, haga clic en **Restablecer contraseña**.

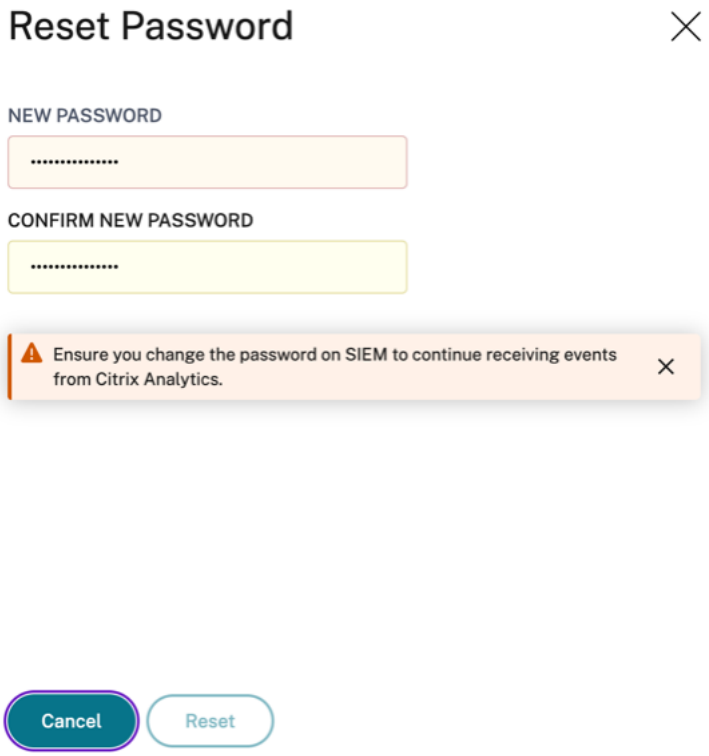



2. En la ventana **Restablecer contraseña**, especifique la contraseña actualizada en los campos **NUEVA CONTRASEÑA** y **CONFIRMAR NUEVA CONTRASEÑA**. Siga las reglas de contraseña que se muestran.




3. Haga clic en **Restablecer**. Se ha iniciado la preparación del archivo de configuración.




> **Nota**
>
> Después de restablecer la contraseña de configuración, asegúrese de actualizar la nueva contraseña cuando configure la entrada de datos en la página **Agregar datos**del entorno Splunk. Ayuda a Citrix Analytics for Security a seguir transmitiendo datos a Splunk.

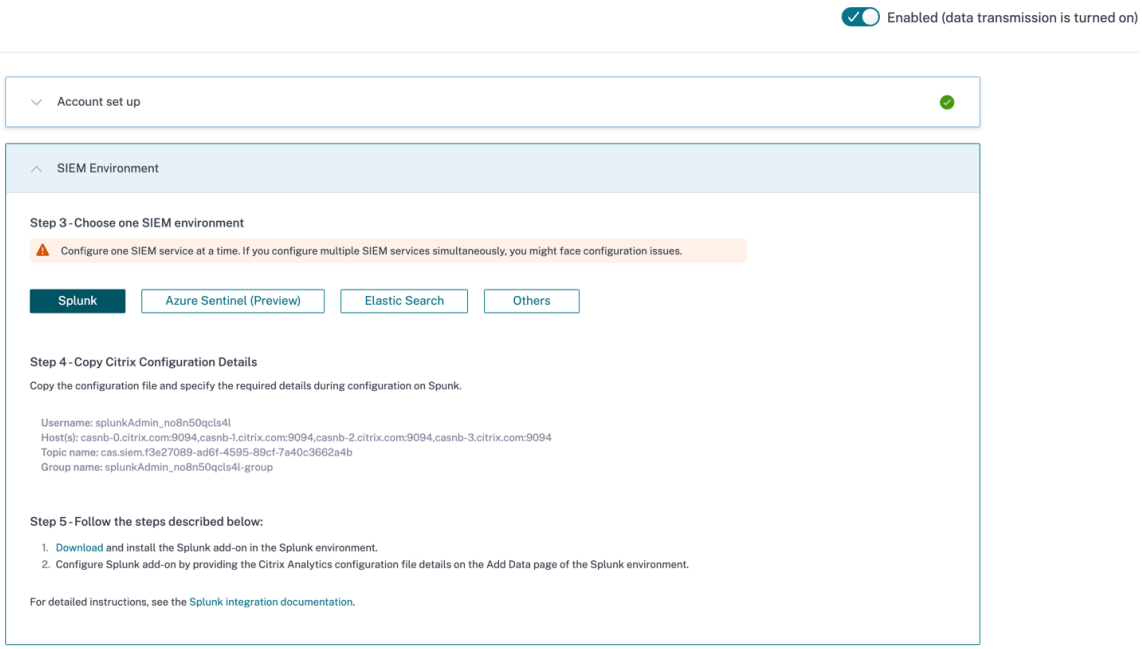
### Activar o desactivar la transmisión de datos

La transmisión de datos para la exportación de datos de Splunk desde Citrix Analytics está activada de forma predeterminada.

Para dejar de transmitir datos de Citrix Analytics for Security:

1. Ve a **Configuración > Exportaciones de datos**.
2. Apague el botón para desactivar la **transmisión de datos**.




Para habilitar de nuevo la transmisión de datos, active el botón.

## Complemento de Citrix Analytics para Splunk

Puede optar por instalar la aplicación complementaria en cualquiera de las siguientes plataformas:

- Splunk Enterprise (Heavy Forwarder)
- Nube de Splunk

## Complemento de Citrix Analytics para Splunk (local o empresarial)

### Versiones compatibles

Citrix Analytics for Security admite la integración de Splunk en los siguientes sistemas operativos:

- CentOS Linux 7 y versiones posteriores
- Debian GNU/Linux 10.0 y versiones posteriores
- Red Hat Enterprise Linux Server 7.0 y versiones posteriores
- Ubuntu 18.04 LTS y versiones posteriores

> **Nota**
>
> - Citrix recomienda utilizar la versión más reciente de los sistemas operativos anteriores o las versiones que aún reciben soporte de los proveedores respectivos.
> - Para los sistemas operativos del núcleo de Linux (64 bits), utilice una versión del núcleo

> compatible con Splunk. Para obtener más información, consulte la documentación de Splunk.

Puedes configurar nuestra integración con Splunk en la siguiente versión de Splunk: Splunk 8.1 (64 bits) y versiones posteriores.

#### Requisitos previos

- El **complemento Citrix Analytics para Splunk** se conecta a los siguientes puntos finales de Citrix Analytics for Security. Asegúrese de que los dispositivos de punto final se encuentren en la lista de permitidos de su red.

| Dispositivo de punto final | Región de los Estados Unidos | Región de la Unión Europea | Región Asia-Pacífico Sur |
|---|---|---|---|
| Intermediarios de Kafka | `casnb-0.citrix.com:9094`<br>`casnb-1.citrix.com:9094`<br>`casnb-2.citrix.com:9094`<br>`casnb-3.citrix.com:9094` | `casnb-eu-0.citrix.com:9094`<br>`casnb-eu-1.citrix.com:9094`<br>`casnb-eu-2.citrix.com:9094` | `casnb-aps-0.citrix.com:9094`<br>`casnb-aps-1.citrix.com:9094`<br>`casnb-aps-2.citrix.com:9094` |

> **Nota**
>
> Intente utilizar los nombres de los extremos, no las direcciones IP. Las direcciones IP públicas de los puntos finales pueden cambiar.

#### Descargue e instale el complemento Citrix Analytics para Splunk

Puedes elegir instalar el complemento mediante **Instalar la aplicación desde un archivo o desde** el entorno de
Splunk.

#### Instalar app desde un archivo

1. Vaya a Splunk base.
2. Descargue el complemento Citrix Analytics para el archivo Splunk.

3. En la página principal de Splunk Web, haga clic en el icono de engranaje situado junto a **Aplicaciones**.
4. Haga clic en **Instalar aplicación desde archivo**.
5. Localiza el archivo descargado y haga clic en **Subir**.

> **Notas**
>
> - Si tiene una versión anterior del complemento, seleccione **Actualizar aplicación** para sobrescribirla.
> - Si actualiza **Citrix Analytics Add-on for Splunk** desde una versión anterior a la 2.0.0, debe eliminar los siguientes archivos y carpetas ubicados en la carpeta */bin* de la carpeta de instalación del complemento y reiniciar el entorno de Splunk Forwarder o Splunk Standalone:
>
> ```
> - cd $SPLUNK_HOME$/etc/apps/TA_CTXS_AS/bin
> - rm -rf splunklib
> - rm -rf mac
> - rm -rf linux_x64
> - rm CARoot.pem
> - rm certificate.pem
> ```

6. Compruebe que la aplicación aparezca en la lista **Aplicaciones**.

#### Instala la aplicación desde Splunk

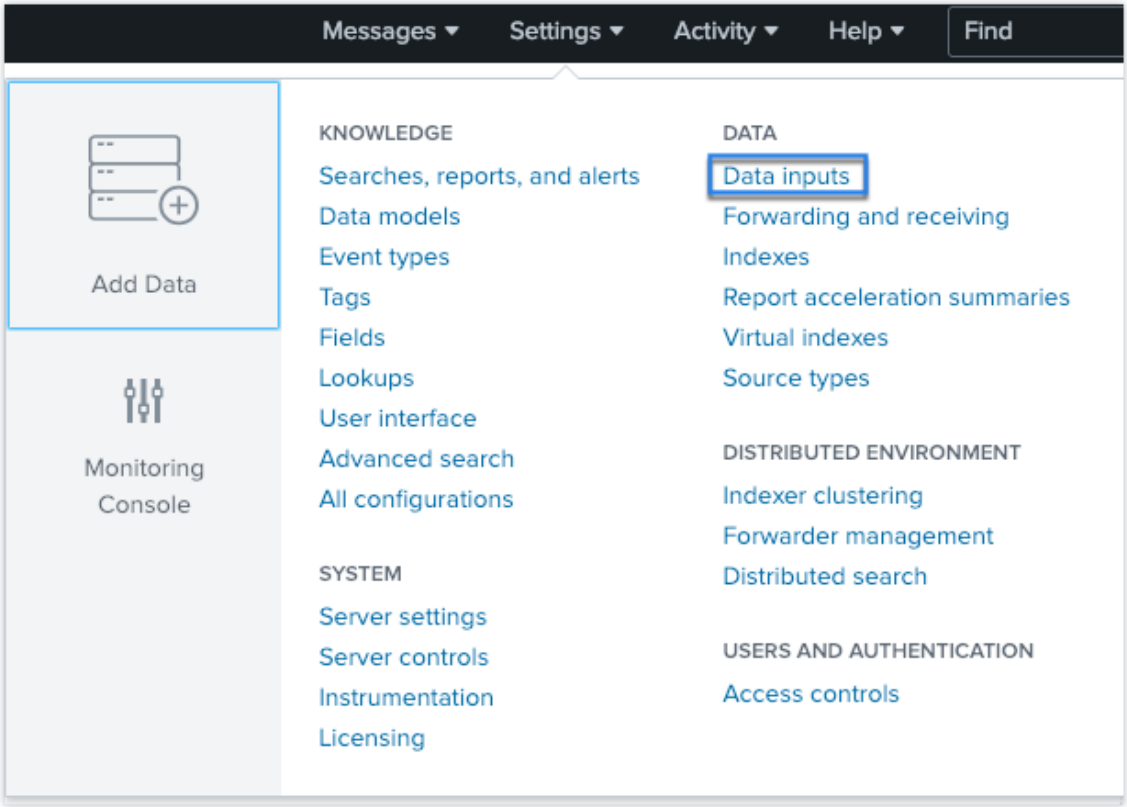
1. En la página de inicio de Splunk Web, haga clic en **+Buscar más aplicaciones**.
2. En la página Examinar más aplicaciones, busque **Complemento de Citrix Analytics para Splunk**.
3. Haga clic en **Instalar** junto a la aplicación.
4. Compruebe que la aplicación aparezca en la lista **Aplicaciones**.

#### Configurar el complemento Citrix Analytics para Splunk

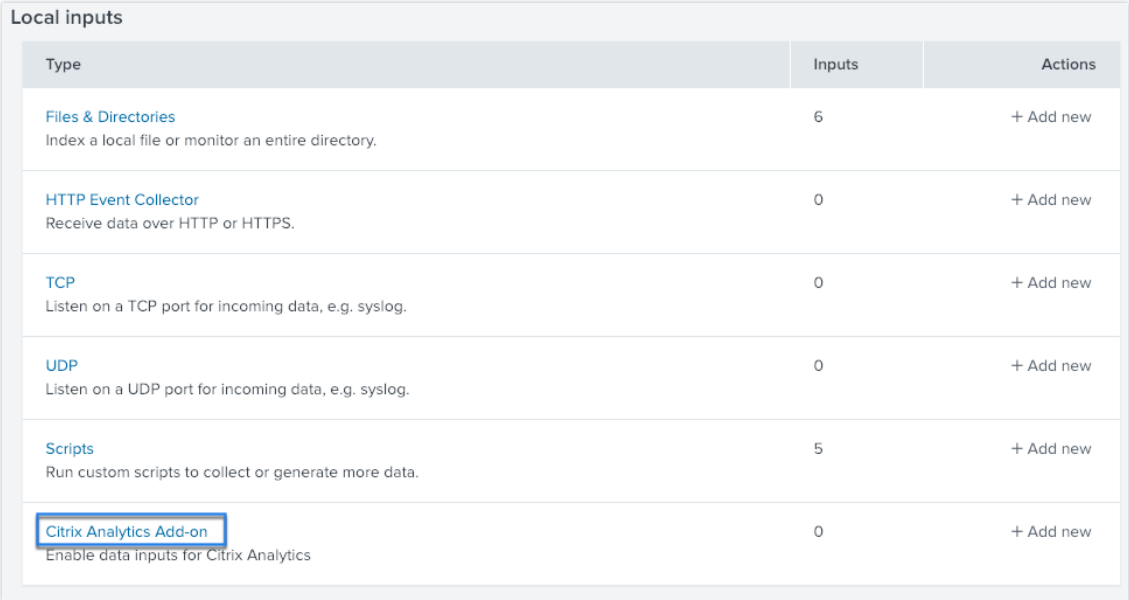
Configure el complemento Citrix Analytics para Splunk mediante los detalles de configuración proporcionados por Citrix Analytics for Security. Una vez configurado correctamente el complemento, Splunk comienza a consumir eventos de Citrix Analytics for Security.

1. En la página de inicio de Splunk, vaya a **Configuración** > **Entradas de datos**.

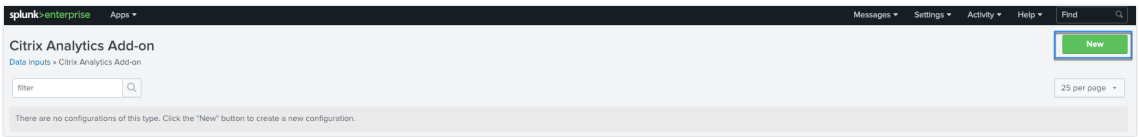



2. En la sección **Entradas locales**, haga clic en **Complemento de Citrix Analytics**.

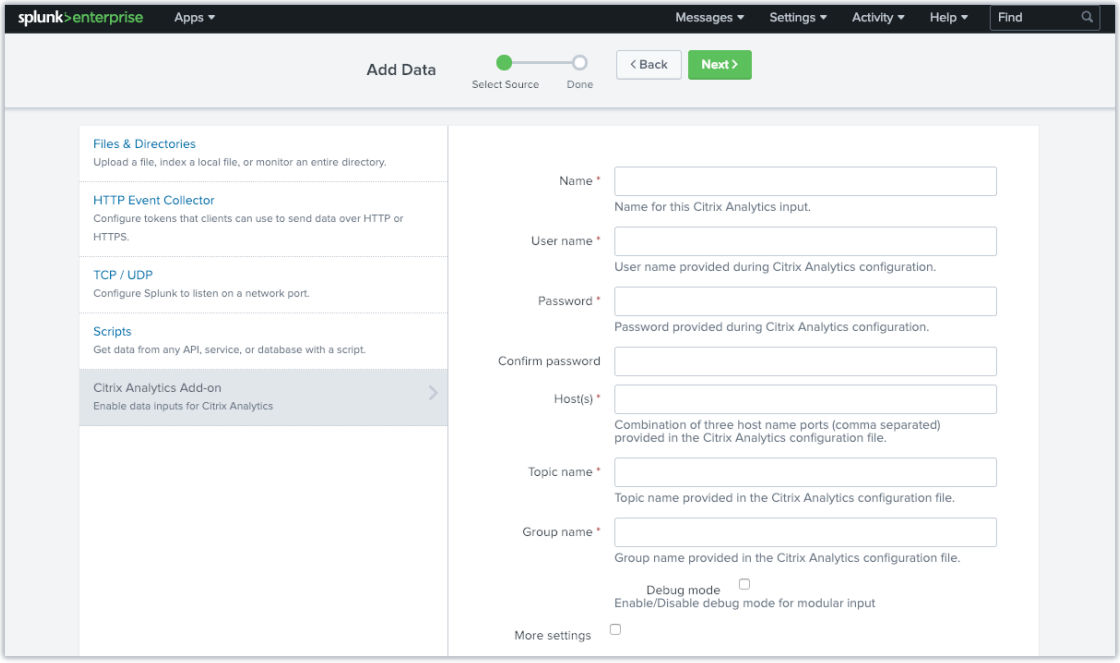



3. Haga clic en **New**.

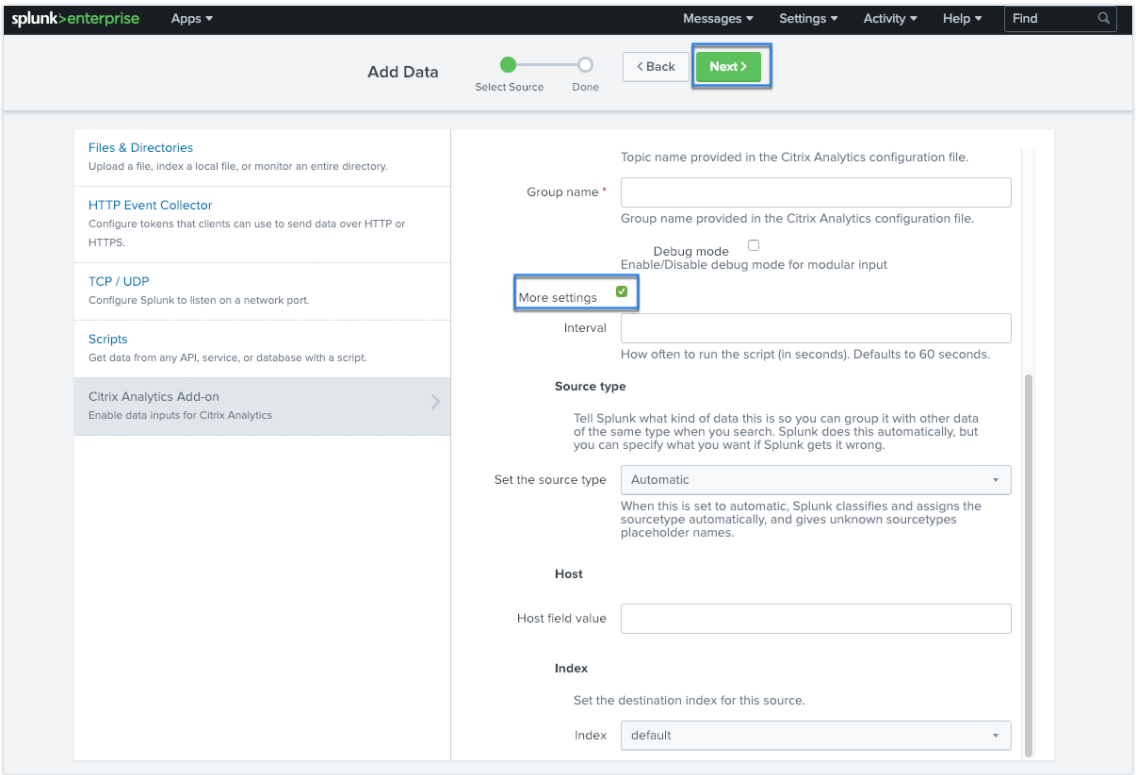



4. En la página **Agregar datos**, introduzca los detalles proporcionados en el archivo de configuración de Citrix Analytics.




5. Para personalizar la configuración predeterminada, haga clic en **Más ajustes** y configure la entrada de datos. Puede definir su propio índice de Splunk, nombre de host y tipo de fuente.




6. Haga clic en **Siguiente**. La entrada de datos de Citrix Analytics se crea y el complemento Citrix Analytics para Splunk se ha configurado correctamente.

## Complemento de Citrix Analytics para Splunk (nube)

Puedes configurar nuestra integración con Splunk en la siguiente versión de Splunk: Splunk 8.1 y versiones
posteriores.

### Requisitos previos

El complemento Citrix Analytics para Splunk se conecta a las siguientes direcciones IP y puertos de salida para conectarse a Citrix Analytics for Security. Asegúrese de que las siguientes direcciones IP y puertos de salida (según la región de Citrix Cloud) estén en la lista de direcciones permitidas de su red. Para configurar estas direcciones IP y puertos de salida, consulte la sección **Agregar direcciones IP y puertos de salida de Citrix Analytics a la lista de permitidos de Splunk Cloud mediante el servicio de configuración de administración (ACS)**.

| Región de los Estados Unidos | IP | Puerto de salida | Región de la Unión Europea | IP | Puerto de salida | Región Asia-Pacífico Sur | IP | Puerto de salida |
|---|---|---|---|---|---|---|---|---|
| casnb-0 cit-rix.com | 20.242.21.84 | 9094 | casnb-eu-0 cit-rix.com | 20.229.150.41 | 9094 | casnb-aps-0 cit-rix.com | 20.211.0.214 | 9094 |
| casnb-1.citrix.com | 20.98.232.69 | 9094 | casnb-eu-1.citrix.com | 20.107.97.59 | 9094 | casnb-aps-1 cit-rix.com | 20.211.38.102 | 9094 |
| casnb-2.citrix.com | 20.242.21.108 | 9094 | casnb-eu-2.citrix.com | 51.124.223.162 | 9094 | casnb-aps-2 cit-rix.com | 20.211.36.180 | 9094 |
| casnb-3.citrix.com | 20.242.57.14 | 9094 | | | | | | |

> **Nota:**
>
> Estas direcciones IP están sujetas a rotación. Asegúrese de mantener su lista de direcciones IP permitidas actualizada con las IP
> más recientes, tal como se muestra arriba.

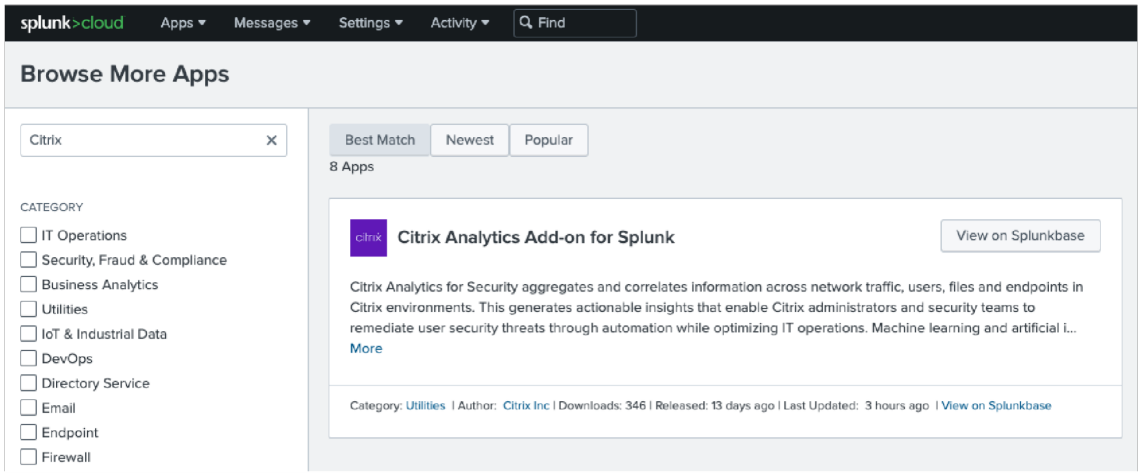
**Agregue las direcciones IP y los puertos salientes de Citrix Analytics a la lista de permitidos de Splunk Cloud mediante el Servicio de configuración de administración (ACS)**

1. Según la región de Citrix Cloud, compruebe las direcciones IP que deben agregarse a la lista de direcciones permitidas.
2. Habilite el servicio de configuración de administración (ACS) en la plataforma Splunk Cloud.
3. Cree un token para la lista de permitidos mediante una cuenta local con privilegios de administrador.
4. Ejecute los comandos cURL GET y POST para agregar subredes a la lista de permitidos en los puertos respectivos y validar si se agregaron correctamente.
5. Ejecute los comandos cURL GET y POST para agregar los puertos de salida a la lista de permitidos y validarlos si se agregaron correctamente.

### Descargue e instale el complemento Citrix Analytics para Splunk

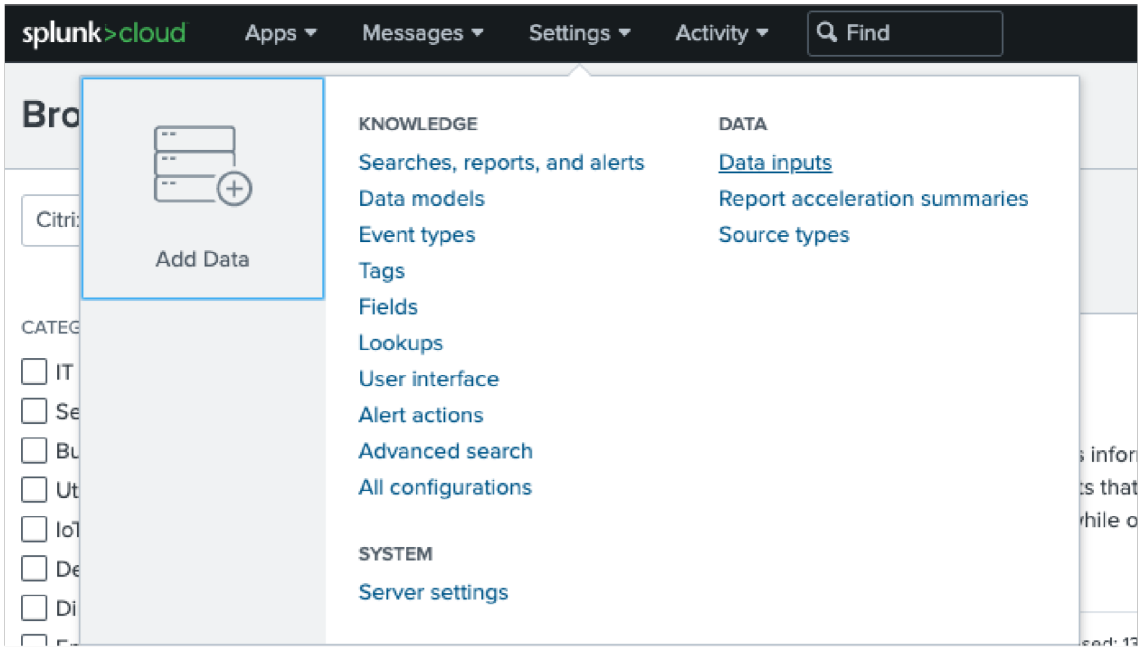
1. Vaya a **Aplicaciones > Buscar más aplicaciones > Busque el complemento Citrix Analytics para Splunk**.




2. Instala la aplicación.
3. Compruebe que la aplicación aparezca en la lista Aplicaciones.

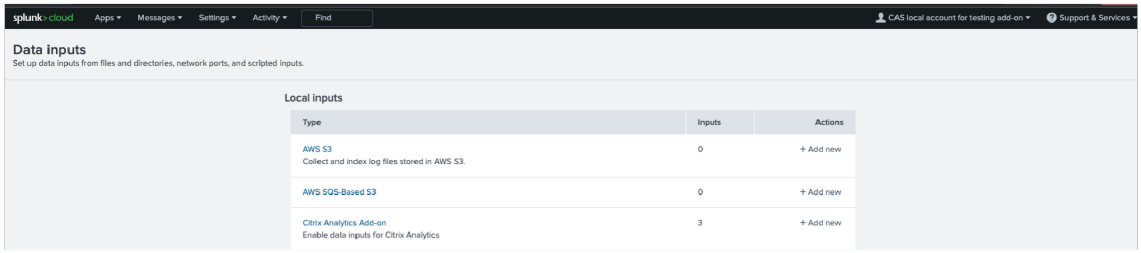
### Configurar el complemento Citrix Analytics para Splunk

1. Vaya a **Configuración > Entradas de datos > Complemento de Citrix Analytics**.

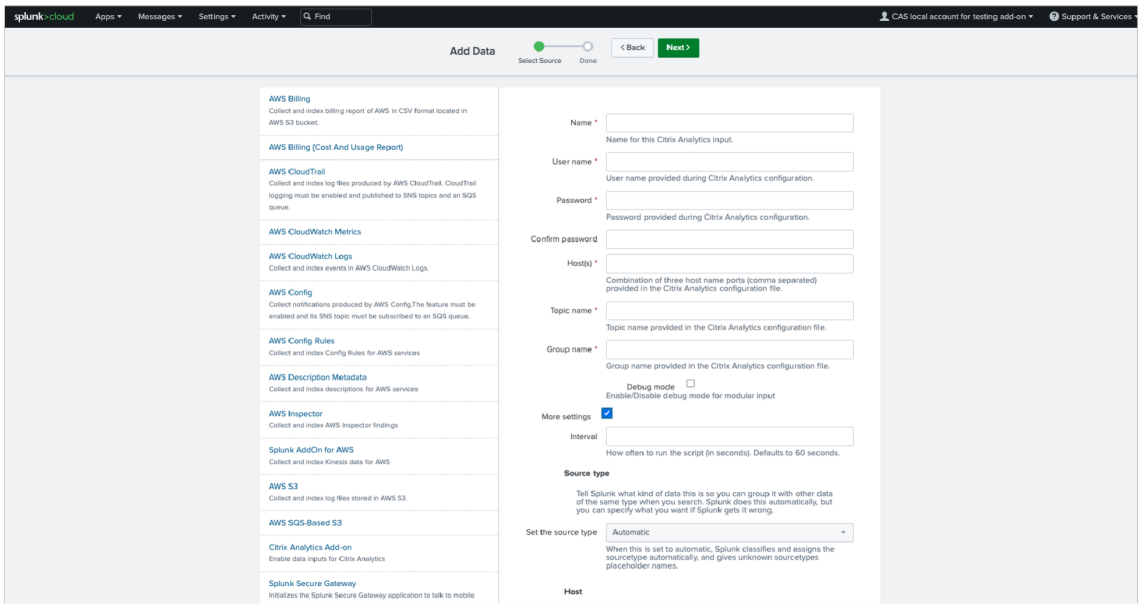


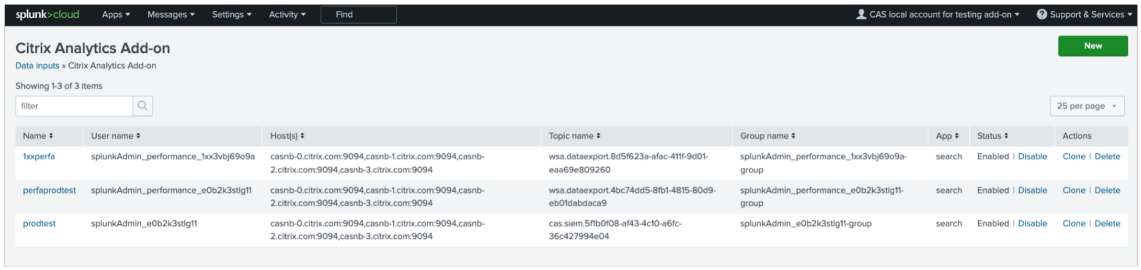
| | |
|---|---|
| Agregue la entrada: integración de Splunk | Citrix Analytics para seguridad. Haga clic en **Agregar nuevo**. |

2. 


3. Configure la entrada de datos introduciendo los detalles configurados en la página **Exportaciones de datos de Citrix Analytics**.




4. Compruebe si la entrada de datos se ha agregado correctamente.



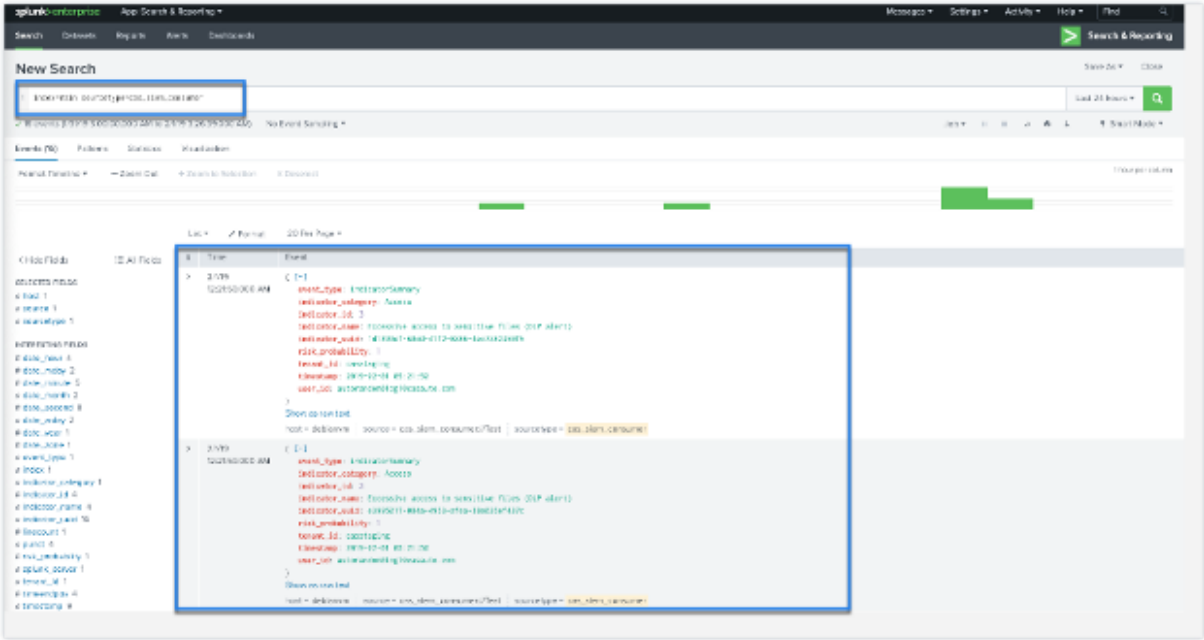

### Cómo consumir eventos en su entorno de Splunk

Después de configurar el complemento, Splunk comienza a recuperar información sobre riesgos de Citrix Analytics for Security. Puede comenzar a buscar los eventos de su organización en el cabezal de

búsqueda Splunk basado en la entrada de datos configurada.

Los resultados de la búsqueda se muestran en el siguiente formato:




Un ejemplo de salida:

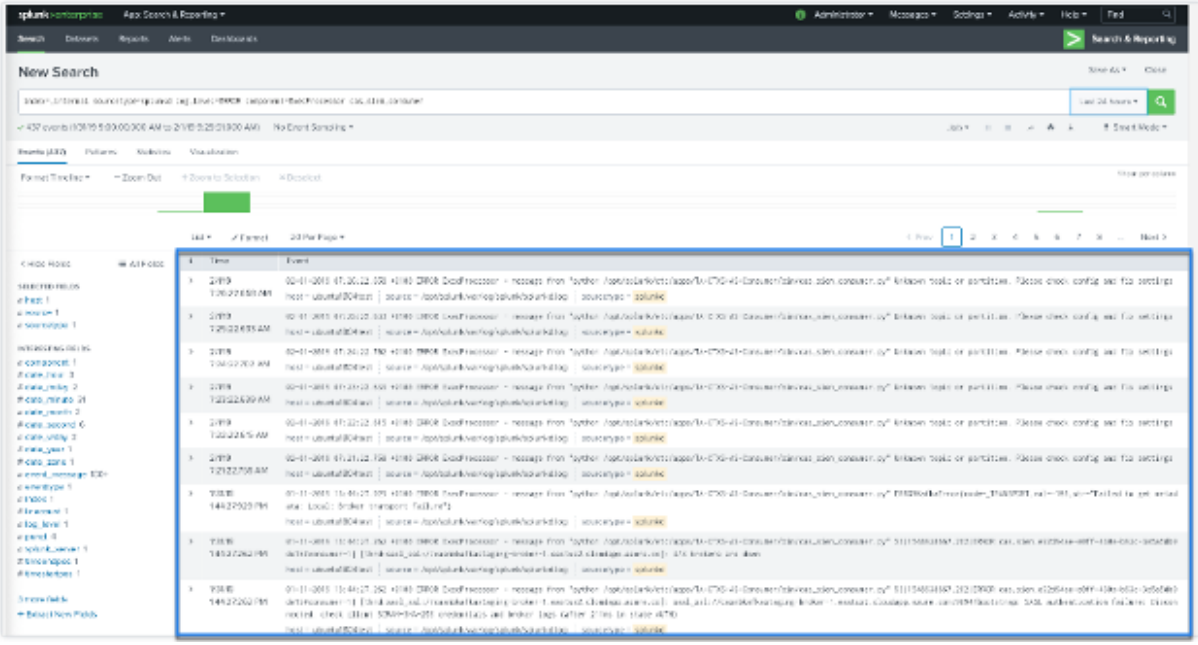
```
{"event_type": "indicatorSummary", "indicator_category": "Access",
"indicator_id": 200, "indicator_name": "Jailbroken / Rooted Device
Detected", "indicator_uuid": "1b97c3be-0000-000-0000-0000000000",
"risk_probability": 1.0, "tenant_id": "notcloud", "timestamp": "2017-11-16
23:59:59", "user_id": "testuser00001"}
```

Para buscar y depurar incidencias con el complemento, utilice la siguiente consulta de búsqueda:

```
index=_internal sourcetype=splunkd log_level=ERROR component=ExecProcessor
cas_siem_consumer
```

Los resultados se muestran en el siguiente formato:




Para obtener más información sobre el formato de datos, consulte Formato de datos de Citrix Analytics para SIEM.

## Solución de problemas del complemento Citrix Analytics para Splunk

Si no ve ningún dato en los paneles de Splunk o si encuentra problemas al configurar el complemento Citrix Analytics para Splunk, lleve a cabo los pasos de depuración para solucionar el problema. Para obtener más información, consulte Problemas de configuración con el complemento Citrix Analytics para Splunk.

> **Nota**
>
> Contacte con CAS-PM-Ext@cloud.com para solicitar ayuda para la integración de Splunk, la exportación de datos a Splunk o para enviar comentarios.

## Aplicación Citrix Analytics para Splunk

> **Nota**
>
> Esta aplicación está en versión preliminar.

La aplicación Citrix Analytics para Splunk permite a los administradores de Splunk Enterprise ver los datos de usuario recopilados de Citrix Analytics for Security en forma de paneles útiles y útiles en Splunk. Con estos paneles, obtendrá una visión detallada del comportamiento de riesgo de los usuarios en su organización y tomará las medidas oportunas para mitigar cualquier amenaza interna. También puede correlacionar los datos recopilados de Citrix Analytics for Security con otros orígenes de

datos configurados en su Splunk. Esta correlación le proporciona visibilidad de las actividades de riesgo de los usuarios desde múltiples fuentes y toma medidas para proteger su entorno de TI.

### Versión de Splunk compatible

La aplicación Citrix Analytics para Splunk se ejecuta en las siguientes versiones de Splunk:

- Splunk 9.0 de 64 bits
- Splunk 8.2 de 64 bits
- Splunk 8.1 de 64 bits

### Requisitos previos para la aplicación Citrix Analytics para Splunk

- Instale el complemento Citrix Analytics para Splunk.
- Asegúrese de que se cumplen los requisitos previos mencionados para el complemento Citrix Analytics para Splunk.
- Asegúrese de que los datos fluyan de Citrix Analytics for Security a Splunk.

### Instalación y configuración

**¿Dónde instalar la aplicación?** Cabezal de búsqueda Splunk

**¿Cómo instalar y configurar la aplicación?** Puede instalar la aplicación Citrix Analytics para Splunk descargándola de Splunk o instalándola desde Splunk.

### Instalar app desde un archivo

1. Vaya a Splunk base.
2. Descargue el archivo de la aplicación Citrix Analytics para Splunk.
3. En la página principal de Splunk Web, haga clic en el icono de engranaje situado junto a **Aplicaciones**.
4. Haga clic en **Instalar aplicación desde archivo**.
5. Localiza el archivo descargado y haga clic en **Subir**.

   > **Nota**

> Si tiene una versión anterior de la aplicación, seleccione **Actualizar aplicación** para sobrescribirla.

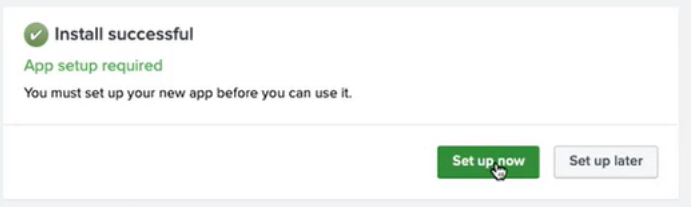
6. Compruebe que la aplicación aparezca en la lista **Aplicaciones**.

### Instala la aplicación desde Splunk

1. En la página de inicio de Splunk Web, haga clic en **+Buscar más aplicaciones**.
2. En la página Examinar más aplicaciones, busque la **aplicación Citrix Analytics para Splunk**.
3. Haga clic en **Instalar** junto a la aplicación.

### Configure el índice y el tipo de origen para correlacionar los datos

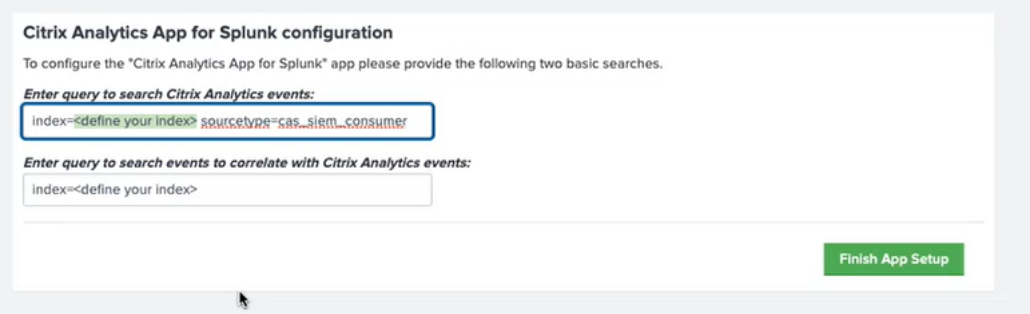
1. Después de instalar la aplicación, haga clic en **Configurar ahora**.




2. Introduzca las siguientes consultas:
   - Tipo de índice y origen donde se almacenan los datos de Citrix Analytics for Security.

     > **Nota**
     >
     > Estos valores de consulta deben ser los mismos que los especificados en el complemento Citrix Analytics para Splunk. Para obtener más información, consulte Configurar el complemento Citrix Analytics para Splunk.

   - Índice del que quiere correlacionar los datos con Citrix Analytics for Security.




3. Haga clic en **Finalizar configuración de la aplicación** para completar la configuración.

Una vez configurada y configurada la aplicación Citrix Analytics para Splunk, utilice los paneles de control de Citrix Analytics para ver los eventos de usuario en su Splunk.

Para obtener más información sobre la integración de Splunk, consulte los siguientes enlaces:

- Citrix Analytics Integration with Splunk
- The Citrix Analytics app for Splunk, now in Splunkbase

## Arquitectura Splunk con aplicación complementaria de Citrix Analytics

February 13, 2023

Splunk sigue una arquitectura que contiene los tres niveles siguientes:

- Colección
- Indexación
- Buscando

Splunk admite una amplia gama de mecanismos de recopilación de datos que ayudan a introducir datos en Splunk con facilidad, de modo que puedan indexarse y estar disponibles para la búsqueda. Este nivel no es más que su transportista pesado o transportista universal.

Debe instalar la aplicación complementaria en la capa de reenvío pesado en lugar de en la capa de reenvío universal. Porque, con pocas excepciones en el caso de datos bien estructurados (como json, csv, tsv), el reenviador universal no analiza las fuentes de registro en eventos, por lo que no puede realizar ninguna acción que requiera comprender el formato de los registros.

También incluye una versión reducida de Python, lo que lo hace incompatible con cualquier aplicación de entrada modular que requiera una pila completa de Splunk para funcionar. El reenviador pesado no es más que tu nivel de colección.

La diferencia clave entre un reenviador universal y un reenviador pesado es que el reenviador pesado contiene toda la canalización de análisis y realiza las mismas funciones que realiza un indexador sin escribir ni indexar eventos en el disco. Esto permite al transportista pesado comprender eventos individuales y actuar sobre ellos, como enmascarar datos, filtrar y enrutar en función de los datos de eventos. Como la aplicación complementaria cuenta con una instalación completa de Splunk Enterprise, puede alojar entradas modulares que requieren una pila completa de Python para una recopilación de datos adecuada, o actuar como punto final para el recopilador de eventos HTTP (HEC) de Splunk.

Una vez recopilados los datos, se indexan o procesan y almacenan de manera que se puedan buscar.

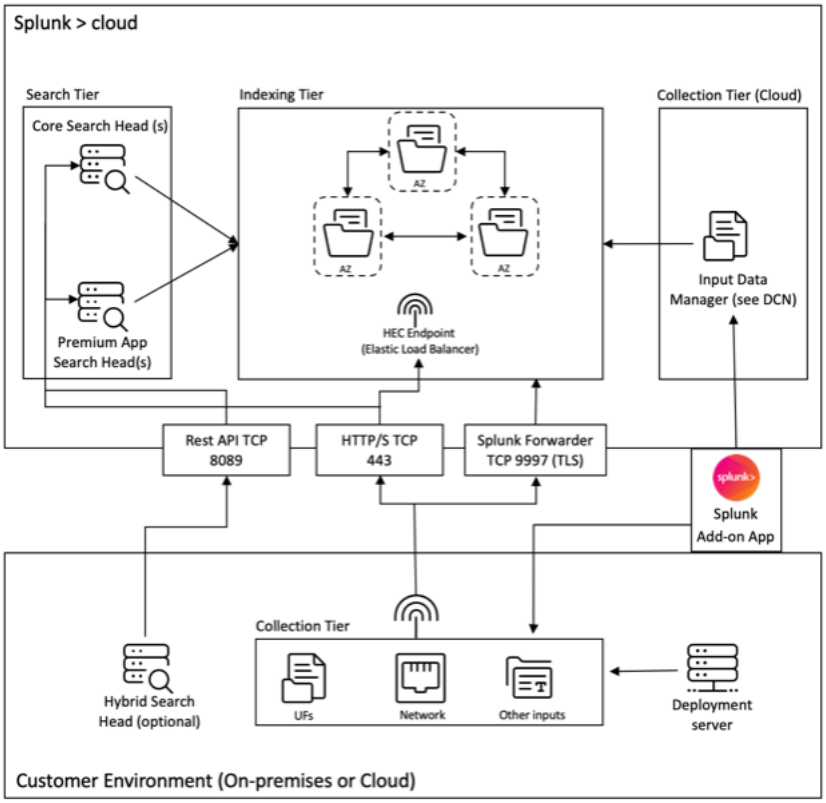
 

La forma principal de que los clientes exploren sus datos es mediante la búsqueda. Una búsqueda puede guardarse como un informe y utilizarse para alimentar los paneles del panel de control. Las búsquedas son la forma de extraer información de sus datos.

En general, la aplicación complementaria de Splunk se implementa en el nivel de colección (a nivel empresarial de Splunk), mientras que nuestra aplicación de paneles se implementa en la capa de búsqueda (a nivel de Splunk Cloud). Con una configuración local sencilla, puedes tener estos tres niveles en un único host de Splunk (lo que se conoce como implementación de un solo servidor).

El nivel de colección es una forma mucho mejor de utilizar la aplicación complementaria de Splunk. Hay dos formas de instalar la aplicación complementaria. Puede instalarlo en el nivel de recopilación en el entorno del cliente o puede instalarlo en el administrador de datos de entradas de la **instancia de Splunk Cloud**.

Consulte el siguiente diagrama para entender la arquitectura de implementación de Splunk con nuestra aplicación complementaria:




El administrador de datos de entradas (IDM) que se muestra en el diagrama mencionado anteriormente es la implementación gestionada por Splunk Cloud de un nodo de recopilación de datos (DCN) que solo admite entradas modulares y programadas. Para necesidades de recopilación de datos más allá de eso, puede implementar y administrar una DCN en su entorno utilizando un reenviador pesado de Splunk.

Splunk permite recopilar, indexar y buscar datos de varias fuentes. Una forma de recopilar datos es

a través de las API, que permiten a Splunk acceder a los datos almacenados en otros sistemas o aplicaciones. Estas API pueden incluir REST, servicios web, JMS y/o JDBC como mecanismo de consulta. Splunk y cualquier desarrollador externo ofrecen una gama de aplicaciones que permiten las interacciones de la API a través del marco de entrada modular de Splunk. Estas aplicaciones suelen requerir una instalación completa del software empresarial de Splunk para funcionar correctamente.

Para facilitar la recopilación de datos a través de las API, es habitual implementar un reenviador pesado como DCN. Los transportistas pesados son agentes más poderosos que los transportistas universales, ya que contienen todo el proceso de análisis y pueden comprender eventos individuales y actuar en función de ellos. Esto les permite recopilar datos a través de las API y procesarlos antes de enviarlos a una instancia de Splunk para su indexación.

Para obtener más información sobre la arquitectura de alto nivel de una implementación de Splunk Cloud, consulte Arquitecturas validadas de Splunk.

## Paneles de Citrix Analytics para Splunk

December 7, 2023

> **Nota**
>
> :**Citrix**Content Collaboration y ShareFile han llegado al final de su vida útil y ya no están disponibles para los usuarios.
>
> Esta función se encuentra en Tech Preview.

### Requisito previo

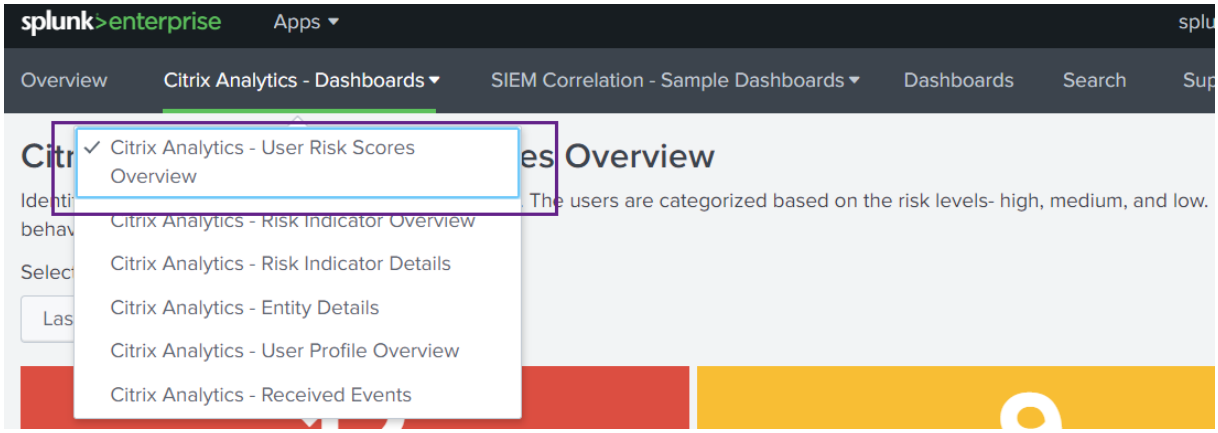
Para utilizar los siguientes paneles de control de Citrix Analytics, asegúrese de que ya ha configurado y configurado la aplicación Citrix Analytics para Splunk.

### Descripción general de la puntuación de riesgo

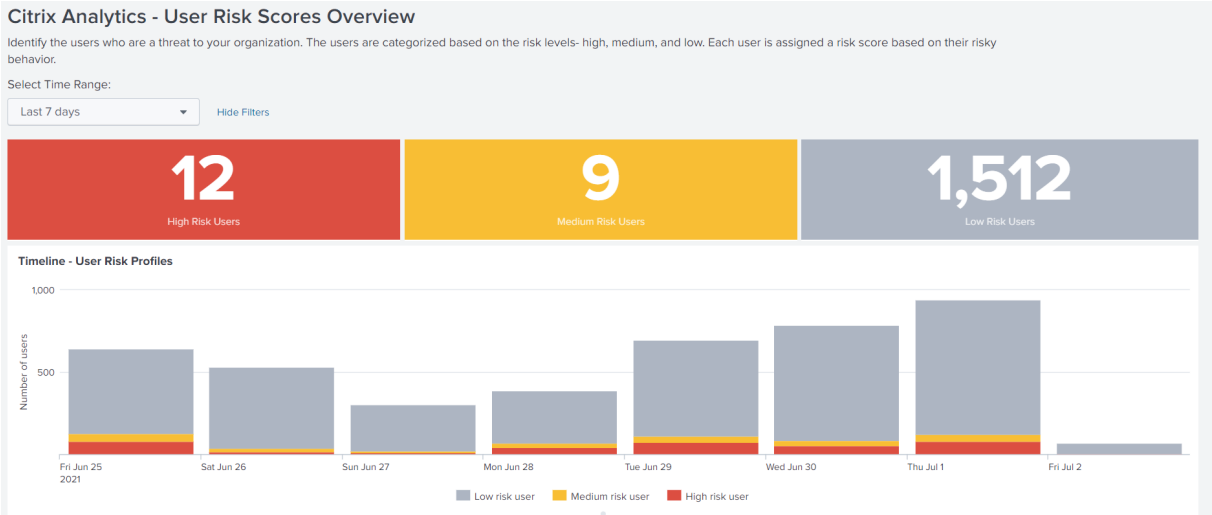
Este panel proporciona una vista consolidada de los usuarios de riesgo de su organización. Los usuarios se clasifican según los niveles de riesgo: alto, medio y bajo. Los niveles de riesgo se basan en las anomalías de las actividades de los usuarios y, en consecuencia, se asigna una puntuación de riesgo. Para obtener más información sobre los tipos de usuarios de riesgo, consulte el panel Usuarios.

Para ver este panel, haga clic en **Citrix Analytics- Paneles > Citrix Analytics- Descripción general de las puntuaciones de riesgo del usuario**.




Seleccione un intervalo de tiempo preestablecido o un intervalo de tiempo personalizado para ver la cronología de los usuarios con riesgos y sus detalles.




La tabla Usuarios con riesgos proporciona la siguiente información:

- **Usuario**: indica el nombre de usuario. Haga clic en un nombre de usuario para ver los detalles sobre el comportamiento de riesgo del usuario en el panel Citrix Analytics - Detalles de entidad.
- **Riesgos de dispositivo de punto finales comprometidos detectados**: indica el número de indicadores de riesgo activados por el usuario que pertenece a la categoría de riesgo de dispositivo de punto finales comprometidos.
- **Riesgos detectados para usuarios comprometidos**: indica el número de indicadores de riesgo activados por el usuario que pertenece a la categoría de riesgo de usuarios comprometidos.
- **Riesgos de exfiltración de datos detectados**: indica el número de indicadores de riesgo activados por el usuario que pertenece a la categoría de riesgo de exfiltración de datos.
- **Riesgos de amenazas internas detectados**: indica el número de indicadores de riesgo activados por el usuario que pertenecen a la categoría de riesgo de amenazas internas.

- **Puntuación de riesgo**: indica la puntuación de riesgo del usuario.

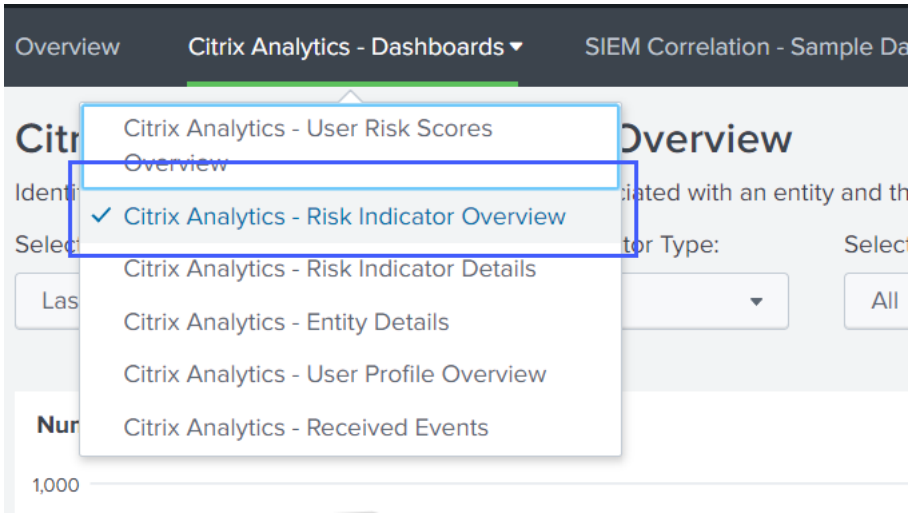
También puede buscar un usuario por su nombre de usuario y obtener los detalles necesarios.

Para obtener más información, consulte las categorías de riesgo.


## Resumen de indicadores de riesgo

El panel proporciona una vista consolidada de los indicadores de riesgo activados por los usuarios de su organización.

Para ver el panel, haga clic en **Citrix Analytics- Paneles > Citrix Analytics- Descripción general del indicador de riesgo**.



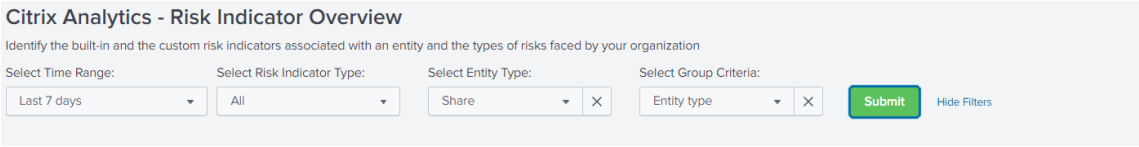

### Seleccione la categoría para ver el informe

Busque los indicadores de riesgo seleccionando una o varias categorías:

- **Intervalo de tiempo**: seleccione un intervalo de tiempo preestablecido o un intervalo de tiempo personalizado para ver los indicadores de riesgo desencadenados para ese período.

- **Tipo de indicador de riesgo**: Seleccione el tipo de indicador de riesgo: integrado o personalizado.
- **Tipo de entidad**: seleccione un usuario para ver los indicadores de riesgo asociados.
- **Grupo**: seleccione un criterio para agrupar los eventos de usuario por origen de datos, categoría de indicador, nombre de indicador, tipo de indicador o tipo de entidad y ver los indicadores de riesgo asociados.

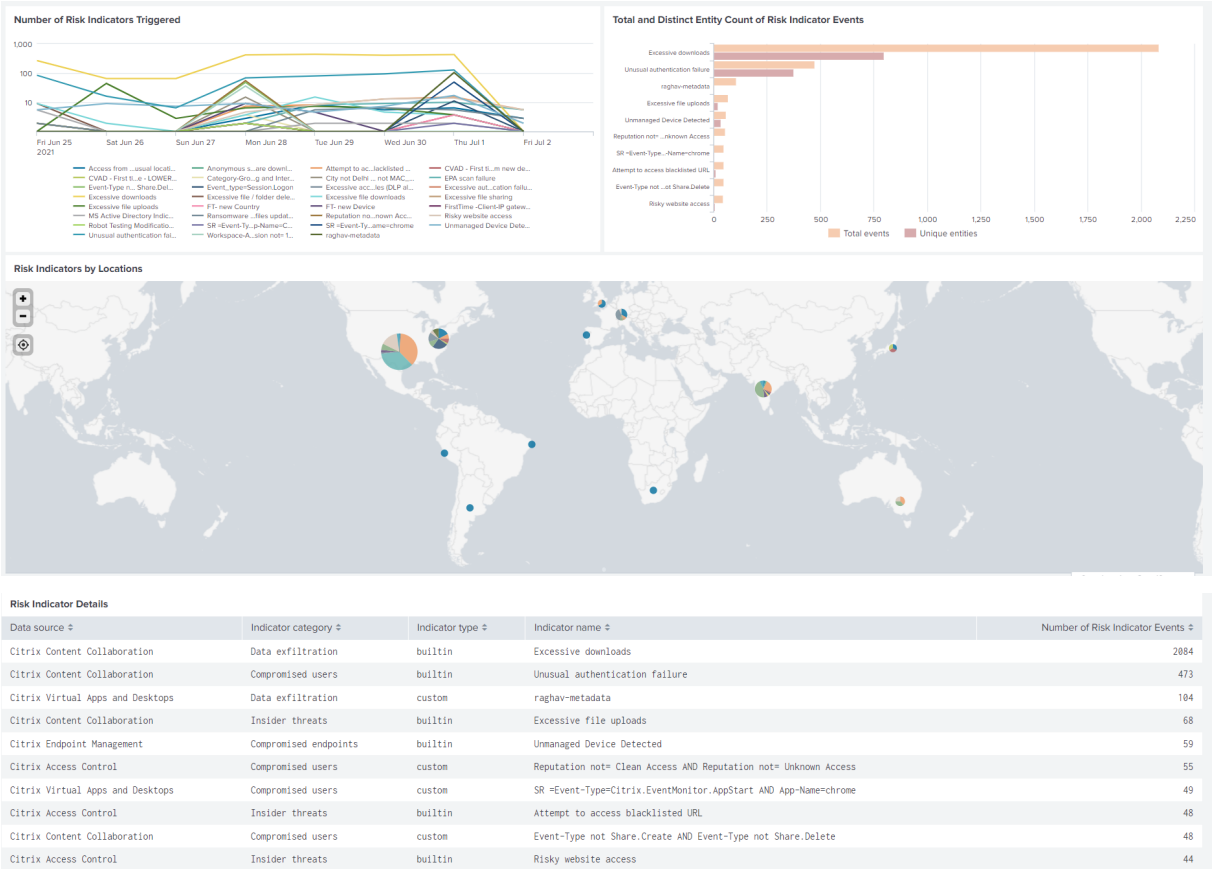



### Ver informe

Utilice los siguientes informes para ver detalles sobre los indicadores de riesgo seleccionando una o varias categorías:

- **Número de indicadores de riesgo activados**: muestra el número de indicadores de riesgo activados para el período seleccionado. Utilice este informe para identificar el patrón y las áreas de las actividades de riesgo. Además, identifique las actividades más riesgosas de su organización.
- **Recuento total y distinto de entidades de eventos del indicador de riesgo**: muestra el total de eventos y los eventos únicos correspondientes a un indicador de riesgo. Utilice este informe para identificar las ocurrencias de cada indicador de riesgo y los principales indicadores de riesgo de su organización. También puede identificar cuántos usuarios únicos activaron un indicador de riesgo en particular y comprobar si el indicador de riesgo lo activa un grupo de usuarios más grande o más pequeño.
- **Indicadores de riesgo por ubicaciones**: muestra el número de indicadores de riesgo activados por los usuarios en todas las ubicaciones. Utilice este informe para identificar las ubicaciones que muestran actividades más riesgosas y comprobar si las ubicaciones están fuera del área de operación de su organización.
- **Detalles del indicador de riesgo**: muestra los detalles del indicador de riesgo, como la fuente de datos asociada, la categoría del indicador, el tipo de indicador y el número de incidencias.

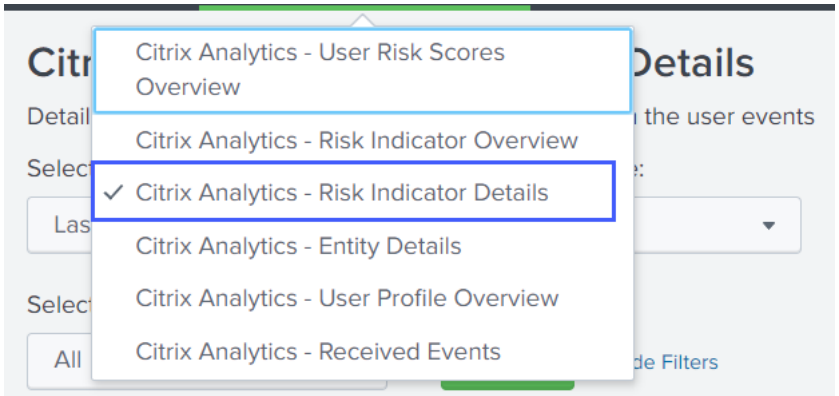



| Data source | Indicator category | Indicator type | Indicator name | Number of Risk Indicator Events |
|---|---|---|---|---|
| Citrix Content Collaboration | Data exfiltration | builtin | Excessive downloads | 2084 |
| Citrix Content Collaboration | Compromised users | builtin | Unusual authentication failure | 473 |
| Citrix Virtual Apps and Desktops | Data exfiltration | custom | raghav-metadata | 104 |
| Citrix Content Collaboration | Insider threats | builtin | Excessive file uploads | 68 |
| Citrix Endpoint Management | Compromised endpoints | builtin | Unmanaged Device Detected | 59 |
| Citrix Access Control | Compromised users | custom | Reputation not= Clean Access AND Reputation not= Unknown Access | 55 |
| Citrix Virtual Apps and Desktops | Compromised users | custom | SR =Event-Type=Citrix.EventMonitor.AppStart AND App-Name=chrome | 49 |
| Citrix Access Control | Insider threats | builtin | Attempt to access blacklisted URL | 48 |
| Citrix Content Collaboration | Compromised users | custom | Event-Type not Share.Create AND Event-Type not Share.Delete | 48 |
| Citrix Access Control | Insider threats | builtin | Risky website access | 44 |

## Detalles del indicador de riesgo

El panel de control proporciona información detallada sobre los indicadores de riesgo integrados y personalizados activados por los usuarios. Para obtener más información, consulte Indicadores de riesgo de usuario de Citrix e Indicadoresde riesgo personalizados.

Para ver el panel, haga clic en **Citrix Analytics- Paneles > Citrix Analytics- Detalles del indicador de riesgo**.



#### Seleccione la categoría para ver los informes

Consulte los detalles de los indicadores de riesgo seleccionando una o varias categorías:

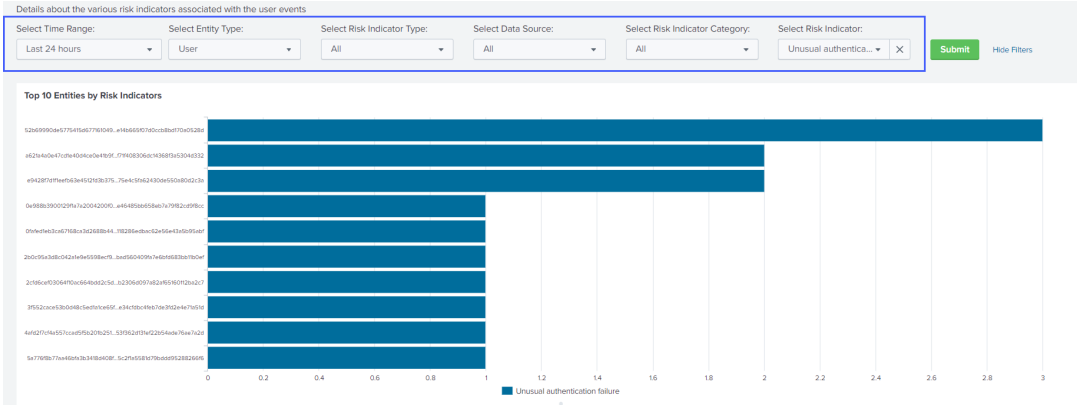
- **Intervalo de tiempo**: seleccione un intervalo de tiempo preestablecido o un intervalo de tiempo personalizado para ver los detalles de los indicadores de riesgo desencadenados para ese período.
- **Tipo de entidad**: seleccione un usuario para ver los detalles de los indicadores de riesgo asociados.
- **Tipo de indicador de riesgo**: seleccione el tipo de indicador de riesgo integrado o personalizado para ver sus detalles.
- **Origen de datos**: seleccione la fuente de datos para ver los detalles de los indicadores de riesgo asociados.
- **Categoría de indicador de riesgo**: seleccione la categoría de riesgo para ver los detalles de los indicadores de riesgo asociados.
- **Indicador de riesgo**: seleccione el indicador de riesgo para ver sus detalles.

#### Ver los informes

Por ejemplo, en la lista Seleccionar indicador de riesgo, seleccione **Error de autenticación inusual (Citrix Content Collaboration)**, haga clic en **Enviar**y consulte la siguiente información:

- Los 10 principales usuarios asociados al indicador de riesgo
- Detalles sobre el indicador de riesgo como
  - Fecha y hora del desencadenador
  - Origen de datos asociado
  - Categoría de riesgo asociada
  - ID de entidad asociada y tipo de entidad de usuario
  - Gravedad del riesgo alta, media o baja
  - Probabilidad de riesgo del evento de usuario
  - Identidad única del indicador de riesgo (UUID)




En **10 entidades principales por indicadores de riesgo**, haga clic en una entidad para ver sus detalles en el panel **Citrix Analytics- Detalles de entidad** .

**Risk Indicator Details**

| Date and Time | Data Source | Risk Indicator Category | Risk Indicator Name | Entity ID | Entity Type | Severity | Risk Probability | Risk Indicator UUID |
|---|---|---|---|---|---|---|---|---|
| 2021-07-01T21:29:59Z | Citrix Content Collaboration | Compromised users | Unusual authentication failure | 6e130e9b07e28bea778eef5e21809150ce7bb05da8d821fbcff235b962796586 | user | medium | 1.0 | babe4ada-34cd-5266-bc36-1142a4e9278c |
| 2021-07-01T21:29:59Z | Citrix Content Collaboration | Compromised users | Unusual authentication failure | 102854bc92af241d303ab4c3cc62ec969a0c64c6998757032933728b1d10a848 | user | medium | 1.0 | f594a2bf-8121-5231-ab32-a2e3735ee6d5 |
| 2021-07-01T21:29:59Z | Citrix Content Collaboration | Compromised users | Unusual authentication failure | dc61f0b0a9218cb5f1925778069c112a4236d40e73f2dd8170e89eeabe717714 | user | medium | 1.0 | 6720f113-dc3e-5986-967e-26a748b0d00b |

Haga clic en cada fila de la tabla **Detalles del indicador de riesgo** para ver el resumen del evento, los detalles del evento y los eventos sin procesar del indicador de riesgo seleccionado.

En la sección **Resumen de eventos del indicador de riesgo**, haga clic en el **enlace de la interfaz de usuario de Citrix Analytics** para ir directamente a la cronología del usuario en Citrix Analytics for Security desde su Splunk. En el cronograma del usuario, vea el indicador de riesgo, los eventos asociados y cualquier acción aplicada al usuario.

Para obtener más información sobre el resumen de eventos y los detalles de los eventos, consulte Formato de datos de Citrix Analytics para SIEM.

**Risk Indicator Event Summary**

- Indicator UUID: babe4ada-34cd-5266-bc36-1142a4e9278c
- Data source: Citrix Content Collaboration
- Risk indicator category: Compromised users
- Risk indicator name: Unusual authentication failure
- Citrix Analytics UI link: https://analytics-staging.cloud.com/user/eyJoaWdob...oic2lIbSJ9

**Risk Indicator Event Details**

| Date and Time | city | client_ip | country | device_id | entity_id | entity_type | indicator_vector.id | indicator_vector.name |
|---|---|---|---|---|---|---|---|---|
| 2021-07-01T20:52:21Z | NA | 7fcdef4547a054315fe9a9614e012fa77b2ec1d11885e5d59d29eb9fb67fd08b | NA | NA | 6e130e9b07e28bea778eef5e21809150ce7bb05da8d821fbcff235b962796586 | user | 3 | Logon-Failure-Based Risk Indicators |

ℹ Click each value in a row to correlate it with other Splunk events

3m ago

**Raw Events**

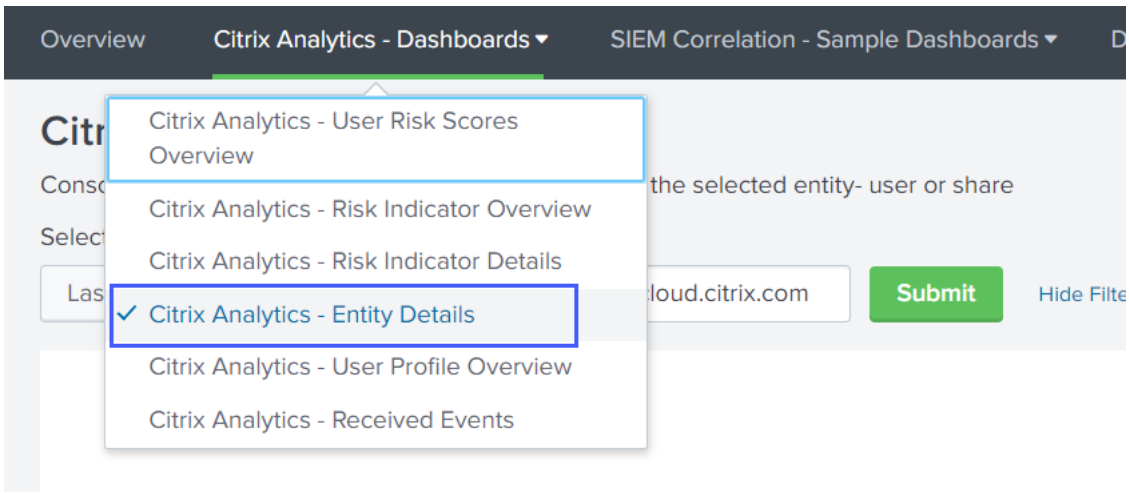
| ℹ | Time | Event |
|---|---|---|
| > | 7/1/21 9:29:59.000 PM | { [-] cas_consumer_debug_details: { [+] } data_source: Citrix Content Collaboration data_source_id: 0 entity_id: 6e130e9b07e28bea778eef5e21809150ce7bb05da8d821fbcff235b962796586 entity_type: user |

## Detalles de entidad

Utilice el panel de control para ver los detalles sobre un usuario de la entidad de usuario y su comportamiento riesgoso.

Para ver el panel, haga clic en **Citrix Analytics- Paneles > Citrix Analytics- Detalles de la entidad**.

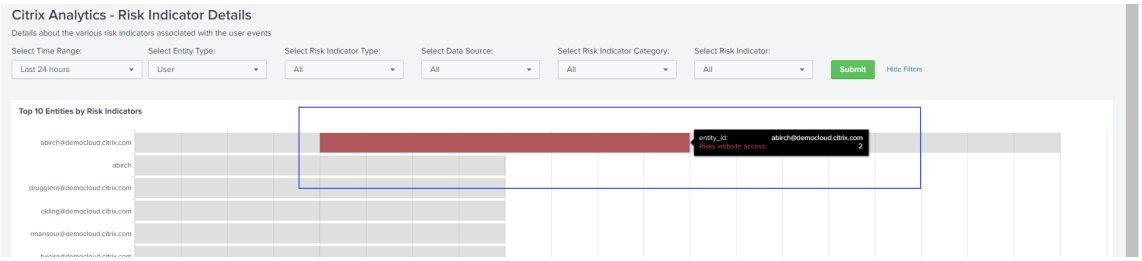



### Ver el informe

Introduzca un intervalo de tiempo y la entidad (nombre de usuario) y haga clic en **Enviar** para ver la información detallada.

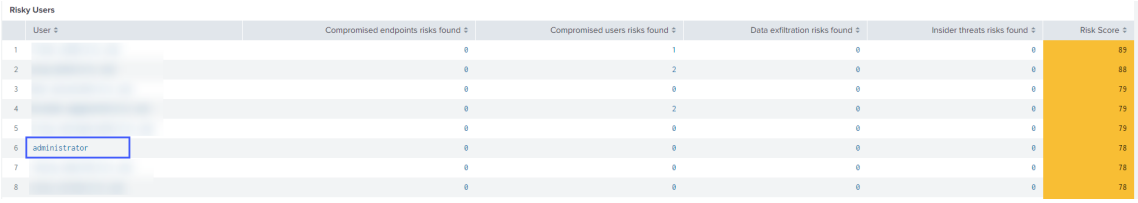
De forma alternativa, también puede ver la información detallada sobre una entidad en los siguientes paneles:

- En **Citrix Analytics: detalles del indicador de riesgo**, vaya a **las 10 principales entidades por indicadores de riesgo**y haga clic en una entidad.




- En **Citrix Analytics: descripción general de la puntuación de riesgo**, vaya a **Usuarios con riesgos** y haga clic en un nombre de usuario.

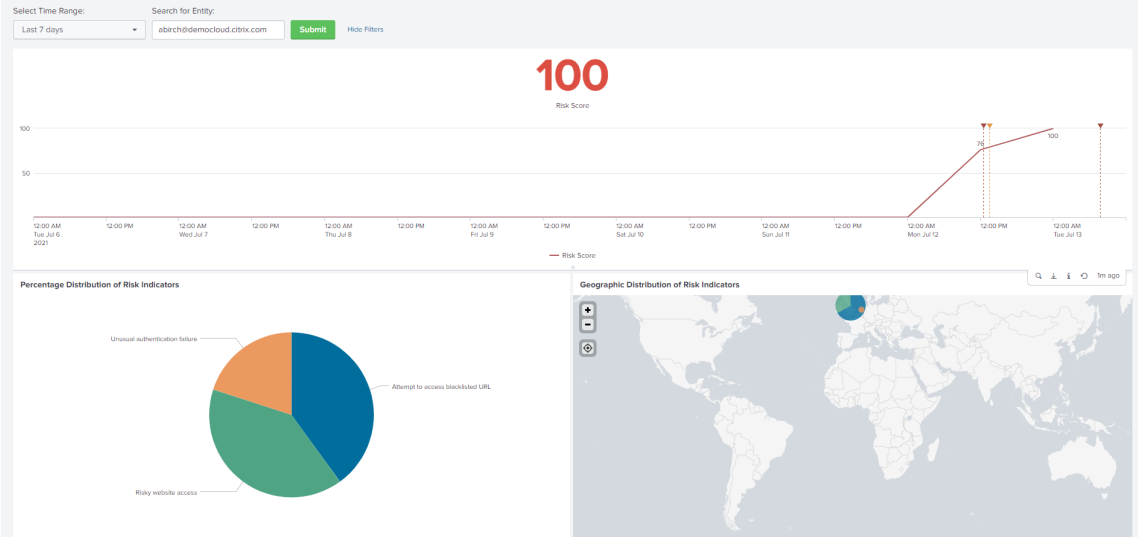


Risky Users

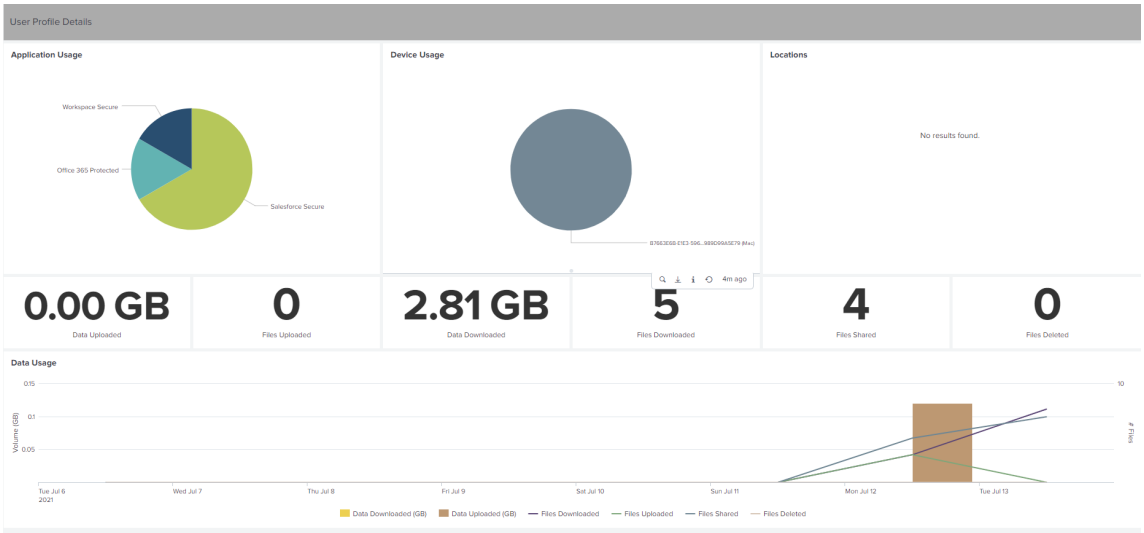
| | User | Compromised endpoints risks found | Compromised users risks found | Data exfiltration risks found | Insider threats risks found | Risk Score |
|---|---|---|---|---|---|---|
| 1 | [illegible] | 0 | 1 | 0 | 0 | 89 |
| 2 | [illegible] | 0 | 2 | 0 | 0 | 88 |
| 3 | [illegible] | 0 | 0 | 0 | 0 | 79 |
| 4 | [illegible] | 0 | 2 | 0 | 0 | 79 |
| 5 | [illegible] | 0 | 0 | 0 | 0 | 79 |
| 6 | administrator | 0 | 0 | 0 | 0 | 78 |
| 7 | [illegible] | 0 | 0 | 0 | 0 | 78 |
| 8 | [illegible] | 0 | 0 | 0 | 0 | 78 |

Se muestra la siguiente información detallada:

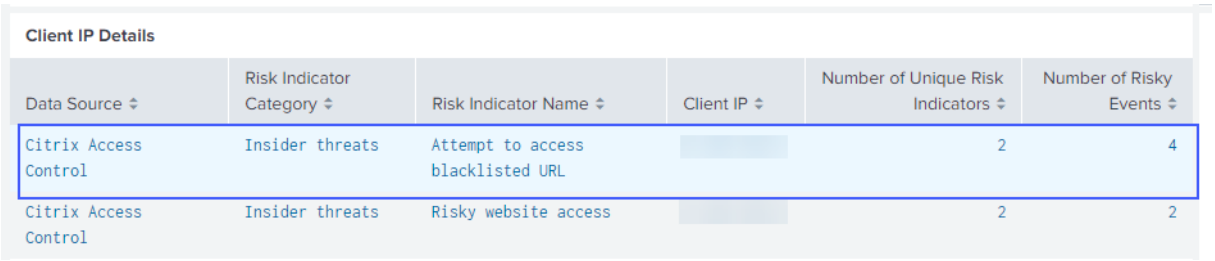
- Puntuación de riesgo actual y cronograma de la puntuación de riesgo para el intervalo de tiempo seleccionado.
- Distribución porcentual de los indicadores de riesgo. Le ayuda a analizar el patrón de actividades de riesgo de la entidad.
- Distribución geográfica de los indicadores de riesgo. Le ayuda a identificar las ubicaciones inusuales y de alto riesgo.
- Detalles de IP del cliente asociados a las actividades de riesgo.
- Detalles del dispositivo del usuario asociados a las actividades de riesgo.
- Detalles del indicador de riesgo, como la fuente de datos asociada, la categoría de riesgo, la gravedad del riesgo, etc.





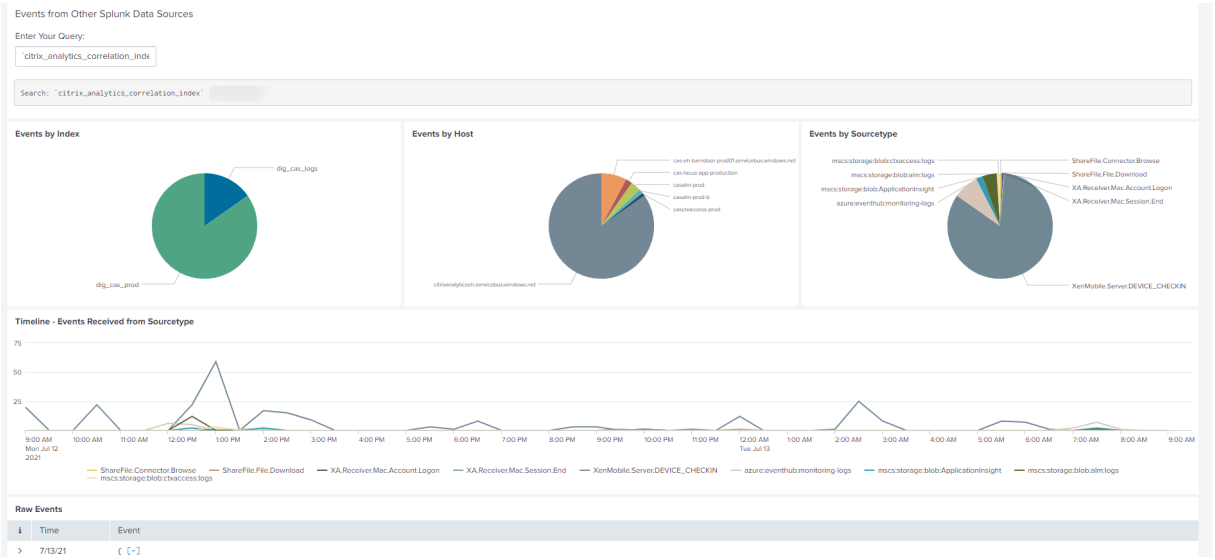

Correlaciona las IP de los clientes y los dispositivos de usuario asociados a actividades de riesgo con los eventos recopilados de otras fuentes de seguridad que están conectadas a tu Splunk. Por ejemplo, haga clic en una fila de la tabla **Detalles de IP del cliente** .



**Client IP Details**

| Data Source | Risk Indicator Category | Risk Indicator Name | Client IP | Number of Unique Risk Indicators | Number of Risky Events |
|---|---|---|---|---|---|
| Citrix Access Control | Insider threats | Attempt to access blacklisted URL | | 2 | 4 |
| Citrix Access Control | Insider threats | Risky website access | | 2 | 2 |

En el panel de control de **correlación de eventos de Citrix Analytics**, puede ver los eventos asociados a la IP del cliente seleccionada que se correlacionan desde los demás orígenes de datos de seguridad (según el índice y el tipo de origen). Estos eventos proporcionan información más detallada sobre las actividades maliciosas asociadas con la IP del cliente.

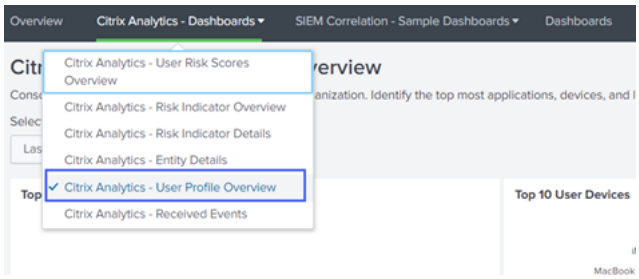


## Descripción general del perfil de usuario

Utilice el panel de control para ver las métricas de eventos asociadas a los usuarios de su organización.

Para ver el panel, haga clic en **Citrix Analytics- Paneles > Citrix Analytics- Descripción general del perfil de usuario**.



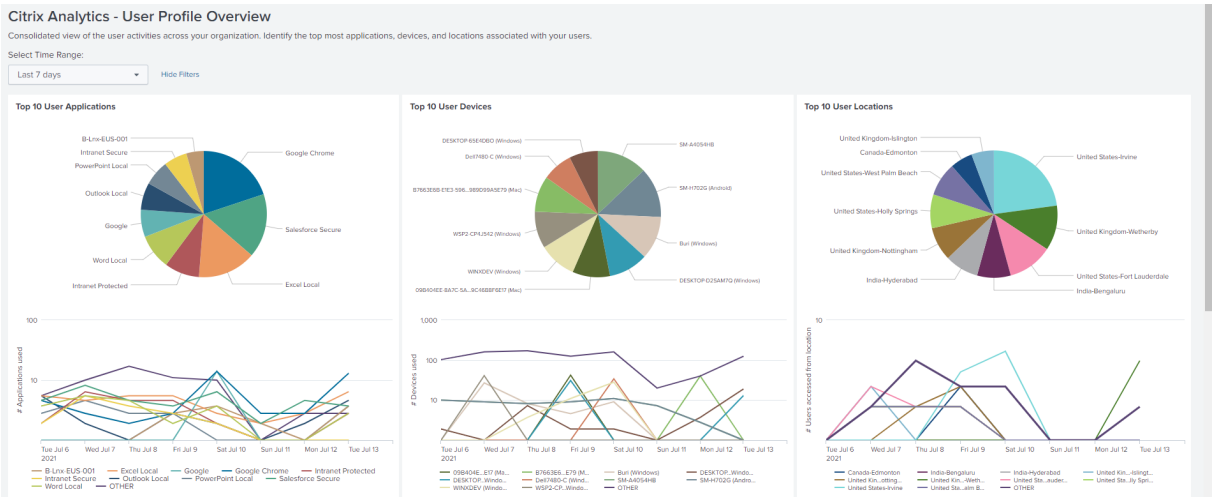

### Ver los eventos

Selecciona un intervalo de tiempo y consulta las siguientes métricas:

- Las 10 aplicaciones más utilizadas por los usuarios
- Los 10 dispositivos más utilizados por los usuarios
- Las 10 mejores ubicaciones utilizadas por los usuarios
- Número de aplicaciones web y SaaS utilizadas
- Número de dispositivos utilizados
- Número de usuarios que han accedido a todas las ubicaciones
- Métricas de uso de datos como archivos cargados, descargados y compartidos

Estas métricas le proporcionan información sobre las actividades de los usuarios en su organización. Puede identificar las aplicaciones y dispositivos más importantes, los patrones de uso, los dispositivos y aplicaciones que no cumplen los requisitos, las ubicaciones inusuales, el acceso de riesgo y las actividades de archivos inusuales.

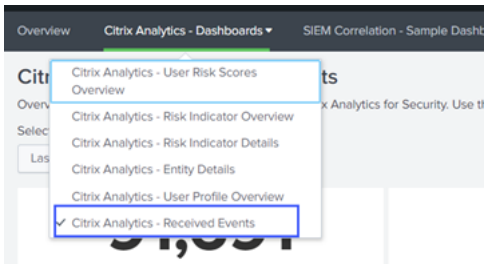
 




## Eventos recibidos

Utilice el panel de control para ver los eventos recibidos de Citrix Analytics for Security. Un evento indica un tipo de actividad del usuario.

Para ver el panel, haga clic en **Citrix Analytics- Paneles > Citrix Analytics- Eventos recibidos**.



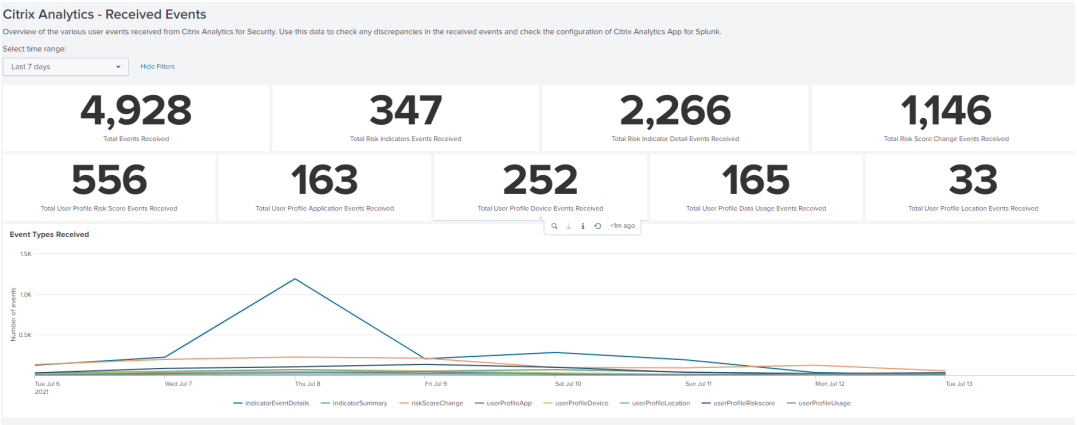

### Ver los informes

Seleccione un intervalo de tiempo para ver y comparar los distintos tipos de eventos recibidos. El panel de control proporciona la siguiente información:

- Total de eventos recibidos: es la suma de todos los eventos recibidos de Citrix Analytics for Security, incluidos los siguientes:
  - Eventos del indicador de riesgo total: indica los eventos asociados a los indicadores de riesgo desencadenados por los usuarios.
  - Eventos detallados del indicador de riesgo total: indica los eventos asociados con los detalles de los indicadores de riesgo desencadenados.
  - Eventos de cambio de puntuación de riesgo total: indica los eventos asociados con el cambio de puntuación de riesgo del usuario.

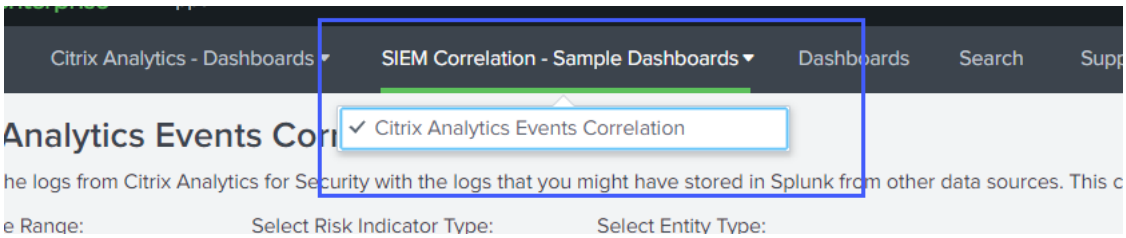
- Total de eventos de puntuación de riesgo del perfil de usuario: indica los eventos asociados a las puntuaciones de riesgo de los usuarios.
- Sucesos totales de aplicaciones de perfil de usuario: indica los eventos asociados a las aplicaciones utilizadas por los usuarios.
- Sucesos totales de dispositivos de perfil de usuario: indica los eventos asociados a los dispositivos utilizados por los usuarios.
- Sucesos totales de uso de datos de perfil de usuario: indica los eventos asociados con el uso de datos de los usuarios.
- Sucesos totales de ubicación de perfil de usuario: indica los eventos asociados a las ubicaciones a las que acceden los usuarios.




## Correlación de eventos de ejemplo

Utilice el panel para correlacionar los eventos recibidos de Citrix Analytics for Security con los eventos recopilados de otros orígenes de datos de seguridad configurados en su Splunk. Obtiene información más profunda sobre las actividades riesgosas del usuario recopiladas de múltiples fuentes de datos, encuentra relaciones entre los eventos e identifica cualquier amenaza.

Para ver el panel, haga clic en **Correlación SIEM - Paneles de ejemplo > Correlación de eventos de Citrix Analytics**.



### Requisitos previos

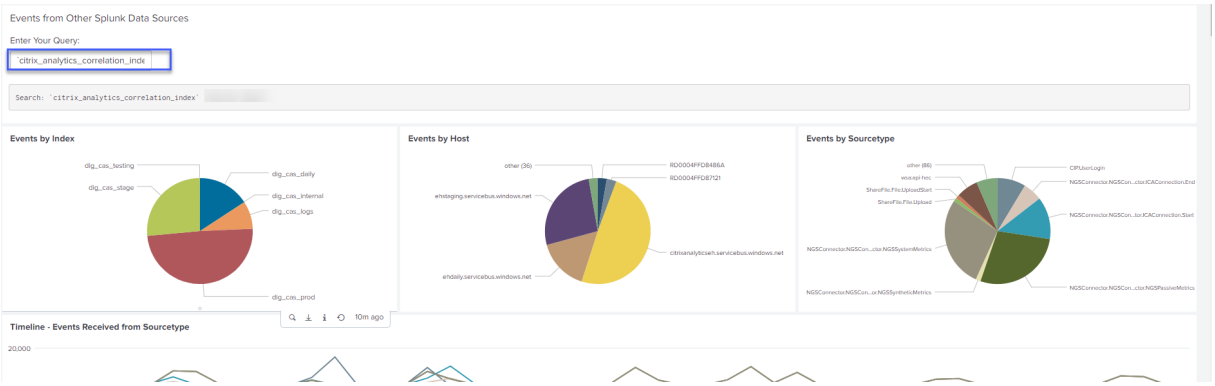
Para llevar a cabo la correlación, asegúrese de lo siguiente:

- Debe tener eventos de otros orígenes de datos de seguridad para correlacionarlos. Por ejemplo, eventos asociados a usuarios, dispositivos y direcciones IP de clientes recibidos de otros orígenes de datos configuradas en su Splunk.
- Debe tener un índice de correlación definido durante la configuración.

### Correlaciona los eventos

Puede ver las entidades de mayor riesgo y las direcciones IP de mayor riesgo detectadas por Citrix Analytics for Security. Para correlacionar estos eventos con otros orígenes de datos (definidos en el índice y en el tipo de origen), haga clic en una entidad o en una dirección IP de las tablas.


El valor de índice que se muestra en el campo de consulta se define durante la configuración de la aplicación. Puede cambiar el valor del índice a una fuente de datos de seguridad diferente en función de sus requisitos.



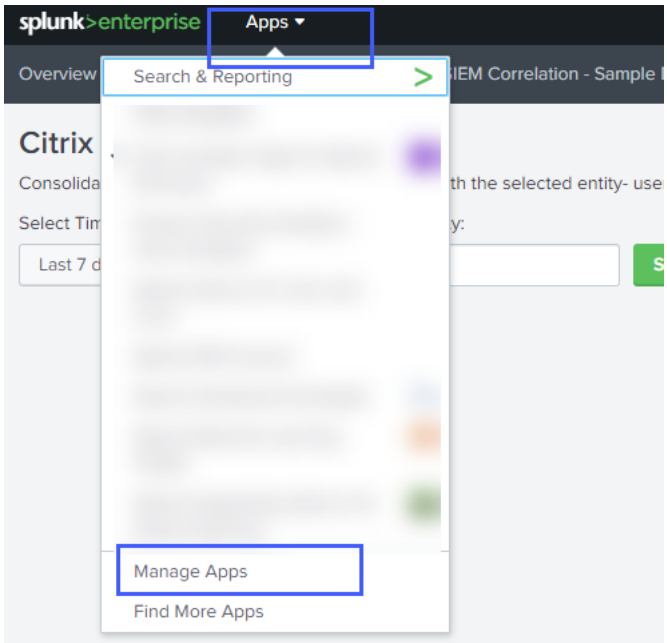

### Solución de problemas de ausencia de eventos

Si no encuentre ningún evento en todos los paneles, puede deberse a problemas de configuración de la aplicación Citrix Analytics para Splunk y del complemento Citrix Analytics para Splunk. En este caso, compruebe el valor del índice y el valor del tipo de origen. Asegúrese de que los valores del índice y del tipo de fuente sean los mismos en la aplicación y en el complemento.

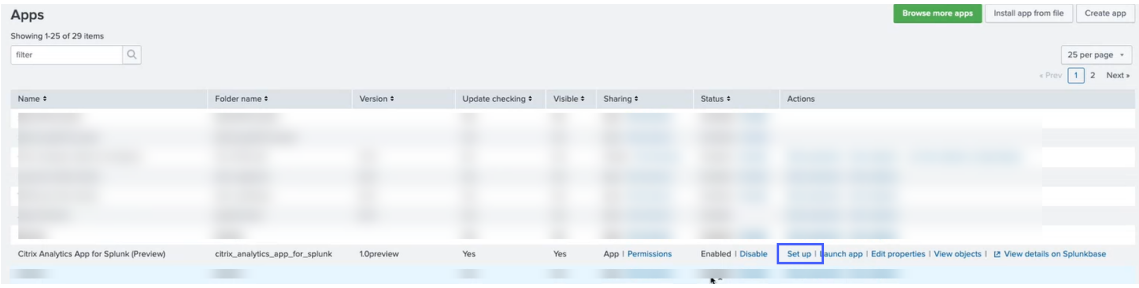
Para ver los valores de configuración de la aplicación Citrix Analytics para Splunk:

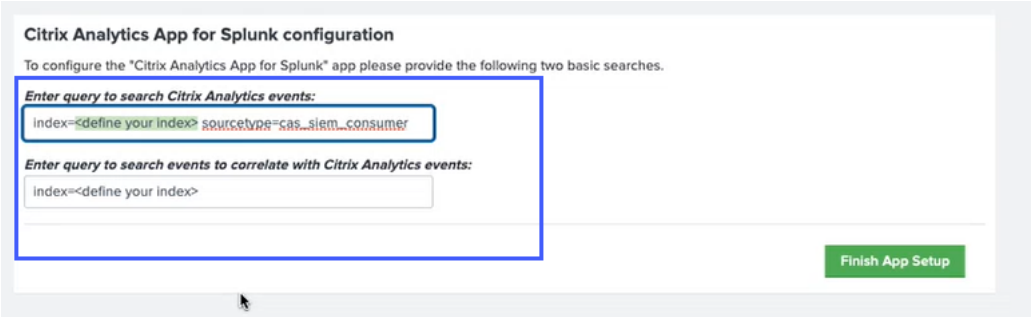
1. Haga clic en **Aplicaciones > Administrar aplicaciones**.




2. Busque la aplicación Citrix Analytics para Splunk en la lista. Haga clic en **Configurar**.



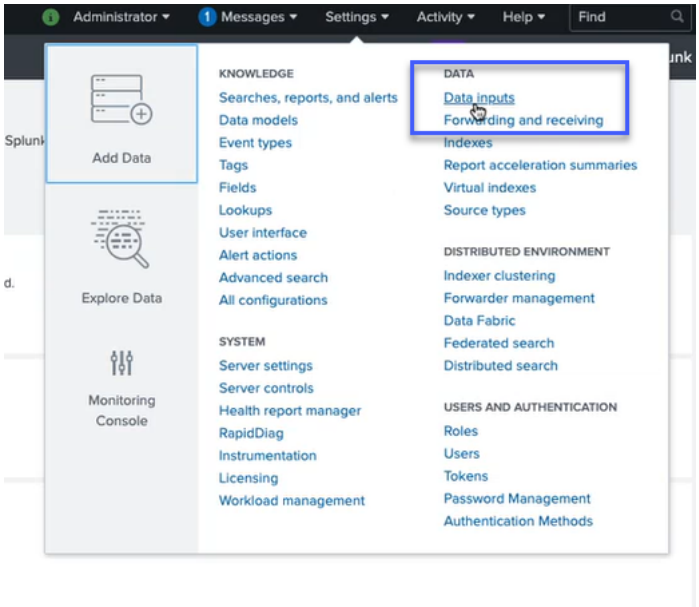

3. Compruebe el tipo de fuente y el índice.



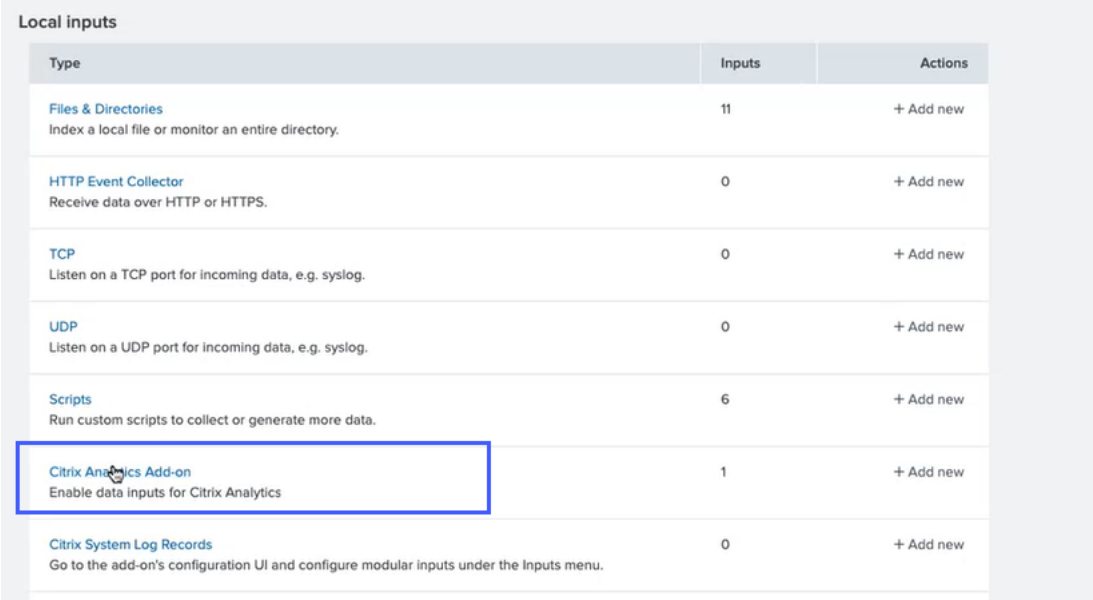

Para ver los valores de configuración del complemento Citrix Analytics para Splunk:

1. Haga clic en **Configuración > Entradas de datos**.

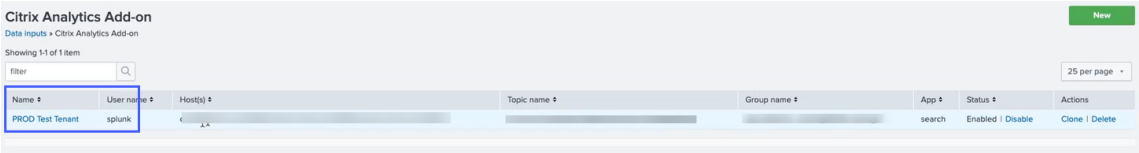
 




2. Haga clic en **Complemento de Citrix Analytics**.

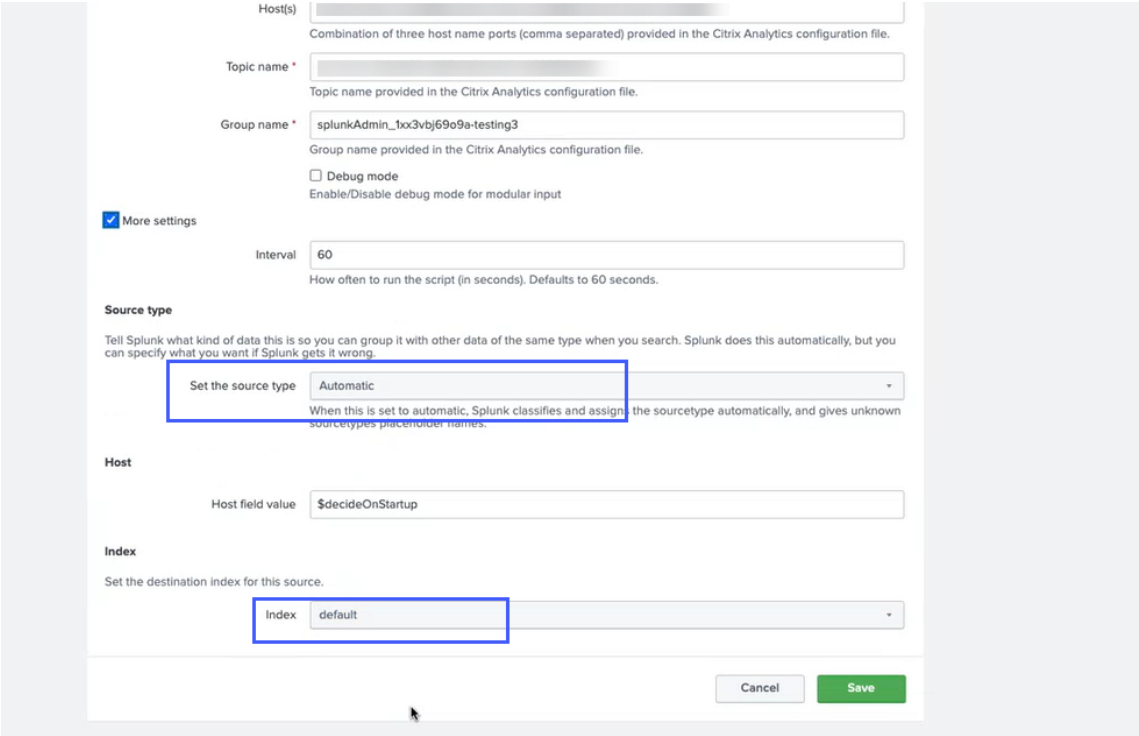



3. Haga clic en el arrendatario del que obtiene los eventos.
4. Selecciona **Más ajustes**.




5. Compruebe el tipo de fuente y el índice.




Para obtener más información sobre la configuración, consulte Configurar el complemento Citrix Analytics para Splunk.

## Problemas de configuración con el complemento Citrix Analytics para Splunk

July 12, 2022

### La configuración del complemento Citrix Analytics no está

Después de instalar Citrix Analytics Add-on for Splunk en su entorno de Splunk Forwarder o Splunk Standalone, no verá la configuración del **complemento de Citrix Analytics** en **Configuración > Entradas de datos**.

#### Motivo

Este problema se produce cuando se instala el complemento Citrix Analytics para Splunk en un entorno de Splunk no compatible.

#### Correcciones

Instale el complemento Citrix Analytics para Splunk en un entorno de Splunk compatible. Para obtener información sobre las versiones compatibles, consulte Integración de Splunk.

### No hay datos disponibles en los paneles de Splunk

Después de instalar y configurar Citrix Analytics Add-on for Splunk en su entorno de Splunk Forwarder o Splunk Standalone, no verá ningún dato de Citrix Analytics en los paneles de Splunk.

#### Cheques

Para solucionar el problema, verifique lo siguiente en su entorno de Splunk Forwarder o Splunk Standalone:

1. Asegúrese de que se cumplan los requisitos previos para la integración de Splunk.
2. Vaya a **Configuración > Entradas de datos > Complemento de Citrix Analytics**. Asegúrese de que los detalles de configuración de Citrix Analytics estén disponibles.
3. Si los detalles de configuración están disponibles, ejecute la siguiente consulta para comprobar los registros en busca de errores relacionados con el complemento Citrix Analytics para Splunk:

   ```
   index=_internal sourcetype=splunkd log_level=ERROR component=
      ExecProcessor cas_siem_consumer
   ```

4. Si no encuentra ningún error, el complemento Citrix Analytics para Splunk funciona como se esperaba. Si encuentra algún error en los registros, puede deberse a una de las siguientes razones:

   - No se pudo establecer la conexión entre el entorno de Splunk y los puntos finales de Citrix Analytics Kafka. Este problema puede deberse a la configuración del firewall.

     **Correcciones**: consulte con el administrador de red para resolver este problema.

   - Detalles de configuración incorrectos en **Configuración > Entradas de datos > Complemento de Citrix Analytics**.

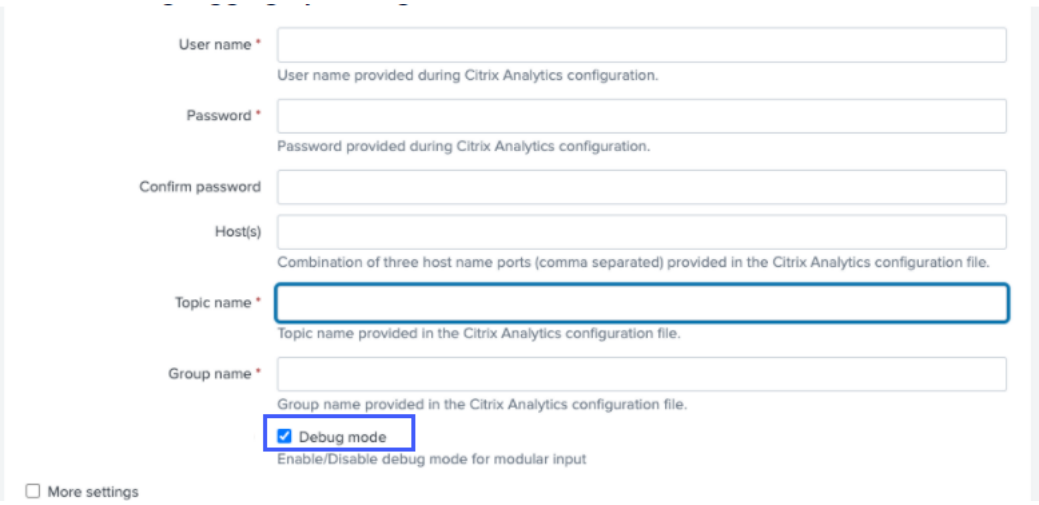
     **Correcciones**: Asegúrese de que los detalles de configuración de Citrix Analytics, como el nombre de usuario, la contraseña, los puntos finales del host, el tema y el grupo de consumidores, se escriben correctamente según el archivo de configuración de Citrix Analytics. Para obtener más información, consulte Configurar el complemento Citrix Analytics para Splunk.

5. Si no puede encontrar la causa del problema en los registros anteriores y quiere investigar más a fondo:

a) Habilite el **modo de depuración** en **Configuración > Entradas de datos > Complemento de Citrix Analytics**.

> Nota
>
> De forma predeterminada, el **modo de depuración** está inhabilitado. Al habilitar este modo, se generan demasiados registros. Por lo tanto, use esta opción solo cuando sea necesario y desactívela después de completar la tarea de depuración.




b) Busque los registros de depuración generados en la siguiente ubicación y compruebe si hay algún error:

```
$SPLUNK_HOME$/var/log/splunk.Filename
    splunk_citrix_analytics_add_on_debug_connection.log
```

c) (Opcional) Use el script de depuración `splunk cmd python cas_siem_consumer_debug.py` que está disponible con el complemento Citrix Analytics para Splunk. Este script genera un archivo de registro que contiene los detalles de su entorno de Splunk y las comprobaciones de conectividad. Puede usar los detalles para depurar el problema. Ejecute el script con el siguiente comando:

```
cd $SPLUNK_HOME$/etc/apps/TA_CTXS_AS/bin/; /opt/splunk/bin/
    splunk cmd python cas_siem_consumer_debug.py
```

### Mensaje de error

En los registros relacionados con el complemento Citrix Analytics para Splunk, es posible que consulte el siguiente error:

```
ERRORKafkaError{ code=_TRANSPORT,val=-195,str="Failed to get metadata
: Local: Broker transport failure"}
```

Este error se debe a un problema de conectividad de red o a un problema de autenticación.

Para depurar el problema:

1. En su entorno Splunk Forwarder o Splunk Standalone, habilite el **modo de depuración** para obtener los registros de depuración. Consulte el paso anterior 5.a.
2. Ejecute la siguiente consulta para encontrar cualquier problema de autenticación en los registros de depuración:

```
index=_internal source="*
    splunk_citrix_analytics_add_on_debug_connection.log*" "
    Authentication failure"
```

3. Si no encuentra ningún problema de autenticación en los registros de depuración, el error se debe a un problema de conectividad de red.
4. Busque y resuelva el problema mediante telnet o el script de depuración mencionado en el paso anterior 5.c.

### La actualización del complemento falla desde una versión anterior a la 2.0.0

En su entorno de Splunk Forwarder o Splunk Standalone, cuando actualiza el complemento Citrix Analytics para Splunk a la última versión desde una versión anterior a la 2.0.0, la actualización falla.

#### Correcciones

1. Elimine los siguientes archivos y carpetas ubicados en la carpeta de instalación `/bin` del complemento Citrix Analytics para Splunk:
   - `cd $SPLUNK_HOME$/etc/apps/TA_CTXS_AS/bin`
   - `rm -rf splunklib`
   - `rm -rf mac`
   - `rm -rf linux_x64`
   - `rm CARoot.pem`
   - `rm certificate.pem`
2. Reinicie su entorno Splunk Forwarder o Splunk Standalone.

# Integración de Microsoft Sentinel

November 17, 2023

> **Notas**
>
> - Póngase en contacto CAS-PM-Ext@cloud.com para solicitar ayuda para la integración de Microsoft Sentinel, la exportación de datos a Microsoft Sentinel o para enviar comentarios.
> - La exportación de datos a Microsoft Sentinel mediante el motor Logstash está en versión preliminar. Esta función se proporciona sin un acuerdo de nivel de servicio y no se recomienda para cargas de trabajo de producción. Para obtener más información, consulte la documentación de Microsoft Sentinel.

Integre Citrix Analytics for Security con su Microsoft Sentinel mediante el motor Logstash.

Esta integración le permite exportar y correlacionar los datos de los usuarios desde su entorno de TI de Citrix a Microsoft Sentinel y obtener información más profunda sobre la postura de seguridad de su organización. Vea los paneles de control perspicaces que son exclusivos de Citrix Analytics for Security en su entorno Splunk. También puede crear vistas personalizadas en función de sus requisitos de seguridad.

Para obtener más información sobre los beneficios de la integración y el tipo de datos procesados que se envían a su SIEM, consulte Integración de la información de seguridad y la gestión de eventos.

## Requisitos previos

- Active el procesamiento de datos para al menos un origen de datos. Ayuda a Citrix Analytics for Security a iniciar el proceso de integración de Microsoft Sentinel.
- Asegúrese de que el siguiente punto de enlace esté en la lista de permitidos en su red.

| Dispositivo de punto final | Región de los Estados Unidos | Región de la Unión Europea | Región Asia-Pacífico Sur |
|---|---|---|---|
| Intermediarios de Kafka | `casnb-0.citrix.com:9094`<br>`casnb-1.citrix.com:9094`<br>`casnb-2.citrix.com:9094` | `casnb-eu-0.citrix.com:9094`<br>`casnb-eu-1.citrix.com:9094`<br>`casnb-eu-2.citrix.com:9094` | `casnb-aps-0.citrix.com:9094`<br>`casnb-aps-1.citrix.com:9094`<br>`casnb-aps-2.citrix.com:9094` |

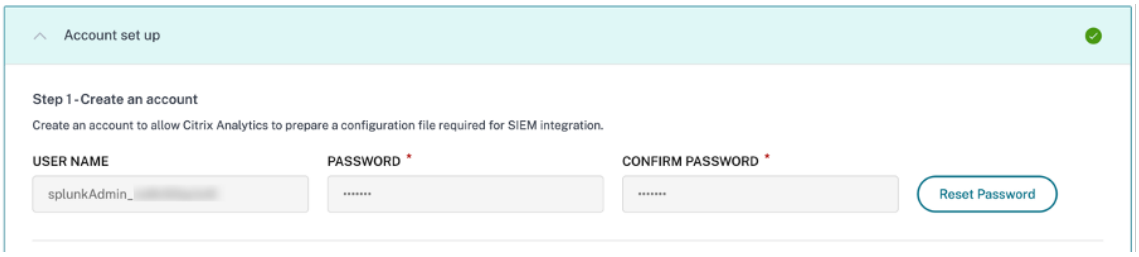
 

| Dispositivo de punto final | Región de los Estados Unidos | Región de la Unión Europea | Región Asia-Pacífico Sur |
|---|---|---|---|
| | `casnb-3.citrix.com:9094` | | |

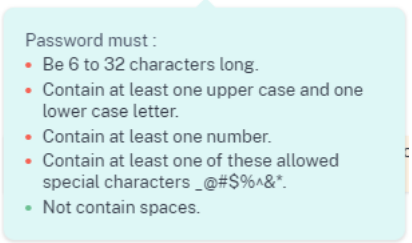
- Asegúrese de utilizar las versiones 7.17.7 o posteriores de logstash (versiones probadas para comprobar su compatibilidad con Citrix Analytics for Security: v7.17.7 y v8.5.3) con el complemento de salida Microsoft Sentinel para Logstash.

## Integración con Microsoft Sentinel

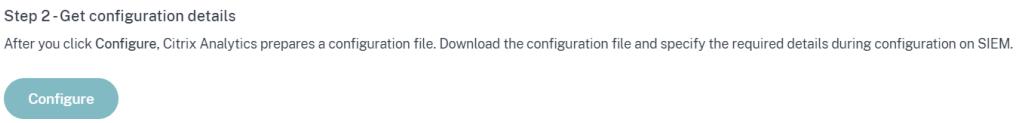
1. Ve a **Configuración > Exportaciones de datos**.
2. En la sección **Configuración de la cuenta**, cree una cuenta especificando el nombre de usuario y la contraseña. Esta cuenta se usa para preparar un archivo de configuración, que se requiere para la integración.




3. Asegúrese de que la contraseña cumpla con las siguientes condiciones:




4. Haga clic en **Configurar** para generar el archivo de configuración de Logstash.




5. Seleccione la ficha Azure Sentinel (versión Tech Preview) para descargar los archivos de configuración:

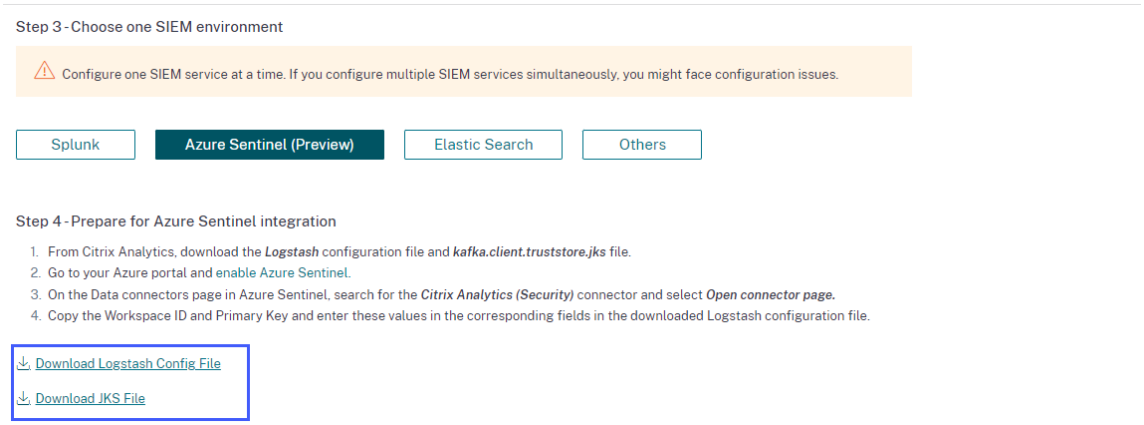
 

- **Archivo de configuración de Logstash**: contiene los datos de configuración (secciones de entrada, filtro y salida) para enviar eventos de Citrix Analytics for Security a Microsoft Sentinel mediante el motor de recopilación de datos Logstash.

  Para obtener información sobre la estructura de archivos de configuración de Logstash, consulte la documentación de Logstash.

- **Archivo JKS**: contiene los certificados necesarios para la conexión SSL.

> **Nota**
>
> Estos archivos contienen información confidencial. Manténgalos en un lugar seguro y protegido.




6. Prepare la integración de Azure Sentinel:

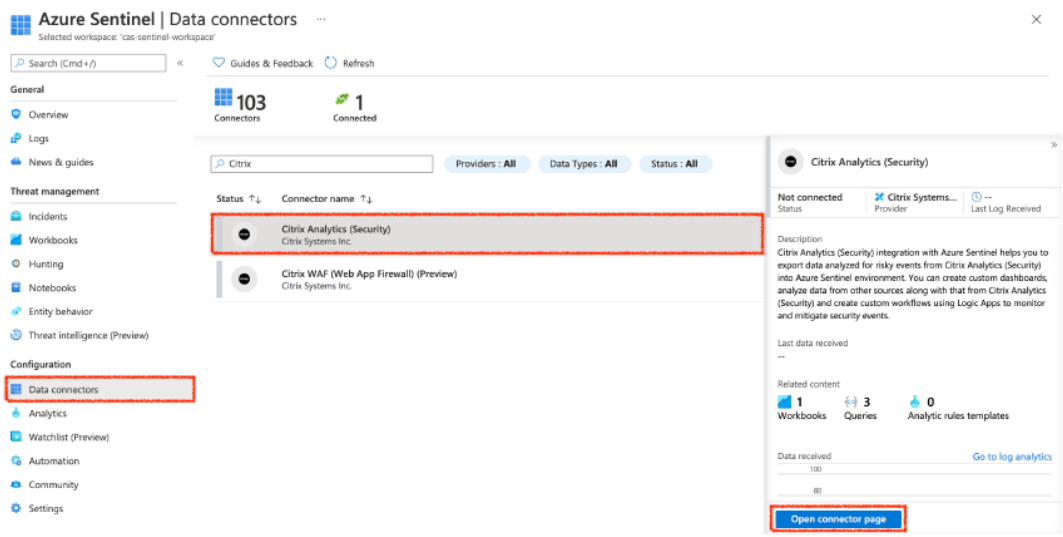
   a) En el portal de Azure, habilite Microsoft Sentinel. Puede crear un espacio de trabajo o usar su espacio de trabajo existente para ejecutar Microsoft Sentinel.

   b) En el menú principal, seleccione **Conectores de datos** para abrir la galería de conectores de datos.

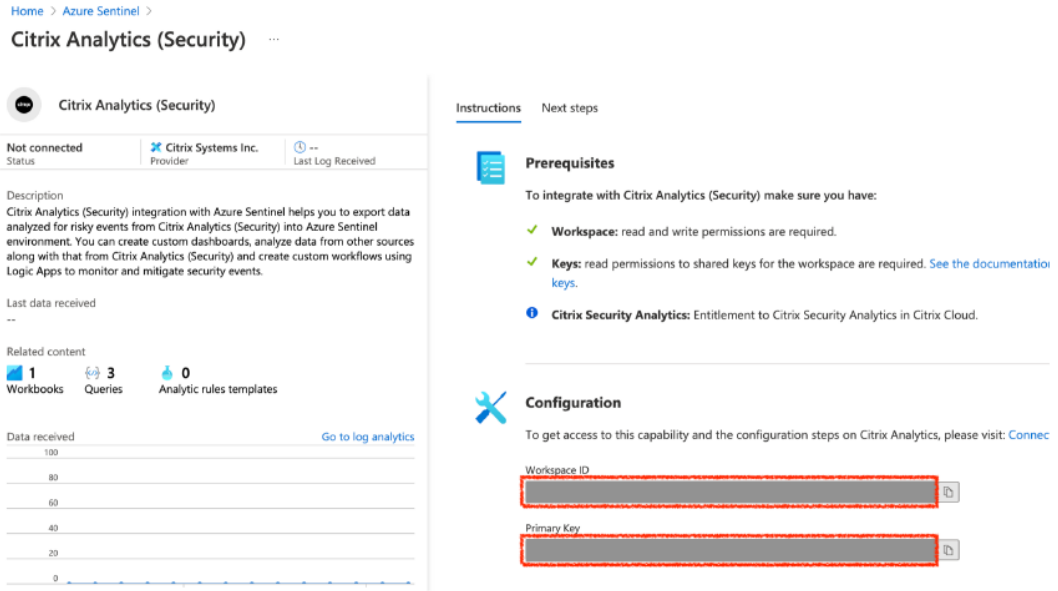
   c) Busque **Citrix Analytics (seguridad)**.

   d) Seleccione **Citrix Analytics (seguridad)** y seleccione **Abrir página de conector**.




e) En la página **Citrix Analytics (seguridad)**, copie el **ID del espacio de trabajo** y la **clave principal**. Debe introducir esta información en el archivo de configuración de Logstash en los pasos posteriores.




f) Configure Logstash en su máquina host:

i. En su máquina host Linux o Windows, instale el complemento de salida [Logstash](https://www.ela logstash.html) y Microsoft Sentinel para Logstash.

ii. En la máquina host donde ha instalado Logstash, coloque los siguientes archivos en el directorio especificado:

| Tipo de máquina host | Nombre de archivo | Ruta del directorio |
|---|---|---|
| Linux | CAS_AzureSentinel_LogStash_Config.conf | Para paquetes Debian y RPM: `/etc/logstash/conf.d/`<br>Para archivos.zip y.tar.gz: `{ extract.path } /config` |
| | kafka.client.truststore.jks | Para paquetes Debian y RPM: `/etc/logstash/ssl/`<br>Para archivos.zip y.tar.gz: `{ extract.path } /ssl` |
| Windows | CAS_AzureSentinel_LogStash_Config.conf | `C:\logstash-7.xx.x\config` |
| | kafka.client.truststore.jks | |

Para obtener información sobre la estructura de directorios predeterminada de los paquetes de instalación de Logstash, consulte la documentación de Logstash.

iii. Abra el archivo de configuración de Logstash y haga lo siguiente:

A. En la sección de entrada del archivo, introduzca lo siguiente:

- **Contraseña**: la contraseña de la cuenta que creó en Citrix Analytics for Security para preparar el archivo de configuración.
- **Ubicación del almacén de confianza SSL**: la ubicación de su certificado de cliente SSL. Esta es la ubicación del archivo kafka.client.truststore.jks en su máquina host.

```
input {
  kafka {
    bootstrap_servers => "[redacted]"
    topics => ["[redacted]"]
    group_id => "[redacted]"
    session_timeout_ms => 60000
    auto_offset_reset => "earliest"
    security_protocol => "SASL_SSL"
    sasl_mechanism => "SCRAM-SHA-256"
    ssl_endpoint_identification_algorithm => ""
    sasl_jaas_config => "org.apache.kafka.common.security.scram.ScramLoginModule required username='[redacted]' password='<your password>';"
    ssl_truststore_location => "/etc/logstash/ssl/kafka.client.truststore.jks"
  }
}
```

B. En la sección de salida del archivo, introduzca el **identificador del espacio** de trabajo y la **clave principal** (que ha copiado de Microsoft Sentinel) en la sección de salida del archivo.

```
output {
  if [event_type] == "indicatorSummary" {
    microsoft-logstash-output-azure-loganalytics {
          workspace_id => "<your Azure Log analytics Workspace ID>"
          workspace_key => "<your Shared Key>"
          custom_log_table_name => "CitrixAnalytics_indicatorSummary"
          time_generated_field => "timestamp"
    }
  } else if [event_type] == "indicatorEventDetails" {
    microsoft-logstash-output-azure-loganalytics {
          workspace_id => "<your Azure Log analytics Workspace ID>"
          workspace_key => "<your Shared Key>"
          custom_log_table_name => "CitrixAnalytics_indicatorEventDetails"
          time_generated_field => "timestamp"
    }
  }else if [event_type] == "riskScoreChange" {
    microsoft-logstash-output-azure-loganalytics {
          workspace_id => "<your Azure Log analytics Workspace ID>"
          workspace_key => "<your Shared Key>"
          custom_log_table_name => "CitrixAnalytics_riskScoreChange"
          time_generated_field => "timestamp"
    }
  } else if [event_type] =~ "userProfile.+" {
    microsoft-logstash-output-azure-loganalytics {
          workspace_id => "<your Azure Log analytics Workspace ID>"
          workspace_key => "<your Shared Key>"
          custom_log_table_name => "CitrixAnalytics_userProfile"
          time_generated_field => "timestamp"
    }
  } else {
    microsoft-logstash-output-azure-loganalytics {
          workspace_id => "<your Azure Log analytics Workspace ID>"
          workspace_key => "<your Shared Key>"
          custom_log_table_name => "CitrixAnalytics_misc"
          time_generated_field => "timestamp"
```

iv. Reinicie la máquina host Logstash para enviar los datos procesados de Citrix Analytics for Security a Microsoft Sentinel.

g) Vaya a su Microsoft Sentinel Workspace y vea los datos en el libro de trabajo de Citrix Analytics.

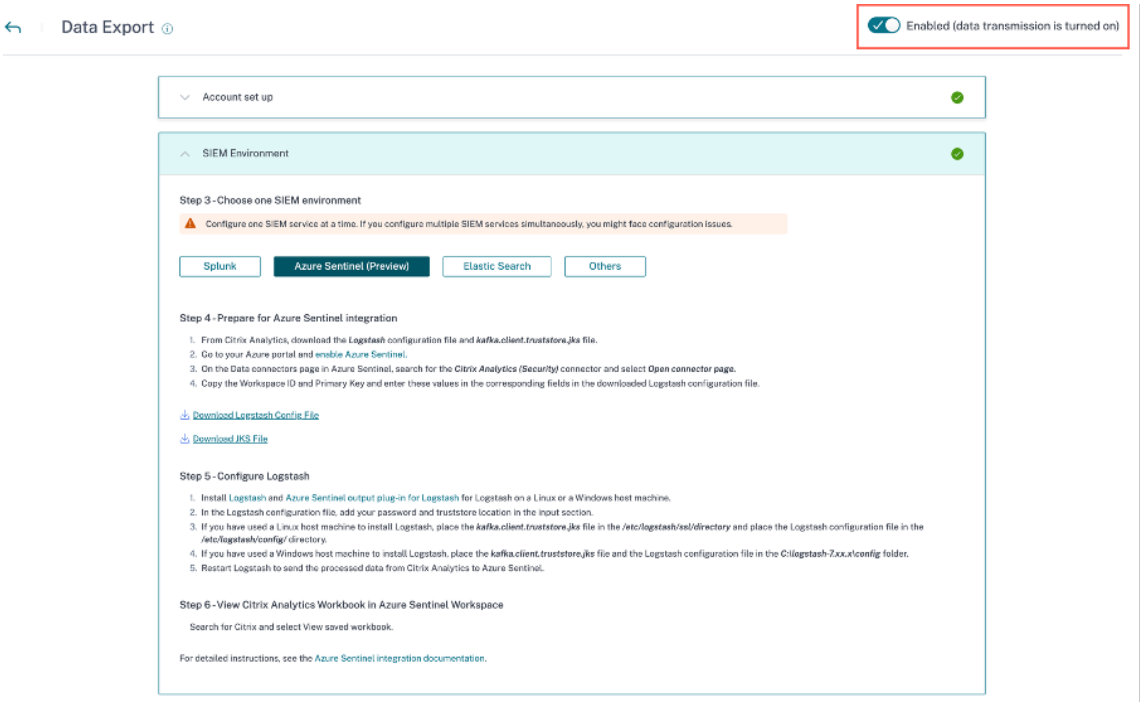
## Activar o desactivar la transmisión de datos

Después de que Citrix Analytics for Security prepare el archivo de configuración, se activa la transmisión de datos para Microsoft Sentinel.

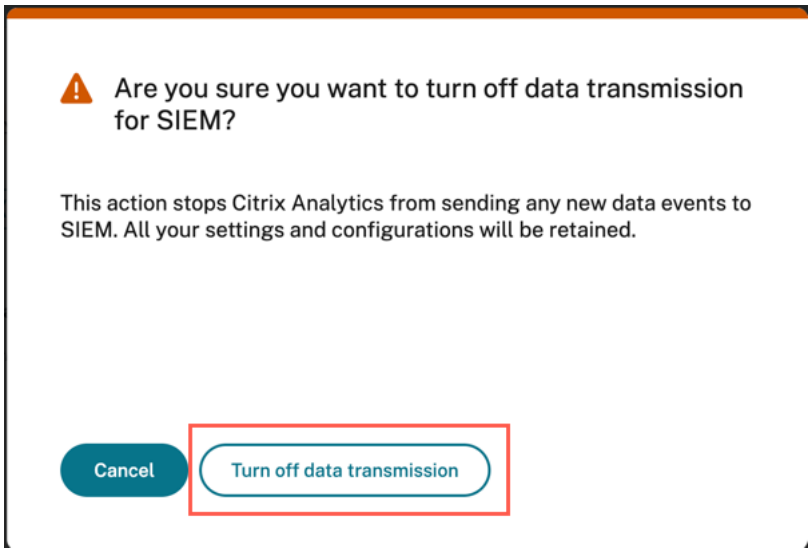
Para dejar de transmitir datos de Citrix Analytics for Security:

1. Ve a **Configuración > Exportaciones de datos**.
2. Apague el botón para desactivar la **transmisión de datos**. De forma predeterminada, la transmisión de datos siempre está habilitada.




Aparece una ventana de advertencia para su confirmación. Haga clic en el botón **Desactivar la transmisión de datos** para detener la actividad de transmisión.




Para habilitar de nuevo la transmisión de datos, active el botón.

Para obtener más información sobre la integración de Microsoft Sentinel, consulte los siguientes enlaces:

- Citrix Analytics Integration with Microsoft Sentinel
- Raise your threat-hunting game with Citrix Analytics for Security and Microsoft Sentinel

# Libro de trabajo de Citrix Analytics para Microsoft Sentinel

December 7, 2023

> **Nota**
>
> Esta función se encuentra en Tech Preview.

En este artículo se describe el libro de trabajo de Citrix Analytics que está disponible en el espacio de trabajo de Microsoft Sentinel.

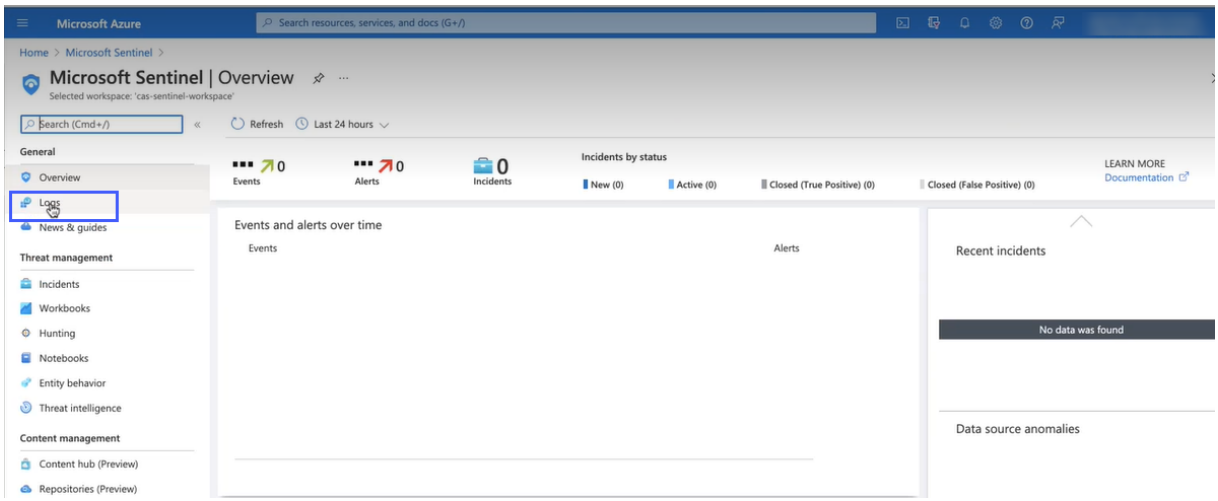
## Requisito previo

Para usar el libro de trabajo de Citrix Analytics, asegúrese de que ya ha integrado Microsoft Sentinel con Citrix Analytics for Security. Para obtener más información, consulte Integración de Microsoft Sentinel.

## Ver los eventos de Citrix Analytics

Después de integrar Citrix Analytics for Security con Microsoft Sentinel, el conector de Logstash comienza a enviar eventos de Citrix Analytics for Security al espacio de trabajo de Microsoft Sentinel. En su **portal de Azure**, abra el espacio de trabajo de Microsoft Sentinel que ha utilizado para la integración.

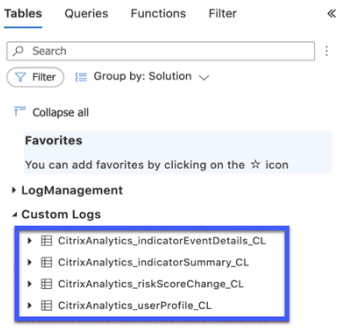
Para comprobar que Microsoft Sentinel recibe los eventos de Citrix Analytics for Security, seleccione **Registros > Registros personalizados**.



En la sección **Registros personalizados**, puede ver las tablas de registros que se crean automáticamente para almacenar los eventos recibidos de Citrix Analytics for Security. Estas tablas de registro sirven como origen de los paneles del libro de trabajo de Citrix Analytics.

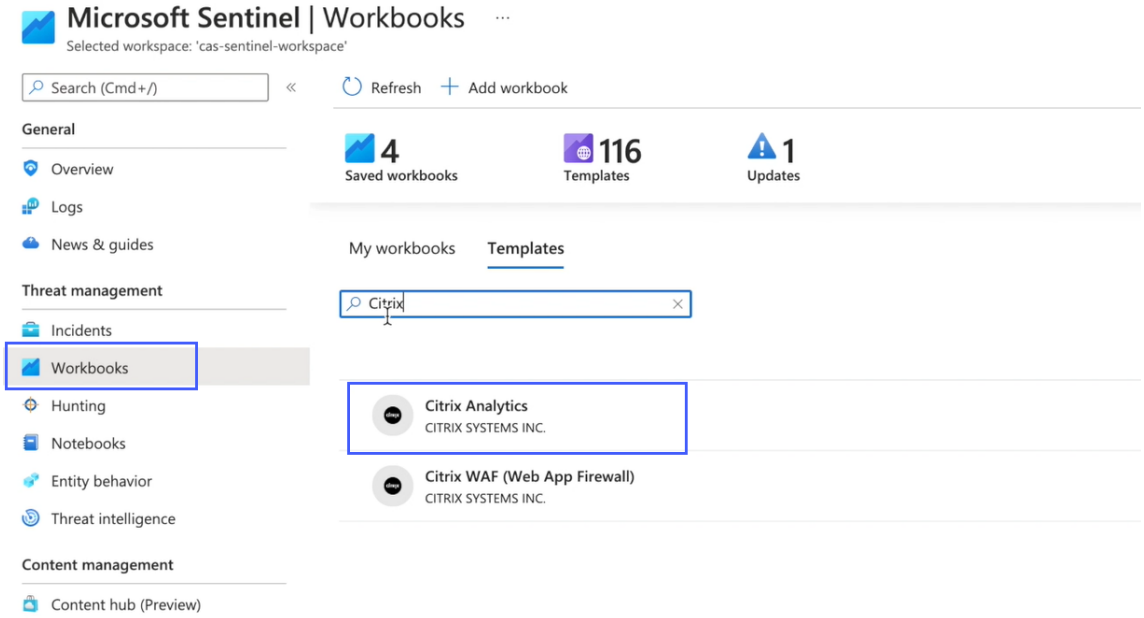
> **Nota**
>
> Los eventos enviados desde Citrix Analytics for Security pueden tardar unas horas en aparecer en el espacio de trabajo de Microsoft Sentinel. Por lo tanto, es posible que vea un retraso en la creación de las tablas de registro para los eventos.




## Ver el libro de trabajo de Citrix Analytics

Cuando las tablas de registro se hayan creado correctamente, haga lo siguiente:

1. Seleccione **Libros de trabajo** y busque en **Citrix Analytics**. Seleccione **Citrix Analytics**.

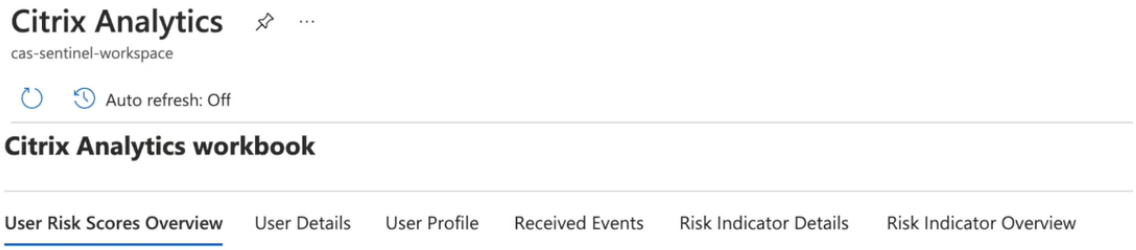



2. Seleccione **Ver plantilla** para abrir el libro de trabajo de Citrix Analytics.


En el libro de trabajo de Citrix Analytics, puede ver los eventos del usuario en los siguientes paneles:

- **Descripción general de las puntuaciones de riesgo del usuario**: proporciona una vista consolidada de los usuarios de riesgo en su organización.
- **Detalles del usuario**: proporciona detalles de los usuarios y su comportamiento de riesgo.
- **Perfil de usuario**: proporciona las métricas de eventos asociadas a los usuarios.
- **Eventos recibidos**: proporciona los eventos recibidos de Citrix Analytics for Security.
- **Detalles del indicador de riesgo**: proporciona detalles sobre los indicadores de riesgo integrados y personalizados activados por los usuarios.
- **Descripción general de los indicadores de riesgo**: proporciona una vista consolidada de los indicadores de riesgo activados por los usuarios.

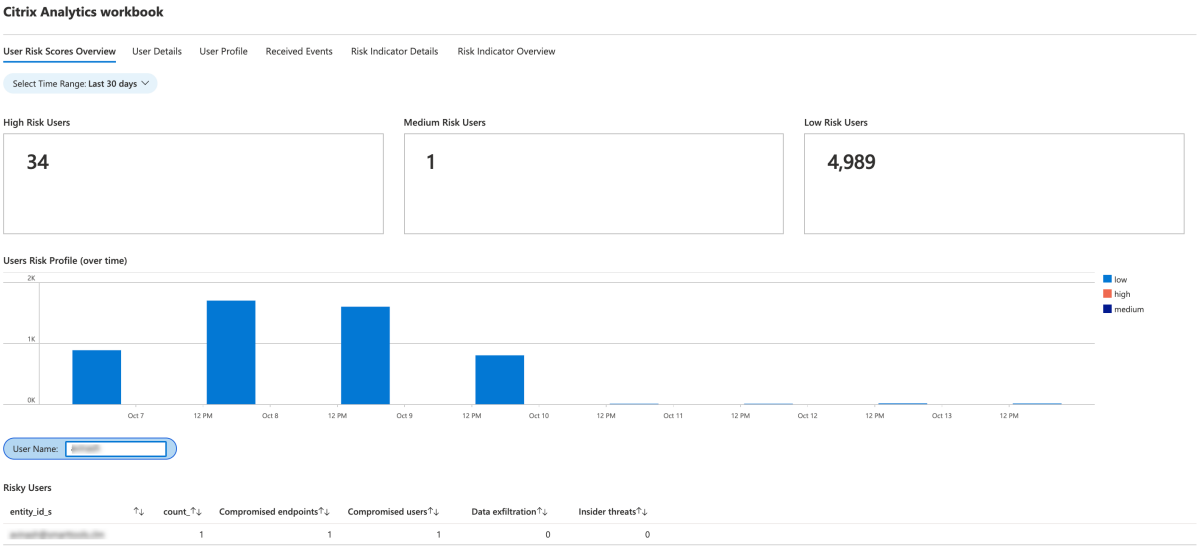



## Descripción general de la puntuación de riesgo

Este panel proporciona una vista consolidada de los usuarios de riesgo de su organización. Los usuarios se clasifican según los niveles de riesgo: alto, medio y bajo. Los niveles de riesgo se basan en las anomalías de las actividades de los usuarios y, en consecuencia, se asigna una puntuación de riesgo. Para obtener más información sobre los tipos de usuarios de riesgo, consulte el panel Usuarios.

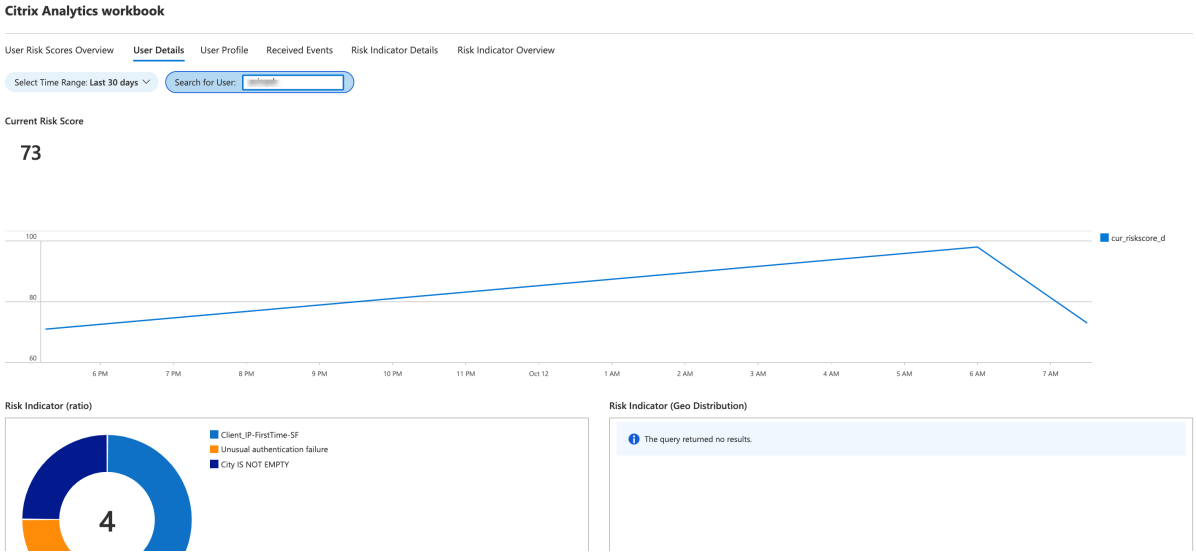
Seleccione un período de tiempo para ver los usuarios riesgosos de su organización.




## Detalles del usuario

Este panel proporciona la puntuación de riesgo y los indicadores de riesgo asociados con un usuario.

Busque un usuario y vea sus actividades de riesgo que pueden representar una amenaza para su organización. Para mitigar la amenaza, puede tomar las medidas adecuadas en las cuentas de usuario en función de su gravedad del riesgo.



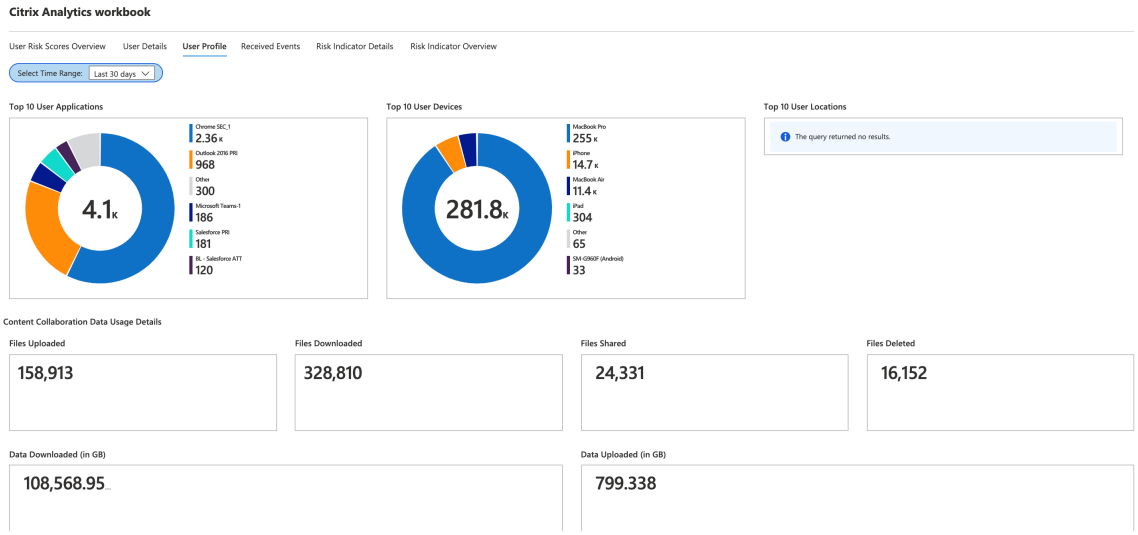
## Perfil de usuario

Este panel proporciona los detalles de las métricas de eventos asociadas a sus usuarios durante un período de tiempo seleccionado. Las métricas proporcionan información sobre las actividades de los usuarios, tales como:

- Las 10 aplicaciones más utilizadas por los usuarios
- Los 10 dispositivos más utilizados por los usuarios
- Las 10 ubicaciones principales desde las que los usuarios han iniciado sesión

Con los informes, puede:

- Identificar la tendencia de uso de sus usuarios
- Descubra los dispositivos no conformes que se utilizan para acceder a los recursos
- Compruebe si hay posibles accesos con riesgos de sus usuarios




## Eventos recibidos

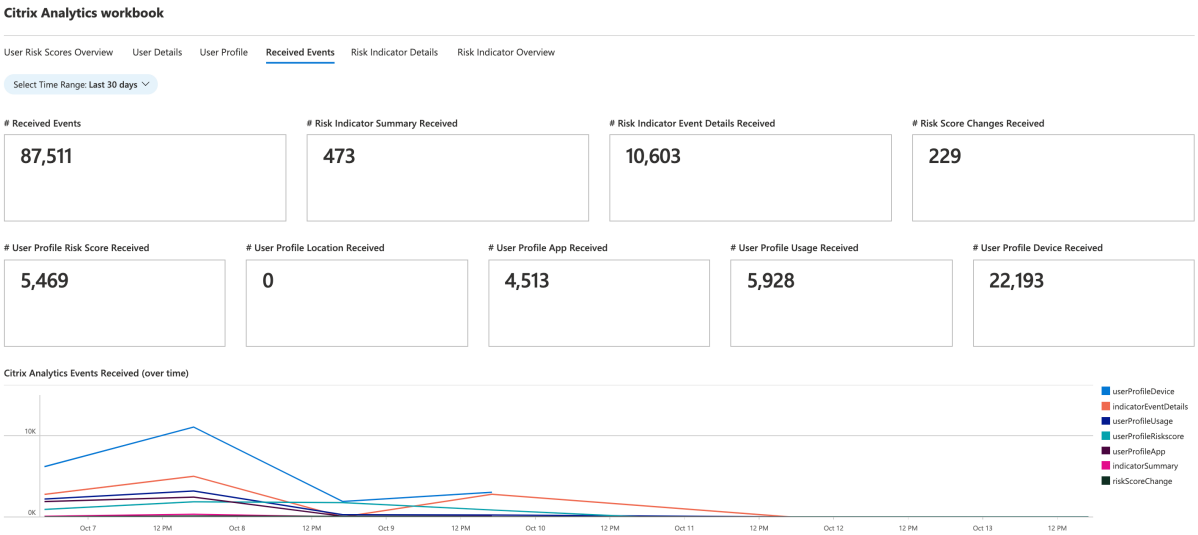
Durante un período de tiempo seleccionado, puede ver el número total de eventos recibidos de Citrix Analytics for Security. El total de eventos recibidos incluye lo siguiente:

- Resumen de indicadores de riesgo: indica los eventos asociados con el resumen de los indicadores de riesgo del usuario. Para obtener información sobre varios eventos de resumen de indicadores de riesgo, consulte Esquema de indicadores de riesgo.
- Detalles del evento indicador de riesgo: indica los eventos asociados con los detalles de los indicadores de riesgo del usuario. Para obtener información sobre varios eventos detallados de indicadores de riesgo, consulte Esquema de indicadores de riesgo.

- Puntuación de riesgo del perfil de usuario: indica los eventos asociados con la puntuación de riesgo de los usuarios. Para obtener información, consulte Panel de usuarios.
- Cambios en la puntuación de riesgo: indica los eventos asociados al cambio en la puntuación de riesgo de los usuarios Para obtener información, consulte Panel de usuarios.
- Ubicaciones del perfil de usuario: indica los eventos asociados a las ubicaciones desde las que los usuarios iniciaron sesión.
- Aplicación de perfil de usuario: indica los eventos asociados a las aplicaciones utilizadas por los usuarios.
- Uso del perfil de usuario: indica los eventos asociados con el uso de datos de los usuarios.
- Dispositivo de perfil de usuario: indica los eventos asociados a los dispositivos utilizados por los usuarios.

Al revisar el panel a intervalos regulares, puede asegurarse de que los eventos fluyan correctamente a su espacio de trabajo de Microsoft Sentinel. Cualquier discrepancia en el total de eventos recibidos puede indicar problemas de integración con Citrix Analytics for Security. Puede llevar a cabo los pasos necesarios para depurar los problemas.




## Detalles del indicador de riesgo

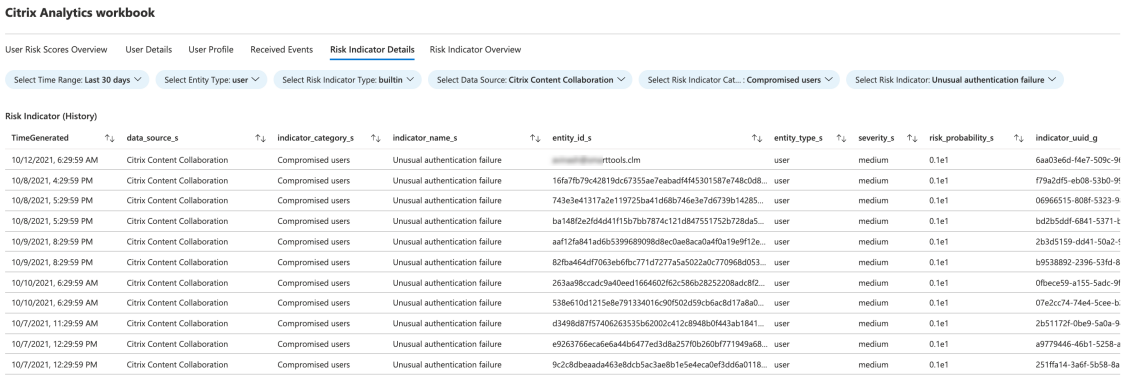
Este panel proporciona los detalles de los indicadores de riesgo activados por sus usuarios.

Puede ver los detalles del indicador de riesgo seleccionando una o más categorías:

- Rango de tiempo: seleccione un rango de tiempo para ver los detalles de los indicadores de riesgo activados durante el período.

- Tipo de entidad: seleccione un usuario para ver los detalles de los indicadores de riesgo asociados.
- Tipo de indicador de riesgo: seleccione indicadores de riesgo incorporados o personalizados para ver sus detalles.
- Fuente de datos: seleccione una fuente de datos para ver los indicadores de riesgo asociados.
- Categoría de indicador de riesgo: seleccione la categoría de riesgo para ver los indicadores de riesgo asociados.
- Indicador de riesgo: seleccione un indicador de riesgo por su nombre y vea sus detalles.




| TimeGenerated | data_source_s | indicator_category_s | indicator_name_s | entity_id_s | entity_type_s | severity_s | risk_probability_s | indicator_uuid_g |
|---|---|---|---|---|---|---|---|---|
| 10/12/2021, 6:29:59 AM | Citrix Content Collaboration | Compromised users | Unusual authentication failure | [redacted]rttools.clm | user | medium | 0.1e1 | 6aa03e6d-f4e7-509c-9 |
| 10/8/2021, 4:29:59 PM | Citrix Content Collaboration | Compromised users | Unusual authentication failure | 16fa7fb79c42819dc67355ae7eabadf4f45301587e748c0d8... | user | medium | 0.1e1 | f79a2df5-eb08-53b0-9 |
| 10/8/2021, 5:29:59 PM | Citrix Content Collaboration | Compromised users | Unusual authentication failure | 743e3e41317a2e119725ba41d68b746e3e7d6739b14285... | user | medium | 0.1e1 | 06966515-808f-5323-9 |
| 10/8/2021, 5:29:59 PM | Citrix Content Collaboration | Compromised users | Unusual authentication failure | ba148f2e2fd4d41f15b7bb7874c121d84755175 2b728da5... | user | medium | 0.1e1 | bd2b5ddf-6841-5371-b |
| 10/9/2021, 8:29:59 PM | Citrix Content Collaboration | Compromised users | Unusual authentication failure | aaf12fa841ad6b5399689098d8ec0ae8aca0a4f0a19e9f12e... | user | medium | 0.1e1 | 2b3d5159-dd41-50a2- |
| 10/9/2021, 8:29:59 PM | Citrix Content Collaboration | Compromised users | Unusual authentication failure | 82fba464df7063eb6fbc771d7277a5a5022a0c770968d053... | user | medium | 0.1e1 | b9538892-2396-53fd-8 |
| 10/10/2021, 6:29:59 AM | Citrix Content Collaboration | Compromised users | Unusual authentication failure | 263aa98ccadc9a40eed1664602f62c586b28252208adc8f2... | user | medium | 0.1e1 | 0fbece59-a155-5adc-9 |
| 10/10/2021, 6:29:59 AM | Citrix Content Collaboration | Compromised users | Unusual authentication failure | 538e610d1215e8e791334016c90f502d59cb6ac8d17a8a0... | user | medium | 0.1e1 | 07e2cc74-74e4-5cee-b |
| 10/7/2021, 11:29:59 AM | Citrix Content Collaboration | Compromised users | Unusual authentication failure | d3498d87f57406263535b62002c412c8948b0f443ab1841... | user | medium | 0.1e1 | 2b51172f-0be9-5a0a-9 |
| 10/7/2021, 12:29:59 PM | Citrix Content Collaboration | Compromised users | Unusual authentication failure | e9263766eca6e6a44b6477ed3d8a257f0b260bf771949a68... | user | medium | 0.1e1 | a9779446-46b1-5258-a |
| 10/7/2021, 12:29:59 PM | Citrix Content Collaboration | Compromised users | Unusual authentication failure | 9c2c8dbeaada463e8dcb5ac3ae8b1e5e4eca0ef3dd6a0118... | user | medium | 0.1e1 | 251ffa14-3a6f-5b58-8a |

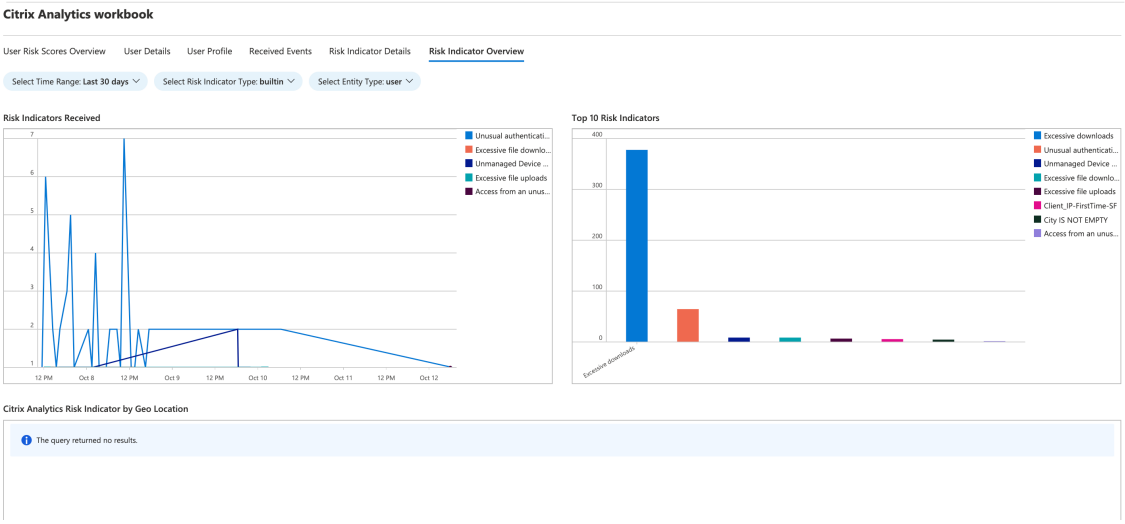
## Resumen de indicadores de riesgo

Este panel proporciona una vista consolidada de todos los indicadores de riesgo activados por sus usuarios.

Puede ver los indicadores de riesgo seleccionando una o más categorías:

- Rango de tiempo: seleccione un período de tiempo para ver los indicadores de riesgo que se activan durante ese período.
- Tipo de indicador de riesgo: seleccione integrado o personalizado para ver los indicadores de riesgo asociados.
- Tipo de entidad: seleccione cualquiera de los usuarios para ver los indicadores de riesgo asociados.




# Guía de solución de problemas para la integración de Sentinel a través de Logstash

May 2, 2023

En este artículo se enumeran los consejos que debe detectar para resolver un problema que puede surgir al integrar Microsoft Sentinel con Citrix Analytics mediante Logstash. Para obtener más información sobre el mismo, consulte Integración de SIEM mediante un conector de datos basado en Kafka o Logstash.

## Compruebe los registros del servidor Logstash

Puede comprobar los registros del servidor Logstash que aparecen en la ventana de su terminal para comprobar si los datos se han incorporado correctamente en las tablas de registro personalizadas de su espacio de trabajo de Sentinel.

1. Para ver los detalles del registro, debe descargar el archivo de configuración de Logstash desde **Configuración > Exportaciones de datos > pestaña Configuración ****** expandir el entorno**SIEM**. En**Azure Sentinel (versión preliminar)**, haga clic en**Descargar el archivo de configuración de Logstash**.
2. Una vez que inicie el servidor Logstash con el archivo de configuración, podrá buscar los siguientes registros en la misma ventana de terminal que indican que se ha conectado correctamente con el espacio de trabajo de Log Analytics alojado en Microsoft Azure.

```
Terminal                                Oct 27 00:25
group at generation 9: {logstash-0-3e65a1e3-e919-4b54-8ceb-6e77dc20b6c9=Assignment(partitions=[cas.siem.d62c49dd-1553-4e4b-978d-226
d4fbb27ec-0, cas.siem.d62c49dd-1553-4e4b-978d-226d4fbb27ec-1, cas.siem.d62c49dd-1553-4e4b-978d-226d4fbb27ec-2, cas.siem.d62c49dd-155
3-4e4b-978d-226d4fbb27ec-3])}
[2022-10-26T22:35:27,469][INFO ][org.apache.kafka.clients.consumer.internals.AbstractCoordinator][main][5fae264bdefa00973f7cc30ae7f9
30699fa3dee6a02a7876761dd62f778becd1] [Consumer clientId=logstash-0, groupId=splunkAdmin_gramh2zx04yk-group] Successfully synced gro
up in generation Generation{generationId=9, memberId='logstash-0-3e65a1e3-e919-4b54-8ceb-6e77dc20b6c9', protocol='range'}
[2022-10-26T22:35:27,470][INFO ][org.apache.kafka.clients.consumer.internals.ConsumerCoordinator][main][5fae264bdefa00973f7cc30ae7f9
30699fa3dee6a02a7876761dd62f778becd1] [Consumer clientId=logstash-0, groupId=splunkAdmin_gramh2zx04yk-group] Notifying assignor abou
t the new Assignment(partitions=[cas.siem.d62c49dd-1553-4e4b-978d-226d4fbb27ec-0, cas.siem.d62c49dd-1553-4e4b-978d-226d4fbb27ec-1, c
as.siem.d62c49dd-1553-4e4b-978d-226d4fbb27ec-2, cas.siem.d62c49dd-1553-4e4b-978d-226d4fbb27ec-3])
[2022-10-26T22:35:27,472][INFO ][org.apache.kafka.clients.consumer.internals.ConsumerCoordinator][main][5fae264bdefa00973f7cc30ae7f9
30699fa3dee6a02a7876761dd62f778becd1] [Consumer clientId=logstash-0, groupId=splunkAdmin_gramh2zx04yk-group] Adding newly assigned p
artitions: cas.siem.d62c49dd-1553-4e4b-978d-226d4fbb27ec-1, cas.siem.d62c49dd-1553-4e4b-978d-226d4fbb27ec-2, cas.siem.d62c49dd-1553-
4e4b-978d-226d4fbb27ec-0, cas.siem.d62c49dd-1553-4e4b-978d-226d4fbb27ec-3
[2022-10-26T22:35:27,725][INFO ][org.apache.kafka.clients.consumer.internals.ConsumerCoordinator][main][5fae264bdefa00973f7cc30ae7f9
30699fa3dee6a02a7876761dd62f778becd1] [Consumer clientId=logstash-0, groupId=splunkAdmin_gramh2zx04yk-group] Setting offset for part
ition cas.siem.d62c49dd-1553-4e4b-978d-226d4fbb27ec-1 to the committed offset FetchPosition{offset=0, offsetEpoch=Optional.empty, cu
rrentLeader=LeaderAndEpoch{leader=Optional[20.242.21.84:9094 (id: 3 rack: null)], epoch=absent}}
[2022-10-26T22:35:27,725][INFO ][org.apache.kafka.clients.consumer.internals.ConsumerCoordinator][main][5fae264bdefa00973f7cc30ae7f9
30699fa3dee6a02a7876761dd62f778becd1] [Consumer clientId=logstash-0, groupId=splunkAdmin_gramh2zx04yk-group] Setting offset for part
ition cas.siem.d62c49dd-1553-4e4b-978d-226d4fbb27ec-2 to the committed offset FetchPosition{offset=504, offsetEpoch=Optional.empty,
currentLeader=LeaderAndEpoch{leader=Optional[20.98.232.61:9094 (id: 4 rack: null)], epoch=absent}}
[2022-10-26T22:35:27,726][INFO ][org.apache.kafka.clients.consumer.internals.ConsumerCoordinator][main][5fae264bdefa00973f7cc30ae7f9
30699fa3dee6a02a7876761dd62f778becd1] [Consumer clientId=logstash-0, groupId=splunkAdmin_gramh2zx04yk-group] Setting offset for part
ition cas.siem.d62c49dd-1553-4e4b-978d-226d4fbb27ec-0 to the committed offset FetchPosition{offset=0, offsetEpoch=Optional.empty, cu
rrentLeader=LeaderAndEpoch{leader=Optional[20.242.57.140:9094 (id: 6 rack: null)], epoch=absent}}
[2022-10-26T22:35:27,726][INFO ][org.apache.kafka.clients.consumer.internals.ConsumerCoordinator][main][5fae264bdefa00973f7cc30ae7f9
30699fa3dee6a02a7876761dd62f778becd1] [Consumer clientId=logstash-0, groupId=splunkAdmin_gramh2zx04yk-group] Setting offset for part
ition cas.siem.d62c49dd-1553-4e4b-978d-226d4fbb27ec-3 to the committed offset FetchPosition{offset=0, offsetEpoch=Optional.empty, cu
rrentLeader=LeaderAndEpoch{leader=Optional[20.242.21.108:9094 (id: 5 rack: null)], epoch=absent}}
[2022-10-27T00:24:06,953][INFO ][logstash.outputs.azureloganalytics][main][e175a2e3e3ff640c81735fb3814cba6ac18f778632db23ee93f4a609c
e880073] Changing buffer size.[configuration='2000' , new size='1000']
[2022-10-27T00:24:12,208][INFO ][logstash.outputs.azureloganalytics][main][e175a2e3e3ff640c81735fb3814cba6ac18f778632db23ee93f4a609c
e880073] Successfully posted 1 logs into custom log analytics table[CitrixAnalytics_indicatorSummary].
```

## Error común: uso de JDK empaquetado

Al intentar instalar el complemento de análisis de registros de Microsoft, se informa de un error común que se muestra a continuación:

```
Administrator: Command Prompt

C:\windows\system32>C:\logstash-7.16.1\bin\logstash-plugin install microsoft-logstash-output-azure-loganalytics
"Using bundled JDK: ."

C:\windows\system32>_
```

Después de esto, al intentar ejecutar el servidor Logstash, es posible que aparezca el siguiente error:

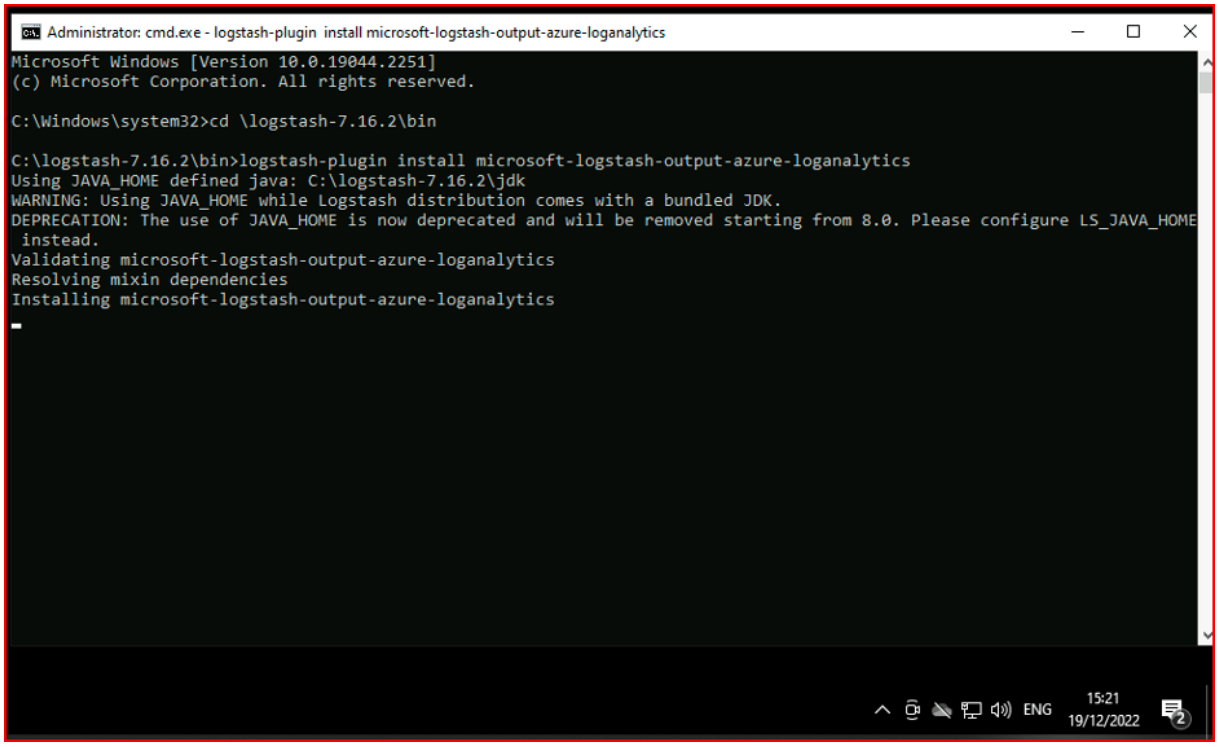
```
Administrator: Command Prompt
a future release.
Sending Logstash logs to C:/logstash-7.16.2/logs which is now configured via log4j2.properties
[2022-12-16T16:07:29,238][INFO ][logstash.runner          ] Log4j configuration path used is: C:\logstash-7.16.2\config\
log4j2.properties
[2022-12-16T16:07:29,286][INFO ][logstash.runner          ] Starting Logstash {"logstash.version"=>"7.16.2", "jruby.vers
ion"=>"jruby 9.2.20.1 (2.5.8) 2021-11-30 2a2962fbd1 OpenJDK 64-Bit Server VM 11.0.13+8 on 11.0.13+8 +indy +jit [mswin32-
x86_64]"}
[2022-12-16T16:07:29,820][WARN ][logstash.config.source.multilocal] Ignoring the 'pipelines.yml' file because modules or
 command line options are specified
[2022-12-16T16:07:41,913][INFO ][logstash.agent           ] Successfully started Logstash API endpoint {:port=>9600, :ss
l_enabled=>false}
[2022-12-16T16:07:50,497][INFO ][org.reflections.Reflections] Reflections took 454 ms to scan 1 urls, producing 119 keys
 and 417 values
[2022-12-16T16:07:57,617][ERROR][logstash.plugins.registry] Unable to load plugin. {:type=>"output", :name=>"microsoft-l
ogstash-output-azure-loganalytics"}
[2022-12-16T16:07:57,717][ERROR][logstash.agent           ] Failed to execute action {:action=>LogStash::PipelineAction:
:Create/pipeline_id:main, :exception=>"Java::JavaLang::IllegalStateException", :message=>"Unable to configure plugins: (
PluginLoadingError) Couldn't find any output plugin named 'microsoft-logstash-output-azure-loganalytics'. Are you sure t
his is correct? Trying to load the microsoft-logstash-output-azure-loganalytics output plugin resulted in this error: Un
able to load the requested plugin named microsoft-logstash-output-azure-loganalytics of type output. The plugin is not i
nstalled.", :backtrace=>["org.logstash.config.ir.CompiledPipeline.<init>(CompiledPipeline.java:119)", "org.logstash.exec
ution.JavaBasePipelineExt.initialize(JavaBasePipelineExt.java:86)", "org.logstash.execution.JavaBasePipelineExt$INVOKER$
```

Para resolver este problema, defina JAVA_HOME en el JDK incluido:

1. Ir a Variables de entorno de Windows
2. Cree una nueva variable de sistema con el nombre «JAVA_HOME»
3. < path_to_logstash >Añada la ruta al JDK Logstash incluido (/logstash-x.x.x/jdk)

Tras realizar los pasos anteriores, al intentar instalar de nuevo el complemento, aparece la siguiente pantalla:




Si usa LS_JAVA_HOME (ya que JAVA_HOME está en desuso), también debe especificar la ubicación del JDK incluido en la variable PATH del sistema, y esta ruta debe apuntar a la carpeta **jdk\bin** (a diferencia de la variable LS_JAVA_HOME):

```
Administrator: cmd.exe - logstash-plugin install microsoft-logstash-output-azure-loganalytics
Microsoft Windows [Version 10.0.19044.2251]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd \logstash-7.16.2\bin

C:\logstash-7.16.2\bin>logstash-plugin install microsoft-logstash-output-azure-loganalytics
Using JAVA_HOME defined java: C:\logstash-7.16.2\jdk
WARNING: Using JAVA_HOME while Logstash distribution comes with a bundled JDK.
DEPRECATION: The use of JAVA_HOME is now deprecated and will be removed starting from 8.0. Please configure LS_JAVA_HOME
 instead.
Validating microsoft-logstash-output-azure-loganalytics
Resolving mixin dependencies
Installing microsoft-logstash-output-azure-loganalytics
```

Si usa LS_JAVA_HOME (ya que JAVA_HOME está en desuso), también debe especificar la ubicación del JDK incluido en la variable PATH del sistema, y esta ruta debe apuntar a la carpeta **jdk\bin** (a diferencia de la variable LS_JAVA_HOME):

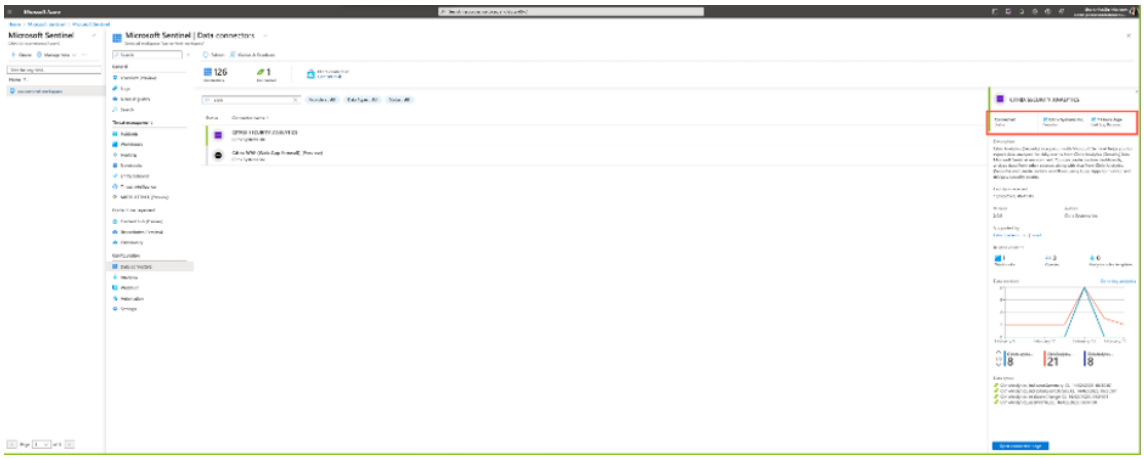
```
Administrator: Command Prompt - C:\logstash-7.16.2\bin\logstash.bat -f C:\logstash-7.16.2\config\CAS_AzureSentinel_LogStash_Config.conf

C:\logstash-7.16.2\bin>set path
Path=C:\windows\system32;C:\windows;C:\windows\System32\Wbem;C:\windows\System32\WindowsPowerShell\v1.0\;C:\windows\Syst
em32\OpenSSH\;C:\logstash-7.16.2\jdk\bin;C:\Users\ltc_simonw\AppData\Local\Microsoft\WindowsApps
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH;.MSC

C:\logstash-7.16.2\bin>set ls
LS_JAVA_HOME=C:\logstash-7.16.2\jdk

C:\logstash-7.16.2\bin>C:\logstash-7.16.2\bin\logstash.bat -f C:\logstash-7.16.2\config\CAS_AzureSentinel_LogStash_Confi
g.conf
Using LS_JAVA_HOME defined java: C:\logstash-7.16.2\jdk
WARNING: Using LS_JAVA_HOME while Logstash distribution comes with a bundled JDK.
OpenJDK 64-Bit Server VM warning: Option UseConcMarkSweepGC was deprecated in version 9.0 and will likely be removed in
a future release.
Sending Logstash logs to C:/logstash-7.16.2/logs which is now configured via log4j2.properties
[2022-12-19T16:04:08,918][INFO ][logstash.runner          ] Log4j configuration path used is: C:\logstash-7.16.2\config\
log4j2.properties
[2022-12-19T16:04:08,978][INFO ][logstash.runner          ] Starting Logstash {"logstash.version"=>"7.16.2", "jruby.vers
ion"=>"jruby 9.2.20.1 (2.5.8) 2021-11-30 2a2962fbd1 OpenJDK 64-Bit Server VM 11.0.13+8 on 11.0.13+8 +indy +jit [mswin32-
x86_64]"}
```

## Consulte el libro de trabajo de Microsoft Sentinel

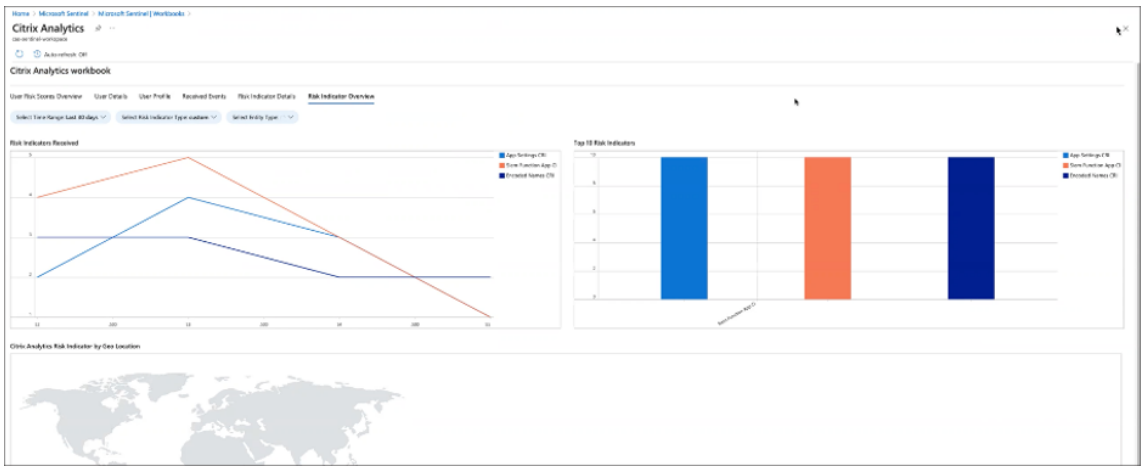
Para confirmar si los datos enviados por Citrix Analytics se han introducido correctamente en la tabla de registro personalizada correspondiente del espacio de trabajo de Log Analytics (para obtener más información sobre la integración de Microsoft Sentinel con Citrix Analytics, consulte la integración de Microsoft Sentinel):

1. Vaya al **portal de Azure > Microsoft Sentinel > Seleccione appropriate workspace > Conectores de datos >** seleccione **Citrix Security Analytics** y haga clic en él.
2. Compruebe la barra superior para comprobar el estado de la conectividad.



3. En los libros de trabajo, puede utilizar filtros intuitivos para profundizar en los datos y obtener la información del indicador de riesgo. Para obtener la información, vaya al **portal de Azure > Microsoft Sentinel > Conectores de datos > CITRIX SECURITY ANALYTICS >**Libros de trabajo.



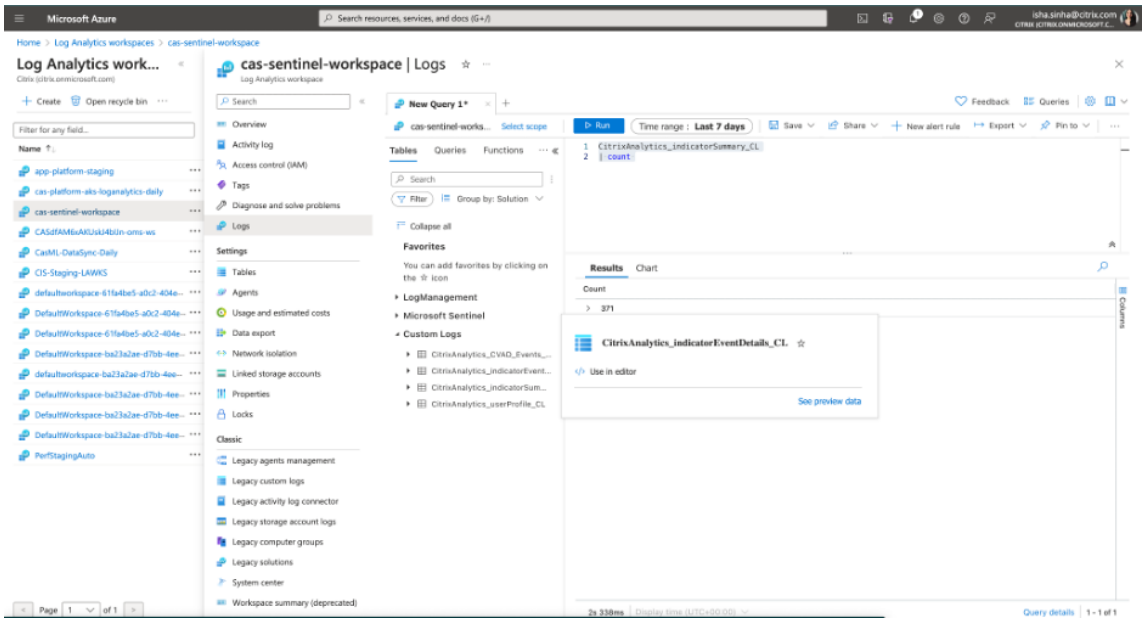

## Compruebe los registros del espacio de trabajo de Log Analytics con KQL

También puede comprobar si los datos correctos llegaron a su espacio de trabajo de LogAnalytics ejecutando consultas de KQL en las tablas de registro personalizadas respectivas.

1. Vaya al **portal de Azure > Áreas de trabajo de Log Analytics** y busque el espacio de trabajo correcto.
2. En el panel izquierdo, selecciona **Registros** y busca la tabla de análisis de registros personalizada en la pestaña **Tablas**.

3. Seleccione la tabla de análisis de registros personalizada y haga clic **en Usar en el editor**. (Para obtener información sobre las consultas de KQL en el espacio de trabajo de Log Analytics, consulte el tutorial de Log Analytics).
4. Haga clic en **Ejecutar**.




## Integración de Elasticsearch

November 17, 2023

> **Nota**
>
> Contacte con CAS-PM-Ext@cloud.com para solicitar ayuda para la integración de Elasticsearch, la exportación de datos a Elasticsearch o para enviar comentarios.

Integre Citrix Analytics for Security con Elasticsearch mediante el motor Logstash. Esta integración le permite exportar y correlacionar los datos de los usuarios de su entorno de TI de Citrix con Elasticsearch y obtener información más profunda sobre la postura de seguridad de su organización. También puede usar Elasticsearch con los servicios de visualización y los SIEMs como Kibana y LogRhythm respectivamente.

Para obtener más información sobre los beneficios de la integración y el tipo de datos procesados que se envían a su SIEM, consulte Integración de la información de seguridad y la gestión de eventos.

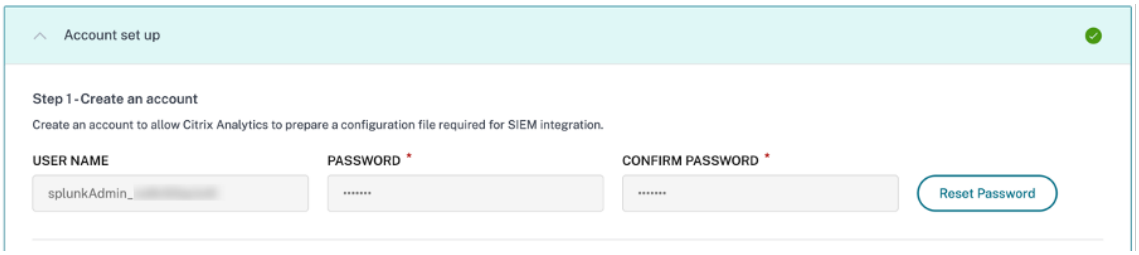
### Requisitos previos

- Active el procesamiento de datos para al menos un origen de datos. Ayuda a Citrix Analytics for Security a iniciar el proceso de integración de Elasticsearch.
- Asegúrese de que el siguiente punto de enlace esté en la lista de permitidos en su red.

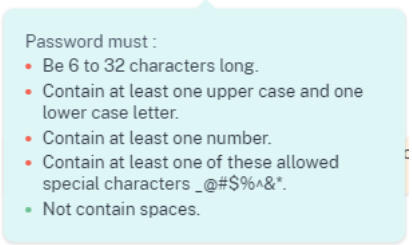
| Dispositivo de punto final | Región de los Estados Unidos | Región de la Unión Europea | Región Asia-Pacífico Sur |
|---|---|---|---|
| Intermediarios de Kafka | casnb-0.citrix.com:9094<br>casnb-1.citrix.com:9094<br>casnb-2.citrix.com:9094<br>casnb-3.citrix.com:9094 | casnb-eu-0.citrix.com:9094<br>casnb-eu-1.citrix.com:9094<br>casnb-eu-2.citrix.com:9094 | casnb-aps-0.citrix.com:9094<br>casnb-aps-1.citrix.com:9094<br>casnb-aps-2.citrix.com:9094 |

### Integración con Elasticsearch

1. Ve a **Configuración > Exportaciones de datos**.
2. En la sección **Configuración de la cuenta**, cree una cuenta especificando el nombre de usuario y la contraseña. Esta cuenta se usa para preparar un archivo de configuración, que se requiere para la integración.

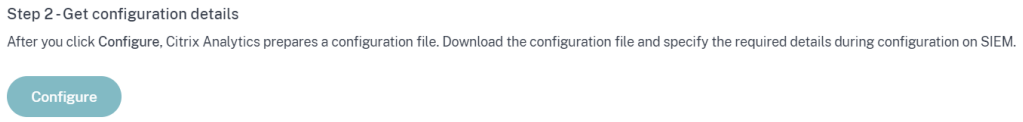



3. Asegúrese de que la contraseña cumpla con las siguientes condiciones:



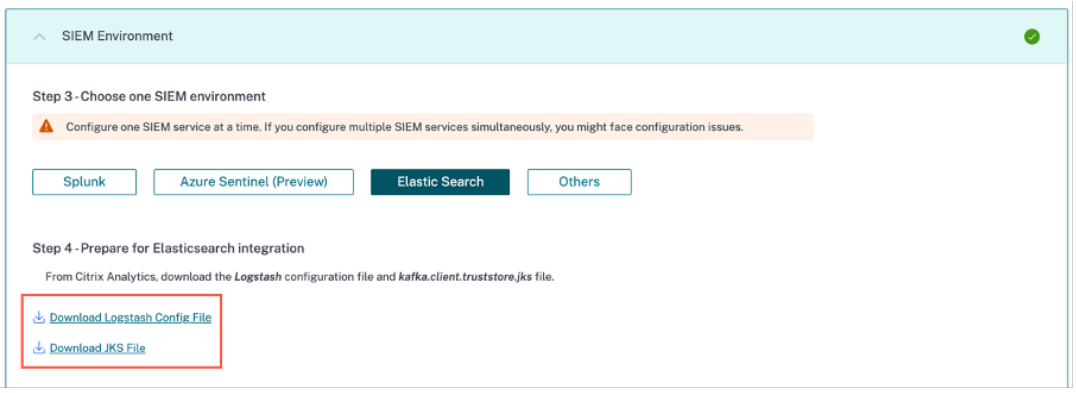
4. Haga clic en **Configurar** para generar el archivo de configuración de Logstash.




5. Seleccione la ficha **Elastic Search** de la sección Entorno de SIEM para descargar los archivos de configuración:

   - **Archivo de configuración de Logstash**: contiene los datos de configuración (secciones de entrada, filtro y salida) para enviar eventos desde Citrix Analytics for Security a Elasticsearch mediante el motor de recopilación de datos Logstash. Para obtener información sobre la estructura de archivos de configuración de Logstash, consulte la documentación de Logstash.
   - **Archivo JKS**: contiene los certificados necesarios para la conexión SSL.

   > **Nota**
   >
   > Estos archivos contienen información confidencial. Manténgalos en un lugar seguro y protegido.




6. Configurar Logstash:

   a) En su máquina host Linux o Windows, instale Logstash. También puede usar su instancia de Logstash existente.

   b) En la máquina host donde ha instalado Logstash, coloque los siguientes archivos en el directorio especificado:

| Tipo de máquina host | Nombre de archivo | Ruta del directorio |
|---|---|---|
| Linux | CAS_Elasticsearch_LogStash_Config.conf | Para paquetes Debian y RPM: `/etc/logstash/conf.d/`<br>Para archivos.zip y.tar.gz: `{ extract.path } /config` |
| | kafka.client.truststore.jks | Para paquetes Debian y RPM: `/etc/logstash/ssl/`<br>Para archivos.zip y.tar.gz: `{ extract.path } /ssl` |
| Windows | CAS_Elasticsearch_LogStash_Config.conf | `C:\logstash-7.xx.x\config` |
| | kafka.client.truststore.jks | |

Para obtener información sobre la estructura de directorios predeterminada de los paquetes de instalación de Logstash, consulte la documentación de Logstash.

c) Abra el archivo de configuración de Logstash y haga lo siguiente:

i. En la sección de entrada del archivo, introduzca la siguiente información:

- **Contraseña**: la contraseña de la cuenta que creó en Citrix Analytics for Security para preparar el archivo de configuración.
- **Ubicación del almacén de confianza SSL**: la ubicación de su certificado de cliente SSL. Esta es la ubicación del archivo kafka.client.truststore.jks en su máquina host.

```
input {
  kafka {
    bootstrap_servers => "[redacted]"
    topics => ["[redacted]"]
    group_id => "[redacted]"
    session_timeout_ms => 60000
    auto_offset_reset => "earliest"
    security_protocol => "SASL_SSL"
    sasl_mechanism => "SCRAM-SHA-256"
    ssl_endpoint_identification_algorithm => ""
    sasl_jaas_config => "org.apache.kafka.common.security.scram.ScramLoginModule required username='[redacted]' password='<your password>';"
    ssl_truststore_location => "/etc/logstash/ssl/kafka.client.truststore.jks"
  }
```

ii. En la sección de salida del archivo, introduzca la dirección de su máquina host o del clúster donde se ejecuta Elasticsearch.

```
  }
output {
  elasticsearch {
    hosts => ["<your logstash host : port>"]
    index => "citrixanalytics-%{+YYYY.MM.dd}"
  }
}
```

d) Reinicie su máquina host para enviar los datos procesados de Citrix Analytics for Security a Elasticsearch.

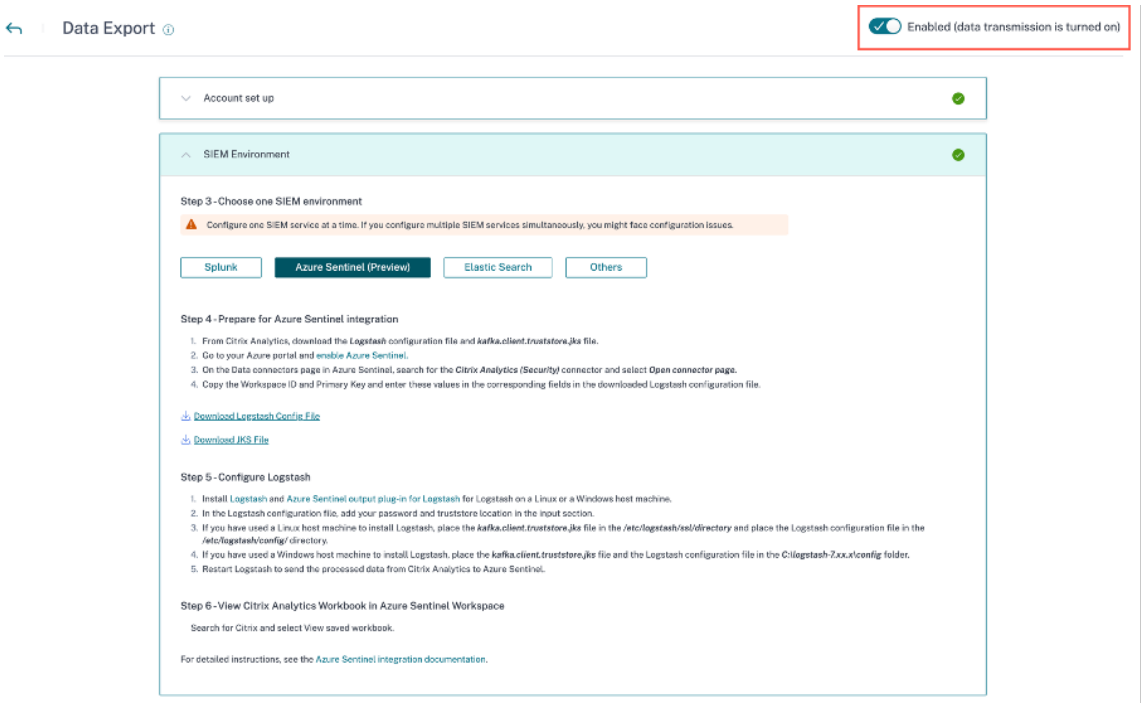
Una vez completada la configuración, compruebe que puede ver los datos de Citrix Analytics en su Elasticsearch.

## Activar o desactivar la transmisión de datos

Después de que Citrix Analytics for Security prepare el archivo de configuración, se activa la transmisión de datos para Elasticsearch.

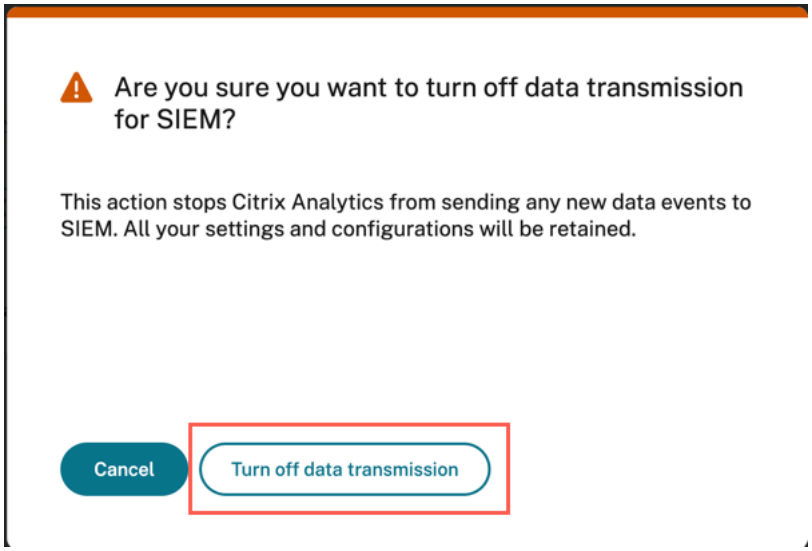
Para dejar de transmitir datos de Citrix Analytics for Security:

1. Ve a **Configuración > Exportaciones de datos**.
2. Apague el botón para desactivar la transmisión de datos. De forma predeterminada, la **transmisión de datos** siempre está habilitada.



Aparece una ventana de advertencia para su confirmación. Haga clic en el botón **Desactivar la transmisión de datos** para detener la actividad de transmisión.




Para habilitar de nuevo la transmisión de datos, active el botón.

## Integración de SIEM mediante conector de datos basado en Kafka o Logstash

November 17, 2023

La integración con SIEM de Citrix Analytics for Security le permite exportar y correlacionar los datos de los usuarios de Citrix Analytics con su entorno SIEM y obtener información más detallada sobre la postura de seguridad de su organización.

Para obtener más información sobre las ventajas de la integración y el tipo de eventos de datos (información sobre el riesgo y eventos de la fuente de datos) que se envían a su SIEM, consulte Integración de información de seguridad y administración de eventos.

Puede integrar Citrix Analytics for Security con sus soluciones de SIEM mediante los dos mecanismos siguientes (compatibles con su implementación de SIEM y TI):

1. Conéctese a través de puntos finales de Kafka
2. Conéctese a través del agente de datos Logstash con ingestión basada en Kafka

### Requisitos previos

- Active el procesamiento de datos para al menos un origen de datos. Ayuda a Citrix Analytics for Security a iniciar la integración con la herramienta SIEM.
- Asegúrese de que el siguiente punto de enlace esté en la lista de permitidos en su red.

| Dispositivo de punto final | Región de los Estados Unidos | Región de la Unión Europea | Región Asia-Pacífico Sur |
|---|---|---|---|
| Intermediarios de Kafka | casnb-0.citrix.com:9094<br>casnb-1.citrix.com:9094<br>casnb-2.citrix.com:9094<br>casnb-3.citrix.com:9094 | casnb-eu-0.citrix.com:9094<br>casnb-eu-1.citrix.com:9094<br>casnb-eu-2.citrix.com:9094 | casnb-aps-0.citrix.com:9094<br>casnb-aps-1.citrix.com:9094<br>casnb-aps-2.citrix.com:9094 |

### Realice la integración con un servicio SIEM mediante Kafka

Kafka es un software de código abierto que se utiliza para la transmisión de datos en tiempo real. Con Kafka, puede analizar los datos en tiempo real para obtener información más rápida. En su mayoría, las grandes organizaciones que manejan datos adecuados utilizan Kafka.

Northbound Kafka es una capa intermedia interna que permite a Citrix Analytics compartir fuentes de datos en tiempo real con los clientes de SIEM a través de puntos de conexión de Kafka. Si su SIEM admite puntos de enlace de Kafka, utilice los parámetros proporcionados en el archivo de configuración de Logstash y los detalles del certificado en el archivo JKS o el archivo PEM para integrar su SIEM con Citrix Analytics for Security.

Se requieren los siguientes parámetros para integrar Kafka:

| Nombre de atributo | Descripción | Ejemplo de datos de configuración |
|---|---|---|
| Nombre de usuario | Nombre de usuario proporcionado por Kafka. | `'sasl.username': cas_siem_user_name,` |
| Host | Nombre de host del servidor de Kafka al que desea conectarse. | `'bootstrap.servers': cas_siem_host,` |

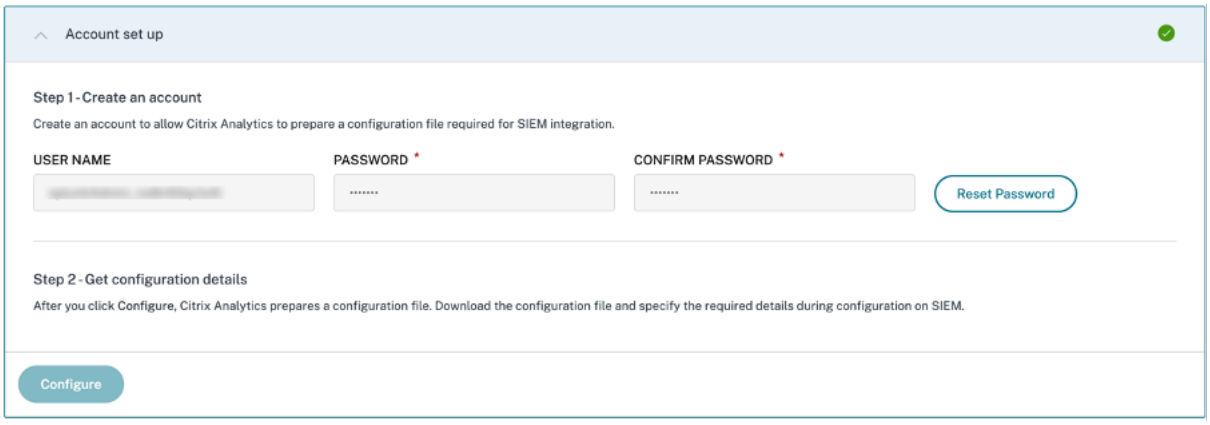
| Nombre de atributo | Descripción | Ejemplo de datos de configuración |
|---|---|---|
| Nombre del tema/ID de cliente | ID de cliente asignada a cada arrendatario. | `'client.id': cas_siem_topic,` |
| Nombre/ID del grupo | Nombre del grupo que necesita para leer los mensajes compartidos por los consumidores. | `'group.id': cas_siem_group_id,` |
| Protocolo de seguridad | Nombre del protocolo de seguridad. | `'security.protocol': 'SASL_SSL',` |
| mecanismos SASL | Mecanismo de autenticación que se utiliza normalmente para el cifrado a fin de implementar una autenticación segura. | `'sasl.mechanisms': 'SCRAM-SHA-256',` |
| Ubicación de truststore de SSL | Ubicación en la que puede almacenar el archivo de certificado. La contraseña de truststore del cliente es opcional y se espera que quede vacía. | `'ssl.ca.location': ca_location` |
| Tiempo de espera de la sesión | El tiempo de espera de la sesión utilizado para detectar errores del cliente al usar Kafka. | `'session.timeout.ms': 60000,` |
| Restablecimiento de compensación automática | Define el comportamiento al consumir datos de una partición de temas cuando no hay ningún desplazamiento inicial. Puede establecer valores como, último, más antiguo o ninguno. | `'auto.offset.reset': 'earliest',` |

A continuación se muestra un ejemplo de salida de configuración:

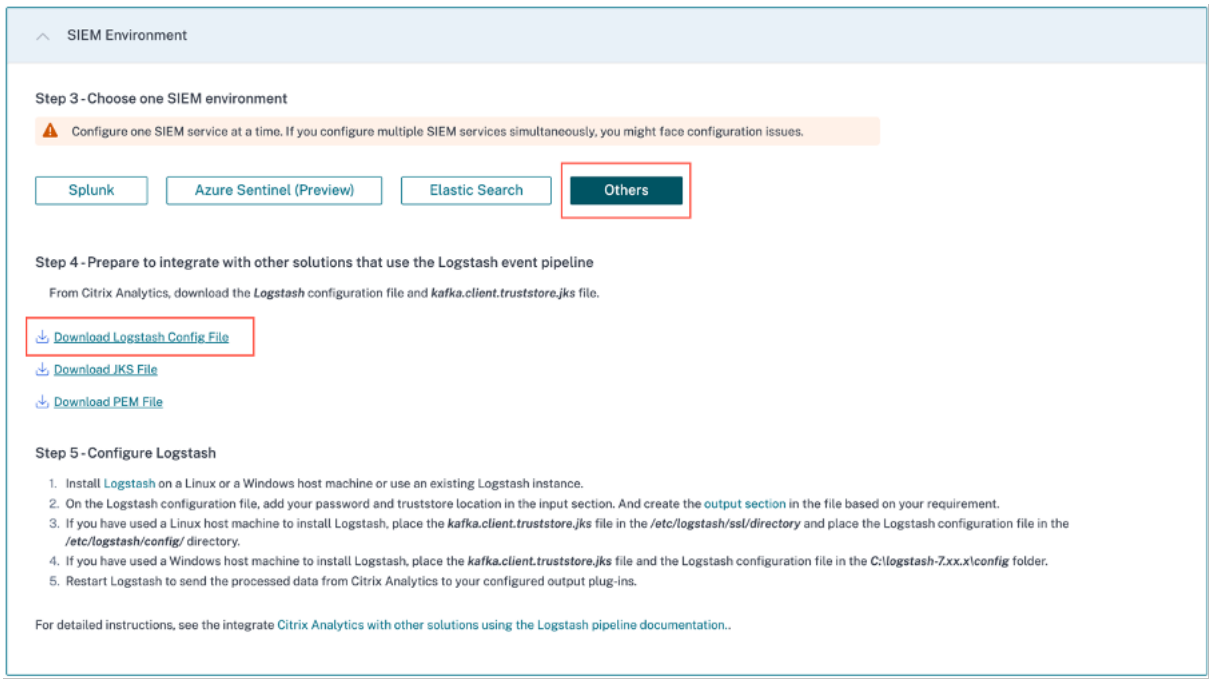
```
{
 'bootstrap.servers': cas_siem_host,
                      'client.id': cas_siem_topic,
                      'group.id': cas_siem_group_id,
                      'session.timeout.ms': 60000,
```

```
                    'auto.offset.reset': 'earliest',
                    'security.protocol': 'SASL_SSL',
                    'sasl.mechanisms': 'SCRAM-SHA-256',
                    'sasl.username': cas_siem_user_name,
                    'sasl.password': self.CLEAR_PASSWORD,
                    'ssl.ca.location': ca_location
                }
```




Los parámetros antes mencionados están disponibles en el archivo de configuración de Logstash. Para descargar el archivo de configuración, vaya a **Configuración > Exportaciones de datos > Entorno SIEM** seleccione la ficha **Otros** > haga clic en **Descargar archivo de configuración de Logstash**.




Para entender o saber más acerca de los valores de configuración, consulte Configuración.

### Flujo de datos

La comunicación de datos de autenticación se produce entre los Brokers del lado del servidor de Kafka (Citrix Analytics for Security cloud) y los clientes de Kafka. Todas las comunicaciones entre intermediarios y clientes externos utilizan el protocolo de seguridad SASL_SSL habilitado y el puerto 9094 de destino para el acceso público.

Apache Kafka tiene un componente de seguridad para cifrar los datos en vuelo mediante el cifrado SSL.
La transmisión de datos a través de la red se cifra y se protege cuando se habilita el cifrado y se configuran los certificados SSL. Solo la primera y la última máquina poseen la capacidad de descifrar los paquetes que se envían a través de SSL.

### Autenticaciones

Hay dos niveles de autenticación disponibles, como se indica a continuación:

1. TLS/entre el cliente y el servidor.
    - Los certificados de servidor (claves públicas) para el intercambio de autenticación TLS entre el cliente y el servidor.
    - No se admite la autenticación basada en el cliente ni las autenticaciones bidireccionales (cuando se requieren certificados de clave privada del cliente).
2. Nombre de usuario/contraseña para el control de acceso a los temas/puntos finales
    - Garantiza que un cliente específico solo pueda leer un tema específico del cliente
    - El SASL/SCRAM se utiliza para el mecanismo de autenticación de nombre de usuario y contraseña junto con el cifrado TLS para implementar la autenticación segura.

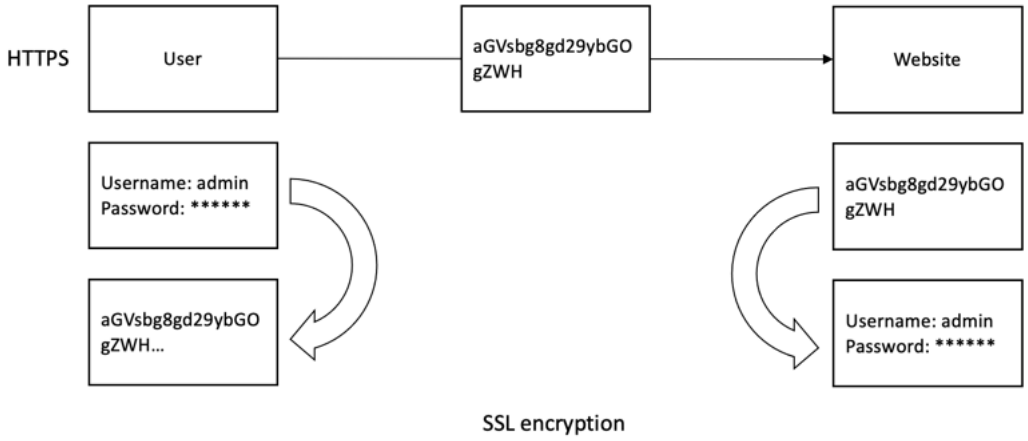
### Cifrado con SSL y autenticación con SASL/SSL y SASL/PLAINTEXT

De forma predeterminada, Apache Kafka se comunica en formato PLAINTEXT, donde todos los datos se envían sin cifrar y cualquiera de los enrutadores puede leer el contenido de los datos. Apache Kafka tiene un componente de seguridad para cifrar los datos en vuelo mediante el cifrado SSL. Con el cifrado activado y los certificados SSL cuidadosamente configurados, los datos ahora se cifran y se transmiten de forma segura a través de la red. Con el cifrado SSL, solo la primera y la última máquina tienen la capacidad de descifrar el paquete que se envía.

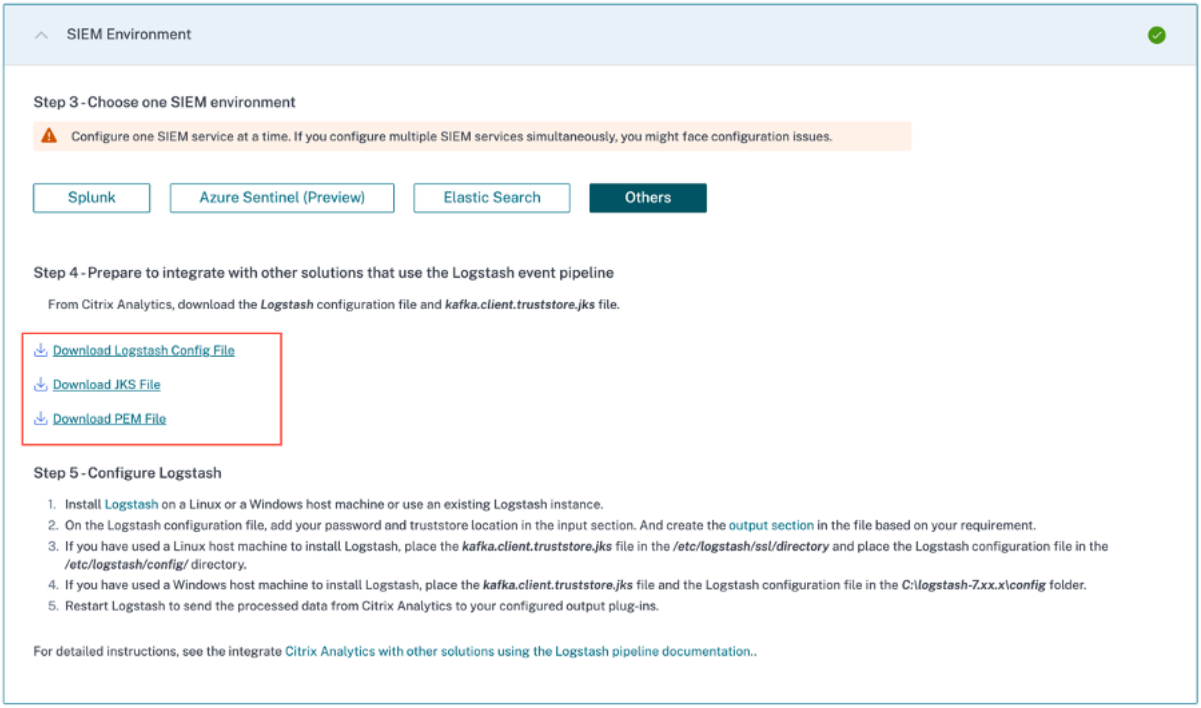
Dado que se utiliza el cifrado SSL bidireccional, el inicio de sesión con nombre de usuario/contraseña es seguro para las comunicaciones externas.

El cifrado solo se realiza durante el vuelo y los datos aún permanecen sin cifrar en el disco del intermediario.




En la configuración del cliente, se requieren el archivo JKS y el archivo PEM del cliente (convertidos del archivo truststore jks). Puede descargar estos archivos desde la GUI de Citrix Analytics for Security, como se muestra en la siguiente captura de pantalla:




## Integración de SIEM mediante Logstash

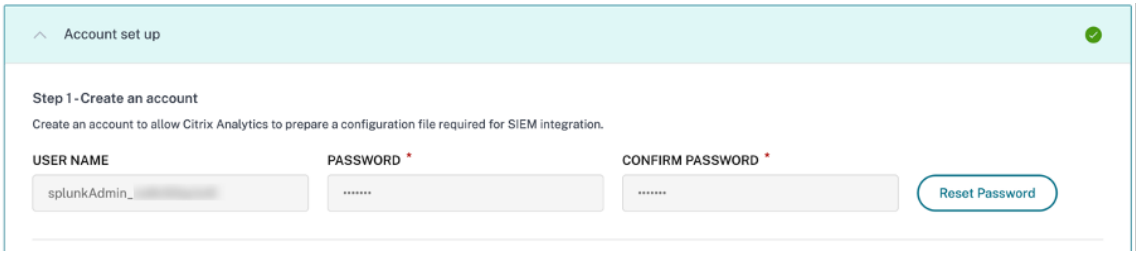
Si su SIEM no admite puntos finales de Kafka, puede utilizar el motor de recopilación de **datos Logstash**. Puede enviar los eventos de datos desde Citrix Analytics for Security a uno de los complementos de salida compatibles con Logstash.

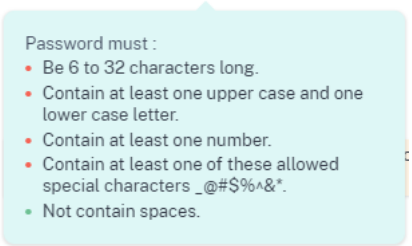
En la siguiente sección se describen los pasos que debe seguir para integrar su SIEM con Citrix Analytics for Security mediante Logstash.

## Integración con un servicio SIEM mediante Logstash

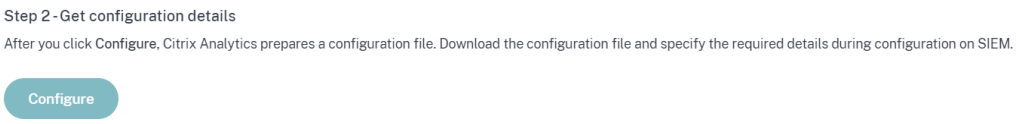
1. Ve a **Configuración > Exportaciones de datos**.
2. En la página **Configuración de la cuenta**, cree una cuenta especificando el nombre de usuario y la contraseña. Esta cuenta se usa para preparar un archivo de configuración, que se requiere para la integración.




3. Asegúrese de que la contraseña cumpla con las siguientes condiciones:




4. Seleccione **Configurar** para generar el archivo de configuración de Logstash.

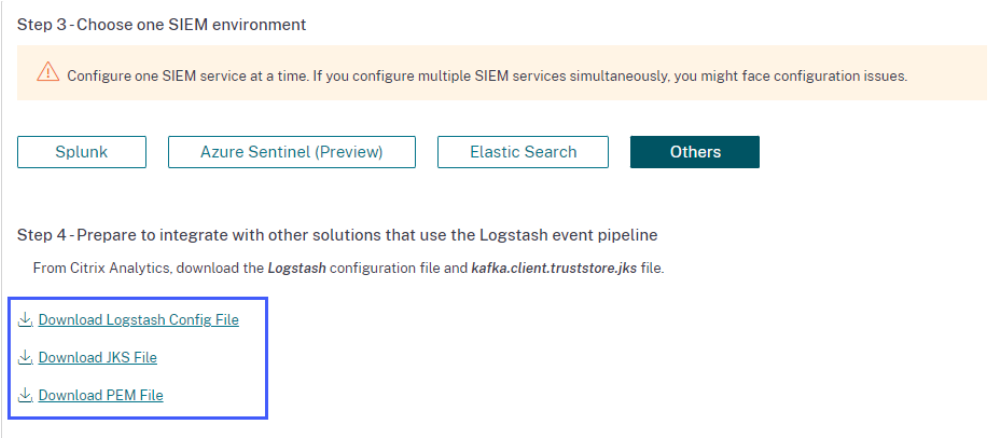



5. Seleccione la ficha **Otros** para descargar los archivos de configuración.
   - **Archivo de configuración de Logstash**: este archivo contiene los datos de configuración (secciones de entrada, filtro y salida) para enviar eventos desde Citrix Analytics for Security mediante el motor de recopilación de datos Logstash. Para obtener información sobre la estructura de archivos de configuración de Logstash, consulte la documentación de Logstash.
   - **Archivo JKS**: este archivo contiene los certificados necesarios para la conexión SSL. Este archivo es obligatorio cuando integras su SIEM con Logstash.

- **Archivo PEM**: este archivo contiene los certificados necesarios para la conexión SSL. Este archivo es obligatorio al integrar su SIEM con Kafka.

> **Nota**
>
> Estos archivos contienen información confidencial. Manténgalos en un lugar seguro y protegido.




6. Configurar Logstash:

   a) En su máquina host de Linux o Windows, instale Logstash (versiones probadas de compatibilidad con Citrix Analytics for Security: v7.17.7 y v8.5.3). También puede usar su instancia de Logstash existente.

   b) En la máquina host donde ha instalado Logstash, coloque los siguientes archivos en el directorio especificado:

| Tipo de máquina host | Nombre de archivo | Ruta del directorio |
|---|---|---|
| Linux | CAS_Others_LogStash_Config.conf | Para paquetes Debian y RPM: `/etc/logstash/conf.d/`<br>Para archivos.zip y.tar.gz: `{ extract.path } /config` |
| | kafka.client.truststore.jks | Para paquetes Debian y RPM: `/etc/logstash/ssl/`<br>Para archivos.zip y.tar.gz: `{ extract.path } /ssl` |
| Windows | CAS_Others_LogStash_Config.conf | `fig\logstash-7.xx.x\config` |

| Tipo de máquina host | Nombre de archivo | Ruta del directorio |
|---|---|---|
| | kafka.client.truststore.jks | `C:\logstash-7.xx.x\config` |

c) El archivo de configuración de Logstash contiene información confidencial, como las credenciales de Kafka, los ID de LogAnalytics Workspace y las claves principales. Se recomienda que estas credenciales confidenciales no se almacenen como texto sin formato. Para garantizar la integración, se puede utilizar un almacén de claves de Logstash para agregar claves con sus valores respectivos, a los que, a su vez, se puede hacer referencia mediante los nombres de las claves en el archivo de configuración. Para obtener información adicional sobre el almacén de claves de Logstash y cómo mejora la seguridad de la configuración, consulte el almacén de claves de Secretspara obtener una configuración segura.

d) Abra el archivo de configuración de Logstash y haga lo siguiente:

En la sección de entrada del archivo, introduzca la siguiente información:

- **Contraseña**: la contraseña de la cuenta que creó en Citrix Analytics for Security para preparar el archivo de configuración.
- **Ubicación del almacén de confianza SSL**: la ubicación de su certificado de cliente SSL. Esta es la ubicación del archivo kafka.client.truststore.jks en su máquina host.

```
input {
  kafka {
    bootstrap_servers => [redacted]
    topics => [redacted]
    group_id => [redacted]
    session_timeout_ms => 60000
    auto_offset_reset => "earliest"
    security_protocol => "SASL_SSL"
    sasl_mechanism => "SCRAM-SHA-256"
    ssl_endpoint_identification_algorithm => ""
    sasl_jaas_config => "org.apache.kafka.common.security.scram.ScramLoginModule required username='[redacted]' password='<your password>';"
    ssl_truststore_location => "/etc/logstash/ssl/kafka.client.truststore.jks"
  }
}
```

En la sección de salida del archivo, introduzca la ruta de destino o los detalles a los que quiere enviar los datos. Para obtener información sobre los plug-ins de salida, consulte la documentación de Logstash.

El siguiente fragmento muestra que la salida se escribe en un archivo de registro local.

```
output {
        file {
        path => "./citrixanalytics-%{+YYYY.MM.dd}.log"
    }
}
```

e) Reinicie su máquina host para enviar los datos procesados de Citrix Analytics for Security a su servicio SIEM.

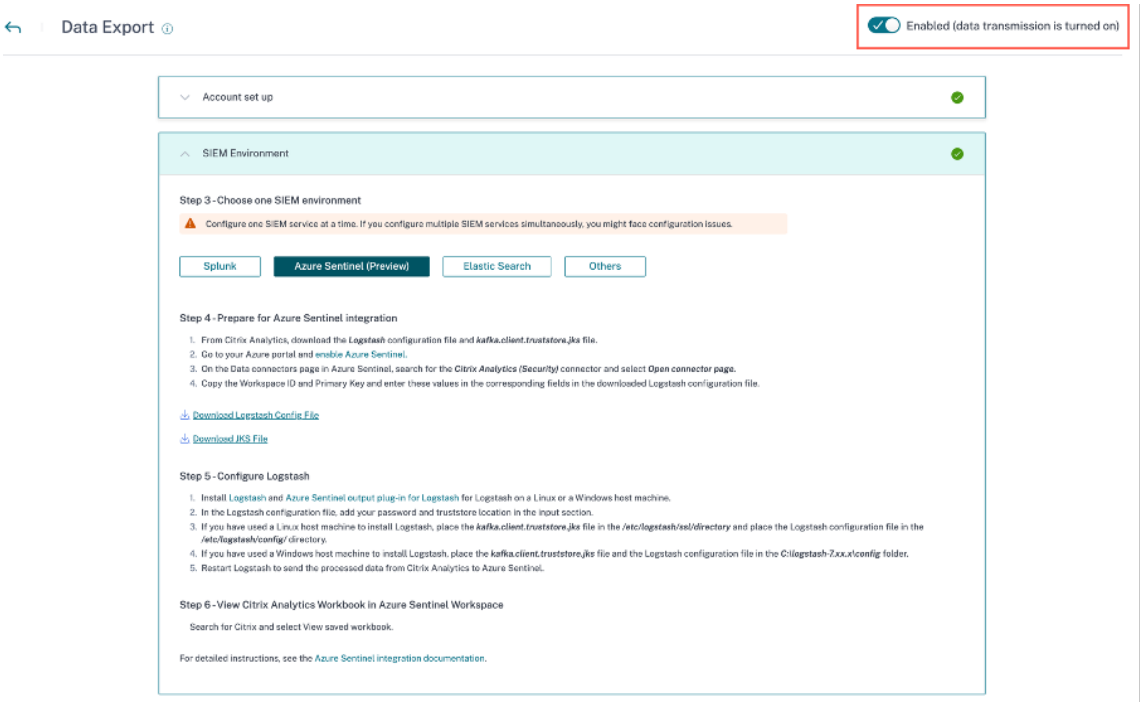
Una vez completada la configuración, inicie sesión en el servicio SIEM y verifique los datos de Citrix Analytics en su SIEM.

### Activar o desactivar la transmisión de datos

Después de que Citrix Analytics for Security prepare el archivo de configuración, se activa la transmisión de datos para el SIEM.

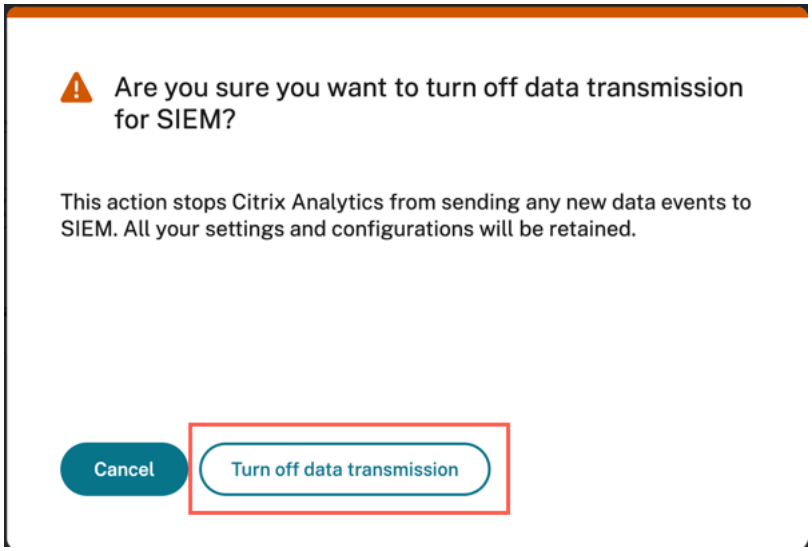
Para dejar de transmitir datos de Citrix Analytics for Security:

1. Ve a **Configuración > Exportaciones de datos**.
2. Apague el botón para desactivar la **transmisión de datos**. De forma predeterminada, la transmisión de datos siempre está habilitada.




Aparece una ventana de advertencia para su confirmación. Haga clic en el botón **Desactivar la transmisión de datos** para detener la actividad de transmisión.




Para habilitar de nuevo la transmisión de datos, active el botón.

> **Nota**
>
> Contacte con CAS-PM-Ext@cloud.com para solicitar ayuda para la integración de tu SIEM, la exportación de datos a tu SIEM o para enviar comentarios.

## Formato de exportación de datos de Citrix Analytics para SIEM

February 12, 2024

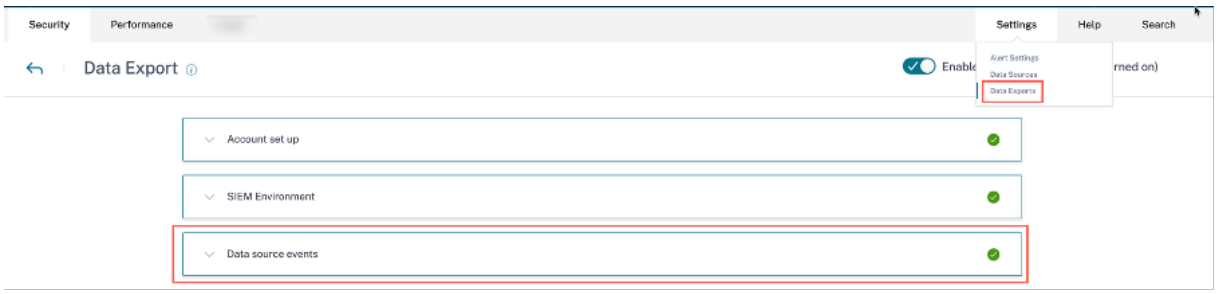
Citrix Analytics for Security le permite integrarse con sus servicios de administración de eventos e información de seguridad (SIEM). Esta integración permite a Citrix Analytics for Security enviar datos a sus servicios SIEM y le ayuda a obtener información sobre la posición de riesgo de seguridad de su organización.

Actualmente, puede integrar Citrix Analytics for Security con los siguientes servicios SIEM:

- Splunk
- Centinela de Microsoft Azure
- Elasticsearch
- Otros SIEM que utilizan un conector de datos basado en Kafka o Logstash

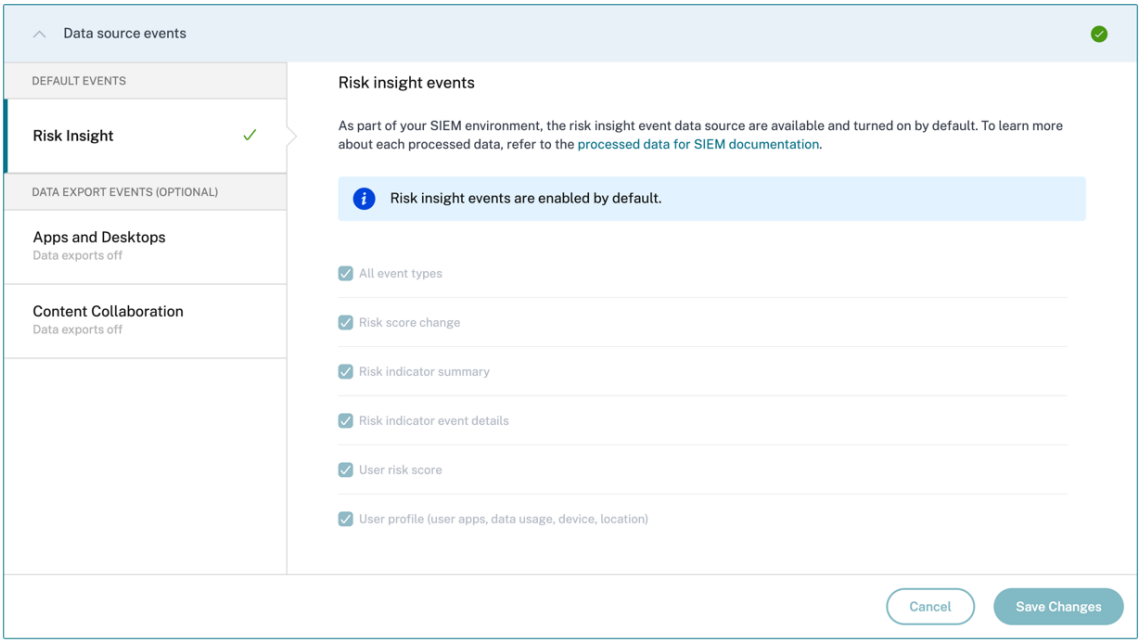
La **opción Exportación de datos** ahora está disponible globalmente en **Configuración**. Para ver los eventos del origen de datos, vaya a **Configuración > Exportaciones de datos > Eventos del origen de datos**.




Los datos de información sobre riesgos que Citrix Analytics for Security envía a su servicio SIEM son de dos tipos:

- Eventos de información sobre riesgos (exportaciones predeterminadas)
- Eventos de fuentes de datos (exportaciones opcionales)




## Datos de información sobre riesgos para SIEM

Una vez que haya completado la configuración de la cuenta y la configuración de SIEM, los conjuntos de datos predeterminados (eventos de información sobre riesgos) comienzan a fluir hacia su implementación de SIEM. Los conjuntos de datos de información sobre riesgos incluyen eventos de puntuación de riesgo de los usuarios, eventos de perfil de usuario y alertas de indicadores de riesgo. Estos se generan mediante los algoritmos de aprendizaje automático de Citrix Analytics y el análisis del comportamiento de los usuarios, aprovechando los eventos de los usuarios.

Los conjuntos de datos de información sobre riesgos de un usuario incluyen lo siguiente:

- **Cambio en la puntuación de riesgo**: Indica un cambio en la puntuación de riesgo del usuario.

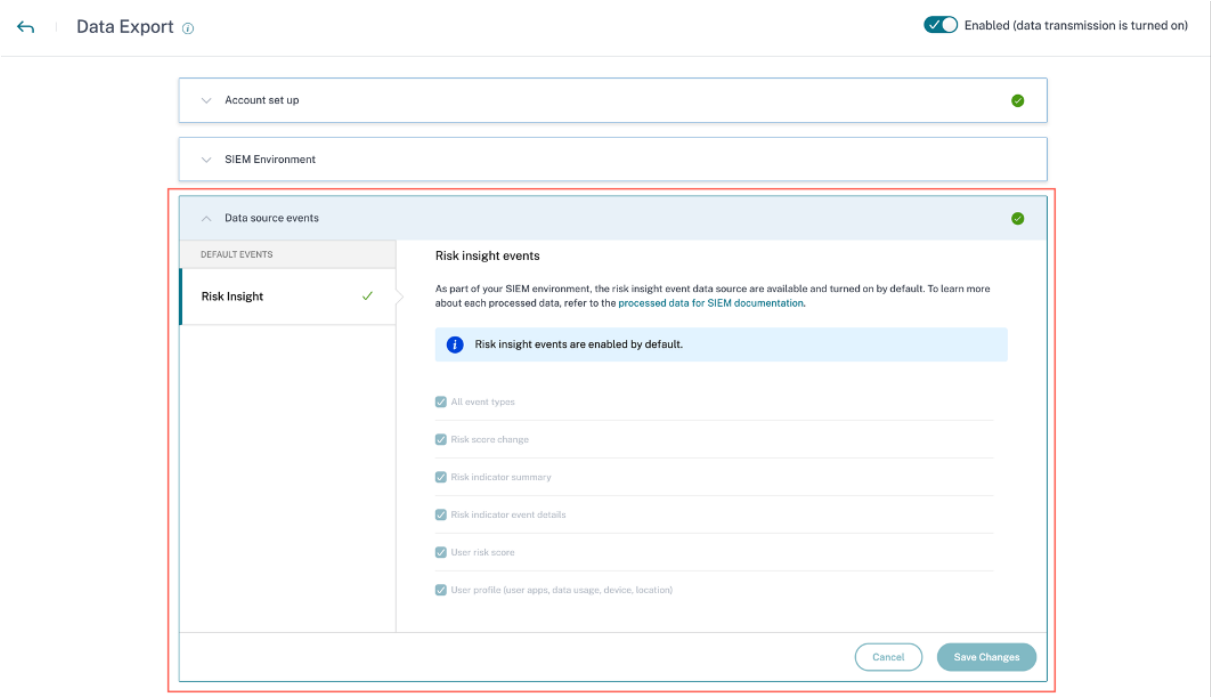
Cuando el cambio en la puntuación de riesgo de un usuario es igual o posterior a 3 y este cambio aumenta en cualquier caso o disminuye en más del 10 %, los datos se envían al servicio SIEM.

- **Resumen del indicador de riesgo**: Los detalles del indicador de riesgo activado para un usuario.
- **Detalles del evento del indicador de riesgo**: Los eventos de usuario asociados a un indicador de riesgo. Citrix Analytics envía un máximo de 1000 detalles de eventos por cada aparición de indicador de riesgo a su servicio SIEM. Estos eventos se envían en orden cronológico de ocurrencia.
- **Evento de puntuación de riesgo del usuario**: La puntuación de riesgo actual de un usuario. Citrix Analytics for Security envía estos datos al servicio SIEM cada 12 horas.
- **Perfil de usuario**: Los datos del perfil de usuario se pueden clasificar en:
  - **Aplicaciones de usuario**: Las aplicaciones que un usuario ha lanzado y utilizado. Citrix Analytics for Security recupera estos datos de Citrix Virtual Apps y los envía al servicio SIEM cada 12 horas.
  - **Dispositivo de usuario**: Los dispositivos asociados a un usuario. Citrix Analytics for Security recupera estos datos de Citrix Virtual Apps y Citrix Endpoint Management y los envía al servicio SIEM cada 12 horas.
  - **Ubicación del usuario**: La ciudad en la que se detectó a un usuario por última vez. Citrix Analytics for Security recupera estos datos de Citrix Virtual Apps and Desktops y Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service). Citrix Analytics for Security envía esta información al servicio SIEM cada 12 horas.
  - **IP del cliente del usuario**: La dirección IP del cliente del dispositivo del usuario. Citrix Analytics for Security recupera estos datos de Citrix Virtual Apps and Desktops y Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) y envía esta información a su servicio SIEM cada 12 horas.

Si solo puede ver pero no puede configurar las preferencias de eventos de la fuente de datos, no tiene los permisos de administrador necesarios.
Para obtener más información, consulte Administrar funciones de administrador para Security Analytics.

En el ejemplo siguiente, el botón **Guardar cambios** está desactivado. Los eventos de información de riesgos están habilitados de forma predeterminada.




## Detalles del esquema de los eventos de información sobre riesgos

En la siguiente sección se describe el esquema de los datos procesados generados por Citrix Analytics for Security.

> **Nota**
>
> Los valores de campo que se muestran en los siguientes ejemplos de esquema solo tienen fines representativos. Los valores de campo reales varían según el perfil del usuario, los eventos del usuario y el indicador de riesgo.

En la tabla siguiente se describen los nombres de campo comunes en todo el esquema para todos los datos de perfil de usuario, puntuación de riesgo del usuario y cambio de puntuación de riesgo.

| Nombre del campo | Descripción |
|---|---|
| `entity_id` | Identidad asociada a la entidad. En este caso, la entidad es el usuario. |
| `entity_type` | La entidad en riesgo. En este caso, la entidad es el usuario. |
| `event_type` | Tipo de datos enviados a su servicio SIEM. Por ejemplo: ubicación del usuario, uso de datos del usuario o información de acceso al dispositivo del usuario. |

| Nombre del campo | Descripción |
|---|---|
| tenant_id | La identidad única del cliente. |
| timestamp | Fecha y hora de la actividad reciente del usuario. |
| version | Versión del esquema de los datos procesados. La versión actual del esquema es 2. |

### Esquema de datos de perfil de usuario

#### Esquema de ubicación del usuario

```
1 {
2
3   "tenant_id": "demo_tenant", "entity_id": "demo_user", "entity_type":
       "user", "timestamp": "2021-02-10T15:00:00Z", "event_type": "
       userProfileLocation", "country": "India", "city": "Bengaluru", "
       cnt": 4, "version": 2
4    }
```

Descripción del campo de la ubicación del usuario

| Nombre del campo | Descripción |
|---|---|
| event_type | Tipo de datos enviados al servicio SIEM. En este caso, el tipo de evento es la ubicación del usuario. |
| country | El país desde el que el usuario ha iniciado sesión. |
| city | Ciudad desde la que el usuario ha iniciado sesión. |
| cnt | Número de veces que se ha accedido a la ubicación en las últimas 12 horas. |

#### Esquema IP de usuario y cliente

```
1 {
2
3   "client_ip": "149.147.136.10",
4   "cnt": 3,
5   "entity_id": "r2_up_user_1",
6   "entity_type": "user",
7   "event_type": "userProfileClientIps",
8   "tenant_id": "xaxddaily1",
9   "timestamp": "2023-09-18T10:45:00Z",
10  "version": 2
11 }
```

Descripción del campo para la IP del cliente

| Nombre del campo | Descripción |
|---|---|
| client_ip | Dirección IP del dispositivo del usuario. |
| cnt | El número de veces que el usuario ha accedido al dispositivo en las últimas 12 horas. |
| entity_id | Identidad asociada a la entidad. En este caso, la entidad es el usuario. |
| entity_type | La entidad en riesgo. En este caso, el tipo de evento es la IP del cliente del usuario. |
| event_type | Tipo de datos enviados a su servicio SIEM. Por ejemplo: la ubicación del usuario, el uso de datos del usuario o la información de acceso al dispositivo del usuario. |
| tenant_id | La identidad única del cliente. |
| timestamp | La fecha y la hora de la actividad reciente del usuario. |
| version | Versión del esquema de los datos procesados. La versión actual del esquema es 2. |

**Esquema de uso de datos de usuario**

```
{

  "data_usage_bytes": 87555255, "deleted_file_cnt": 0, "
     downloaded_bytes": 87555255, "downloaded_file_cnt": 5, "entity_id"
     : "demo@demo.com", "entity_type": "user", "event_type": "
     userProfileUsage", "shared_file_cnt": 0, "tenant_id": "demo_tenant
     ", "timestamp": "2021-02-10T21:00:00Z", "uploaded_bytes": 0, "
     uploaded_file_cnt": 0, "version": 2
   }
```

Descripción del campo para uso de datos de usuario

| Nombre del campo | Descripción |
|---|---|
| data_usage_bytes | Cantidad de datos (en bytes) que utiliza el usuario. Es el agregado del volumen descargado y cargado de un usuario. |
| deleted_file_cnt | Número de archivos eliminados por el usuario. |
| downloaded_bytes | Cantidad de datos descargados por el usuario. |
| downloaded_file_count | Número de archivos descargados por el usuario. |

| Nombre del campo | Descripción |
| --- | --- |
| event_type | Tipo de datos enviados al servicio SIEM. En este caso, el tipo de evento es el perfil de uso del usuario. |
| shared_file_count | Número de archivos compartidos por el usuario. |
| uploaded_bytes | Cantidad de datos cargados por el usuario. |
| uploaded_file_cnt | Número de archivos cargados por el usuario. |

**Esquema de dispositivo de usuario**

```
1 {
2
3   "cnt": 2, "device": "user1612978536 (Windows)", "entity_id": "demo",
       "entity_type": "user", "event_type": "userProfileDevice", "
       tenant_id": "demo_tenant", "timestamp": "2021-02-10T21:00:00Z", "
       version": 2
4    }
```

Descripción del campo del dispositivo de usuario.

| Nombre del campo | Descripción |
| --- | --- |
| cnt | Número de veces que se ha accedido al dispositivo en las últimas 12 horas. |
| device | Nombre del dispositivo. |
| event_type | Tipo de datos enviados al servicio SIEM. En este caso, el tipo de evento es la información de acceso al dispositivo del usuario. |

**Esquema de aplicación de usuario**

```
1 {
2
3   "tenant_id": "demo_tenant", "entity_id": "demo", "entity_type": "user
       ", "timestamp": "2021-02-10T21:00:00Z", "event_type": "
       userProfileApp", "version": 2, "session_domain": "99
       e38d488136f62f828d4823edd120b4f32d724396a7410e6dd1b0", "
       user_samaccountname": "testnameeikragz779", "app": "
       Chromeeikragz779", "cnt": 189
4    }
```

Descripción del campo de la aplicación de usuario.

| Nombre del campo | Descripción |
|---|---|
| event_type | Tipo de datos enviados al servicio SIEM. En este caso, el tipo de evento es la información de acceso al dispositivo del usuario. |
| session_domain | Identificador de la sesión en la que el usuario ha iniciado sesión. |
| user_samaccountname | Nombre de inicio de sesión de clientes y servidores de una versión anterior de Windows, como Windows NT 4.0, Windows 95, Windows 98 y LAN Manager. Este nombre se utiliza para iniciar sesión en Citrix StoreFront y también en una máquina Windows remota. |
| app | Nombre de la aplicación a la que accede el usuario. |
| cnt | Número de veces que se ha accedido a la aplicación en las últimas 12 horas. |

**Esquema de puntuación de riesgo del usuario**

```
1 {
2
3   "cur_riskscore": 7, "entity_id": "demo", "entity_type": "user", "
       event_type": "userProfileRiskscore", "last_update_timestamp": "
       2021-01-21T16:14:29Z", "tenant_id": "demo_tenant", "timestamp": "
       2021-02-10T20:45:00Z", "version": 2
4    }
```

Descripción del campo para la puntuación de riesgo del usuario.

| Nombre del campo | Descripción |
|---|---|
| cur_riskscore | La puntuación de riesgo actual asignada al usuario. La puntuación de riesgo varía de 0 a 100 en función de la gravedad de la amenaza asociada a la actividad del usuario. |
| event_type | Tipo de datos enviados al servicio SIEM. En este caso, el tipo de evento es la puntuación de riesgo del usuario. |
| last_update_timestamp | Hora en que se actualizó por última vez la puntuación de riesgo de un usuario. |

| Nombre del campo | Descripción |
| --- | --- |
| `timestamp` | Hora en que se recopila el evento de puntuación de riesgo del usuario y se envía a su servicio SIEM. Este evento se envía a su servicio SIEM cada 12 horas. |

**Esquema de cambio de puntuación de riesgo**

**Muestra 1**:

```
{

  "alert_message": "Large risk score drop percent since last check", "
     alert_type": "riskscore_large_drop_pct", "alert_value": -21.73913,
      "cur_riskscore": 18, "entity_id": "demo_user", "entity_type": "
     user", "event_type": "riskScoreChange", "tenant_id": "demo_tenant"
     , "timestamp": "2021-02-11T05:45:00Z", "version": 2
   }
```

**Muestra 2**:

```
{

  "alert_message": "Risk score increase since last check", "alert_type"
     : "riskscore_increase", "alert_value": 39.0, "cur_riskscore": 76,
     "entity_id": "demo_user", "entity_type": "user", "event_type": "
     riskScoreChange", "tenant_id": "demo_tenant", "timestamp": "
     2021-02-11T03:45:00Z", "version": 2
   }
```

Descripción del campo para el cambio de la puntuación de riesgo.

| Nombre del campo | Descripción |
| --- | --- |
| `alert_message` | El mensaje mostrado para el cambio de la puntuación de riesgo. |
| `alert_type` | Indica si la alerta es para un aumento de la puntuación de riesgo o una disminución significativa del porcentaje de puntuación de riesgo. Cuando el cambio en la puntuación de riesgo de un usuario es igual o superior a tres y este cambio aumenta en cualquier caso o disminuye en más del 10%, los datos se envían al servicio SIEM. |

| Nombre del campo | Descripción |
|---|---|
| `alert_value` | Valor numérico asignado para el cambio en la puntuación de riesgo. El cambio en la puntuación de riesgo es la diferencia entre la puntuación de riesgo actual y la puntuación de riesgo anterior de un usuario. El valor de alerta varía de -100 a 100. |
| `cur_riskscore` | La puntuación de riesgo actual asignada al usuario. La puntuación de riesgo varía de 0 a 100 en función de la gravedad de la amenaza asociada a la actividad del usuario. |
| `event_type` | Tipo de datos enviados al servicio SIEM. En este caso, el tipo de evento es el cambio en la puntuación de riesgo del usuario. |
| `timestamp` | Fecha y hora en que se detecta el último cambio en la puntuación de riesgo para el usuario. |

**Esquema indicador de riesgo**

El esquema del indicador de riesgo consta de dos partes: el esquema resumido del indicador y el esquema de detalles del evento del indicador. Según el indicador de riesgo, los campos y sus valores del esquema cambian en consecuencia.

En la tabla siguiente se describen los nombres de campo comunes en todos los esquemas de resumen de indicadores.

| Nombre del campo | Descripción |
|---|---|
| `data source` | Los productos que envían datos a Citrix Analytics for Security. Por ejemplo: Citrix Secure Private Access, Citrix Gateway y Citrix Apps and Desktops. |
| `data_source_id` | Identificador asociado a un origen de datos. ID 1 = Citrix Gateway, ID 2 = Citrix Endpoint Management, ID 3 = Citrix Apps and Desktops, ID 4 = Citrix Secure Private Access |
| `entity_type` | La entidad en riesgo. Puede ser un usuario. |
| `entity_id` | Identificador asociado a la entidad en riesgo. |

| Nombre del campo | Descripción |
| --- | --- |
| `event_type` | Tipo de datos enviados al servicio SIEM. En este caso, el tipo de evento es el resumen del indicador de riesgo. |
| `indicator_category` | Indica las categorías de indicadores de riesgo. Los indicadores de riesgo se agrupan en una de las categorías de riesgo: dispositivo de punto final comprometido, usuarios comprometidos, exfiltración de datos o amenazas internas. |
| `indicator_id` | Identificador exclusivo asociado al indicador de riesgo. |
| `indicator_category_id` | ID asociado a una categoría de indicador de riesgo. ID 1 = Exfiltración de datos, ID 2 = amenazas internas, ID 3 = usuarios comprometidos, ID 4 = dispositivo de punto final comprometido |
| `indicator_name` | Nombre del indicador de riesgo. Para un indicador de riesgo personalizado, este nombre se define al crear el indicador. |
| `indicator_type` | Indica si el indicador de riesgo es predeterminado (integrado) o personalizado. |
| `indicator_uuid` | Identificador exclusivo asociado a la instancia del indicador de riesgo. |
| `indicator_vector_name` | Indica el vector de riesgo asociado a un indicador de riesgo. Los vectores de riesgo son indicadores de riesgo basados en dispositivos, indicadores de riesgo basados en la ubicación, indicadores de riesgo basados en fallos de inicio de sesión, indicadores de riesgo basados en IP, indicadores de riesgo basados en datos, indicadores de riesgo basados en archivos y otros indicadores de riesgo. |

| Nombre del campo | Descripción |
| --- | --- |
| `indicator_vector_id` | Identificación asociada a un vector de riesgo. ID 1 = Indicadores de riesgo basados en dispositivos, ID 2 = Indicadores de riesgo basados en la ubicación, ID 3 = Indicadores de riesgo basados en fallos de inicio de sesión, ID 4 = Indicadores de riesgo basados en IP, ID 5 = Indicadores de riesgo basados en datos, ID 6 = Indicadores de riesgo basados en archivos, ID 7 = Otros indicadores de riesgo e ID 999 = No disponible |
| `occurrence_details` | Los detalles sobre la condición desencadenante del indicador de riesgo. |
| `risk_probability` | Indica las posibilidades de riesgo asociadas al evento de usuario. El valor varía de 0 a 1,0. Para un indicador de riesgo personalizado, risk_probability siempre es 1.0 porque es un indicador basado en directivas. |
| `severity` | Indica la gravedad del riesgo. Puede ser bajo, medio o alto. |
| `tenant_id` | La identidad única del cliente. |
| `timestamp` | Fecha y hora en que se activa el indicador de riesgo. |
| `ui_link` | El vínculo a la vista de cronograma del usuario en la interfaz de usuario de Citrix Analytics. |
| `observation_start_time` | El momento desde el que Citrix Analytics comienza a supervisar la actividad del usuario hasta que se marca la hora. Si se detecta algún comportamiento anómalo en este período de tiempo, se activa un indicador de riesgo. |

En la tabla siguiente se describen los nombres de campo comunes en todo el esquema de detalles de eventos del indicador.

| Nombre del campo | Descripción |
| --- | --- |
| data_source_id | Identificador asociado a un origen de datos. ID 1 = Citrix Gateway, ID 2 = Citrix Endpoint Management, ID 3 = Citrix Apps and Desktops, ID 4 = Citrix Secure Private Access |
| indicator_category_id | ID asociado a una categoría de indicador de riesgo. ID 1 = Exfiltración de datos, ID 2 = amenazas internas, ID 3 = usuarios comprometidos, ID 4 = dispositivo de punto final comprometido |
| entity_id | Identificador asociado a la entidad en riesgo. |
| entity_type | Entidad que está en riesgo. Puede ser usuario. |
| event_type | Tipo de datos enviados al servicio SIEM. En este caso, el tipo de evento son los detalles del evento indicador de riesgo. |
| indicator_id | Identificador exclusivo asociado al indicador de riesgo. |
| indicator_uuid | Identificador exclusivo asociado a la instancia del indicador de riesgo. |
| indicator_vector_name | Indica el vector de riesgo asociado a un indicador de riesgo. Los vectores de riesgo son indicadores de riesgo basados en dispositivos, indicadores de riesgo basados en la ubicación, indicadores de riesgo basados en fallos de inicio de sesión, indicadores de riesgo basados en IP, indicadores de riesgo basados en datos, indicadores de riesgo basados en archivos y otros indicadores de riesgo. |
| indicator_vector_id | Identificación asociada a un vector de riesgo. ID 1 = Indicadores de riesgo basados en dispositivos, ID 2 = Indicadores de riesgo basados en la ubicación, ID 3 = Indicadores de riesgo basados en fallos de inicio de sesión, ID 4 = Indicadores de riesgo basados en IP, ID 5 = Indicadores de riesgo basados en datos, ID 6 = Indicadores de riesgo basados en archivos, ID 7 = Otros indicadores de riesgo e ID 999 = No disponible |

| Nombre del campo | Descripción |
|---|---|
| `tenant_id` | La identidad única del cliente. |
| `timestamp` | Fecha y hora en que se activa el indicador de riesgo. |
| `version` | Versión del esquema de los datos procesados. La versión actual del esquema es 2. |
| `client_ip` | Dirección IP del dispositivo del usuario. |

> **Nota**
>
> - Si un valor de campo de tipo de datos enteros no está disponible, el valor asignado es -999. Por ejemplo, `"latitude": -999`, `"longitude": -999`.
> - Si un valor de campo de tipo de datos de cadena de caracteres no está disponible, el valor asignado es NA. Por ejemplo, `"city": "NA"`, `"region": "NA"`.

### Esquema de indicadores de riesgo de Citrix Secure Private Access

#### Intento de acceder al esquema de indicador de riesgo de URL incluido en la lista de bloqueados

**Esquema resumen de indicadores**

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 401,
  "indicator_uuid": "8f2a39bd-c7c2-5555-a86a-5cfe5b64dfef",
  "indicator_category_id": 2,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "data_source_id": 4,
  "timestamp": "2018-03-15T10:59:58Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Insider threats",
  "indicator_name": "Attempt to access blacklisted URL",
  "severity": "low",
  "data_source": "Citrix Secure Private Access",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
```

```
25   "occurrence_details": {
26
27     "observation_start_time": "2018-03-15T10:44:59Z",
28     "relevant_event_type": "Blacklisted External Resource Access"
29    }
30
31  }
```

**Esquema de detalles del evento indicador**

```
1  {
2
3    "tenant_id": "demo_tenant",
4    "indicator_id": 401,
5    "indicator_uuid": "c421f3f8-33d8-59b9-ad47-715b9d4f65f4",
6    "indicator_category_id": 2,
7    "indicator_vector": {
8
9      "name": "Other Risk Indicators",
10     "id": 7  }
11   ,
12   "data_source_id": 4,
13   "timestamp": "2018-03-15T10:57:21Z",
14   "event_type": "indicatorEventDetails",
15   "entity_type": "user",
16   "entity_id": "demo_user",
17   "version": 2,
18   "domain_name": "googleads.g.doubleclick.net",
19   "executed_action": "blocked",
20   "reason_for_action": "URL Category match",
21   "client_ip": "157.xx.xxx.xxx"
22  }
```

En la tabla siguiente se describen los nombres de campo específicos del esquema de resumen y del esquema de detalles del evento para intentar acceder a la URL de la lista negra.

| Nombre del campo | Descripción |
|---|---|
| observation_start_time | El momento desde el que Citrix Analytics comienza a supervisar la actividad del usuario hasta que se marca la hora. Si se detecta algún comportamiento anómalo en este período de tiempo, se activa un indicador de riesgo. |
| executed_action | Acción aplicada en la URL incluida en la lista de bloqueados. La acción incluye Permitir y Bloquear. |
| reason_for_action | El motivo por el que se aplica la acción a la URL. |

### Esquema indicador de riesgo de descargas excesivas de datos

#### Esquema resumen de indicadores

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 403,
  "indicator_uuid": "67d21b81-a89a-531e-af0b-c5688c2e9d40",
  "indicator_category_id": 2,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "data_source_id": 4,
  "timestamp": "2018-03-16T10:59:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Insider threats",
  "indicator_name": "Excessive data download",
  "severity": "low",
  "data_source": "Citrix Secure Private Access",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "observation_start_time": "2018-03-16T10:00:00Z",
    "data_volume_in_bytes": 24000,
    "relevant_event_type": "External Resource Access"
   }

 }
```

#### Esquema de detalles del evento indicador

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 403,
  "indicator_uuid": "67d21b81-a89a-531e-af0b-c5688c2e9d40",
  "indicator_category_id": 2,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "data_source_id": 4,
  "timestamp": "2018-03-16T10:30:00Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
```

```
16    "entity_id": "demo_user",
17    "version": 2,
18    "domain_name": "www.facebook.com",
19    "client_ip": "157.xx.xxx.xxx",
20    "downloaded_bytes": 24000
21   }
```

En la tabla siguiente se describen los nombres de campo específicos del esquema de resumen y el esquema de detalles del evento para descargas de datos excesivas.

| Nombre del campo | Descripción |
|---|---|
| observation_start_time | El momento desde el que Citrix Analytics comienza a supervisar la actividad del usuario hasta que se marca la hora. Si se detecta algún comportamiento anómalo en este período de tiempo, se activa un indicador de riesgo. |
| data_volume_in_bytes | Cantidad de datos en bytes que se descargan. |
| relevant_event_type | Indica el tipo de evento de usuario. |
| domain_name | Nombre del dominio del que se descargan los datos. |
| downloaded_bytes | Cantidad de datos en bytes que se descargan. |

### Esquema indicador de riesgo de volumen de carga inusual

#### Esquema resumen de indicadores

```
1  {
2
3    "tenant_id": "demo_tenant",
4    "indicator_id": 402,
5    "indicator_uuid": "4f2a249c-9d05-5409-9c5f-f4c764f50e67",
6    "indicator_category_id": 2,
7    "indicator_vector": {
8
9      "name": "Other Risk Indicators",
10     "id": 7  }
11   ,
12   "data_source_id": 4,
13   "timestamp": "2018-03-16T10:59:59Z",
14   "event_type": "indicatorSummary",
15   "entity_type": "user",
16   "entity_id": "demo_user",
17   "version": 2,
18   "risk_probability": 1,
19   "indicator_category": "Insider threats",
```

```
20    "indicator_name": "Unusual upload volume",
21    "severity": "low",
22    "data_source": "Citrix Secure Private Access",
23    "ui_link": "https://analytics.cloud.com/user/",
24    "indicator_type": "builtin",
25    "occurrence_details": {
26
27      "observation_start_time": "2018-03-16T10:00:00Z",
28      "data_volume_in_bytes": 24000,
29      "relevant_event_type": "External Resource Access"
30     }
31
32   }
```

**Esquema de detalles del evento indicador**

```
1  {
2
3    "tenant_id": "demo_tenant",
4    "indicator_id": 402,
5    "indicator_uuid": "c6abf40c-9b62-5db4-84bc-5b2cd2c0ca5f",
6    "indicator_category_id": 2,
7    "indicator_vector": {
8
9      "name": "Other Risk Indicators",
10     "id": 7  }
11   ,
12   "data_source_id": 4,
13   "timestamp": "2018-03-16T10:30:00Z",
14   "event_type": "indicatorEventDetails",
15   "entity_type": "user",
16   "entity_id": "demo_user",
17   "version": 2,
18   "domain_name": "www.facebook.com",
19   "client_ip": "157.xx.xxx.xxx",
20   "uploaded_bytes": 24000
21  }
```

En la tabla siguiente se describen los nombres de campo específicos del esquema de resumen y el esquema de detalles del evento del volumen de carga inusual.

| Nombres de campo | Descripción |
| --- | --- |
| `observation_start_time` | El momento desde el que Citrix Analytics comienza a supervisar la actividad del usuario hasta que se marca la hora. Si se detecta algún comportamiento anómalo en este período de tiempo, se activa un indicador de riesgo. |
| `data_volume_in_bytes` | Cantidad de datos en bytes que se cargan. |

| Nombres de campo | Descripción |
| --- | --- |
| relevant_event_type | Indica el tipo de evento de usuario. |
| domain_name | El nombre del dominio en el que se cargan los datos. |
| uploaded_bytes | Cantidad de datos en bytes que se cargan. |

### Esquema de indicadores de riesgo de Citrix Endpoint Management

### Esquema de indicadores detectados de dispositivos con jailbreak o rooteado

#### Esquema resumen de indicadores

```
{

  "data_source": "Citrix Endpoint Management",
  "data_source_id": 2,
  "indicator_id": 200,
  "indicator_name": "Jailbroken / Rooted Device Detected",
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorSummary",
  "indicator_category": "Compromised endpoints",
  "indicator_category_id": 4,
  "indicator_vector": {

    "name": "Other Risk Indicators",
    "id": 7  }
 ,
  "indicator_type": "builtin",
  "indicator_uuid": "aa872f86-a991-4219-ad01-2a070b6e633d",
  "occurrence_details": {
  }
 ,
  "risk_probability": 1.0,
  "severity": "low",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-04-13T17:49:05Z",
  "ui_link": "https://analytics.cloud.com/user/",
  "version": 2
 }
```

#### Esquema de detalles del evento indicador

```
{

  "indicator_id": 200,
  "client_ip": "122.xx.xx.xxx",
  "data_source_id": 2,
```

```
6    "entity_id": "demo_user",
7    "entity_type": "user",
8    "event_type": "indicatorEventDetails",
9    "indicator_category_id": 4,
10   "indicator_vector": {
11
12     "name": "Other Risk Indicators",
13     "id": 7  }
14  ,
15   "indicator_uuid": "9aaaa9e1-39ad-4daf-ae8b-2fa2caa60732",
16   "tenant_id": "demo_tenant",
17   "timestamp": "2021-04-09T17:50:35Z",
18   "version": 2
19  }
```

### Dispositivo con aplicaciones en la lista de bloqueados detectado

#### Esquema resumen de indicadores

```
1  {
2
3    "data_source": "Citrix Endpoint Management",
4    "data_source_id": 2,
5    "indicator_id": 201,
6    "indicator_name": "Device with Blacklisted Apps Detected",
7    "entity_id": "demo_user",
8    "entity_type": "user",
9    "event_type": "indicatorSummary",
10   "indicator_category": "Compromised endpoints",
11   "indicator_category_id": 4,
12   "indicator_vector": {
13
14     "name": "Other Risk Indicators",
15     "id": 7  }
16  ,
17   "indicator_type": "builtin",
18   "indicator_uuid": "3ff7bd54-4319-46b6-8b98-58a9a50ae9a7",
19   "occurrence_details": {
20   }
21  ,
22   "risk_probability": 1.0,
23   "severity": "low",
24   "tenant_id": "demo_tenant",
25   "timestamp": "2021-04-13T17:49:23Z",
26   "ui_link": "https://analytics.cloud.com/user/",
27   "version": 2
28  }
```

#### Esquema de detalles del evento indicador

```
1  {
2
3    "indicator_id": 201,
```

```
4    "client_ip": "122.xx.xx.xxx",
5    "data_source_id": 2,
6    "entity_id": "demo_user",
7    "entity_type": "user",
8    "event_type": "indicatorEventDetails",
9    "indicator_category_id": 4,
10   "indicator_vector": {
11
12     "name": "Other Risk Indicators",
13     "id": 7  }
14  ,
15   "indicator_uuid": "743cd13a-2596-4323-8da9-1ac279232894",
16   "tenant_id": "demo_tenant",
17   "timestamp": "2021-04-09T17:50:39Z",
18   "version": 2
19  }
```

### Dispositivo no administrado detectado

#### Esquema resumen de indicadores

```
1  {
2
3    "data_source": "Citrix Endpoint Management",
4    "data_source_id": 2,
5    "indicator_id": 203,
6    "indicator_name": "Unmanaged Device Detected",
7    "entity_id": "demo_user",
8    "entity_type": "user",
9    "event_type": "indicatorSummary",
10   "indicator_category": "Compromised endpoints",
11   "indicator_category_id": 4,
12   "indicator_vector": {
13
14     "name": "Other Risk Indicators",
15     "id": 7  }
16  ,
17   "indicator_type": "builtin",
18   "indicator_uuid": "e28b8186-496b-44ff-9ddc-ae50e87bd757",
19   "occurrence_details": {
20   }
21  ,
22   "risk_probability": 1.0,
23   "severity": "low",
24   "tenant_id": "demo_tenant",
25   "timestamp": "2021-04-13T12:56:30Z",
26   "ui_link": "https://analytics.cloud.com/user/",
27   "version": 2
28  }
```

#### Esquema de detalles del evento indicador

```
1  {
```

```
2
3   "indicator_id": 203,
4   "client_ip": "127.xx.xx.xxx",
5   "data_source_id": 2,
6   "entity_id": "demo_user",
7   "entity_type": "user",
8   "event_type": "indicatorEventDetails",
9   "indicator_category_id": 4,
10  "indicator_vector": {
11
12    "name": "Other Risk Indicators",
13    "id": 7  }
14 ,
15  "indicator_uuid": "dd280122-04f2-42b4-b9fc-92a715c907a0",
16  "tenant_id": "demo_tenant",
17  "timestamp": "2021-04-09T18:41:30Z",
18  "version": 2
19 }
```


### Esquema de indicadores de riesgo de Citrix Gateway

### Esquema indicador de riesgo de fallo del escaneo de la EPA

#### Esquema resumen de indicadores


```
1 {
2
3   "tenant_id": "demo_tenant",
4   "indicator_id": 100,
5   "indicator_uuid": "3c17454c-86f5-588a-a4ac-0342693d8a70",
6   "indicator_category_id": 3,
7   "indicator_vector": {
8
9     "name": "Other Risk Indicators",
10    "id": 7  }
11 ,
12  "data_source_id": 1,
13  "timestamp": "2017-12-21T07:14:59Z",
14  "event_type": "indicatorSummary",
15  "entity_type": "user",
16  "entity_id": "demo_user",
17  "version": 2,
18  "risk_probability": 1,
19  "indicator_category": "Compromised users",
20  "indicator_name": "EPA scan failure",
21  "severity": "low",
22  "data_source": "Citrix Gateway",
23  "ui_link": "https://analytics.cloud.com/user/",
24  "indicator_type": "builtin",
25  "occurrence_details": {
26
27    "event_description": "Post auth failed, no quarantine",
```

```
28      "observation_start_time": "2017-12-21T07:00:00Z",
29      "relevant_event_type": "EPA Scan Failure at Logon"
30     }
31
32   }
```

**Esquema de detalles del evento indicador**

```
1  {
2
3    "tenant_id": "demo_tenant",
4    "indicator_id": 100,
5    "indicator_uuid": "3c17454c-86f5-588a-a4ac-0342693d8a70",
6    "indicator_category_id": 3,
7    "indicator_vector": {
8
9      "name": "Other Risk Indicators",
10     "id": 7  }
11   ,
12   "data_source_id": 1,
13   "timestamp": "2017-12-21T07:12:00Z",
14   "event_type": "indicatorEventDetails",
15   "entity_type": "user",
16   "entity_id": "demo_user",
17   "version": 2,
18   "event_description": "Post auth failed, no quarantine",
19   "gateway_domain_name": "10.102.xx.xx",
20   "gateway_ip": "56.xx.xxx.xx",
21   "policy_name": "postauth_act_1",
22   "client_ip": "210.91.xx.xxx",
23   "country": "United States",
24   "city": "San Jose",
25   "region": "California",
26   "cs_vserver_name": "demo_vserver",
27   "device_os": "Windows OS",
28   "security_expression": "CLIENT.OS(Win12) EXISTS",
29   "vpn_vserver_name": "demo_vpn_vserver",
30   "vserver_fqdn": "10.xxx.xx.xx"
31 }
```

En la tabla se describen los nombres de campo específicos del esquema de resumen y el esquema de detalles del evento del indicador de riesgo de fallo de la exploración de la EPA.

| Nombres de campo | Descripción |
| --- | --- |
| `event_description` | Describe los motivos del error del análisis de la EPA, como un error posterior a la autenticación y la ausencia de grupos de cuarentena. |
| `relevant_event_type` | Indica el tipo de suceso de error de exploración de la EPA. |

| Nombres de campo | Descripción |
|---|---|
| gateway_domain_name | Nombre de dominio de Citrix Gateway. |
| gateway_ip | Dirección IP de Citrix Gateway. |
| policy_name | El nombre de la directiva de análisis EPA configurado en Citrix Gateway. |
| country | País desde el que se ha detectado la actividad del usuario. |
| city | Ciudad desde la que se ha detectado la actividad del usuario. |
| region | Región desde la que se ha detectado la actividad del usuario. |
| cs_vserver_name | Nombre del servidor virtual del conmutador de contenido. |
| device_os | El sistema operativo del dispositivo del usuario. |
| security_expression | Expresión de seguridad configurada en Citrix Gateway. |
| vpn_vserver_name | Nombre del servidor virtual de Citrix Gateway. |
| vserver_fqdn | FQDN del servidor virtual de Citrix Gateway. |

**Esquema indicador de riesgo de fallo de autenticación excesivo**

**Esquema resumen de indicadores**

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 101,
  "indicator_uuid": "4bc0f759-93e0-5eea-9967-ed69de9dd09a",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Logon-Failure-Based Risk Indicators",
    "id": 3  }
 ,
  "data_source_id": 1,
  "timestamp": "2017-12-21T07:14:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Compromised users",
  "indicator_name": "Excessive authentication failures",
```

```
21    "severity": "medium",
22    "data_source": "Citrix Gateway",
23    "ui_link": "https://analytics.cloud.com/user/” ,
24    "indicator_type": "builtin",
25    "occurrence_details": {
26
27      "observation_start_time": "2017-12-21T07:00:00Z",
28      "relevant_event_type": "Logon Failure"
29     }
30
31   }
```

**Esquema de detalles del evento indicador**

```
1  {
2
3    "tenant_id": "demo_tenant",
4    "indicator_id": 101,
5    "indicator_uuid": "a391cd1a-d298-57c3-a17b-01f159b26b99",
6    "indicator_category_id": 3,
7    "indicator_vector": {
8
9      "name": "Logon-Failure-Based Risk Indicators",
10     "id": 3  }
11   ,
12   "data_source_id": 1,
13   "timestamp": "2017-12-21T07:10:00Z",
14   "event_type": "indicatorEventDetails",
15   "entity_type": "user",
16   "entity_id": "demo-user",
17   "version": 2,
18   "event_description": "Bad (format) password passed to nsaaad",
19   "authentication_stage": "Secondary",
20   "authentication_type": "LDAP",
21   "auth_server_ip": "10.xxx.x.xx",
22   "client_ip": "24.xxx.xxx.xx",
23   "gateway_ip": "24.xxx.xxx.xx",
24   "vserver_fqdn": "demo-fqdn.citrix.com",
25   "vpn_vserver_name": "demo_vpn_vserver",
26   "cs_vserver_name": "demo_cs_vserver",
27   "gateway_domain_name": "xyz",
28   "country": "United States",
29   "region": "California",
30   "city": "San Jose",
31   "nth_failure": 5
32  }
```

En la tabla siguiente se describen los nombres de campo específicos del esquema de resumen y el esquema de detalles del evento para un error de autenticación excesivo.

| Nombres de campo | Descripción |
|---|---|
| relevant_event_type | Indica el tipo de suceso, como un error de inicio de sesión. |
| event_description | Describe el motivo del evento de error de autenticación excesivo, como una contraseña incorrecta. |
| authentication_stage | Indica si la fase de autenticación es primaria, secundaria o terciaria. |
| authentication_type | Indica los tipos de autenticación como LDAP, Local u OAuth. |
| auth_server_ip | Dirección IP del servidor de autenticación. |
| gateway_domain_name | Nombre de dominio de Citrix Gateway. |
| gateway_ip | Dirección IP de Citrix Gateway. |
| cs_vserver_name | Nombre del servidor virtual del conmutador de contenido. |
| vpn_vserver_name | Nombre del servidor virtual de Citrix Gateway. |
| vserver_fqdn | FQDN del servidor virtual de Citrix Gateway. |
| nth_failure | Número de veces que se ha producido un error en la autenticación del usuario. |
| country | País desde el que se ha detectado la actividad del usuario. |
| city | Ciudad desde la que se ha detectado la actividad del usuario. |
| region | Región desde la que se ha detectado la actividad del usuario. |

### Indicador de riesgo de trayecto imposible

**Esquema resumen de indicadores**

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": "111",
  "indicator_uuid": "83d68a6d-6588-5b77-9118-8a9e6a5b462b",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Location-Based Risk Indicators",
    "id": 2
   }
```

```
12  ,
13   "data_source_id": 1,
14   "timestamp": "2020-06-06T12:14:59Z",
15   "event_type": "indicatorSummary",
16   "entity_type": "user",
17   "entity_id": "demo_user",
18   "version": 2,
19   "risk_probability": 1,
20   "indicator_category": "Compromised users",
21   "indicator_name": "Impossible travel",
22   "severity": "medium",
23   "data_source": "Citrix Gateway",
24   "ui_link": "https://analytics.cloud.com/user/",
25   "indicator_type": "builtin",
26   "occurrence_details": {
27
28     "relevant_event_type": "Impossible travel",
29     "distance": 7480.44718,
30     "observation_start_time": "2020-06-06T12:00:00Z",
31     "historical_logon_locations": "[{
32  "country":"United States","region":"Florida","city":"Miami","latitude"
       :25.7617,"longitude":-80.191,"count":28 }
33  ,{
34  "country":"United States","latitude":37.0902,"longitude":-95.7129,"
       count":2 }
35  ]",
36     "historical_observation_period_in_days": 30
37    }
38
39  }
```


**Esquema de detalles del evento indicador**


```
1  {
2
3   "tenant_id": "demo_tenant",
4   "indicator_id": "111",
5   "indicator_uuid": "83d68a6d-6588-5b77-9118-8a9e6a5b462b",
6   "pair_id": 2,
7   "indicator_category_id": 3,
8   "indicator_vector": {
9
10     "name": "Location-Based Risk Indicators",
11     "id": 2
12    }
13  ,
14   "data_source_id": 1,
15   "timestamp": "2020-06-06T05:05:00Z",
16   "event_type": "indicatorEventDetails",
17   "entity_type": "user",
18   "entity_id": "demo_user",
19   "version": 2,
20   "client_ip": "95.xxx.xx.xx",
21   " ip_organization " :  " global telecom ltd " ,
```

```
22    " ip_routing_type " : " mobile gateway " ,
23    "country": "Norway",
24    "region": "Oslo",
25    "city": "Oslo",
26    "latitude": 59.9139,
27    "longitude": 10.7522,
28    "device_os": "Linux OS",
29    "device_browser": "Chrome 62.0.3202.94"
30   }
```

En la siguiente tabla se describen los nombres de campo específicos del esquema de resumen y el esquema de detalles del evento para Trayectos imposibles.

| Nombre del campo | Descripción |
|---|---|
| distance | La distancia (km) entre los eventos asociados a trayectos imposibles. |
| historical_logon_locations | Las ubicaciones a las que ha accedido el usuario y el número de veces que se ha accedido a cada ubicación durante el período de observación. |
| historical_observation_period_in_days | Cada ubicación se supervisa durante 30 días. |
| relevant_event_type | Indica el tipo de suceso, como el inicio de sesión. |
| observation_start_time | El momento desde el que Citrix Analytics comienza a supervisar la actividad del usuario hasta que se marca la hora. Si se detecta algún comportamiento anómalo en este período de tiempo, se activa un indicador de riesgo. |
| country | El país desde el que el usuario ha iniciado sesión. |
| city | Ciudad desde la que el usuario ha iniciado sesión. |
| region | Indica la región desde la que el usuario ha iniciado sesión. |
| latitude | Indica la latitud de la ubicación desde la que el usuario ha iniciado sesión. |
| longitude | Indica la longitud de la ubicación desde la que el usuario ha iniciado sesión. |
| device_browser | El explorador web utilizado por el usuario. |
| device_os | El sistema operativo del dispositivo del usuario. |
| ip_organization | Organización de registro de la dirección IP del cliente |

| Nombre del campo | Descripción |
| --- | --- |
| `ip_routing_type` | Tipo de redirección IP del cliente |

### Inicio de sesión desde un esquema de indicador de riesgo de IP sospechoso

#### Esquema resumen de indicadores

```
1  {
2
3    "tenant_id": "demo_tenant",
4    "indicator_id": 102,
5    "indicator_uuid": "0100e910-561a-5ff3-b2a8-fc556d199ba5",
6    "indicator_category_id": 3,
7    "indicator_vector": {
8
9      "name": "IP-Based Risk Indicators",
10     "id": 4  }
11   ,
12   "data_source_id": 1,
13   "timestamp": "2019-10-10T10:14:59Z",
14   "event_type": "indicatorSummary",
15   "entity_type": "user",
16   "entity_id": "demo_user",
17   "version": 2,
18   "risk_probability": 0.91,
19   "indicator_category": "Compromised users",
20   "indicator_name": "Logon from suspicious IP",
21   "severity": "medium",
22   "data_source": "Citrix Gateway",
23   "ui_link": "https://analytics.cloud.com/user/",
24   "indicator_type": "builtin",
25   "occurrence_details": {
26
27     "relevant_event_type": "Logon",
28     "client_ip": "1.0.xxx.xx",
29     "observation_start_time": "2019-10-10T10:00:00Z",
30     "suspicion_reasons": "brute_force|external_threat"
31    }
32
33  }
```

#### Esquema de detalles del evento indicador

```
1  {
2
3    "tenant_id": "demo_tenant",
4    "indicator_id": 102,
5    "indicator_uuid": "4ba77b6c-bac0-5ad0-9b4a-c459a3e2ec33",
6    "indicator_category_id": 3,
7    "indicator_vector": {
```

```
8
9       "name": "IP-Based Risk Indicators",
10      "id": 4  }
11    ,
12     "data_source_id": 1,
13     "timestamp": "2019-10-10T10:11:00Z",
14     "event_type": "indicatorEventDetails",
15     "entity_type": "user",
16     "entity_id": "demo_user",
17     "version": 2,
18     "suspicion_reasons": "external_threat",
19     "gateway_ip": "gIP1",
20     "client_ip": "128.0.xxx.xxx",
21     "country": "Sweden",
22     "city": "Stockholm",
23     "region": "Stockholm",
24     "webroot_reputation": 14,
25     "webroot_threat_categories": "Windows Exploits|Botnets|Proxy",
26     "device_os": "Windows OS",
27     "device_browser": "Chrome"
28    }
```


En la tabla siguiente se describen los nombres de campo específicos del esquema de resumen y del esquema de detalles del evento para iniciar sesión desde una IP sospechosa.

| Nombre del campo | Descripción |
|---|---|
| `suspicious_reasons` | El motivo por el que se identifica la dirección IP como sospechosa. |
| `webroot_reputation` | El índice de reputación de IP proporcionado por el proveedor de inteligencia de amenazas Webroot. |
| `webroot_threat_categories` | La categoría de amenaza identificada para la IP sospechosa por el proveedor de inteligencia de amenazas Webroot. |
| `device_os` | El sistema operativo del dispositivo del usuario. |
| `device_browser` | El explorador web utilizado. |
| `country` | País desde el que se ha detectado la actividad del usuario. |
| `city` | Ciudad desde la que se ha detectado la actividad del usuario. |
| `region` | Región desde la que se ha detectado la actividad del usuario. |

**Esquema indicador de riesgo de fallo de autenticación inusual**

**Esquema resumen de indicadores**


```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 109,
  "indicator_uuid": "dc0174c9-247a-5e48-a2ab-d5f92cd83d0f",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Logon-Failure-Based Risk Indicators",
    "id": 3  }
 ,
  "data_source_id": 1,
  "timestamp": "2020-04-01T06:44:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Compromised users",
  "indicator_name": "Unusual authentication failure",
  "severity": "medium",
  "data_source": "Citrix Gateway",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "relevant_event_type": "Logon Failure",
    "observation_start_time": "2020-04-01T05:45:00Z"
   }

 }
```


**Esquema de detalles del evento indicador**


```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 109,
  "indicator_uuid": "ef4b9830-39d6-5b41-bdf3-84873a77ea9a",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Logon-Failure-Based Risk Indicators",
    "id": 3  }
 ,
  "data_source_id": 1,
  "timestamp": "2020-04-01T06:42:00Z",
  "event_type": "indicatorEventDetails",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "event_description": "Success",
  "authentication_stage": "Secondary",
```

```
20    "authentication_type": "LDAP",
21    "client_ip": "99.xxx.xx.xx",
22    "country": "United States",
23    "city": "San Jose",
24    "region": "California",
25    "device_os": "Windows OS ",
26    "device_browser": "Chrome",
27    "is_risky": "false"
28   }
```

En la tabla siguiente se describen los nombres de campo específicos del esquema de resumen y el esquema de detalles del evento para Error de autenticación inusual.

| Nombres de campo | Descripción |
|---|---|
| `relevant_event_type` | Indica el tipo de suceso, como un error de inicio de sesión. |
| `event_description` | Indica si el inicio de sesión se ha realizado correctamente o no. |
| `authentication_stage` | Indica si la fase de autenticación es primaria, secundaria o terciaria. |
| `authentication_type` | Indica los tipos de autenticación como LDAP, Local u OAuth. |
| `is_risky` | Para un inicio de sesión correcto, el valor is_risky es false. Para un inicio de sesión fallido, el valor is_risky es true. |
| `device_os` | El sistema operativo del dispositivo del usuario. |
| `device_browser` | El explorador web utilizado por el usuario. |
| `country` | País desde el que se ha detectado la actividad del usuario. |
| `city` | Ciudad desde la que se ha detectado la actividad del usuario. |
| `region` | Región desde la que se ha detectado la actividad del usuario. |

### Indicador de riesgo de inicio de sesión sospechoso

#### Esquema resumen de indicadores

```
1  {
2
3    "tenant_id": "demo_tenant",
4    "indicator_id": "110",
5    "indicator_uuid": "67fd935-a6a3-5397-b596-636aa1588c",
```

```
  "indicator_category_id": 3,
  "indicator_vector": [
    {

      "name": "Location-Based Risk Indicators",
      "id": 2
     }
 ,
    {

      "name": "IP-Based Risk Indicators",
      "id": 4
     }
 ,
    {

      "name": "Other Risk Indicators",
      "id": 7
     }

  ],
  "data_source_id": 1,
  "timestamp": "2020-06-06T12:14:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 0.71,
  "indicator_category": "Compromised users",
  "indicator_name": "Suspicious logon",
  "severity": "medium",
  "data_source": "Citrix Gateway",
  "ui_link": "https://analytics.cloud.com/user/",
  "indicator_type": "builtin",
  "occurrence_details": {

    "observation_start_time": "2020-06-06T12:00:00Z",
    "relevant_event_type": "Logon",
    "event_count": 1,
    "historical_observation_period_in_days": 30,
    "country": "United States",
    "region": "Florida",
    "city": "Miami",
    "historical_logon_locations": "[{
"country":"United States","region":"New York","city":"New York City","
    latitude":40.7128,"longitude":-74.0060,"count":9 }
]",
    "user_location_risk": 75,
    "device_id": "",
    "device_os": "Windows OS",
    "device_browser": "Chrome",
    "user_device_risk": 0,
    "client_ip": "99.xxx.xx.xx",
```

```
58      "user_network_risk": 75,
59      "webroot_threat_categories": "Phishing",
60      "suspicious_network_risk": 89
61    }
62
63  }
```

**Esquema de detalles del evento indicador**

```
1  {
2
3    "tenant_id": "demo_tenant",
4    "indicator_id": "110",
5    "indicator_uuid": "67fd6935-a6a3-5397-b596-63856aa1588c",
6    "indicator_category_id": 3,
7    "indicator_vector": [
8      {
9
10       "name": "Location-Based Risk Indicators",
11       "id": 2
12      }
13   ,
14     {
15
16       "name": "IP-Based Risk Indicators",
17       "id": 4
18      }
19   ,
20     {
21
22       "name": "Other Risk Indicators",
23       "id": 7
24      }
25
26   ],
27   "data_source_id": 1,
28   "timestamp": "2020-06-06T12:08:40Z",
29   "event_type": "indicatorEventDetails",
30   "entity_type": "user",
31   "entity_id": "demo_user",
32   "version": 2,
33   "country": "United States",
34   "region": "Florida",
35   "city": "Miami",
36   "latitude": 25.7617,
37   "longitude": -80.1918,
38   "device_browser": "Chrome",
39   "device_os": "Windows OS",
40   "device_id": "NA",
41   "client_ip": "99.xxx.xx.xx"
42  }
```

En la tabla siguiente se describen los nombres de campo específicos del esquema de resumen y el

esquema de detalles del evento para inicios de sesión sospechosos.

| Nombre del campo | Descripción |
|---|---|
| historical_logon_locations | Las ubicaciones a las que ha accedido el usuario y el número de veces que se ha accedido a cada ubicación durante el período de observación. |
| historical_observation_period_in_days | Cada ubicación se supervisa durante 30 días. |
| relevant_event_type | Indica el tipo de suceso, como el inicio de sesión. |
| observation_start_time | El momento desde el que Citrix Analytics comienza a supervisar la actividad del usuario hasta que se marca la hora. Si se detecta algún comportamiento anómalo en este período de tiempo, se activa un indicador de riesgo. |
| occurrence_event_type | Indica el tipo de evento de usuario, como el inicio de sesión de la cuenta. |
| country | El país desde el que el usuario ha iniciado sesión. |
| city | Ciudad desde la que el usuario ha iniciado sesión. |
| region | Indica la región desde la que el usuario ha iniciado sesión. |
| latitude | Indica la latitud de la ubicación desde la que el usuario ha iniciado sesión. |
| longitude | Indica la longitud de la ubicación desde la que el usuario ha iniciado sesión. |
| device_browser | El explorador web utilizado por el usuario. |
| device_os | El sistema operativo del dispositivo del usuario. |
| device_id | Nombre del dispositivo utilizado por el usuario. |
| user_location_risk | Indica el nivel de sospecha de la ubicación desde la que el usuario ha iniciado sesión. Nivel de sospecha bajo: 0—69, nivel de sospecha medio: 70—89 y nivel de sospecha alto: 90—100 |
| user_device_risk | Indica el nivel de sospecha del dispositivo desde el que el usuario ha iniciado sesión. Nivel de sospecha bajo: 0—69, nivel de sospecha medio: 70—89 y nivel de sospecha alto: 90—100 |

| Nombre del campo | Descripción |
|---|---|
| user_network_risk | Indica el nivel de sospecha de la red o de la subred desde la que el usuario ha iniciado sesión. Nivel de sospecha bajo: 0—69, nivel de sospecha medio: 70—89 y nivel de sospecha alto: 90—100 |
| suspicious_network_risk | Indica el nivel de amenaza de IP según el feed de inteligencia de amenazas IP de Webroot. Nivel de amenaza bajo: 0 a 69, nivel de amenaza medio: 70 a 89 y nivel de amenaza alto: 90 a 100 |
| webroot_threat_categories | Indica los tipos de amenazas detectadas desde la dirección IP según el origen de información sobre amenazas IP de Webroot. Las categorías de amenazas pueden ser fuentes de spam, vulnerabilidades de Windows, ataques web, botnets, escáneres, denegación de servicio, reputación, phishing, proxy, no especificado, amenazas móviles y proxy Tor |

**Esquema de indicadores de riesgo de Citrix DaaS y Citrix Virtual Apps and Desktops**

**Indicador de riesgo de trayecto imposible**

**Esquema resumen de indicadores**

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": "313",
  "indicator_uuid": "c78d1dd4-5e70-5642-ba6f-1cdf31bc6ab2",
  "indicator_category_id": 3,
  "indicator_vector": {

    "name": "Location-Based Risk Indicators",
    "id": 2
   }
 ,
  "data_source_id": 3,
  "timestamp": "2020-06-06T12:14:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
```

```
20    "indicator_category": "Compromised users",
21    "indicator_name": "Impossible travel",
22    "severity": "medium",
23    "data_source": "Apps and Desktops",
24    "ui_link": "https://analytics.cloud.com/user/",
25    "indicator_type": "builtin",
26    "occurrence_details": {
27
28      "relevant_event_type": "Impossible travel",
29      "distance": 7480.44718,
30      "observation_start_time": "2020-06-06T12:00:00Z",
31      "historical_logon_locations": "[{
32   "country":"United States","region":"Florida","city":"Miami","latitude"
        :25.7617,"longitude":-80.191,"count":28 }
33   ,{
34   "country":"United States","latitude":37.0902,"longitude":-95.7129,"
        count":2 }
35   ]",
36      "historical_observation_period_in_days": 30
37     }
38
39   }
```


**Esquema de detalles del evento indicador**


```
1  {
2
3    "tenant_id": "demo_tenant",
4    "indicator_id": "313",
5    "indicator_uuid": "c78d1dd4-5e70-5642-ba6f-1cdf31bc6ab2",
6    "pair_id": 2,
7    "indicator_category_id": 3,
8    "indicator_vector": {
9
10     "name": "Location-Based Risk Indicators",
11     "id": 2
12    }
13   ,
14   "data_source_id": 3,
15   "timestamp": "2020-06-06T05:05:00Z",
16   "event_type": "indicatorEventDetails",
17   "entity_type": "user",
18   "entity_id": "demo_user",
19   "version": 2,
20   "occurrence_event_type": "Account.Logon",
21   "client_ip": "95.xxx.xx.xx",
22   "ip_organization": "global telecom ltd",
23   "ip_routing_type": "mobile gateway",
24   "country": "Norway",
25   "region": "Oslo",
26   "city": "Oslo",
27   "latitude": 59.9139,
28   "longitude": 10.7522,
29   "device_id": "device1",
```

```
30    "receiver_type": "XA.Receiver.Linux",
31    "os": "Linux OS",
32    "browser": "Chrome 62.0.3202.94"
33   }
```

En la siguiente tabla se describen los nombres de campo específicos del esquema de resumen y el esquema de detalles del evento para Trayectos imposibles.

| Nombre del campo | Descripción |
|---|---|
| `distance` | La distancia (km) entre los eventos asociados a trayectos imposibles. |
| `historical_logon_locations` | Las ubicaciones a las que ha accedido el usuario y el número de veces que se ha accedido a cada ubicación durante el período de observación. |
| `historical_observation_period_in_days` | Cada ubicación se supervisa durante 30 días. |
| `relevant_event_type` | Indica el tipo de suceso, como el inicio de sesión. |
| `observation_start_time` | El momento desde el que Citrix Analytics comienza a supervisar la actividad del usuario hasta que se marca la hora. Si se detecta algún comportamiento anómalo en este período de tiempo, se activa un indicador de riesgo. |
| `country` | El país desde el que el usuario ha iniciado sesión. |
| `city` | Ciudad desde la que el usuario ha iniciado sesión. |
| `region` | Indica la región desde la que el usuario ha iniciado sesión. |
| `latitude` | Indica la latitud de la ubicación desde la que el usuario ha iniciado sesión. |
| `longitude` | Indica la longitud de la ubicación desde la que el usuario ha iniciado sesión. |
| `browser` | El explorador web utilizado por el usuario. |
| `os` | El sistema operativo del dispositivo del usuario. |
| `device_id` | Nombre del dispositivo utilizado por el usuario. |
| `receiver_type` | Tipo de aplicación Citrix Workspace o Citrix Receiver instalada en el dispositivo del usuario. |
| `ip_organization` | Organización de registro de la dirección IP del cliente |

| Nombre del campo | Descripción |
| --- | --- |
| `ip_routing_type` | Tipo de redirección IP del cliente |

### Indicador de riesgo potencial de exfiltración de datos

#### Esquema resumen de indicadores

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 303,
  "indicator_uuid": "fb649ff7-5b09-5f48-8a04-12836b9eed85",
  "indicator_category_id": 1,
  "indicator_vector": {

    "name": "Data-Based Risk Indicators",
    "id": 5  }
 ,
  "data_source_id": 3,
  "timestamp": "2018-04-02T10:59:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "demo_user",
  "version": 2,
  "risk_probability": 1,
  "indicator_category": "Data exfiltration",
  "indicator_name": "Potential data exfiltration",
  "severity": "low",
  "data_source": "Citrix Apps and Desktops",
  "ui_link": "https://analytics.cloud.com/user/ ",
  "indicator_type": "builtin",
  "occurrence_details": {

    "relevant_event_type": "Download/Print/Copy",
    "observation_start_time": "2018-04-02T10:00:00Z",
    "exfil_data_volume_in_bytes": 1172000
   }

 }
```

#### Esquema de detalles del evento indicador

```
{

  "tenant_id": "demo_tenant",
  "indicator_id": 303,
  "indicator_uuid": "fb649ff7-5b09-5f48-8a04-12836b9eed85",
  "indicator_category_id": 1,
  "indicator_vector": {

```

```
9       "name": "Data-Based Risk Indicators",
10      "id": 5  }
11    ,
12     "data_source_id": 3,
13     "timestamp": "2018-04-02T10:57:36Z",
14     "event_type": "indicatorEventDetails",
15     "entity_type": "user",
16     "entity_id": "demo_user",
17     "version": 2,
18     "occurrence_event_type": "App.SaaS.Clipboard",
19     "file_size_in_bytes": 98000,
20     "file_type": "text",
21     "device_id": "dvc5",
22     "receiver_type": "XA.Receiver.Windows",
23     "app_url": "https://www.citrix.com",
24     "client_ip": "10.xxx.xx.xxx",
25     "entity_time_zone": "Pacific Standard Time"
26    }
```

En la tabla siguiente se describen los campos específicos del esquema de resumen y el esquema de detalles del evento de Potencial filtración de datos.

| Nombre del campo | Descripción |
|---|---|
| observation_start_time | El momento desde el que Citrix Analytics comienza a supervisar la actividad del usuario hasta que se marca la hora. Si se detecta algún comportamiento anómalo en este período de tiempo, se activa un indicador de riesgo. |
| relevant_event_type | Indica la actividad del usuario, como descargar, imprimir o copiar los datos. |
| exfil_data_volume_in_bytes | La cantidad de filtración de datos. |
| occurrence_event_type | Indica cómo se ha producido la filtración de datos, como la operación del portapapeles en una aplicación SaaS. |
| file_size_in_bytes | Tamaño del archivo. |
| file_type | Tipo de archivo. |
| device_id | Identificador del dispositivo de usuario. |
| receiver_type | La aplicación Citrix Workspace o Citrix Receiver instalada en el dispositivo del usuario. |
| app_url | Dirección URL de la aplicación a la que accede el usuario. |
| entity_time_zone | Zona horaria del usuario. |

**Esquema indicador de riesgo de inicio de sesión sospechoso**

**Esquema resumen de indicadores**

```
{

  "tenant_id": "tenant_1",
  "indicator_id": "312",
  "indicator_uuid": "1b97c3be-abcd-efgh-ijkl-1234567890",
  "indicator_category_id": 3,
  "indicator_vector":
  [
    {

      "name": "Other Risk Indicators",
      "id": 7
     }
 ,
    {

      "name":"Location-Based Risk Indicators",
      "id":2
     }
 ,
    {

      "name":"IP-Based Risk Indicators",
      "id":4
     }
 ,
    {

      "name": "Device-Based Risk Indicators",
      "id": 1
     }
 ,
  ],
  "data_source_id": 3,
  "timestamp": "2020-06-06T12:14:59Z",
  "event_type": "indicatorSummary",
  "entity_type": "user",
  "entity_id": "user2",
  "version": 2,
  "risk_probability": 0.78,
  "indicator_category": "Compromised users",
  "indicator_name": "Suspicious logon",
  "severity": "medium",
  "data_source": "Citrix Apps and Desktops",
  "ui_link": "https://analytics.cloud.com/user/ ",
  "indicator_type": "builtin",
  "occurrence_details":
  {

    "user_location_risk": 0,
```

```
    "city": "Some_city",
    "observation_start_time": "2020-06-06T12:00:00Z",
    "event_count": 1,
    "user_device_risk": 75,
    "country": "United States",
    "device_id": "device2",
    "region": "Some_Region",
    "client_ip": "99.xx.xx.xx",
    "webroot_threat_categories": "'Spam Sources', 'Windows Exploits', '
       Web Attacks', 'Botnets', 'Scanners', 'Denial of Service'",
    "historical_logon_locations": "[{
"country":"United States","latitude":45.0,"longitude":45.0,"count":12
    }
,{
"country":"United States","region":"Some_Region_A","city":"Some_City_A
    ","latitude":0.0,"longitude":0.0,"count":8 }
]",
    "relevant_event_type": "Logon",
    "user_network_risk": 100,
    "historical_observation_period_in_days": 30,
    "suspicious_network_risk": 0
  }

}
```

**Esquema de detalles del evento indicador**

```
{

  "tenant_id": "tenant_1",
  "indicator_id": "312",
  "indicator_uuid": "1b97c3be-abcd-efgh-ijkl-1234567890",
  "indicator_category_id": 3,
  "indicator_vector":
  [
    {

      "name": "Other Risk Indicators",
      "id": 7
     }
,
    {

      "name":"Location-Based Risk Indicators",
      "id":2
     }
,
    {

      "name":"IP-Based Risk Indicators",
      "id":4
     }
,
    {
```

```
28
29        "name": "Device-Based Risk Indicators",
30        "id": 1
31       }
32   ,
33    ],
34    "data_source_id": 3,
35    "timestamp": "2020-06-06 12:02:30",
36    "event_type": "indicatorEventDetails",
37    "entity_type": "user",
38    "entity_id": "user2",
39    "version": 2,
40    "occurrence_event_type": "Account.Logon",
41    "city": "Some_city",
42    "country": "United States",
43    "region": "Some_Region",
44    "latitude": 37.751,
45    "longitude": -97.822,
46    "browser": "Firefox 1.3",
47    "os": "Windows OS",
48    "device_id": "device2",
49    "receiver_type": "XA.Receiver.Chrome",
50    "client_ip": "99.xxx.xx.xx"
51   }
```


En la tabla siguiente se describen los nombres de campo específicos del esquema de resumen y el esquema de detalles del evento para inicios de sesión sospechosos.

| Nombre del campo | Descripción |
|---|---|
| `historical_logon_locations` | Las ubicaciones a las que ha accedido el usuario y el número de veces que se ha accedido a cada ubicación durante el período de observación. |
| `historical_observation_period_in_days` | Cada ubicación se supervisa durante 30 días. |
| `relevant_event_type` | Indica el tipo de suceso, como el inicio de sesión. |
| `observation_start_time` | El momento desde el que Citrix Analytics comienza a supervisar la actividad del usuario hasta que se marca la hora. Si se detecta algún comportamiento anómalo en este período de tiempo, se activa un indicador de riesgo. |
| `occurrence_event_type` | Indica el tipo de evento de usuario, como el inicio de sesión de la cuenta. |
| `country` | El país desde el que el usuario ha iniciado sesión. |
| `city` | Ciudad desde la que el usuario ha iniciado sesión. |

| Nombre del campo | Descripción |
| --- | --- |
| `region` | Indica la región desde la que el usuario ha iniciado sesión. |
| `latitude` | Indica la latitud de la ubicación desde la que el usuario ha iniciado sesión. |
| `longitude` | Indica la longitud de la ubicación desde la que el usuario ha iniciado sesión. |
| `browser` | El explorador web utilizado por el usuario. |
| `os` | El sistema operativo del dispositivo del usuario. |
| `device_id` | Nombre del dispositivo utilizado por el usuario. |
| `receiver_type` | Tipo de aplicación Citrix Workspace o Citrix Receiver instalada en el dispositivo del usuario. |
| `user_location_risk` | Indica el nivel de sospecha de la ubicación desde la que el usuario ha iniciado sesión. Nivel de sospecha bajo: 0—69, nivel de sospecha medio: 70—89 y nivel de sospecha alto: 90—100 |
| `user_device_risk` | Indica el nivel de sospecha del dispositivo desde el que el usuario ha iniciado sesión. Nivel de sospecha bajo: 0—69, nivel de sospecha medio: 70—89 y nivel de sospecha alto: 90—100 |
| `user_network_risk` | Indica el nivel de sospecha de la red o de la subred desde la que el usuario ha iniciado sesión. Nivel de sospecha bajo: 0—69, nivel de sospecha medio: 70—89 y nivel de sospecha alto: 90—100 |
| `suspicious_network_risk` | Indica el nivel de amenaza de IP según el feed de inteligencia de amenazas IP de Webroot. Nivel de amenaza bajo: 0 a 69, nivel de amenaza medio: 70 a 89 y nivel de amenaza alto: 90 a 100 |
| `webroot_threat_categories` | Indica los tipos de amenazas detectadas desde la dirección IP según el origen de información sobre amenazas IP de Webroot. Las categorías de amenazas pueden ser fuentes de spam, vulnerabilidades de Windows, ataques web, botnets, escáneres, denegación de servicio, reputación, phishing, proxy, no especificado, amenazas móviles y proxy Tor |

### Indicador de Microsoft Active Directory

#### Esquema resumen de indicadores

```
{

  "data_source": "Microsoft Graph Security",
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorSummary",
  "indicator_category": "Compromised users",
  "indicator_id": 1000,
  "indicator_name": "MS Active Directory Indicator",
  "indicator_vector": {

    "name": "IP-Based Risk Indicators",
    "id": 4  }
 ,
  "indicator_type": "builtin",
  "indicator_uuid": "9880f479-9fbe-4ab0-8348-a613f9de5eba",
  "occurrence_details": {
  }
 ,
  "risk_probability": 1.0,
  "severity": "low",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-01-27T16:03:46Z",
  "ui_link": "https://analytics-daily.cloud.com/user/",
  "version": 2
 }
```

#### Esquema de detalles del evento indicador

```
{

  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorEventDetails",
  "indicator_id": 1000,
  "indicator_vector": {

    "name": "IP-Based Risk Indicators",
    "id": 4  }
 ,
  "indicator_uuid": "9880f479-9fbe-4ab0-8348-a613f9de5eba",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-01-27T16:03:46Z",
  "version": 2
 }
```

### Esquema indicador de riesgo personalizado

En la siguiente sección se describe el esquema del indicador de riesgo personalizado.

> **Nota**
>
> Actualmente, Citrix Analytics envía los datos relacionados con los indicadores de riesgo personalizados de Citrix DaaS y Citrix Virtual Apps and Desktops a su servicio SIEM.

En la tabla siguiente se describen los nombres de campo del esquema de resumen del indicador de riesgo personalizado.

| Nombre del campo | Descripción |
|---|---|
| `data source` | Los productos que envían datos a Citrix Analytics for Security. Por ejemplo: Citrix Secure Private Access, Citrix Gateway y Citrix Apps and Desktops. |
| `data_source_id` | Identificador asociado a un origen de datos. ID 1 = Citrix Gateway, ID 2 = Citrix Endpoint Management, ID 3 = Citrix Apps and Desktops, ID 4 = Citrix Secure Private Access |
| `entity_id` | Identificador asociado a la entidad en riesgo. |
| `entity_type` | La entidad en riesgo. En este caso, la entidad es un usuario. |
| `event_type` | Tipo de datos enviados al servicio SIEM. En este caso, el tipo de evento es el resumen del indicador de riesgo. |
| `indicator_category` | Indica las categorías de indicadores de riesgo. Los indicadores de riesgo se agrupan en una de las categorías de riesgo: dispositivo de punto final comprometido, usuarios comprometidos, exfiltración de datos o amenazas internas. |
| `indicator_id` | Identificador exclusivo asociado al indicador de riesgo. |
| `indicator_category_id` | El identificador asociado a la categoría de indicador de riesgo. ID 1 = Exfiltración de datos, ID 2 = amenazas internas, ID 3 = usuarios comprometidos, ID 4 = puntos finales comprometidos |
| `indicator_name` | Nombre del indicador de riesgo. Para un indicador de riesgo personalizado, este nombre se define al crear el indicador. |

| Nombre del campo | Descripción |
|---|---|
| `indicator_type` | Indica si el indicador de riesgo es predeterminado (integrado) o personalizado. |
| `indicator_uuid` | Identificador exclusivo asociado a la instancia del indicador de riesgo. |
| `occurrence_details` | Los detalles sobre la condición desencadenante del indicador de riesgo. |
| `pre_configured` | Indica si el indicador de riesgo personalizado está preconfigurado. |
| `risk_probability` | Indica las posibilidades de riesgo asociadas al evento de usuario. El valor varía de 0 a 1,0. Para un indicador de riesgo personalizado, risk_probability siempre es 1.0 porque es un indicador basado en directivas. |
| `severity` | Indica la gravedad del riesgo. Puede ser bajo, medio o alto. |
| `tenant_id` | La identidad única del cliente. |
| `timestamp` | Fecha y hora en que se activa el indicador de riesgo. |
| `ui_link` | El vínculo a la vista de cronograma del usuario en la interfaz de usuario de Citrix Analytics. |
| `version` | Versión del esquema de los datos procesados. La versión actual del esquema es 2. |

En la tabla siguiente se describen los nombres de campo comunes en el esquema de detalles de eventos del indicador de riesgo personalizado.

| Nombre del campo | Descripción |
|---|---|
| `data_source_id` | Identificador asociado a un origen de datos. ID 1 = Citrix Gateway, ID 2 = Citrix Endpoint Management, ID 3 = Citrix Apps and Desktops, ID 4 = Citrix Secure Private Access |
| `indicator_category_id` | El identificador asociado a la categoría de indicador de riesgo. ID 1 = Exfiltración de datos, ID 2 = amenazas internas, ID 3 = usuarios comprometidos, ID 4 = puntos finales comprometidos |

| Nombre del campo | Descripción |
| --- | --- |
| `event_type` | Tipo de datos enviados al servicio SIEM. En este caso, el tipo de evento son los detalles del evento indicador de riesgo. |
| `tenant_id` | La identidad única del cliente. |
| `entity_id` | Identificador asociado a la entidad en riesgo. |
| `entity_type` | Entidad que está en riesgo. En este caso, es el usuario. |
| `indicator_id` | Identificador exclusivo asociado al indicador de riesgo. |
| `indicator_uuid` | Identificador exclusivo asociado a la instancia del indicador de riesgo. |
| `timestamp` | Fecha y hora en que se activa el indicador de riesgo. |
| `version` | Versión del esquema de los datos procesados. La versión actual del esquema es 2. |
| `event_id` | Identificador asociado al evento de usuario. |
| `occurrence_event_type` | Indica el tipo de evento de usuario, como el inicio de sesión, el inicio de sesión y el inicio de sesión de cuenta. |
| `product` | Indica el tipo de aplicación Citrix Workspace, como la aplicación Citrix Workspace para Windows. |
| `client_ip` | Dirección IP del dispositivo del usuario. |
| `session_user_name` | El nombre de usuario asociado a la sesión de Citrix Apps and Desktops. |
| `city` | Nombre de la ciudad desde la que se detecta la actividad del usuario. |
| `country` | Nombre del país desde el que se detecta la actividad del usuario. |
| `device_id` | Nombre del dispositivo utilizado por el usuario. |
| `os_name` | Sistema operativo instalado en el dispositivo del usuario. Para obtener más información, consulte Búsqueda de autoservicio de aplicaciones y escritorios. |

| Nombre del campo | Descripción |
| --- | --- |
| os_version | Versión del sistema operativo instalada en el dispositivo del usuario. Para obtener más información, consulte Búsqueda de autoservicio de aplicaciones y escritorios. |
| os_extra_info | Los detalles adicionales asociados al sistema operativo instalado en el dispositivo del usuario. Para obtener más información, consulte Búsqueda de autoservicio de aplicaciones y escritorios. |

### Indicador de riesgo personalizado para Citrix DaaS y Citrix Virtual Apps and Desktops

#### Esquema resumen de indicadores

```
{

  "data_source": " Citrix Apps and Desktops",
  "data_source_id": 3,
  "entity_id": "demo_user",
  "entity_type": "user",
  "event_type": "indicatorSummary",
  "indicator_category": "Compromised users",
  "indicator_category_id": 3,
  "indicator_id": "ca97a656ab0442b78f3514052d595936",
  "indicator_name": "Demo_user_usage",
  "indicator_type": "custom",
  "indicator_uuid": "8e680e29-d742-4e09-9a40-78d1d9730ea5",
  "occurrence_details": {

    "condition": "User-Name ~ demo_user", "happen": 0, "new_entities":
       "", "repeat": 0, "time_quantity": 0, "time_unit": "", "type": "
       everyTime" }
 ,
  "pre_configured": "N",
  "risk_probability": 1.0,
  "severity": "low",
  "tenant_id": "demo_tenant",
  "timestamp": "2021-02-10T14:47:25Z",
  "ui_link": "https://analytics.cloud.com/user/ ",
  "version": 2
 }
```

#### Esquema de detalles del evento indicador para el suceso de inicio de sesión

```
{

  "event_type": "indicatorEventDetails",
```

```
4    "data_source_id": 3,
5    "indicator_category_id": 3,
6    "tenant_id": "demo_tenant",
7    "entity_id": "demo_user",
8    "entity_type": "user",
9    "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
10   "timestamp": "2021-03-19T10:08:05Z",
11   "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
12   "version": 2,
13   "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
14   "occurrence_event_type": "Session.Logon",
15   "product": "XA.Receiver.Windows",
16   "client_ip": "103.xx.xxx.xxx",
17   "session_user_name": "user01",
18   "city": "Mumbai",
19   "country": "India",
20   "device_id": "5-Synthetic_device",
21   "os_name": "Windows NT 6.1",
22   "os_version": "7601",
23   "os_extra_info": "Service Pack 1",
24   "app_name": "notepad",
25   "launch_type": "Application",
26   "domain": "test_domain",
27   "server_name": "SYD04-MS1-S102",
28   "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
29  }
```

En la siguiente tabla se describen los nombres de campo específicos del esquema de detalles del evento de inicio de sesión.

| Nombre del campo | Descripción |
|---|---|
| `app_name` | Nombre de una aplicación o escritorio iniciados. |
| `launch_type` | Indica la aplicación o el escritorio. |
| `domain` | Nombre de dominio del servidor que envió la solicitud. |
| `server_name` | Nombre del servidor. |
| `session_guid` | GUID de la sesión activa. |

**Esquema de detalles del evento indicador para el evento de inicio de sesión**

```
1  {
2
3    "event_type": "indicatorEventDetails",
4    "data_source_id": 3,
5    "indicator_category_id": 3,
6    "tenant_id": "demo_tenant",
7    "entity_id": "demo_user",
8    "entity_type": "user",
```

```
9    "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
10   "timestamp": "2021-03-19T10:08:05Z",
11   "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
12   "version": 2,
13   "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
14   "occurrence_event_type": "Session.Launch",
15   "product": "XA.Receiver.Windows",
16   "client_ip": "103.xx.xxx.xxx",
17   "session_user_name": "user01",
18   "city": "Mumbai",
19   "country": "India",
20   "device_id": "5-Synthetic_device",
21   "os_name": "Windows NT 6.1",
22   "os_version": "7601",
23   "os_extra_info": "Service Pack 1",
24   "app_name": "notepad",
25   "launch_type": "Application",
26  }
```

En la siguiente tabla se describen los nombres de campo específicos del esquema de detalles del evento para el evento de inicio de sesión.

| Nombre del campo | Descripción |
|---|---|
| app_name | Nombre de una aplicación o escritorio iniciados. |
| launch_type | Indica la aplicación o el escritorio. |

**Esquema de detalles del evento indicador para el evento de inicio de sesión de cuenta**

```
1  {
2
3    "event_type": "indicatorEventDetails",
4    "data_source_id": 3,
5    "indicator_category_id": 3,
6    "tenant_id": "demo_tenant",
7    "entity_id": "demo_user",
8    "entity_type": "user",
9    "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
10   "timestamp": "2021-03-19T10:08:05Z",
11   "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
12   "version": 2,
13   "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
14   "occurrence_event_type": "Account.Logon",
15   "product": "XA.Receiver.Windows",
16   "client_ip": "103.xx.xxx.xxx",
17   "session_user_name": "user01",
18   "city": "Mumbai",
19   "country": "India",
20   "device_id": "5-Synthetic_device",
21   "os_name": "Windows NT 6.1",
22   "os_version": "7601",
```

```
  "os_extra_info": "Service Pack 1",
  "app_name": "notepad",
 }
```

En la siguiente tabla se describen los nombres de campo específicos del esquema de detalles del evento de inicio de sesión de cuenta.

| Nombre del campo | Descripción |
| --- | --- |
| app_name | Nombre de una aplicación o escritorio iniciados. |

**Esquema de detalles del evento indicador para el evento de finalización de sesión**

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "Session.End",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "app_name": "notepad",
  "launch_type": "Application",
  "domain": "test_domain",
  "server_name": "test_server",
  "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
 }
```

En la siguiente tabla se describen los nombres de campo específicos del esquema de detalles del evento de fin de sesión.

| Nombre del campo | Descripción |
| --- | --- |
| app_name | Nombre de una aplicación o escritorio iniciados. |

| Nombre del campo | Descripción |
| --- | --- |
| launch_type | Indica la aplicación o el escritorio. |
| domain | Nombre de dominio del servidor que envió la solicitud. |
| server_name | Nombre del servidor. |
| session_guid | GUID de la sesión activa. |

**Esquema de detalles del evento indicador para el evento de inicio de la aplicación**

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "App.Start",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "app_name": "notepad",
  "launch_type": "Application",
  "domain": "test_domain",
  "server_name": "test_server",
  "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
  "module_file_path": "/root/folder1/folder2/folder3"
 }
```

En la siguiente tabla se describen los nombres de campo específicos del esquema de detalles del evento de inicio de la aplicación.

| Nombre del campo | Descripción |
| --- | --- |
| app_name | Nombre de una aplicación o escritorio iniciados. |
| launch_type | Indica la aplicación o el escritorio. |

| Nombre del campo | Descripción |
| --- | --- |
| domain | Nombre de dominio del servidor que envió la solicitud. |
| server_name | Nombre del servidor. |
| session_guid | GUID de la sesión activa. |
| module_file_path | Ruta de acceso de la aplicación que se está utilizando. |

**Esquema de detalles del evento indicador para el evento final de la aplicación**

```
1  {
2
3    "event_type": "indicatorEventDetails",
4    "data_source_id": 3,
5    "indicator_category_id": 3,
6    "tenant_id": "demo_tenant",
7    "entity_id": "demo_user",
8    "entity_type": "user",
9    "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
10   "timestamp": "2021-03-19T10:08:05Z",
11   "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
12   "version": 2,
13   "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
14   "occurrence_event_type": "App.End",
15   "product": "XA.Receiver.Windows",
16   "client_ip": "103.xx.xxx.xxx",
17   "session_user_name": "user01",
18   "city": "Mumbai",
19   "country": "India",
20   "device_id": "5-Synthetic_device",
21   "os_name": "Windows NT 6.1",
22   "os_version": "7601",
23   "os_extra_info": "Service Pack 1",
24   "app_name": "notepad",
25   "launch_type": "Application",
26   "domain": "test_domain",
27   "server_name": "test_server",
28   "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
29   "module_file_path": "/root/folder1/folder2/folder3"
30  }
```

En la siguiente tabla se describen los nombres de campo específicos del esquema de detalles del evento de finalización de la aplicación.

| Nombre del campo | Descripción |
| --- | --- |
| app_name | Nombre de una aplicación o escritorio iniciados. |

| Nombre del campo | Descripción |
| --- | --- |
| launch_type | Indica la aplicación o el escritorio. |
| domain | Nombre de dominio del servidor que envió la solicitud. |
| server_name | Nombre del servidor. |
| session_guid | GUID de la sesión activa. |
| module_file_path | Ruta de acceso de la aplicación que se está utilizando. |

**Esquema de detalles del evento indicador para el evento de descarga de archivos**

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "File.Download",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "file_download_file_name": "File5.txt",
  "file_download_file_path": "/root/folder1/folder2/folder3",
  "file_size_in_bytes": 278,
  "launch_type": "Desktop",
  "domain": "test_domain",
  "server_name": "test_server",
  "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
  "device_type": "USB"
 }
```

En la siguiente tabla se describen los nombres de campo específicos del esquema de detalles del evento de descarga de archivos.

| Nombre del campo | Descripción |
| --- | --- |
| file_download_file_name | Nombre del archivo de descarga. |
| file_download_file_path | Ruta de destino en la que se descarga el archivo. |
| launch_type | Indica la aplicación o el escritorio. |
| domain | Nombre de dominio del servidor que envió la solicitud. |
| server_name | Nombre del servidor. |
| session_guid | GUID de la sesión activa. |
| device_type | Indica el tipo de dispositivo en el que se descarga el archivo. |

**Esquema de detalles del evento indicador para el evento de impresión**

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "Printing",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "printer_name": "Test-printer",
  "launch_type": "Desktop",
  "domain": "test_domain",
  "server_name": "test_server",
  "session_guid": "f466e318-9065-440c-84a2-eec49d978a96",
  "job_details_size_in_bytes": 454,
  "job_details_filename": "file1.pdf",
  "job_details_format": "PDF"
 }
```

En la siguiente tabla se describen los nombres de campo específicos del esquema de detalles del

evento de impresión.

| Nombre del campo | Descripción |
|---|---|
| printer_name | Nombre de la impresora utilizada para el trabajo de impresión. |
| launch_type | Indica la aplicación o el escritorio. |
| domain | Nombre de dominio del servidor que envió la solicitud. |
| server_name | Nombre del servidor. |
| session_guid | GUID de la sesión activa. |
| job_details_size_in_bytes | El tamaño del trabajo impreso, como un archivo o una carpeta. |
| job_details_filename | Nombre del archivo impreso. |
| job_details_format | Formato del trabajo impreso. |

**Esquema de detalles del evento indicador para el evento de lanzamiento de SaaS de la aplicación**

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "App.SaaS.Launch",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "launch_type": "Desktop",
 }
```

En la siguiente tabla se describen los nombres de campo específicos del esquema de detalles del evento para el evento de lanzamiento de SaaS de la aplicación.

| Nombre del campo | Descripción |
| --- | --- |
| launch_type | Indica la aplicación o el escritorio. |

**Esquema de detalles del evento indicador para el evento final de SaaS de la aplicación**

```
{

  "event_type": "indicatorEventDetails",
  "data_source_id": 3,
  "indicator_category_id": 3,
  "tenant_id": "demo_tenant",
  "entity_id": "demo_user",
  "entity_type": "user",
  "indicator_id": "9033b2f6a8914a9282937b35ce497bcf",
  "timestamp": "2021-03-19T10:08:05Z",
  "indicator_uuid": "e0abfcb4-fd41-4612-ad59-ef7567508ac0",
  "version": 2,
  "event_id": "8fc3dd5e-d049-448a-ab70-0fc4d554e41e",
  "occurrence_event_type": "App.SaaS.End",
  "product": "XA.Receiver.Windows",
  "client_ip": "103.xx.xxx.xxx",
  "session_user_name": "user01",
  "city": "Mumbai",
  "country": "India",
  "device_id": "5-Synthetic_device",
  "os_name": "Windows NT 6.1",
  "os_version": "7601",
  "os_extra_info": "Service Pack 1",
  "launch_type": "Desktop",
 }
```

En la siguiente tabla se describen los nombres de campo específicos del esquema de detalles del evento para el evento final de SaaS de la aplicación.

| Nombre del campo | Descripción |
| --- | --- |
| launch_type | Indica la aplicación o el escritorio. |

## Eventos de fuentes de datos

Además, puede configurar la función de exportación de datos para exportar eventos de usuario desde sus fuentes de datos de productos habilitadas para Citrix Analytics for Security. Al realizar cualquier actividad en el entorno Citrix, se generan los eventos del origen de datos. Los eventos exportados son datos de uso de usuarios y productos en tiempo real sin procesar, tal como están disponibles en la vista de autoservicio. Los metadatos contenidos en estos eventos se pueden utilizar además para

realizar un análisis más profundo de las amenazas, crear nuevos paneles y correlacionarlos con otros eventos de fuentes de datos que no sean de Citrix en su infraestructura de TI y seguridad.

Actualmente, Citrix Analytics for Security envía eventos de usuario a su SIEM para la fuente de datos de Citrix Virtual Apps and Desktops.

## Detalles del esquema de los eventos del origen de datos

### Eventos de Citrix Virtual Apps and Desktops

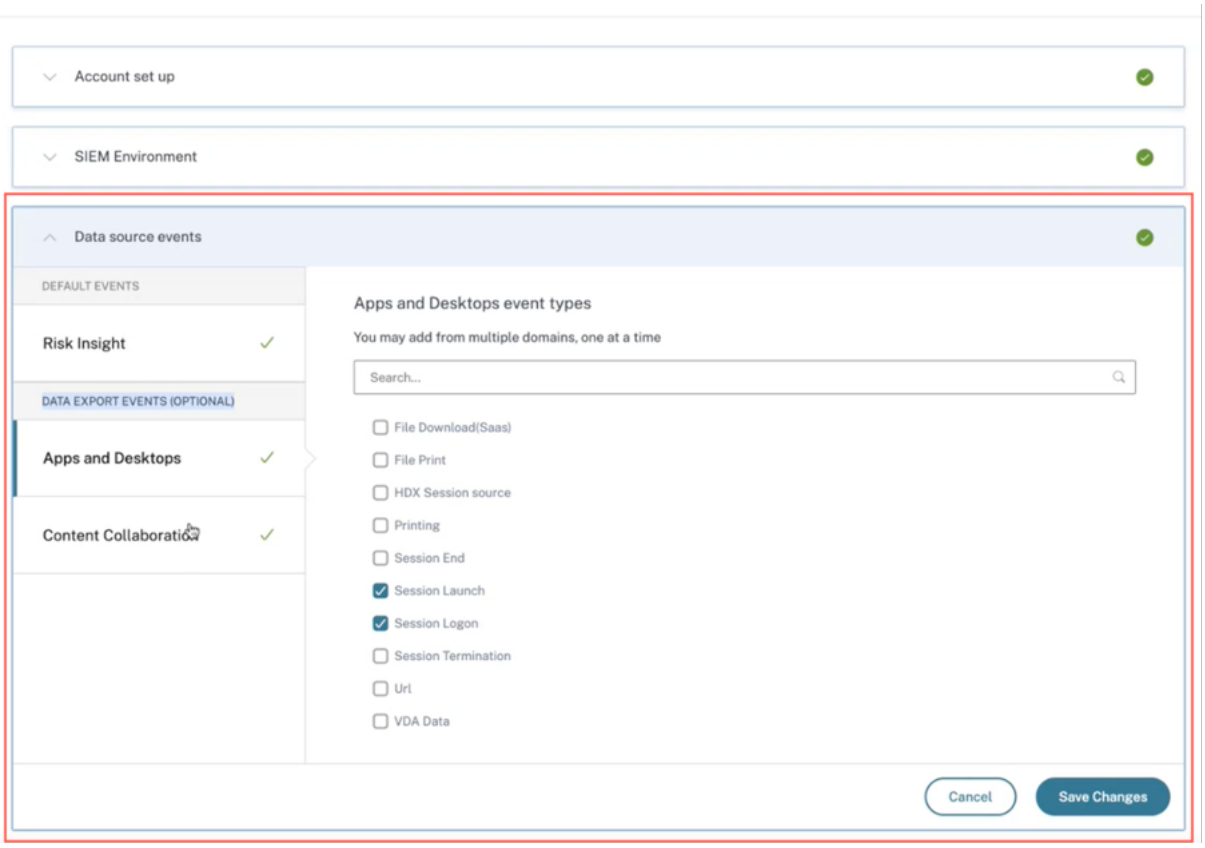
Los eventos de usuario se reciben en tiempo real en Citrix Analytics for Security cuando los usuarios utilizan aplicaciones virtuales o escritorios virtuales. Para obtener más información, consulte Origen de datos de Citrix Virtual Apps and Desktops y Citrix DaaS. Puede ver los siguientes eventos de usuario asociados a Citrix Virtual Apps and Desktops en su SIEM:

- Todos los tipos de eventos
- Inicio de sesión de cuenta
- Aplicación (inicio, lanzamiento, fin)
- Portapapeles
- Archivo (imprimir, descargar)
- Descarga de archivos (SaaS)
- Fuente de sesión HDX
- Impresión
- Sesión (inicio, inicio, finalización, finalización)
- URL
- Datos de VDA
- Creación de procesos de VDA

Para obtener más información sobre los eventos y sus atributos, consulte Búsqueda de autoservicio para Virtual Apps and Desktops.

Puede revisar qué tipos de eventos están habilitados y fluyen a SIEM. Puede configurar o eliminar el tipo de evento aplicable a un arrendatario y hacer clic en el botón **Guardar cambios** para guardar la configuración.




## Aprovechar el modelo de datos SIEM de Citrix Analytics para el análisis de amenazas y la correlación de datos

June 19, 2023

En este artículo se explica la relación entre los datos de la entidad que muestran los eventos enviados al entorno SIEM de un cliente. Para aclarar esto, tomemos un ejemplo de un escenario de búsqueda de amenazas en el que los atributos (la IP del cliente y el sistema operativo) son los puntos focales. Se analizarán las siguientes formas de correlacionar dichos atributos con el usuario:

- Uso de información personalizada sobre indicadores de riesgo
- Uso de eventos de fuentes de datos

Splunk es el entorno SIEM elegido para mostrarse en el siguiente ejemplo. También se puede realizar una correlación de datos similar en Sentinel mediante la plantilla de libro de trabajo de Citrix Analytics. Para explorar esto más a fondo, consulte el libro de trabajo de Citrix Analytics para Microsoft Sentinel.

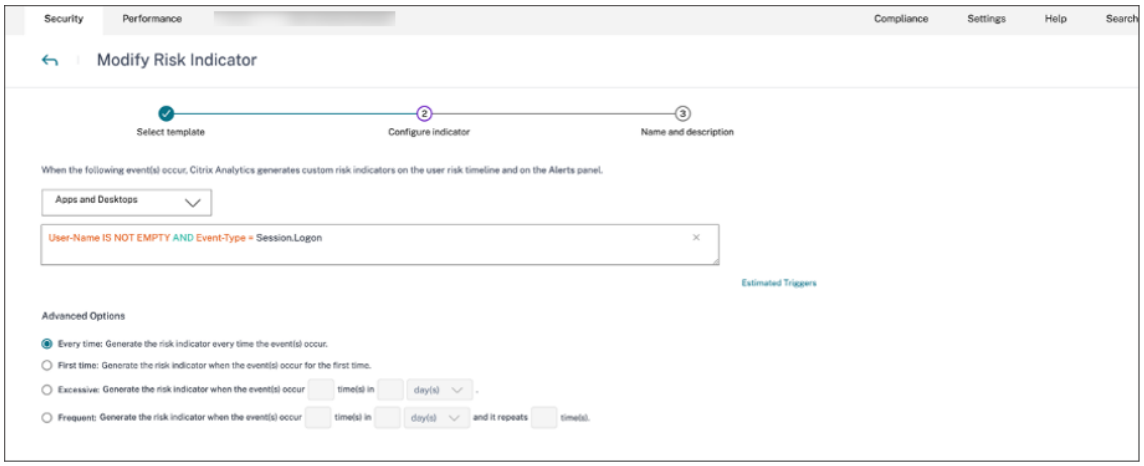
 

## Información sobre indicadores de riesgo personalizados

Como se menciona en el formato de exportación de datos de Citrix Analytics para SIEM, el resumen de los indicadores y los detalles de los eventos forman parte del conjunto de datos de información de riesgo predeterminado. Para el conjunto de datos del indicador Citrix Virtual Apps and Desktops, la IP y el sistema operativo del cliente se exportan de forma predeterminada. Por lo tanto, si un administrador configura un indicador personalizado con o sin la condición que incluya estos campos, dichos puntos de datos fluirán a su entorno de Splunk.

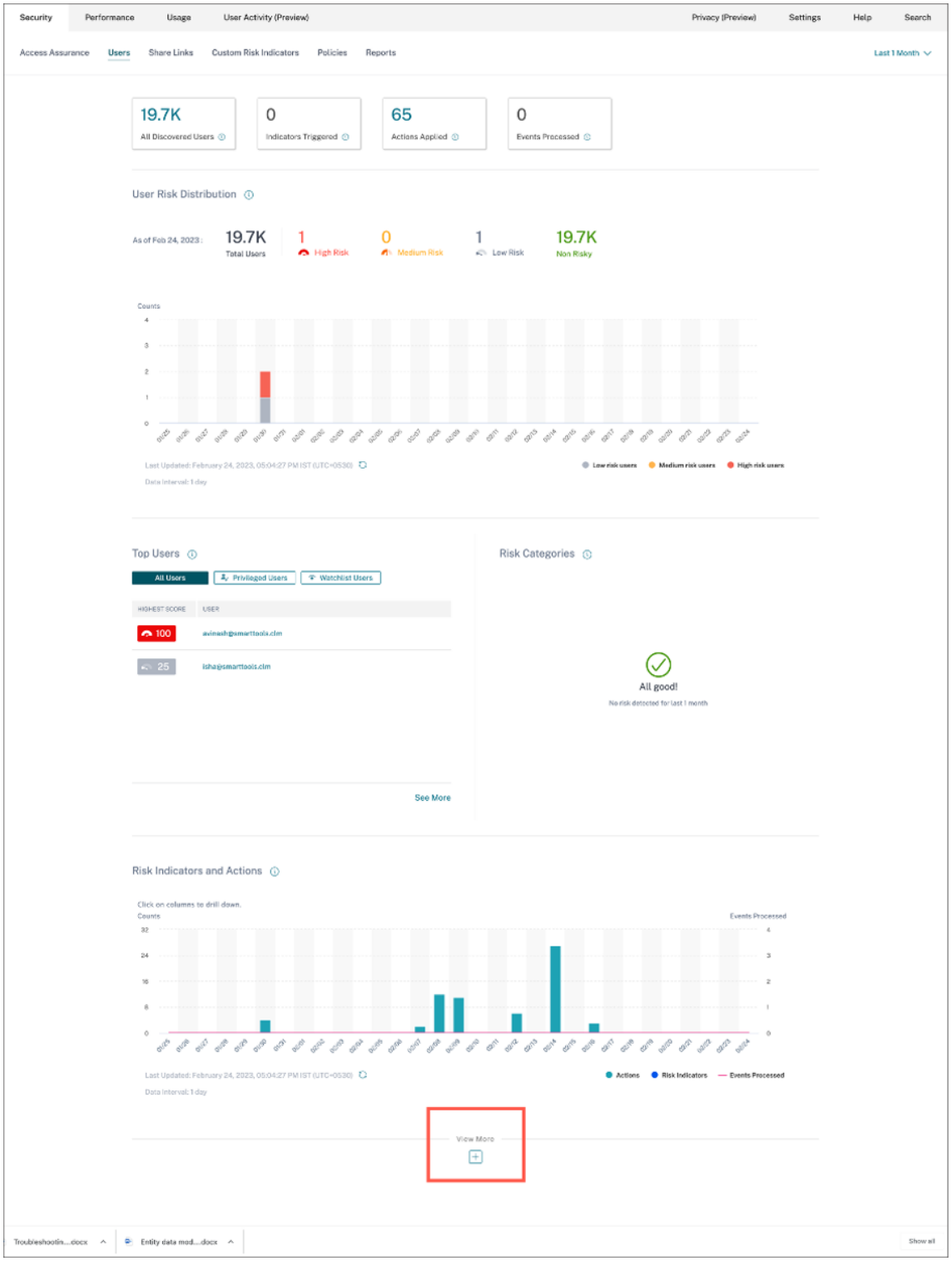
### Configuración de un indicador de riesgo personalizado en Citrix Analytics

1. Vaya al **panel de control de Citrix Analytics for Security > Indicadores de riesgo personalizados > Crear indicador**. Puede crear un indicador de riesgo personalizado con cualquier condición que le ayude a monitorear el comportamiento del usuario. Después de configurar el indicador personalizado, todos los usuarios que activan la condición asociada estarán visibles en su entorno de Splunk.



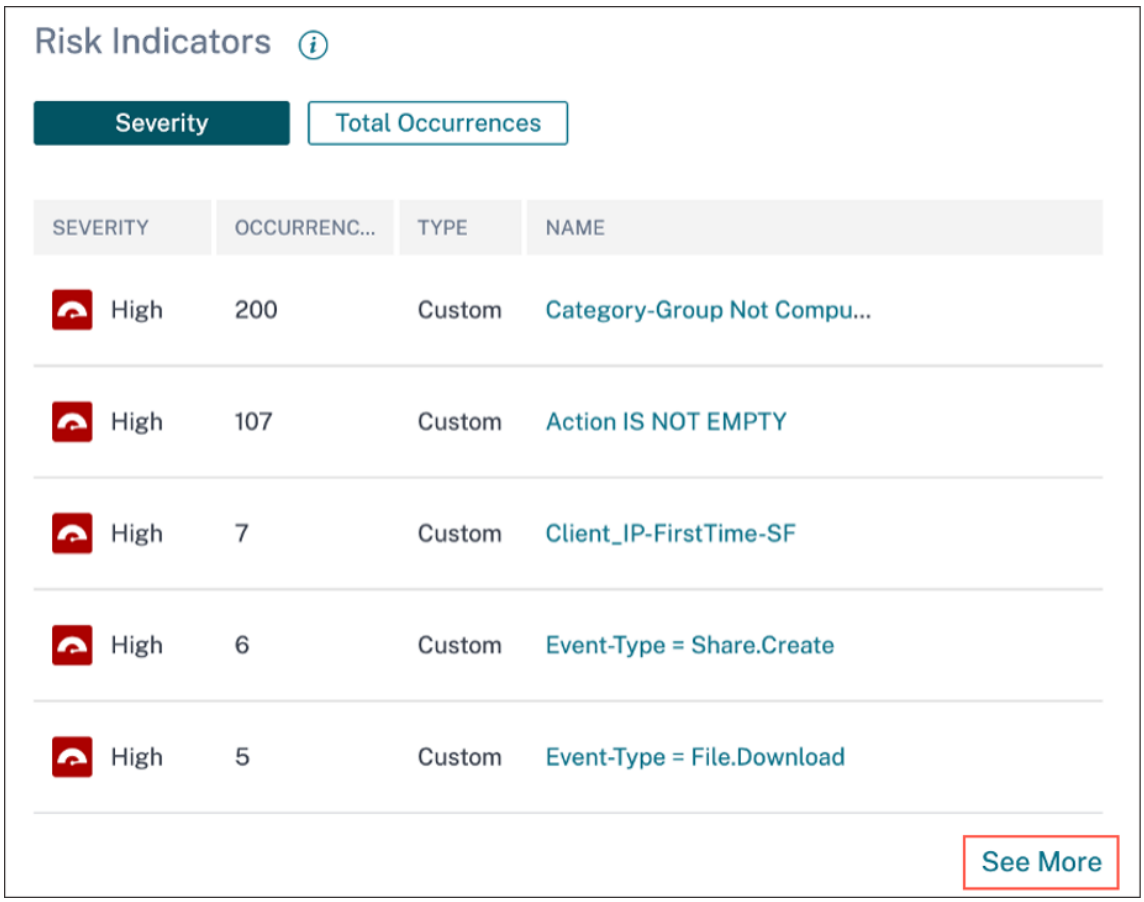

2. Para ver las ocurrencias de los indicadores de riesgo creados en Citrix Analytics for Security, vaya a **Seguridad > Usuarios. Navega hasta la parte inferior de la página y haz clic en el icono con el signo más (+)**.

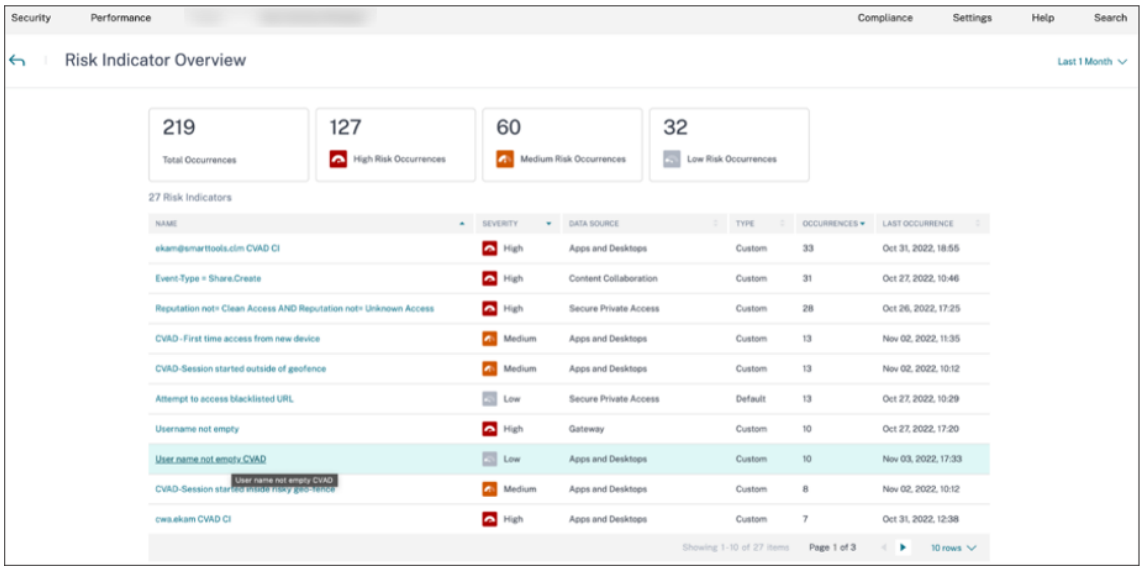



Aparece la tarjeta de indicadores de riesgo. Puede ver los detalles del indicador de riesgo, la gravedad y la incidencia.



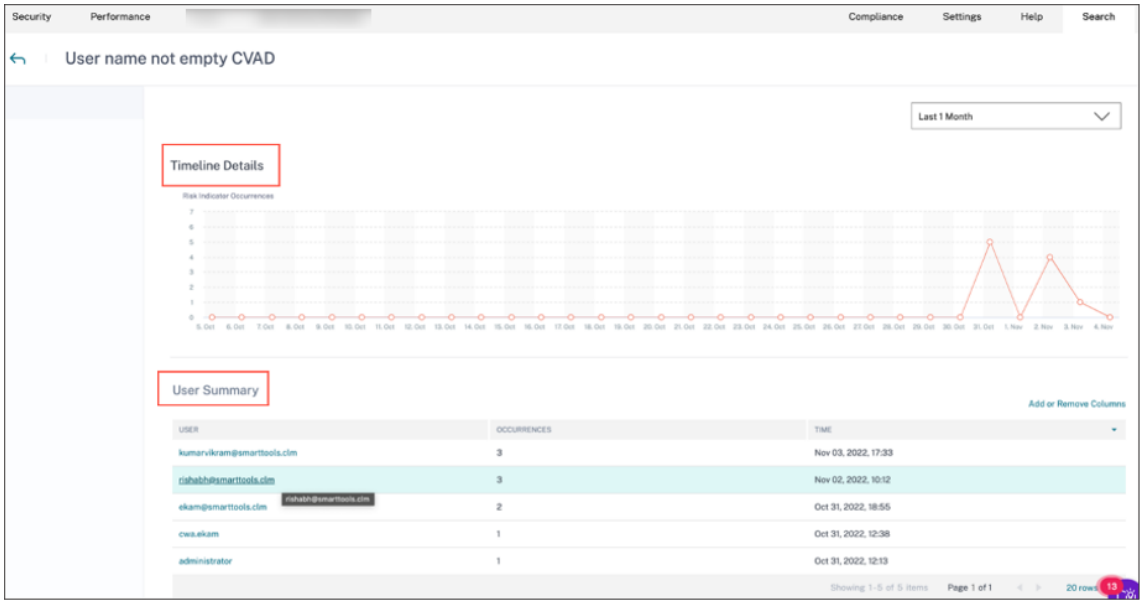

3. Haz clic en **Ver más**. Aparece la página de **descripción general del** indicador de riesgo.




En la página de descripción general del indicador de riesgo, puede ver los detalles del usuario que activó el indicador con una vista cronológica detallada y un resumen del usuario. Para obtener más información sobre el cronograma, consulte Cronología y perfil de riesgo del

usuario.



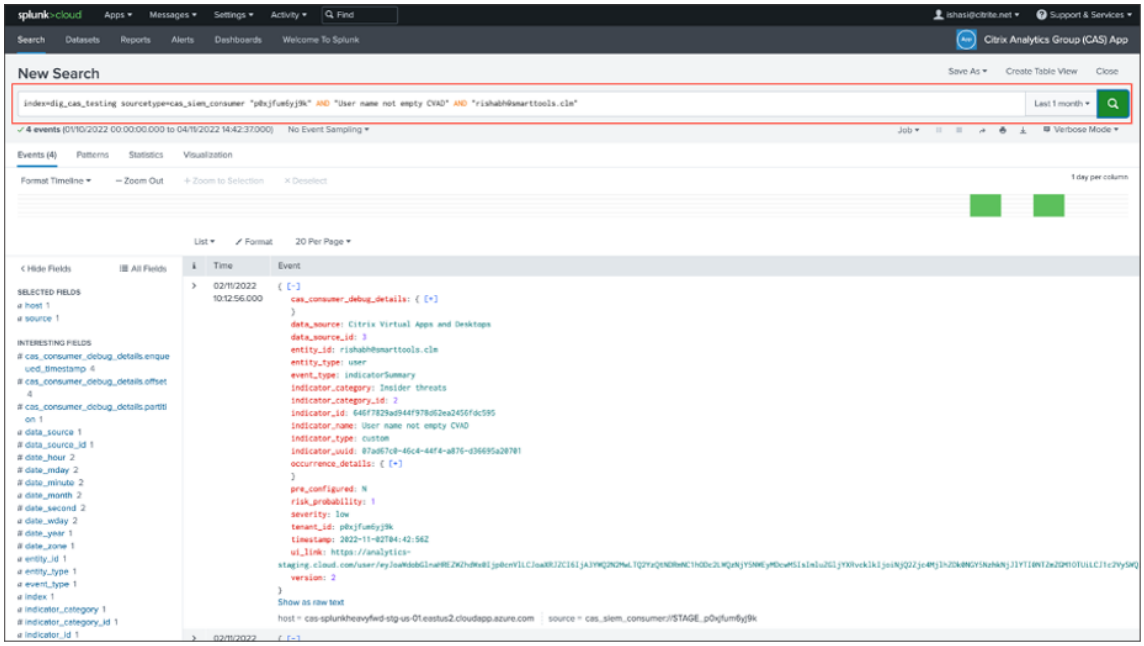

### Apariciones de indicadores de riesgo en Splunk: consultas sin procesar

También puede obtener la información sobre la IP y el sistema operativo del cliente mediante el índice y el tipo de fuente que utilizó el administrador de la infraestructura de Splunk al configurar la entrada de datos en el complemento Splunk Enterprise para Citrix Analytics for Security.

1. Ve a **Splunk > Nueva búsqueda**. En la consulta de búsqueda, introduzca y ejecute la siguiente consulta:

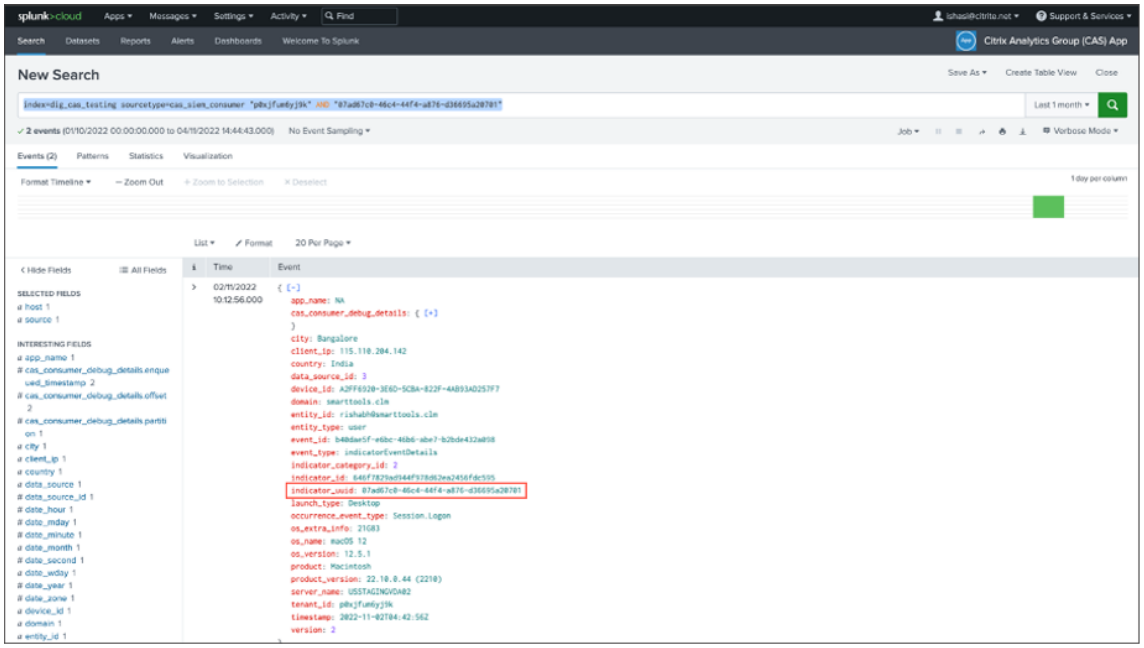
```
index=<index configured by you> sourcetype=<sourcetype configured by you> AND "<tenant_id>" AND "<indicator name configured by you on CAS>" AND "<user you are interested in>"
```




2. Recoge el indicator_uuid y ejecuta la siguiente consulta:

```
index=<index configured by you> sourcetype=<sourcetype configured by you> "<tenant_id>" AND "<indicator_uuid>"
```




El resultado del evento contiene el **resumen del evento** del **indicador y los detalles del evento** del indicador (la actividad que desencadena el indicador). El detalle del evento contiene la **información del sistema operativo** y la **IP del cliente** (nombre, versión, información adicional).

Para obtener más información sobre el formato de datos, consulte el formato de exportación de datos de Citrix Analytics para SIEM.

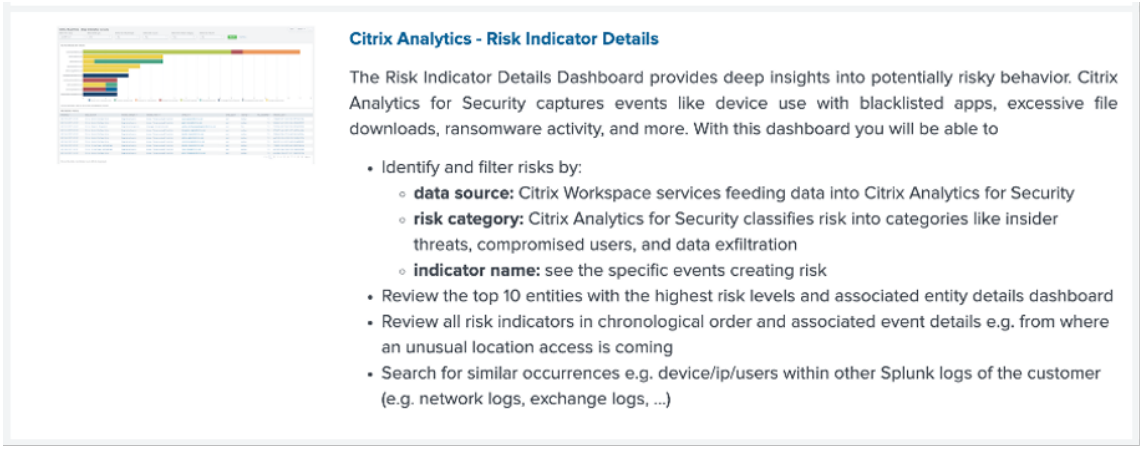
 

### Indicadores de riesgo que aparecen en la aplicación Splunk - Dashboarding

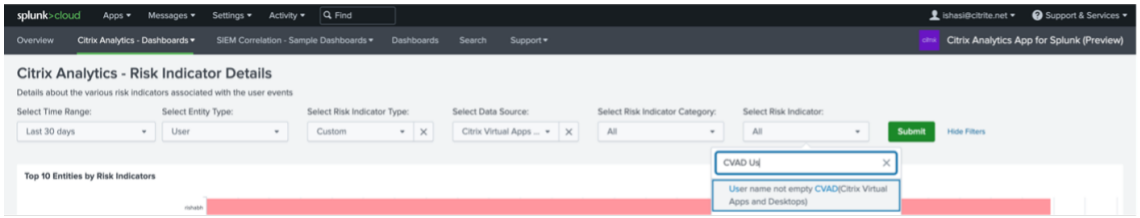
Consulte los siguientes artículos para obtener instrucciones sobre cómo instalar la aplicación Citrix Analytics para Splunk:

- Aplicación Citrix Analytics para Splunk
- Paneles de Citrix Analytics para Splunk

1. Haga clic en la pestaña **Citrix Analytics** —**Panel** de control y seleccione la opción **Detalles del indicador de riesgo** en la lista desplegable.

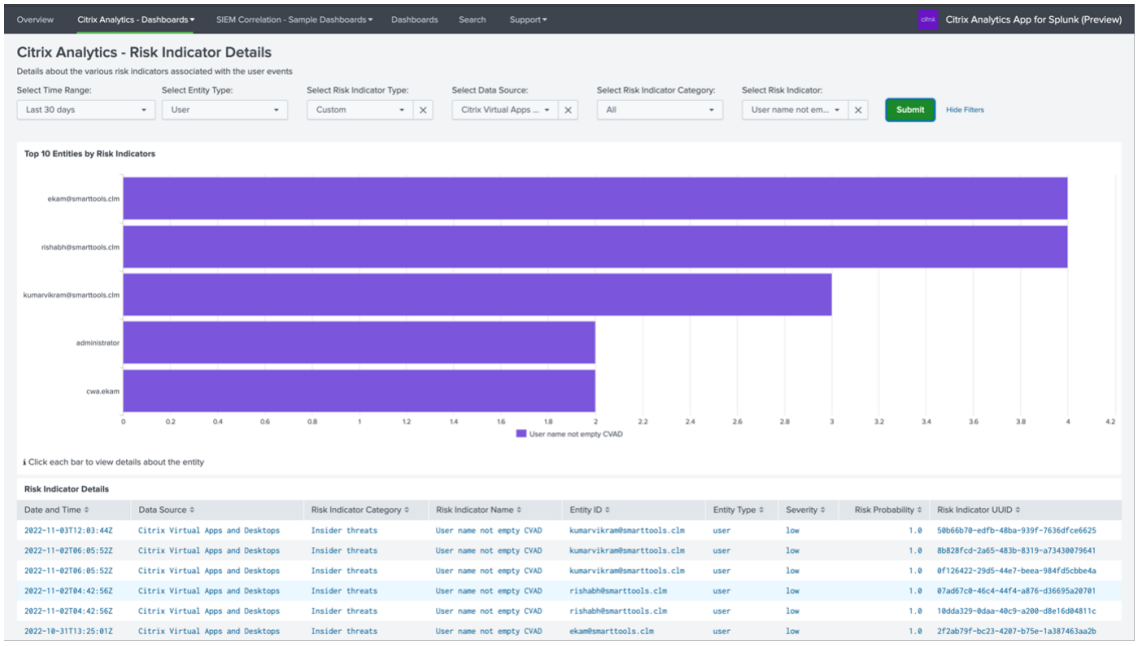



2. Filtre el contenido de la lista desplegable de forma adecuada y haga clic en **Enviar**.

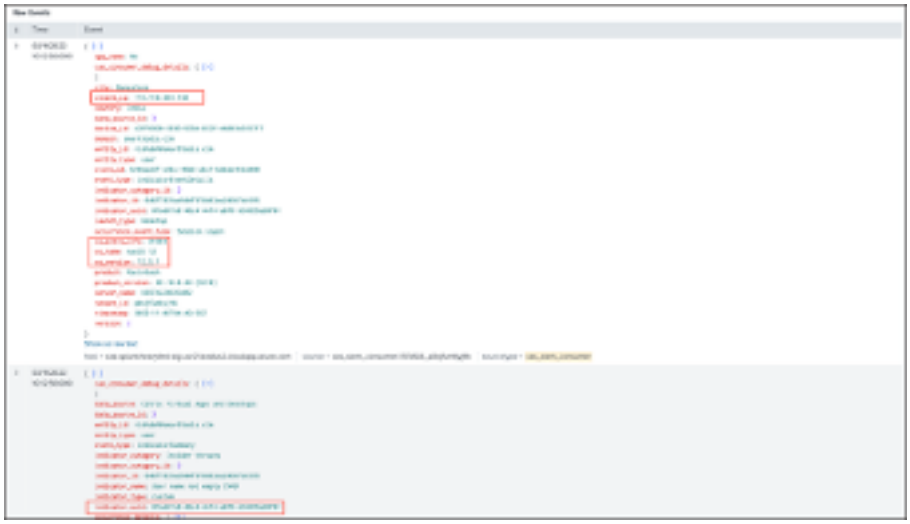



3. Haga clic en la instancia de usuario para obtener los detalles.




4. Puede ver la **información sobre la IP y el sistema operativodel cliente** (nombre, versión, información adicional) en la parte inferior de esta página:



## Eventos de fuentes de datos

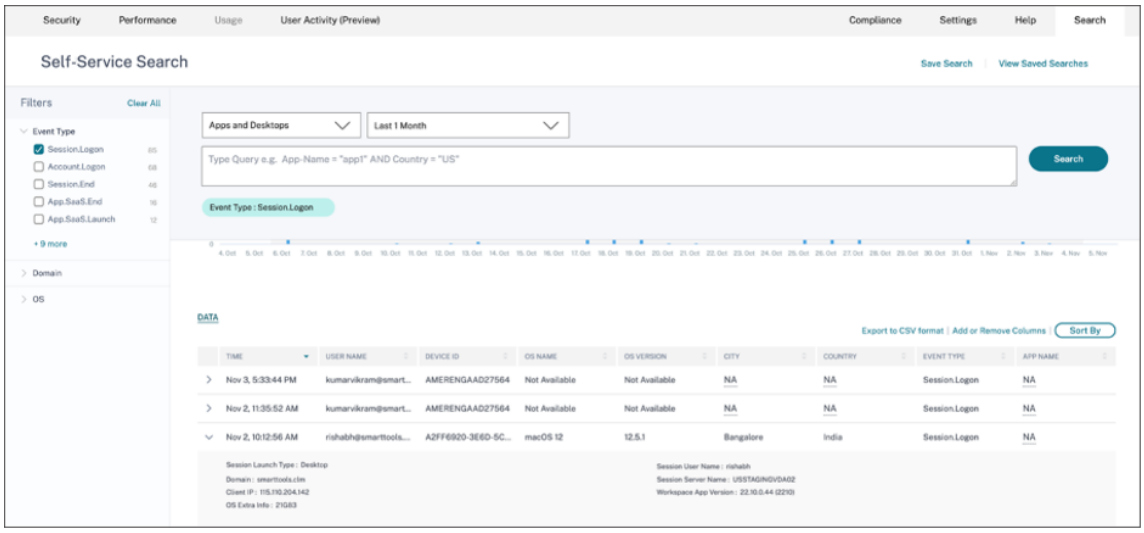
Otro método para obtener la IP del cliente y los detalles del sistema operativo en su entorno de Splunk consiste en configurar los eventos de la fuente de datos para su exportación. Esta función permite que los eventos presentes en la vista de búsqueda automática fluyan directamente a su entorno de Splunk. Para obtener más información sobre cómo configurar los tipos de eventos para que las Virtual Apps and Desktops se exporten a SIEM, consulte los siguientes artículos:

- Eventos de datos exportados de Citrix Analytics for Security a su servicio SIEM.

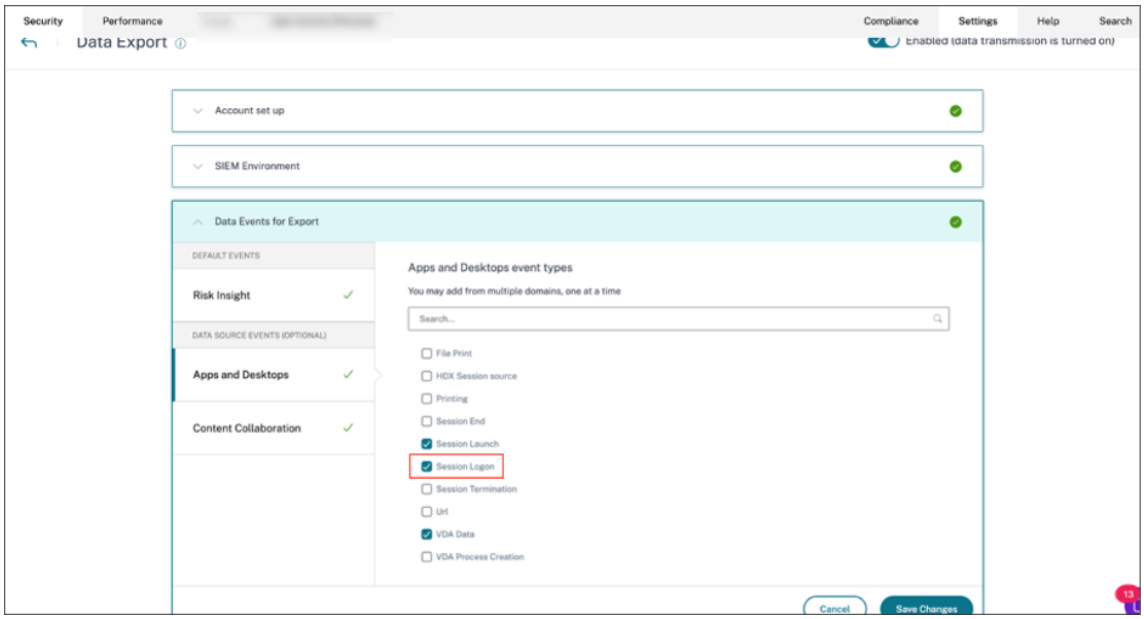
 

- Eventos de fuentes de datos

1. Vaya al **panel de control de Citrix Analytic for Security > Buscar**. En esta página de búsqueda automática, están disponibles todos los tipos de eventos y su información relacionada. Puede ver el tipo de evento **Session.Logon** como ejemplo en la siguiente captura de pantalla:




2. Configura **Session.Logon** en los eventos de la fuente de datos para exportarlos y pulsa **Guardar** para que fluya a tu entorno de Splunk.

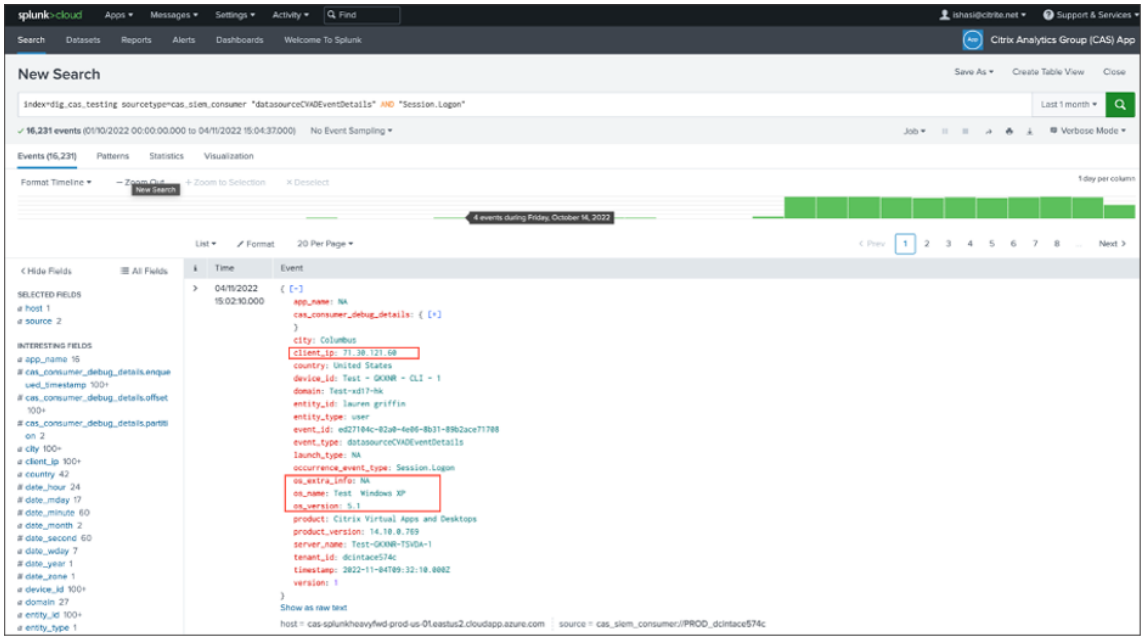



3. Ve a Splunk y, a continuación, introduce y ejecuta la siguiente consulta:

```
index="<index you configured>" sourcetype="<sourcetype you
    configured>" "<tenant_id>" AND "datasourceCVADEventDetails" AND
     "Session.Logon"  AND "<user you ' re interested in>"
```

Los campos relacionados con la IP y el sistema operativo del cliente están resaltados.

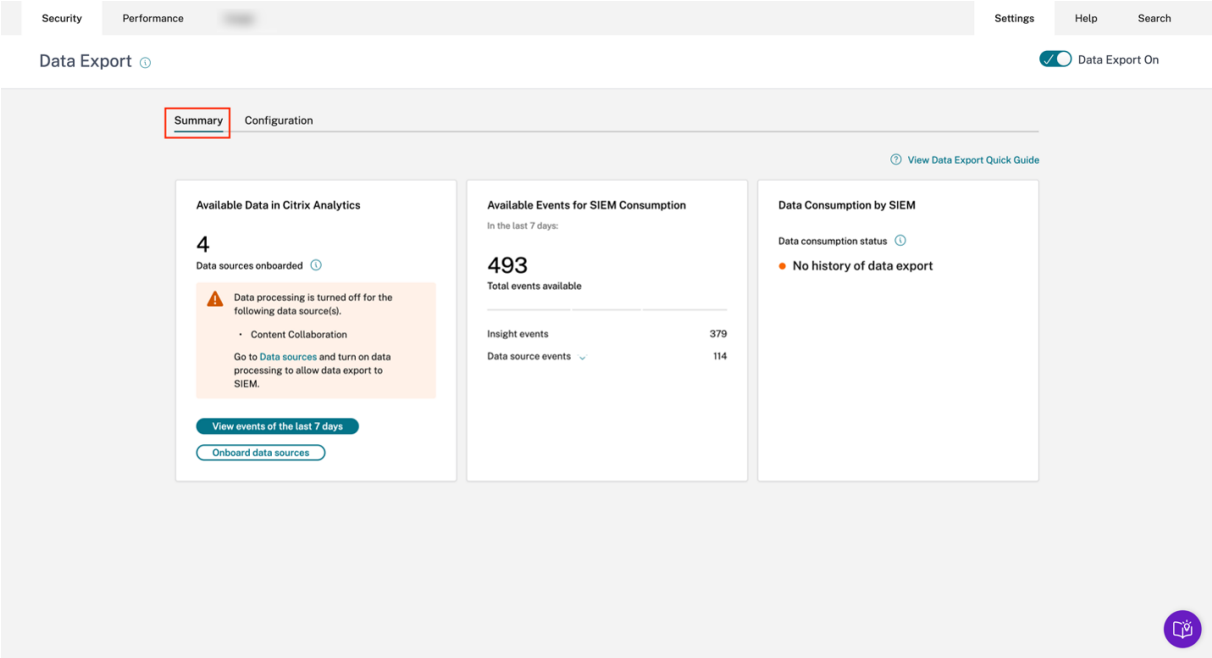



## Solución de problemas de exportación de datos

December 7, 2023

La vista Exportaciones de datos por motivos de seguridad incluye una ficha de **resumen** para ayudar a los administradores a solucionar problemas de integración de SIEM con Citrix Analytics. El panel de **resumen** proporciona visibilidad sobre el estado y el flujo de los datos al guiarlos por los puntos de control que ayudan al proceso de solución de problemas.



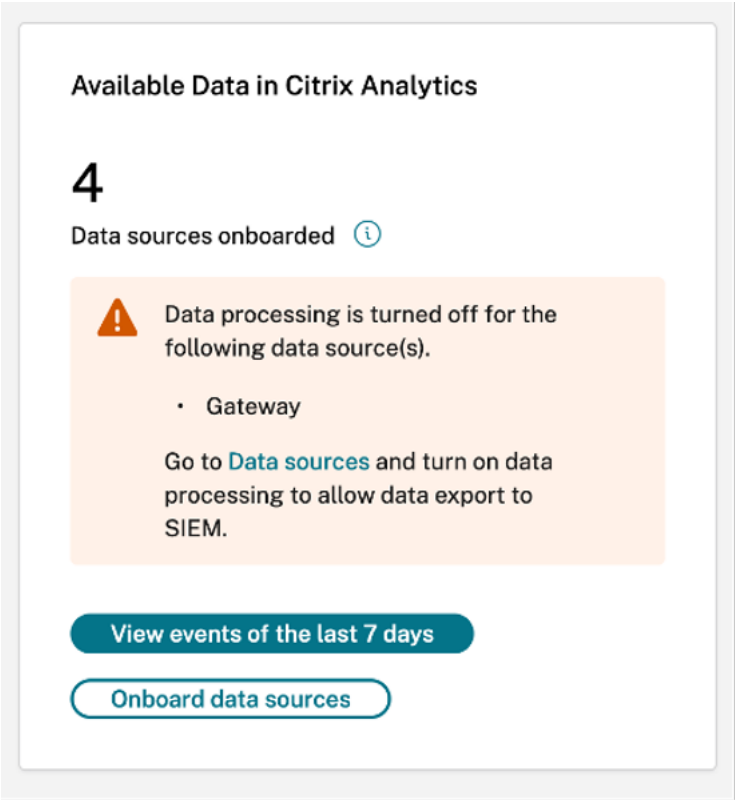

## Ficha Resumen

La ficha **Resumen** constituye la base del flujo de trabajo de solución de problemas de autoservicio en la vista de exportaciones de datos. Describe la configuración de su SIEM mediante estas tres tarjetas:

- **Datos disponibles en Citrix Analytics**: esta tarjeta muestra el estado de las configuraciones de las fuentes de datos.
- **Eventos disponibles para el consumo de SIEM**: esta tarjeta muestra la cantidad de eventos que están listos para ser consumidos por su entorno SIEM.
- **Consumo de datos por SIEM**: esta tarjeta muestra el estado del flujo de datos en su entorno SIEM.

**Datos disponibles en Citrix Analytics**

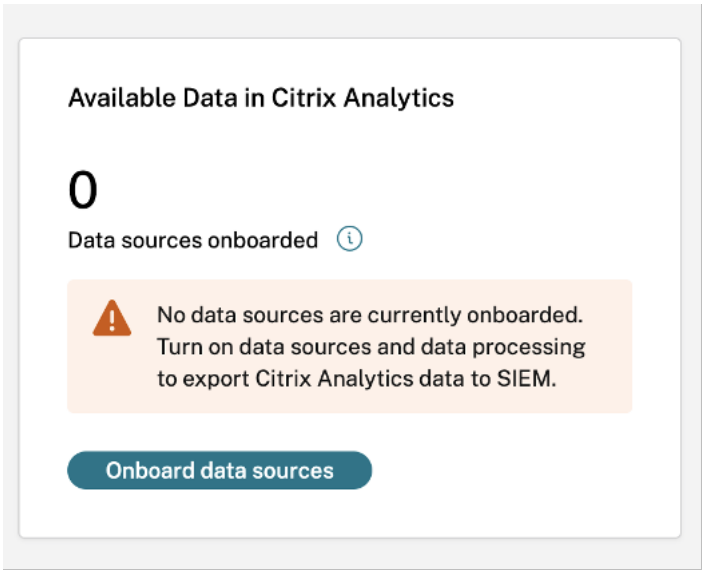



La tarjeta **Datos disponibles en Citrix Analytics** muestra la cantidad de fuentes de datos que eventualmente pueden contribuir a la información de SIEM que se han incorporado a Citrix Analytics for Security. Actualmente, se admiten tres fuentes de datos para la exportación de datos: Apps and Desktops, Gateway y Secure Private Access. Incluso si se han incorporado estas fuentes de datos, la exportación de datos no funcionará para las fuentes de datos que tengan el procesamiento de datos desactivado. Cuando se detectan dichas fuentes de datos, se muestra un mensaje de advertencia apropiado, como el que se muestra en la imagen de arriba.

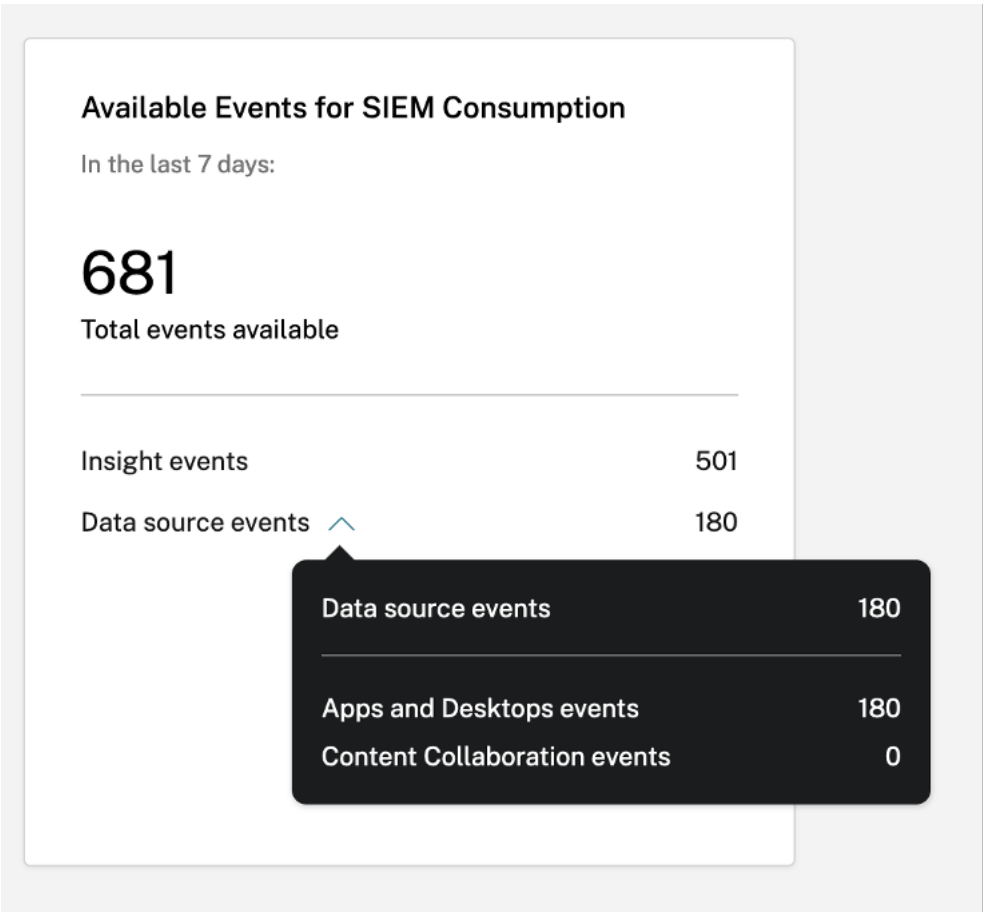
El botón **Ver eventos de los últimos 7 días** redirige al administrador a la vista de búsqueda de autoservicio, a través de la cual los administradores pueden comprobar que los eventos han llegado a Citrix Analytics for Security. El botón **Incorporar fuentes de datos** redirige a la vista Fuentes de datos, donde puede ver el proceso de incorporación en profundidad.

Si no hay fuentes de datos incorporadas, se muestra un mensaje de advertencia apropiado, como se muestra en la siguiente captura de pantalla:




**Eventos disponibles para el consumo de SIEM**




La tarjeta **Eventos disponibles para el consumo de SIEM** muestra la cantidad de eventos de Insight y de fuentes de datos, junto con su desglose, que se espera que lleguen a su entorno SIEM. Tras la

expansión, también está disponible un desglose adicional de cada tipo de evento de datos para la exportación.

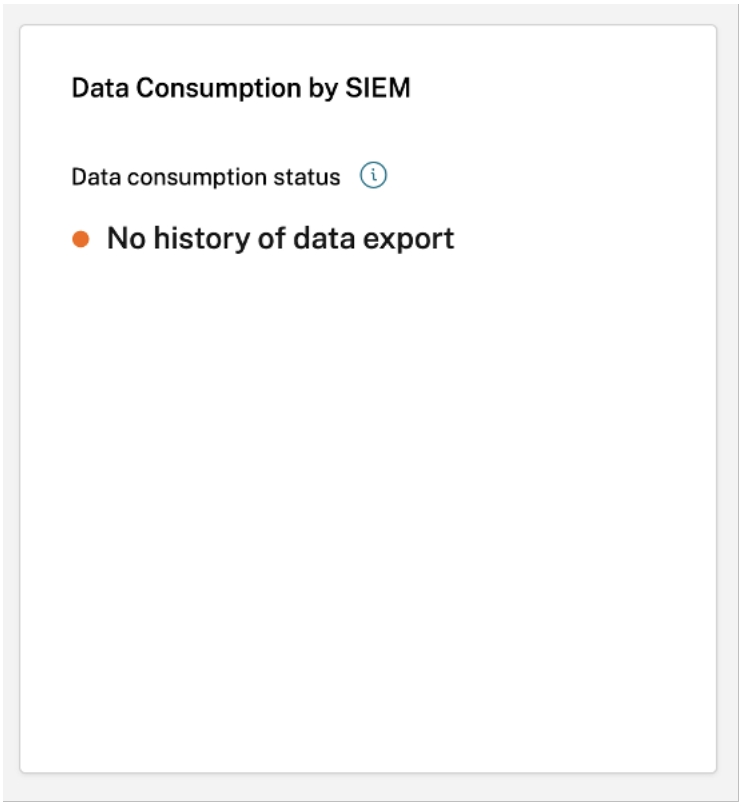
#### Consumo de datos por SIEM

La tarjeta **Consumo de datos por SIEM** muestra el estado del flujo de datos preparado por Citrix Analytics en su entorno SIEM. El estado del consumo de datos se basa en el movimiento de desfase dentro del tema de **Kafka**. Cuando está disponible, la tarjeta también muestra la fecha y hora de la última vez que se detectó un consumo de datos correcto. Tanto el estado del consumo de datos como la marca de tiempo se actualizan cada 10 minutos. Haga clic aquí para obtener más información sobre la gestión de grupos de consumidores y compensaciones de Kafka.

El estado de consumo de datos puede adoptar los siguientes estados:

1. **Consumo inactivo**

   - **Sin historial de exportación de datos**: este estado se representa con un punto naranja para indicar que ningún dato preparado por Citrix Analytics ha llegado correctamente a su entorno SIEM.




     Esto puede deberse a -

     – Configuración de fuente de datos incorrecta/incompleta. La tarjeta **Datos disponibles en Citrix Analytics** se puede utilizar para comprobar si hay sufi-

cientes fuentes de datos y si tienen activado el procesamiento de datos para permitir la exportación.

- Falta de actividad de los usuarios. El botón **Ver los eventos de los últimos 7 días** de la tarjeta **Datos disponibles en Citrix Analytics** se puede utilizar para comprobar la ausencia de actividad del usuario. Además, la tarjeta **Events for SIEM Consumption** se puede utilizar para comprobar si Citrix Analytics ha preparado algún evento de Insight o fuente de datos para fluir a su SIEM.
- Configuración de SIEM incorrecta/incompleta. Compruebe que la etapa de configuración de la cuenta en la ficha **Configuración** se haya completado correctamente. Si la configuración se ha completado, aparecerá una marca de verificación verde en la etapa de configuración de la cuenta.

  Si el estado no cambia incluso después de configurar correctamente la cuenta, solucione el problema comprobando lo siguiente:

  * Problemas con el firewall o ajustes de SIEM mal configurados; consulte Configuración del entorno SIEM.
  * Problemas de credenciales con la configuración de la cuenta de Kafka o su entorno SIEM; consulte Integración de SIEMmediante Kafka.

- **No se ha detectado ningún consumo activo**: este estado indica que, al menos en los últimos 10 minutos, los datos no han llegado correctamente a su entorno SIEM. La tarjeta también mostrará la fecha y hora del último movimiento de datos correcto. Al igual que con **Sin historial de exportación de datos**, puede solucionar este problema utilizando las tarjetas **Datos disponibles en Citrix Analytics** y **Eventos disponibles para el consumo de SIEM**. Si hay suficiente actividad de los usuarios y aumenta el recuento de eventos disponibles, sería una buena idea centrarse en la última marca de tiempo correcta para comprobar si se ha producido algún cambio en el firewall o si se ha producido algún cambio de contraseña después de dicha marca de tiempo.


- **Exportado hace más de 7 días**: este estado indica que el consumo activo en su SIEM se detectó por última vez hace más de una semana. Al igual que en los dos estados anteriores, utilice los **datos disponibles en Citrix Analytics** y las tarjetas **Available Events for SIEM Consumption para solucionar problemas de configuración de SIEM si este es el estado de consumo** de datos detectado.

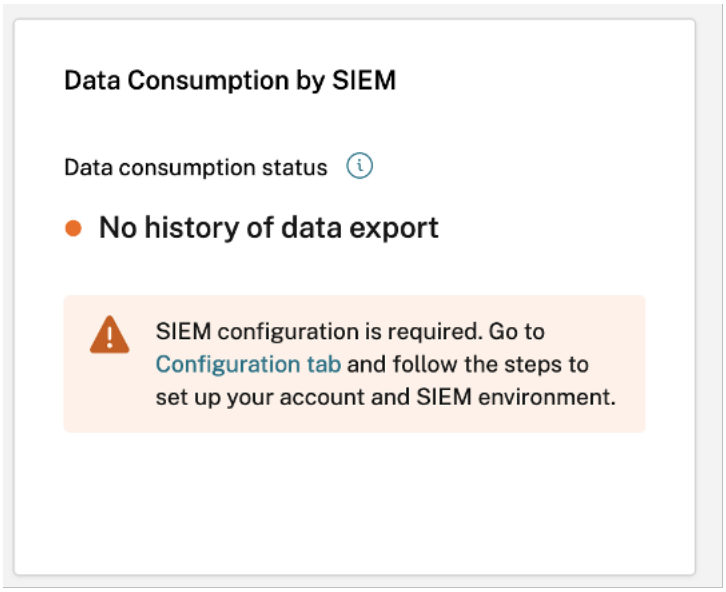

> **Nota**
>
> **Directiva de retención de Kafka**: los temas de Citrix Analytics Kafka conservan los

> eventos solo durante un máximo de 7 días. Para evitar o prevenir la posible pérdida de datos, se recomienda configurar un intervalo de sondeo de datos que no supere los 7 días.

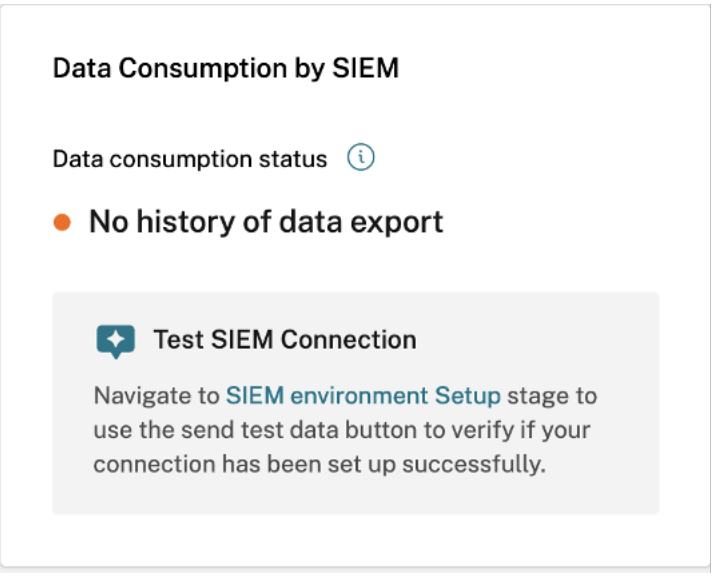
En consumo inactivo, puedes ver los siguientes mensajes de advertencia que te ayudarán a navegar por el proceso de solución de problemas.

Como se destacó en el caso **Sin historial de exportación de datos**, si la configuración del SIEM no se completa, ningún dato fluye al entorno SIEM. Por lo tanto, se redirige al usuario a la ficha **Configuración** para completar la configuración de la cuenta, como se muestra en la siguiente captura de pantalla:



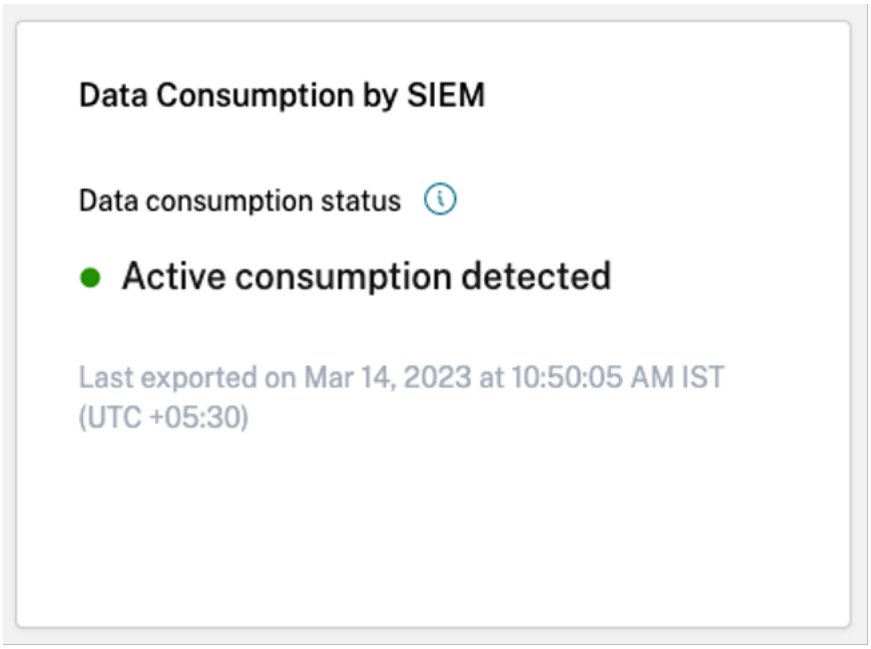

Si se completa la configuración del SIEM, es posible que los datos no fluyan activamente, como se muestra en el estado **No se detectó ni exportó consumo activo** o **Hace más de 7 días**. Por lo tanto, se recomienda al usuario que vaya a la sección **Generación de eventos** de prueba para probar la conexión SIEM, tal como se indica en el siguiente mensaje de advertencia.




2. **Consumo activo**

   - **Consumo activo detectado**: este estado indica que se ha detectado un consumo activo en su SIEM.

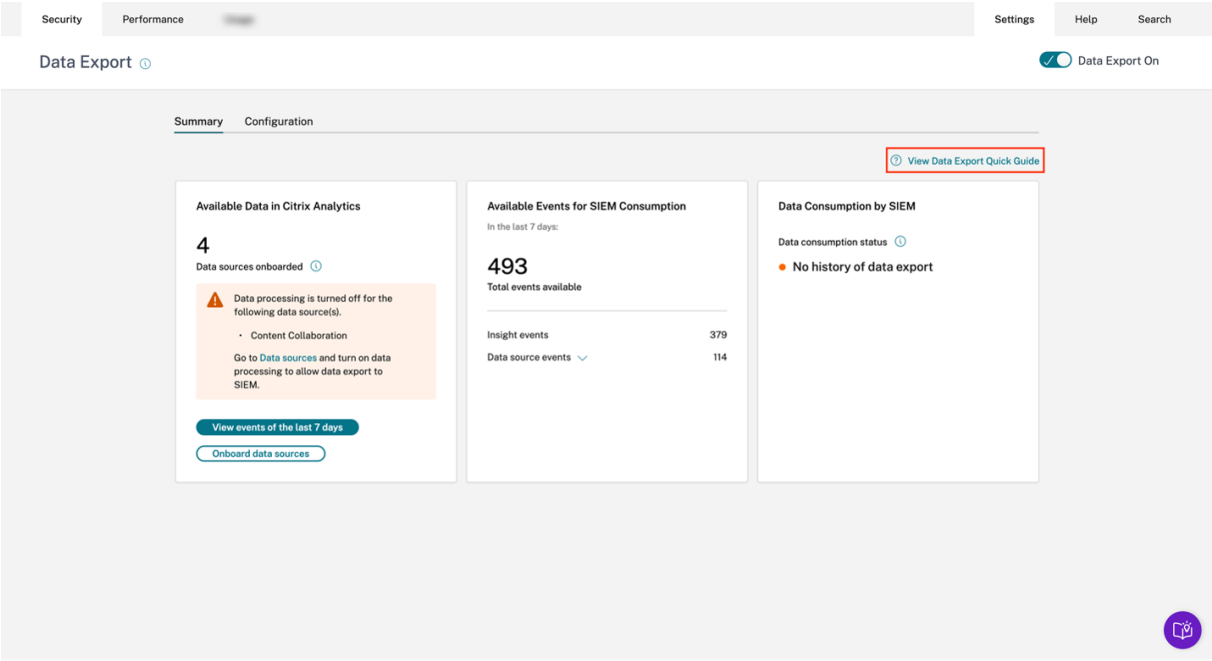


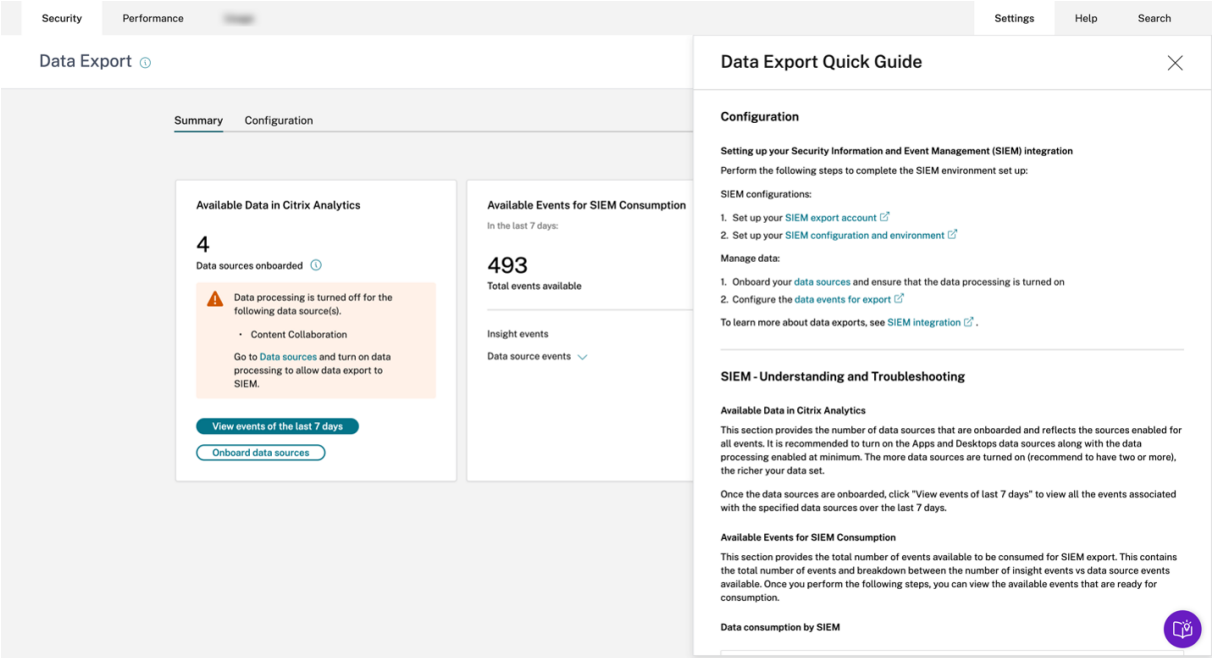

### Guía rápida de exportación de datos

La ficha **Resumen** se complementa con la **guía rápida de exportación de datos** para facilitar la implementación, la administración y la solución de problemas de las configuraciones de SIEM. Además de proporcionar una guía completa sobre la vista Exportación de datos por motivos de seguridad, la

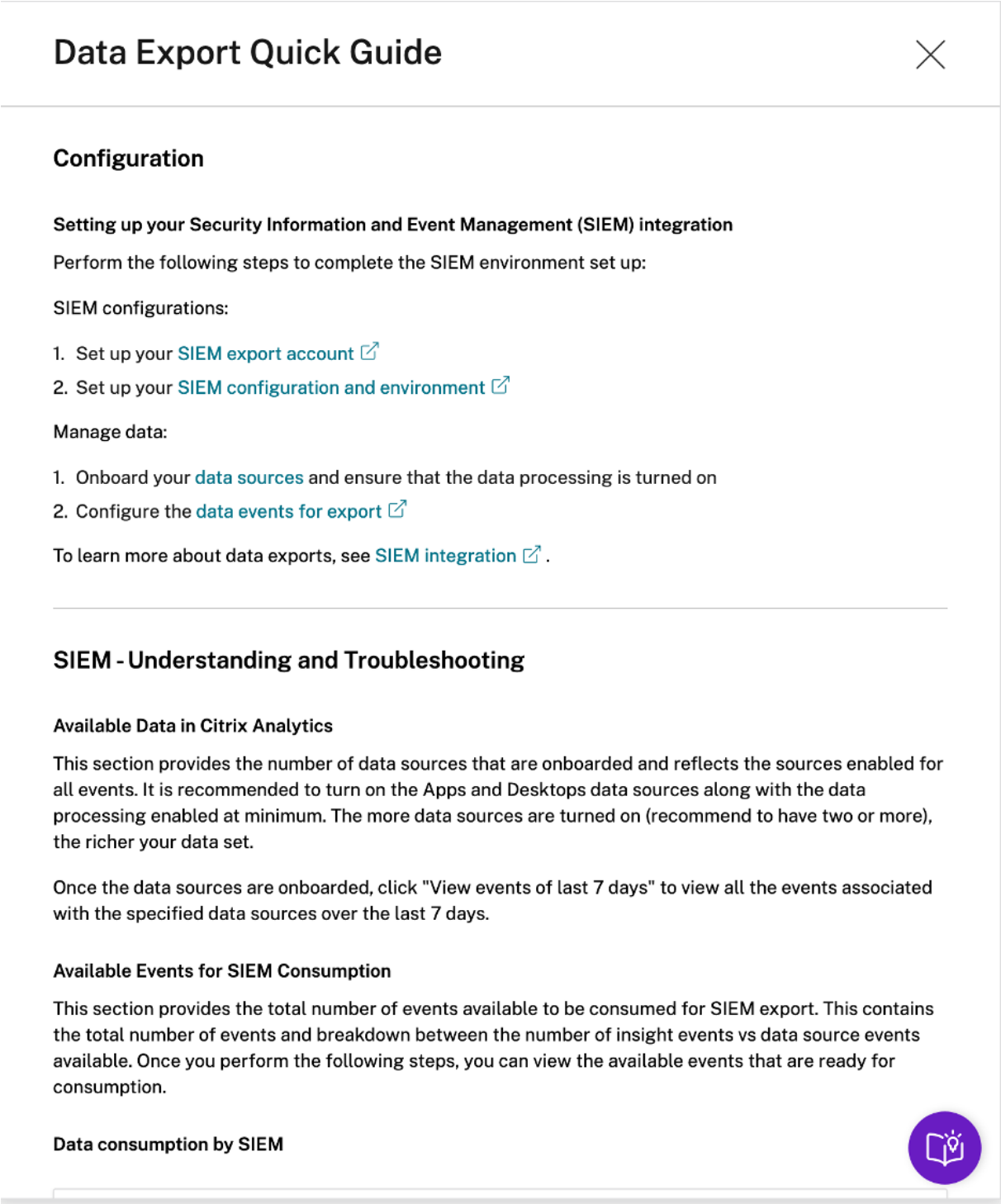
 

Guía rápida también incluye consejos útiles sobre cómo configurar y administrar su entorno SIEM al proporcionar enlaces a la documentación pertinente.





# Data Export Quick Guide

## Configuration

**Setting up your Security Information and Event Management (SIEM) integration**

Perform the following steps to complete the SIEM environment set up:

SIEM configurations:

1. Set up your SIEM export account
2. Set up your SIEM configuration and environment

Manage data:

1. Onboard your data sources and ensure that the data processing is turned on
2. Configure the data events for export

To learn more about data exports, see SIEM integration .

## SIEM - Understanding and Troubleshooting

**Available Data in Citrix Analytics**

This section provides the number of data sources that are onboarded and reflects the sources enabled for all events. It is recommended to turn on the Apps and Desktops data sources along with the data processing enabled at minimum. The more data sources are turned on (recommend to have two or more), the richer your data set.

Once the data sources are onboarded, click "View events of last 7 days" to view all the events associated with the specified data sources over the last 7 days.

**Available Events for SIEM Consumption**

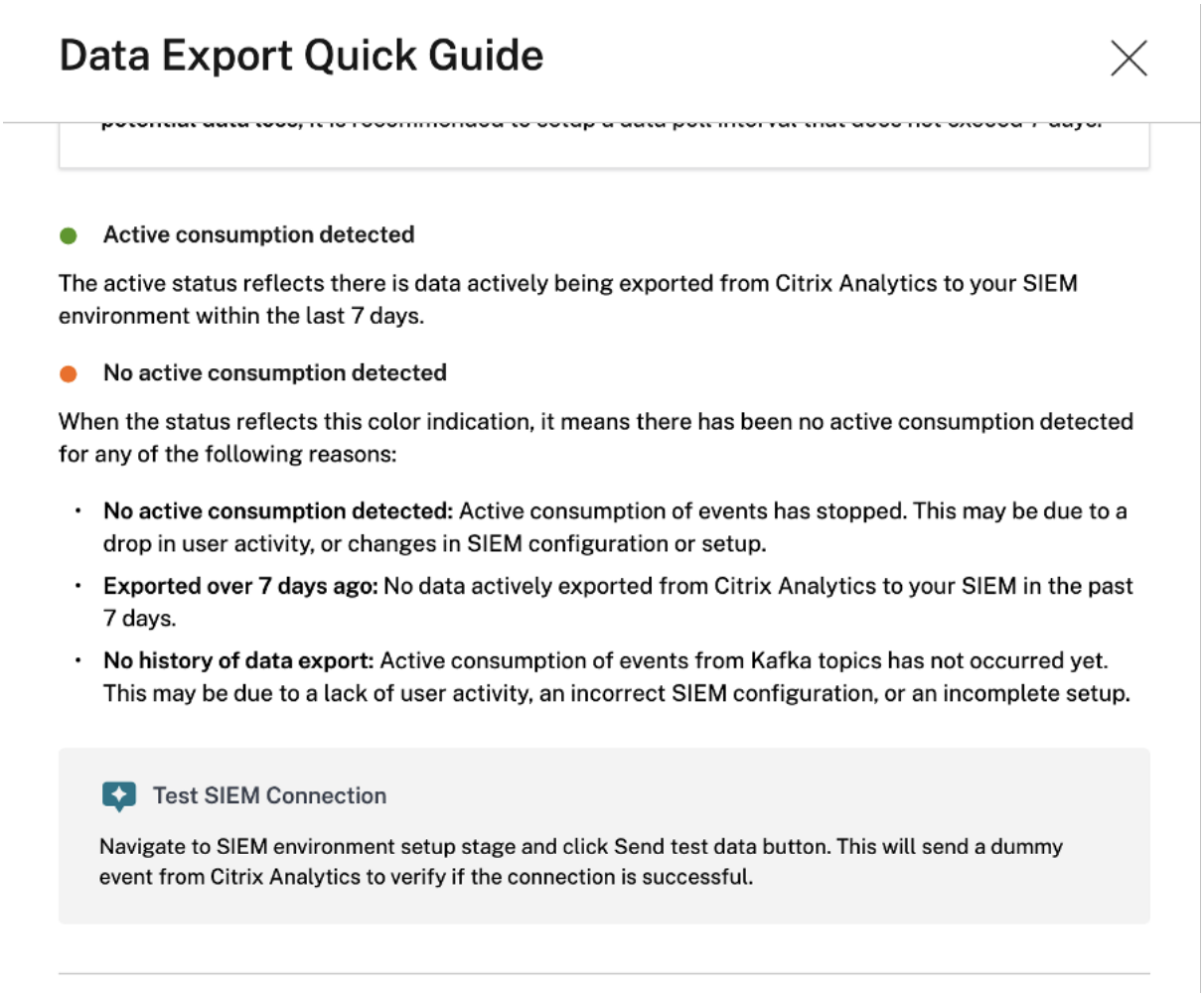
This section provides the total number of events available to be consumed for SIEM export. This contains the total number of events and breakdown between the number of insight events vs data source events available. Once you perform the following steps, you can view the available events that are ready for consumption.

**Data consumption by SIEM**

También hay una sección de **prueba de conexión a SIEM** en el módulo de guía rápida que redirige al usuario a la etapa de prueba de conexión a SIEM dentro de la etapa de configuración del entorno SIEM. Esto permite al usuario investigar si la integración de SIEM está rota en sí misma, lo que descarta la posibilidad de que se produzcan problemas con el procesamiento de los eventos por parte de Citrix Analytics for Security. A continuación, el usuario puede arreglar la conexión SIEM para habilitar el

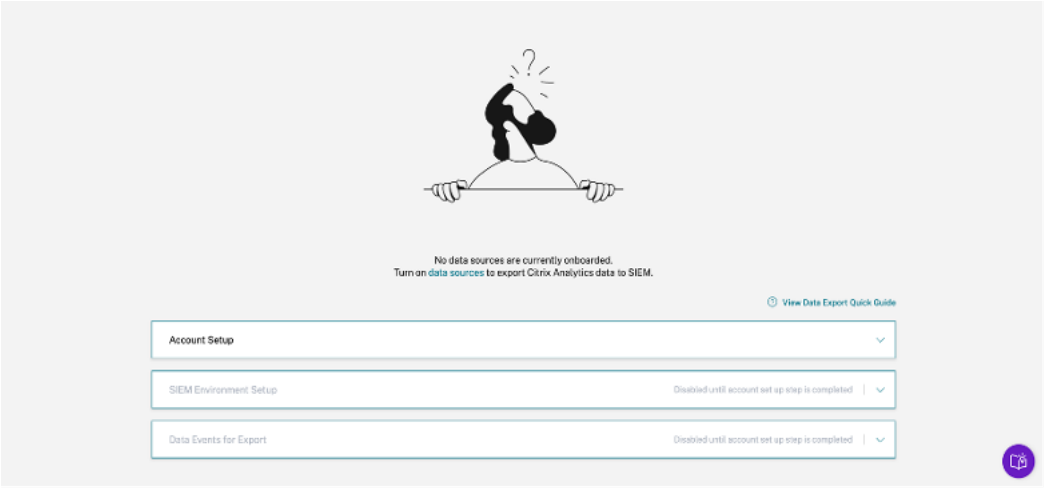
flujo de datos.



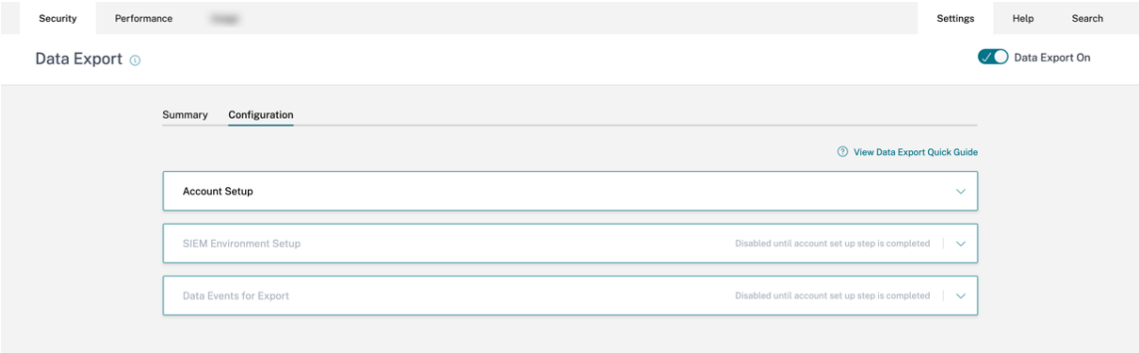

La ficha **Configuración**, al mismo tiempo que guía a través de la configuración de la implementación, también ayuda a los administradores con consejos útiles, mensajes de advertencia y errores comunes al configurar su SIEM. Se muestran las advertencias apropiadas cuando:

- Citrix Analytics detecta que no se ha incorporado ninguna fuente de datos. Se recomienda incorporar Apps and Desktops para recopilar telemetría en función de la actividad del usuario. En ausencia de la fuente de datos incorporada, no se observa ningún flujo de datos, aunque la configuración del SIEM se haya realizado correctamente.

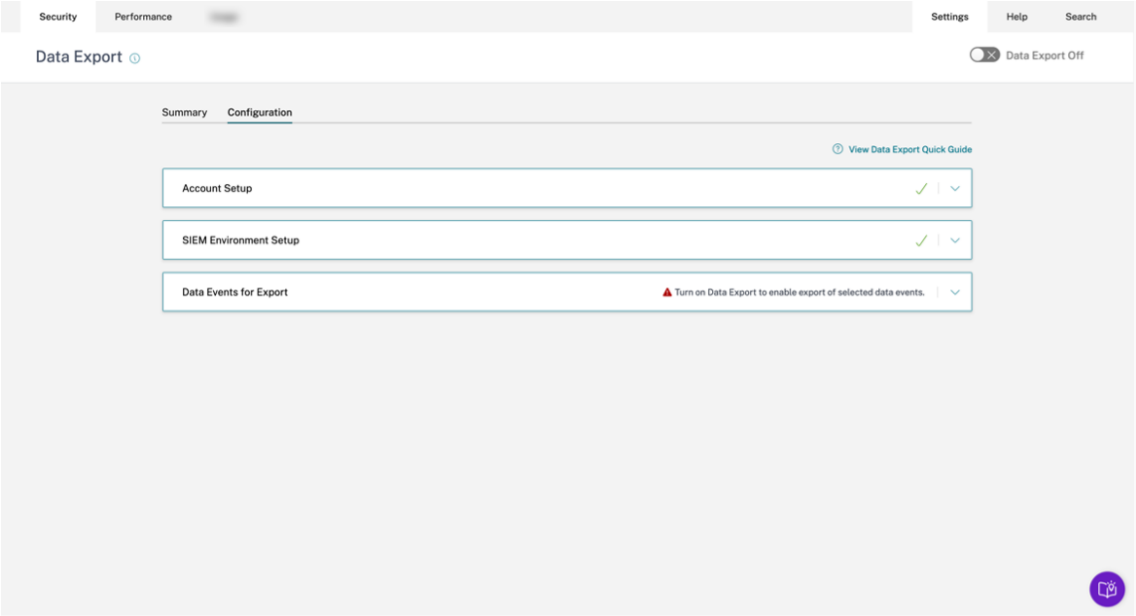



- Como se muestra en la siguiente imagen, las etapas Configuración del entorno SIEM y Eventos de datos para exportación están inhabilitadas hasta que la configuración de la cuenta se complete correctamente.

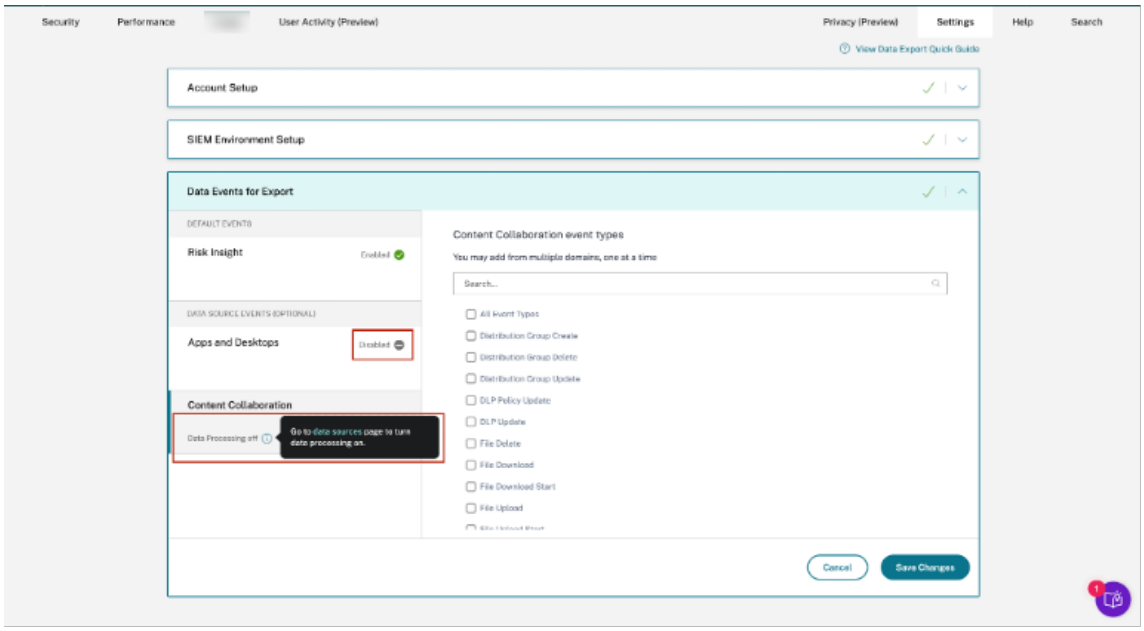



- Se han desactivado las exportaciones de datos. La advertencia en la fase de eventos de datos para la exportación sirve como recordatorio para permitir que la exportación de datos efectúe cualquier cambio.




- En la etapa Eventos de datos para la exportación, si la exportación de datos para una fuente de datos en particular está inhabilitada, ningún evento de fuente de datos fluirá al SIEM. Debe habilitarlo configurando y seleccionando los tipos de eventos de la fuente de datos que desee. Además, asegúrese de que el procesamiento de datos de la fuente de datos correspondiente esté habilitado para garantizar que los datos lleguen a Citrix Analytics.



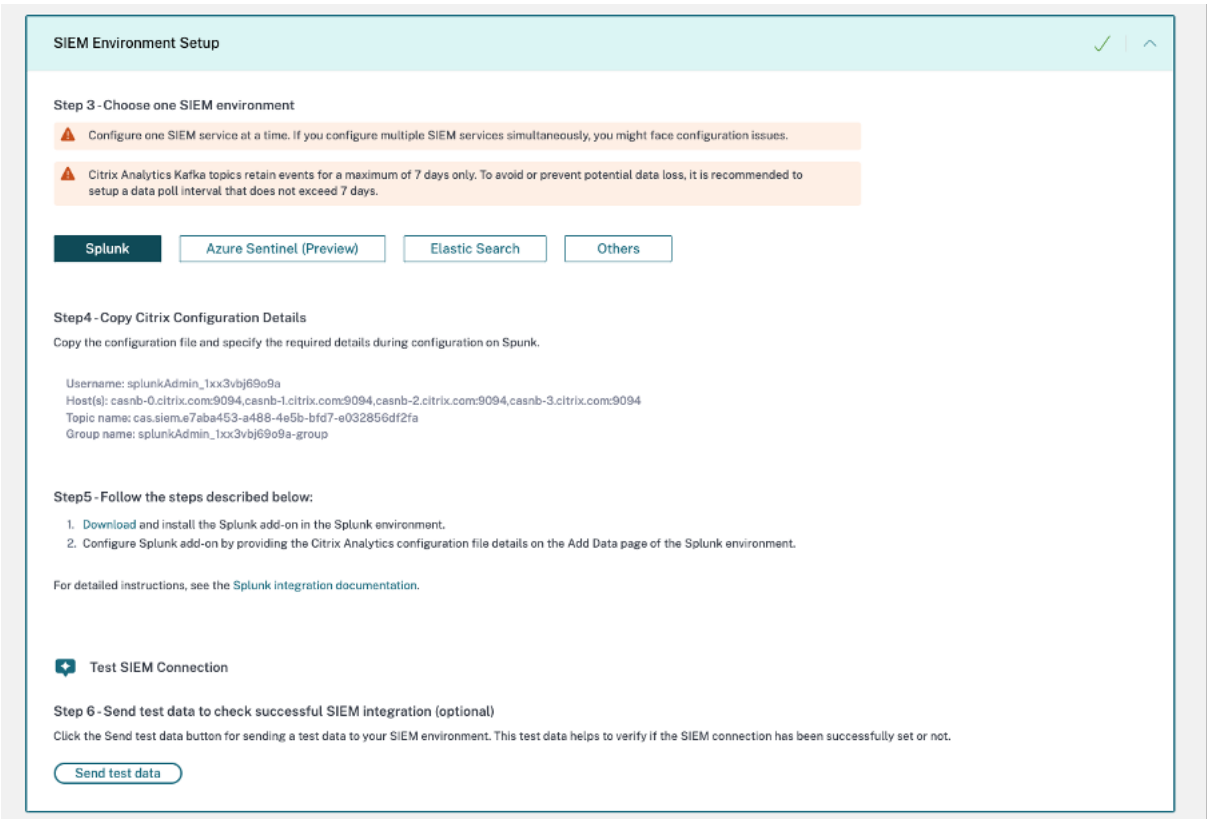

## Generación de eventos de prueba

La generación de eventos de prueba se proporciona como parte de la etapa de **configuración del entorno SIEM** para mejorar la experiencia de solución de problemas. Una vez que el usuario completa la

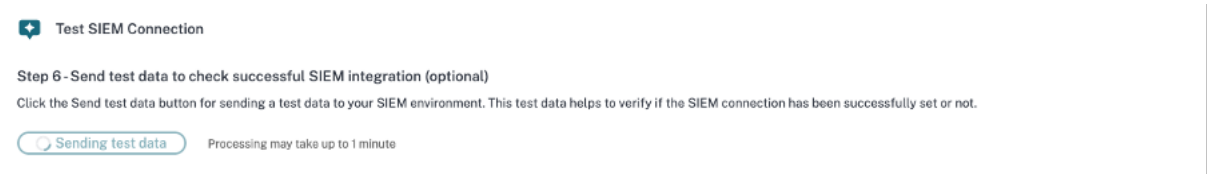
 

configuración del SIEM, la generación de eventos de prueba proporciona una forma de probar rápidamente la conexión SIEM enviando un evento de prueba directamente al tema de Kafka de exportación de datos de SIEM del cliente.

También permite a los nuevos usuarios probar rápidamente su integración de SIEM con Citrix Analytics sin tener que incorporar explícitamente una nueva fuente de datos y, posteriormente, generar la actividad de los usuarios.

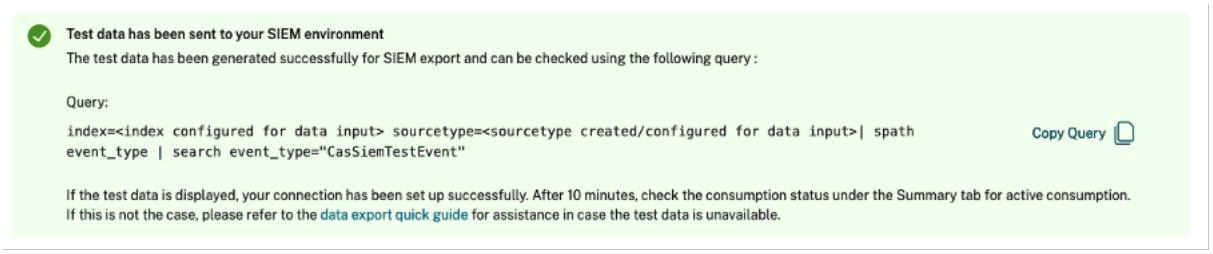


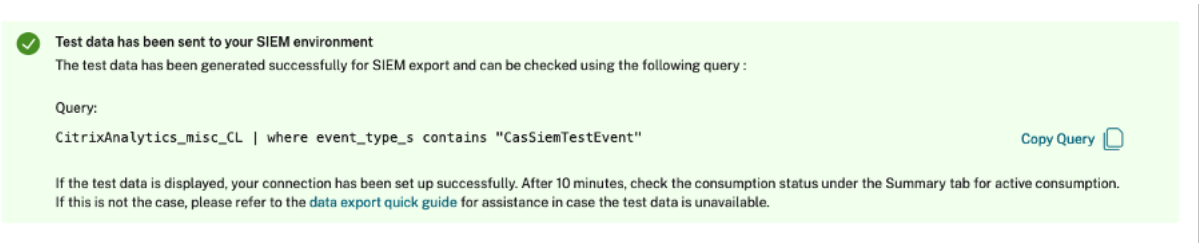

Para probar esta funcionalidad, el usuario debe hacer clic en el botón **Enviar datos de prueba**. Esto genera un evento de prueba ficticio y lo envía al tema Kafka de exportación de datos de SIEM del cliente. Este proceso de generación de eventos de prueba puede tardar hasta 1 minuto, como se muestra en la siguiente captura de pantalla:



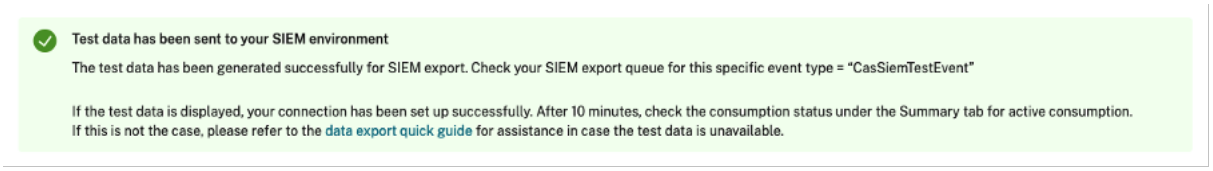

Si los datos del evento de prueba se han escrito correctamente en el tema Kafka del cliente, aparecerá un mensaje de confirmación que indica que la conexión SIEM se ha realizado correctamente. Según el entorno elegido (Splunk y Sentinel), los administradores pueden copiar la consulta y comprobar sus entornos SIEM para el evento de prueba.

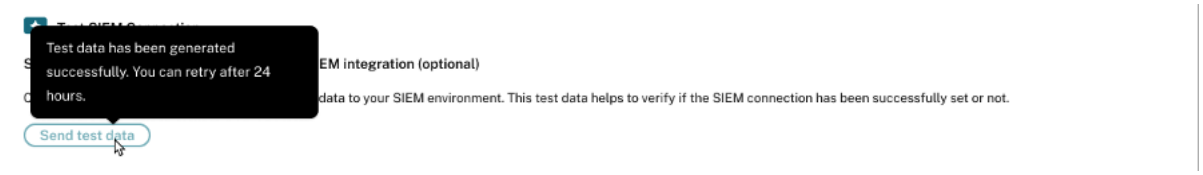


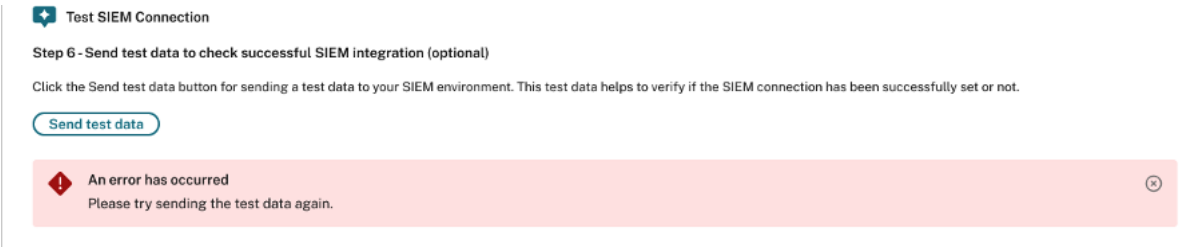

Para Elasticsearch y otros entornos, se muestra el siguiente mensaje de éxito.




> **Nota**
>
> Una vez que se genera un evento de **prueba, el botón Enviar datos** de prueba se desactiva durante las próximas 24 horas y los usuarios ven la siguiente ventana emergente al pasar el ratón sobre el botón. Transcurridas 24 horas desde la última fecha de éxito, se habilita el botón para que los usuarios vuelvan a probar la funcionalidad.




Si los datos del evento de prueba no se han escrito correctamente en el tema Kafka del cliente, aparecerá un mensaje de error como se muestra en la siguiente captura de pantalla. El usuario puede volver a enviar los datos para probar la conexión.



## Alerta de correo electrónico de SIEM

Citrix Analytics envía alertas por correo electrónico para informar a los administradores sobre situaciones que podrían provocar la interrupción del flujo de datos a su entorno SIEM. Contiene información situacional sobre las actividades que podrían provocar una pérdida de datos temporal o permanente por motivos de seguridad. También ayuda a abordar el proceso de solución de problemas de autoservicio para la exportación de datos de SIEM.

Algunas propiedades importantes de este conjunto de alertas por correo electrónico te ayudarán a localizarlas en tu bandeja de entrada:

- El correo electrónico se distribuye entre los administradores de Citrix Cloud, los administradores de seguridad de solo lectura, los administradores de seguridad de solo lectura y los administradores de seguridad y rendimiento de solo lectura.
- El remitente es Citrix Cloud **donotreplynotifications@citrix.com**.
- La línea de asunto es:
  - **Alerta de exportación de datos de SIEM: se restableció la contraseña** para las alertas de correo electrónico de restablecimiento de contraseña.
  - **Alerta de exportación de datos de SIEM: el flujo de datos se detuvo** por alertas por correo electrónico de interrupción del flujo de datos.

### ¿Cómo habilitar las notificaciones por correo electrónico?

Si es administrador de Citrix Cloud con permisos de acceso personalizados (administrador completo de seguridad, administrador de solo lectura de seguridad, seguridad y solo lectura de rendimiento) para administrar los análisis de seguridad, las notificaciones por correo electrónico siempre están habilitadas en su cuenta de Citrix Cloud. De forma predeterminada, las notificaciones semanales por correo electrónico se envían a la lista predeterminada de administradores de seguridad de Citrix. También puede modificar la lista de distribución que recibe esta alerta. Para obtener más información, consulta .

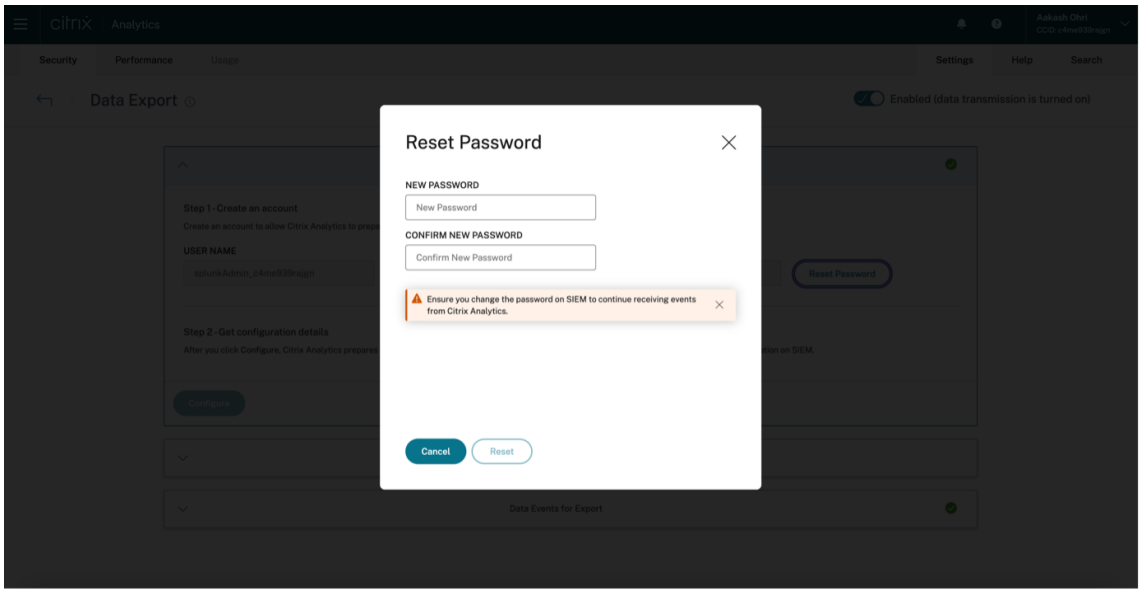
Si es un administrador de Citrix Cloud con permisos de acceso personalizados (administrador total de seguridad, administrador de solo lectura de seguridad, solo lectura de seguridad y rendimiento) para administrar Security Analytics, las notificaciones por correo electrónico siempre están habilitadas para su cuenta de Citrix Cloud.

### Tipos de alertas de correo electrónico de SIEM

1. **Alerta por correo electrónico de restablecimiento de contraseña de SIEM**

El correo electrónico de alerta de restablecimiento de contraseña del SIEM se recibe cuando se restablece la contraseña de la cuenta a través de la página Exportación de datos. Restablecer la contraseña del SIEM solo en la interfaz de usuario de Citrix Analytics puede provocar que la contraseña no coincida con la configurada en el SIEM. Esto lleva a la interrupción del flujo de datos. Esta alerta por correo electrónico contiene la hora a la que se restableció la contraseña. Si el flujo de datos se detiene, puede ir a la ficha **Resumen**, comprobar si la fecha de «última exportación» se encuentra cerca de la fecha de restablecimiento de la contraseña y, por lo tanto, transmitir los cambios de contraseña necesarios. Esto acorta el proceso de depuración y le ayuda a volver al flujo de datos correcto en su entorno SIEM en poco tiempo.



citrix | Analytics for Security

# Password reset was detected

**What you need to know:**
A password reset was detected for the SIEM export account. Please update your SIEM environment with new password to avoid losing critical VDI in-session events and security insights.

Customer name: freshsiem

Organization ID: int40b94891

What happened?

Password reset/change has been detected for the SIEM export account on 04 Apr, 2023 at 04:08 UTC.

What do you need to do?

1. Reach out to your SIEM administrator to update your SIEM environment with the new password.
2. Check the consumption status to ensure that the password reset has not caused any disruptions to active data flow.

Check the Data Flow Status

For more in product guidance on SIEM integration troubleshooting, please leverage Citrix Analytics for Security Data Export Quick Guide workflow.

Regards,
Citrix Analytics for Security team



Privacy | Set Email Preferences

2. **Alerta por correo electrónico de interrupción del flujo de datos durante 24 horas**

   Esta alerta por correo electrónico se envía cuando el flujo de datos del servicio Citrix Analytics al entorno SIEM se interrumpe durante más de 24 horas. El correo electrónico incluye la hora a la que se exportó el último evento, junto con consejos útiles para la solución de problemas que se pueden seguir para restablecer el flujo de datos. Este sería el momento adecuado para restablecer rápidamente el flujo de datos y no perder ningún dato relacionado con la seguridad.

3. **Alerta por correo electrónico de interrupción del flujo de datos durante 7 días**

   Esta alerta por correo electrónico se envía cuando el flujo de datos del servicio Citrix Analytics al entorno SIEM se interrumpe durante más de 7 días. Dado que el período de retención del tema Kafka del cliente es de 7 días, es fundamental seguir los consejos de solución de problemas y utilizar la guía rápida disponible en la página de **exportación de datos** para no perder más datos, ya que este correo electrónico advierte de una situación de pérdida permanente de información basada en la seguridad.

4. **Alerta por correo electrónico de interrupción del flujo de datos durante 30 días**

   Esta alerta por correo electrónico se envía cuando el flujo de datos del servicio Citrix Analytics al entorno SIEM se interrumpe durante más de 30 días. A estas alturas, el cliente ha perdido datos relacionados con la postura de seguridad y es imperativo utilizar las funciones de solución de problemas para restablecer el flujo lo antes posible.

citrix | Analytics for Security

# Data Flow Stopped 24 hours ago

**Impact:**
We have detected that data flow has stopped from Citrix Analytics service into your SIEM environment in the last 24 hours. Further disruption will lead to **loss of critical VDI in-session events and security insights.**

Customer name: CAS-SIEM-TEST

Organization ID: int511e492f

What happened?

In the last 24 hours, no Risk insight or Data source events have been exported to your SIEM. Last event export reported at: 04 Apr, 2023 at 04:20 UTC.

What do you need to do?

- Check SIEM environment for any firewall issues
- Check for credential mismatch issues between Kafka account setup and your SIEM environment
- Ensure you have turned on data processing for requisite data sources
- Ensure you have adequate user activity for your Citrix deployment

Troubleshoot Data Flow Issues

For more in product guidance on SIEM integration troubleshooting, please leverage Citrix Analytics for Security Data Export Quick Guide workflow.

Regards,
Citrix Analytics for Security team



Privacy | Set Email Preferences

citrix | Analytics for Security

## Data Flow Stopped 7 days ago

**Impact:**
We have detected that data flow has stopped from Citrix Analytics service into your SIEM environment in past 7 days. Further disruption will lead to **loss of critical VDI in-session events and security insights.**

Customer name: CAS-SIEM-TEST

Organization ID: int511e492f

What happened?

In the last 7 days, no Risk insight or Data source events have been exported to your SIEM. Last event export reported at: 29 Mar, 2023 at 04:20 UTC.

What do you need to do?

- Check SIEM environment for any firewall issues
- Check for credential mismatch issues between Kafka account setup and your SIEM environment
- Ensure you have turned on data processing for requisite data sources
- Ensure you have adequate user activity for your Citrix deployment

Troubleshoot Data Flow Issues

For more in product guidance on SIEM integration troubleshooting, please leverage Citrix Analytics for Security Data Export Quick Guide workflow.

How can you benefit from the SIEM integration?

You can enhance the value of your SIEM by integrating it with Citrix Analytics for Security. This integration enables you to correlate your users' data with the data available in your SIEM environment along with deeper insights into your organization's security posture.

Explore SIEM integration

Regards,
Citrix Analytics for Security team



Privacy | Set Email Preferences

citrix | Analytics for Security

## Data Flow Stopped 30 days ago

**Impact:**
We have detected that data flow has stopped from Citrix Analytics service into your SIEM environment in past 30 days. Further disruption will lead to **loss of critical VDI in-session events and security insights.**

Customer name: CAS-SIEM-TEST

Organization ID: int511e492f

What happened?

In the last 30 days, no Risk insight or Data source events have been exported to your SIEM. Last event export reported at: 06 Mar, 2023 at 04:20 UTC.

What do you need to do?

- Check SIEM environment for any firewall issues
- Check for credential mismatch issues between Kafka account setup and your SIEM environment
- Ensure you have turned on data processing for requisite data sources
- Ensure you have adequate user activity for your Citrix deployment

Troubleshoot Data Flow Issues

For more in product guidance on SIEM integration troubleshooting, please leverage Citrix Analytics for Security Data Export Quick Guide workflow.

How can you benefit from the SIEM integration?

You can enhance the value of your SIEM by integrating it with Citrix Analytics for Security. This integration enables you to correlate your users' data with the data available in your SIEM environment along with deeper insights into your organization's security posture.

Explore SIEM integration

Regards,
Citrix Analytics for Security team

**We want to hear your thoughts about your SIEM integration**
Share your feedback about your SIEM integration to help us improve at CAS-PM-Ext@citrix.com or if you need any assistance.



Privacy | Set Email Preferences

# Ejemplos de firmas Sigma para obtener información sobre seguridad

December 7, 2023

Esta página contiene ejemplos de consultas para ayudar a los administradores a lograr resultados significativos con Citrix Security Analytics.

Estos ejemplos cubren los riesgos de las siguientes categorías:

- Endpoints comprometidos
- Amenazas internas
- Exfiltración de datos

## Cómo utilizar estos ejemplos

### Ver la fuente de datos y activar el procesamiento de datos

Para ver la fuente de datos, haga clic en **Configuración > Fuentes de datos > Seguridad** en la GUI de Citrix Analytics. La tarjeta del sitio **Aplicaciones y escritorios: Aplicación Workspace** aparece en la página **Orígenes de datos**. Haga clic **en Activar procesamiento de datos** para permitir que Citrix Analytics comience a procesar los datos de esta fuente de datos.

Citrix Analytics for Security envía los dos tipos siguientes de datos de información sobre riesgos a su servicio SIEM:

- Eventos de información sobre riesgos (exportaciones predeterminadas)
- Eventos de fuentes de datos (exportaciones opcionales)

Como parte de su entorno SIEM, las fuentes de datos de eventos de Risk Insight están disponibles y siempre están activadas de forma predeterminada. Para obtener más información, consulte Eventos de datos exportados de Citrix Analytics for Security a su servicio SIEM.

Puede usar firmas CAS o Sigma para verificar cualquier evento de usuario en particular en sus fuentes de datos. Se puede acceder a las consultas de CAS a través de la página de búsqueda de autoservicio de la GUI de Citrix Analytics. Las firmas Sigma están escritas en un formato simple o fácil de usar, lo que las hace compatibles con varios entornos SIEM.

### Uso de consultas CAS

Puede usar la consulta CAS de la página de **búsqueda de autoservicio** para buscar y filtrar los eventos de usuario recibidos de varias fuentes de datos. Haga clic en **Buscar** desde la GUI de Citrix Analytics

e introduzca la consulta en el cuadro de búsqueda. Para obtener más información, consulta Cómo utilizar la búsqueda de autoservicio.

También puede crear indicadores de riesgo personalizados con las plantillas existentes. Para crear un indicador de riesgo personalizado, vaya a **Seguridad > Indicadores de riesgo personalizados > Crear indicador**. Para obtener más información, consulte Creación de un indicador de riesgo personalizado.

### Uso de firmas Sigma

Sigma es un formato de firma abierto y fácil de usar para crear consultas basadas en texto que los analistas pueden usar para describir eventos de registro, lo que facilita la escritura de las detecciones. Hay varias formas de convertir una firma Sigma al lenguaje de consulta de la herramienta SIEM.

- Puede utilizar las herramientas de CLI y los SDK de Python que ofrece Sigma. Para obtener más información sobre la firma Sigma, consulte Uso de reglas.
- Puedes usar herramientas públicas como el motor de traducción Sigma de uncoder.io, que ofrece un nivel gratuito.

Consulte los siguientes casos de uso de indicadores personalizados para obtener información sobre los diferentes riesgos:

- Navegador no autorizado
- Sistema operativo no autorizado
- Versiones no autorizadas de la aplicación Workspace
- Sistemas operativos no autorizados fuera de la lista de permitidos
- Dirección IP o subredes no autorizadas
- Aplicaciones virtuales no autorizadas
- Nombres de escritorio inusuales
- Supervise una aplicación específica
- Impresión desde aplicaciones SaaS
- Uso del portapapeles en aplicaciones SaaS

## Endpoints comprometidos

November 17, 2023

### Navegador no autorizado

Esto ocurre cuando un usuario intenta acceder al contenido desde un tipo o versión de navegador que no está permitido por la directiva de TI de la organización o debido a vulnerabilidades de seguridad.

#### Detalles

**Fuente de datos**: aplicaciones y escritorios (aplicación Workspace)

#### Consulta CAS

```
Event-Type = "Session.Logon" AND Browser-Name !~ "<Browser-Name>"
```

El evento Session.Logon se desencadena cuando un usuario introduce sus credenciales e inicia sesión en su aplicación o escritorio.

#### Firma Sigma

```
author: Citrix
date: 2023/01/31
description: This occurs when a user accesses content from an
    authorized browser which might cause an undesirable event or action
    through the internet.
detection:
  condition: index_selection and selection and not filter
  filter:
  - browser_name|contains: '<Browser-Name>'
  index_selection:
    source: cas_siem_consumer://<env>_<tenant_identifier>
  selection:
  - occurrence_event_type: Session.logon
logsource:
  product: citrixanalytics
  service: security
title: Access from unauthorized browser
```

### Sistemas operativos no autorizados

Esto ocurre cuando un usuario intenta acceder a un dispositivo con un tipo o versión de sistema operativo que no está permitido por la directiva de TI de la organización o debido a vulnerabilidades de seguridad.

#### Detalles

**Fuente de datos**: aplicaciones y escritorios (aplicación Workspace)

#### Consulta CAS

```
Event-Type = "Session.Logon" AND OS-Name ~ "<OS-Name>" AND OS-Version =
    "<OS-Version>" AND OS-Extra-Info = "<OS-Extra-Info>"
```

#### Firma Sigma

```
author: Citrix
date: 2023/01/31
description: This occurs when a user attempts to access apps from
   servers with blocked listed operating systems.
detection:
  condition: index_selection and selection
  filter_null: []
  index_selection:
    source: cas_siem_consumer://<env>_<tenant_identifier>
  selection:
    occurrence_event_type: Session.logon
    os_name|contains: '<OS-Name>'
    os_version: '<OS-Version>'
    os_extra_info: '<OS-Extra-Info>'
logsource:
  product: citrixanalytics
  service: security
title: Unauthorized operating systems in block list
```

### Dirección IP o subredes no autorizadas

Esto ocurre cuando un usuario intenta acceder desde una dirección IP o un rango que la directiva de TI de su organización marca como no autorizados.

#### Detalles

**Fuente de datos**: aplicaciones y escritorios (aplicación Workspace)

#### Consulta CAS

```
Event-Type = "Session.Logon" AND Client-IP = "<XX.YY.ZZ.*>"
```

#### Firma Sigma

```
author: Citrix
date: 2023/01/31
description: This occurs when a user accessing content from an
    unauthorized IPs which might cause an undesirable event or action
    through the internet.
detection:
  condition: selection and not filter_null and filter
  filter:
  - client_ip: '<IP>'
  filter_null:
  - client_ip: null
  selection:
  - occurrence_event_type: Session.Logon
logsource:
  product: citrixanalytics
  service: security
title: Access from unauthorized IP
```

### Sistemas operativos no autorizados fuera de la lista de permitidos

Esto ocurre cuando un usuario intenta acceder a las aplicaciones desde servidores que alojan sistemas operativos fuera de la lista de permitidos.

#### Detalles

**Fuente de datos**: aplicaciones y escritorios (aplicación Workspace)

#### Consulta CAS

```
Event-Type = "Session.Logon" AND OS-Name !~ "<OS-Name>" AND OS-Version
    != "<OS-Version>" AND OS-Extra-Info != "<OS-Extra-Info>"
```

#### Firma Sigma

```
author: Citrix
date: 2023/01/31
description: Unauthorized operating systems outside allow list
detection:
  condition: selection and not filter_null and not filter_os and not
      filter_os_version and not filter_os_extra
  filter_os:
  - os_name|contains: '<OS INFO>'
  filter_os_version:
```

```
9     - os_version: '<OS Version>'
10    filter_os_extra:
11    - os_extra_info: '<OS Extra Info>'
12    filter_null:
13    - os_name: null
14    - os_version: null
15    - os_extra_info: null
16    selection:
17    - occurrence_event_type: Session.Logon
18  logsource:
19    product: citrixanalytics
20    service: security
21  title: Unauthorized operating systems outside allow list
```

### Versiones no autorizadas de la aplicación Workspace

Esto ocurre cuando un usuario intenta acceder a una versión de la aplicación Workspace que no es una versión de cliente compatible. En esos casos, los usuarios deben actualizar su cliente a una versión compatible. Para obtener más información, consulte Compatibilidad con las versiones de los clientes.

#### Detalles

**Fuente de datos**: aplicaciones y escritorios (aplicación Workspace)

#### Consulta CAS

```
1  Event-Type = "Session.Logon" AND Client-Type IN ("Windows", "Macintosh"
       , "Unix/Linux") AND Workspace-App-Version != "20*" AND Workspace-App
       -Version != "21*"
```

#### Firma Sigma

```
1  author: Citrix
2  date: 2023/01/31
3  description: Unsupported Workspace app versions
4  detection:
5    condition: selection and not filter_null and filter_product and not
         filter_product_version
6    filter_product:
7    - product: ['Windows', 'Mac', '<Other type>']
8    filter_product_version:
9    - product_version|contains: ['<Product Version1>', '<Product Version2
         >']
```

```
10    filter_null:
11    - product: null
12    - product_version: null
13    selection:
14    - occurrence_event_type: Session.Logon
15  logsource:
16    product: citrixanalytics
17    service: security
18  title: Unsupported Workspace app versions
```

## Amenazas internas

November 17, 2023

### Nombres de escritorio inusuales

Esto ocurre cuando el usuario intenta iniciar un escritorio que no se considera habitual.

#### Detalles

**Fuente de datos**: aplicaciones y escritorios (aplicación Workspace)

#### Consulta CAS

```
1  Event-Type = "Session.Logon" AND Session-Launch-Type = "desktop" AND
       App-Name ~ "<Desktop Name>"
```

#### Firma Sigma

```
1  author: Citrix
2  date: 2023/01/31
3  description: Unusual desktop names
4  detection:
5    condition: selection1 and selection2 and not filter_null and
         filter_app_name
6    filter_app_name:
7    - app_name|contains: '<App Name>'
8    filter_null:
9    - app_name: null
10   selection1:
11   - occurrence_event_type: Citrix.EventMonitor.AppStart
```

```
12    selection2:
13    - launch_type: 'desktop'
14  logsource:
15    product: citrixanalytics
16    service: security
17  title: Unusual desktop names
```

### Supervise un proceso específico

Esto ocurre cuando el usuario inicia una aplicación publicada que está en la lista de observación. El propósito podría ser monitorear el uso de aplicaciones publicadas específicas.

#### Detalles

**Fuente de datos**: aplicaciones y escritorios (grabación de sesiones)

#### Consulta CAS

```
1  Event-Type = "Citrix.EventMonitor.AppStart" AND App-Name IN ("<App-Name
      -1>", "<App-Name-2>")
```

#### Firma Sigma

```
1  author: Citrix
2  date: 2023/01/31
3  description: Monitor specific process
4  detection:
5    condition: selection and not filter_null and filter_app_name
6    filter_app_name:
7    - app_name: ['<App-Name1>', '<App-Name2>']
8    filter_null:
9    - app_name: null
10   selection:
11   - occurrence_event_type: Citrix.EventMonitor.AppStart
12 logsource:
13   product: citrixanalytics
14   service: security
15 title: Monitor specific process
```

### Aplicaciones virtuales no autorizadas

Esto ocurre cuando el usuario accede a aplicaciones virtuales no autorizadas.

#### Detalles

**Fuente de datos**: aplicaciones y escritorios (aplicación Workspace)

#### Consulta CAS

```
Event-Type = "App.Start" AND App-Name IN ("<App-Name1>", "<App-Name2>")
```

#### Firma Sigma

```
date: 2023/01/31
description: Unauthorized virtual apps
detection:
  condition: selection and not filter_null and filter_app_name
  filter_app_name:
  - app_name: ['<App-Name1>', '<App-Name2>']
  filter_null:
  - app_name: null
  selection:
  - occurrence_event_type: App.Start
logsource:
  product: citrixanalytics
  service: security
title: Unauthorized virtual apps
```

## Exfiltración de datos

November 17, 2023

### Impresión desde aplicaciones SaaS

Esto ocurre cuando se imprime un archivo desde una aplicación SaaS desde la que no se permite la impresión. Detecta la posible exfiltración de datos mediante operaciones de impresión en aplicaciones SaaS.

#### Detalles

**Fuente de datos**: aplicaciones y escritorios (Citrix Enterprise Browser)

#### Consulta CAS

```
Event-Type = "App.SaaS.File.Print" AND SaaS-App-Name = "<App-Name>"
```

#### Firma Sigma

```
author: Citrix
date: 2023/01/31
description: Printing from SaaS apps
detection:
  condition: selection and not filter_null and filter_saas_app_name
  filter_saas_app_name:
  - saas_app_name: '<App-Name>'
  filter_null:
  - saas_app_name: null
  selection:
  - occurrence_event_type: App.SaaS.File.Print
logsource:
  product: citrixanalytics
  service: security
title: Printing from SaaS apps
```

### Uso del portapapeles en aplicaciones SaaS

Esto ocurre cuando se realiza una actividad de cortar, copiar o pegar desde cualquier aplicación SaaS. Detecta la posible exfiltración de datos de las aplicaciones SaaS de su organización mediante la supervisión de las operaciones del portapapeles.

#### Detalles

**Fuente de datos**: aplicaciones y escritorios (Citrix Enterprise Browser)

#### Consulta CAS

```
Event-Type = "App.SaaS.Clipboard" AND Clipboard-Result = "success" AND
    Clipboard-Operation IN ( "copy" , "cut" )
```

#### Firma Sigma

```
author: Citrix
date: 2023/01/31
description: Clipboard usage on SaaS apps
```

```
4  detection:
5    condition: selection and not filter_null and
        filter_clipboard_details_result and filter_clipboard_operation
6    filter_clipboard_details_result:
7    - clipboard_details_result: 'success'
8    filter_clipboard_operation:
9    - clipboard_operation: ['cut', 'copy', '<Other Operation>']
10   filter_null:
11   - clipboard_operation: null
12   - clipboard_details_result: null
13   selection:
14   - occurrence_event_type: App.SaaS.Clipboard
15 logsource:
16   product: citrixanalytics
17   service: security
18 title: Clipboard usage on SaaS apps
```

## Panel de usuarios

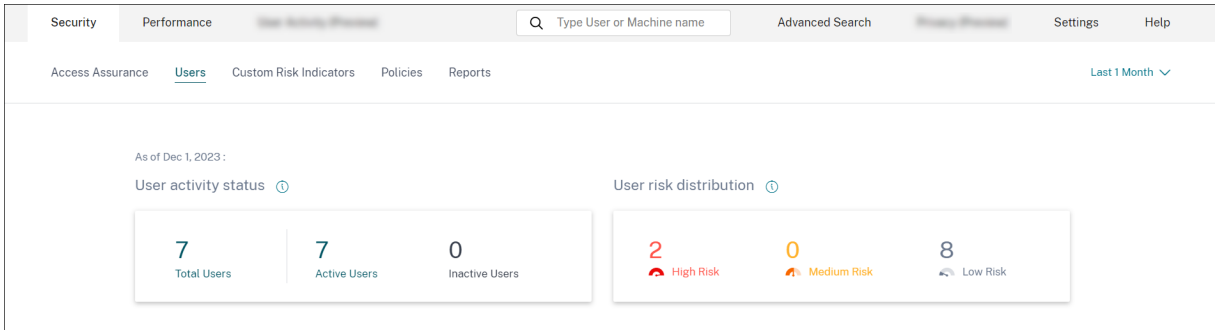
February 12, 2024

### Descripción general

El panel de **usuarios** es el punto de partida para el análisis del comportamiento de los usuarios y la prevención de amenazas.

Este panel proporciona visibilidad de los patrones de comportamiento de los usuarios en toda la organización. Con estos datos, puede supervisar, detectar y marcar de forma proactiva los comportamientos que no cumplen los estándares, como los ataques de phishing o ransomware.

Para ver el panel de usuarios, vaya a **Seguridad > Usuarios**. El panel Usuarios contiene las siguientes secciones:




- **Estado activo del usuario**: distribución del total de usuarios activos e inactivos.

- **Distribución del riesgo de los usuarios**: distribución de los usuarios activos, inactivos y totales, y distribución de los usuarios de riesgo en perfiles altos, medios y bajos en función de su puntuación de riesgo calculada más alta en el período de tiempo seleccionado.
- **Usuarios principales: los usuarios**principales se ordenan por su puntuación de riesgo y se segmentan por todos los usuarios, usuarios privilegiados y usuarios de la lista de seguimiento.
- **Categorías de riesgo**: muestra las categorías de riesgo compatibles con Citrix Analytics. Los indicadores de riesgo con patrones de comportamiento similares se agrupan en categorías.
- **Indicadores de riesgo y acciones**: distribución de los indicadores de riesgo y las acciones trazados durante un período seleccionado entre todos los usuarios de su organización.
- **Resumen de acceso**: resume el número total de intentos que los usuarios han realizado para acceder a los recursos de la organización.
- **Directivas y acciones**: muestra las cinco directivas y acciones principales aplicadas a los perfiles de usuario.
- **Indicadores de riesgo**: muestra los cinco indicadores de riesgo principales de su organización.

#### Estado de la actividad del usuario

Número total de usuarios de su organización que utilizan los orígenes de datos para las que ha habilitado Analytics. Es posible que tengan o no una puntuación de riesgo asociada a su cuenta. Este mosaico muestra el número de usuarios activos. Los usuarios activos son los usuarios con eventos detectados dentro del período de tiempo seleccionado. Puede hacer clic en el menú desplegable del estado de la actividad del usuario para ver la distribución del total de usuarios en usuarios activos e inactivos.

- Total de usuarios: número total de usuarios en el período de tiempo seleccionado.
- Usuarios activos: usuarios con eventos detectados en el período de tiempo seleccionado.
- Usuarios inactivos: usuarios sin eventos detectados en el período de tiempo seleccionado.

La cantidad total de usuarios en el panel de **usuarios** puede ser mayor que la cantidad de usuarios riesgosos, ya que no se espera que todos los usuarios sean riesgosos.

> **Nota:**
>
> En la página **Usuarios**, se muestra el número total de usuarios de los últimos 30 días, independientemente del período de tiempo seleccionado.

#### Facetas

Filtra los eventos de usuario según las siguientes categorías:

- **Puntuación de riesgo**: eventos de usuario basados en puntuaciones de riesgo alto, riesgo medio, riesgo bajo y riesgo cero.
- **Usuario**: eventos de usuario basados en privilegios de administrador, privilegios ejecutivos y usuarios de listas de seguimiento.
- **Orígenes de datos descubiertos**: eventos de usuario basados en la fuente de datos incorporada.

#### Cuadro de búsqueda

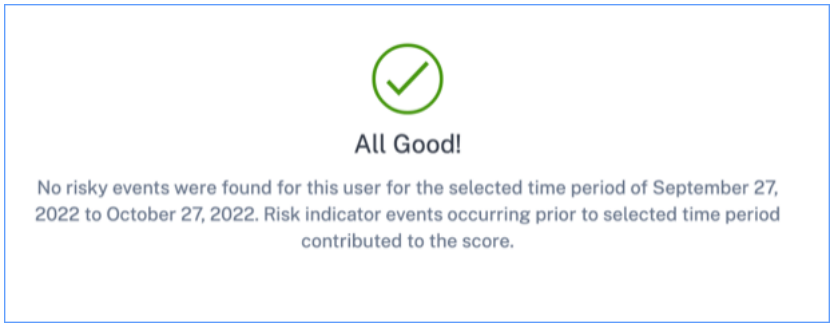
Utilice el cuadro de búsqueda para buscar eventos para los usuarios. Puede utilizar operadores en la consulta para reducir el enfoque de la búsqueda. Para obtener información sobre los operadores válidos que puede utilizar en la consulta, consulte Búsqueda de autoservicio.

#### Puntuación más reciente

La puntuación de riesgo determina el nivel de riesgo que un usuario supone para una organización durante un período de tiempo específico. El valor de la puntuación de riesgo es dinámico y varía según el análisis del comportamiento de los usuarios. Según la puntuación de riesgo más reciente, un usuario puede pertenecer a una de las siguientes categorías: usuario de alto riesgo, usuario de riesgo medio, usuario de bajo riesgo y usuario con puntuación de riesgo cero.

#### Usuario

Lista de todos los usuarios descubiertos por Analytics. Seleccione un nombre de usuario para ver la información del usuario y el cronograma de riesgos del usuario. El usuario puede o no haber activado ningún indicador de riesgo. Si no hay eventos de riesgo asociados a este usuario, aparece el siguiente mensaje.




Si hay eventos de riesgo asociados con un usuario, verá los indicadores de riesgo en su cronología de riesgo. Seleccione el usuario para ver su cronograma de riesgo.

Se puede marcar a un usuario como `privileged` y agregarlo a la lista de seguimiento.

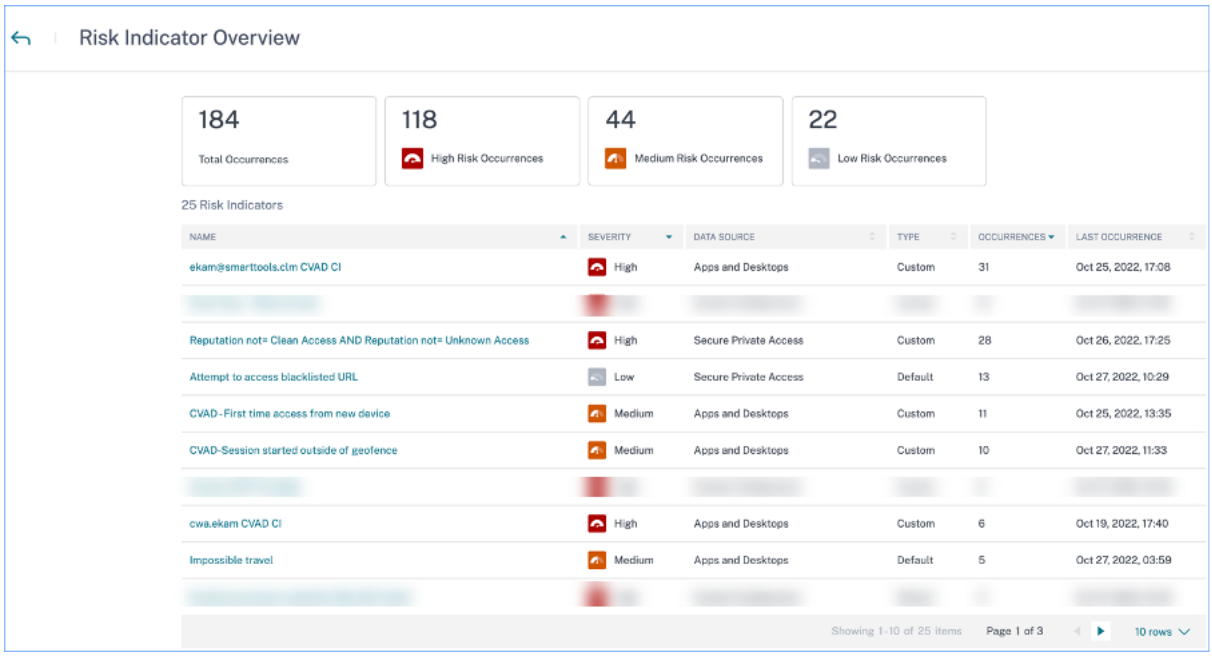
### Fuente de datos descubierta

La fuente de datos asociada a un usuario. Cuando un usuario utiliza activamente la fuente de datos, Analytics recibe los eventos de usuario de esa fuente de datos. Para recibir eventos de usuario, debe activar el procesamiento de datos en la tarjeta del sitio de origen de datos, que está disponible en la página **Orígenes de datos**.

### Indicadores activados

Indica el número de indicadores de riesgo activados en todos los usuarios durante el período seleccionado. Haga clic en el mosaico **Indicadores activados** para ver los detalles de los indicadores de riesgo. La tabla de indicadores de riesgo proporciona los siguientes detalles:

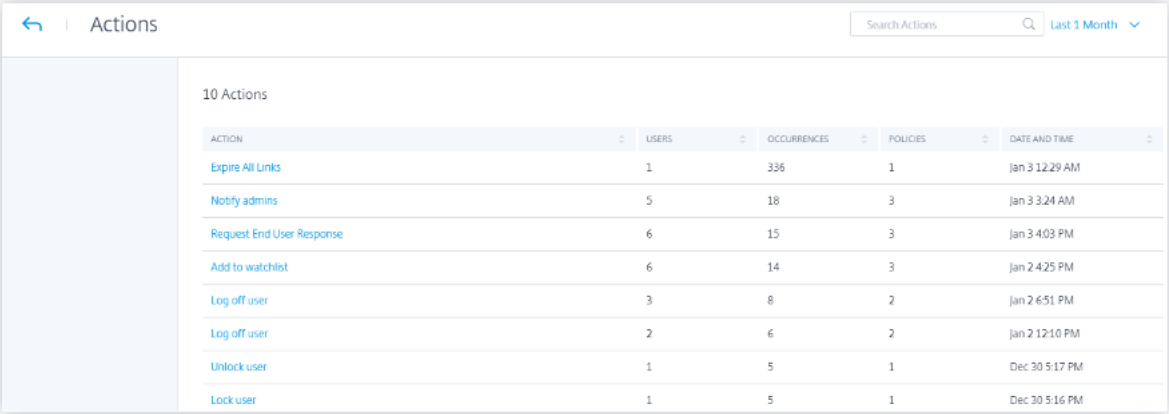
- **Nombre**: el nombre del indicador de riesgo.
- **Gravedad**: la gravedad del riesgo asociado con el evento. El riesgo puede ser alto, medio o bajo.
- **Fuente de datos**: la fuente de datos a la que se aplica la plantilla del indicador de riesgo.
- **Tipo**: Tipo de indicador de riesgo. Un indicador de riesgo puede ser por defecto o personalizado.
- **Ocurrencias**: número de veces que se activa un indicador de riesgo para un usuario. Al seleccionar el período de tiempo, las incidencias del indicador de riesgo cambian en función de la selección de tiempo.
- **Última aparición**: muestra la fecha y hora de la última aparición.



### Acciones aplicadas

Indica el número de acciones aplicadas a los usuarios durante la duración seleccionada. Esto incluye las acciones aplicadas manualmente por los administradores y las acciones basadas en directivas. Haga clic en el icono **Acción aplicada** para ver los detalles de la acción. En esta sección no se muestran las acciones que ha aplicado manualmente en los perfiles de usuario.




| ACTION | USERS | OCCURRENCES | POLICIES | DATE AND TIME |
|---|---|---|---|---|
| Expire All Links | 1 | 336 | 1 | Jan 3 12:29 AM |
| Notify admins | 5 | 18 | 3 | Jan 3 3:24 AM |
| Request End User Response | 6 | 15 | 3 | Jan 3 4:03 PM |
| Add to watchlist | 6 | 14 | 3 | Jan 2 4:25 PM |
| Log off user | 3 | 8 | 2 | Jan 2 6:51 PM |
| Log off user | 2 | 6 | 2 | Jan 2 12:10 PM |
| Unlock user | 1 | 5 | 1 | Dec 30 5:17 PM |
| Lock user | 1 | 5 | 1 | Dec 30 5:16 PM |

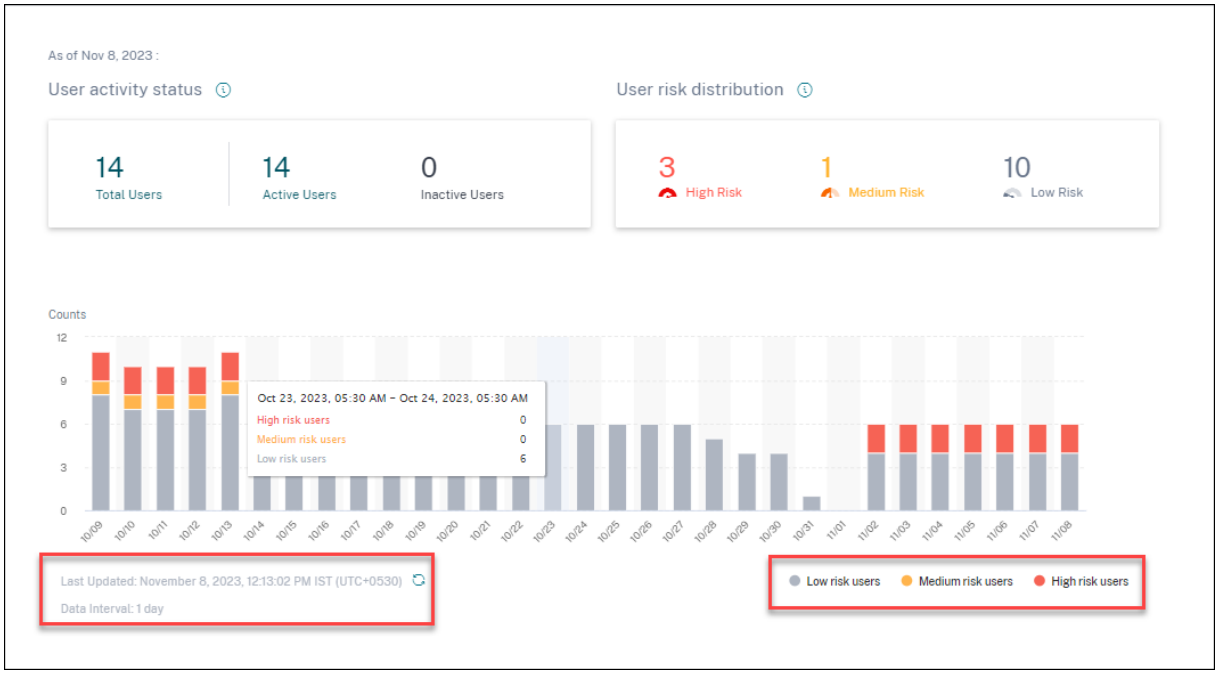
La tabla de **acciones** proporciona la siguiente información:

- **Acción**: nombre de la acción aplicada según la directiva.
- **Usuarios**: número de usuarios a los que se ha aplicado la acción.
- **Apariciones**: número de ocurrencias de la acción.
- **Fecha y hora**: fecha y hora de la acción aplicada.

### Eventos procesados

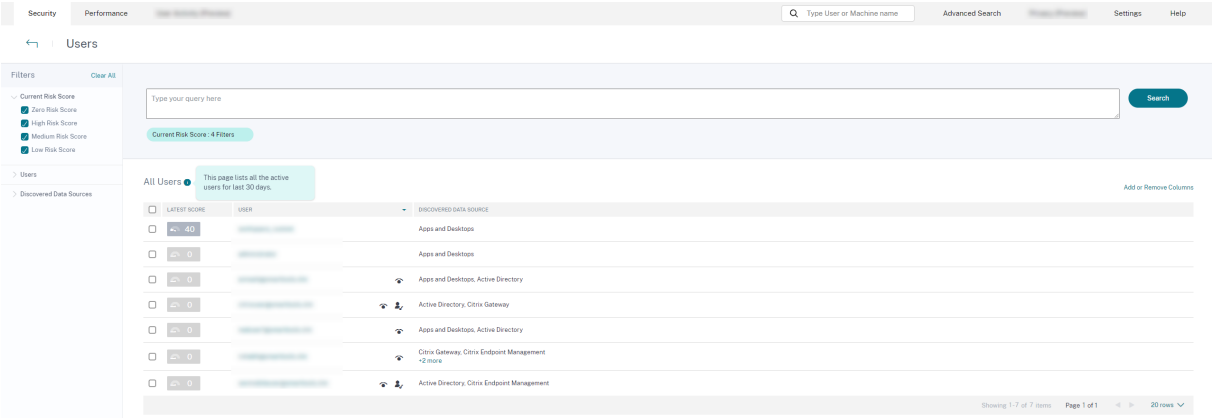
Número total de eventos de usuario recibidos de las fuentes de datos conectadas y procesados por Analytics.




## Distribución de riesgos para los usuarios

Puede ver la cantidad de usuarios con perfiles altos, medios y bajos en función de su puntuación de riesgo calculada más alta en el período de tiempo seleccionado. Debajo de los recuentos generales, un gráfico de barras muestra los cambios a lo largo del tiempo en la distribución de los usuarios de riesgo bajo, medio y alto.




El nivel de riesgo se clasifica en tres códigos de colores.

- **Rojo** : representa a los usuarios de alto riesgo.
- **Naranja** : representa a los usuarios de riesgo medio.
- **Gris** : representa a los usuarios de bajo riesgo.

Puede ver el número de usuarios riesgosos (alto, medio y bajo) mientras coloca el ratón sobre las

barras de colores en función de un período de tiempo específico. Puede ver los detalles de la última actualización (fecha y hora) con la información del intervalo de datos. Haga clic en cualquier barra de colores para ver los usuarios en riesgo durante ese período. Haga clic en la opción de actualización para obtener los datos actualizados.

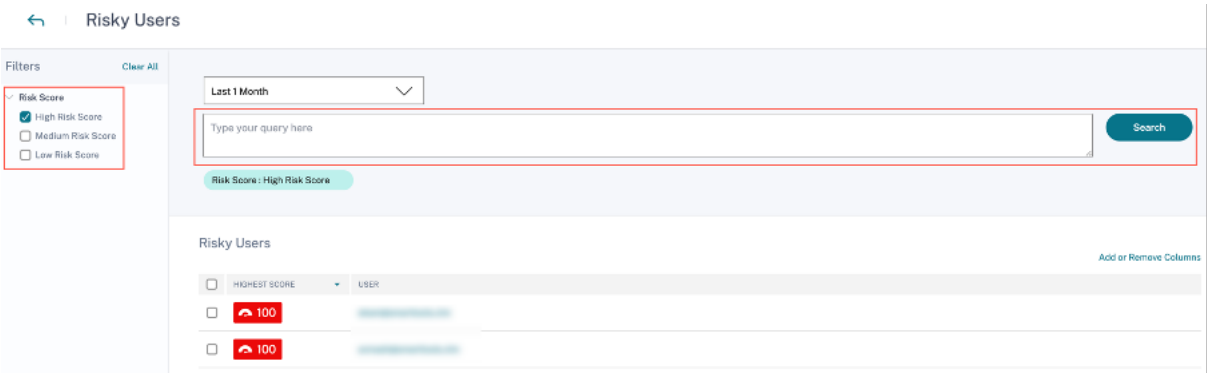
### Usuarios con riesgos

Los usuarios riesgosos son usuarios que tienen eventos de riesgo asociados y han activado al menos un indicador de riesgo. El nivel de riesgo que un usuario plantea a la red durante un período de tiempo específico viene determinado por la puntuación de riesgo asociada al usuario. El valor de la puntuación de riesgo es dinámico y se basa en el análisis del comportamiento de los usuarios.

El riesgo de cada usuario se actualiza periódicamente a lo largo del tiempo en función de la actividad del usuario. Por lo tanto, un usuario puede tener un riesgo medio o alto en un momento dado, pero caer a un nivel de riesgo más bajo más adelante. Según la puntuación de riesgo, un usuario riesgoso puede clasificarse en una de las siguientes categorías:

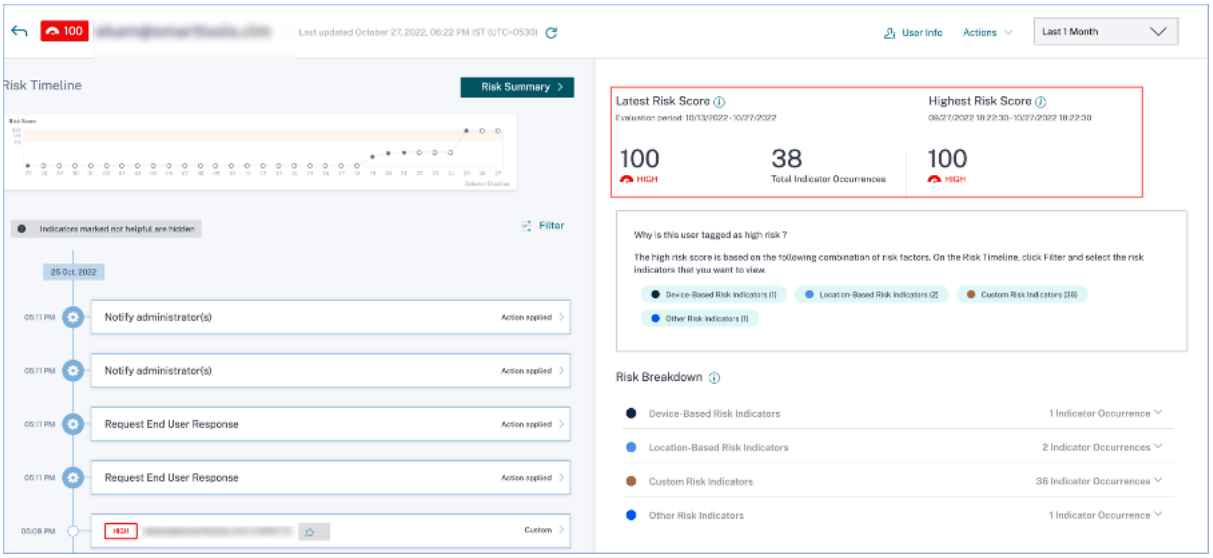
- Riesgo alto
- Riesgo medio
- Riesgo bajo

En la página **Usuarios de riesgo**, puede utilizar las facetas para filtrar en función de los niveles de riesgo asociados al período de tiempo seleccionado y la barra de búsqueda para consultar a un usuario o usuarios específicos.




Haga clic en el ID de correo electrónico del usuario para ver la página de **cronograma de riesgos** de ese usuario seleccionado en particular. Esta página muestra los indicadores de riesgo junto con los detalles de las **puntuaciones de riesgo más**recientes**y más altas** según el período de tiempo seleccionado.




### Riesgo alto

Usuarios con puntuaciones de riesgo entre 90 y 100. Estos usuarios han mostrado múltiples comportamientos consistentes con factores de riesgo de moderados a graves y podrían representar amenazas inmediatas para la organización.

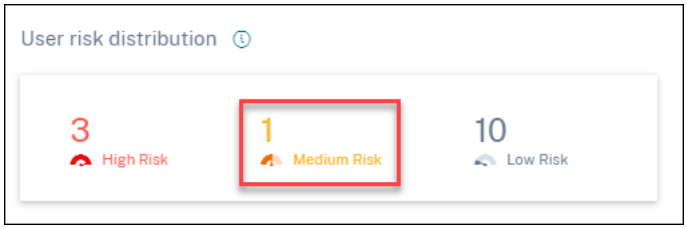
En el panel de **usuarios**, puede ver la cantidad de usuarios de alto riesgo en función de la puntuación de riesgo calculada más alta en el período de tiempo seleccionado.


Haga clic en la opción **Alto riesgo** para ver la página **Usuarios de riesgo**. La página muestra los detalles sobre los usuarios de alto riesgo.

### Riesgo medio

Usuarios con puntuaciones de riesgo entre 70 y 89. Estos usuarios suelen realizar una o más actividades que parecen potencialmente sospechosas o anómalas y que podrían merecer la pena supervisarlas de cerca.

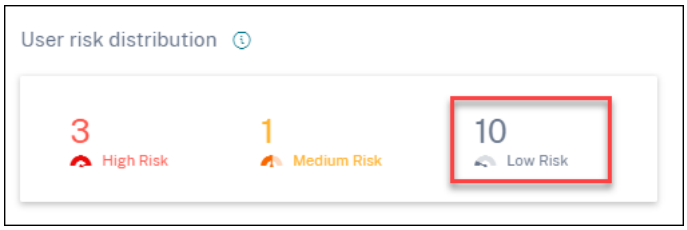
 



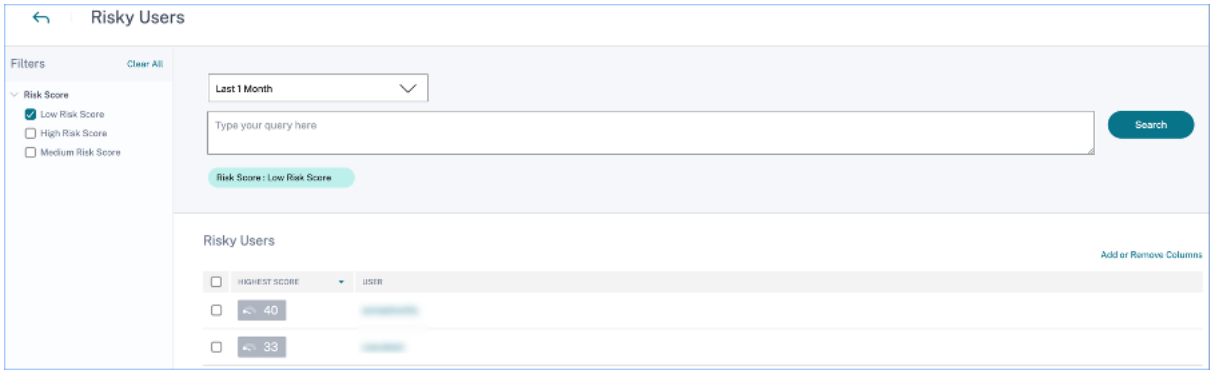

Haga clic en la opción **Riesgo medio** para ver la página **Usuarios de riesgo**. La página muestra los detalles sobre los usuarios de riesgo medio.

### Riesgo bajo

Usuarios con puntuaciones de riesgo entre 1 y 69. Estos usuarios tienen al menos un indicador de riesgo que refleja algún comportamiento inusual o inesperado, pero no lo suficiente como para merecer una clasificación de riesgo más seria.



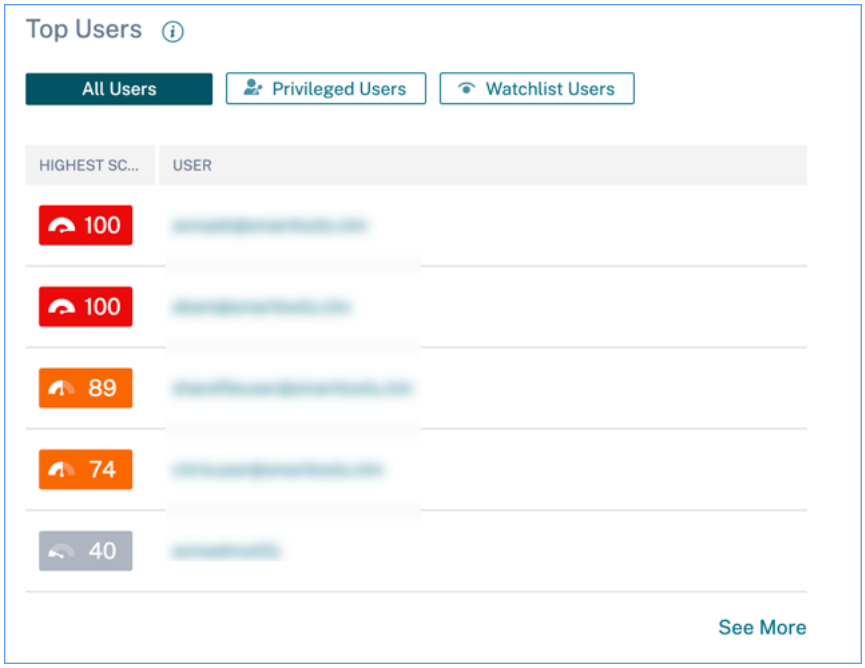

Haga clic en la opción **Bajo riesgo** para ver la página **Usuarios de riesgo**. La página muestra los detalles sobre los usuarios de bajo riesgo.




## Usuarios principales

Puede ver los principales usuarios de varias categorías de usuarios ordenados según las puntuaciones de riesgo más altas para el período de tiempo seleccionado. La siguiente tabla de **usuarios principales** muestra los cinco usuarios con mayor riesgo (todos, usuarios con privilegios y de listas de seguimiento) en función de su puntuación de riesgo calculada durante el período de tiempo seleccionado, en lugar de la puntuación de riesgo más reciente.



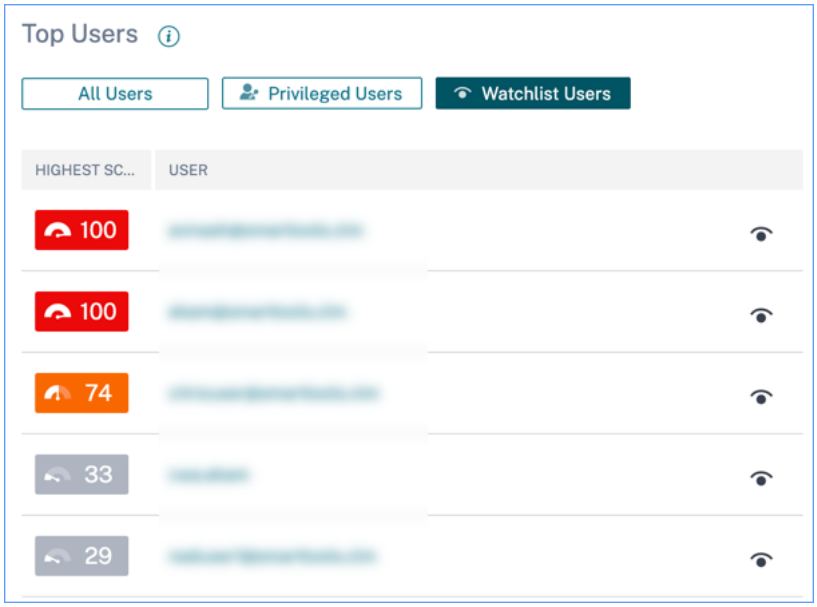

> **Nota:**
>
> En versiones anteriores, la tabla de usuarios principales siempre mostraba la puntuación de riesgo más reciente, independientemente del período de tiempo seleccionado.

### Usuarios de la lista de seguimiento

Lista de usuarios supervisados de cerca para detectar posibles amenazas. Por ejemplo, puede supervisar a los usuarios que no son empleados a tiempo completo en su organización si los agrega a la lista de seguimiento. También puede supervisar a los usuarios que activan un indicador de riesgo específico con frecuencia. Puede agregar un usuario a la lista de seguimiento manualmente o definir directivas para agregar usuarios a la lista de seguimiento.

Si has añadido usuarios a la lista de seguimiento, puedes ver los cinco primeros usuarios de la lista de seguimiento en función de la puntuación más alta.




Haga clic en el enlace **Ver más** del panel **Todos los usuarios** para ver la **página Usuarios**. La página muestra la lista de todos los usuarios de la lista de seguimiento.

> **Nota**
>
> En el panel **Usuarios** y en la página **Usuarios**, se muestra el número de usuarios de la lista de seguimiento durante los últimos 13 meses, independientemente del período de tiempo seleccionado. Al seleccionar un período de tiempo, las incidencias del indicador de riesgo cambian en función de la selección de tiempo.

Más información: Lista de seguimiento

## Categorías de riesgo

El gráfico **circular de categorías de riesgo** resume el número de casos de indicadores por categoría de riesgo durante el período de tiempo seleccionado. Los recuentos de usuarios únicos se muestran al pasar el ratón sobre cada segmento del gráfico, que a su vez enlaza con la página de descripción general de la **categoría de indicadores de riesgo** correspondiente. La categorización de riesgos cuenta con indicadores de riesgo predeterminados y personalizados.

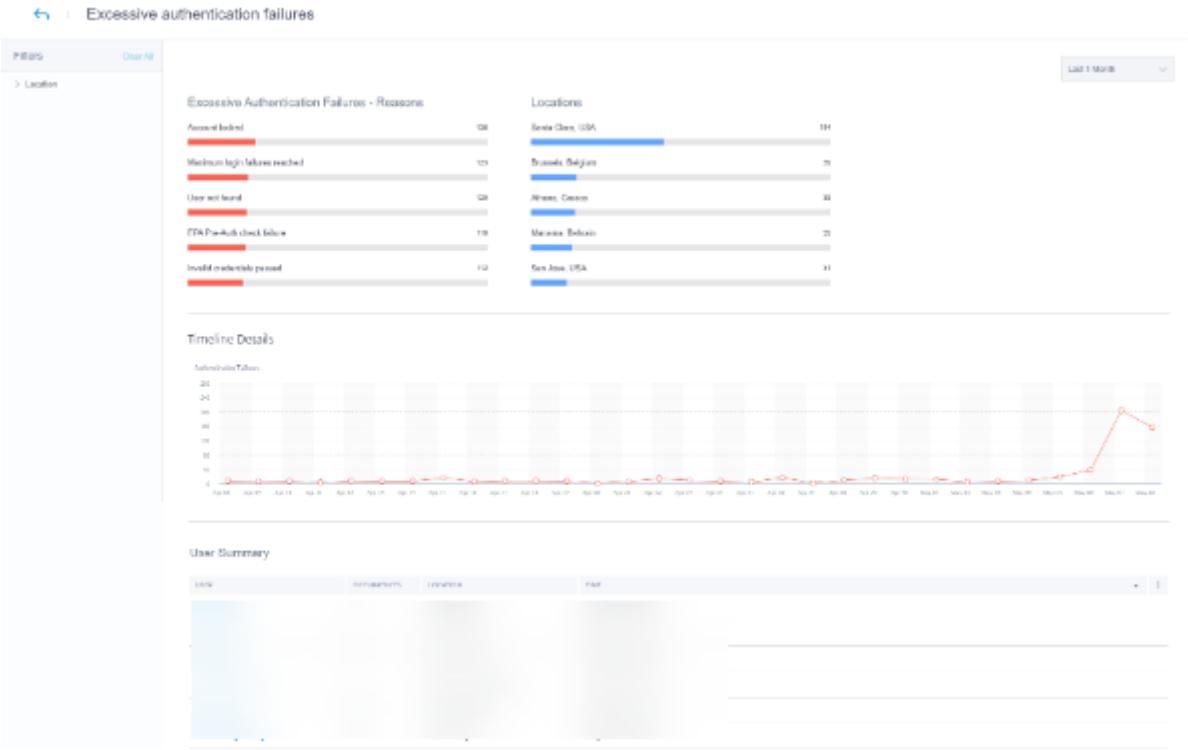
 


El objetivo del panel de **categorías de riesgo** es permitir a los administradores de Citrix Virtual Apps and Desktops y Citrix DaaS gestionar los riesgos de los usuarios y mantener conversaciones simplificadas con sus homólogos de seguridad sin necesidad de tener conocimientos de seguridad de nivel experto. Permite que la aplicación de la seguridad surta efecto a nivel organizativo y no se limita únicamente a los administradores de seguridad.

### Caso de uso

Tenga en cuenta que es administrador de Citrix Virtual Apps and Desktops y administra los derechos de acceso a las aplicaciones de los empleados de su organización. Si va a la sección **Categorías de riesgo** > **Usuarios comprometidos** > **Errores de autenticación excesivos: indicador de riesgo de Citrix Gateway**, puede evaluar si los empleados a los que ha concedido acceso se han visto comprometidos. Si sigue navegando, podrá obtener información más precisa sobre este indicador de riesgo, como los motivos de los fallos, las ubicaciones de inicio de sesión, los detalles del cronograma y el resumen del usuario. Si observa alguna discrepancia entre los usuarios a los que se concedió acceso y los usuarios que se vieron comprometidos, puede notificárselo al administrador de seguridad. Esta notificación oportuna al administrador de seguridad contribuye a la aplicación de la seguridad a nivel organizativo.

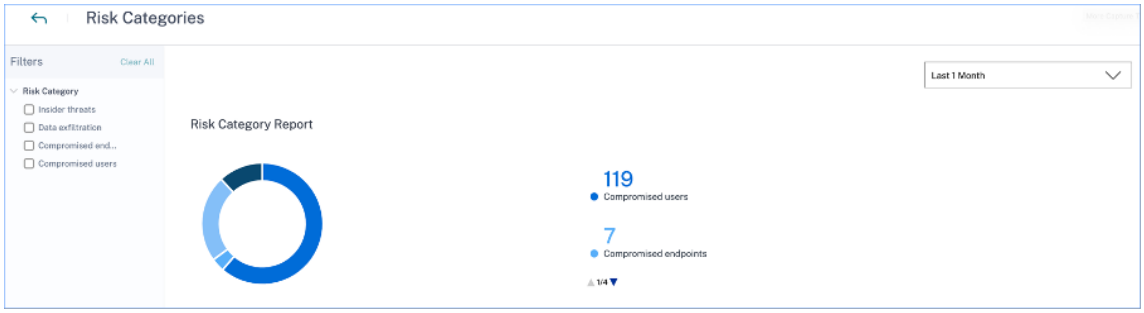
 




### ¿Cómo analizar el panel de control de categorías de riesgo?

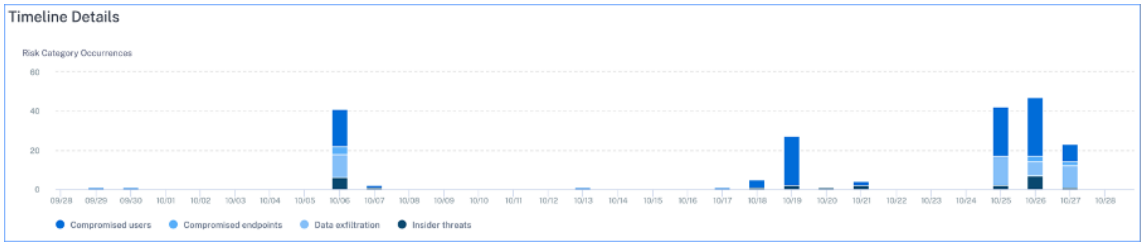
Cuando selecciona **Ver más** en el panel **Categorías de riesgo**, se le redirige a la página que resume los detalles sobre las categorías de riesgo. Esta página contiene los siguientes detalles:

- **Informe de categoría de riesgo**: representa el total de incidencias del indicador de riesgo de cada categoría durante un período de tiempo seleccionado.

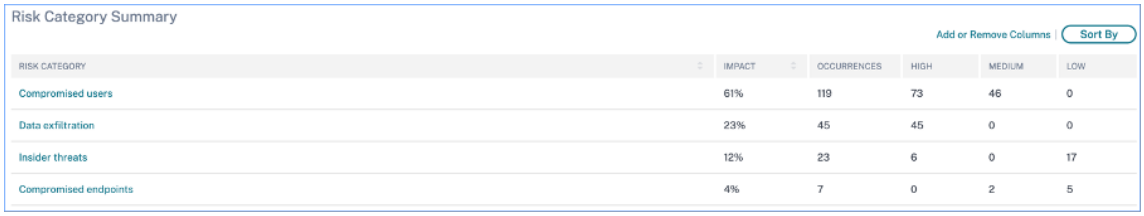



- **Detalles del cronograma**: proporciona una representación gráfica de las incidencias totales del indicador de riesgo de cada categoría de riesgo durante un período de tiempo seleccionado. Si navega hasta la parte inferior de esta sección, puede ordenar según las categorías de riesgo para obtener información más precisa sobre los indicadores de riesgo.



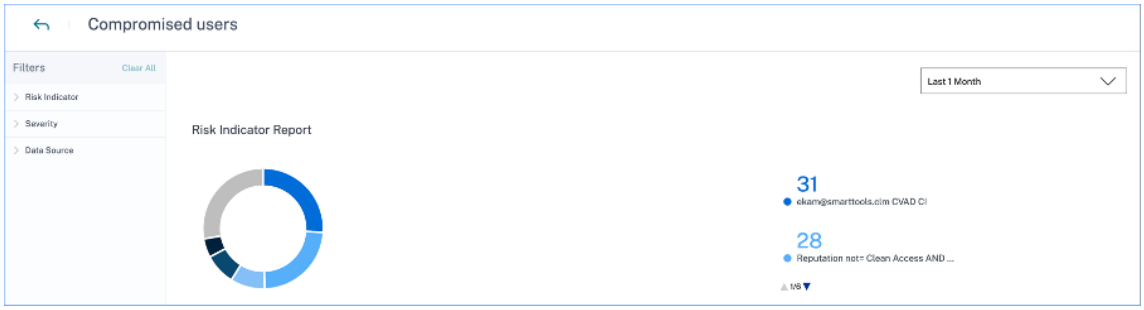

- **Resumen de categorías de riesgo**: En esta sección se proporcionan detalles como el impacto, la incidencia y la gravedad de los indicadores de riesgo asociados a cada categoría. Seleccione cualquier categoría de riesgo para ver detalles sobre los indicadores de riesgo asociados a esa categoría. Por ejemplo, cuando selecciona la categoría **Usuarios comprometidos**, se le redirige a la página **Usuarios comprometidos**.



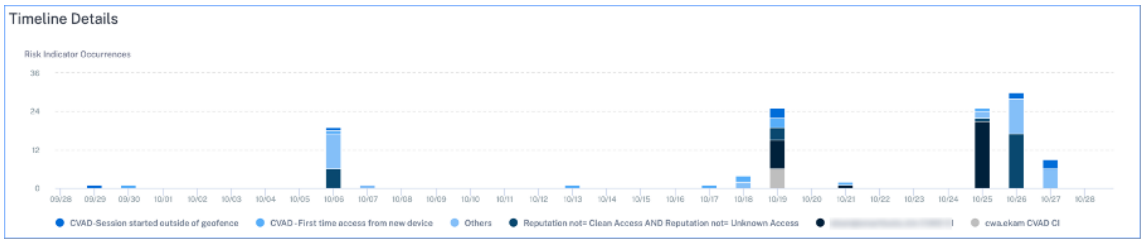

| RISK CATEGORY | IMPACT | OCCURRENCES | HIGH | MEDIUM | LOW |
|---|---|---|---|---|---|
| Compromised users | 61% | 119 | 73 | 46 | 0 |
| Data exfiltration | 23% | 45 | 45 | 0 | 0 |
| Insider threats | 12% | 23 | 6 | 0 | 17 |
| Compromised endpoints | 4% | 7 | 0 | 2 | 5 |

La página **Usuarios comprometidos** muestra los siguientes detalles:

- **Informe Indicador de Riesgo**: Muestra los indicadores de riesgo pertenecientes a la categoría Usuarios comprometidos durante un período de tiempo seleccionado. También muestra el total de ocurrencias de los indicadores de riesgo que se activaron durante el período de tiempo seleccionado.



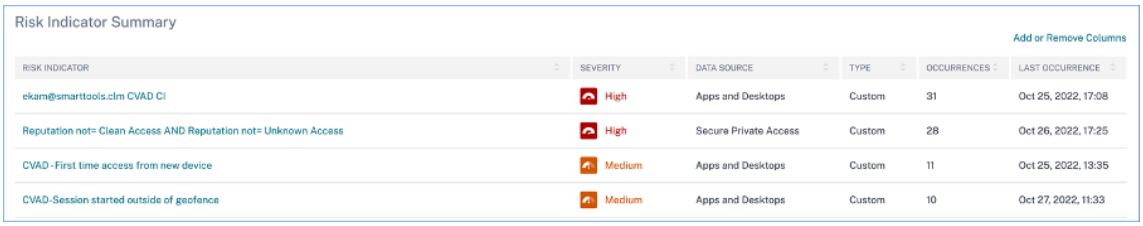

- **Detalles del cronograma**: proporciona una representación gráfica de las incidencias del indicador de riesgo durante un período de tiempo seleccionado.



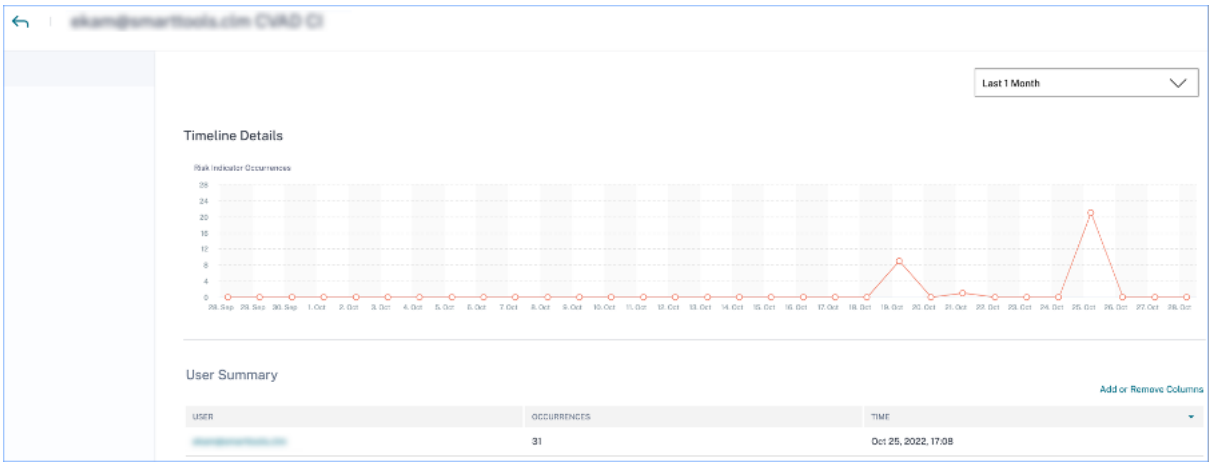

- **Resumen del indicador de riesgo**: muestra un resumen de los indicadores de riesgo generados

en la categoría de usuarios comprometidos. En esta sección también se muestra la gravedad, el origen de datos, el tipo de indicador de riesgo, las incidencias y la última aparición.




Al seleccionar un indicador de riesgo, se le redirige a la página que resume los detalles de ese indicador. Por ejemplo, si selecciona el indicador de riesgo **Acceso por primera vez desde un nuevo dispositivo**, se le redirigirá a la página que resume los detalles de este indicador. El resumen incluye detalles del cronograma sobre las ocurrencias de este evento y un resumen del usuario que enumera los usuarios que activaron este indicador de riesgo, las ocurrencias del indicador de riesgo y la hora del evento. Cuando selecciona un usuario, se le redirige al cronograma de riesgo del usuario.




> **Nota**
>
> Citrix Analytics agrupa los indicadores de riesgo predeterminados en la categoría de riesgo adecuada. Para los indicadores de riesgo personalizados, debe seleccionar una categoría de riesgo en la página **Crear indicador**. Para obtener más información, consulte Indicadores de riesgo personalizados.

### Tipos de categorías de riesgo

**Exfiltración de datos** Esta categoría agrupa los indicadores de riesgo provocados por el malware o por empleados que realizan transferencias de datos no autorizadas o robos de datos hacia o desde un dispositivo de una organización. Puede obtener información sobre todas las actividades de filtración de datos que se han llevado a cabo durante un período de tiempo determinado y mitigar los riesgos asociados a esta categoría aplicando acciones de forma proactiva en los perfiles de usuario.

La categoría de riesgo de exfiltración de datos agrupa los siguientes indicadores de riesgo:

| Orígenes de datos | Indicadores de riesgo del usuario |
|---|---|
| Citrix Virtual Apps and Desktops y Citrix DaaS | Exfiltración potencial de datos |

**Amenazas internas** Esta categoría agrupa los indicadores de riesgo activados por los empleados de una organización. Dado que los empleados tienen niveles más altos de acceso a las aplicaciones específicas de la empresa, las organizaciones tienen más probabilidades de sufrir riesgos de seguridad. Las actividades riesgosas pueden ser causadas intencionalmente por un experto malintencionado o pueden ser el resultado de un error humano. En cualquiera de los escenarios, el impacto en la seguridad de la organización es perjudicial. Esta categoría proporciona información sobre todas las actividades de amenazas internas que han tenido lugar durante un período de tiempo específico. Con la ayuda de esta información, puede mitigar los riesgos asociados a esta categoría aplicando acciones de forma proactiva en los perfiles de usuario.

La categoría de riesgo de amenazas internas agrupa los siguientes indicadores de riesgo:

| Orígenes de datos | Indicadores de riesgo del usuario |
|---|---|
| Citrix Secure Private Access | Intento de acceso a la URL de la lista negra |
| Citrix Secure Private Access | Descarga excesiva de datos |
| Citrix Secure Private Access | Acceso a sitios web con riesgos |
| Citrix Secure Private Access | Volumen de subida |

**Usuarios comprometidos** Esta categoría agrupa los indicadores de riesgo en los que los usuarios muestran patrones de comportamiento inusuales, como inicios de sesión sospechosos y errores de inicio de sesión. Alternativamente, los patrones inusuales pueden ser el resultado de que las cuentas de usuario se vean comprometidas. Puede obtener información sobre todos los eventos de usuario comprometidos que han tenido lugar durante un período de tiempo determinado y mitigar los riesgos asociados a esta categoría aplicando acciones de forma proactiva en los perfiles de usuario.

La categoría de riesgo de usuarios comprometidos agrupa los siguientes indicadores de riesgo:

| Orígenes de datos | Indicadores de riesgo del usuario |
|---|---|
| Citrix Gateway | Fallo en el análisis de punto final |
| Citrix Gateway | Fallos de autenticación excesivos |

| Orígenes de datos | Indicadores de riesgo del usuario |
|---|---|
| Citrix Gateway | Trayectos imposibles |
| Citrix Gateway | Inicio de sesión desde IP sospechosa |
| Citrix Gateway | Error de autenticación inusual |
| Citrix Virtual Apps and Desktops y Citrix DaaS | Inicio de sesión sospechoso |
| Citrix Virtual Apps and Desktops y Citrix DaaS | Trayectos imposibles |
| Microsoft Graph Security | Indicadores de riesgo de protección de identidad de Azure AD |
| Microsoft Graph Security | Indicadores de riesgo de Microsoft Defender for Endpoint |

**Dispositivos de punto final comprometidos** Esta categoría agrupa los indicadores de riesgo que se activan cuando los dispositivos presentan un comportamiento no seguro que podría indicar un riesgo.

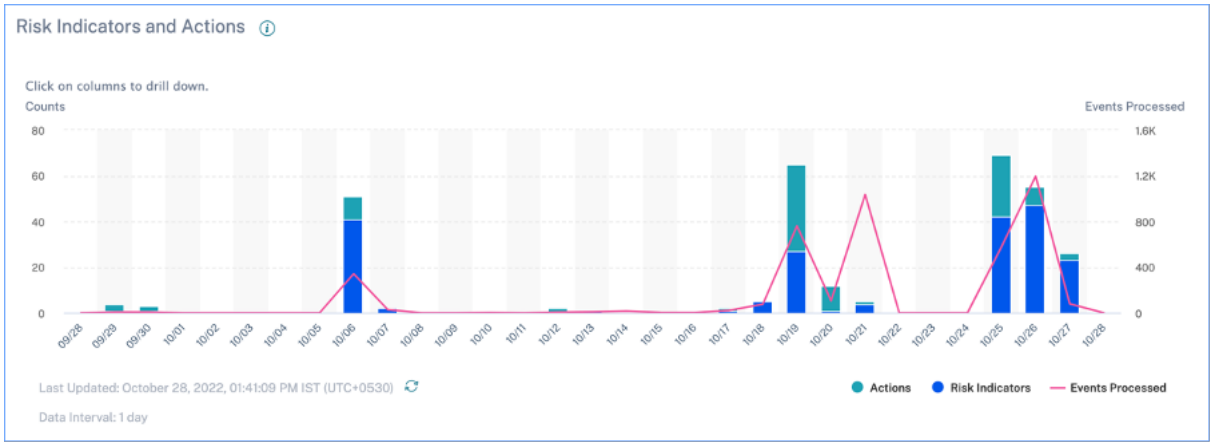
La categoría de riesgo de puntos finales comprometidos agrupa los siguientes indicadores de riesgo:

| Orígenes de datos | Indicadores de riesgo del usuario |
|---|---|
| Citrix Endpoint Management | Dispositivo no administrado detectado |
| Citrix Endpoint Management | Se ha detectado un dispositivo con jailbreak o rooteado |
| Citrix Endpoint Management | Dispositivo con aplicaciones en la lista de bloqueados detectado |

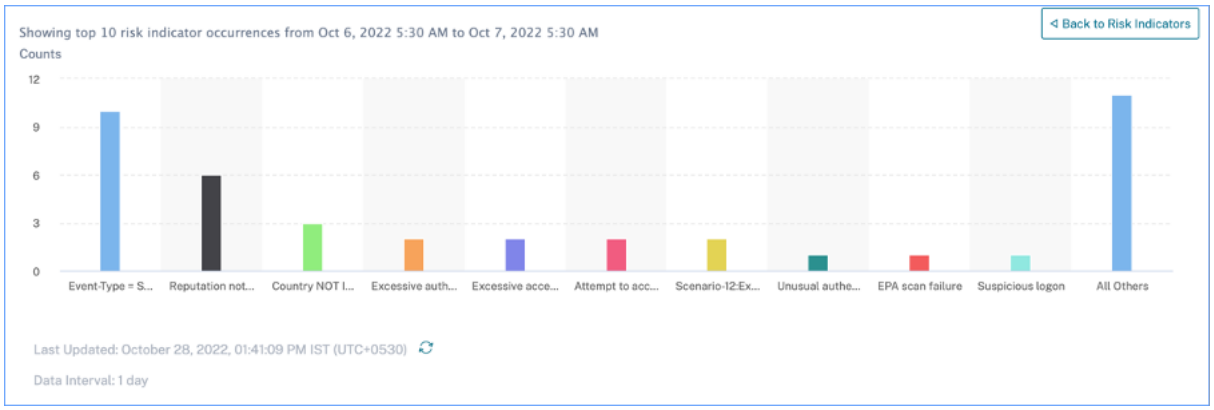
## Indicadores de riesgo y acciones

Puede ver los indicadores de riesgo activados y las acciones aplicadas a sus usuarios durante el período de tiempo seleccionado. El nuevo gráfico de barras de **indicadores de riesgo y acciones** proporciona los recuentos de indicadores, acciones y eventos detallados a lo largo del tiempo, con el rango de tiempo general y el intervalo de barras derivados del período de tiempo seleccionado.




Al hacer clic en un segmento de barra para ver los indicadores o las acciones, se obtiene una visualización detallada de los recuentos por indicador o acción, respectivamente.





En el menú desplegable de indicadores, al hacer clic en una barra indicadora individual, se accede a la página correspondiente del indicador de riesgo para el período de tiempo seleccionado.

## Resumen de acceso

Este panel resume todos los eventos de acceso a Gateway durante un período de tiempo seleccionado. Muestra el número total de accesos, accesos correctos y accesos fallidos a través de Citrix Gateway.

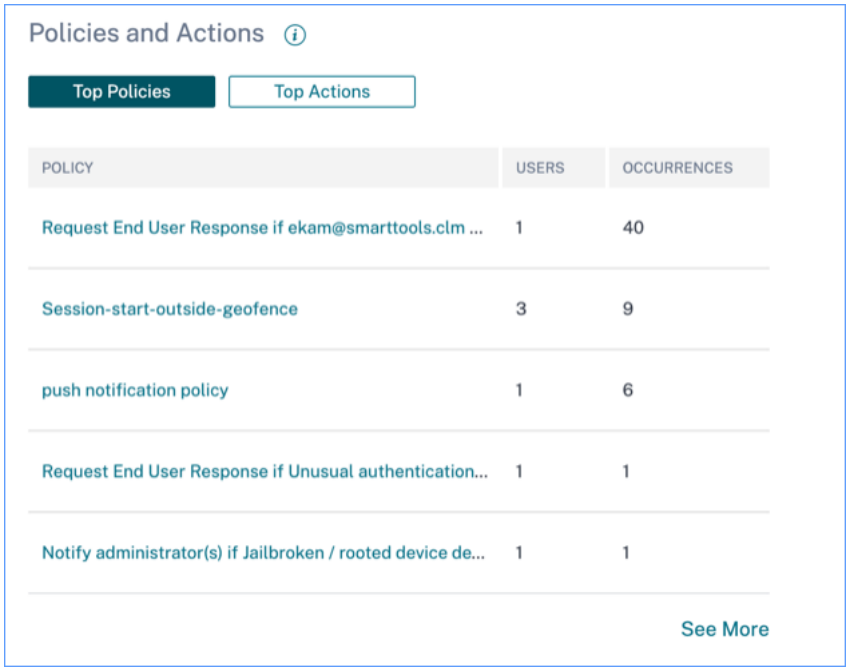
 

Haga clic en los punteros del gráfico para ver la página Búsqueda de autoservicio de puerta de enlace. Para los casos de inicio de sesión satisfactorio, los eventos de acceso a Gateway se ordenan por el código de estado de la página.


## Directivas y acciones

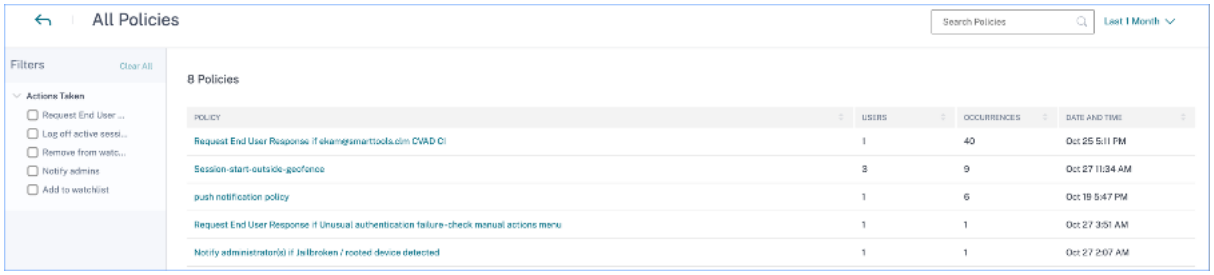
Muestra las cinco directivas y acciones principales aplicadas en los perfiles de usuario durante un período de tiempo seleccionado. Haga clic en el enlace **Ver más** del panel **Directivas y acciones** para obtener información detallada sobre las directivas y acciones.




### Directivas principales

Las cinco directivas configuradas más importantes se determinan en función del número de incidencias. Cuando se encuentre en la sección **Directivas principales** del panel de control y selecciona **Ver más**, se le redirigirá a la página **Todas las directivas**.




**Todas las directivas** En esta página se proporciona información detallada sobre todas las directivas configuradas. Al seleccionar cualquier directiva, se le redirigirá a la página Búsqueda de autoservicio de directivas. En el panel izquierdo, puede filtrar según las acciones aplicadas.

Cuando selecciona un nombre de usuario, se le redirige al cronograma de riesgos. La acción basada en directivas se agrega al cronograma de riesgo del usuario. Al seleccionar la acción, sus detalles se muestran en el panel derecho del cronograma de riesgo.

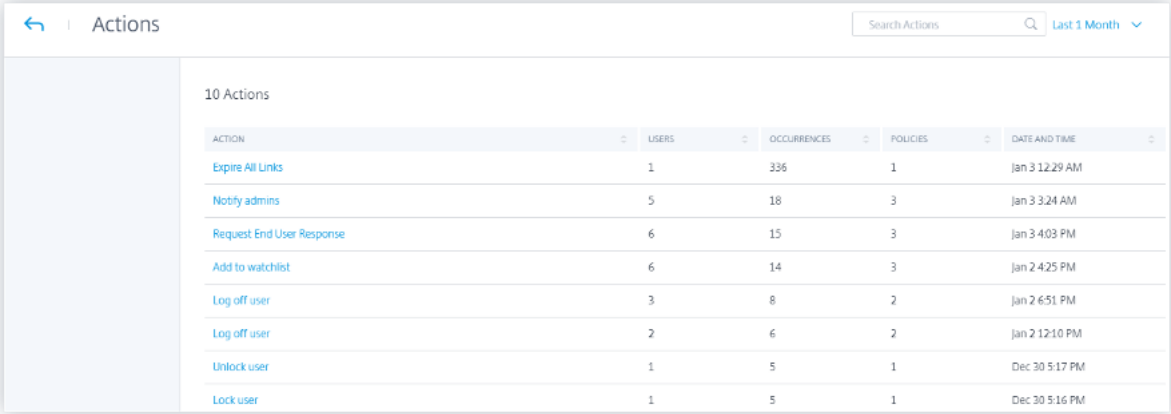
### Acciones principales

Las cinco acciones principales asociadas a las directivas que se aplicaron a los perfiles de usuario. En esta sección no se muestran las acciones que ha aplicado manualmente en los perfiles de usuario. Las acciones principales se determinan por el número de ocurrencias.

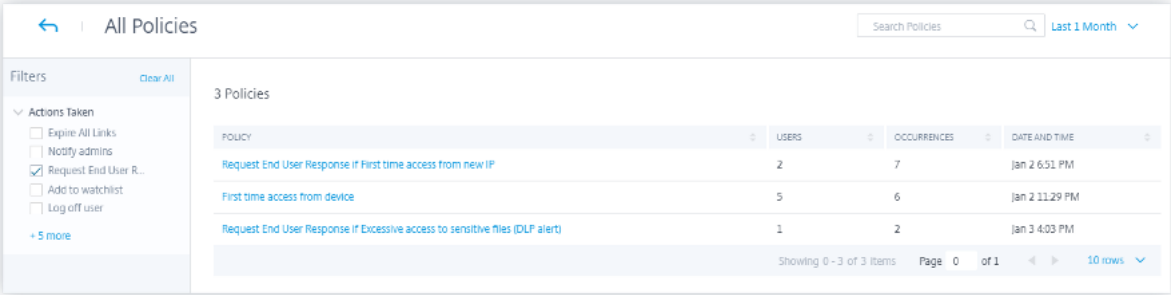
Haga clic en **Ver más** para ver todas las acciones basadas en directivas de la página **Acciones**.

**Acciones** La página proporciona la lista de todas las acciones basadas en directivas que se han aplicado a los usuarios durante el período de tiempo seleccionado. Puede ver la siguiente información:

- Nombre de la acción aplicada según la directiva
- Número de usuarios a los que se ha aplicado la acción
- Número de apariciones de la acción
- Número de directivas asociadas a la acción
- Fecha y hora de la acción aplicada




Haga clic en una acción para ver todas las directivas asociadas. Estas directivas se ordenan según el número de incidencias. Por ejemplo, haga clic en **Solicitar respuesta del usuario final** en la página **Acciones**. La página **Todas las directivas** muestra todas las directivas asociadas a la acción **Solicitar respuesta del usuario final**.



En la página **Todas las directivas**, haga clic en una directiva para ver los eventos de usuario en los que se ha aplicado la acción.

### Indicadores de riesgo

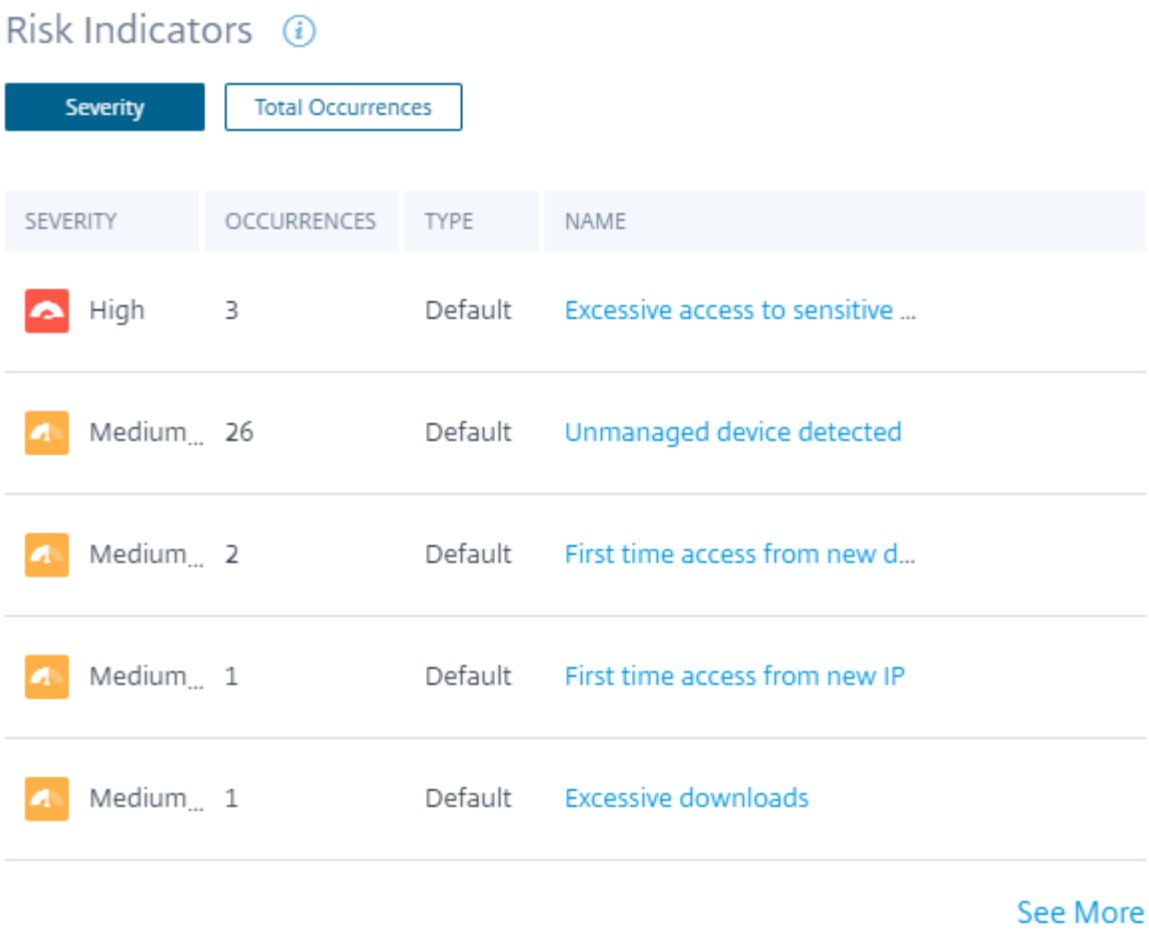
Resume los cinco principales indicadores de riesgo para un período de tiempo seleccionado. Los indicadores de riesgo pueden ser por defecto o personalizados. Para los indicadores de riesgo predeterminados, Citrix Analytics recopila datos de los orígenes de datos detectadas y en las que está habilitado el procesamiento de datos.

Para los indicadores de riesgo personalizados, Citrix Analytics recopila datos de estos orígenes de datos en función de los eventos de riesgo generados:

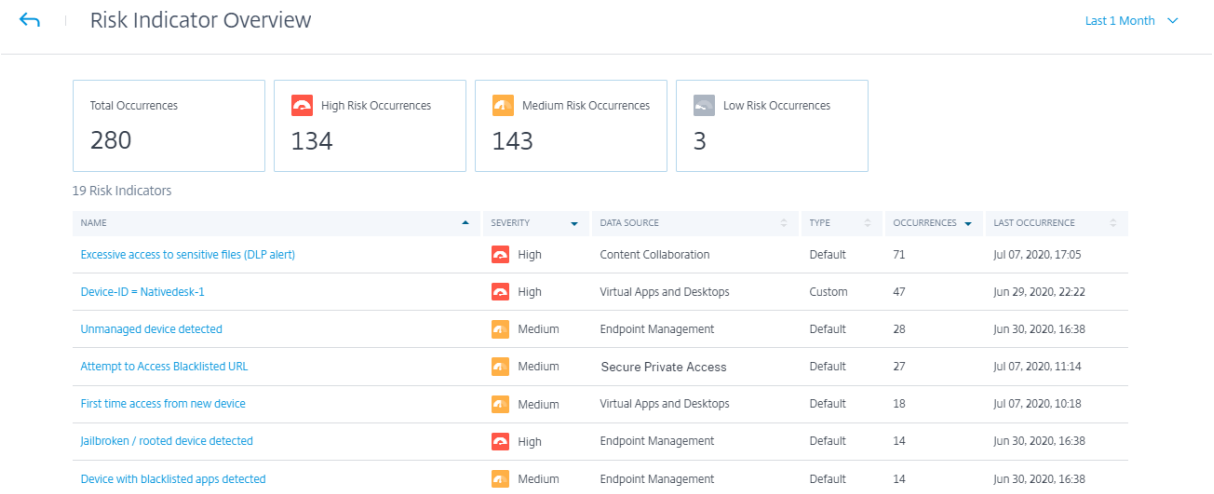
- Citrix Gateway
- Citrix Secure Private Access
- Citrix Virtual Apps and Desktops
- Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service)

En el panel **Indicadores de riesgo**, puede ver los cinco indicadores de riesgo principales y ordenarlos según la incidencia total o la gravedad.




Haga clic en **Ver más** en el panel **Indicadores de riesgo** para ver la página **Resumen de indicadores de riesgo**.



# Panel de mandos de Access Assurance

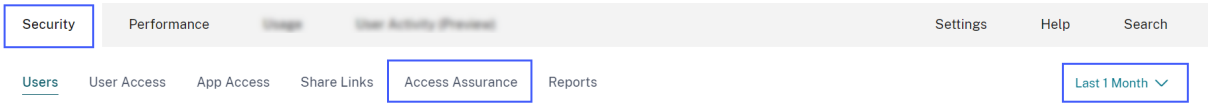
December 6, 2022

Con el aumento del trabajo remoto, como administrador de TI de Citrix, es posible que quiera asegurarse de que sus usuarios acceden a Citrix Virtual Apps and Desktops o a Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service) desde sus ubicaciones habituales y seguras. Si algún usuario ha iniciado sesión desde ubicaciones desconocidas o nuevas ubicaciones, puede validar sus datos de inicio de sesión y tomar las medidas necesarias para mitigar cualquier amenaza a su entorno de TI de Citrix.

El panel de mandos de Access Assurance proporciona una descripción general de las ubicaciones y redes desde las que los usuarios acceden a las aplicaciones o escritorios virtuales. Citrix Analytics for Security recibe estos eventos de inicio de sesión de usuario de la aplicación Citrix Workspace instalada en los dispositivos de los usuarios. Para obtener más información sobre las versiones compatibles, consulte la Tabla de versiones de la aplicación Citrix Workspace.

## Ver el panel

Para ver el panel de control, haga clic en **Seguridad > Garantía de acceso**. Seleccione el período de tiempo para el que quiere ver los detalles de inicio de sesión.

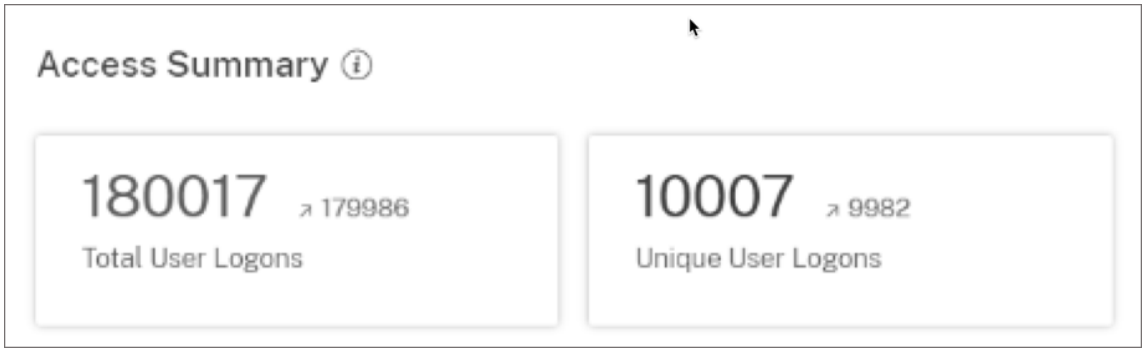



## Resumen del acceso

La sección de resumen del panel de mandos proporciona la siguiente información para un período seleccionado:

1. Número total de inicios de sesión de usuarios en las ubicaciones (en todo el mundo).
2. Número total de inicios de sesión de usuarios únicos en las ubicaciones (en todo el mundo).




### Ubicación de inicio de sesión

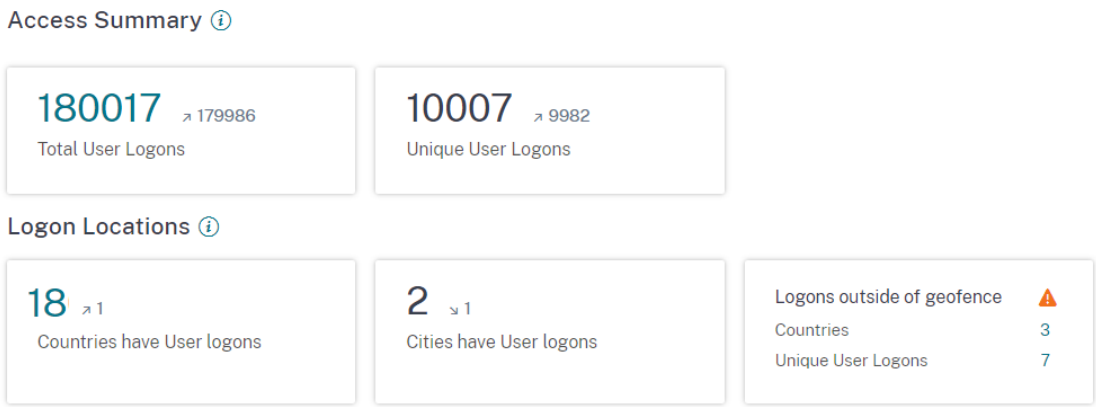
La sección **Ubicaciones de inicio de sesión** proporciona la siguiente información para un período seleccionado:

- Número total de países desde los que los usuarios han iniciado sesión.
- Número total de ciudades desde las que los usuarios han iniciado sesión.
- El número total de países y los inicios de sesión de usuario únicos en las áreas de geocercas. Para ver los detalles de inicio de sesión desde las áreas de geocercas, habilite geocercas.
- Las 10 mejores ubicaciones con inicios de sesión de usuario únicos. A veces, los inicios de sesión de usuario únicos más importantes también proceden de ciudades y países desconocidos y se enumeran en la ficha **Ubicaciones desconocidas**. La lista de ubicaciones desconocidas también es un subconjunto de las 10 ubicaciones principales. Para averiguar los motivos por los que algunas ubicaciones no están identificadas, consulte Ubicaciones identificadas como no disponibles.

También puede ver la tendencia al alza o a la baja del total de inicios de sesión de usuarios en todo el mundo y del total de inicios de sesión de usuarios únicos en todo el mundo. Para las 10 ubicaciones principales, la columna **DESVIACIÓN** muestra el cambio (positivo (+) o negativo (-)) en los inicios de sesión de los usuarios para cada ubicación. Esta comparación se basa en el período de tiempo seleccionado y el período de tiempo anterior de igual longitud. Por ejemplo, si selecciona el período de tiempo **Último 1 mes**, la tendencia de inicio de sesión del usuario y la desviación se comparan entre el último mes y el mes anterior al último.

> **Nota**
>
> La información de ubicación se proporciona a nivel de ciudad y país y no representa una geolocalización precisa. Para obtener más información sobre la garantía de acceso y la geolocalización, consulte las Preguntas frecuentes.

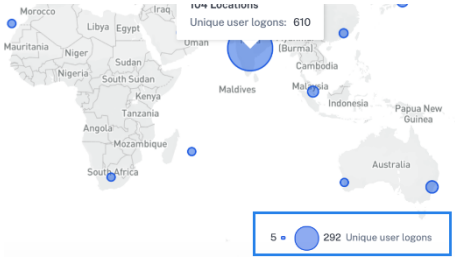



En la tabla **Las 10 principales ubicaciones de inicio de sesión únicas**, seleccione una ubicación para ver los usuarios y sus perfiles de acceso y detalles de inicio de sesión.


El mapa muestra el número de usuarios únicos de varias ubicaciones durante un período seleccionado. Pase el mouse sobre la burbuja azul o amplíe una ubicación para ver el número total de inicios de sesión de usuario únicos desde la ubicación. Haga clic en la burbuja azul para ver los detalles de acceso de una ubicación.


En la esquina inferior derecha del mapa, puede ver el rango de los inicios de sesión de usuario únicos. Durante un período seleccionado, la pequeña burbuja indica el número mínimo de inicios de sesión de usuario únicos en todas las ubicaciones. La burbuja grande indica el número máximo de inicios de sesión de usuario únicos en todas las ubicaciones.



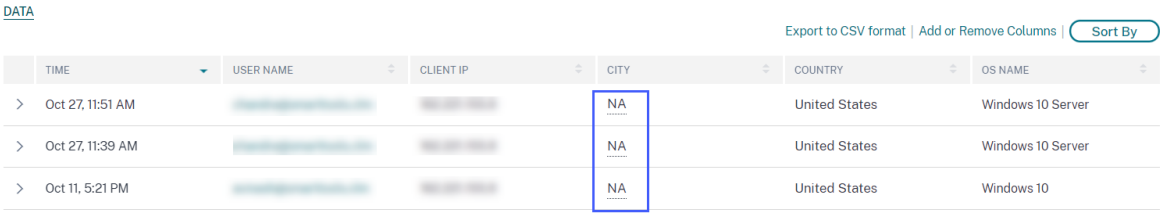

## Ubicaciones identificadas como no disponibles

En la tabla **Las 10 principales ubicaciones de inicio de sesión únicas**, es posible que vea que algunas ubicaciones son desconocidas o no están disponibles. Haga clic en una ubicación desconocida para ver los detalles de inicio de sesión de usuario correspondientes en la página **Inicio de sesión de usuario**.

En la página Inicio de **sesión de usuario**, la tabla **DATA** muestra la etiqueta **NA** si la información de cualquier país o ciudad no está disponible.

Pase el mouse sobre la etiqueta **NA** para ver el motivo por el que la información de ubicación no está disponible.




Es posible que aparezca uno de los siguientes casos de falta de disponibilidad de una ubicación:

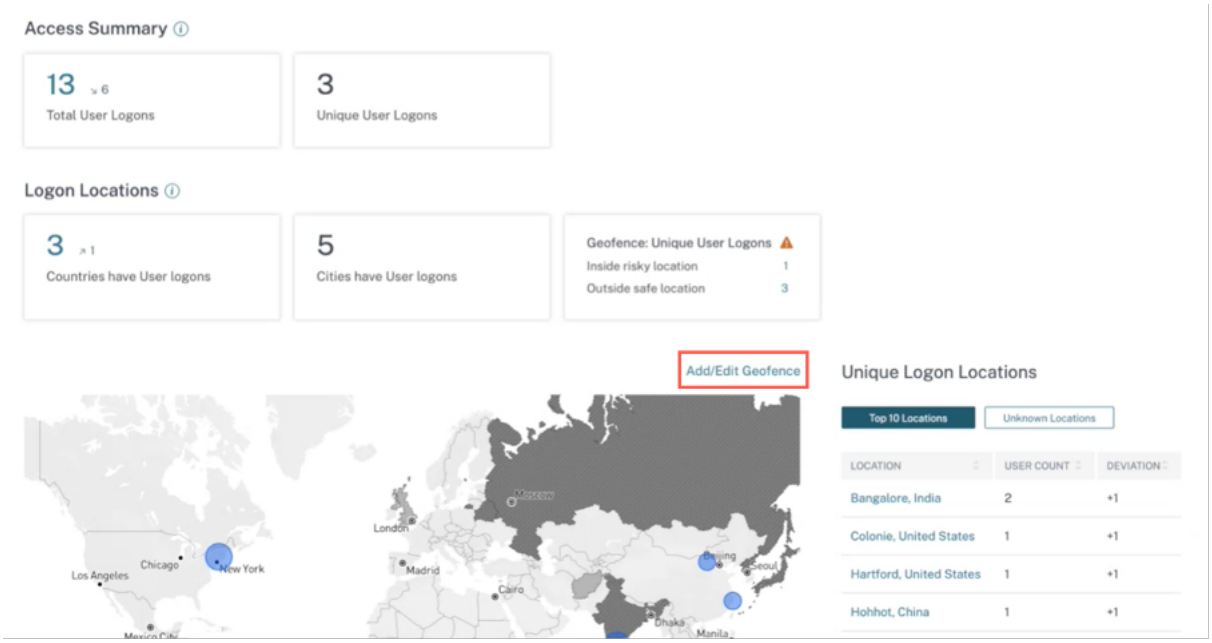
| Caso | Razones |
|---|---|
| El nombre de la ciudad y el nombre del país no están disponibles. | Alguno de los siguientes<br>1. Los usuarios utilizan una versión no compatible de la aplicación Citrix Workspace. Para ver la información de ubicación, actualice el cliente a una versión compatible. |
| Ubicaciones con IP privadas | El dispositivo del usuario se encuentre dentro de una red privada. En este caso, la información de ubicación no está disponible para Citrix Analytics. |
| El nombre del país está disponible pero el nombre de la ciudad no está disponible. | Es posible que el dispositivo del usuario utilice una IP corporativa. Los rangos de IP corporativas están ofuscados en el servicio de geolocalización externa. Por lo tanto, la información de ubicación no está disponible para Citrix Analytics. |

## Habilitar geocercas

Las geocercas le ayudan a identificar a los usuarios que acceden a aplicaciones o escritorios virtuales desde fuera de una geocerca segura y dentro de áreas peligrosas de las geocercas. Para ver la página **Resumen de acceso**, vaya a **Seguridad > Garantía de acceso**.

De forma predeterminada, los **Parámetros de geocercas** siempre están activados. Para configurar la geocerca, haga clic en **Agregar/Modificar geocerca**.

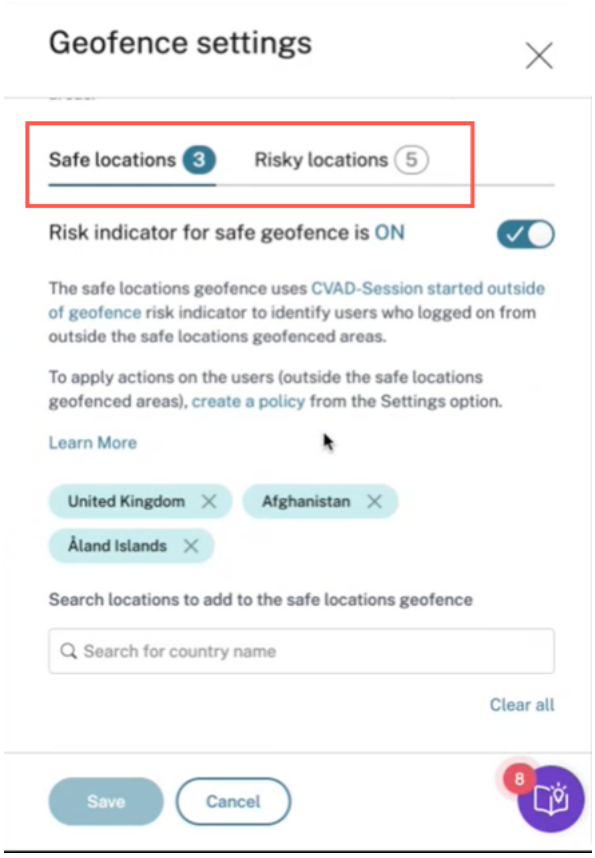



La ventana **Parámetros de geocercas** aparece con dos fichas:

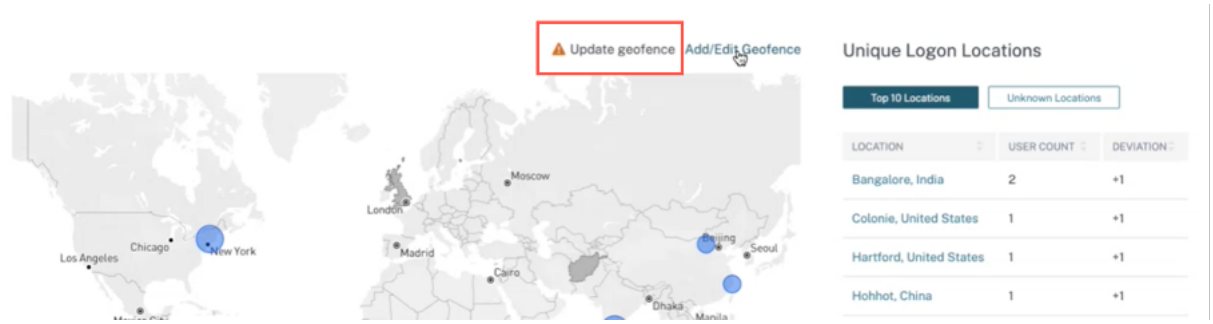
- **Ubicaciones seguras**: Puede configurar o quitar los países que pertenecen a la ubicación segura.
- **Ubicaciones de riesgo**: Puede configurar o quitar los países que se encuentran en ubicaciones de riesgo.

  También puede ver el número total de ubicaciones seguras y de riesgo configuradas en cada ficha. Para eliminar o quitar un país de una geofcerca de ubicación segura o geocerca de ubicación de riesgo, haga clic en el signo de cierre (X) situado junto al país. Haga clic en **Guardar** para guardar los parámetros de geocercas.

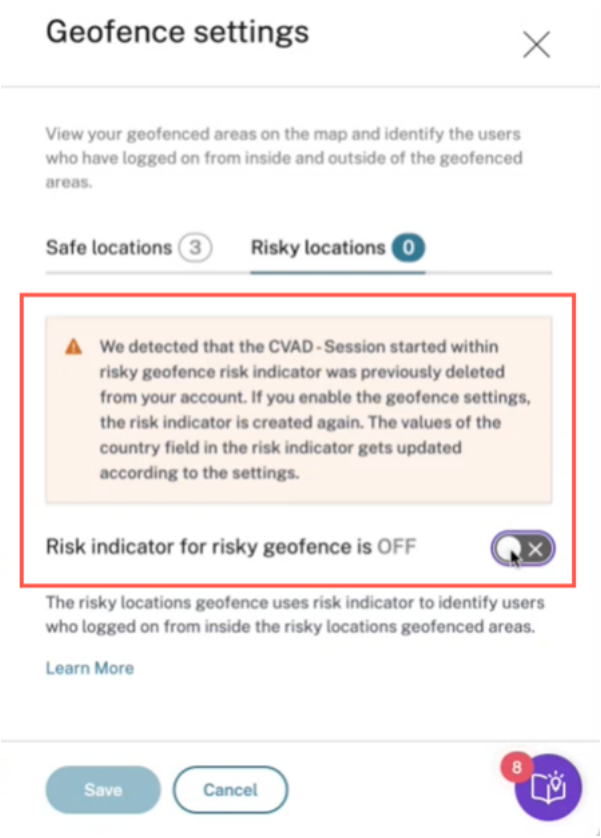



Puede configurar los países que se incluyen en Geocerca de ubicaciones de riesgo. Si no se han agregado indicadores de riesgo para la geocerca de ubicaciones de riesgo o si se eliminan los indicadores de riesgo, puede ver un mensaje de advertencia sobre la **actualización de geofence** junto a **Agregar o modificar geocerca**.




Para recrear el indicador, vaya a la ficha **Ubicaciones de riesgo** y active la opción **Indicador de riesgo para geocercas de riesgo**.




El indicador se crea con la lista predeterminada de ubicaciones de riesgo.

La página **Resumen de acceso** también muestra los países seguros y de riesgo en geocercas.

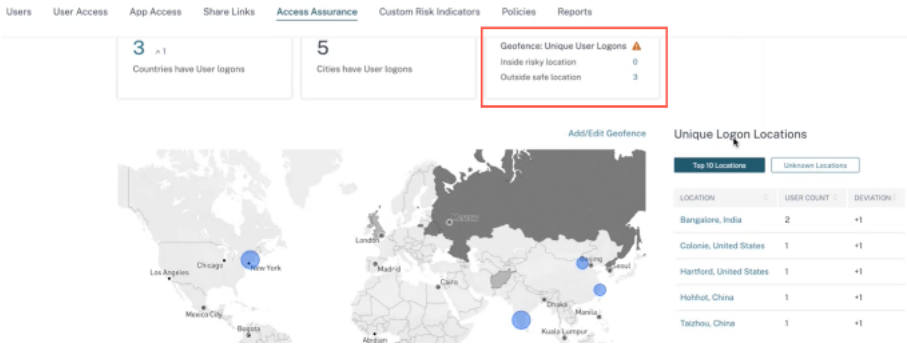
- Los países seguros en geocercas están marcados con un círculo gris claro.
- Los países de riesgo en geocercas están marcados con un círculo gris oscuro.

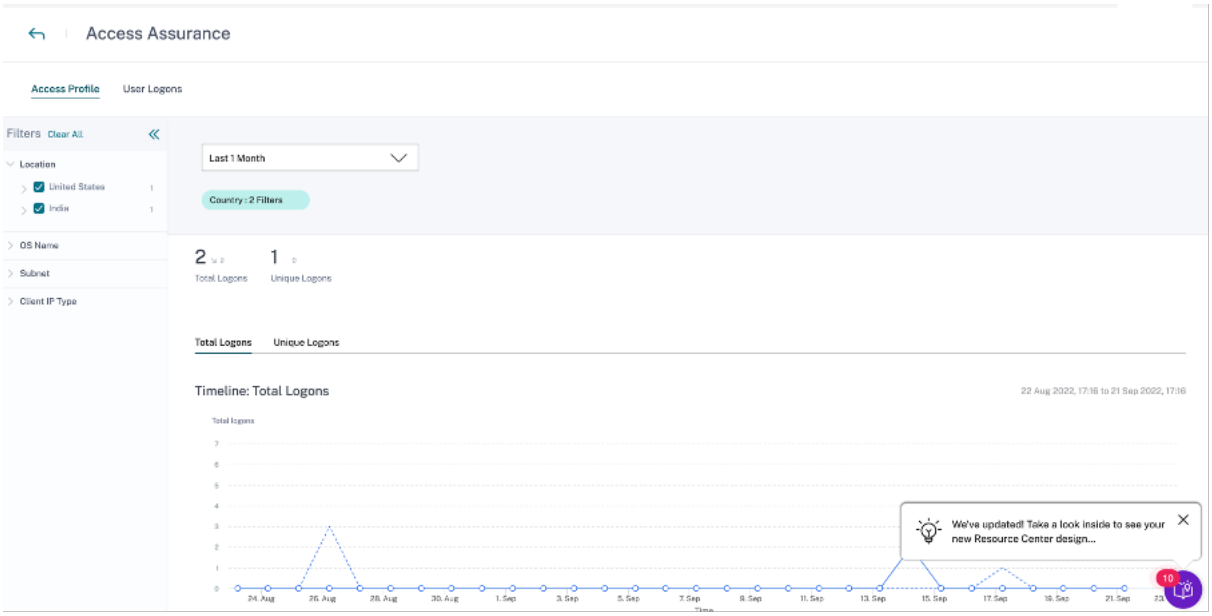
### Geocerca: Inicios de sesión de usuario únicos

Vay a la página Resumen de acceso para ver Geocerca: Inicios de sesión de usuario únicos. La tarjeta muestra el número de ubicaciones seguras dentro y fuera de ubicaciones seguras.

- **Dentro de una ubicación de riesgo**: Identifique a los usuarios que iniciaron sesión desde las áreas en geocercas de las ubicaciones de riesgo.
- **Ubicación segura externa**: Identifique a los usuarios que iniciaron sesión desde fuera de las áreas en geocercas de las ubicaciones seguras.




Para obtener un resumen detallado del total y de los inicios de sesión de usuarios únicos, haga clic en el número situado junto a Ubicación de riesgo interno o Ubicación segura externa.




Esta función utiliza el siguiente indicador de riesgo personalizado preconfigurado:

- **CVAD-Sesión iniciada fuera de geocercas**: Para supervisar inicios de sesión de usuarios fuera de geocercas seguras.
- **CVAD-Sesión iniciada dentro de una geocerca de riesgo**: Para supervisar inicios de sesión de usuarios dentro de geocercas

Si se detectan inicios de sesión de usuario fuera de la geocerca, se activa el indicador de riesgo y se aplica a esos usuarios la directiva Sesión iniciada fuera de la geocerca. La directiva activa la acción *Solicitar respuesta del usuario final* y, en función de la respuesta del usuario, puede tomar las medidas adecuadas para evitar amenazas de inicios de sesión sospechosos. Para obtener más información, consulte indicadores de riesgo personalizados preconfigurados.

> **Notas**
>
> - En la **configuración de geocercas**, al modificar los países, también se actualiza la *sesión de CVAD iniciada fuera del indicador de riesgo de geocercas*.
> - Por ejemplo, si selecciona y guarda los países Australia e India como los nuevos países geocercados, la condición preconfigurada del indicador de riesgo se actualiza con los nuevos países, además de los Estados Unidos (que es la geocerca predeterminada). También puede eliminar el país geocercado predeterminado Estados Unidos.
>
>  Estado preconfigurado del indicador de riesgo:
>
>  ```
>  Event-Type = \"Session.logon\" AND Country != \"\" AND Country
>  ~ \"\" AND Country != \"United States\"
>  ```
>
>  Después de actualizar la **configuración de geocercado**, el estado del indicador de riesgo:
>
>  ```
>  Event-Type = \"Session.logon\" AND Country != \"\" AND Country
>  ~ \"\" AND Country NOT IN (\"Australia\", \"United States\",
>  \"India\"
>  ```
>
> - Si la *sesión de CVAD iniciada fuera del indicador de riesgo de geocercado* se ha eliminado previamente de su cuenta, al activar la **configuración de geocercado** se vuelve a crear el indicador de riesgo. Los países geocercados del indicador de riesgo se controlan desde los **ajustes de geocercado**.

Después de habilitar la **configuración de geocerca**, el mapa muestra las áreas geocercadas y los inicios de sesión de usuario únicos desde estas áreas.

### Red de inicio de sesión

En el panel de mandos de Access Assurance, ahora puede ver los siguientes detalles de usuario adicionales:

- Las organizaciones asociadas a las direcciones IP desde las que los usuarios han iniciado sesión. Estas organizaciones incluyen entidades como empresas, gobiernos, entidades educativas y proveedores de servicios de Internet.
- La subred pública única total y la subred privada desde las que los usuarios han iniciado sesión.

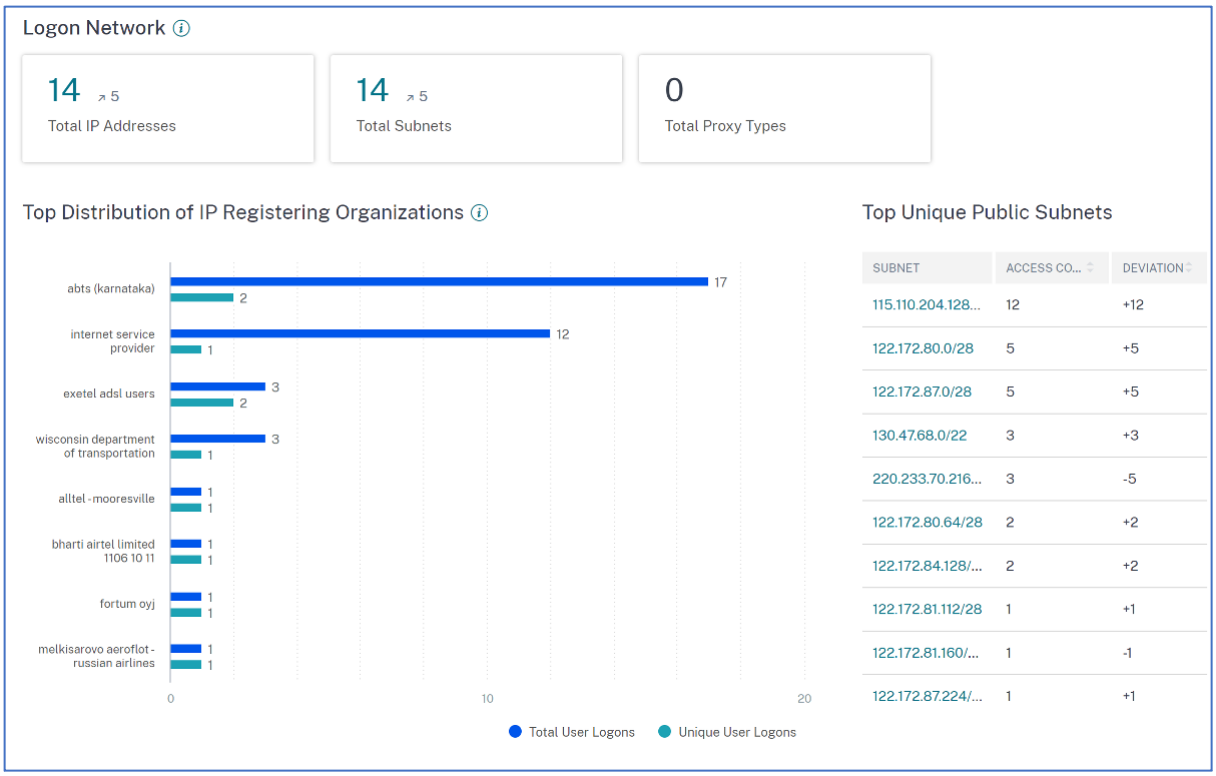
 

- Los detalles de que el usuario ha iniciado sesión mediante servidores proxy y servicios de VPN privadas.

Con estos detalles adicionales, como administrador, puede validar los detalles de inicio de sesión del usuario y asegurarse de que el inicio de sesión del usuario cumple con las expectativas de seguridad de la organización.

### Ver detalles de la red de usuarios

Vaya a **Seguridad > Access Assurance** y desplácese hacia abajo para ver los detalles en **Red de inicio de sesión**.




- **Direcciones IP totales**: Indica el número total de direcciones IP únicas que se utilizan para iniciar sesión en las sesiones virtuales.
- **Total de subredes**: Indica el número total de subredes que se utilizan para iniciar sesión en las sesiones virtuales.
- **Tipos totales de proxy**: Indica los tipos totales de red o protocolo utilizados por el servidor para proxiar la conexión del usuario.
- En **Distribución superior de las organizaciones de registro de IP**, puede visualizar una descripción general del total de inicios de sesión de los usuarios y los detalles de inicio de sesión únicos de cada organización (ISP). Puede hacer clic en el gráfico para ver los detalles de los

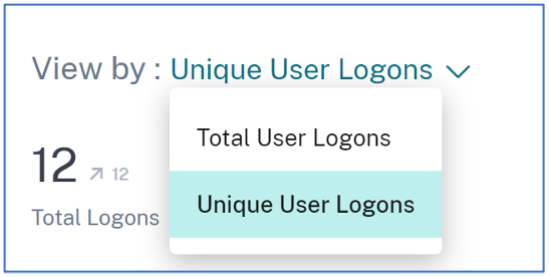
 

usuarios y sus perfiles de acceso y detalles de inicio de sesión asociados a la organización seleccionada.

- En **Total de subredes públicas únicas**, puede visualizar una descripción general de las subredes, el total de inicios de sesión de los usuarios de cada subred y la tendencia de desviación en cada subred. Puede hacer clic en cada subred para ver los detalles de los usuarios y sus perfiles de acceso y detalles de inicio de sesión asociados a la subred seleccionada.

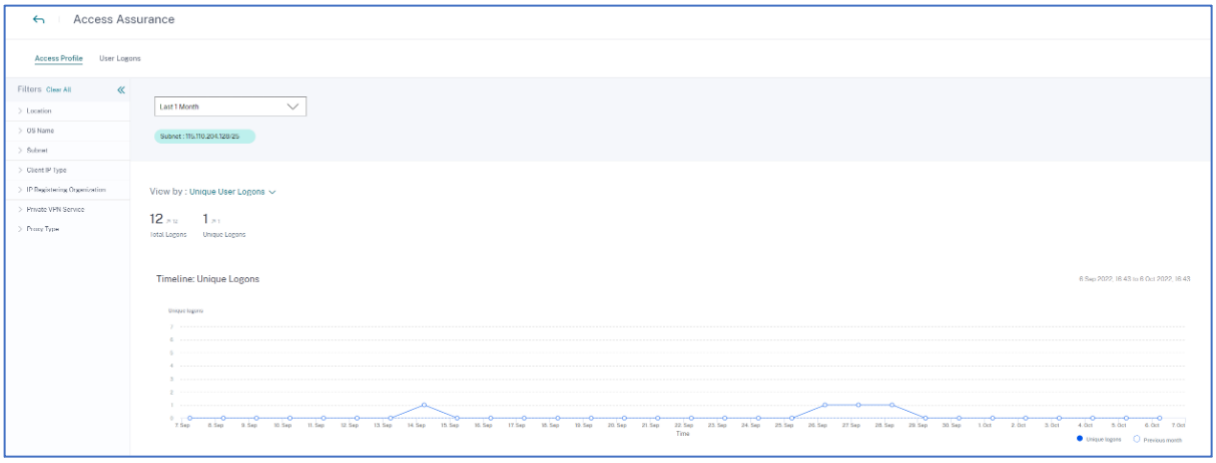
### Ver los perfiles de acceso de los usuarios

Al desglosar cualquier métrica (ubicación, organización o subred), la página **Perfil de acceso** proporciona un resumen de los accesos de los usuarios a las aplicaciones o escritorios virtuales desde las ubicaciones seleccionadas. Puede seleccionar la opción de inicio de sesión único o de inicio de sesión total para ver el análisis de tendencias del período seleccionado.




Puede ver los principales eventos de acceso para la métrica seleccionada (ubicación, organización o subred). Esta información le ayuda a revisar los patrones de acceso y los detalles para la investigación y el análisis de amenazas.

La tendencia ascendente o descendente de los inicios de sesión totales de los usuarios y los inicios de sesión de usuario únicos se compara en función del período de tiempo seleccionado y el período de tiempo anterior de igual longitud. Por ejemplo, si selecciona el período de tiempo como **Último mes**, la tendencia se compara entre el último mes y el anterior al último mes.



### Facetas

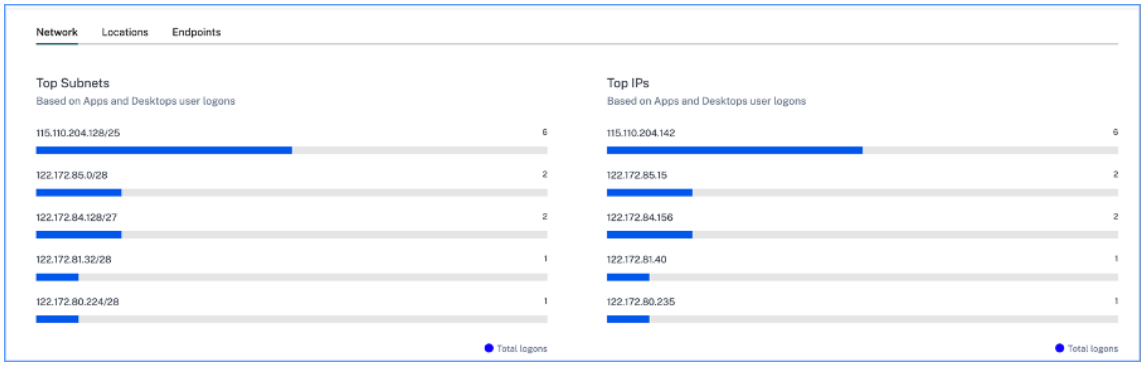
Puede utilizar las siguientes facetas para los eventos de acceso:

- **Ubicación**: filtra los eventos de acceso por países y sus ciudades.
- **SO**: filtre los eventos de acceso por los sistemas operativos y sus versiones.
- **Subred**: Filtra los eventos de acceso por subredes.
- **Tipo de IP de cliente**: Filtra los eventos de acceso por públicos o privados.
- **Organización de registro de IP**: Filtra la organización asociada a la dirección IP pública.
- **Servicio de VPN privada**: Filtra los eventos de acceso por los nombres de las redes VPN privadas.
- **Tipo de proxy**: Filtra los eventos de acceso según las clasificaciones del tipo de proxy, como HTTP, web, Tor y SOCKS.

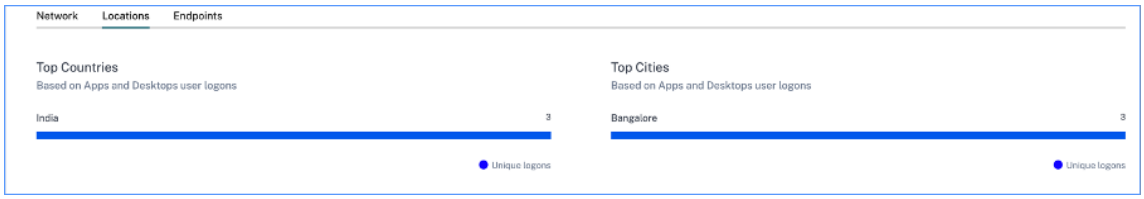
> **Nota**
>
> También puede ver la etiqueta no disponible si los datos no están disponibles o no están identificados.

Según los filtros aplicados, vea la siguiente información para el total de inicios de sesión de usuario y los inicios de sesión de usuario únicos:

- **Red**: Las principales subredes y las direcciones IP desde las que los usuarios han iniciado sesión en aplicaciones o escritorios virtuales.

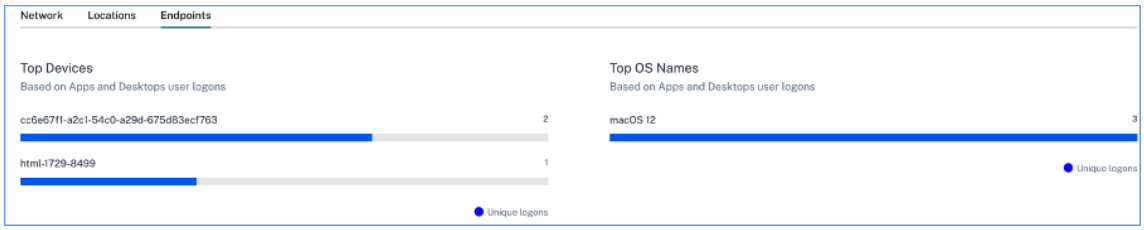



- **Ubicaciones**: Los principales países y ciudades desde los que los usuarios han iniciado sesión en aplicaciones o escritorios virtuales.



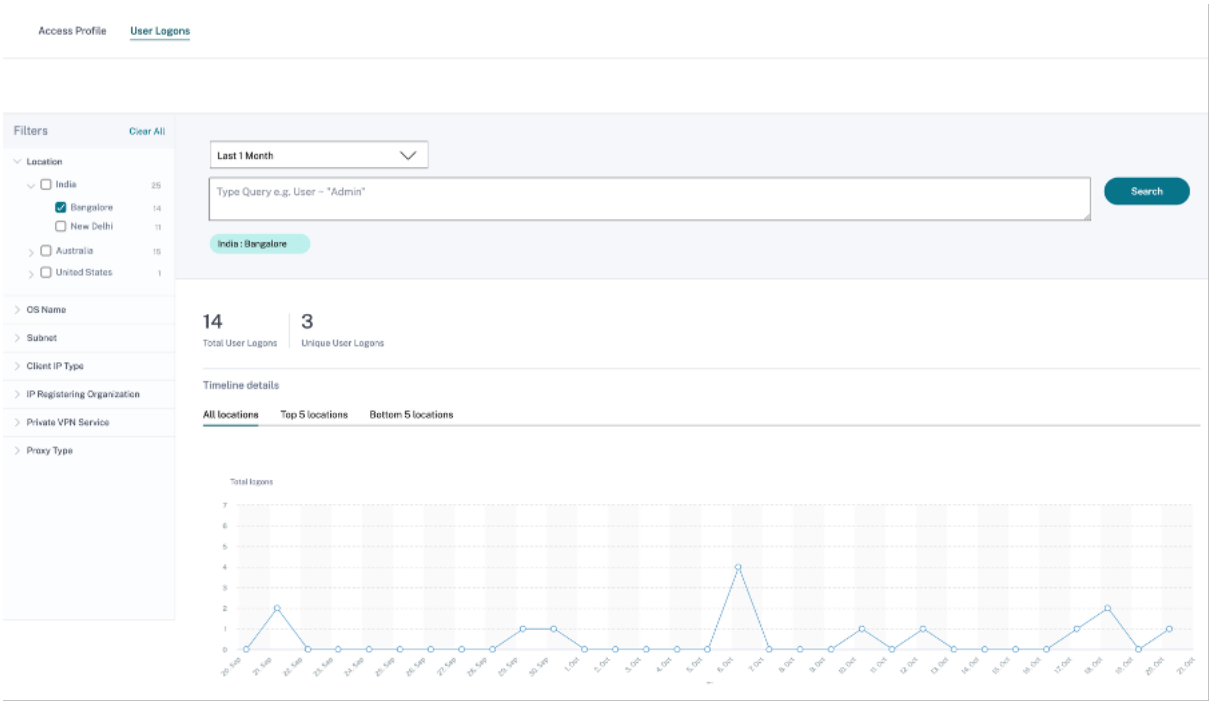

 

- **Dispositivos de punto final**: Los principales nombres de dispositivos y sistemas operativos según los inicios de sesión de los usuarios de aplicaciones y escritorios.




## Ver los detalles de inicio de sesión de los usuarios

La página Inicios de **sesión de usuario** proporciona los detalles de los inicios de sesión de los usuarios en aplicaciones virtuales o escritorios virtuales desde las ubicaciones seleccionadas. Esta información le ayuda durante la investigación y el análisis de amenazas.

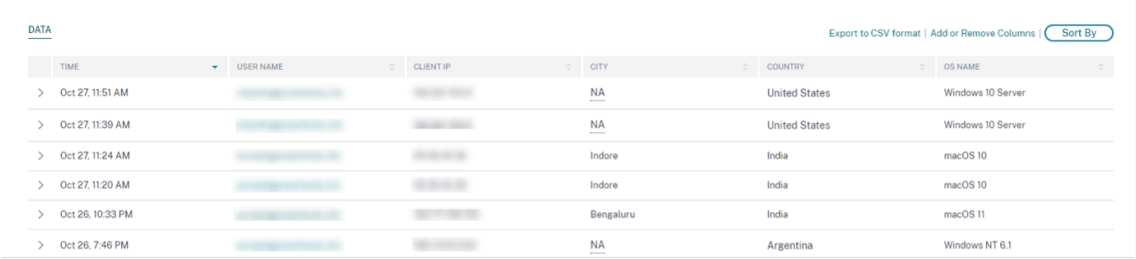



La tabla **DATA** muestra los siguientes detalles de inicio de sesión para las ubicaciones seleccionadas y el período de tiempo:

- **¡Hora**! Fecha y hora en que el usuario inició sesión.
- **Nombre de usuario**. Identidad del usuario.
- **IP del cliente**. Dirección IP del dispositivo del usuario.
- **Tipo de IP de cliente**. El tipo de dirección IP del usuario, como pública o privada.

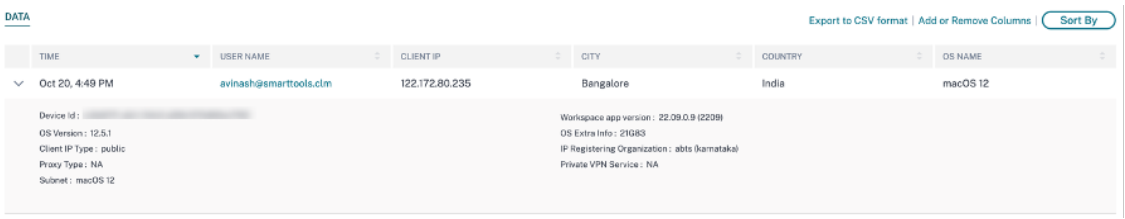
 

- **Ciudad y país**. Las ubicaciones desde las que el usuario inició sesión en aplicaciones virtuales o escritorios virtuales.
- **ID del dispositivo**. El código de identidad del dispositivo de usuario.
- **Nombre del sistema operativo**. El sistema operativo del dispositivo del usuario. Para obtener más información, consulte Búsqueda de autoservicio de aplicaciones y escritorios.




Si amplía cada evento, puede ver los siguientes detalles:

- **Versión del sistema operativo**. La versión del sistema operativo del dispositivo del usuario. Para obtener más información, consulte Búsqueda de autoservicio de aplicaciones y escritorios.
- **Información adicional del sistema operativo**: cualquier información adicional del sistema operativo, como números de compilación, service packs y parches. Para obtener más información, consulte Búsqueda de autoservicio de aplicaciones y escritorios.
- **Versión de la aplicación Workspace**. La versión de compilación de la aplicación Citrix Workspace o Citrix Receiver.




En la tabla **DATA**, puede realizar las siguientes operaciones:

- Haga clic en **Agregar o quitar columnas** para actualizar las columnas de la tabla según cómo quiera ver los datos.
- Haga clic en **Ordenar por** y seleccione los elementos de datos para realizar una clasificación de varias columnas. Para obtener más información, consulte Ordenación de varias columnas.
- Haga clic en **Exportar a formato CSV** para descargar los datos que se muestran en la tabla DATOS en un archivo CSV y utilizarlos para su análisis.

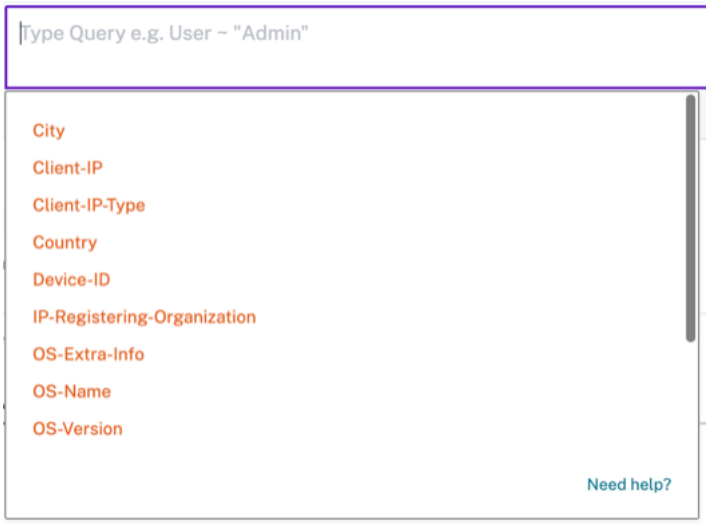
### Barra de búsqueda

También puede utilizar la barra de búsqueda para definir la consulta mediante las dimensiones asociadas a un evento de inicio de sesión.

Por ejemplo:

```
User = “test user” AND Client-IP = “10.xx.xx.xx AND Client-IP-Type = public”
```

```
User = “demo_user@citrix.com” AND OS-Major-Version = “macOS 10.13” AND OS-Minor-Version = 6
```




### Facetas

Puede utilizar las siguientes facetas para los eventos de inicio de sesión:

- **Ubicaciones**: filtre los eventos de inicio de sesión por países y sus ciudades.
- **SO**: filtre los eventos de inicio de sesión por sistema operativo y sus versiones.
- **Subred**: Filtra los eventos de acceso por subredes.
- **Tipo de IP del cliente**: filtre los eventos de acceso por los tipos de IP pública y privada.
- **Organización de registro de IP**: Filtra los eventos de acceso por ISP utilizado por el usuario.
- **Servicio de VPN privada**: Filtra los eventos de acceso por los nombres de las redes VPN privadas.
- **Tipo de proxy**: Filtra los eventos de acceso según las clasificaciones del tipo de proxy, como HTTP, web, Tor y SOCKS.

> **Nota**
>
> También puede ver la etiqueta no disponible si los datos no están disponibles o no están identificados.

## Cronología y perfil de riesgo del usuario

December 7, 2023

> **Nota**
>
> :**Citrix**Content Collaboration y ShareFile han llegado al final de su vida útil y ya no están disponibles para los usuarios.

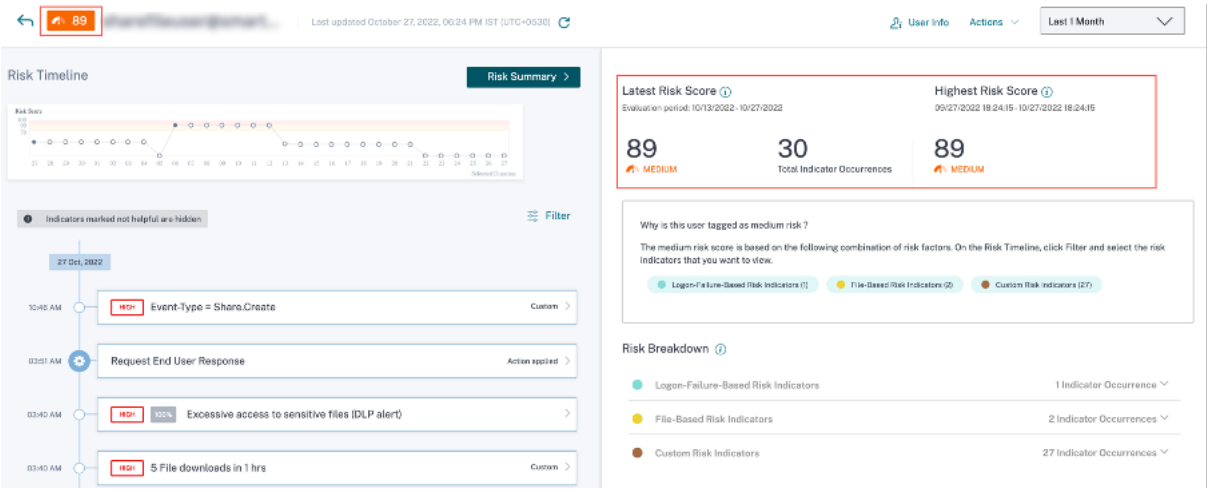
El cronograma de riesgo del usuario en el perfil de un usuario le permite, como administrador de Citrix Analytics, obtener información más detallada sobre el comportamiento de riesgo de un usuario. De forma predeterminada, se muestra el cronograma de riesgo del usuario durante el último mes. También puede ver las acciones correspondientes realizadas en su cuenta durante un período de tiempo seleccionado. Desde el cronograma de riesgos del usuario, puede profundizar en el perfil de un usuario para comprender lo siguiente:

- Uso de aplicaciones
- Uso de datos
- Uso de dispositivos
- Uso de ubicaciones

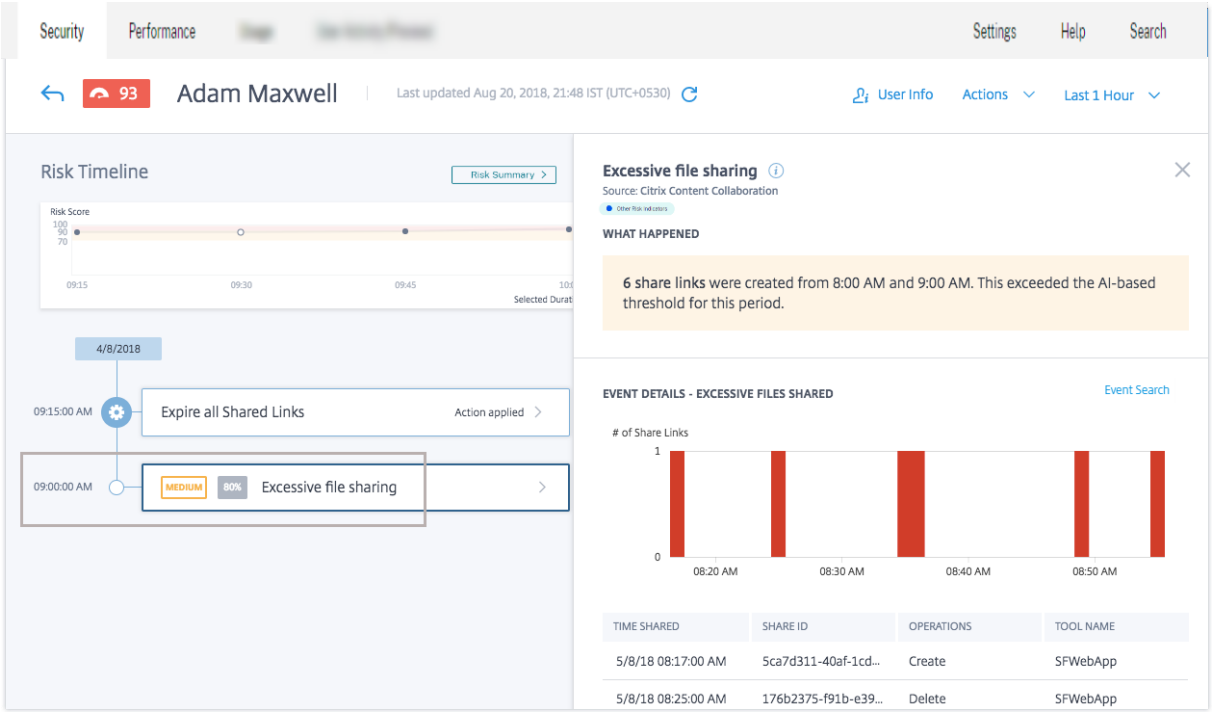
Además, puede ver la puntuación de riesgo y las tendencias de los indicadores de riesgo del usuario y determinar si el usuario es un usuario de alto riesgo o no.

Puede ver la puntuación de riesgo más reciente del usuario en la esquina superior izquierda de la página Cronología de riesgos del usuario. Los informes de la vista de **resumen de riesgos** muestran las puntuaciones máximas más recientes e históricas.




Cuando vas al cronograma de riesgo de un usuario, puede seleccionar un indicador de riesgo o una acción que se haya aplicado a su cuenta. Si elige una de las opciones anteriores, el panel derecho muestra la sección del indicador de riesgo o la sección de acciones.




## Cronología del riesgo

El cronograma de riesgos muestra la siguiente información:

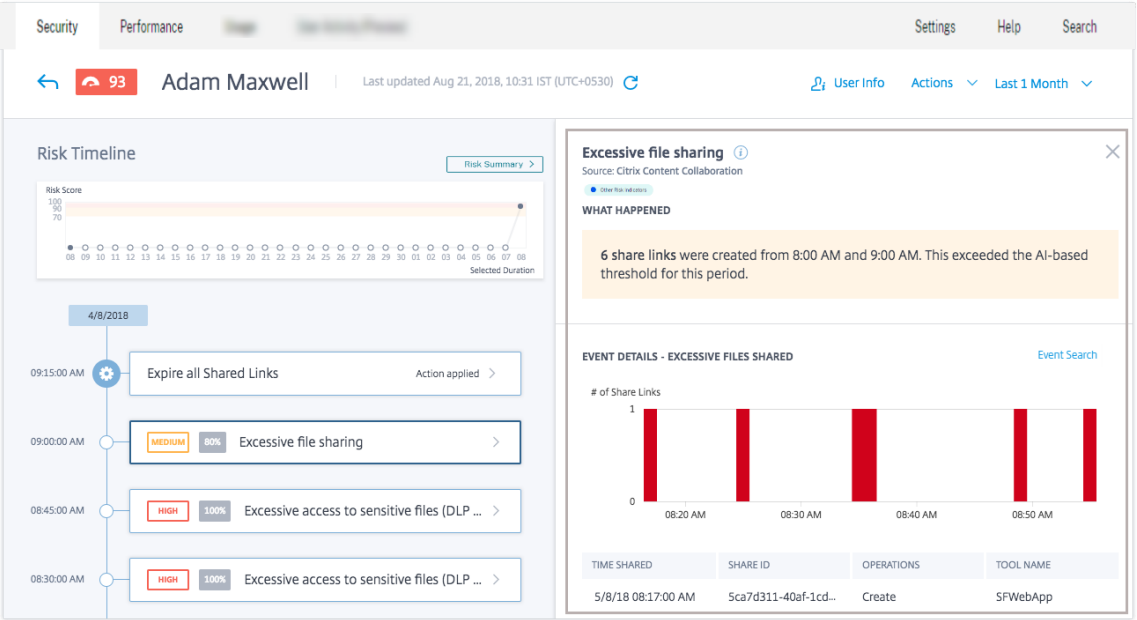
- **Indicadores de riesgo**. Los indicadores de riesgo son actividades de usuario sospechosas o que pueden suponer una amenaza para la seguridad de su organización. Los indicadores se activan cuando el comportamiento del usuario se desvía de su comportamiento normal. Los

indicadores de riesgo pueden ser de estos orígenes de datos:

- Citrix Content Collaboration
- Citrix Gateway
- Citrix Endpoint Management
- Citrix Virtual Apps and Desktops o Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service)
- Citrix Secure Private Access

Al seleccionar un indicador de riesgo en el cronograma del usuario, la sección de información del indicador de riesgo se muestra en el panel derecho. Puede ver el motivo del indicador de riesgo junto con los detalles del evento. Se clasifican a grandes rasgos en las siguientes secciones:




- **Lo que ha pasado**. Puede ver un resumen del indicador de riesgo aquí. Por ejemplo, si ha seleccionado el indicador Riesgo **excesivo de uso compartido de archivos**. En la sección Qué ha pasado, puede ver el número de enlaces compartidos enviados a los destinatarios y cuándo se ha producido el evento de uso compartido.
- **Detalles del evento**. Puede ver las entradas de eventos individuales en formato gráfico y tabular junto con los detalles del evento. Haga clic en **Búsqueda de eventos** para acceder a la página de búsqueda de autoservicio y ver los eventos correspondientes al indicador de riesgo del usuario. Para obtener más información, consulte **Búsqueda de autoservicio**.
- Información**contextual adicional**. Puede ver los datos compartidos, si los hay, durante la ocurrencia de un evento en esta sección.

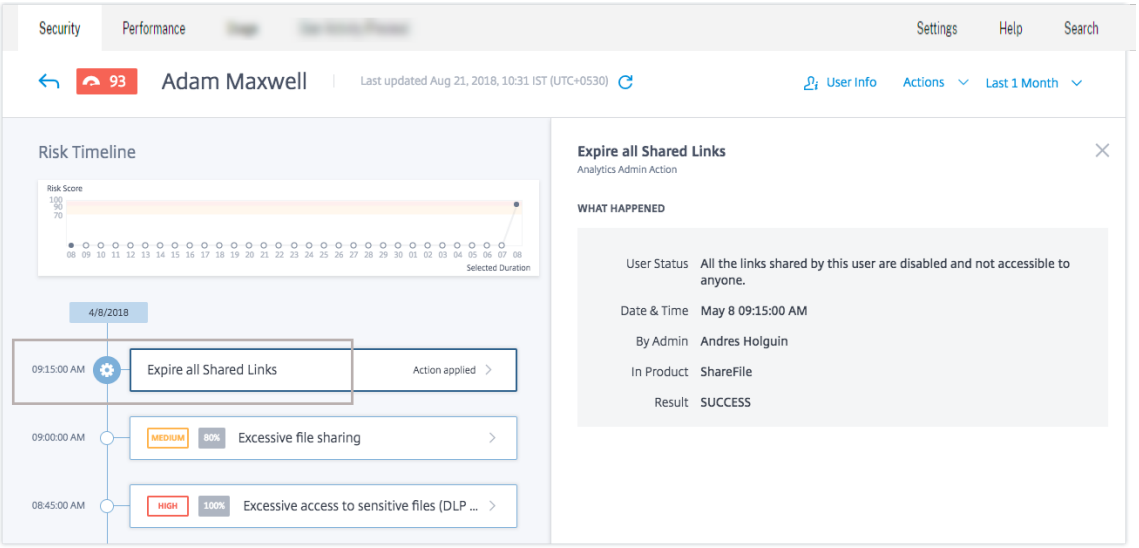
 

Puede marcar manualmente los indicadores de riesgo como útiles o no útiles. Para obtener más información, consulte Proporcionar comentarios sobre los indicadores de riesgo de los usuarios.

Más información: indicadores de riesgo

- **Acciones**. Las acciones ayudan a responder a eventos sospechosos y evitar que se produzcan eventos anómalos en el futuro. Las acciones que se han aplicado al perfil de un usuario se muestran en el cronograma de riesgo. Estas acciones se aplican automáticamente a la cuenta de un usuario mediante directivas configuradas o se puede aplicar una acción específica de forma manual.

  Más información: Directivas y acciones.




- **Eventos de usuario con privilegios**. Los eventos de usuario con privilegios se desencadenan cada vez que se produce un cambio en el estado de privilegio de administrador o ejecutivo de un usuario. Cuando se activa un indicador de riesgo para un usuario, puede correlacionarlo con el evento de cambio de estado de privilegios especificado. Si es necesario, puede aplicar la acción adecuada en el perfil de usuario. Los eventos de privilegios de administrador o ejecutivo que se muestran en el cronograma de riesgo del usuario son los siguientes:

  - Agregado al grupo ejecutivo
  - Eliminado del grupo ejecutivo
  - Privilegio elevado a administrador
  - Privilegio de administrador eliminado

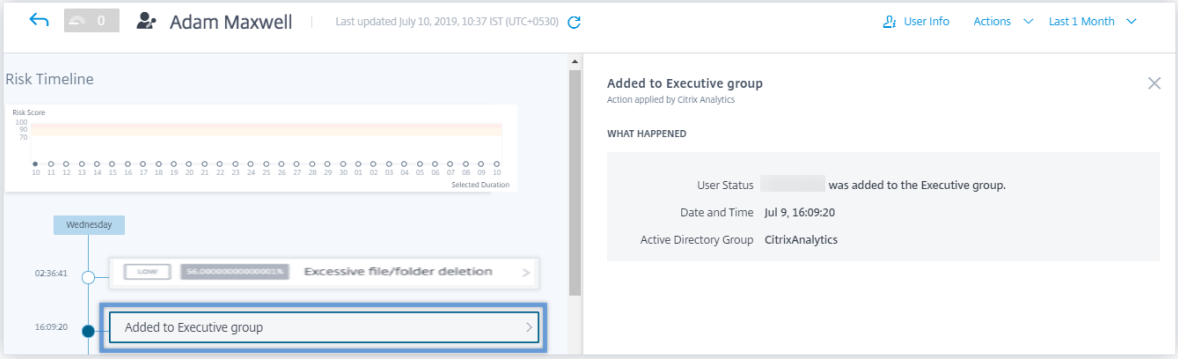
  Piense en el usuario Adam Maxwell que se agregó al grupo privilegiado Executive **CitrixAnalytics**. El evento **Agregado al grupo Ejecutivo** se agrega al cronograma de riesgo del usuario.

Ahora, Adam comienza a eliminar archivos y carpetas en exceso y activa el algoritmo de aprendizaje automático que detecta un comportamiento inusual. El indicador de riesgo de **eliminación excesiva de archivos o carpetas** se agrega al cronograma de riesgo del usuario. Puede comparar el evento y el indicador de riesgo en el cronograma de riesgo. Después de la comparación, puede determinar si el indicador de riesgo se activó como consecuencia del evento. Si es así, puedes aplicar las acciones apropiadas al perfil de Adam. Para obtener más información sobre los usuarios con privilegios, consulte Usuarios con privilegios.

Al seleccionar un evento de la línea de tiempo del usuario, la sección de información del evento se muestra en el panel derecho.

En el caso de un ejecutivo, el panel derecho muestra información como el **estado del usuario**, la **fecha y la hora yel grupo de Active Directory**.

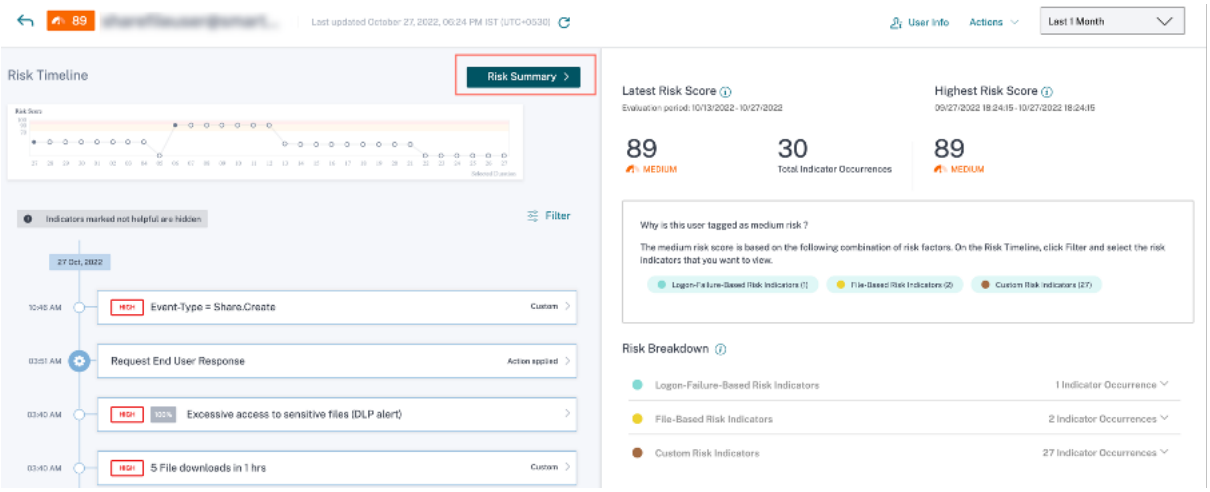



En el caso de un evento de privilegio de administrador, el panel derecho muestra información como **el estado del usuario**, **la fecha y la hora**y **en el producto**.

## Resumen de riesgos

Vea los factores de riesgo asociados al usuario que contribuyeron a su puntuación de riesgo. Puede ver los detalles de la puntuación de riesgo tomados como máximos durante el período de tiempo seleccionado, junto con la puntuación más reciente y el recuento de indicadores de riesgo correspondiente. Al acceder a la cronología del usuario desde la página de destino principal o desde la página de usuarios de riesgo, la selección de hora se conserva de la página de origen. Para obtener más información sobre los factores de riesgo, consulte Indicadores de riesgo de usuario de Citrix.

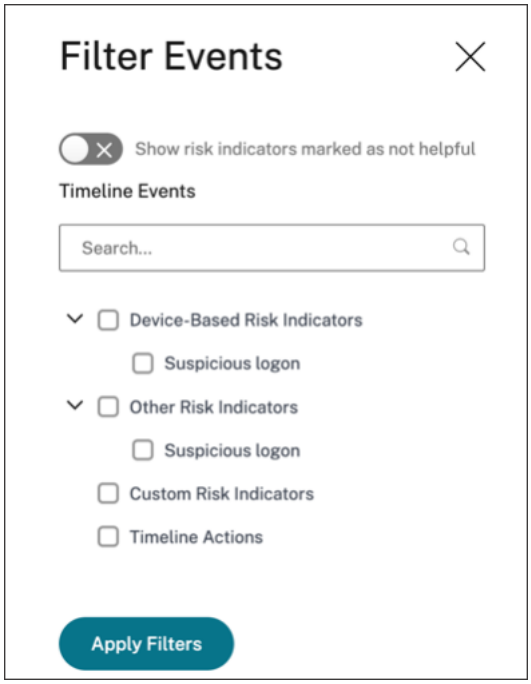



Haga clic en **Resumen de riesgos** para ver la siguiente información:

- **Puntuación de riesgo más**reciente: la puntuación de riesgo más reciente indica el riesgo actual del usuario en función de su comportamiento reciente. La puntuación de riesgo determina el nivel de riesgo que un usuario representa para una organización durante un período de dos semanas. El valor de la puntuación de riesgo es dinámico y varía según el análisis del comportamiento de los usuarios. Según la puntuación, un usuario puede pertenecer a una de las siguientes categorías: usuario de alto riesgo, usuario de riesgo medio, usuario de bajo riesgo y usuario con puntuación de riesgo cero. Para obtener más información sobre las categorías de usuarios, consulte Panel de usuarios.
  - Número**total de incidencias del indicador**: indica el número total de indicadores de riesgo activados por el usuario en las últimas dos semanas. Estos indicadores de riesgo activados determinan la puntuación de riesgo del usuario.
- **Puntuación de riesgo más**alta: la puntuación de riesgo más alta indica el valor máximo de las puntuaciones de riesgo calculadas para este usuario dentro del período de tiempo seleccionado. Es representativo del riesgo agregado para el usuario y puede que no siempre sea igual a la puntuación de riesgo más reciente.
- **Factores de riesgo**: indica una o más combinaciones de los factores de riesgo asociados con las actividades del usuario que contribuyeron a la puntuación de riesgo.
- **Desglose del riesgo**: indica el número de indicadores de riesgo activados por el usuario para cada factor de riesgo. Amplíe la fila para ver los detalles.

En la línea de tiempo del usuario, haga clic en **Filtrar** y seleccione los factores de riesgo, las acciones aplicadas o el estado de usuario privilegiado asociado al usuario y vea los eventos correspondientes.




### Perfil de usuario

La página **de perfil de usuario** muestra la siguiente información de usuario que proviene del directorio activo del usuario:

- Título del puesto
- Dirección
- Correo electrónico
- Teléfono
- Ubicación
- Organización


## Indicadores de riesgo de usuario de Citrix

April 12, 2024

> **Nota**
>
> **Atención**: Citrix Content Collaboration y ShareFile han llegado al final de su ciclo de vida y ya no están disponibles para los usuarios.

Los indicadores de riesgo del usuario son actividades de usuario que parecen sospechosas o que pueden suponer una amenaza para la seguridad de su organización. Estos indicadores de riesgo abarcan todos los productos Citrix utilizados en su implementación. Los indicadores de riesgo se activan cuando el comportamiento del usuario se desvía de lo normal. Cada indicador de riesgo puede tener uno o más factores de riesgo asociados. Estos factores de riesgo ayudan a determinar el tipo de anomalías en los eventos de usuario. Los indicadores de riesgo y sus factores de riesgo asociados determinan la puntuación de riesgo de un usuario.

Los factores de riesgo asociados a los indicadores de riesgo son los siguientes:

- **Indicadores de riesgo basados en dispositivos**: se activa cuando un usuario inicia sesión desde un dispositivo que se considera inusual según el historial del dispositivo del usuario.
- **Indicadores de riesgo basados en la ubicación**: se activa cuando un usuario inicia sesión desde una dirección IP asociada a una ubicación que se considera inusual según el historial de ubicaciones del usuario.
- **Indicadores de riesgo basados en IP**: se activa cuando un usuario intenta acceder a recursos desde una dirección IP que se ha identificado como sospechosa, independientemente de si la dirección IP es inusual para el usuario.
- **Indicadores de riesgo basados en errores de inicio de sesión**: se activa cuando un usuario presenta un patrón de errores de inicio de sesión excesivos o inusuales.
- **Indicadores de riesgo basados en datos**: se activa cuando un usuario intenta exfiltrar datos de una sesión de Workspace. Los comportamientos de los usuarios bajo observación incluyen eventos de copia o pegado, patrones de descarga, etc.
- **Indicadores de riesgo basados en archivos**: se activa cuando el comportamiento de un usuario con respecto al acceso a archivos en Content Collaboration se considera inusual en función de su patrón de acceso histórico. Los comportamientos de los usuarios bajo observación incluyen patrones de descarga, acceso a contenido confidencial, actividades indicativas de ransomware, etc.
- **Indicadores de riesgo personalizados**: se activa cuando se cumple una condición preconfigurada o una condición definida por el usuario. Para obtener información, consulte estos artículos:
  - Indicadores de riesgo personalizados
  - Directivas e indicadores de riesgo personalizados preconfigurados

- Otros indicadores de riesgo: los indicadores de riesgo que no pertenecen a ninguno de los factores de riesgo predefinidos, como los basados en dispositivos, basados en ubicación y fallos de inicio de sesión.

Los indicadores de riesgo también se agrupan en categorías de riesgo en función de los riesgos que son similares. Para obtener más información, consulte Categorías de riesgo.

En la tabla siguiente se muestra la correlación entre los indicadores de riesgo, los factores de riesgo y las categorías de riesgo.

| Productos | Indicador de riesgo del usuario | Factor de riesgo | Categoría de riesgo |
|---|---|---|---|
| Citrix Endpoint Management | Dispositivo con aplicaciones en la lista de bloqueados detectado | Otros indicadores de riesgo | Dispositivos de punto final comprometidos |
| | Se ha detectado un dispositivo con jailbreak o rooteado | Otros indicadores de riesgo | Dispositivos de punto final comprometidos |
| | Dispositivo no administrado detectado | Otros indicadores de riesgo | Dispositivos de punto final comprometidos |
| Citrix Gateway | Fallo en la exploración del análisis de punto final (EPA) | Otros indicadores de riesgo | Usuarios comprometidos |
| | Fallos de autenticación excesivos | Indicadores de riesgo basados en fallos de inicio de sesión | Usuarios comprometidos |
| | Trayectos imposibles | Indicadores de riesgo basados en la ubicación | Usuarios comprometidos |
| | Inicio de sesión desde IP sospechosa | Indicadores de riesgo basados en IP | Usuarios comprometidos |

| Productos | Indicador de riesgo del usuario | Factor de riesgo | Categoría de riesgo |
|---|---|---|---|
| | Inicio de sesión sospechoso | Indicadores de riesgo basados en dispositivos, indicadores de riesgo basados en IP, indicadores de riesgo basados en la ubicación y otros indicadores de riesgo | Usuarios comprometidos |
| | Error de autenticación inusual | Indicadores de riesgo basados en fallos de inicio de sesión | Usuarios comprometidos |
| Citrix Secure Private Access | Intento de acceder a URL de la lista de bloqueados | Otros indicadores de riesgo | Amenazas internas |
| | Descarga excesiva de datos | Otros indicadores de riesgo | Amenazas internas |
| | Acceso a sitios web con riesgos | Otros indicadores de riesgo | Amenazas internas |
| | Volumen de subida | Otros indicadores de riesgo | Amenazas internas |
| Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) y Citrix Virtual Apps and Desktops locales | Trayectos imposibles | Indicadores de riesgo basados en la ubicación | Usuarios comprometidos |
| | Exfiltración potencial de datos | Indicadores de riesgo basados en datos | Exfiltración de datos |

| Productos | Indicador de riesgo del usuario | Factor de riesgo | Categoría de riesgo |
|---|---|---|---|
| | Inicio de sesión sospechoso | Indicadores de riesgo basados en dispositivos, indicadores de riesgo basados en IP, indicadores de riesgo basados en la ubicación y otros indicadores de riesgo | Usuarios comprometidos |

Puede marcar manualmente los indicadores de riesgo como útiles o no útiles. Para obtener más información, consulte Proporcionar comentarios sobre los indicadores de riesgo de los usuarios.

## Indicadores de riesgo de Citrix Endpoint Management

May 9, 2022

### Dispositivo con aplicaciones en la lista de bloqueados detectado

Citrix Analytics detecta las amenazas de acceso en función de la actividad de un dispositivo con aplicaciones incluidas en la lista de bloqueados y activa el indicador de riesgo correspondiente.

El indicador de riesgo de **dispositivo con aplicaciones en lista de bloqueados detectadas** se activa cuando el servicio Endpoint Management detecta una aplicación en lista de bloqueados durante el inventario de software. La alerta garantiza que solo las aplicaciones autorizadas se ejecuten en los dispositivos que se encuentran en la red de su organización.

El factor de riesgo asociado con el indicador de riesgo detectado del dispositivo con aplicaciones incluidas en la lista de bloqueados es el indicador Otros indicadores de riesgo. Para obtener más información sobre los factores de riesgo, consulte Indicadores de riesgo de usuario de Citrix.

#### ¿Cuándo se activa el indicador de riesgo del dispositivo con aplicaciones en la lista de bloqueados?

El indicador de riesgo **detectado del dispositivo con aplicaciones incluidas en** la lista de bloqueados se informa cuando se detectan aplicaciones incluidas en la lista de bloqueados en el dispositivo

de un usuario. Cuando el servicio Endpoint Management detecta una o más aplicaciones incluidas en la lista de bloqueados en un dispositivo durante el inventario de software, se envía un evento a Citrix Analytics.

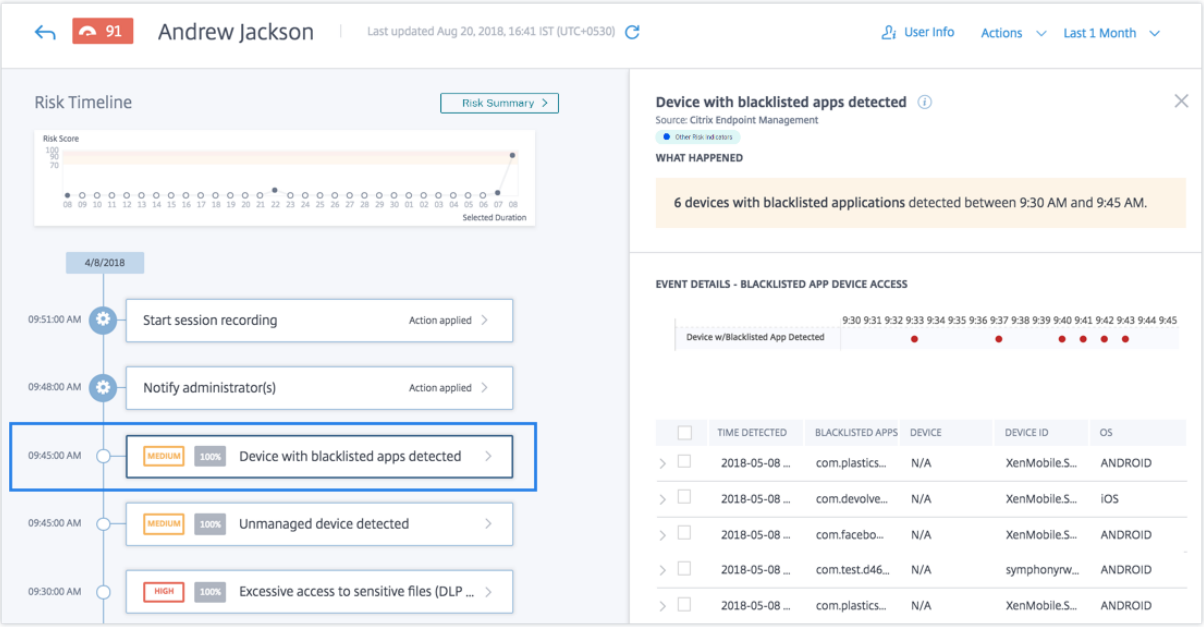
Citrix Analytics supervisa estos eventos y actualiza la puntuación de riesgo del usuario. Además, agrega una entrada del indicador de riesgo **detectado por un dispositivo con aplicaciones incluidas en la lista de bloqueados** a la línea de tiempo de riesgo del usuario.

### ¿Cómo analizar el indicador de riesgo Dispositivo con aplicaciones en la lista de bloqueados detectadas?

Piense en el usuario Andrew Jackson, que utilizó un dispositivo que tenía aplicaciones en la lista de bloqueados instaladas recientemente. Endpoint Management notifica esta condición a Citrix Analytics, que asigna una puntuación de riesgo actualizada a Andrew Jackson.

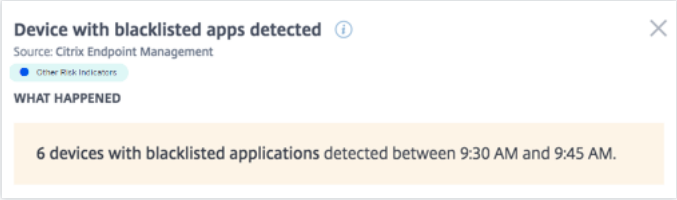
En la cronología de riesgo de Andrew Jackson, puede seleccionar el indicador de riesgo **detectado Dispositivo con aplicaciones incluidas en la lista de bloqueados** . El motivo del evento se muestra junto con detalles como la lista de aplicaciones en la lista de bloqueados, la hora en que Endpoint Management detectó la aplicación en la lista de bloqueados, etc.

Para ver el indicador de riesgo **detectado del dispositivo con aplicaciones incluidas en la lista de bloqueados** para un usuario, vaya a **Seguridad > Usuarios**y seleccione el usuario.

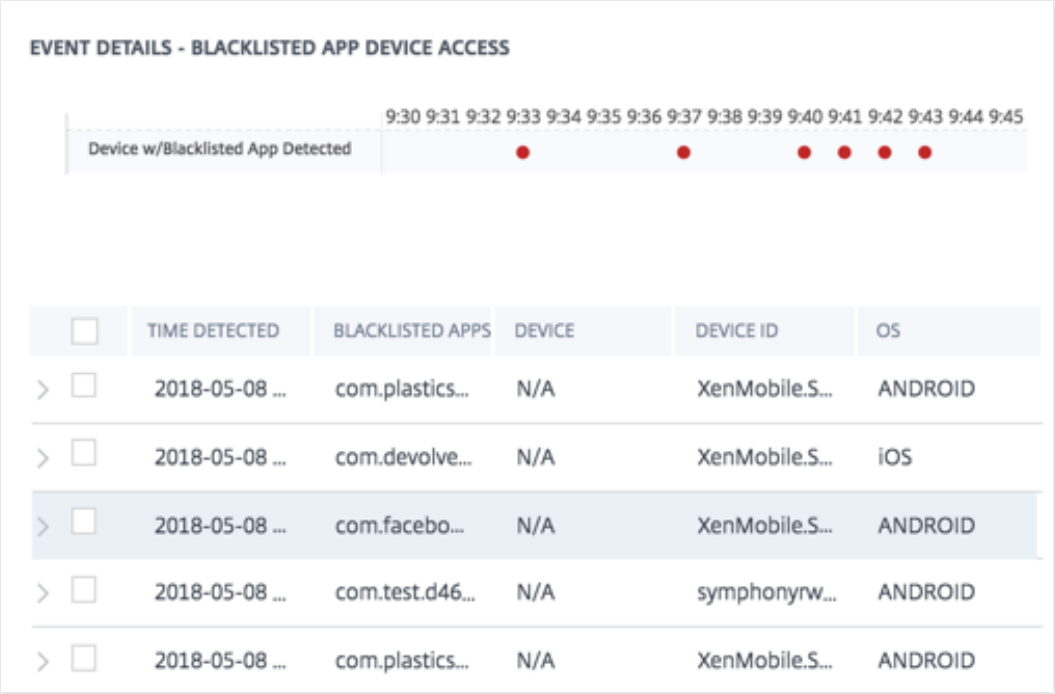



- En la sección **QUÉ PASÓ**, puede ver el resumen del evento. Puede ver el número de dispositivos con aplicaciones incluidas en la lista de bloqueados detectados por el servicio de Endpoint Management y la hora en que se produjeron los eventos.




- En la sección **DETALLES DEL EVENTO: ACCESO A DISPOSITIVOS DE APLICACIONES EN LA LISTA DE BLOQUEADOS**, los eventos se muestran en formato gráfico y tabular. Los eventos también se muestran como entradas individuales en el gráfico y la tabla proporciona la siguiente información clave:
  - **Tiempo detectado**: cuando Endpoint Management informa de la presencia de aplicaciones incluidas en la lista de bloqueados.
  - **Aplicaciones incluidas en**la lista de bloqueados: las aplicaciones incluidas en la lista de bloqueados del dispositivo.
  - **Dispositivo**: el dispositivo móvil utilizado.
  - **ID de dispositivo**: información sobre el ID del dispositivo que se utiliza para iniciar sesión en la sesión.
  - **SO**: el sistema operativo del dispositivo móvil.




> **Nota**
>
> Además de ver los detalles en formato tabular, puede hacer clic en la flecha situada junto a la

> instancia de una alerta para ver más detalles.

#### ¿Qué acciones puede aplicar al usuario?

Puede realizar las siguientes acciones en la cuenta del usuario:

- **Agregar a la lista de seguimiento**. Cuando quiera supervisar a un usuario en busca de futuras amenazas potenciales, puede agregarlas a una lista de seguimiento.
- **Notificar a los administradores**. Cuando hay alguna actividad inusual o sospechosa en la cuenta del usuario, se envía una notificación por correo electrónico a todos los administradores o a los seleccionados.

Para obtener más información sobre las acciones y cómo configurarlas manualmente, consulte Directivas y acciones.

Para aplicar las acciones al usuario manualmente, desplácese hasta el perfil del usuario y seleccione el indicador de riesgo adecuado. En el menú **Acciones**, seleccione una acción y haga clic en **Aplicar**.

> **Nota**
>
> Independientemente del origen de datos que desencadena un indicador de riesgo, se pueden aplicar acciones relacionadas con otros orígenes de datos.

### Se ha detectado un dispositivo con jailbreak o rooteado

Citrix Analytics detecta las amenazas de acceso en función de la actividad de los dispositivos liberados por jailbreak o rooteados y activa el indicador de riesgo correspondiente.

El indicador de riesgo de **dispositivos con jailbreak o rooteado** se activa cuando un usuario utiliza un dispositivo con jailbreak o rooteado para conectarse a la red. Secure Hub detecta el dispositivo e informa del incidente al servicio Endpoint Management. La alerta garantiza que solo los usuarios y dispositivos autorizados estén en la red de su organización.

El factor de riesgo asociado con el indicador de riesgo de Jailbreak o dispositivo rooteado es el Otros indicadores de riesgo. Para obtener más información sobre los factores de riesgo, consulte Indicadores de riesgo de usuario de Citrix.

#### ¿Cuándo se activa el indicador de riesgo Dispositivo liberado por jailbreak o root detectado?

Es importante que los responsables de seguridad puedan garantizar que los usuarios se conecten mediante dispositivos compatibles con la red. El indicador de riesgo **detectado por Jailbreak o dispositivo rooteado** le avisa de los usuarios con dispositivos iOS que tienen jailbreak o dispositivos Android que están rooteados.

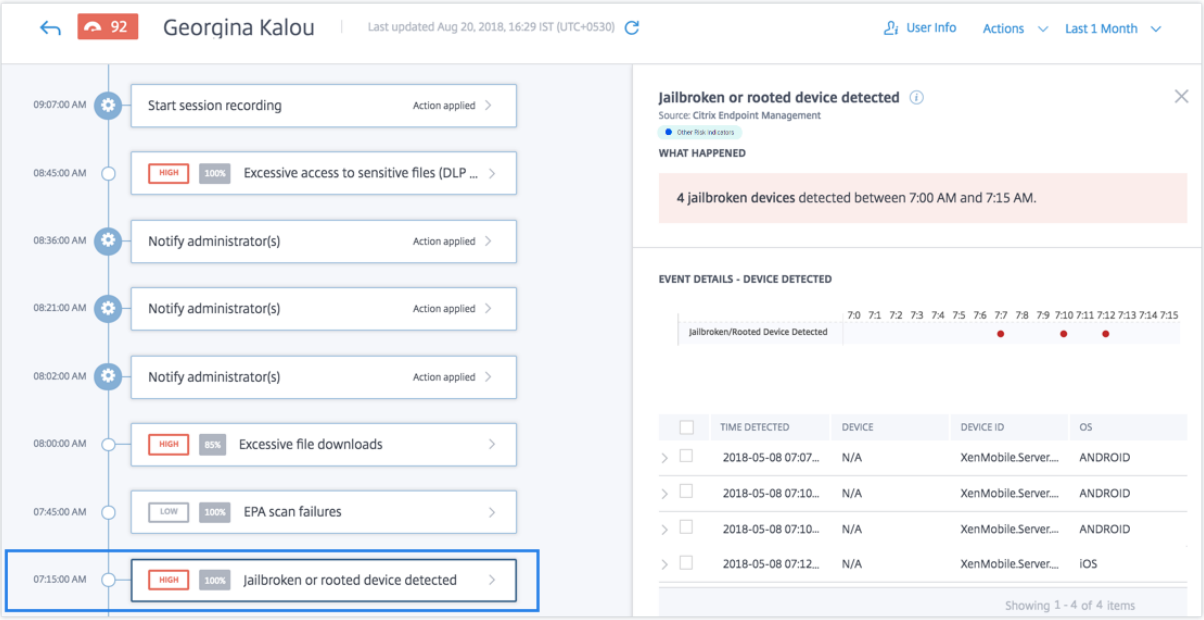
El indicador de riesgo de **dispositivo con jailbreak o rooteado** se activa cuando un dispositivo inscrito se hace jailbreak o rooteado. Secure Hub detecta el evento en el dispositivo y lo informa al servicio Endpoint Management.

### ¿Cómo analizar el indicador de riesgo detectado por jailbreak o dispositivo rooteado?

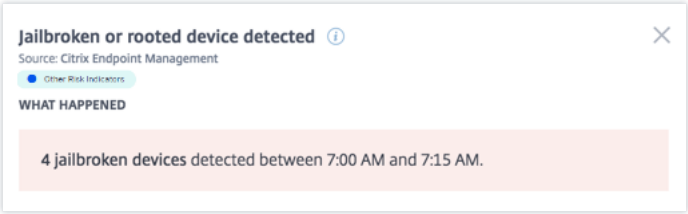
Piense en la usuaria Georgina Kalou, cuyo dispositivo iOS inscrito recientemente fue liberado por jailbreak. Citrix Analytics detecta este comportamiento sospechoso y se asigna una puntuación de riesgo a Georgina Kalou.

En la cronología de riesgos de Georgina Kalou, puede seleccionar el indicador de riesgo **detectado por Jailbreak o dispositivo rooteado** reportado. El motivo del evento se muestra junto con detalles como la hora en que se activó el indicador de riesgo, la descripción del evento, etc.

Para ver el indicador de riesgo **detectado por Jailbreak o dispositivo rooteado** de un usuario, vaya a **Seguridad > Usuarios**y seleccione el usuario.




- En la sección **QUÉ PASÓ**, puede ver el resumen del evento. Puede ver el número de dispositivos con jailbreak o rooteados detectados y la hora en que se produjeron los eventos.

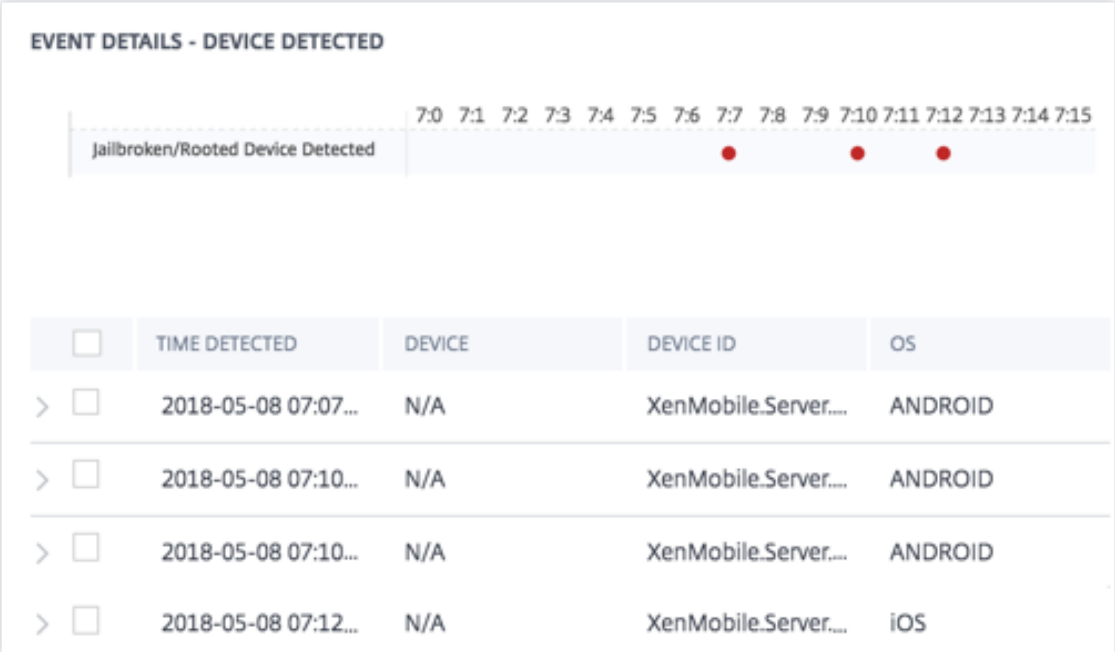



- En la sección **DETALLES DEL EVENTO: DISPOSITIVO DETECTADO**, los eventos se muestran en

formato gráfico y tabular. Los eventos también se muestran como entradas individuales en el gráfico y la tabla proporciona la siguiente información clave:

- **Tiempo detectado**. Hora en que se detecta el dispositivo con jailbreak o rooteado.
- **dispositivo**. El dispositivo móvil utilizado.
- **ID del dispositivo**. Información sobre el ID del dispositivo que se utiliza para iniciar sesión en la sesión.
- **SO**. El sistema operativo del dispositivo móvil.




> **Nota**
>
> Además de ver los detalles en formato tabular, haga clic en la flecha situada junto a la instancia de una alerta para ver más detalles.

#### ¿Qué acciones puede aplicar al usuario?

Puede realizar las siguientes acciones en la cuenta del usuario:

- **Agregar a la lista de seguimiento**. Cuando quiera supervisar a un usuario en busca de futuras amenazas potenciales, puede agregarlas a una lista de seguimiento.
- **Notificar a los administradores**. Cuando hay alguna actividad inusual o sospechosa en la cuenta del usuario, se envía una notificación por correo electrónico a todos los administradores o a los seleccionados.

Para obtener más información sobre las acciones y cómo configurarlas manualmente, consulte Directivas y acciones.

Para aplicar las acciones al usuario manualmente, desplácese hasta el perfil del usuario y seleccione el indicador de riesgo adecuado. En el menú **Acciones**, seleccione una acción y haga clic en **Aplicar**.

> **Nota**
>
> Independientemente del origen de datos que desencadena un indicador de riesgo, se pueden aplicar acciones relacionadas con otros orígenes de datos.

## Dispositivo no administrado detectado

Citrix Analytics detecta las amenazas de acceso en función de la actividad de los dispositivos no administrados y activa el indicador de riesgo correspondiente.

El indicador de riesgo **detectado por dispositivo no administrado** se activa cuando un dispositivo:

- Se borró de forma remota gracias a una acción automatizada.
- Limpiado manualmente por el administrador.
- El usuario ha anular la inscripción.

El factor de riesgo asociado con el indicador de riesgo detectado por dispositivos no administrados es el Otros indicadores de riesgo. Para obtener más información sobre los factores de riesgo, consulte Indicadores de riesgo de usuario de Citrix.

### ¿Cuándo se activa el indicador de riesgo detectado del dispositivo no administrado?

El indicador de riesgo **detectado por dispositivo no administrado** se informa cuando el dispositivo de un usuario se ha quedado sin administrar. Un dispositivo cambia a un estado no administrado debido a:

- Acción realizada por el usuario.
- Acción realizada por el administrador de Endpoint Management o el servidor.

En su organización, con el servicio Endpoint Management, puede administrar los dispositivos y las aplicaciones que acceden a la red. Para obtener más información, consulte Modos de administración.

Cuando el dispositivo de un usuario cambia a un estado no administrado, el servicio Endpoint Management detecta este evento y lo informa a Citrix Analytics. Se actualiza la puntuación de riesgo del usuario. El indicador de riesgo **detectado por dispositivo no administrado** se agrega al cronograma de riesgo del usuario.

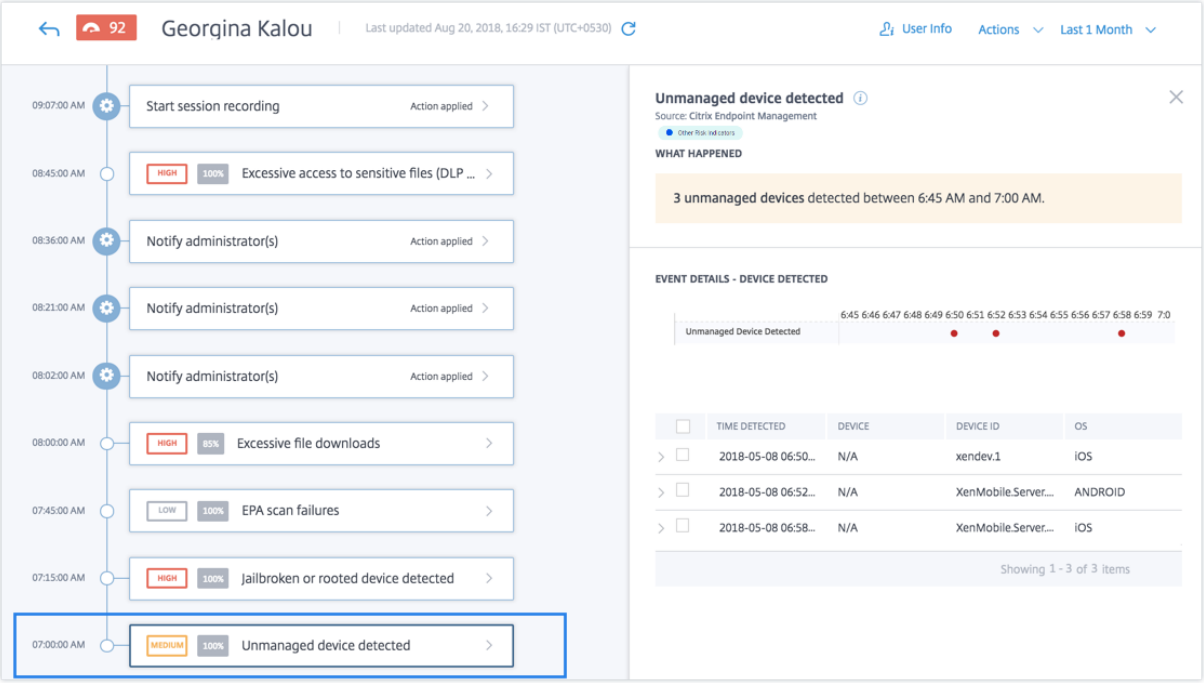
 

### ¿Cómo analizar el indicador de riesgo detectado del dispositivo no administrado?

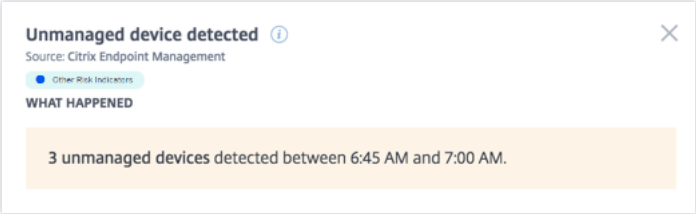
Pensemos en la usuaria Georgina Kalou, cuyo dispositivo se borrado de forma remota mediante una acción automatizada en el servidor. Endpoint Management notifica este evento a Citrix Analytics, que asigna una puntuación de riesgo actualizada a Georgina Kalou.

En la cronología de riesgos de Georgina Kalou, puede seleccionar el indicador de riesgo detectado por dispositivo no administrado notificado. El motivo del evento se muestra junto con detalles como, hora en que se activó el indicador de riesgo, descripción del evento, etc.

Para ver el indicador de riesgo **detectado por dispositivo no administrado** de un usuario, vaya a **Seguridad > Usuarios**y seleccione el usuario.



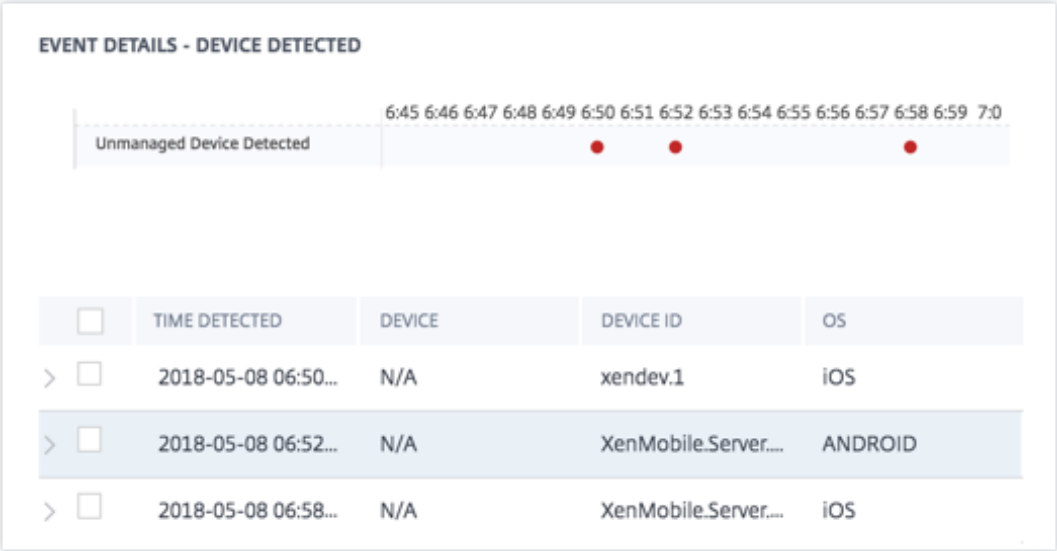

- En la sección **QUÉ PASÓ**, puede ver un resumen del evento. Puede ver el número de dispositivos no administrados detectados y la hora en que se produjeron los eventos.




- En la sección **DETALLES DEL EVENTO: DISPOSITIVO DETECTADO**, los eventos se muestran en formato gráfico y tabular. Los eventos también se muestran como entradas individuales en el gráfico y la tabla proporciona la siguiente información clave:

- **Tiempo detectado**. Hora en que se detectó el evento.
- **dispositivo**. El dispositivo móvil utilizado.
- **ID del dispositivo**. ID de dispositivo del dispositivo móvil.
- **SO**. El sistema operativo del dispositivo móvil.




### ¿Qué acciones puede aplicar al usuario?

Puede realizar las siguientes acciones en la cuenta del usuario:

- **Agregar a la lista de seguimiento**. Cuando quiera supervisar a un usuario en busca de futuras amenazas potenciales, puede agregarlas a una lista de seguimiento.
- **Notificar a los administradores**. Cuando hay alguna actividad inusual o sospechosa en la cuenta del usuario, se envía una notificación por correo electrónico a todos los administradores o a los seleccionados.

Para obtener más información sobre las acciones y cómo configurarlas manualmente, consulte Directivas y acciones.

Para aplicar las acciones al usuario manualmente, desplácese hasta el perfil del usuario y seleccione el indicador de riesgo adecuado. En el menú **Acciones**, seleccione una acción y haga clic en **Aplicar**.

> **Nota**
>
> Independientemente del origen de datos que desencadena un indicador de riesgo, se pueden aplicar acciones relacionadas con otros orígenes de datos.

# Indicadores de riesgo Citrix Gateway

July 12, 2022

## Errores en el análisis de punto final (EPA)

Citrix Analytics detecta las amenazas basadas en el acceso de los usuarios en función de la actividad de errores de exploración de la EPA y activa el indicador de riesgo correspondiente.

El factor de riesgo asociado con el indicador de riesgo de fallo de la exploración de End Point Analysis es Otros indicadores de riesgo. Para obtener más información sobre los factores de riesgo, consulte Indicadores de riesgo de usuario de Citrix.

### ¿Cuándo se activa el indicador de riesgo de fallos de exploración de la EPA?

El indicador de riesgo de error de exploración de la EPA se informa cuando un usuario intenta acceder a la red mediante un dispositivo que ha fallado en las directivas de exploración de End Point Analysis (EPA) de Citrix Gateway para la autenticación previa o posterior a la autenticación.

Citrix Gateway detecta estos eventos y los informa a Citrix Analytics. Citrix Analytics supervisa todos estos eventos para detectar si el usuario ha tenido demasiados errores de exploración EPA. Cuando Citrix Analytics determina errores excesivos en la exploración de la EPA para un usuario, actualiza la puntuación de riesgo del usuario y agrega una entrada del indicador de riesgo de fallo de la exploración de la EPA al cronograma de riesgo del usuario.

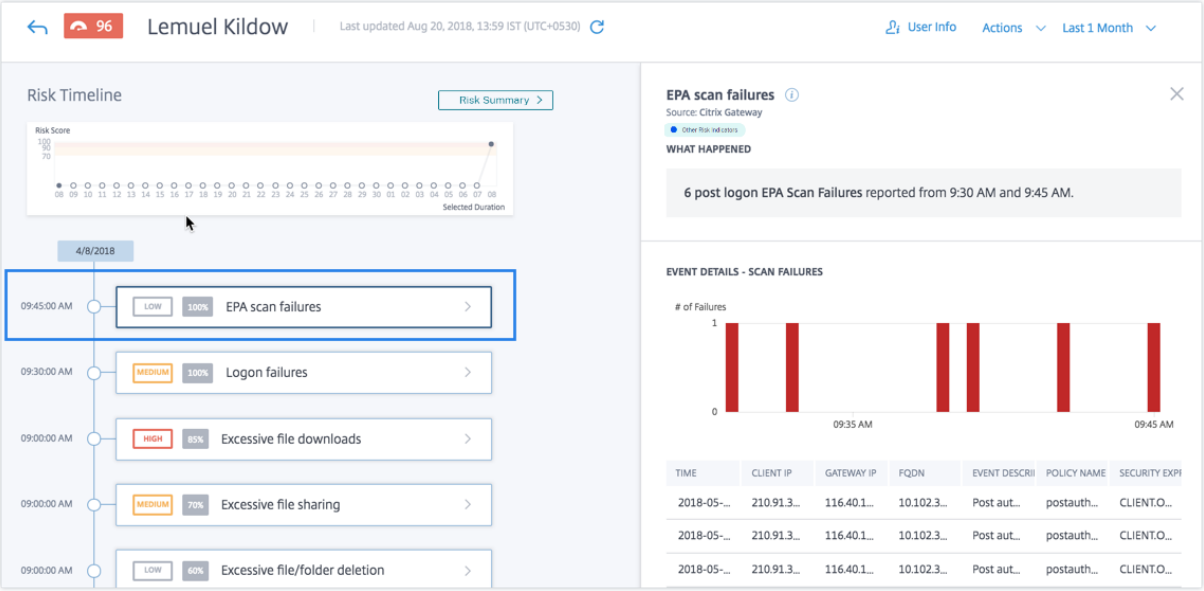
### ¿Cómo analizar el indicador de riesgo de fallas de escaneo EPA?

Piense en el usuario Lemuel, que recientemente intentó acceder a la red varias veces con un dispositivo que no ha superado el análisis EPA de Citrix Gateway. Citrix Gateway informa de este error a Citrix Analytics, que asigna una puntuación de riesgo actualizada a Lemuel. El indicador de riesgo de fallo del escaneo de la EPA se agrega al cronograma de riesgo de Lemuel Kildow.

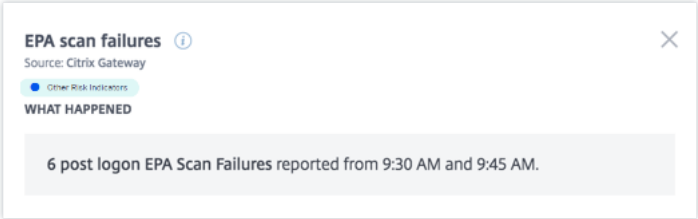
Para ver la entrada de **error de escaneo de la EPA** para un usuario, vaya a **Seguridad > Usuarios**y seleccione el usuario.

En el cronograma de riesgos de Lemuel Kildow, puede seleccionar el último indicador de riesgo de **fallos de escaneo de la EPA** notificado para el usuario. Cuando selecciona una entrada del indicador de riesgo de fallo de escaneo EPA en la línea de tiempo, aparece un panel de información detallado correspondiente en el panel derecho.

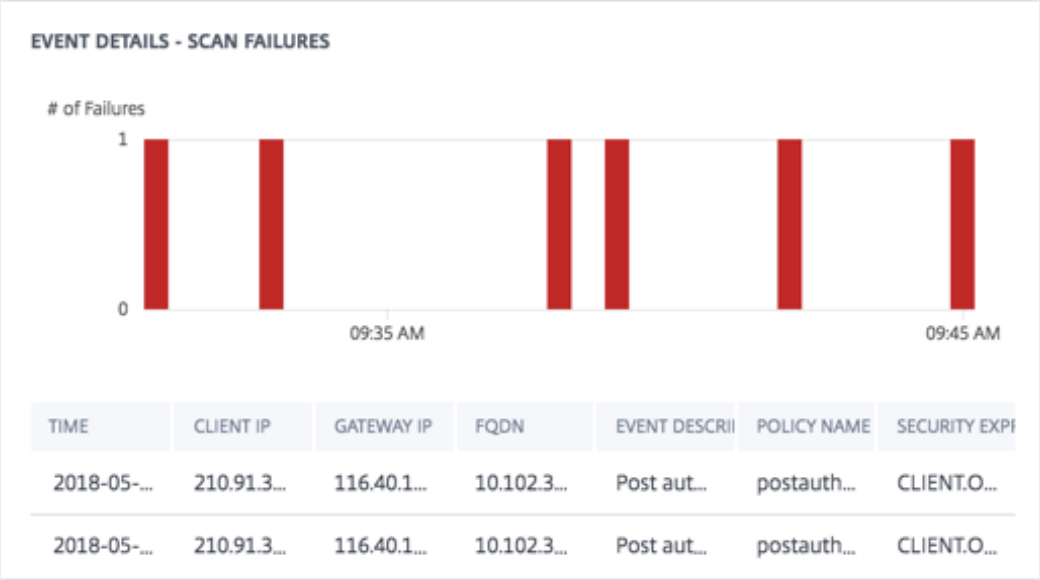



- La sección **QUÉ SUCEDIÓ** proporciona un breve resumen del indicador de riesgo de fallo de la exploración de la EPA. Además, incluye el número de errores de exploración de la EPA posteriores al inicio de sesión notificados durante el período seleccionado.




- La sección **DETALLES DEL EVENTO: FALLOS DE EXPLORACIÓN** incluye una visualización de la línea de tiempo de los eventos individuales de error de exploración de la EPA que se produjeron durante el período de tiempo seleccionado. Además, incluye una tabla que proporciona la siguiente información clave sobre cada evento:
  - **Tiempo**. Hora en que se produjo el error del escaneo de la EPA.
  - **IP del cliente**. Dirección IP del cliente que provoca el error de exploración de la EPA.
  - **IP de puerta de enlace**. Dirección IP de Citrix Gateway que ha notificado el error del análisis de la EPA.
  - **FQDN**. El FQDN de Citrix Gateway.
  - **Descripción del evento**. Breve descripción del motivo del fallo del escaneo de la EPA.
  - **Nombre de la directiva**. El nombre de la directiva de análisis EPA configurado en Citrix Gateway.
  - **Expresión de seguridad**. Expresión de seguridad configurada en Citrix Gateway.




**¿Qué acciones puede aplicar al usuario?**

Puede realizar las siguientes acciones en la cuenta del usuario:

- **Agregar a la lista de seguimiento**. Cuando quiera supervisar a un usuario en busca de futuras amenazas potenciales, puede agregarlas a una lista de seguimiento.
- **Notificar a los administradores**. Cuando hay alguna actividad inusual o sospechosa en la cuenta del usuario, se envía una notificación por correo electrónico a todos los administradores o a los seleccionados.
- **Cierre la sesión del usuario**. Cuando un usuario cierra la sesión de su cuenta, no puede acceder a ningún recurso a través de Citrix Gateway hasta que el administrador de Citrix Gateway borre la acción Cerrar sesión del usuario.
- **Bloquear usuario**: cuando la cuenta de un usuario se bloquea debido a un comportamiento anómalo, no puede acceder a ningún recurso a través de Citrix Gateway hasta que el administrador de Gateway desbloquee la cuenta.

Para obtener más información sobre las acciones y cómo configurarlas manualmente, consulte Directivas y acciones.

Para aplicar las acciones al usuario manualmente, desplácese hasta el perfil del usuario y seleccione el indicador de riesgo adecuado. En el menú **Acciones**, seleccione una acción y haga clic en **Aplicar**.

> **Nota**
>
> Independientemente del origen de datos que desencadena un indicador de riesgo, se pueden

> aplicar acciones relacionadas con otros orígenes de datos.

## Fallos de autenticación excesivos

Citrix Analytics detecta las amenazas basadas en el acceso de los usuarios en función de errores excesivos de autenticación y activa el indicador de riesgo correspondiente.

El factor de riesgo asociado con el indicador de riesgo de fallos de autenticación excesivos son los indicadores de riesgo basados en fallos de inicio de sesión. Para obtener más información sobre los factores de riesgo, consulte Indicadores de riesgo de usuario de Citrix.

### ¿Cuándo se activa el indicador de riesgo de fallos de autenticación excesivos?

El indicador de riesgo de errores de inicio de sesión se informa cuando el usuario encuentre varios errores de autenticación de Citrix Gateway en un período determinado. Los errores de autenticación de Citrix Gateway pueden ser errores de autenticación primaria, secundaria o terciaria, en función de si la autenticación multifactor está configurada para el usuario.

Citrix Gateway detecta todos los errores de autenticación de usuarios e informa de estos sucesos a Citrix Analytics. Citrix Analytics supervisa todos estos eventos para detectar si el usuario ha tenido demasiados errores de autenticación. Cuando Citrix Analytics determina errores de autenticación excesivos, actualiza la puntuación de riesgo del usuario. El indicador de riesgo de fallos de autenticación excesivos se agrega al cronograma de riesgo del usuario.

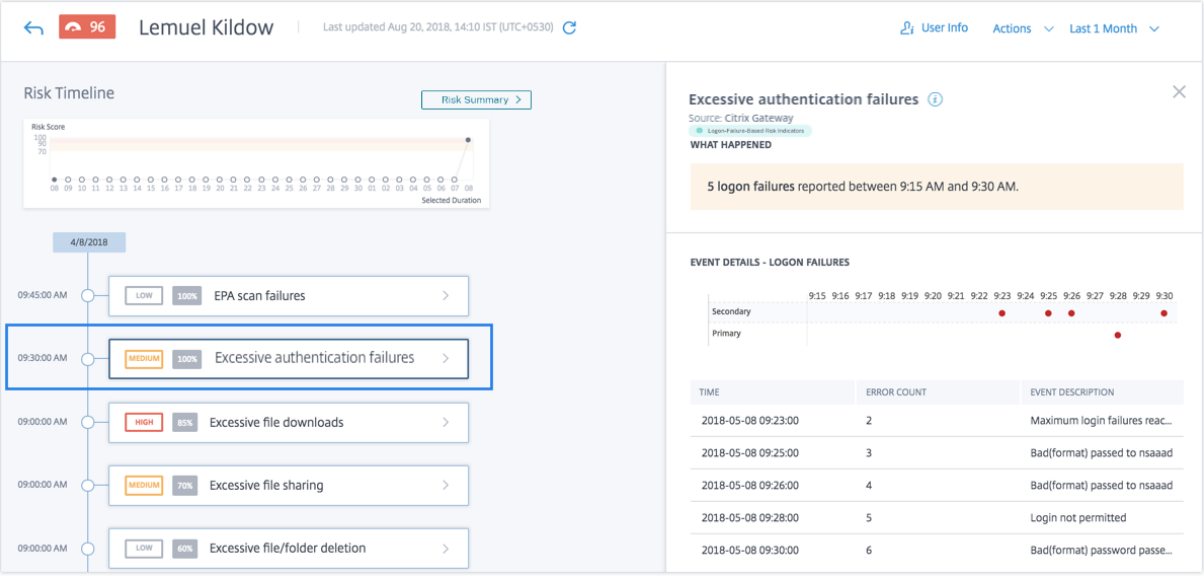
### ¿Cómo analizar el indicador de riesgo de fallas de autenticación excesiva?

Piense en el usuario Lemuel, que recientemente falló varios intentos de autenticar la red. Citrix Gateway informa de estos errores a Citrix Analytics y se asigna una puntuación de riesgo actualizada a Lemuel. El indicador de riesgo de **fallos de autenticación excesivos** se agrega al cronograma de riesgo de Lemuel Kildow.

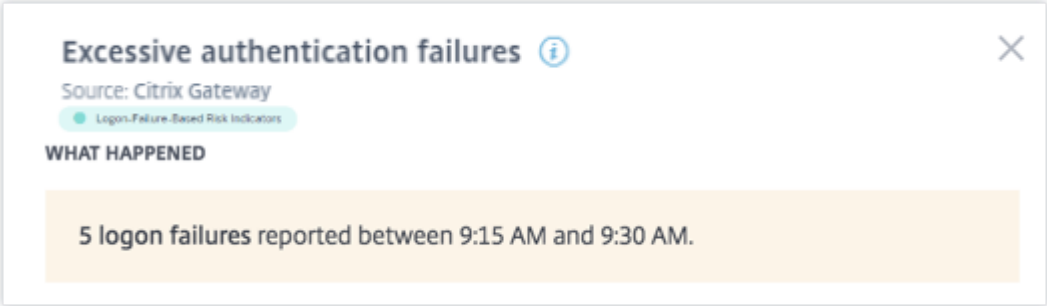
Para ver la entrada del indicador de riesgo de **errores de autenticación excesiva** de un usuario, vaya a **Seguridad > Usuarios**y seleccione el usuario.

En el cronograma de riesgos de Lemuel Kildow, puede seleccionar el último indicador de riesgo de **fallas de autenticación excesivas** notificado para el usuario. Al seleccionar la entrada del indicador de riesgo de **fallos de autenticación excesivos** en el cronograma de riesgos, aparece el panel de información detallada correspondiente en el panel derecho.

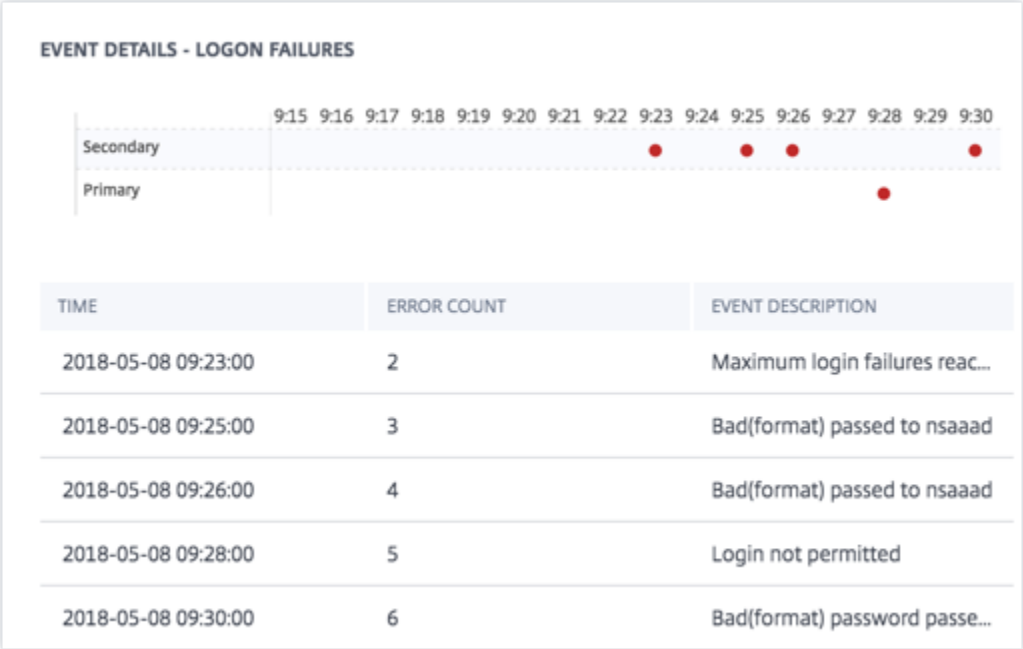



- La sección **QUÉ OCURRIÓ** proporciona un breve resumen del indicador de riesgo, incluido el número de errores de autenticación que se produjeron durante el período seleccionado.




- La sección **DETALLES DEL EVENTO** incluye una visualización de la línea de tiempo de los eventos individuales de error de autenticación excesivo que se produjeron durante el período de tiempo seleccionado. Además, puede ver la siguiente información clave sobre cada evento:
  - **Tiempo**. Hora en que se produjo el error de inicio de sesión.
  - **Recuento de errores**. Número de errores de autenticación detectados para el usuario en el momento del evento y durante las 48 horas anteriores.
  - **Descripción del evento**. Breve descripción del motivo del error de inicio de sesión.




**¿Qué acciones puede aplicar al usuario?**

Puede realizar las siguientes acciones en la cuenta del usuario:

- **Agregar a la lista de seguimiento**. Cuando quiera supervisar a un usuario en busca de futuras amenazas potenciales, puede agregarlas a una lista de seguimiento.
- **Notificar a los administradores**. Cuando hay alguna actividad inusual o sospechosa en la cuenta del usuario, se envía una notificación por correo electrónico a todos los administradores o a los seleccionados.
- **Cierre la sesión del usuario**. Cuando un usuario cierra la sesión de su cuenta, no puede acceder a ningún recurso a través de Citrix Gateway hasta que el administrador de Citrix Gateway borre la acción Cerrar sesión del usuario.
- **Bloquear usuario**: cuando la cuenta de un usuario se bloquea debido a un comportamiento anómalo, no puede acceder a ningún recurso a través de Citrix Gateway hasta que el administrador de Gateway desbloquee la cuenta.

Para obtener más información sobre las acciones y cómo configurarlas manualmente, consulte Directivas y acciones.

Para aplicar las acciones al usuario manualmente, desplácese hasta el perfil del usuario y seleccione el indicador de riesgo adecuado. En el menú **Acciones**, seleccione una acción y haga clic en **Aplicar**.

> **Nota**
>
> Independientemente del origen de datos que desencadena un indicador de riesgo, se pueden aplicar acciones relacionadas con otros orígenes de datos.

## Trayecto imposible

Citrix Analytics detecta los inicios de sesión de un usuario como arriesgados cuando los inicios de sesión consecutivos proceden de dos países diferentes dentro de un período de tiempo inferior al tiempo de trayecto esperado entre los países.

El caso de tiempo de trayecto imposible indica estos riesgos:

- **Credenciales en riesgo**: Un atacante remoto roba las credenciales de un usuario legítimo.
- **Credenciales compartidas**: Diferentes usuarios utilizan las mismas credenciales de usuario.

### ¿Cuándo se activa el indicador de riesgo de trayecto imposible?

El indicador de riesgo de **trayecto imposible** evalúa el tiempo y la distancia estimada entre cada par de inicios de sesión de usuario consecutivos y se activa cuando la distancia es mayor de lo que una persona individual puede recorrer en ese período de tiempo.

> **Nota**
>
> Este indicador de riesgo también contiene una lógica para reducir las alertas de falsos positivos en las siguientes situaciones que no reflejan las ubicaciones reales de los usuarios:
>
> - Cuando los usuarios inician sesión a través de Citrix Gateway desde conexiones proxy.
> - Cuando los usuarios inician sesión a través de Citrix Gateway desde clientes alojados.

### Cómo analizar el indicador de riesgo imposible

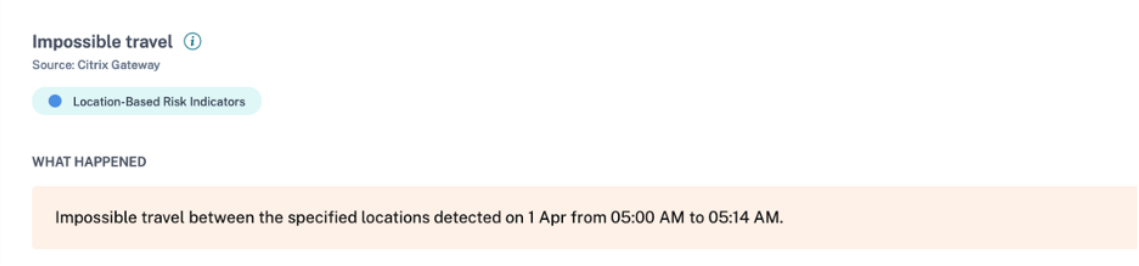
Pongamos como ejemplo al usuario Adam Maxwell, que inicia sesión desde dos ubicaciones, Bangalore (India) y Oslo (Noruega) en un minuto. Citrix Analytics detecta este evento de inicio de sesión como un caso de trayecto imposible y activa el indicador de riesgo de **trayecto imposible**. El indicador de riesgo se agrega al cronograma de riesgo de Adam Maxwell y se le asigna una puntuación de riesgo.

Para ver el cronograma de riesgo de Adam Maxwell, seleccione **Seguridad > Usuarios**. En el panel **Usuarios con riesgos**, seleccione el usuario Adam Maxwell.

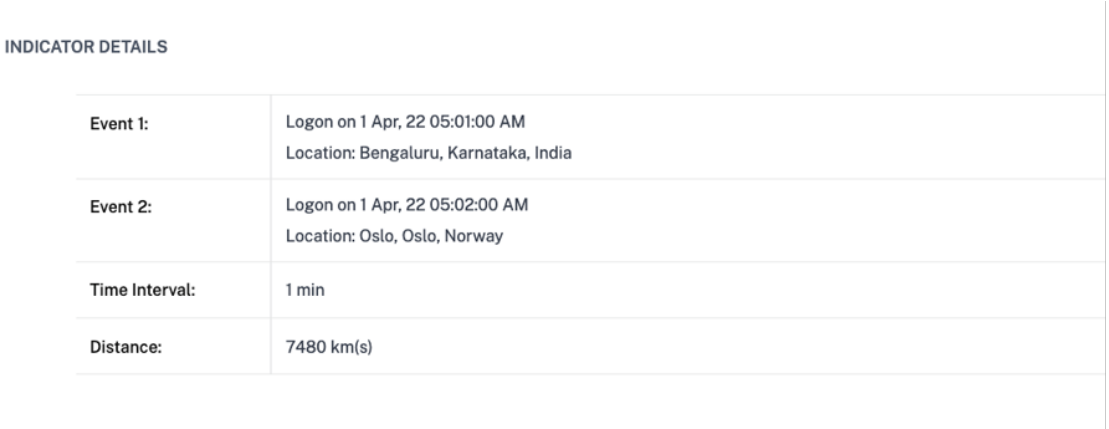
En la cronología de riesgo de Adam Maxwell, seleccione el indicador de riesgo de **trayecto imposible**. Puede ver la siguiente información:

- La sección **QUÉ HA OCURRIDO** ofrece un breve resumen del evento de trayecto imposible.




- La sección **DETALLES DEL INDICADOR** proporciona las ubicaciones desde las que el usuario ha iniciado sesión, el tiempo transcurrido entre los inicios de sesión consecutivos y la distancia entre las dos ubicaciones.




- La sección **UBICACIÓN DE INICIO DE SESIÓN: ÚLTIMOS 30 DÍAS** muestra una vista de mapa geográfico de las ubicaciones de trayecto imposible y las ubicaciones conocidas del usuario. Los datos de ubicación se muestran durante los últimos 30 días. Puede pasar el ratón por encima de los punteros del mapa para ver el total de inicios de sesión de cada ubicación.


- La sección **TRAYECTO IMPOSIBLE: DETALLES DEL EVENTO** proporciona la siguiente información sobre el evento de trayecto imposible:
  - **Fecha**: Indica la fecha y la hora de los inicios de sesión.

- **SO del dispositivo**: indica el sistema operativo del dispositivo del usuario.
- **IP del cliente**: indica la dirección IP del dispositivo del usuario.
- **Ubicación**: indica la ubicación desde la que el usuario ha iniciado sesión.

IMPOSSIBLE TRAVEL - EVENT DETAILS

Add or Remove Columns

| TIME | DEVICE OS | CLIENT IP | LOCATION |
|---|---|---|---|
| 1 Apr, 22 05:02:00 AM | Mac OS | 95.34.6.6 | Oslo, Oslo, Norway |
| 1 Apr, 22 05:01:00 AM | Windows OS | 49.207.220.220 | Bengaluru, Karnataka, India |

Showing 1-2 of 2 items Page 1 of 1

### ¿Qué acciones puede aplicar al usuario?

Puede realizar las siguientes acciones en la cuenta del usuario:

- **Agregar a la lista de seguimiento**. Cuando quiera supervisar a un usuario en busca de futuras amenazas potenciales, puede agregarlas a una lista de seguimiento.
- **Notificar a los administradores**. Cuando hay alguna actividad inusual o sospechosa en la cuenta del usuario, se envía una notificación por correo electrónico a todos los administradores o a los administradores seleccionados.
- **Cierre la sesión del usuario**. Cuando un usuario cierra la sesión de su cuenta, no puede acceder a ningún recurso a través de Citrix Gateway hasta que el administrador de Citrix Gateway borre la acción Cerrar sesión del usuario.
- **Bloquear usuario**: Cuando la cuenta de un usuario se bloquea debido a un comportamiento anómalo, no puede acceder a ningún recurso a través de Citrix Gateway hasta que el administrador de Gateway desbloquee la cuenta.

Para obtener más información sobre las acciones y cómo configurarlas manualmente, consulte Directivas y acciones.

Para aplicar las acciones al usuario manualmente, vaya al perfil del usuario y seleccione el indicador de riesgo correspondiente. En el menú **Acciones**, seleccione una acción y haga clic en **Aplicar**.

> **Nota**
>
> Independientemente del origen de datos que desencadena un indicador de riesgo, se pueden

> aplicar acciones relacionadas con otros orígenes de datos.

## Inicio de sesión desde IP sospechosa

Citrix Analytics detecta las amenazas de acceso de los usuarios en función de la actividad de inicio de sesión desde una IP sospechosa y activa este indicador de riesgo.

El factor de riesgo asociado con el indicador de riesgo de inicio de sesión desde IP sospechosa son los indicadores de riesgo basados en IP. Para obtener más información sobre los factores de riesgo, consulte Indicadores de riesgo de usuario de Citrix.

### ¿Cuándo se activa el indicador de riesgo de IP sospechoso?

El indicador **de riesgo de inicio de sesión desde IP sospechosa** se activa cuando un usuario intenta acceder a la red desde una dirección IP que Citrix Analytics identifica como sospechosa. La dirección IP se considera sospechosa en función de una de las siguientes condiciones:

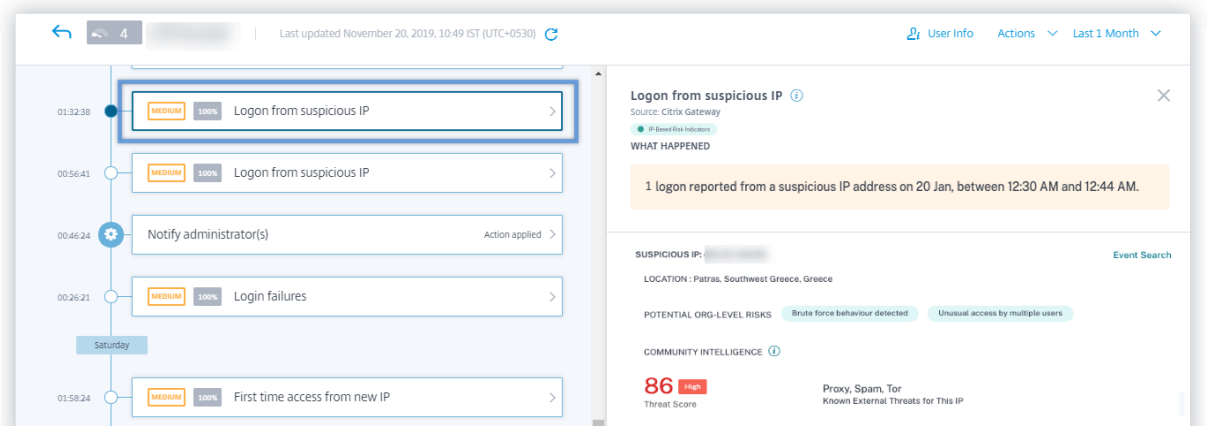
- Aparece en la fuente externa de inteligencia de amenazas IP
- Tiene varios registros de inicio de sesión de usuarios desde una ubicación inusual
- Tiene intentos de inicio de sesión fallidos excesivos que podrían indicar un ataque de fuerza bruta

Citrix Analytics supervisa los eventos de inicio de sesión recibidos de Citrix Gateway y detecta si un usuario ha iniciado sesión desde una IP sospechosa. Cuando Citrix Analytics detecta un intento de inicio de sesión desde una IP sospechosa, actualiza la puntuación de riesgo del usuario y agrega una entrada **del indicador de riesgo de IP sospechosa** al cronograma de riesgo del usuario.

### ¿Cómo analizar el inicio de sesión desde el indicador de riesgo de IP sospechoso?

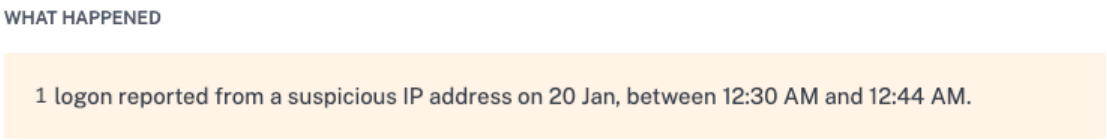
Piense en el usuario Lemuel, que intentó acceder a la red desde una dirección IP que Citrix Analytics identifica como sospechosa. Citrix Gateway informa del evento de inicio de sesión a Citrix Analytics, que asigna una puntuación de riesgo actualizada a Lemuel. El indicador **de riesgo de inicio de sesión desde IP sospechosa** se agrega al cronograma de riesgo de Lemuel Kildow.

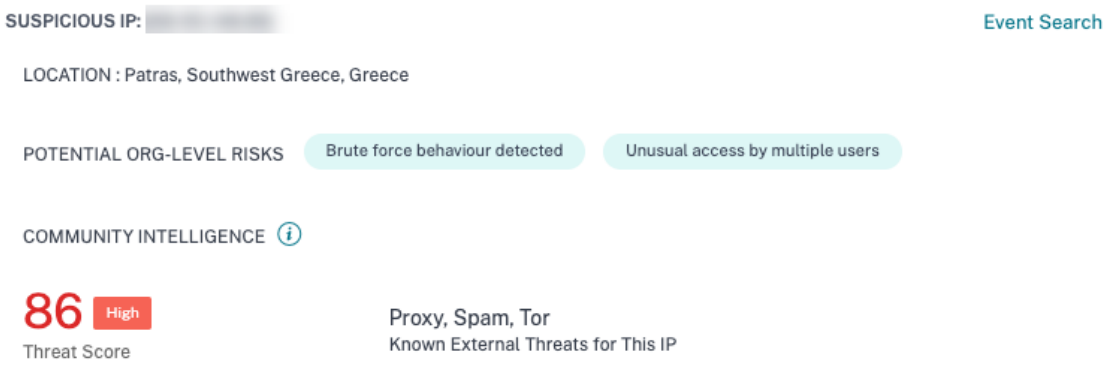



Para ver el indicador de riesgo de inicio de sesión desde IP sospechosa informado para un usuario, vaya a **Seguridad** > **Usuarios** y seleccione el usuario. En el cronograma de riesgo de Lemuel Kildow, puede seleccionar el último **inicio de sesión a partir del indicador de riesgo de IP sospechoso** notificado al usuario. Cuando selecciona la entrada **del indicador de riesgo de IP sospechosa** de la línea de tiempo, aparecerá un panel de información detallada correspondiente en el panel derecho.

- La sección WHAT **Happened** proporciona un breve resumen del indicador de riesgo de inicio de sesión desde IP sospechosa. Además, incluye el número de inicio de sesión desde una dirección IP sospechosa notificada durante el período seleccionado.




- La sección **IP sospechosa** proporciona la siguiente información:

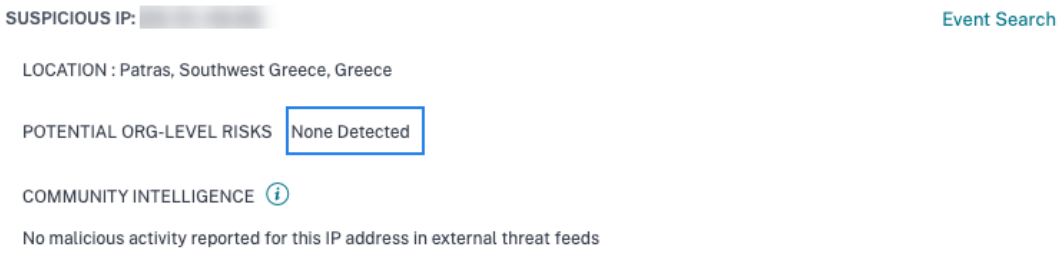



  - **IP sospechosa**. Dirección IP asociada a una actividad de inicio de sesión sospechosa.
  - **Localización**. Ciudad, región y país del usuario. Estas ubicaciones se muestran en función de la disponibilidad de los datos.

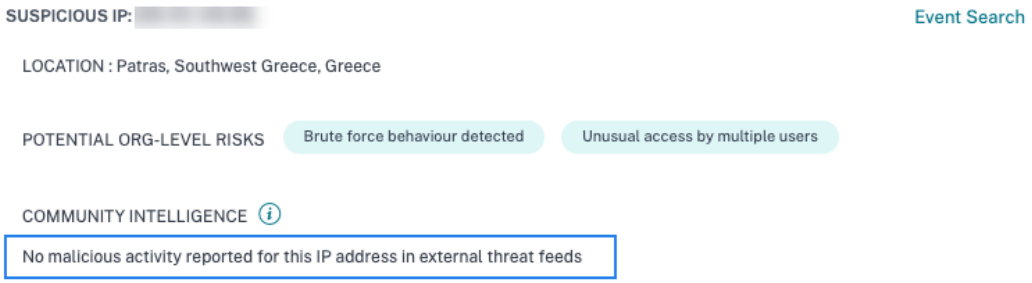
- **Riesgo potencial a nivel de organización**. Indica cualquier patrón de actividad IP sospechosa que Citrix Analytics haya detectado recientemente en su organización. Los patrones de riesgo incluyen fallos excesivos de inicio de sesión coherentes con posibles intentos de fuerza bruta y acceso inusual por parte de varios usuarios.

  Si no se detecta ningún patrón de riesgo para una dirección IP de su organización, verá el siguiente mensaje.




- **Inteligencia comunitaria**. Proporciona la puntuación de amenazas y las categorías de amenazas de una dirección IP que se identifica como de alto riesgo en la fuente de información sobre amenazas IP externas. Citrix Analytics asigna una puntuación de riesgo a la dirección IP de alto riesgo. La puntuación de riesgo comienza a partir de 80.

  Si una dirección IP no tiene información sobre amenazas disponible en la fuente de información sobre amenazas IP externas, aparece el siguiente mensaje.




- La sección **DETALLES DEL EVENTO** proporciona la siguiente información sobre la actividad de inicio de sesión sospechosa:

LOGIN FROM SUSPICIOUS IP - EVENT DETAILS

| TIME | CLIENT IP | DEVICE OS | DEVICE BROWSER |
|---|---|---|---|
| 1 Apr, 19 05:05:00 AM | | Android | Chrome |
| 1 Apr, 19 05:13:00 AM | | Android | Chrome |

- **Tiempo**. Hora de la actividad de inicio de sesión sospechosa.
- **IP del cliente**. Dirección IP del dispositivo del usuario que se utilizó para la actividad de inicio de sesión sospechosa.
- **Sistema operativo del dispositivo**. El sistema operativo del explorador.
- **Explorador de dispositivos**. El explorador web utilizado para la actividad de inicio de sesión sospechosa.

#### ¿Qué acciones puede aplicar al usuario?

Puede realizar las siguientes acciones en la cuenta del usuario:

- **Agregar a la lista de seguimiento**. Cuando quiera supervisar a un usuario en busca de futuras amenazas potenciales, puede agregarlas a una lista de seguimiento.
- **Notificar a los administradores**. Cuando hay alguna actividad inusual o sospechosa en la cuenta del usuario, se envía una notificación por correo electrónico a todos los administradores o a los seleccionados.
- **Cierre la sesión del usuario**. Cuando un usuario cierra la sesión de su cuenta, no puede acceder a ningún recurso a través de Citrix Gateway hasta que el administrador de Citrix Gateway borre la acción Cerrar sesión del usuario.
- **Bloquear usuario**: cuando la cuenta de un usuario se bloquea debido a un comportamiento anómalo, no puede acceder a ningún recurso a través de Citrix Gateway hasta que el administrador de Gateway desbloquee la cuenta.

Para obtener más información sobre las acciones y cómo configurarlas manualmente, consulte Directivas y acciones.

Para aplicar las acciones al usuario manualmente, desplácese hasta el perfil del usuario y seleccione el indicador de riesgo adecuado. En el menú **Acciones**, seleccione una acción y haga clic en **Aplicar**.

> **Nota**
>
> Independientemente del origen de datos que desencadena un indicador de riesgo, se pueden aplicar acciones relacionadas con otros orígenes de datos.

### Inicio de sesión sospechoso

> **Notas**
>
> - Este indicador de riesgo reemplaza el indicador de riesgo de acceso desde una ubicación inusual.

> • Todas las directivas basadas en el indicador de riesgo de acceso desde una ubicación inusual se vinculan automáticamente al indicador de riesgo de inicio de sesión sospechoso.

Citrix Analytics detecta los inicios de sesión del usuario que parecen inusuales o con riesgos en función de varios factores contextuales, definidos conjuntamente por el dispositivo, la ubicación y la red que utiliza el usuario.

**¿Cuándo se activa el indicador de riesgo de inicio de sesión sospechoso?**

El indicador de riesgo se activa mediante la combinación de los siguientes factores, en los que cada factor se considera potencialmente sospechoso en función de una o más condiciones.

| Factor | Condiciones |
|---|---|
| Dispositivo inusual | El usuario inicia sesión desde un dispositivo con una firma diferente a la de los dispositivos utilizados en los últimos 30 días. La firma del dispositivo se basa en el sistema operativo del dispositivo y en el explorador utilizado. |
| Ubicación inusual | Inicie sesión desde una ciudad o un país en el que el usuario no haya iniciado sesión en los últimos 30 días.<br>La ciudad o el país están geográficamente lejos de las ubicaciones de inicio de sesión recientes (últimos 30 días).<br>Ninguno o un mínimo de usuarios han iniciado sesión desde la ciudad o el país en los últimos 30 días. |
| Red inusual | Inicie sesión desde una dirección IP que el usuario no ha utilizado en los últimos 30 días.<br>Inicie sesión desde una subred IP que el usuario no ha utilizado en los últimos 30 días.<br>Ningún usuario o mínimo ha iniciado sesión desde la subred IP en los últimos 30 días. |
| Amenaza IP | La dirección IP se identifica como de alto riesgo por el feed de inteligencia de amenazas de la comunidad: Webroot.<br>Citrix Analytics ha detectado recientemente actividades de inicio de sesión muy sospechosas desde la dirección IP de otros usuarios. |

### Cómo analizar el indicador de riesgo de inicio de sesión sospechoso

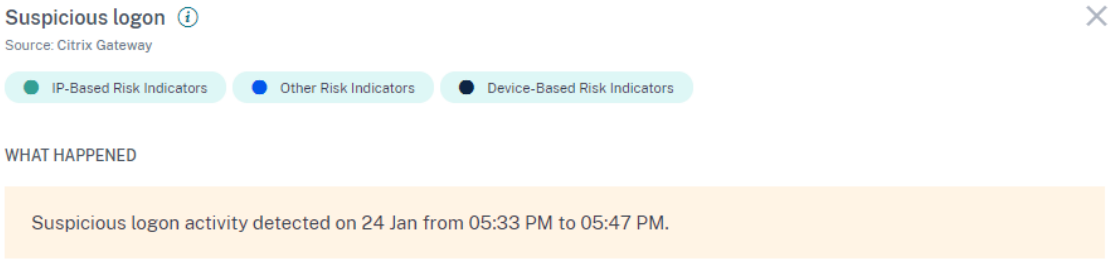
Piense en el usuario Adam Maxwell, que inicia sesión desde Andhra Pradesh, India por primera vez. Usa un dispositivo con una firma conocida para acceder a los recursos de la organización. Pero se conecta desde una red, que no ha utilizado en los últimos 30 días.

Citrix Analytics detecta este evento de inicio de sesión como sospechoso porque los factores, la ubicación y la red, se desvían de su comportamiento habitual y desencadena el indicador de riesgo de inicio de sesión sospechoso. El indicador de riesgo se agrega al cronograma de riesgo de Adam Maxwell y se le asigna una puntuación de riesgo.

Para ver el tiempo de riesgo de Adam Maxwell, seleccione **Seguridad > Usuarios**. En el panel **Usuarios con riesgos**, seleccione el usuario Adam Maxwell.

En la línea de tiempo de riesgo de Adam Maxwell, seleccione el indicador de riesgo de **inicio de sesión sospechoso**. Puede ver la siguiente información:

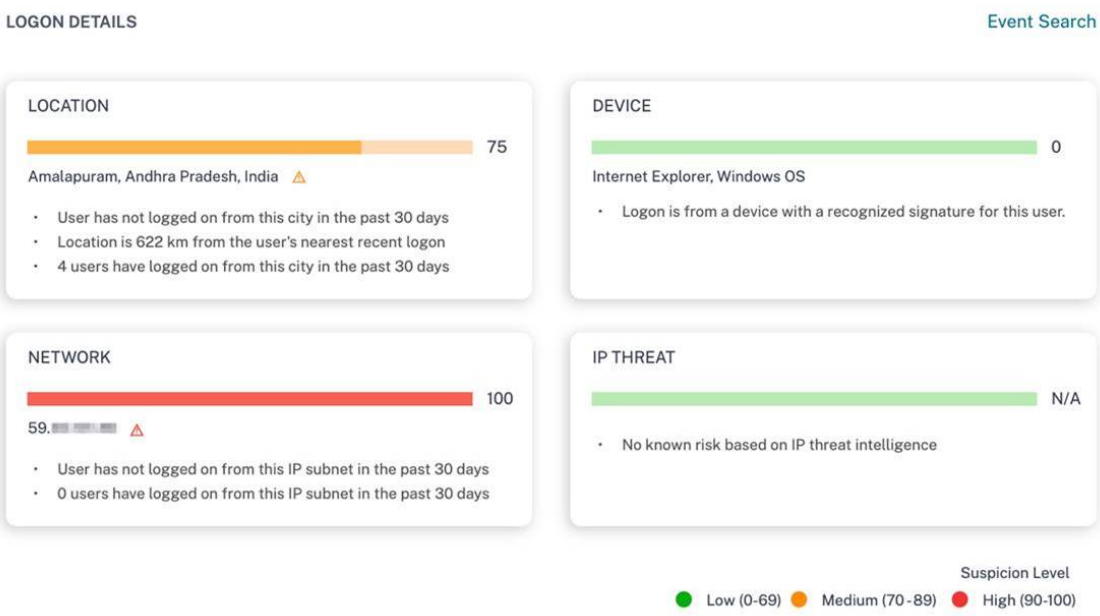
- La sección **QUÉ SUCEDIÓ** proporciona un breve resumen de las actividades sospechosas que incluyen los factores de riesgo y el momento del evento.




- La sección **DETALLES DE INICIO DE SESIÓN** proporciona un resumen detallado de las actividades sospechosas correspondientes a cada factor de riesgo. A cada factor de riesgo se le asigna una puntuación que indica el nivel de sospecha. Un factor de riesgo único no indica un riesgo elevado por parte de un usuario. El riesgo global se basa en la correlación de los múltiples factores de riesgo.

| Nivel de sospecha | Indicación |
|---|---|
| 0–69 | El factor parece normal y no se considera sospechoso. |
| 70–89 | El factor parece un poco inusual y se considera moderadamente sospechoso con otros factores. |
| 90–100 | El factor es totalmente nuevo o inusual y se considera altamente sospechoso con otros factores. |




- La **UBICACIÓN DE INICIO DE SESIÓN: ÚLTIMOS 30 DÍAS** muestra una vista de mapa geográfico de las últimas ubicaciones conocidas y la ubicación actual del usuario. Los datos de ubicación se muestran durante los últimos 30 días. Puede pasar el ratón por encima de los punteros del mapa para ver el total de inicios de sesión de cada ubicación.


- La sección **DETALLES DEL EVENTO DE INICIO DE SESIÓN SOSPECHOSO** proporciona la siguiente información sobre el evento de inicio de sesión sospechoso:
  - **Hora**: indica la fecha y la hora del inicio de sesión sospechoso.
  - **SO del dispositivo**: indica el sistema operativo del dispositivo del usuario.

– **Explorador de dispositivos**: indica el explorador web utilizado para iniciar sesión en Citrix Gateway.

SUSPICIOUS LOGON - EVENT DETAILS

| TIME | DEVICE OS | DEVICE BROWSER |
|---|---|---|
| 24 Jan, 22 05:43:55 PM | Windows OS | Internet Explorer |

### ¿Qué acciones puede aplicar al usuario?

Puede realizar las siguientes acciones en la cuenta del usuario:

- **Agregar a la lista de seguimiento**. Cuando quiera supervisar a un usuario en busca de futuras amenazas potenciales, puede agregarlas a una lista de seguimiento.
- **Notificar a los administradores**. Cuando hay alguna actividad inusual o sospechosa en la cuenta del usuario, se envía una notificación por correo electrónico a todos los administradores o a los seleccionados.
- **Cierre la sesión del usuario**. Cuando un usuario cierra la sesión de su cuenta, no puede acceder a ningún recurso a través de Citrix Gateway hasta que el administrador de Citrix Gateway borre la acción Cerrar sesión del usuario.
- **Bloquear usuario**: cuando la cuenta de un usuario se bloquea debido a un comportamiento anómalo, no puede acceder a ningún recurso a través de Citrix Gateway hasta que el administrador de Gateway desbloquee la cuenta.

Para obtener más información sobre las acciones y cómo configurarlas manualmente, consulte Directivas y acciones.

Para aplicar las acciones al usuario manualmente, desplácese hasta el perfil del usuario y seleccione el indicador de riesgo adecuado. En el menú **Acciones**, seleccione una acción y haga clic en **Aplicar**.

> **Nota**
>
> Independientemente del origen de datos que desencadena un indicador de riesgo, se pueden aplicar acciones relacionadas con otros orígenes de datos.

## Error de autenticación inusual

Citrix Analytics detecta amenazas basadas en el acceso cuando un usuario tiene errores de inicio de sesión desde una dirección IP inusual y activa el indicador de riesgo correspondiente.

El factor de riesgo asociado con el indicador Riesgo de autenticación inusual son los indicadores de riesgo basados en fallos de inicio de sesión. Para obtener más información sobre los factores de riesgo, consulte Indicadores de riesgo de usuario de Citrix.

### ¿Cuándo se activa el indicador de error de autenticación inusual?

Se le puede notificar cuando un usuario de su organización tiene errores de inicio de sesión desde una dirección IP inusual que es contraria a su comportamiento habitual.

Citrix Gateway detecta estos eventos y los informa a Citrix Analytics. Citrix Analytics recibe los eventos y aumenta la puntuación de riesgo del usuario. El indicador de riesgo de **error de autenticación inusual** se agrega al cronograma de riesgo del usuario.

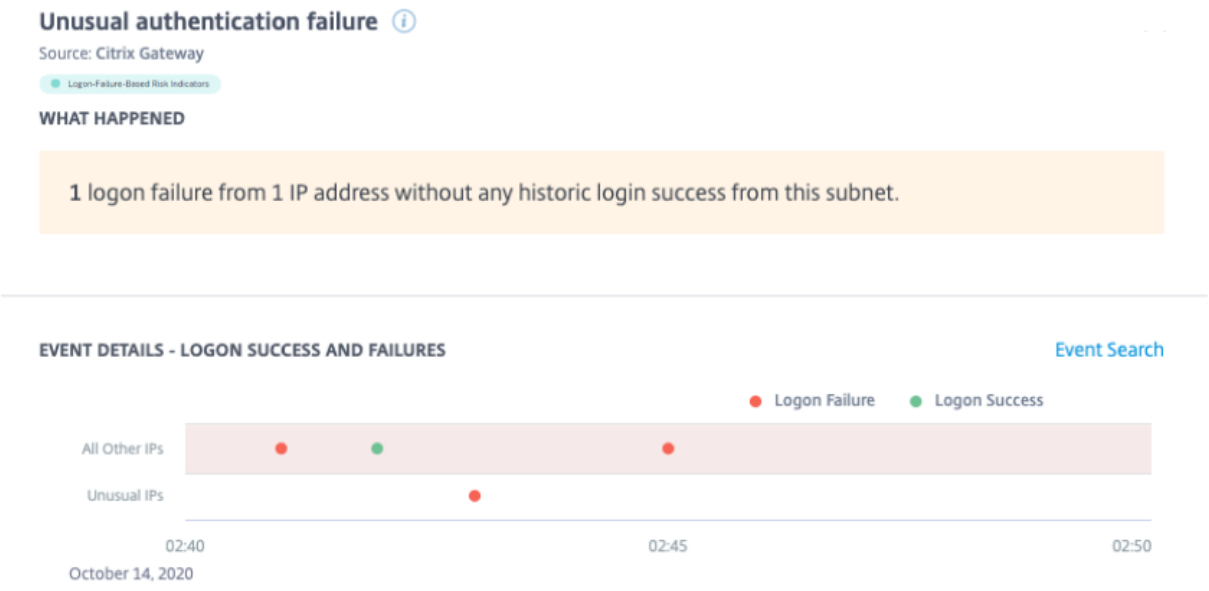
### ¿Cómo analizar el indicador de falla de autenticación inusual?

Piense en la usuaria Georgina Kalou, que inicia sesión habitualmente en Citrix Gateway desde sus redes domésticas y de oficina habituales. Un atacante remoto intenta autenticar la cuenta de Georgina adivinando contraseñas diferentes, lo que provoca errores de autenticación de una red desconocida.

En este caso, Citrix Gateway informa de estos eventos a Citrix Analytics, que asigna una puntuación de riesgo actualizada a Georgina Kalou. El indicador de riesgo de fallo de autenticación inusual se agrega al cronograma de riesgo de Georgina Kalou.

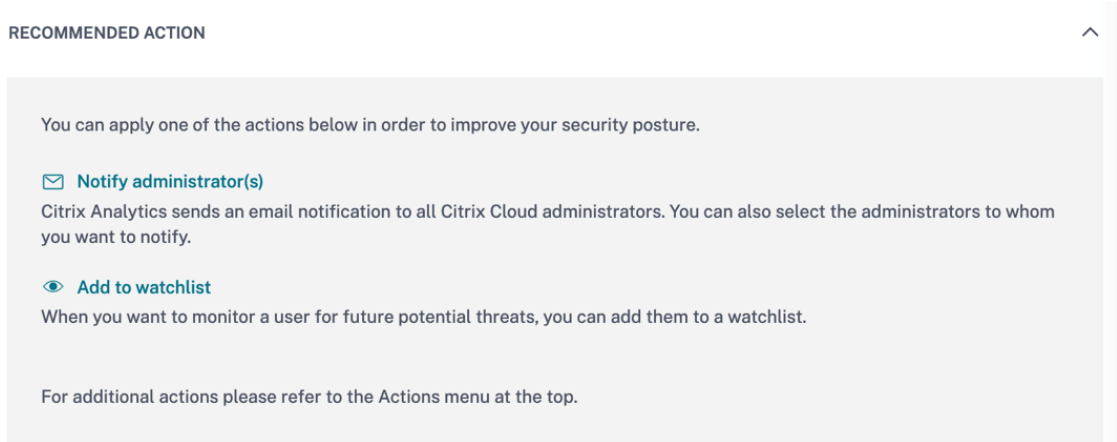
En el cronograma de riesgos de Georgina Kalou, puede seleccionar el indicador de riesgo de fallo de autenticación inusual notificado. El motivo del evento se muestra junto con detalles como la hora del evento y la ubicación.




- En la sección **QUÉ SUCEDIÓ**, puede ver el breve resumen que incluye el número total de errores de autenticación y la hora del evento.
- En la sección **ACCIÓN RECOMENDADA**, encontrará las acciones sugeridas que se pueden aplicar en el indicador de riesgo. Citrix Analytics for Security recomienda las acciones en función de la gravedad del riesgo que presente el usuario. La recomendación puede ser una o una combinación de las siguientes acciones:
  - Notificar a los administradores
  - Agregar a la lista de seguimiento
  - Crear una directiva

  Puede seleccionar una acción en función de la recomendación. O puede seleccionar una acción que quiera aplicar en función de su elección en el menú **Acciones**. Para obtener más información, consulte Aplicar una acción manualmente.



- En la sección **DETALLES DEL EVENTO: ERRORES Y ÉXITO DE INICIO DE SESIÓN**, puede ver un gráfico que indica los errores de autenticación inusuales, junto con cualquier otra actividad de inicio de sesión detectada durante la misma duración.
- En la sección **DETALLES DE AUTENTICACIÓN INUSUALES**, la tabla proporciona la siguiente información sobre los errores de autenticación inusuales:
  - **Hora de inicio de sesión**: Fecha y hora del evento
  - **IP del cliente**: Dirección IP del dispositivo del usuario
  - **Ubicación**: Ubicación desde la que se ha producido el evento
  - **Motivo del error**: El motivo del error de autenticación

UNUSUAL AUTHENTICATION FAILURE DETAILS

| EVENT TIME | CLIENT IP | LOCATION | FAILURE REASON |
|---|---|---|---|
| 10/14/20 02:43:00 | 99.155.88.64 | San Jose, California, United ... | Bad(format) password pass... |

Showing 1 - 1 of 1 items

- En la sección **ACTIVIDAD DE AUTENTICACIÓN DEL USUARIO: 30 DÍAS ANTERIORES**, la tabla proporciona la siguiente información sobre los 30 días anteriores de actividad de autenticación del usuario:
  - Subred: dirección IP de la red de usuarios.
  - Éxito: el número total de eventos de autenticación correctos y la hora del evento de éxito más reciente para el usuario.
  - Error: número total de eventos de autenticación fallidos y la hora del último evento fallido del usuario.
  - Ubicación: ubicación desde la que se ha producido el evento de autenticación.

AUTHENTICATION ACTIVITY - PREVIOUS 30 DAYS

| SUBNET | SUCCESS | Most Recent | FAILURE | Most Recent | LOCATION |
|---|---|---|---|---|---|
| [illegible] | 29 | 03/25/20 00:35:56 | 0 | - - | Nairobi, Kenya |
| [illegible] | 1 | 03/21/20 10:44:22 | 0 | - - | FL, Florida, USA |
| [illegible] | 1004 | 03/21/20 08:34:56 | 0 | - - | Moscow, RS, Russia |
| [illegible] | 0 | - - | 29 | 03/22/20 23:35:56 | Munich, some_state, Germ... |
| [illegible] | 0 | - - | 29 | 03/07/20 19:35:56 | Location not available |

Showing 1 - 5 of 5 items

#### ¿Qué acciones puede aplicar al usuario?

Puede realizar las siguientes acciones en la cuenta del usuario:

- **Agregar a la lista de seguimiento**. Cuando quiera supervisar a un usuario en busca de futuras amenazas potenciales, puede agregarlas a una lista de seguimiento.
- **Notificar a los administradores**. Cuando hay alguna actividad inusual o sospechosa en la cuenta del usuario, se envía una notificación por correo electrónico a todos los administradores o a los seleccionados.
- **Cierre la sesión del usuario**. Cuando un usuario cierra la sesión de su cuenta, no puede acceder a ningún recurso a través de Citrix Gateway hasta que el administrador de Citrix Gateway borre la acción Cerrar sesión del usuario.
- **Bloquear usuario**: cuando la cuenta de un usuario se bloquea debido a un comportamiento anómalo, no puede acceder a ningún recurso a través de Citrix Gateway hasta que el administrador de Gateway desbloquee la cuenta.

Para obtener más información sobre las acciones y cómo configurarlas manualmente, consulte Directivas y acciones.

Para aplicar las acciones al usuario manualmente, desplácese hasta el perfil del usuario y seleccione el indicador de riesgo adecuado. En el menú **Acciones**, seleccione una acción y haga clic en **Aplicar**.

> **Nota**
>
> Independientemente del origen de datos que desencadena un indicador de riesgo, se pueden aplicar acciones relacionadas con otros orígenes de datos.

## Indicadores de riesgo de Citrix Secure Private Access

April 12, 2024

### Acceso a sitios web con riesgos

> **Nota:**
> Estas prestaciones de Citrix Analytics for Security se ven afectadas debido a que Secure Private Access ha dejado de utilizar el filtrado web basado en categorías:
>
> 1. Los campos de datos como el grupo de categorías, la categoría y la reputación de las URL ya no están disponibles en el panel de seguridad de Citrix Analytics.

> 2. El indicador de acceso a sitios web de riesgo, que se basa en los mismos datos, también se ha retirado y no se activa para los clientes.
> 3. Los indicadores de riesgo personalizados existentes que utilicen los campos de datos (categoría, grupo, categoría y reputación de las URL) y sus directivas asociadas ya no se activan.

Para obtener más información sobre la retirada en Secure Private Access, consulte Funciones retiradas.

## Intento de acceder a URL de la lista de bloqueados

Citrix Analytics detecta las amenazas de acceso a los datos en función de las URL incluidas en la lista de bloqueados a las que accede el usuario y activa el indicador de riesgo correspondiente.

El indicador de riesgo **Intento de acceso a URL en lista negra** se informa en Citrix Analytics cuando un usuario intenta acceder a una URL en lista negra configurada en Acceso privado seguro.

El factor de riesgo asociado con el indicador de riesgo **Intento de acceder a una URL incluida en la lista de bloqueados** es Otros indicadores de riesgo. Para obtener más información sobre los factores de riesgo, consulte Indicadores de riesgo de usuario de Citrix.

### ¿Cuándo se activa el indicador de riesgo Intento de acceder a una URL incluida en la lista de bloqueados?

Secure Private Access incluye una función de categorización de URL que proporciona control basado en directivas para restringir el acceso a las URL incluidas en la lista negra. Cuando un usuario intenta acceder a una URL de la lista negra, Secure Private Access informa de este evento a Citrix Analytics. Citrix Analytics actualiza la puntuación de riesgo del usuario y agrega una entrada del indicador de riesgo de **URL de Intento de acceder a la lista de bloqueados** al cronograma de riesgo del usuario.

### ¿Cómo analizar el indicador de riesgo Intento de acceder a la lista de bloqueados de URL?

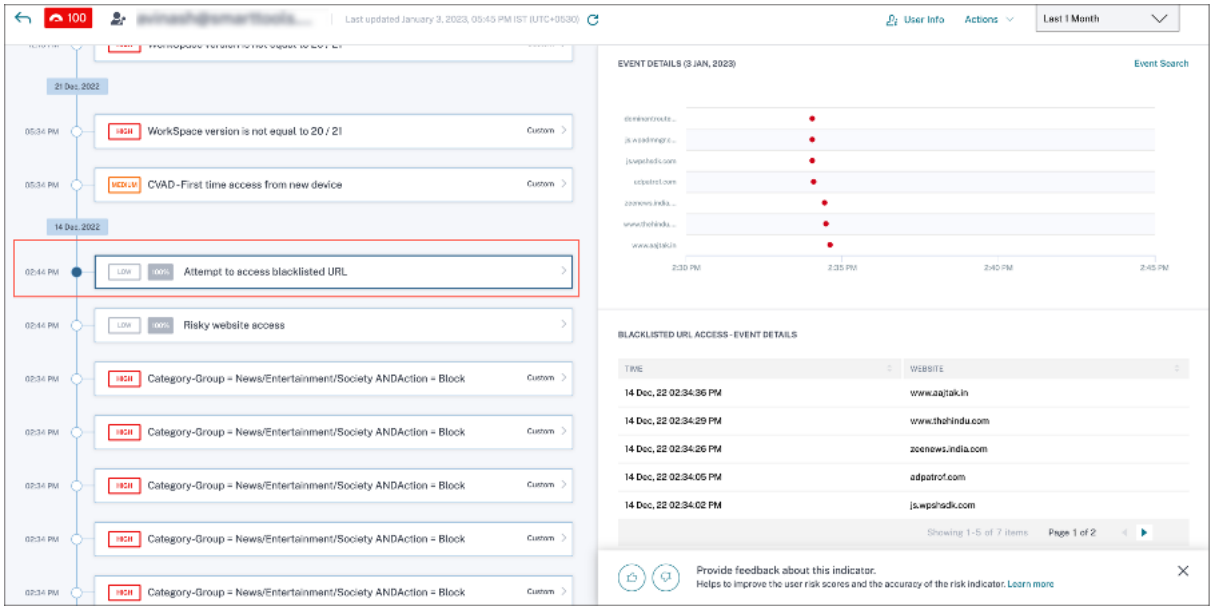
Considere a una usuaria Georgina Kalou, que accedió a una URL en la lista negra configurada en Acceso privado seguro. Secure Private Access informa de este evento a Citrix Analytics, que asigna una puntuación de riesgo actualizada a Georgina Kalou. El indicador de riesgo de **Intento de acceder a la URL de la lista de bloqueados** se agrega a la cronología de riesgo de Georgina Kalou.

En la cronología de riesgos de Georgina Kalou, puede seleccionar el indicador de riesgo de **Intento de acceder a la URL de la lista de bloqueados** . El motivo del evento se muestra junto con los detalles sobre los eventos, como la hora del evento, los detalles del sitio web.

Para ver la entrada de **URL Intento de acceso a la lista de bloqueados** de un usuario, vaya a **Seguridad > Usuarios**y seleccione el usuario.

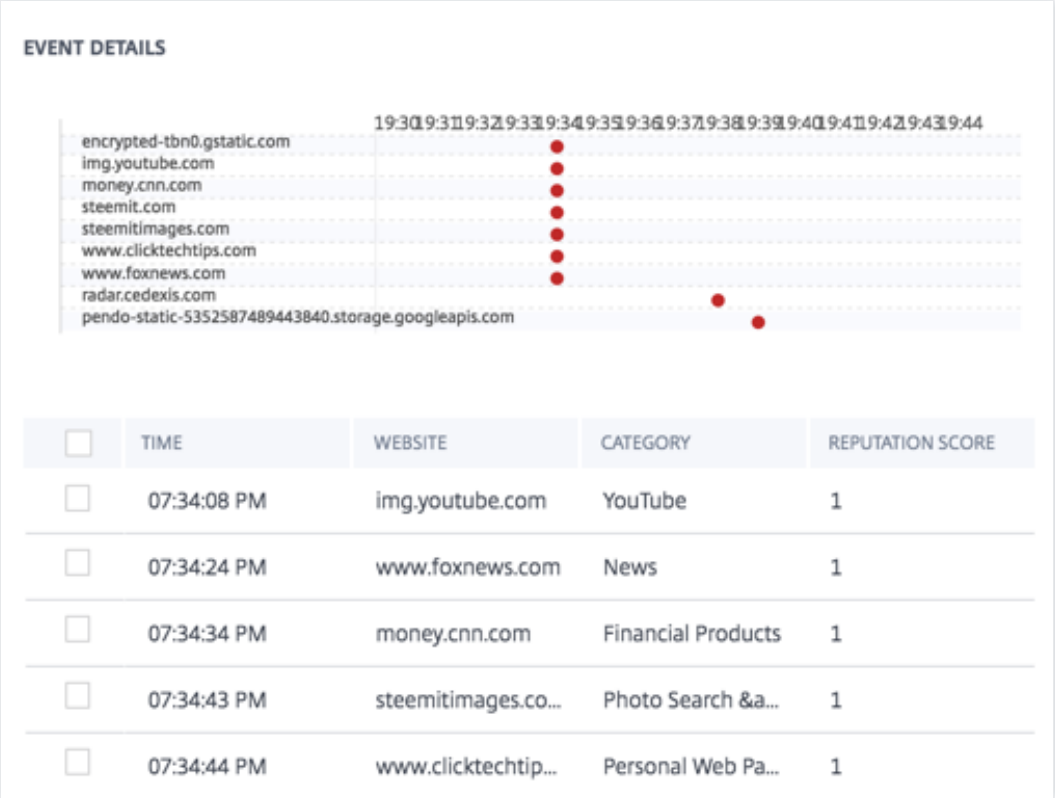
Al seleccionar la entrada del indicador de riesgo de **URL de la lista de bloqueados** en la línea de tiempo, aparece el panel de información detallada correspondiente en el panel derecho.




- La sección **QUÉ PASÓ** proporciona un breve resumen del indicador de riesgo. Incluye los detalles de la URL de la lista de bloqueados a la que accede el usuario durante el período seleccionado.


- La sección **DETALLES DEL EVENTO** incluye una visualización del cronograma de los eventos individuales que se produjeron durante el período de tiempo seleccionado. Además, puede ver la siguiente información clave sobre cada evento:
  - **¡Hora**! Hora en que se produjo el evento.
  - **Sitio web**. El sitio web con riesgos al que accede el usuario.
  - **Categoría**. La categoría especificada por Secure Private Access para la URL de la lista negra.
  - **Calificación de reputación**. La calificación de reputación devuelta por Secure Private Access para la URL de la lista negra. Para obtener más información, consulta Puntuación de reputación de URL.




### ¿Qué acciones puede aplicar al usuario?

Puede realizar las siguientes acciones en la cuenta del usuario:

- **Agregar a la lista de seguimiento**. Cuando quiera supervisar a un usuario en busca de futuras amenazas potenciales, puede agregarlas a una lista de seguimiento.
- **Notificar a los administradores**. Cuando hay alguna actividad inusual o sospechosa en la cuenta del usuario, se envía una notificación por correo electrónico a todos los administradores o a los seleccionados.

Para obtener más información sobre las acciones y cómo configurarlas manualmente, consulte Directivas y acciones.

Para aplicar las acciones al usuario manualmente, desplácese hasta el perfil del usuario y seleccione el indicador de riesgo adecuado. En el menú **Acciones**, seleccione una acción y haga clic en **Aplicar**.

> **Nota**
>
> Independientemente del origen de datos que desencadena un indicador de riesgo, se pueden aplicar acciones relacionadas con otros orígenes de datos.

## Volumen de subida

Citrix Analytics detecta las amenazas de acceso a los datos basándose en la actividad de volumen de carga inusual y activa el indicador de riesgo correspondiente.

El indicador de riesgo de **volumen de carga inusual** se informa cuando un usuario carga un volumen excesivo de datos en una aplicación o sitio web.

El factor de riesgo asociado con el indicador de riesgo de volumen de carga inusual es el Otros indicadores de riesgo. Para obtener más información sobre los factores de riesgo, consulte Indicadores de riesgo de usuario de Citrix.

### ¿Cuándo se activa el indicador de riesgo de volumen de carga inusual?

Puede configurar Secure Private Access para supervisar las actividades de los usuarios, como los sitios web maliciosos, peligrosos o desconocidos visitados y el ancho de banda consumido, y las descargas y cargas peligrosas. Cuando un usuario de su organización carga datos en una aplicación o sitio web, Secure Private Access informa de estos eventos a Citrix Analytics.

Citrix Analytics supervisa todos estos eventos y, si determina que esta actividad del usuario es contraria al comportamiento habitual del usuario, actualiza la puntuación de riesgo del usuario. El indicador de riesgo de **volumen de carga inusual** se agrega al cronograma de riesgo del usuario.

### ¿Cómo analizar el indicador de riesgo de volumen de carga inusual?

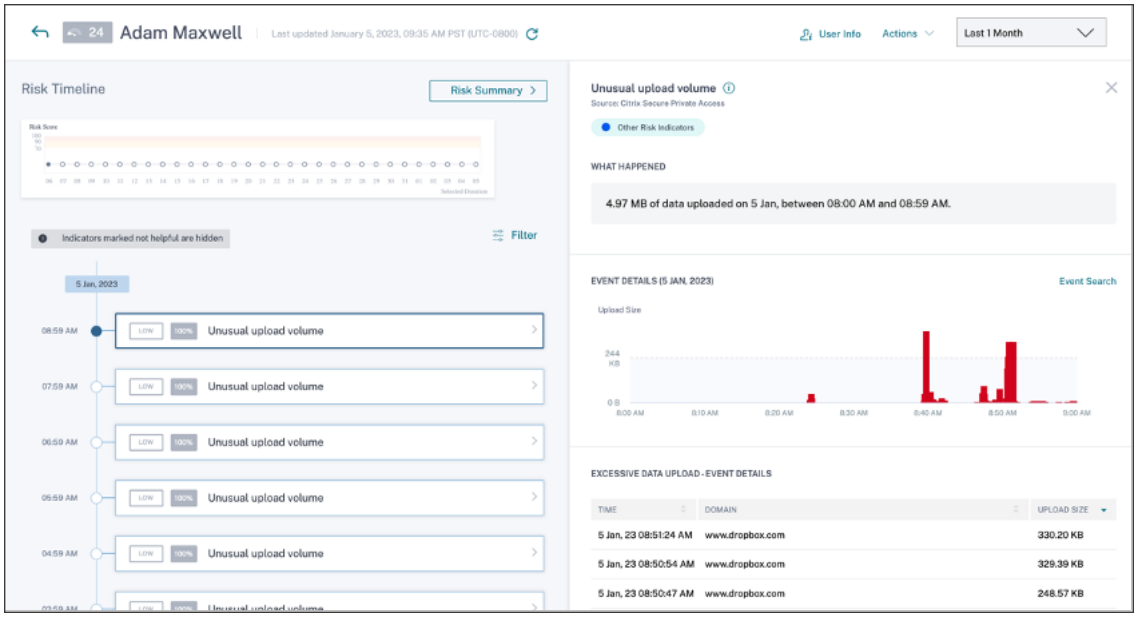
Piense en un usuario Adam Maxwell, que cargó un volumen excesivo de datos en una aplicación o sitio web. Secure Private Access informa de estos eventos a Citrix Analytics, que asigna una puntuación de riesgo actualizada a Adam Maxwell. El indicador de riesgo de **volumen de carga inusual** se agrega al cronograma de riesgo de Adam Maxwell.

En el cronograma de riesgo de Adam Maxwell, puede seleccionar el indicador de riesgo de **volumen de carga inusual** notificado. El motivo del evento se muestra junto con los detalles sobre los eventos, como la hora del evento y el dominio.

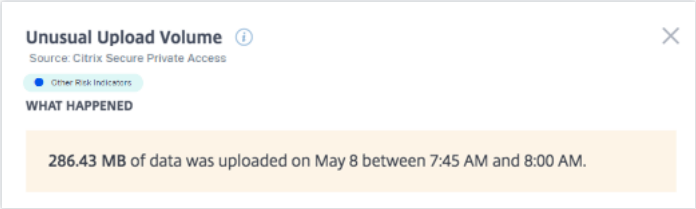
Para ver el indicador de riesgo de **volumen de carga inusual**, vaya a **Seguridad > Usuarios**y seleccione el usuario.

Al seleccionar una entrada del indicador de riesgo de **volumen de carga inusual** en la línea de tiempo, aparece el panel de información detallada correspondiente en el panel derecho.

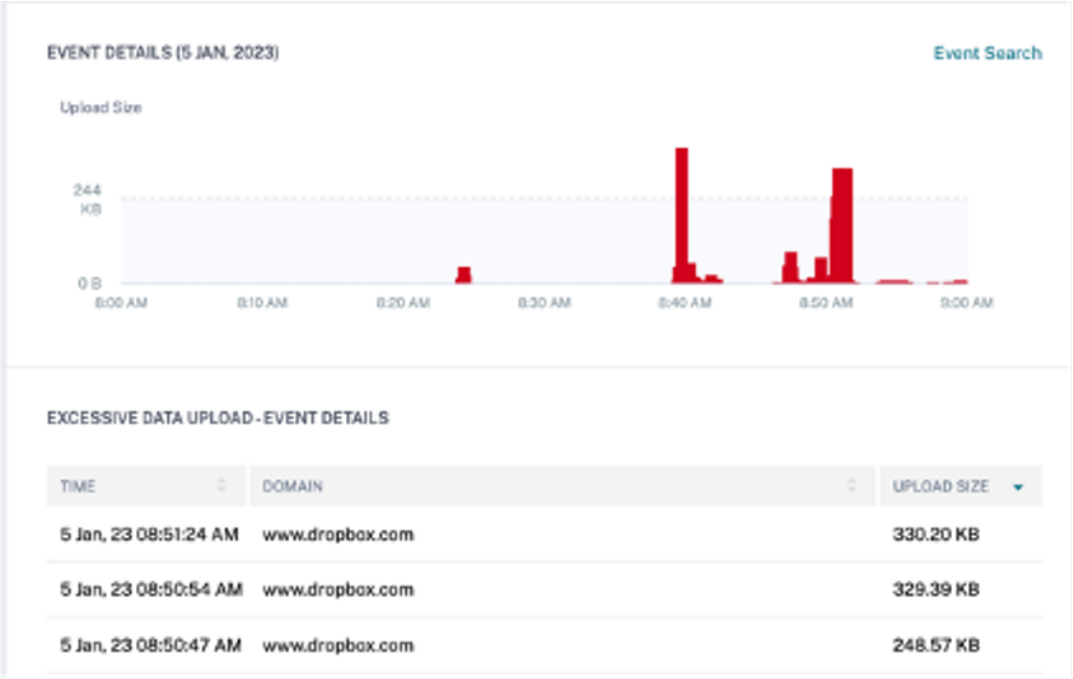



- La sección **QUÉ SUCEDIÓ** proporciona un breve resumen del indicador de riesgo, incluido el volumen de datos cargados durante el período seleccionado.




- La sección **DETALLES DEL EVENTO** incluye una visualización del cronograma de los eventos de carga de datos individuales que se produjeron durante el período de tiempo seleccionado. Además, puede ver la siguiente información clave sobre cada evento:
  - **¡Hora**! La hora en que se cargaron los datos excesivos en una aplicación o en un sitio web.
  - **Dominio**. Dominio en el que el usuario ha cargado los datos.
  - **Tamaño de subida**. Volumen de datos cargados en el dominio.




### ¿Qué acciones puede aplicar al usuario?

Puede realizar las siguientes acciones en la cuenta del usuario:

- **Agregar a la lista de seguimiento**. Cuando quiera supervisar a un usuario en busca de futuras amenazas potenciales, puede agregarlas a una lista de seguimiento.
- **Notificar a los administradores**. Cuando hay alguna actividad inusual o sospechosa en la cuenta del usuario, se envía una notificación por correo electrónico a todos los administradores o a los seleccionados.

Para obtener más información sobre las acciones y cómo configurarlas manualmente, consulte Directivas y acciones.

Para aplicar las acciones al usuario manualmente, desplácese hasta el perfil del usuario y seleccione el indicador de riesgo adecuado. En el menú **Acciones**, seleccione una acción y haga clic en **Aplicar**.

> **Nota**
>
> Independientemente del origen de datos que desencadena un indicador de riesgo, se pueden aplicar acciones relacionadas con otros orígenes de datos.

## Descarga excesiva de datos

Citrix Analytics detecta amenazas de acceso a datos basándose en los datos excesivos descargados por los usuarios en su red y activa el indicador de riesgo correspondiente.

El indicador de riesgo se informa cuando un usuario de su organización descarga un volumen excesivo de datos de una aplicación o sitio web.

### ¿Cuándo se activa el indicador de riesgo de descarga excesiva de datos?

Puede configurar Secure Private Access para supervisar las actividades de los usuarios, como los sitios web maliciosos, peligrosos o desconocidos visitados y el ancho de banda consumido, y las descargas y cargas peligrosas. Cuando un usuario de su organización descarga datos de una aplicación o sitio web, Secure Private Access informa de estos eventos a Citrix Analytics.

Citrix Analytics supervisa todos estos eventos y, si determina que la actividad del usuario es contraria al comportamiento habitual del usuario, actualiza la puntuación de riesgo del usuario. El indicador de riesgo de descarga excesiva de datos se agrega al cronograma de riesgo del usuario.

El factor de riesgo asociado con el indicador de riesgo de descarga excesiva de datos es el Otros indicadores de riesgo. Para obtener más información sobre los factores de riesgo, consulte Indicadores de riesgo de usuario de Citrix.

### ¿Cómo analizar el indicador de riesgo de descarga excesiva de datos?

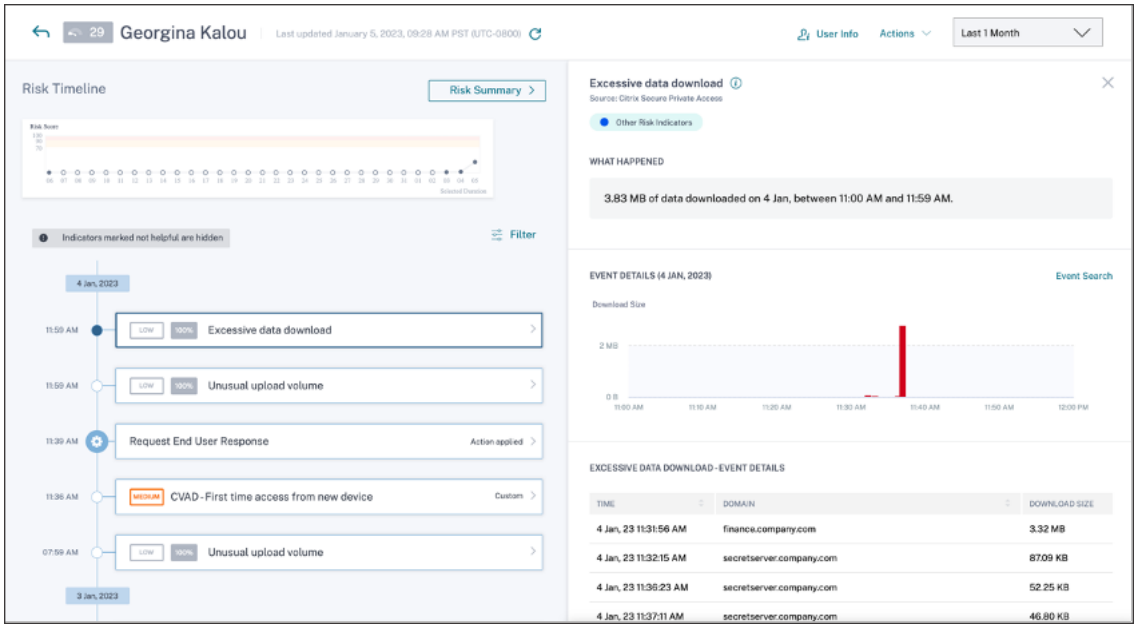
Considere un usuario Georgina Kalou, descargó el exceso de volumen de datos de una aplicación o sitio web. Secure Private Access informa de estos eventos a Citrix Analytics, que asigna una puntuación de riesgo actualizada a Georgina Kalou y agrega la entrada del indicador de riesgo de **descarga excesiva de datos** a la línea de tiempo de riesgo del usuario.

En el cronograma de riesgo de Georgina Kalou, puede seleccionar el indicador de riesgo de **descarga excesiva de datos** notificado. El motivo del evento se muestra junto con los detalles sobre los eventos, como los detalles de hora y dominio.

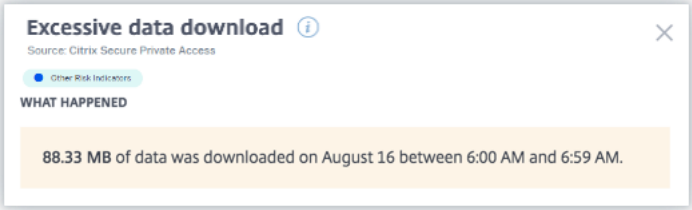
Para ver el indicador de riesgo de **descarga excesiva de datos**, vaya a **Seguridad > Usuarios** y seleccione el usuario.

Al seleccionar la entrada del indicador Riesgo de **descarga excesiva de datos** de la línea de tiempo, aparece un panel de información detallada correspondiente en el panel derecho.

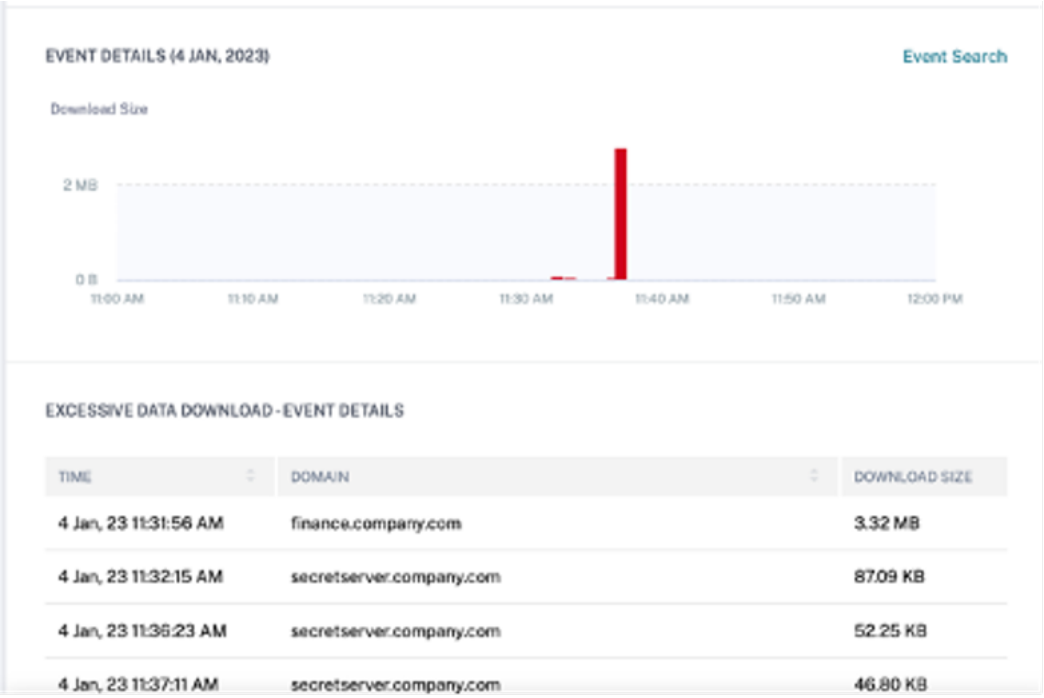



- La sección **QUÉ SUCEDIÓ** proporciona un breve resumen del indicador de riesgo, incluido el volumen de datos cargados y descargados durante el período seleccionado.




- La sección **DETALLES DEL EVENTO** incluye una visualización cronológica de los eventos de descarga de datos individuales que se produjeron durante el período de tiempo seleccionado. Además, puede ver la siguiente información clave sobre cada evento:
  - **¡Hora**! El momento en que se descargaron los datos excesivos en una aplicación o en un sitio web.
  - **Dominio**. Dominio en el que el usuario ha descargado los datos.
  - **Tamaño de descarga**. Volumen de datos descargados en el dominio.




### ¿Qué acciones puede aplicar al usuario?

Puede realizar las siguientes acciones en la cuenta del usuario:

- **Agregar a la lista de seguimiento**. Cuando quiera supervisar a un usuario en busca de futuras amenazas potenciales, puede agregarlas a una lista de seguimiento.
- **Notificar a los administradores**. Cuando hay alguna actividad inusual o sospechosa en la cuenta del usuario, se envía una notificación por correo electrónico a todos los administradores o a los seleccionados.

Para obtener más información sobre las acciones y cómo configurarlas manualmente, consulte Directivas y acciones.

Para aplicar las acciones al usuario manualmente, desplácese hasta el perfil del usuario y seleccione el indicador de riesgo adecuado. En el menú **Acciones**, seleccione una acción y haga clic en **Aplicar**.

> **Nota**
>
> Independientemente del origen de datos que desencadena un indicador de riesgo, se pueden aplicar acciones relacionadas con otros orígenes de datos.

# Indicadores de riesgo de Citrix Virtual Apps and Desktops y Citrix DaaS

July 12, 2022

## Trayecto imposible

Citrix Analytics detecta los inicios de sesión de un usuario como arriesgados cuando los inicios de sesión consecutivos proceden de dos países diferentes dentro de un período de tiempo inferior al tiempo de trayecto esperado entre los países.

El caso de tiempo de trayecto imposible indica estos riesgos:

- **Credenciales en riesgo**: Un atacante remoto roba las credenciales de un usuario legítimo.
- **Credenciales compartidas**: Diferentes usuarios utilizan las mismas credenciales de usuario.

### ¿Cuándo se activa el indicador de riesgo de trayecto imposible?

El indicador de riesgo de **trayecto imposible** evalúa el tiempo y la distancia estimada entre cada par de inicios de sesión de usuario consecutivos y se activa cuando la distancia es mayor de lo que una persona individual puede recorrer en ese período de tiempo.

> **Nota**
>
> Este indicador de riesgo también contiene una lógica para reducir las alertas de falsos positivos en las siguientes situaciones que no reflejan las ubicaciones reales de los usuarios:
>
> - Cuando los usuarios inician sesión en aplicaciones y escritorios virtuales desde conexiones proxy.
> - Cuando los usuarios inician sesión en aplicaciones y escritorios virtuales desde clientes alojados.

### Cómo analizar el indicador de riesgo imposible

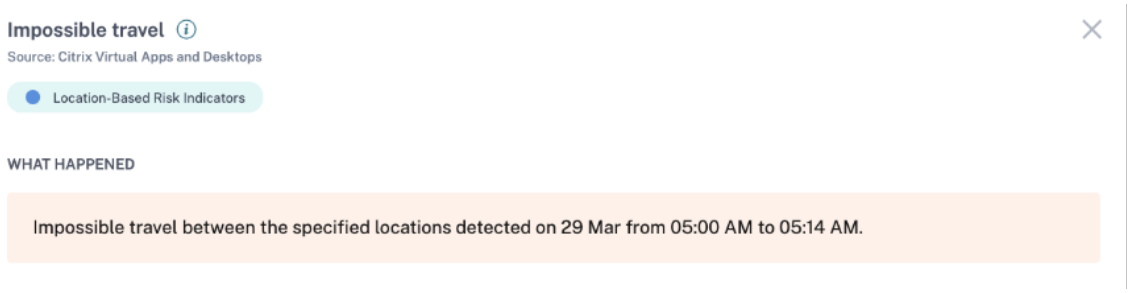
Considere al usuario Adam Maxwell, que inicia sesión desde dos ubicaciones, Moscú (Rusia) y Hohhot (China), en un tiempo de un minuto. Citrix Analytics detecta este evento de inicio de sesión como un caso de trayecto imposible y activa el indicador de riesgo de **trayecto imposible**. El indicador de riesgo se agrega al cronograma de riesgo de Adam Maxwell y se le asigna una puntuación de riesgo.

Para ver el cronograma de riesgo de Adam Maxwell, seleccione **Seguridad > Usuarios**. En el panel **Usuarios con riesgos**, seleccione el usuario Adam Maxwell.

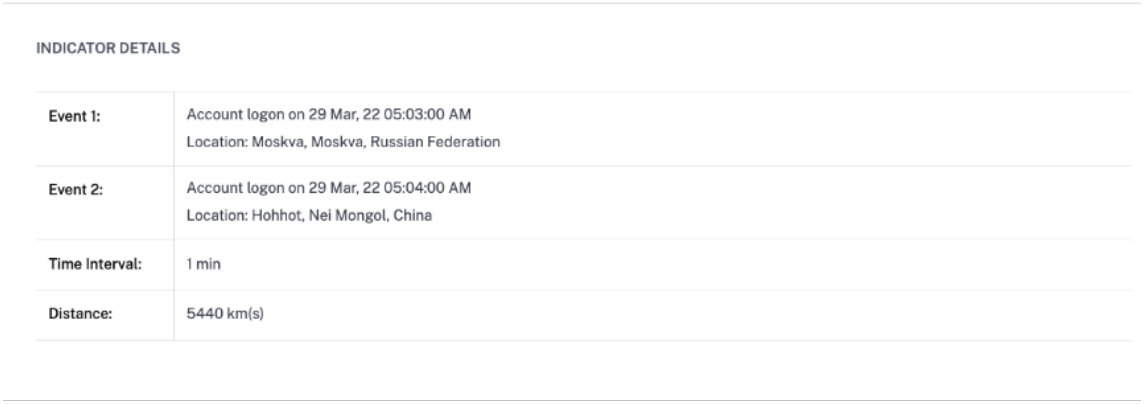
 

En la cronología de riesgo de Adam Maxwell, seleccione el indicador de riesgo de **trayecto imposible**. Puede ver la siguiente información:

- La sección **QUÉ HA OCURRIDO** ofrece un breve resumen del evento de trayecto imposible.

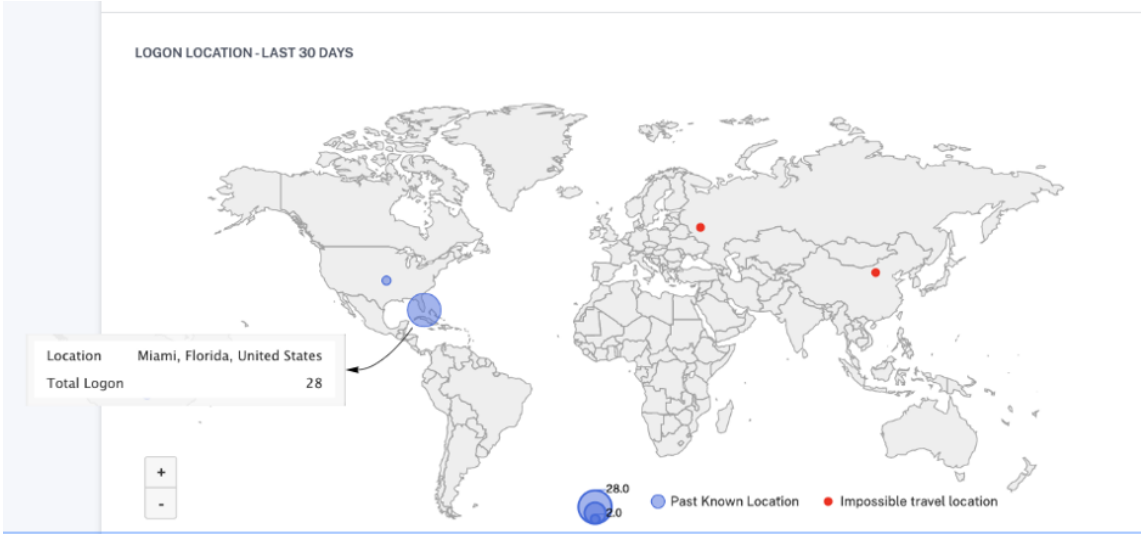



- La sección **DETALLES DEL INDICADOR** proporciona las ubicaciones desde las que el usuario ha iniciado sesión, el tiempo transcurrido entre los inicios de sesión consecutivos y la distancia entre las dos ubicaciones.

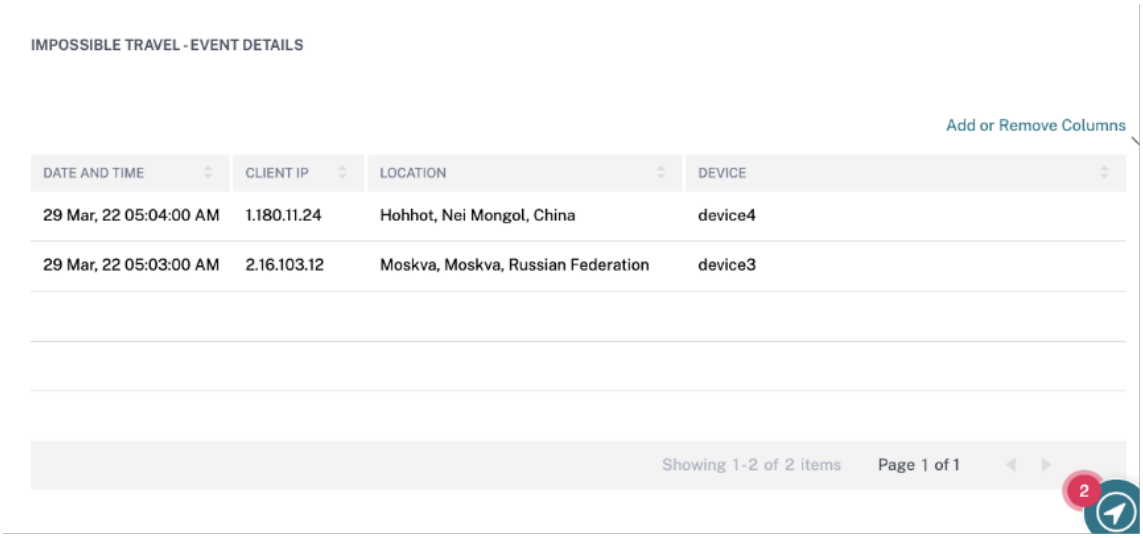



- La sección **UBICACIÓN DE INICIO DE SESIÓN: ÚLTIMOS 30 DÍAS** muestra una vista de mapa geográfico de las ubicaciones de trayecto imposible y las ubicaciones conocidas del usuario. Los datos de ubicación se muestran durante los últimos 30 días. Puede pasar el ratón por encima de los punteros del mapa para ver el total de inicios de sesión de cada ubicación.




- La sección **TRAYECTO IMPOSIBLE: DETALLES DEL EVENTO** proporciona la siguiente información sobre el evento de trayecto imposible:
  - **Fecha y hora**: Indica la fecha y la hora de los inicios de sesión.
  - **IP del cliente**: indica la dirección IP del dispositivo del usuario.
  - **Ubicación**: indica la ubicación desde la que el usuario ha iniciado sesión.
  - **Dispositivo**: indica el nombre del dispositivo del usuario.
  - **Tipo de inicio de sesión**: indica si la actividad del usuario es el inicio de sesión o el inicio de sesión de la cuenta. El evento de inicio de sesión de la cuenta se activa cuando la autenticación de un usuario en su cuenta se realiza correctamente. Mientras que el evento de inicio de sesión se activa cuando un usuario introduce su credencial e inicia sesión en su aplicación o sesión de escritorio.
  - **SO**: indica el sistema operativo del dispositivo del usuario.
  - **Explorador**: indica el explorador web que se utiliza para acceder a la aplicación.



#### ¿Qué acciones puede aplicar a los usuarios?

Puede realizar las siguientes acciones en la cuenta del usuario:

- **Agregar a la lista de seguimiento**. Cuando quiera supervisar a un usuario en busca de futuras amenazas potenciales, puede agregarlas a una lista de seguimiento.
- **Notificar a los administradores**. Cuando hay alguna actividad inusual o sospechosa en la cuenta del usuario, se envía una notificación por correo electrónico a todos los administradores o a los administradores seleccionados.
- **Cierre la sesión del usuario**. Cuando se desactiva la sesión de un usuario de su cuenta, no puede acceder al recurso a través de escritorios virtuales.
- **Inicie la grabación de la sesión**. Si se produce un evento inusual en la cuenta de escritorios virtuales del usuario, el administrador puede empezar a registrar las actividades del usuario en futuras sesiones de inicio de sesión. Sin embargo, si el usuario está en Citrix Virtual Apps and Desktops 7.18 o posterior, el administrador puede iniciar y detener dinámicamente la grabación de la sesión de inicio de sesión actual del usuario.

Para obtener más información sobre las acciones y cómo configurarlas manualmente, consulte Directivas y acciones.

Para aplicar las acciones al usuario manualmente, vaya al perfil del usuario y seleccione el indicador de riesgo correspondiente. En el menú **Acción**, seleccione una acción y haga clic en **Aplicar**.

> **Nota**
>
> Independientemente del origen de datos que desencadena un indicador de riesgo, se pueden aplicar acciones relacionadas con otros orígenes de datos.

### Exfiltración potencial de datos

Citrix Analytics detecta amenazas a los datos basándose en intentos excesivos de filtración de datos y activa el indicador de riesgo correspondiente.

El factor de riesgo asociado con el indicador de riesgo potencial de exfiltración de datos son los indicadores de riesgo basados en datos. Para obtener más información sobre los factores de riesgo, consulte Indicadores de riesgo de usuario de Citrix.

El indicador de riesgo **potencial de filtración de datos** se activa cuando un usuario de Citrix Receiver intenta descargar o transferir archivos a una unidad o impresora. Estos datos pueden ser un evento de descarga de archivos, como descargar un archivo en una unidad local, unidades asignadas o un dispositivo de almacenamiento externo. Los datos también se pueden exfiltrar mediante el portapapeles o mediante la acción de copiar y pegar.

> **Nota**
>
> Las operaciones del portapapeles solo son compatibles con las aplicaciones SaaS.

### ¿Cuándo se activa el indicador de riesgo potencial de exfiltración de datos?

Se le puede notificar cuando un usuario ha transferido un número excesivo de archivos a una unidad o impresora en un período de tiempo determinado. Este indicador de riesgo también se activa cuando el usuario utiliza la acción copiar y pegar en su equipo local.

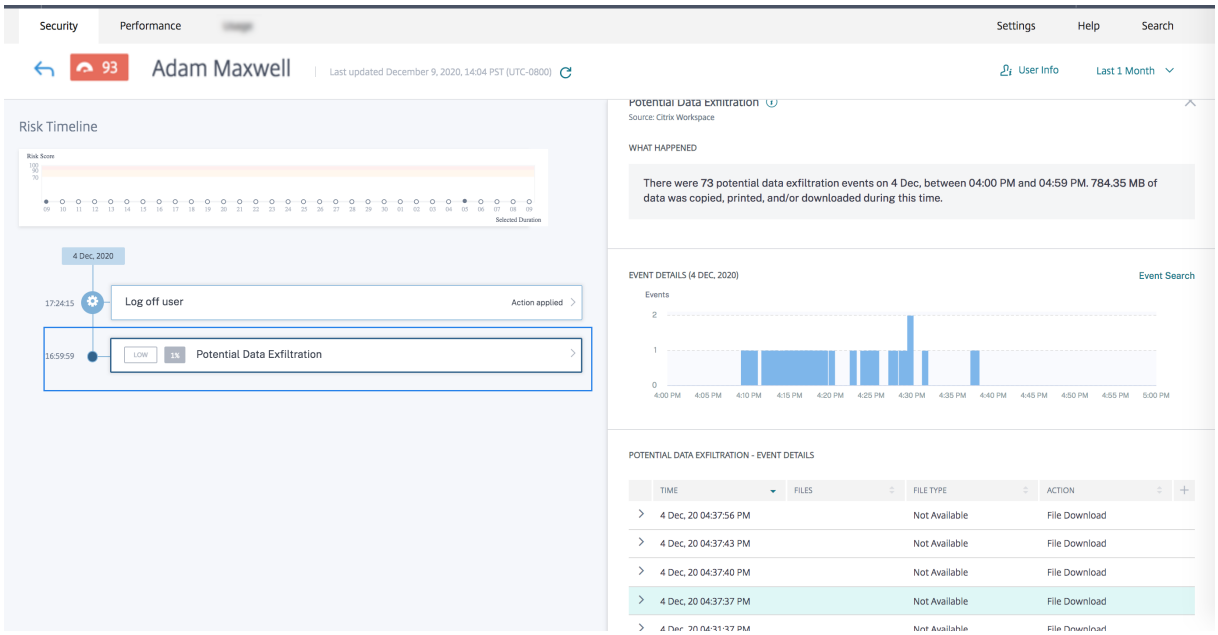
Cuando Citrix Receiver detecta este comportamiento, Citrix Analytics recibe este evento y asigna una puntuación de riesgo al usuario respectivo. El indicador de riesgo **potencial de exfiltración de datos** se agrega al cronograma de riesgo del usuario.

### ¿Cómo analizar el Indicador de riesgo potencial de exfiltración de datos?

Piense en el usuario Adam Maxwell, que ha iniciado sesión en una sesión e intenta imprimir archivos que superan el límite predefinido. Con esta acción, Adam Maxwell había excedido su comportamiento normal de transferencia de archivos basado en algoritmos de aprendizaje automático.

En el cronograma de Adam Maxwell, puede seleccionar el indicador de riesgo **potencial de exfiltración de datos**. El motivo del evento se muestra junto con los detalles como los archivos transferidos y el dispositivo utilizado para transferir el archivo.

Para ver el indicador de riesgo **potencial de exfiltración de datos** notificado para un usuario, vaya a **Seguridad > Usuarios**y seleccione el usuario.



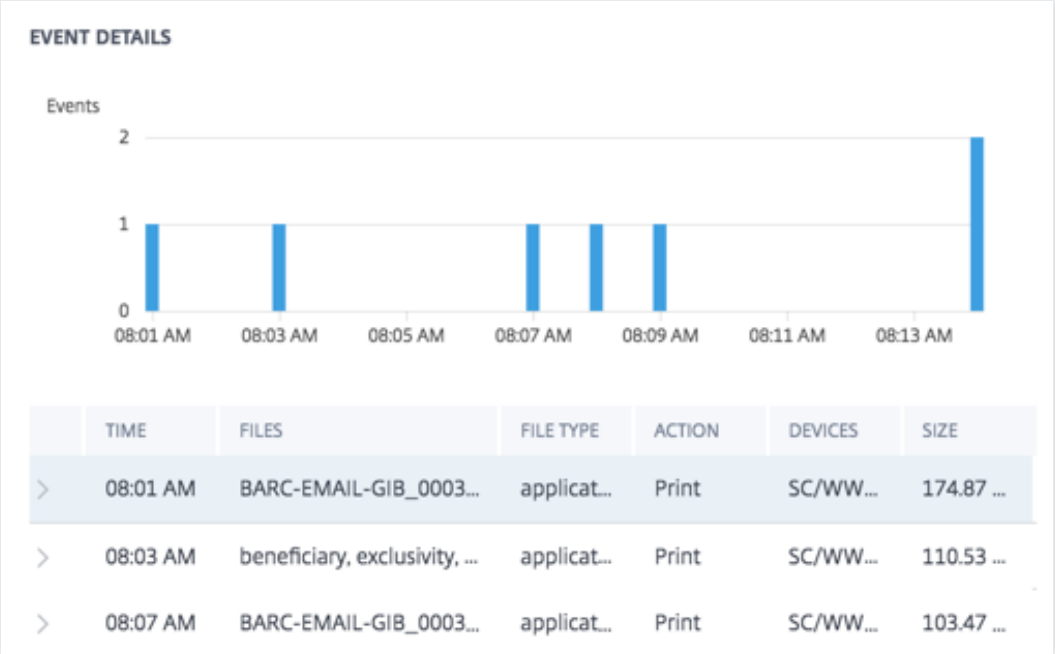
- En la sección **QUÉ PASÓ**, puede ver el resumen del posible evento de filtración de datos. Puede ver el número de eventos de exfiltración de datos durante un período de tiempo específico.


- En la sección **DETALLES DEL EVENTO**, los intentos de exfiltración de datos aparecen en formato gráfico y tabular. Los eventos aparecen como entradas individuales en el gráfico y la tabla proporciona la siguiente información clave:
  - **Tiempo**. Hora en que se produjo el evento de exfiltración de datos.
  - **Archivos**. El archivo que se descargó, imprimió o copió.
  - **Tipo de archivo**. Tipo de archivo descargado, impreso o copiado.

    > **Nota**
    >
    > El nombre del archivo impreso solo está disponible en el evento de impresión de aplicaciones SaaS.

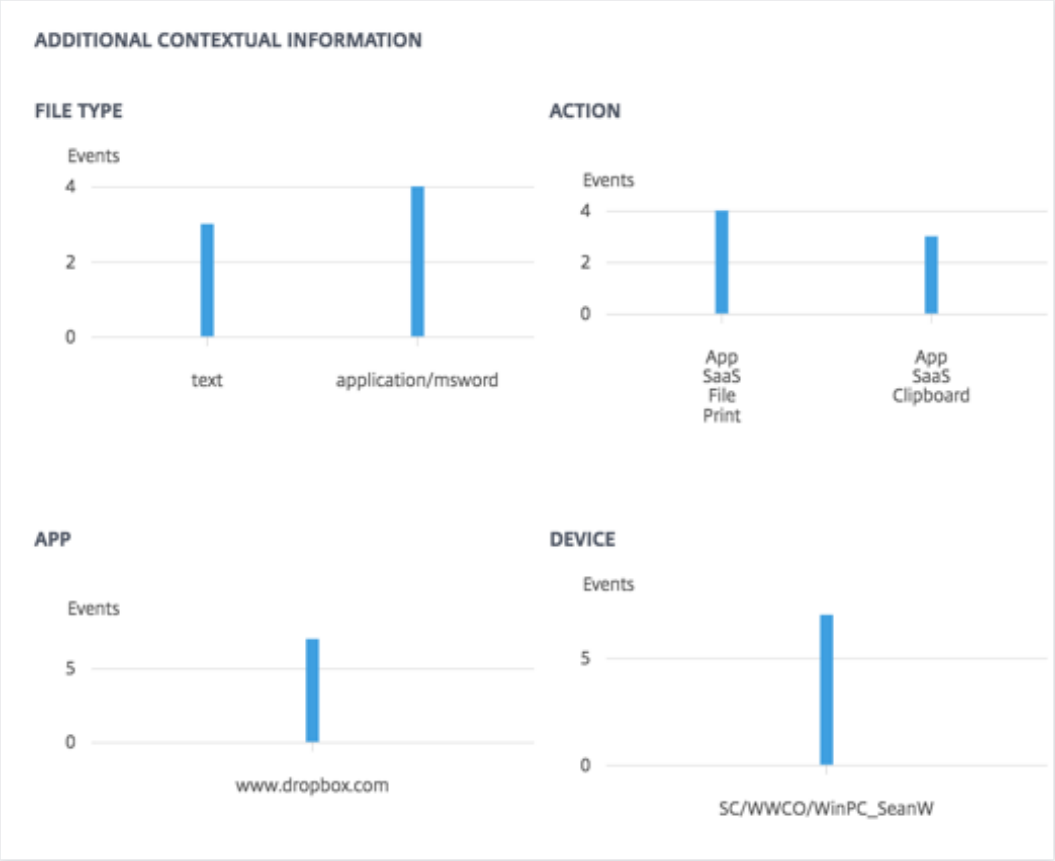
  - **Acción**. Los tipos de sucesos de filtración de datos que se realizaron: impresión, descarga o copia.
  - **Dispositivos**. El dispositivo utilizado.
  - **Talla** El tamaño del archivo que se exfiltra.
  - **Localización**. La ciudad desde la que el usuario intenta exfiltrar datos.




- En la sección **INFORMACIÓN CONTEXTUAL ADICIONAL**, durante la ocurrencia del evento, puede ver lo siguiente:
  - La cantidad de archivos que se han filtrado.
  - Las acciones realizadas.
  - Las aplicaciones utilizadas.
  - Dispositivo utilizado por el usuario.




**¿Qué acciones puede aplicar al usuario?**

Puede realizar las siguientes acciones en la cuenta del usuario:

- **Agregar a la lista de seguimiento**. Cuando quiera supervisar a un usuario en busca de futuras amenazas potenciales, puede agregarlas a una lista de seguimiento.
- **Notificar a los administradores**. Cuando hay alguna actividad inusual o sospechosa en la cuenta del usuario, se envía una notificación por correo electrónico a todos los administradores o a los seleccionados.
- **Cierre la sesión del usuario**. Cuando se desactiva la sesión de un usuario de su cuenta, no puede acceder al recurso a través de escritorios virtuales.
- **Inicie la grabación de la sesión**. Si se produce un evento inusual en la cuenta de escritorios virtuales del usuario, el administrador puede empezar a registrar las actividades del usuario en futuras sesiones de inicio de sesión. Sin embargo, si el usuario tiene la versión 7.18 de Citrix Virtual Apps and Desktops o una posterior, el administrador puede iniciar y detener la grabación de la sesión de inicio de sesión actual del usuario de forma dinámica.

Para obtener más información sobre las acciones y cómo configurarlas manualmente, consulte Directivas y acciones.

Para aplicar las acciones al usuario manualmente, desplácese hasta el perfil del usuario y seleccione el indicador de riesgo adecuado. En el menú **Acción**, seleccione una acción y haga clic en **Aplicar**.

> **Nota**
>
> Independientemente del origen de datos que desencadena un indicador de riesgo, se pueden aplicar acciones relacionadas con otros orígenes de datos.

## Inicio de sesión sospechoso

Citrix Analytics detecta los inicios de sesión del usuario que parecen inusuales o con riesgos en función de varios factores contextuales, definidos conjuntamente por el dispositivo, la ubicación y la red que utiliza el usuario.

### ¿Cuándo se activa el indicador de riesgo de inicio de sesión sospechoso?

El indicador de riesgo se activa mediante la combinación de los siguientes factores, en los que cada factor se considera potencialmente sospechoso en función de una o más condiciones.

| Factor | Condiciones |
| --- | --- |
| Dispositivo inusual | El usuario inicia sesión desde un dispositivo que no se ha utilizado en los últimos 30 días.<br><br>El usuario inicia sesión desde un cliente HTML5 o un cliente Chrome en el que la firma del dispositivo no coincide con el historial del usuario. |
| Ubicación inusual | Inicie sesión desde una ciudad o un país en el que el usuario no haya iniciado sesión en los últimos 30 días.<br>La ciudad o el país están geográficamente lejos de las ubicaciones de inicio de sesión recientes (últimos 30 días).<br>Ninguno o un mínimo de usuarios han iniciado sesión desde la ciudad o el país en los últimos 30 días. |

| Factor | Condiciones |
| --- | --- |
| Red inusual | Inicie sesión desde una dirección IP que el usuario no ha utilizado en los últimos 30 días.<br>Inicie sesión desde una subred IP que el usuario no ha utilizado en los últimos 30 días.<br>Ningún usuario o mínimo ha iniciado sesión desde la subred IP en los últimos 30 días. |
| Amenaza IP | La dirección IP se identifica como de alto riesgo por el feed de inteligencia de amenazas de la comunidad: Webroot.<br>Citrix Analytics ha detectado recientemente actividades de inicio de sesión muy sospechosas desde la dirección IP de otros usuarios. |

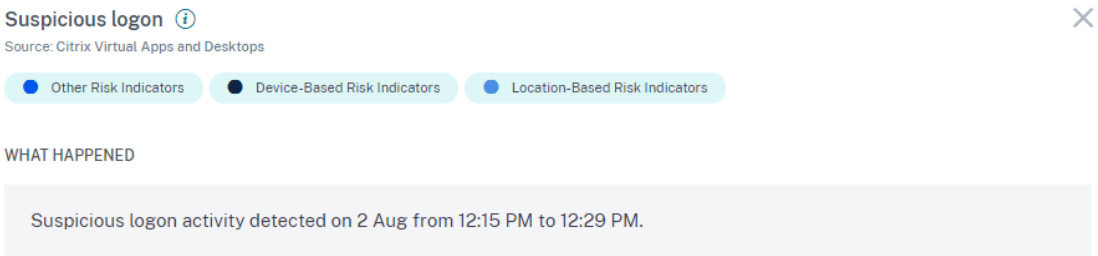
**Cómo analizar el indicador de riesgo de inicio de sesión sospechoso**

Piense en el usuario Adam Maxwell, que inicia sesión desde Mumbai, India por primera vez. Usa un dispositivo nuevo o un dispositivo que no se usó durante los últimos 30 días para iniciar sesión en Citrix Virtual Apps and Desktops y conectarse a una red nueva. Citrix Analytics detecta este evento de inicio de sesión como sospechoso porque los factores: ubicación, dispositivo y red se desvían de su comportamiento habitual y desencadena el indicador de riesgo de inicio de **sesión sospechoso**. El indicador de riesgo se agrega al cronograma de riesgo de Adam Maxwell y se le asigna una puntuación de riesgo.

Para ver el tiempo de riesgo de Adam Maxwell, seleccione **Seguridad > Usuarios**. En el panel **Usuarios con riesgos**, seleccione el usuario Adam Maxwell.

En la línea de tiempo de riesgo de Adam Maxwell, seleccione el indicador de riesgo de inicio de sesión sospechoso. Puede ver la siguiente información:

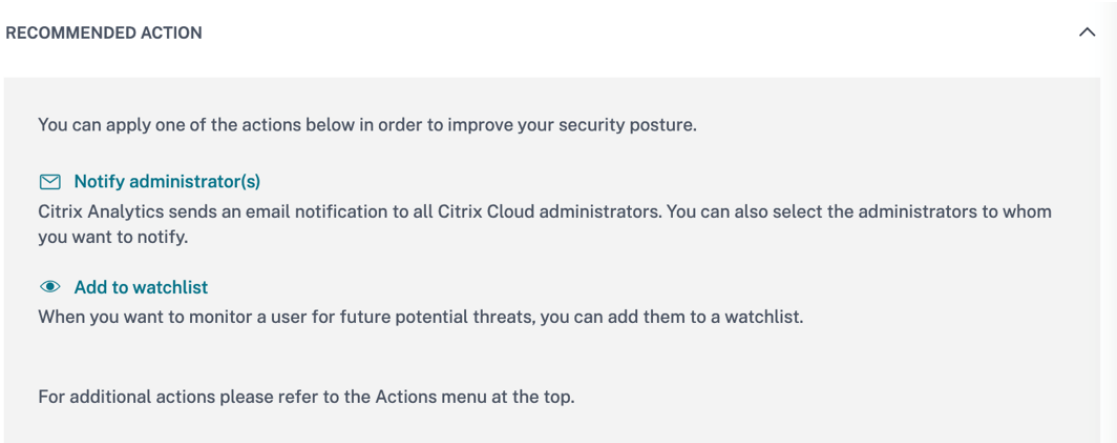
- La sección **QUÉ SUCEDIÓ** proporciona un breve resumen de las actividades sospechosas que incluyen los factores de riesgo y el momento del evento.



- En la sección **ACCIÓN RECOMENDADA**, encontrará las acciones sugeridas que se pueden aplicar en el indicador de riesgo. Citrix Analytics for Security recomienda las acciones en función de la gravedad del riesgo que presente el usuario. La recomendación puede ser una o una combinación de las siguientes acciones:
  - Notificar a los administradores
  - Agregar a la lista de seguimiento
  - Crear una directiva

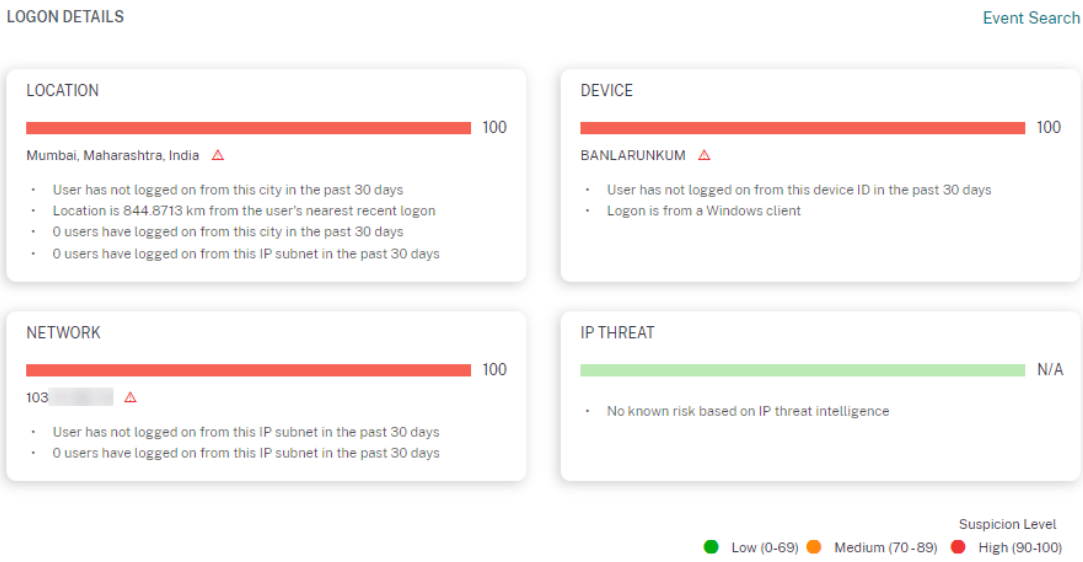
  Puede seleccionar una acción en función de la recomendación. O puede seleccionar una acción que quiera aplicar en función de su elección en el menú **Acciones**. Para obtener más información, consulte Aplicar una acción manualmente.




- La sección **DETALLES DE INICIO DE SESIÓN** proporciona un resumen detallado de las actividades sospechosas correspondientes a cada factor de riesgo. A cada factor de riesgo se le asigna una puntuación que indica el nivel de sospecha. Un factor de riesgo único no indica un riesgo elevado por parte de un usuario. El riesgo global se basa en la correlación de los múltiples factores de riesgo.

| Nivel de sospecha | Indicación |
|---|---|
| 0–69 | El factor parece normal y no se considera sospechoso. |
| 70–89 | El factor parece un poco inusual y se considera moderadamente sospechoso con otros factores. |
| 90–100 | El factor es totalmente nuevo o inusual y se considera altamente sospechoso con otros factores. |



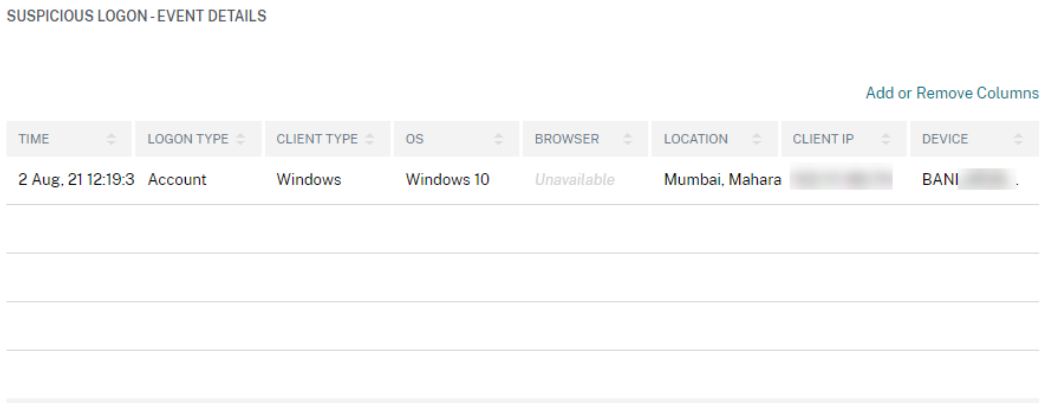

- La sección **UBICACIÓN DE INICIO DE SESIÓN: ÚLTIMOS 30 DÍAS** muestra una vista de mapa geográfico de las últimas ubicaciones conocidas y la ubicación actual del usuario. Los datos de ubicación se muestran durante los últimos 30 días. Puede pasar el ratón por encima de los punteros del mapa para ver el total de inicios de sesión de cada ubicación.


- La sección **DETALLES DEL EVENTO DE INICIO DE SESIÓN SOSPECHOSO** proporciona la siguiente información sobre el evento de inicio de sesión sospechoso:
  - **Hora**: indica la fecha y la hora del inicio de sesión sospechoso.
  - **Tipo de inicio de sesión**: indica si la actividad del usuario es el inicio de sesión o el inicio de sesión de la cuenta. El evento de inicio de sesión de cuenta se desencadena cuando la

autenticación de un usuario en su cuenta se realiza correctamente. Mientras que el evento de inicio de sesión se activa cuando un usuario introduce su credencial e inicia sesión en su aplicación o sesión de escritorio.

- **Tipo de cliente**: indica el tipo de aplicación Citrix Workspace instalada en el dispositivo del usuario. Según el sistema operativo del dispositivo del usuario, el tipo de cliente puede ser Android, iOS, Windows, Linux, Mac, etc.
- **SO**: indica el sistema operativo del dispositivo del usuario.
- **Explorador**: indica el explorador web que se utiliza para acceder a la aplicación.
- **Ubicación**: indica la ubicación desde la que el usuario ha iniciado sesión.
- **IP del cliente**: indica la dirección IP del dispositivo del usuario.
- **Dispositivo**: indica el nombre del dispositivo del usuario.




### ¿Qué acciones puede aplicar a los usuarios?

Puede realizar las siguientes acciones en la cuenta del usuario:

- **Agregar a la lista de seguimiento**. Cuando quiera supervisar a un usuario en busca de futuras amenazas potenciales, puede agregarlas a una lista de seguimiento.
- **Notificar a los administradores**. Cuando hay alguna actividad inusual o sospechosa en la cuenta del usuario, se envía una notificación por correo electrónico a todos los administradores o a los seleccionados.
- **Cierre la sesión del usuario**. Cuando se desactiva la sesión de un usuario de su cuenta, no puede acceder al recurso a través de escritorios virtuales.
- **Inicie la grabación de la sesión**. Si se produce un evento inusual en la cuenta de escritorios virtuales del usuario, el administrador puede empezar a registrar las actividades del usuario en futuras sesiones de inicio de sesión. Sin embargo, si el usuario tiene la versión 7.18 de Citrix

Virtual Apps and Desktops o una posterior, el administrador puede iniciar y detener la grabación de la sesión de inicio de sesión actual del usuario de forma dinámica.

Para obtener más información sobre las acciones y cómo configurarlas manualmente, consulte Directivas y acciones.

Para aplicar las acciones al usuario manualmente, desplácese hasta el perfil del usuario y seleccione el indicador de riesgo adecuado. En el menú **Acción**, seleccione una acción y haga clic en **Aplicar**.

> **Nota**
>
> Independientemente del origen de datos que desencadena un indicador de riesgo, se pueden aplicar acciones relacionadas con otros orígenes de datos.

## Proporcione comentarios sobre los indicadores de riesgo del usuario

October 18, 2022

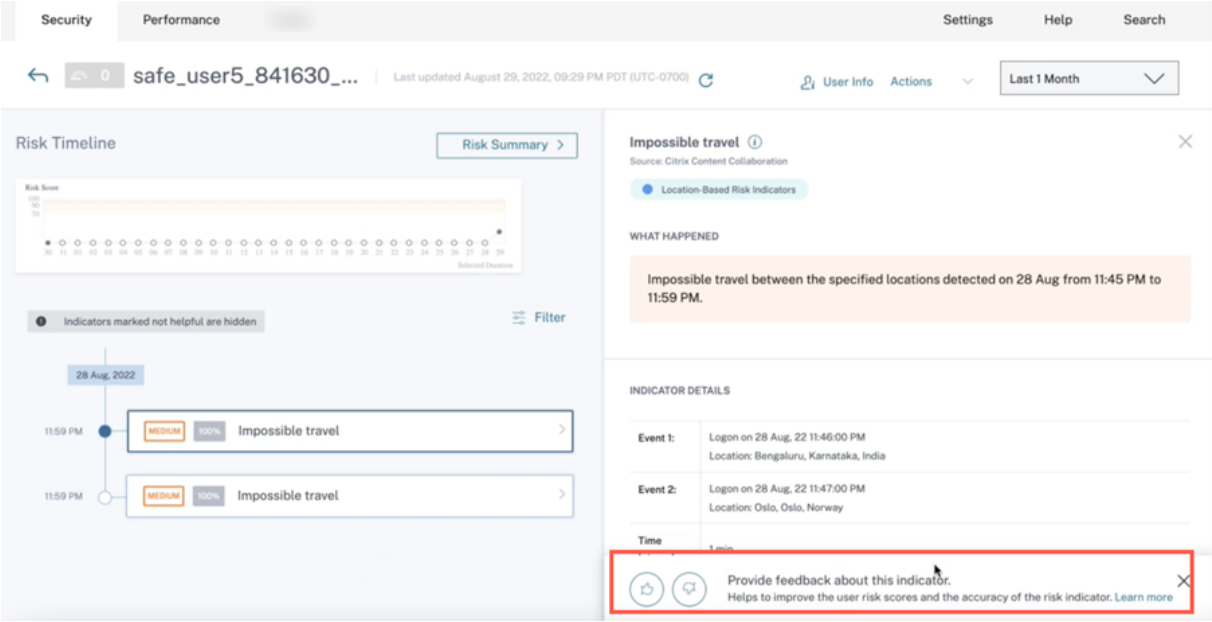
Los indicadores de riesgo están diseñados para detectar y reportar actividades de usuarios potencialmente sospechosas o anómalas, a la vez que aumentan automáticamente la puntuación de riesgo del usuario. En la práctica, aunque algunos casos de un indicador de riesgo corresponden a una amenaza de seguridad subyacente legítima, otros resultan ser benignos.

La función de retroalimentación de los indicadores le permite marcar explícitamente las ocurrencias de los indicadores de riesgo:

- Tan útil cuando crees que existe un verdadero riesgo subyacente para el usuario
- No es útil si ha determinado que no hay ninguna amenaza a la seguridad. En este caso, la aparición del indicador se oculta en la cronología del usuario de forma predeterminada y la puntuación de riesgo del usuario se ajusta automáticamente para excluir la aparición de este indicador en los cálculos posteriores.

Además, sus comentarios colectivos se utilizan para impulsar futuras mejoras en los algoritmos de los indicadores de riesgo.

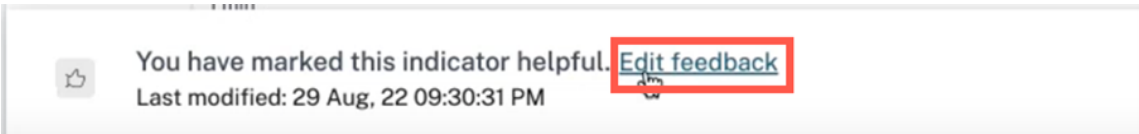
 




Se muestra un banner de comentarios (con un icono con el pulgar hacia arriba y hacia abajo) para cada entrada del indicador de riesgo predeterminado en la cronología del usuario.

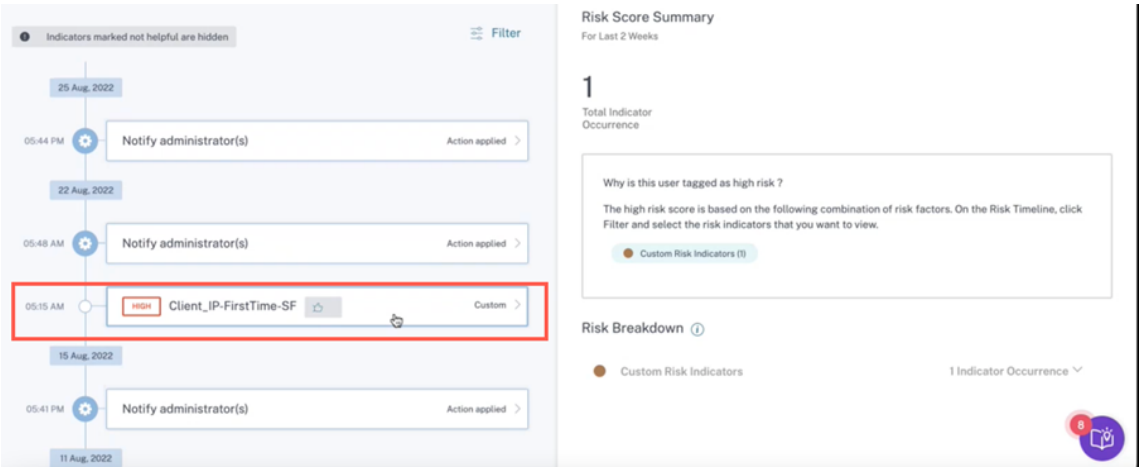
- Icono**con el pulgar hacia arriba** : el indicador es útil y ha identificado correctamente la actividad de riesgo. Puede hacer clic en el icono del pulgar hacia arriba y proporcionar comentarios adicionales sobre la utilidad del indicador y sus beneficios.

  Puede guardar sus comentarios y marcar el indicador como útil. También puedes editar tu comentario haciendo clic en Editar comentarios. El banner de comentarios muestra el cronograma de los últimos comentarios enviados.

  Cuando un indicador de riesgo se marca como útil, estos comentarios se muestran en la entrada correspondiente del cronograma del usuario y se notifican a Citrix Analytics. La puntuación de riesgo del usuario no se ve afectada.

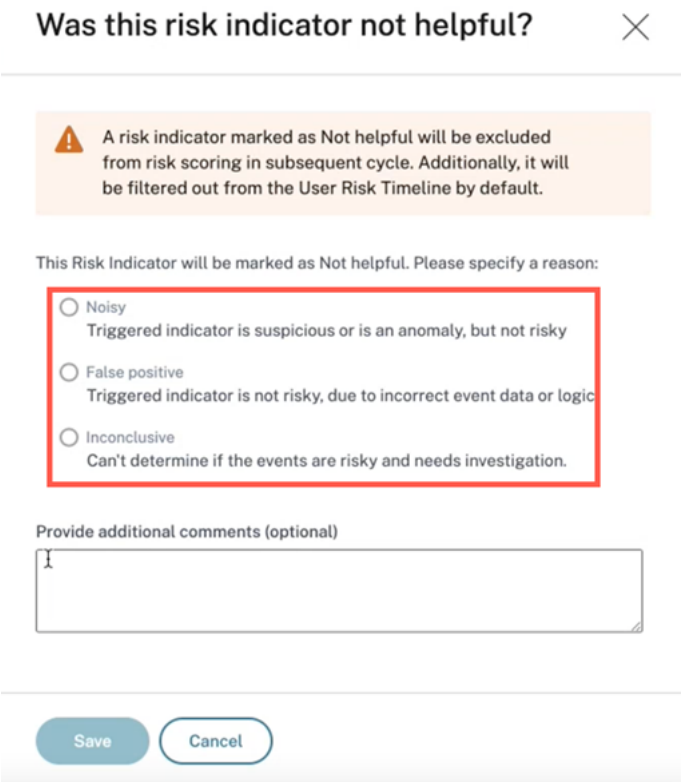
 




- Icono con el**pulgar hacia abajo** : el indicador no es útil o se activa incorrectamente. Puede marcar el indicador como poco útil y clasificarlo como **Ruidoso**, **Falso positivo**o No **concluyente**. Esta aparición del indicador de riesgo se excluirá de todas las actualizaciones posteriores de la puntuación de riesgo del usuario. También puede proporcionar comentarios adicionales, si es necesario.
  - **Ruidoso** : el indicador activado es sospechoso o es una anomalía, pero no es riesgoso.
  - **Falso positivo** : el indicador activado no es riesgoso porque los datos o la lógica del evento son incorrectos.
  - No**es concluyente** : no se puede determinar si los eventos son riesgosos y requieren una investigación.

    > **Nota**
    >
    > Se necesitan hasta 15 minutos para recalibrar la puntuación de riesgo.



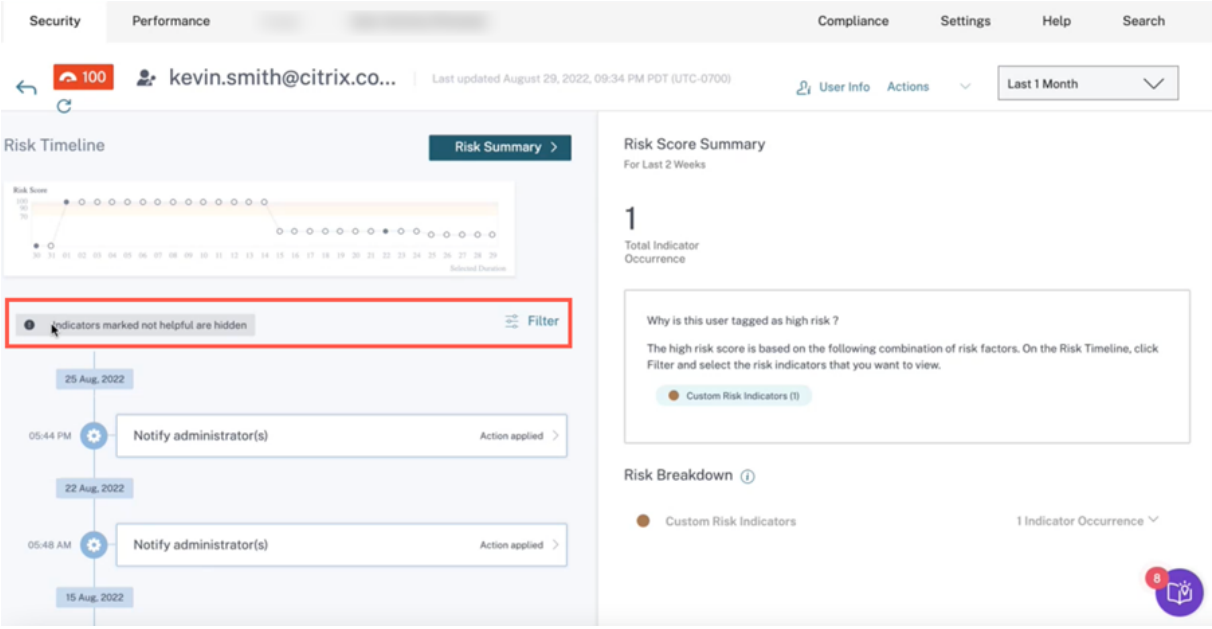

Puede ver los siguientes resultados si un indicador está marcado como no útil:

- Ese indicador en particular está oculto en el cronograma.
- La puntuación de riesgo se recalibra como resultado de excluir la aparición de este indicador del cálculo de la puntuación de riesgo en actualizaciones posteriores.
- Cualquier información adicional proporcionada como comentario textual se conserva para referencia posterior.

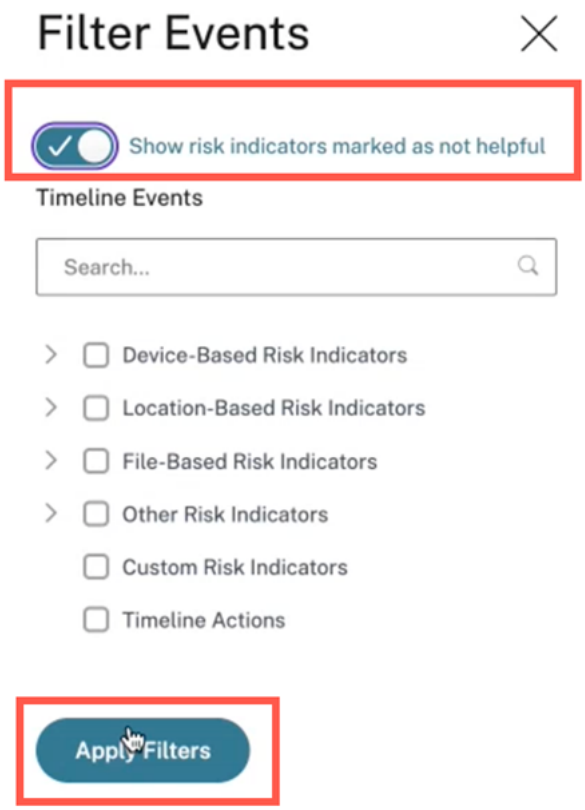
### Ver filtros

Los indicadores que están marcados como no útiles se ocultan de forma predeterminada.



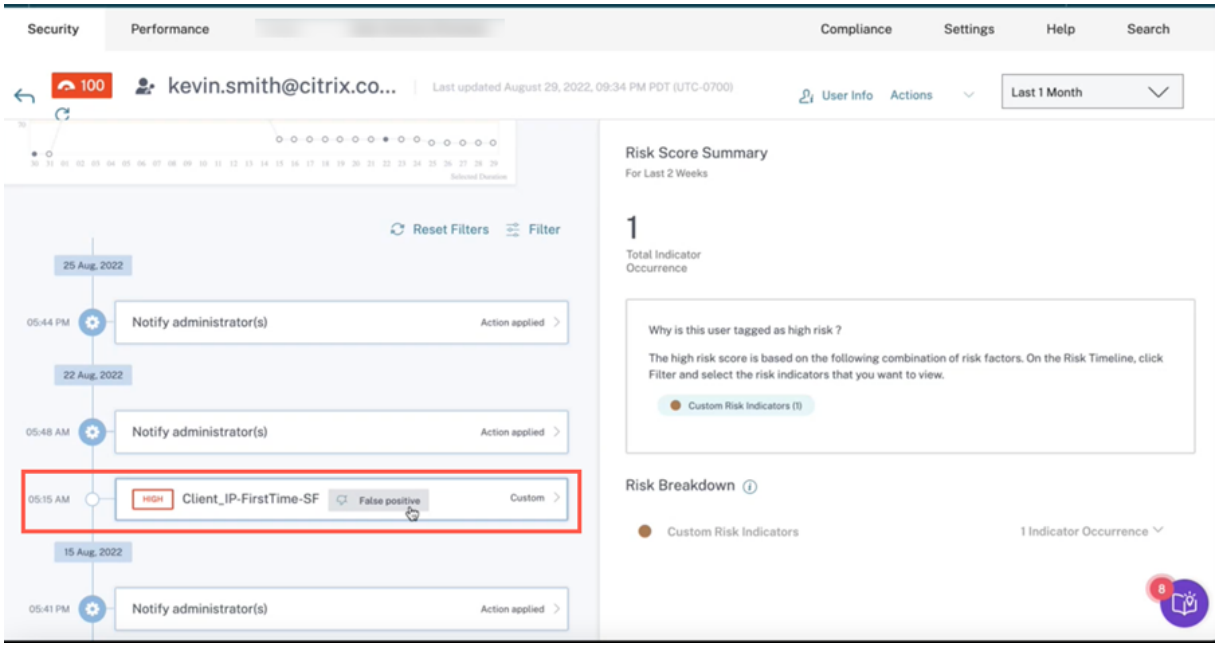

Para ver los indicadores ocultos, haga clic en **Filtrar**. En la ventana **Filtrar eventos** que aparece, active **Mostrar indicadores de riesgo marcados como no útiles**.




Puede buscar los indicadores en función de las categorías. Por ejemplo, para ver los indicadores de

riesgo ocultos basados en la ubicación, seleccione la categoría y haga clic en **Aplicar filtros**. Puedes ver todos los indicadores basados en la ubicación que no son útiles con los detalles de los comentarios.




Como administrador, también puede realizar las siguientes acciones según sea necesario:

- Cambiar los comentarios
- Revise los comentarios anteriores y los metadatos asociados
- Revise los comentarios proporcionados por otro administrador y los metadatos asociados

> **Nota**
>
> - Puede proporcionar los comentarios por nivel de usuario, no por nivel de inquilino. La retroalimentación de un indicador de riesgo no se aplica a todos los casos de ese indicador de riesgo en particular.
> - Los comentarios de un usuario no se aplican a los demás usuarios.

## Indicadores de riesgo para Microsoft Graph Security

September 11, 2024

> **Nota:**
>
> Desde julio de 2023, Microsoft cambió el nombre de Azure Active Directory (Azure AD) a Microsoft

> Entra ID. En este documento, cualquier referencia a Azure Active Directory, Azure AD o AAD ahora se refiere a Microsoft Entra ID.

Microsoft Graph Security recibe datos de los proveedores de seguridad de **Azure AD Identity Protection** o **Microsoft Defender for Endpoint** y envía la información a Citrix Analytics.

Azure AD Identity Protection activa los siguientes indicadores de riesgo y envía la información a Microsoft Graph Security:

- Dirección IP anónima
- Viaje imposible a lugares atípicos
- Usuarios con credenciales filtradas
- Inicios de sesión desde dispositivos infectados
- Inicios de sesión desde direcciones IP con actividad sospechosa
- Inicios de sesión desde ubicaciones desconocidas

Para obtener información sobre Defender for Endpoint, consulte Microsoft Defender para Endpoint.

El factor de riesgo asociado a los indicadores de riesgo son los indicadores de riesgo basados en IP. Para obtener más información sobre los factores de riesgo, consulte Indicadores de riesgo de usuario de Citrix.

### Cómo analizar los indicadores de riesgo de Microsoft Graph Security

Piense en una usuaria Maria Brown que exhibe uno de los comportamientos de riesgo mencionados anteriormente. Microsoft detecta el incidente y genera una alerta. Citrix Analytics recupera esta alerta y asigna una puntuación de riesgo actualizada a Maria Brown. Además, se agrega el indicador de riesgo adecuado al cronograma de riesgo de Maria Brown.

Para ver la entrada del indicador de riesgo de Microsoft Graph Security de un usuario, vaya a **Seguridad** > **Usuarios** y seleccione el usuario.

En el cronograma de María, puede seleccionar la última entrada del indicador de riesgo del cronograma de riesgo. El panel de información detallada correspondiente aparece en el panel derecho. La sección **QUÉ PASÓ** proporciona un breve resumen del indicador de riesgo.

### Cómo obtener más información sobre los indicadores de riesgo

Para obtener más información, consulte Sucesos de riesgo de Azure Active Directory.

### Qué acciones puede aplicar al usuario

En la actualidad, la capacidad de realizar las acciones adecuadas en la cuenta del usuario a través del origen de datos de Microsoft Graph Security no está disponible.

Para obtener información sobre la incorporación de Microsoft Graph Security, consulte Microsoft Graph Security.

## Indicadores de riesgo personalizados

December 7, 2023

Hay dos tipos de indicadores de riesgo que se ven en Citrix Analytics for Security:

- **Indicadores de riesgo predeterminados**: Estos indicadores de riesgo se basan en el algoritmo de aprendizaje automático. Para obtener más información, consulte Indicadores de riesgo de usuarios de Citrix.
- **Indicadores de riesgo personalizados**: estos indicadores de riesgo los crean manualmente los administradores.

Cuando crea un indicador de riesgo personalizado, puede definir las condiciones desencadenantes y los parámetros en función de sus casos de uso. Si los eventos del usuario coinciden con los criterios definidos, Citrix Analytics activa el indicador de riesgo personalizado y lo muestra en el cronograma de riesgo del usuario.

Cree indicadores de riesgo personalizados para estos orígenes de datos:

- Citrix Gateway
- Citrix Secure Private Access
- Citrix Virtual Apps and Desktops local
- Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service)
- Citrix Secure Browser

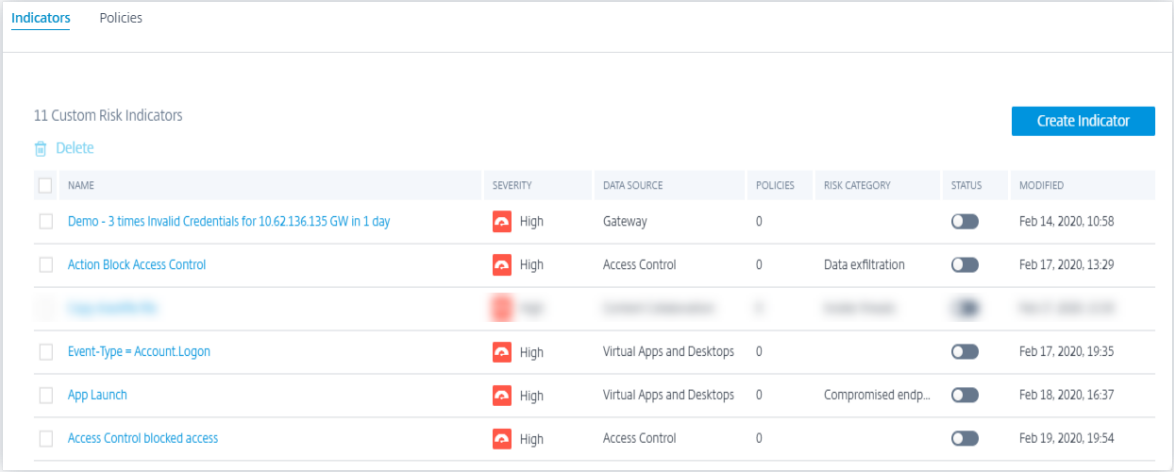
### Indicadores de riesgo personalizados preconfigurados

Citrix también proporciona algunos indicadores de riesgo personalizados con condiciones preconfiguradas para ayudarle a supervisar la seguridad de su infraestructura de Citrix. Puede modificar las condiciones preconfiguradas en función de sus casos de uso. Para obtener más información, consulte Indicadores de riesgo personalizados preconfigurados.

## Página de indicadores de riesgo personalizados

La página **Indicadores de riesgo personalizados** proporciona información sobre todos los indicadores de riesgo personalizados generados para un usuario, gravedad, origen de datos, número de directivas, categoría de riesgo, estado y la fecha y hora de la última modificación del indicador. Para crear un indicador de riesgo personalizado, consulte Creación de un indicador de riesgo personalizado.




Al seleccionar el indicador de riesgo, se le redirigirá a la página **Modificar indicador de riesgo**. Para obtener más información, consulte Modificación de un indicador de riesgo personalizado.

## Análisis de un indicador de riesgo personalizado

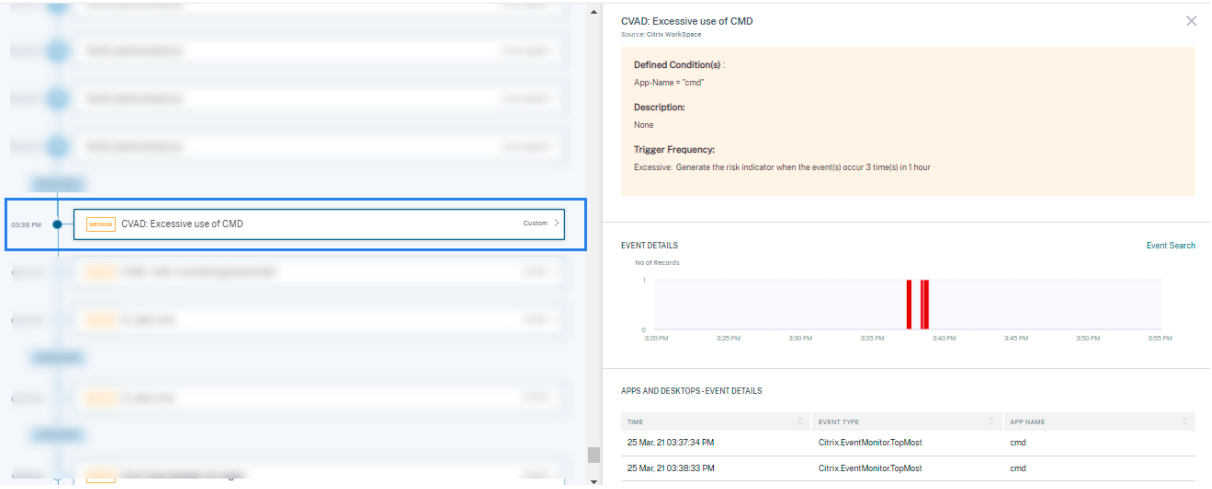
Piense en un usuario cuya acción ha desencadenado un indicador de riesgo personalizado que ha definido. Citrix Analytics muestra el indicador de riesgo personalizado en el cronograma de riesgos del usuario.

Al seleccionar el indicador de riesgo personalizado en el cronograma de riesgos del usuario, el panel derecho muestra la siguiente información:

- **Condición (s) definida (s)**: muestra un resumen de las condiciones que define al crear un indicador de riesgo personalizado.
- **Descripción**: proporciona un resumen de la descripción que proporciona al crear el indicador de riesgo personalizado. Si no se proporciona ninguna descripción al crear el indicador de riesgo personalizado, esta sección refleja **Ninguno**.
- **Frecuencia de disparo**: Muestra la opción seleccionada en la sección **Opciones avanzadas**al crear el indicador de riesgo personalizado.

- **Detalles del evento**: muestra el cronograma y los detalles de los eventos de usuario que han desencadenado el indicador de riesgo personalizado. Puede hacer clic en **Búsqueda de eventos** para ver los eventos de usuario en la página de búsqueda de autoservicio. La página de búsqueda de autoservicio muestra los eventos asociados al usuario y el indicador de riesgo personalizado. La consulta de búsqueda muestra las condiciones definidas para el indicador de riesgo personalizado.




> **Nota**
>
> Los indicadores de riesgo personalizados se representan con una etiqueta en el cronograma de riesgo del usuario.

## Acciones que puede aplicar al usuario

Cuando se activa un indicador de riesgo personalizado para un usuario, puede aplicar una acción manualmente o crear una directiva para aplicar una acción automáticamente. Para obtener más información, consulte Directivas y acciones.

## Plantillas de indicadores de riesgo personalizadas

Puede crear un indicador de riesgo personalizado mediante el uso de una de las plantillas predefinidas o continuar sin usar una plantilla.

Las plantillas actúan como punto de partida para crear un indicador de riesgo personalizado. Le guía para crear un indicador de riesgo personalizado al proporcionar consultas y parámetros predefinidos que puede seleccionar en función de sus casos de uso.

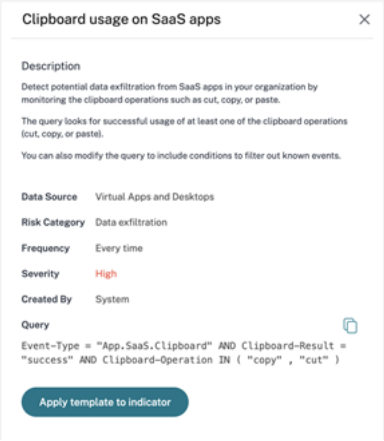
Puede utilizar una plantilla tal cual o modificarla para que cumpla con sus requisitos. Con las plantillas, los administradores pueden crear indicadores de riesgo de interés sin formación adicional.

Una plantilla se compone de la siguiente información:

- **Descripción**: indica el propósito de la consulta definida en la plantilla.
- **Fuente de datos**: indica la fuente de datos a la que se aplica la plantilla.
- **Categoría de riesgo**: indica la categoría de riesgo asociada a los eventos buscados por la consulta. Hay cuatro categorías de eventos de riesgo: exfiltración de datos, amenazas internas, usuarios comprometidos y puntos finales de compromiso. Para obtener información, consulte las categorías de riesgo.
- **Frecuencia**: indica la frecuencia con la que se activa la consulta.
- **Gravedad**: indica la gravedad del riesgo asociado con el evento. El riesgo puede ser alto, medio o bajo.
- **Creado por**: indica el creador de la plantilla. Las plantillas siempre están definidas por el sistema.
- **Consulta**: indica las condiciones definidas en la plantilla. La consulta recupera los eventos del usuario que cumplen las condiciones.

La siguiente imagen muestra la plantilla para el uso del portapapeles de casos de uso en aplicaciones SaaS.

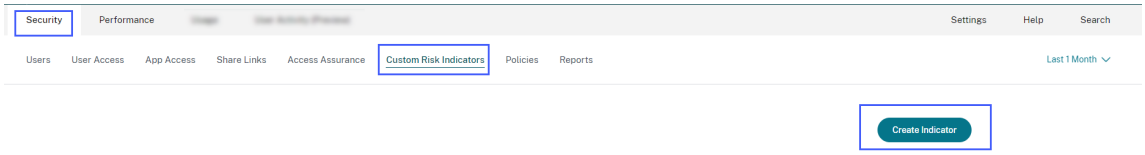



Si no encuentra una plantilla para su caso de uso o si desea definir su propia consulta, puede continuar sin una plantilla.

## Creación de un indicador de riesgo personalizado

Para crear un indicador de riesgo personalizado:

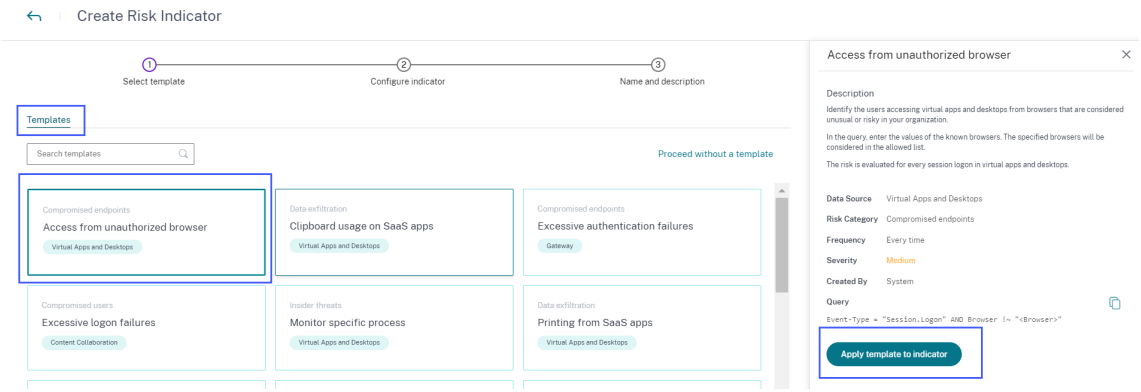
1. Vaya a **Seguridad > Indicadores de riesgo personalizados > Crear indicador**.



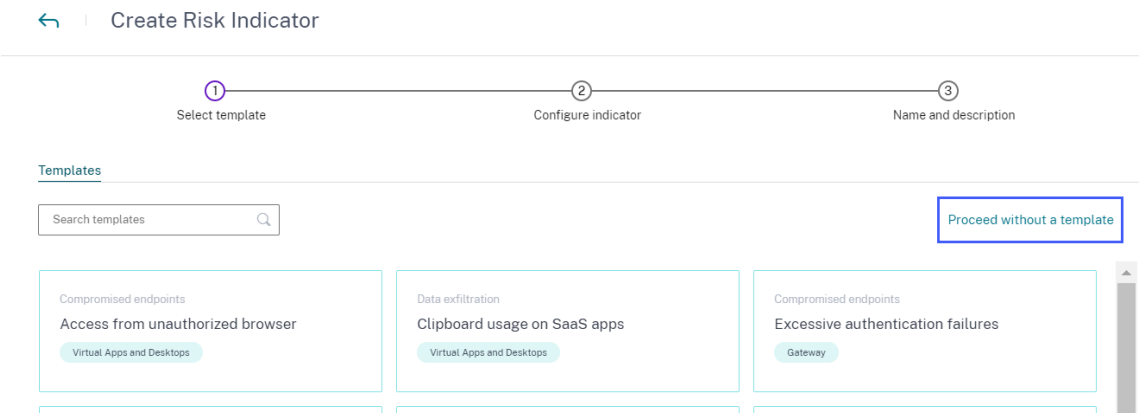

 

2. Seleccione una plantilla para ver el caso de uso. Si cumple con sus requisitos, seleccione **Aplicar plantilla al indicador**.

> **Nota**
>
> También puede modificar las condiciones predefinidas y los parámetros de una plantilla.




3. Si no encuentra la plantilla deseada o quiere crear su propia condición, seleccione **Continuar sin plantilla**.




4. Siga las instrucciones que aparecen en pantalla para crear un indicador.

> **Notas**
>
> - Puede crear indicadores de riesgo personalizados hasta un límite máximo de 50. Si alcanza este límite máximo, debe eliminar o modificar cualquier indicador de riesgo personalizado existente para crear un indicador de riesgo personalizado.
> - Cuando se activa un indicador de riesgo personalizado, se muestra inmediatamente en la línea de tiempo del usuario. Sin embargo, el resumen de riesgos y la puntuación de riesgo del usuario se actualizan al cabo de unos minutos (aproximadamente 15-20 minutos).

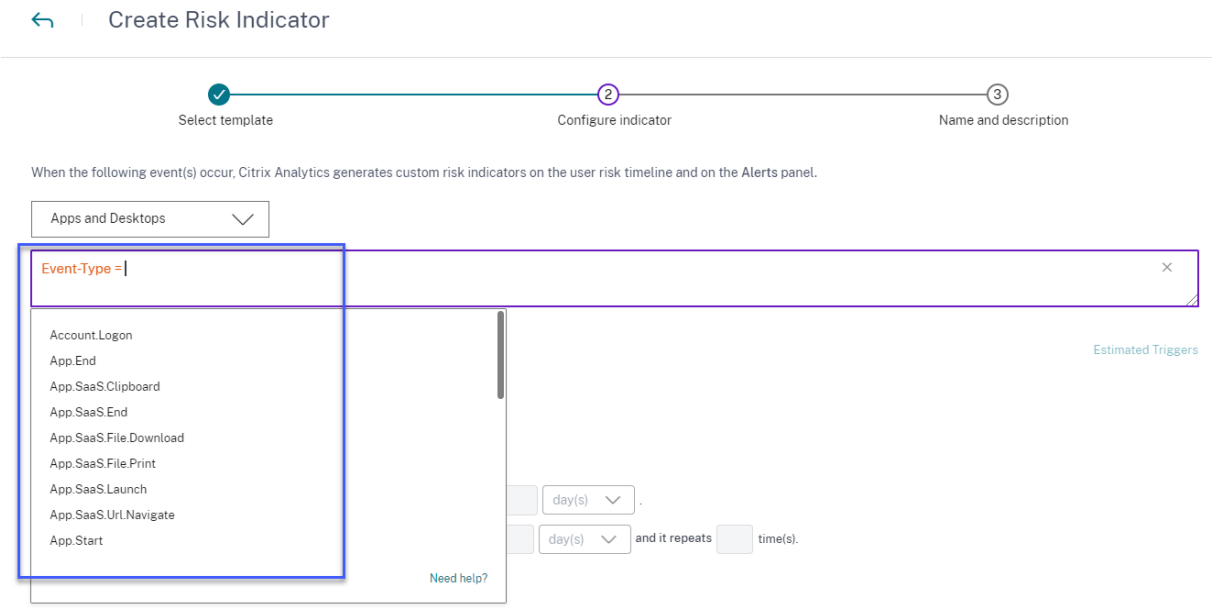
 

### Definición de una condición para un indicador de riesgo personalizado

Use el cuadro de consulta para definir sus condiciones para el indicador de riesgo personalizado. Según la fuente de datos seleccionada, obtendrá las dimensiones correspondientes y los operadores válidos para definir sus condiciones.

Al seleccionar determinadas dimensiones, como `Event-Type` y `Clipboard-Operation` junto con un operador válido, los valores de la dimensión se muestran automáticamente. Puede elegir un valor de las opciones sugeridas o introducir un valor nuevo según sus requisitos.

La siguiente imagen muestra los valores sugeridos de la dimensión `Event-Type`.




Si usa una plantilla, la condición está predefinida. Sin embargo, puede agregar o modificar la condición predefinida en función de su caso de uso.

Debajo del cuadro de consulta, verá el enlace **Desencadenadores estimados**. Haga clic en el enlace para predecir las instancias aproximadas del indicador de riesgo personalizado que se activarían para las condiciones definidas. Estas instancias se calculan en función de los datos históricos que Citrix Analytics mantiene y cumplen las condiciones definidas.

Asegúrese de hacer clic en **Desencadenadores estimados** para predecir el número de ocurrencias de indicadores de riesgo personalizados para la última condición definida.

### Uso de las opciones avanzadas

En la sección **Opciones avanzadas**, seleccione la frecuencia del evento para activar el indicador de riesgo personalizado. Cuando no selecciona ninguna opción, Citrix Analytics considera **Cada vez:**

**Generar el indicador de riesgo cada vez que se producen los eventos** como opción predeterminada y genera el indicador de riesgo personalizado. Se pueden seleccionar una de las siguientes opciones:

- **Cada vez**: El indicador de riesgo se activa siempre que los eventos cumplan las condiciones definidas.
- **Primera vez**: El indicador de riesgo se activa cuando los eventos cumplen las condiciones definidas por primera vez.
  - **Primera vez para una nueva**: habilite esta opción para detectar los eventos recibidos de una nueva entidad por primera vez. Algunos ejemplos de las entidades son IP del cliente, país, ciudad e ID de dispositivo. Solo puede seleccionar una entidad en función de la fuente de datos. Esta opción permite crear un indicador de riesgo sin especificar un valor explícito para las entidades. Por ejemplo, al seleccionar la entidad como "Ciudad", no es necesario especificar el nombre de la ciudad. El indicador de riesgo se activa cuando se reciben eventos de una nueva ciudad por primera vez.

    En la tabla siguiente se enumeran las entidades correspondientes a cada origen de datos y se describen las condiciones del desencadenador.

| Origen de datos | Entidad | Condición de activación |
|---|---|---|
| Secure Private Access | City | Cuando un usuario inicia sesión desde una nueva ciudad por primera vez. |
| | Client-IP | Cuando un usuario inicia sesión desde una nueva dirección IP por primera vez. |
| | País | Cuando un usuario inicia sesión desde un nuevo país por primera vez. |
| Aplicaciones y escritorios | Nombre de la aplicación | Cuando un usuario abre una nueva aplicación virtual o una aplicación SaaS por primera vez. |
| | URL de la aplicación | Cuando un usuario introduce una nueva URL de aplicación en un explorador de su escritorio virtual por primera vez. |

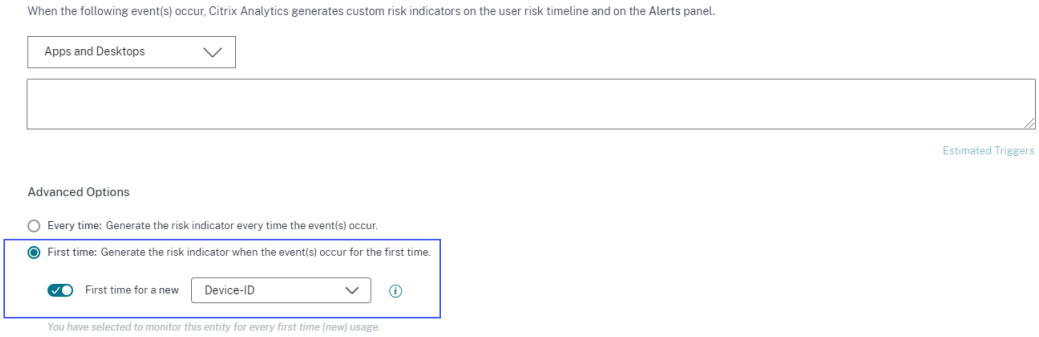
 

| Origen de datos | Entidad | Condición de activación |
|---|---|---|
| | City | Cuando un usuario inicia aplicaciones o escritorios desde una nueva ciudad por primera vez. |
| | Client-IP | Cuando un usuario inicia sesión desde una nueva dirección IP por primera vez. |
| | País | Cuando un usuario inicia aplicaciones o escritorios desde un nuevo país por primera vez. |
| | Device-ID | Cuando un usuario inicia aplicaciones virtuales o escritorios virtuales desde un dispositivo nuevo, como un dispositivo móvil, portátil o de escritorio, por primera vez. |
| | Download-Device-Type | Cuando un usuario utiliza por primera vez un nuevo medio de almacenamiento, como una unidad USB. |
| | Formato de archivo de impresión | Formato del archivo impreso. |
| | Print-File-Size | Tamaño del archivo impreso en bytes. |
| | Print-File-Name | Nombre del archivo impreso. |
| | Printer-Name | Nombre de la impresora utilizada. |
| | Total-Copies-Printed | Número total de copias impresas por el usuario. |
| | Total-Pages-Printed | Número total de páginas del documento impresas por el usuario. |
| Gateway | Client-IP | Cuando un usuario inicia sesión desde una nueva dirección IP por primera vez. |

| Origen de datos | Entidad | Condición de activación |
|---|---|---|
| Secure Browser | User-Name | El nombre del usuario que inició el evento. |
| | Acceso permitido | Si se permite o deniega al usuario el acceso al servicio host. |
| | Client-IP | Dirección IP del dispositivo del usuario. |
| | Nombre de host al que se ha accedido | El servicio host al que accede el usuario a través de la red. |
| | ID de sesión | El número único asignado a la sesión de usuario. |

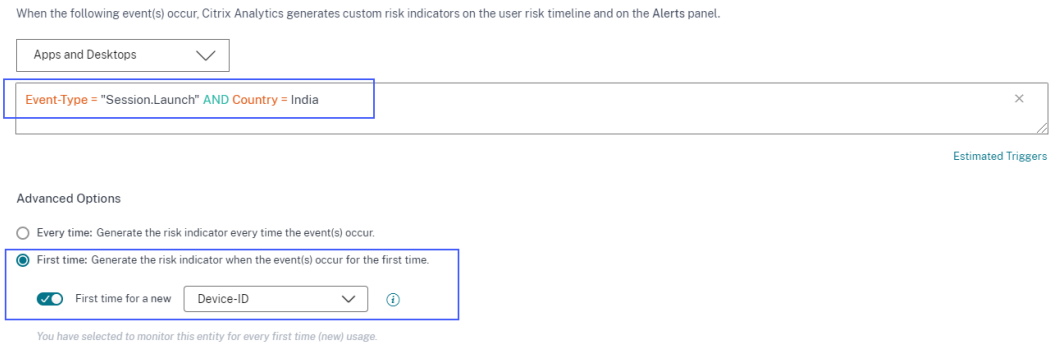
En el siguiente ejemplo, se muestra un indicador de riesgo personalizado creado para la fuente de datos de Apps and Desktops. El indicador de riesgo se activa cuando un usuario inicia un escritorio virtual o una aplicación virtual desde un dispositivo nuevo por primera vez.




También puede agregar una condición junto con la **primera vez para una nueva** opción. En este caso, el indicador de riesgo se activa cuando detecta los eventos de la nueva entidad por primera vez y cuando los eventos cumplen la condición definida.

En el siguiente ejemplo se muestra una condición definida para el indicador de riesgo personalizado y la opción **Primera vez para un nuevo ID de dispositivo** habilitada. El indicador de riesgo se activa cuando un usuario ubicado en la India inicia una sesión de escritorio virtual desde un nuevo dispositivo por primera vez.




- **Excesivo**: El indicador de riesgo se activa cuando se cumplen las siguientes condiciones:
  - Los eventos cumplen las condiciones definidas.
  - Los eventos se producen un número determinado de veces durante el período especificado.
- **Frecuentes**: El indicador de riesgo se activa cuando se cumplen las siguientes condiciones:
  - Los eventos cumplen las condiciones definidas.
  - Los eventos se producen durante el número de veces especificado durante el período especificado.
  - El patrón de eventos se repite el número de veces especificado.

### Selección de la categoría de riesgo

Seleccione la categoría de riesgo para su indicador de riesgo personalizado.

Los indicadores de riesgo se agrupan según el tipo de exposición al riesgo del indicador de riesgo personalizado. Para obtener ayuda sobre la selección de categorías de riesgo, consulte Categorías de riesgo.

### Selección de la gravedad

La gravedad indica el nivel de gravedad de un evento de riesgo, que se detecta mediante el indicador de riesgo. Cuando cree un indicador de riesgo personalizado, seleccione un nivel de gravedad alto, medio o bajo.

Si aplica una plantilla, se preselecciona la opción de gravedad. Puede modificar esta preselección en función de su caso de uso.

### Operadores compatibles para definir una condición

Puede utilizar los siguientes operadores al definir una condición.

| Operador | Descripción | Ejemplo | Resultado |
|---|---|---|---|
| | Asigna un valor a la consulta de búsqueda. | User-Name: John | Muestra los eventos del usuario John. |
| = | Asigna un valor a la consulta de búsqueda. | User-Name = John | Muestra los eventos del usuario John. |
| ~ | Busca valores similares. | User-Name ~ test | Muestra los eventos con nombres de usuario similares. |
| ”” | Encierra valores separados por espacios. | User-Name = “John Smith” | Muestra los eventos del usuario John Smith. |
| <, > | Búsqueda de valor relacional. | Volumen de datos > 100 | Muestra los eventos en los que el volumen de datos es superior a 100 GB. |
| AND | Busca valores en los que se cumplan ambas condiciones. | User-Name: John AND Data Volume > 100 | Muestra los eventos del usuario John en los que el volumen de datos es superior a 100 GB. |
| * | Busca valores que coincidan con el carácter cero o más veces. | User-Name = John* | Muestra los eventos de todos los nombres de usuario que empiezan por John. |
| | | User-Name = *John* | Muestra los eventos de todos los nombres de usuario que contienen John. |
| | | User-Name = *Smith | Muestra los eventos de todos los nombres de usuario que terminan en Smith. |

| Operador | Descripción | Ejemplo | Resultado |
|---|---|---|---|
| !~ | Comprueba los eventos de usuario para el patrón coincidente que especifique. Este operador NOT LIKE devuelve los eventos que no contienen el patrón coincidente en ninguna parte de la cadena de eventos. | User-Name !~ John | Muestra los eventos de los usuarios excepto John, John Smith o cualquier otro usuario que contenga el nombre coincidente “John”. |
| != | Comprueba los eventos de usuario de la cadena exacta que especifique. Este operador NOT EQUAL devuelve los eventos que no contienen la cadena exacta en ninguna parte de la cadena de eventos. | Country != USA | Muestra los eventos de los países excepto EE. UU. |
| IN | Asigna varios valores a una dimensión para obtener los eventos relacionados con uno o varios valores. | User-Name IN (John, Kevin) | Busca todos los eventos relacionados con John o Kevin. |
| NOT IN | Asigna varios valores a una dimensión y busca los eventos que no contienen los valores especificados. | User-Name NOT IN (John, Kevin) | Busca los eventos para todos los usuarios excepto John y Kevin. |

| Operador | Descripción | Ejemplo | Resultado |
|---|---|---|---|
| IS EMPTY | Comprueba si hay un valor nulo o un valor vacío para una dimensión. Este operador solo funciona para dimensiones de tipo cadena como `App-Name`, `Browser` y `Country`. No funciona para dimensiones de tipo no cadena (número) como `Upload-File-Size`, `Download-File-Size` y `Client-IP`. | Country IS EMPTY | Busca eventos en los que el nombre del país no está disponible o está vacío (no especificado). |
| IS NOT EMPTY | Comprueba si hay un valor no nulo o un valor específico para una dimensión. Este operador solo funciona para dimensiones de tipo cadena como `App-Name`, `Browser` y `Country`. No funciona para dimensiones de tipo no cadena (número) como `Upload-File-Size`, `Download-File-Size` y `Client-IP`. | Country IS NOT EMPTY | Busca eventos en los que el nombre del país esté disponible o especificado. |

| Operador | | Descripción | Ejemplo | Resultado |
|---|---|---|---|---|
| | O BIEN | Busca valores en los que una o ambas condiciones son verdaderas. | (User-Name = `John*` OR User-Name = `*Smith`) AND Event-Type = "Session.Logon" | Muestra eventos de `Session.Logon` para todos los nombres de usuario que comienzan por John o terminan por Smith. |

> **Nota**
>
> Para el operador **NOT EQUAL**, al introducir los valores de las dimensiones de su condición, utilice los valores exactos disponibles en la página de búsqueda de autoservicio de un origen de datos. Los valores de cota distinguen entre mayúsculas y minúsculas

## Modificación de un indicador de riesgo personalizado

1. Vaya a **Seguridad > Indicadores de riesgo personalizados**.
2. Seleccione el indicador de riesgo personalizado que quiere modificar.
3. En la página **Modificar indicador**, modifique la información según sea necesario.
4. Haga clic en **Guardar cambios**.

> **Nota**
>
> Si modifica los atributos como condición, categoría de riesgo, gravedad y nombre de un indicador de riesgo personalizado existente, en el cronograma del usuario, podrá ver las apariciones anteriores del indicador de riesgo personalizado (con los atributos antiguos) que se activaron para el usuario.
>
> Por ejemplo, ha creado un indicador de riesgo personalizado con la condición *País. = India*. Por lo tanto, este indicador de riesgo personalizado se activa cuando un usuario inicia sesión desde fuera del país India. Ahora, modifica la condición del indicador de riesgo personalizado a *País. = "Estados Unidos"*. En este caso, puede seguir viendo las apariciones anteriores del indicador de riesgo personalizado con la condición *País. = India* en los plazos de los usuarios que activaron el indicador de riesgo.

## Eliminación de un indicador de riesgo personalizado

1. Vaya a **Seguridad > Indicadores de riesgo personalizados**.

2. Seleccione el indicador de riesgo personalizado que quiere eliminar.
3. Haga clic en **Eliminar**.
4. En el cuadro de diálogo, confirma su solicitud para eliminar el indicador de riesgo personalizado.

> **Nota**
>
> Si elimina un indicador de riesgo personalizado, en el cronograma del usuario, podrá seguir viendo las apariciones anteriores del indicador de riesgo personalizado que se activaron para el usuario.
>
> Por ejemplo, elimina un indicador de riesgo personalizado existente con la condición *País. = India*. En este caso, puede seguir viendo las apariciones anteriores del indicador de riesgo personalizado con la condición *País. = India* en los plazos de los usuarios que activaron el indicador de riesgo.

## Evaluación continua del riesgo

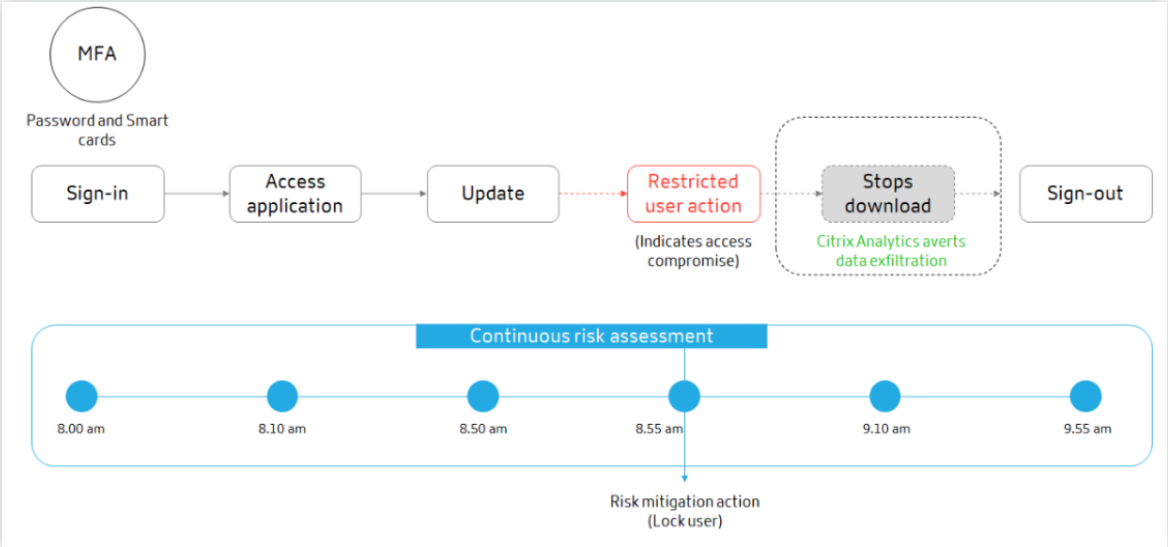
December 7, 2023

Un mayor uso de dispositivos informáticos portátiles e Internet permite a los usuarios de Citrix Workspace trabajar desde casi cualquier ubicación y en cualquier dispositivo. El desafío de esta flexibilidad es que el acceso remoto expone los datos confidenciales a riesgos de seguridad a través de actividades cibernéticas como la exfiltración de datos, el robo, el vandalismo y las interrupciones del servicio. También es probable que los empleados de las organizaciones contribuyan a este daño.

Algunas formas convencionales de abordar estos riesgos son implementar autenticación multifactor, sesiones de inicio de sesión breves, etc. Aunque estos métodos de evaluación de riesgos garantizan un mayor nivel de seguridad, no proporcionan una seguridad completa tras la validación inicial de los usuarios. Si un usuario malintencionado consigue acceder a la red, hace un mal uso de los datos confidenciales que son perjudiciales para una organización.

Para mejorar el aspecto de la seguridad y garantizar una mejor experiencia de usuario, Citrix Analytics presenta la solución de evaluación continua de riesgos. Esta solución protege sus datos tanto de ciberdelincuentes externos como de personas con información privilegiada malintencionada al garantizar que la exposición al riesgo de los usuarios que utilizan Citrix Virtual Apps and Desktops o Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) siga siendo la misma que cuando se verificó durante la fase inicial, sin necesidad de que el usuario lo demuestre cada vez. Esta solución se logra evaluando continuamente un evento de riesgo durante una sesión y aplicando automáticamente acciones para evitar que los recursos de la organización sigan haciendo un uso indebido.




## Casos de uso

Piense en un usuario Adam Maxwell, que pudo acceder a una red por primera vez tras varios intentos fallidos de inicio de sesión desde una ubicación inusual que es contraria a su comportamiento habitual. Además, la ubicación tiene un historial de ataques cibernéticos. En este caso, debes tomar medidas inmediatas para evitar que la cuenta de Adam se use indebidamente. Puede bloquear la cuenta de Adam y notificarle sobre la acción tomada. Esta acción podría crear interrupciones del servicio temporalmente en la cuenta del usuario. El usuario puede ponerse en contacto con el administrador para que le ayude a restaurar la cuenta.

Considere otro caso en el que Adam ha accedido a una red desde un dispositivo nuevo y desde una nueva IP por primera vez. Puede ponerse en contacto con Adam para confirmar si identifica esta actividad. Si es así, puede ser que Adam haya cambiado su dispositivo de trabajo y esté trabajando desde su red doméstica. Esta actividad no daña la seguridad de su organización y se puede ignorar. Sin embargo, si el usuario no realizó esta actividad, es probable que la cuenta se haya visto comprometida. En este caso, puede bloquear la cuenta del usuario para evitar daños adicionales.

## Funciones principales

La evaluación continua de riesgos automatiza algunas de las funcionalidades asociadas con las directivas y los paneles de control de visibilidad:

### Soporta múltiples condiciones

Al crear o modificar una directiva, puede agregar hasta cuatro condiciones. Las condiciones pueden contener combinaciones de indicadores de riesgo de incumplimiento e indicadores de riesgo personalizados, puntuaciones de riesgo del usuario o ambos.

Para obtener más información, consulte Qué son las directivas.

### Notificación a los usuarios antes de aplicar acciones

Antes de aplicar una acción apropiada en la cuenta de un usuario, puede notificar al usuario y evaluar la naturaleza de una actividad inusual que se ha detectado.

Para obtener más información, consulte Solicitar la respuesta del usuario final.

### Notificar a los usuarios tras aplicar acciones

Para algunas actividades, esperar la respuesta del usuario antes de aplicar una acción puede poner en riesgo la cuenta del usuario y la seguridad de su organización. En estos casos, puede aplicar una acción disruptiva cuando detecta una actividad inusual y notificar al usuario sobre la misma.

Para obtener más información, consulte Notificar al usuario después de aplicar una acción disruptiva.

### Modos de aplicación y supervisión

Puede establecer directivas para los modos de cumplimiento o supervisión en función de sus requisitos. Las directivas en modo de cumplimiento tienen un impacto directo en las cuentas de los usuarios. Sin embargo, si quiere evaluar el impacto o el resultado de sus directivas antes de implementarlas, puede configurar las directivas en modo de supervisión.

Para obtener más información, consulte Modos compatibles.

### Visibilidad de los paneles de control de directivas y acceso

Con el panel **Resumen de acceso**, puede obtener información sobre el número de intentos de acceso realizados por los usuarios. Para obtener más información, consulte Resumen de acceso.

Mediante el panel **Directivas y acciones**, puede obtener información sobre las directivas y acciones aplicadas en las cuentas de usuario. Para obtener más información, consulte Directivas y acciones.

### Directivas predeterminadas

Citrix Analytics introduce directivas predefinidas que están habilitadas en el panel **Directivas** de forma predeterminada. Estas directivas se crean mediante indicadores de riesgo y puntuaciones de riesgo del usuario como condiciones predefinidas. Se asigna una acción global a todas las directivas predeterminadas.

> **Nota**
>
> Las directivas que aparecen en su entorno pueden variar en función de cuándo comenzó a usar Citrix Analytics y de si ha realizado algún cambio local.

Para obtener más información, consulte Qué son las directivas.

Puede utilizar las siguientes directivas predeterminadas o modificarlas según sus requisitos:

| Nombre de directiva | Condición | Origen de datos | Acción |
|---|---|---|---|
| Explotación de credenciales correcta | Cuando se activan los errores de autenticación excesivos y los indicadores de riesgo de inicios de sesión sospechosos | Citrix Gateway | Bloquear usuario |
| Exfiltración potencial de datos | Cuando se activa el indicador de riesgo filtración de datos potencial | Citrix Virtual Apps and Desktops y Citrix DaaS | Cerrar sesión usuario |
| Acceso inusual desde una IP sospechosa | Cuando se activan los indicadores de riesgo de inicios de sesión sospechosos e inicios de sesión sospechosos desde direcciones IP sospechosas | Citrix Gateway | Bloquear usuario |
| Acceso por primera vez desde el dispositivo | Cuando se activa el indicador de riesgo CVAD: acceso por primera vez desde un dispositivo nuevo | Citrix Virtual Apps and Desktops y Citrix DaaS | Solicitud de respuesta del usuario final |

| Nombre de directiva | Condición | Origen de datos | Acción |
|---|---|---|---|
| Trayecto imposible al acceder | Cuando se activa el indicador de riesgo de trayecto imposible. | Citrix Virtual Apps and Desktops y Citrix DaaS | Solicitud de respuesta del usuario final |
| Trayecto imposible al autenticarse | Cuando se activa el indicador de riesgo de trayecto imposible. | Citrix Gateway | Solicitud de respuesta del usuario final |

## Directivas y acciones

December 7, 2023

> **Nota**
>
> :**Citrix**Content Collaboration y ShareFile han llegado al final de su vida útil y ya no están disponibles para los usuarios.

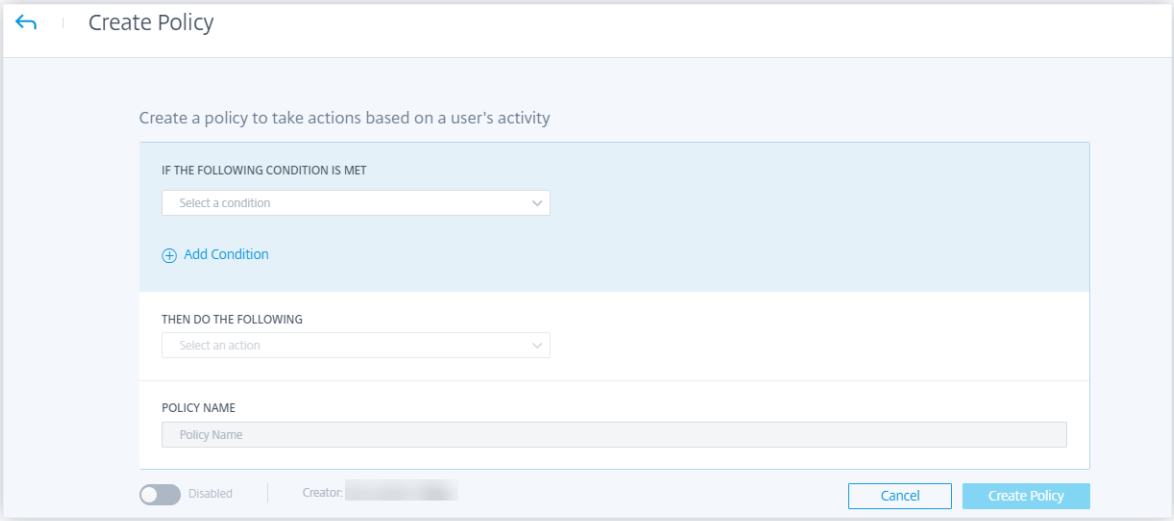
Puede crear directivas en Citrix Analytics para ayudarle a realizar acciones en las cuentas de usuario cuando se producen actividades inusuales o sospechosas. Las directivas permiten automatizar el proceso de aplicación de acciones como inhabilitar un usuario y añadir usuarios a una lista de seguimiento. Al habilitar directivas, se aplica una acción correspondiente inmediatamente después de que se produce un evento anómalo y se cumple la condición de la directiva. También puede aplicar acciones manualmente en cuentas de usuario con actividades anómalas.

### ¿Cuáles son las directivas?

Una directiva es un conjunto de condiciones que deben cumplirse para aplicar una acción. Una directiva contiene una o varias condiciones y una sola acción. Puede crear una directiva con varias condiciones y una acción que se puede aplicar a la cuenta de un usuario.

La**puntuación de riesgo** es una condición global. Las condiciones globales se pueden aplicar a un usuario específico para un origen de datos específico. Puede vigilar las cuentas de usuario que muestran actividades inusuales. Otras condiciones son específicas de los orígenes de datos y sus indicadores de riesgo. Las condiciones contienen combinaciones de puntuaciones de riesgo, indicadores de riesgo de impago e indicadores de riesgo personalizados. Puede agregar hasta 4 condiciones al crear una directiva.




Por ejemplo, si su organización utiliza datos confidenciales, es posible que quiera restringir la cantidad de datos compartidos o a los que tienen acceso los usuarios internamente. Pero si tiene una organización grande, no sería factible que un solo administrador administre y supervise a muchos usuarios. Puede crear una directiva en la que cualquier persona que comparta datos confidenciales en exceso pueda agregarse a una lista de seguimiento o tener su cuenta desactivada inmediatamente.

### Directivas predeterminadas

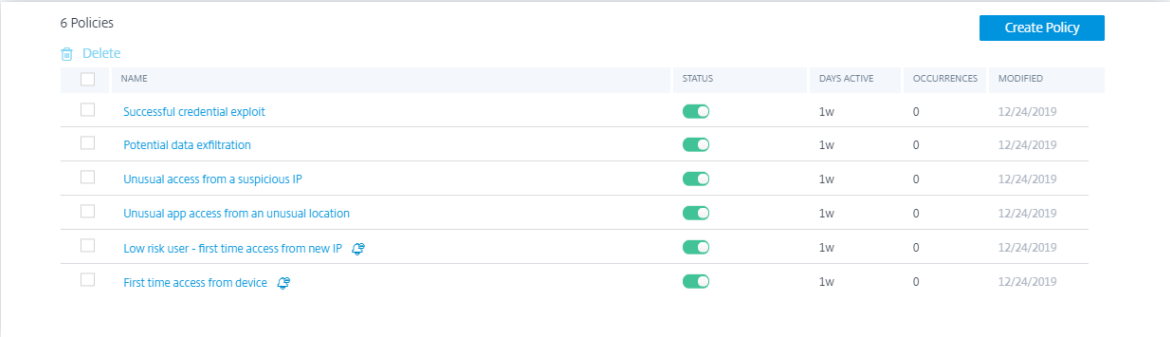
Las directivas predeterminadas están predefinidas y habilitadas en el panel **Directivas**. Se crean en función de condiciones predefinidas y se asigna una acción correspondiente a cada directiva predeterminada. Puede utilizar una directiva predeterminada o modificarla según sus requisitos.

Citrix Analytics admite las siguientes directivas predeterminadas:

- Explotación de credenciales exitosas
- Exfiltración potencial de datos
- Acceso inusual desde una IP sospechosa
- Acceso por primera vez desde el dispositivo
- Virtual Apps and Desktops y Citrix DaaS: Trayecto imposible al acceder
- Gateway: Trayecto imposible al autenticarse

Para obtener información sobre las condiciones y acciones predefinidas con respecto a las directivas predeterminadas anteriores, consulte Evaluación continua del riesgo.




Para obtener información sobre la directiva predefinida para el caso de uso de geocercas, consulte Directiva preconfigurada.

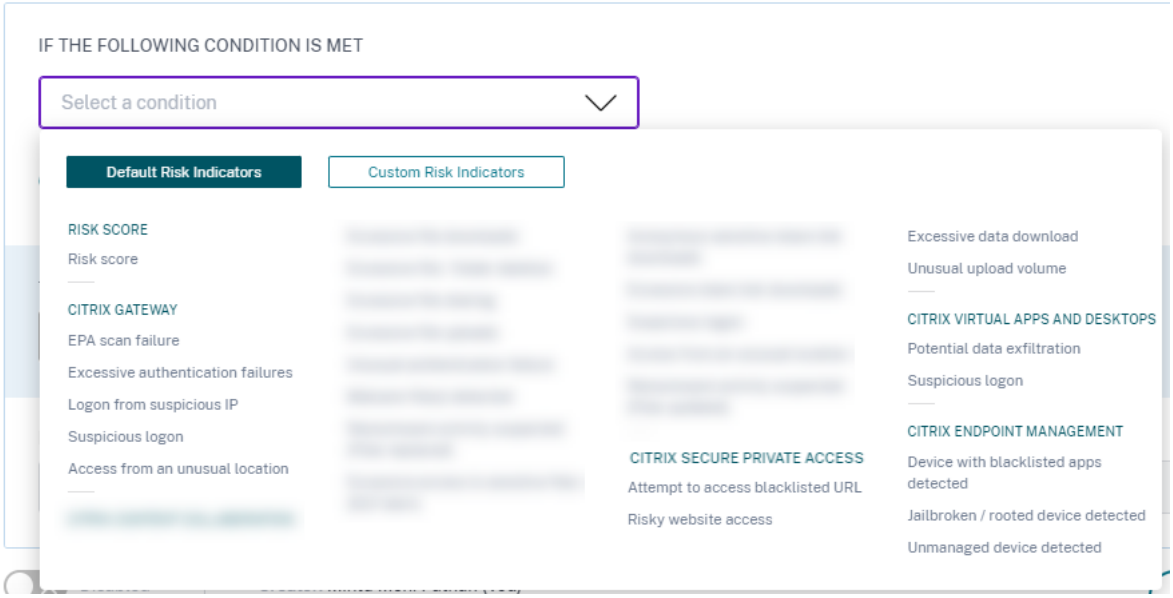
### ¿Cómo agregar o eliminar condiciones?

Para agregar más condiciones, seleccione **Agregar condición** en la sección **SI SE CUMPLE LA SIGUIENTE CONDICIÓN** de la página **Crear directiva**. Para eliminar una condición, seleccione el icono **-** que aparece junto a la condición.


### Indicadores de riesgo de incumplimiento y personalizados

El menú de condiciones se segrega en función de las fichas **Indicadores de riesgo predeterminados** e **Indicadores de riesgo personalizados** de la página **Crear directiva**. Con estas fichas, puede identificar fácilmente el tipo de indicador de riesgo que quiere elegir al seleccionar una condición para la configuración de directivas.




## ¿Cuáles son las acciones?

Las acciones son respuestas a eventos sospechosos que impiden que se produzcan eventos anómalos en el futuro. Puede aplicar acciones en cuentas de usuario que muestren comportamientos inusuales o sospechosos. Puede configurar directivas para aplicar acciones en la cuenta del usuario de forma automática o aplicar una acción específica manualmente desde el cronograma de riesgo del usuario.

Puede ver acciones o acciones globales para cada origen de datos de Citrix. También puede inhabilitar las acciones aplicadas previamente a un usuario en cualquier momento.

> **Nota**
>
> Independientemente del origen de datos que desencadena un indicador de riesgo, se pueden aplicar acciones relacionadas con otros orígenes de datos.

En la tabla siguiente se describen las acciones que se pueden llevar a cabo.

| Nombre de acción | Descripción | Orígenes de datos aplicables |
|---|---|---|
| **Acciones globales** | | |
| **Agregar a la lista de seguimiento** | Cuando quiera supervisar a un usuario en busca de futuras amenazas potenciales, puede agregarlas a una lista de seguimiento. | Todas los orígenes de datos |

| Nombre de acción | Descripción | Orígenes de datos aplicables |
| --- | --- | --- |
| | El panel **Usuarios en Lista** de seguimiento muestra todos los usuarios que quiere supervisar para detectar posibles amenazas en función de la actividad inusual de su cuenta. Según la directiva de su organización, puede agregar un usuario a la lista de seguimiento mediante la acción Agregar a la lista de seguimiento.<br>Para agregar un usuario a la lista de seguimiento, navegue hasta el perfil del usuario, desde el menú **Acciones**, seleccione **Agregar a la lista de seguimiento**. Haga clic en **Aplicar** para aplicar la acción. | |

| Nombre de acción | Descripción | Orígenes de datos aplicables |
| --- | --- | --- |
| **Notificar a los administradores** | Cuando se activa un indicador de riesgo para un usuario, puede notificar manualmente a los administradores o crear una directiva para la notificación automática. Puede seleccionar los administradores del dominio de Citrix Cloud y otros dominios que no sean de Citrix Cloud en su organización. Si es administrador de Citrix Cloud con permisos de acceso total, de forma predeterminada, las notificaciones por correo electrónico están inhabilitadas para su cuenta de Citrix Cloud. Para recibir notificaciones por correo electrónico, habilítelo en su cuenta de Citrix Cloud. Para obtener más información, consulte Recibir notificaciones por correo electrónico. Si es administrador de Citrix Cloud con permisos de acceso personalizados (solo lectura y acceso completo) para administrar Security Analytics, las notificaciones por correo electrónico están habilitadas para su cuenta de Citrix Cloud. Para dejar de recibir notificaciones por correo electrónico de Citrix Analytics, solicite al administrador de acceso total de Citrix Cloud que elimine su nombre de la lista de distribución de notificaciones a los administradores. Para obtener información sobre, consulte Lista de distribución de correo electrónico. | |

| Nombre de acción | Descripción | Orígenes de datos aplicables |
|---|---|---|
| **Solicitud de respuesta del usuario final** | Cuando hay alguna actividad inusual o sospechosa en la cuenta del usuario, puede notificar al usuario para confirmar si el usuario identifica la actividad. En función de la actividad, puede determinar el siguiente curso de acción que se tomará en la cuenta del usuario. Para obtener más información, consulte Solicitar la respuesta del usuario final. | |
| **Notificar al usuario final** | Cuando se produce alguna actividad inusual o sospechosa en la cuenta del usuario, puedes notificárselo al usuario final mediante una notificación por correo electrónico. Para obtener más información, consulte Notificar al usuario final. | |
| **Acciones de Citrix Gateway** | | |
| **Cerrar sesión activas** | Cuando se aplica la acción, cierra la sesión de usuario que está activa actualmente. No bloquea ninguna sesión de usuario futura. | Citrix Gateway local y Citrix Application Delivery Management |
| **Bloquear cuenta de usuario** | Cuando la cuenta de un usuario está bloqueada debido a un comportamiento anómalo, no puede acceder a ningún recurso a través de Citrix Gateway hasta que el administrador de Gateway desbloquee la cuenta. | Citrix Gateway local |

| Nombre de acción | Descripción | Orígenes de datos aplicables |
| --- | --- | --- |
| **Desbloquear cuenta de usuario** | Cuando la cuenta de un usuario se bloquea accidentalmente aunque no se haya detectado un comportamiento anómalo, puede aplicar esta acción para desbloquearla y restaurar el acceso a la cuenta. | Citrix Gateway local |
| **Acciones de Citrix Virtual Apps and Desktops y Citrix DaaS** | | |
| **Cerrar sesión activas** | Cuando se aplica la acción, cierra la sesión de usuario que está activa actualmente. No bloquea ninguna sesión de usuario futura. | Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service) |
| **Iniciar grabación de sesiones** | Si se produce un evento inusual en la cuenta de escritorios virtuales del usuario, el administrador puede empezar a grabar las sesiones activas actuales del usuario. Si el usuario usa Citrix Virtual Apps and Desktops 7.18 o una versión posterior y ha iniciado sesión en la sesión virtual, un administrador puede activar dinámicamente una acción de inicio de grabación de sesiones desde Citrix Analytics for Security que inicia la grabación de la sesión activa actual del usuario. | Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service) |

**Notas**

- Puede aplicar cualquier acción a un indicador de riesgo independientemente de los orígenes de datos.

> - Los administradores ahora pueden ejecutar acciones de grabación dinámica de sesiones en los sitios de Citrix DaaS y grabar dinámicamente las sesiones virtuales de los usuarios.
> - Las acciones **Solicitar respuesta al usuariofinal y Notificar al usuario final**no se pueden aplicar a usuarios anónimos porque no tienen direcciones de correo electrónico en**Active Directory**. Por lo tanto, asegúrese de que las direcciones de correo electrónico de los usuarios estén disponibles en**Active Directory** con una conexión establecida entre Active Directory y Citrix Cloud.

**Uso compartido de solo lectura**

Antes de aplicar la acción **Cambiar vínculos a uso compartido de solo lectura** en la cuenta de un usuario, asegúrese de que se cumplen las siguientes condiciones:

**Requisitos previos**

- El administrador debe tener una cuenta Enterprise en Content Collaboration para utilizar la acción **Cambiar vínculos a uso compartido de solo lectura**.
- El uso compartido de solo lectura es una función disponible en una solicitud en las cuentas empresariales de Citrix Content Collaboration. Antes de aplicar la acción **Cambiar vínculos al uso compartido de solo lectura** en Citrix Analytics, asegúrese de que la función Compartir solo lectura ya esté habilitada en las cuentas de Content Collaboration Enterprise del usuario y del administrador. Para obtener más información, consulte el artículo de asistencia técnica de Citrix: CTX208601.

**Tipos de archivo admitidos** La acción de compartir solo lectura se aplica a los siguientes tipos de archivo:

- Archivos de Microsoft Office
- PDF
- Archivos de imagen (requiere SZC v3.4.1 o posterior):
  - BMP
  - GIF
  - JPG
  - JPEG
  - PNG
  - TIF

  - TIFF

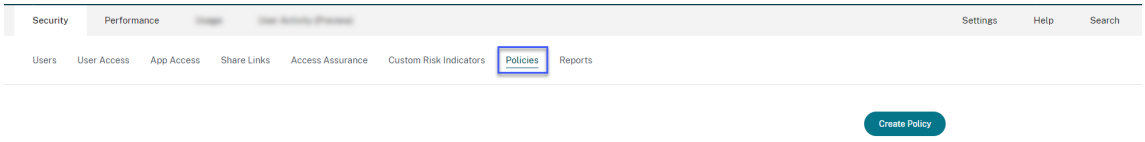
- Archivos de audio y vídeo almacenados en una zona de almacenamiento administrada por Citrix.

## Configurar directivas y acciones

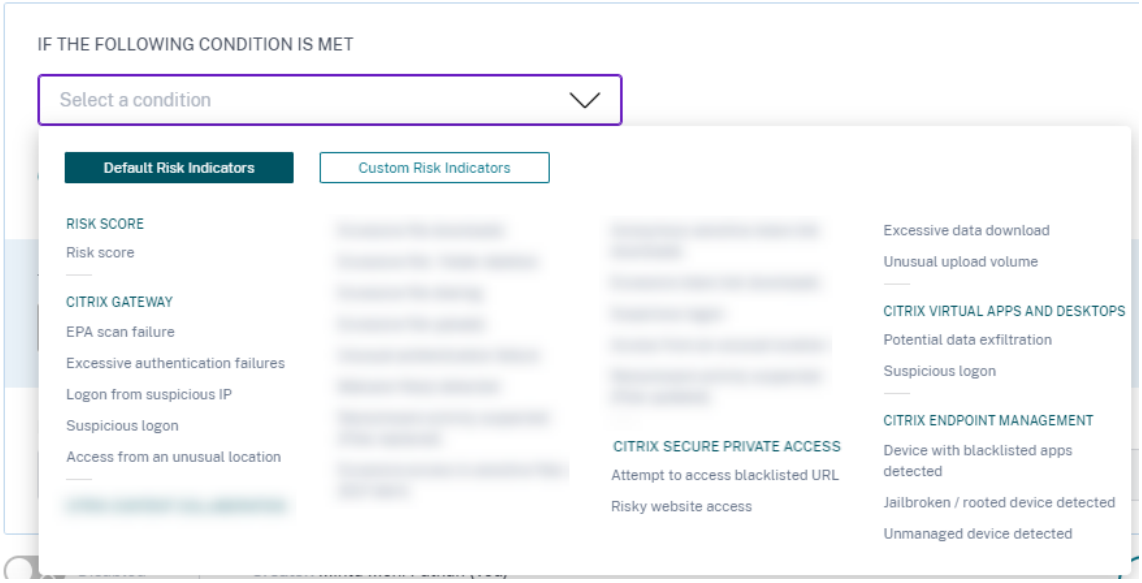
Por ejemplo, siguiendo los pasos que se indican a continuación, puede crear una directiva de uso compartido excesivo de archivos. Con esta directiva, cuando un usuario de la organización comparte una cantidad inusualmente grande de datos, los vínculos del recurso compartido caducaron automáticamente. Se le notifica cuando un usuario comparte datos que superan el comportamiento normal de ese usuario. Si aplica la directiva de uso compartido excesivo de archivos y toma medidas inmediatas, puede evitar la filtración de datos de la cuenta de cualquier usuario.

Para crear una directiva, haga lo siguiente:

1. Después de iniciar sesión en Citrix Analytics, vaya a **Seguridad > Directivas > Crear directiva**.

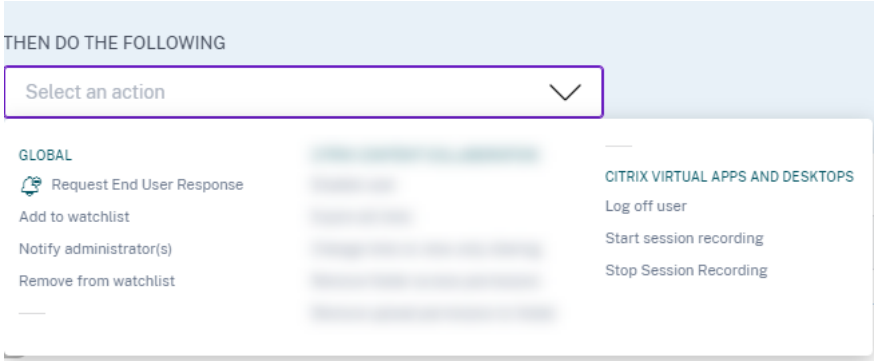



2. En el cuadro de lista **SI SE CUMPLE LA SIGUIENTE CONDICIÓN**, seleccione las condiciones predeterminadas o personalizadas del indicador de riesgo a las que quiere aplicar una acción.

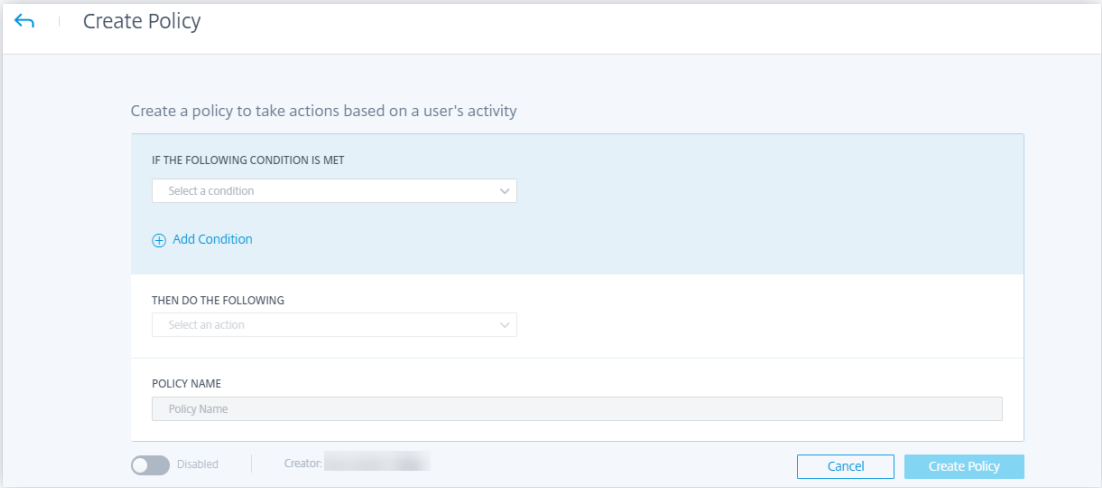



3. En la lista **THEN DO THE FOLLOWING**, seleccione una acción.




4. En el cuadro de texto **Nombre de la directiva**, proporcione un nombre y habilite la directiva mediante el botón de alternancia proporcionado.




5. Haga clic en **Crear directiva**.

Después de crear una directiva, la directiva aparece en el panel de control **Directivas**.

El panel **Directivas** muestra las directivas asociadas a los orígenes de datos que se han detectado correctamente y se han conectado a Citrix Analytics. El panel no muestra las directivas que tienen condiciones definidas para los orígenes de datos no descubiertas.

Sin embargo, desactivar el procesamiento de datos de un origen de datos ya conectada no afecta a las directivas existentes en el panel **Directivas**.

### Solicitud de respuesta del usuario final

**Solicitar respuesta del usuario final** es una acción global mediante la cual puede alertar a un usuario inmediatamente después de detectar una actividad inusual en su cuenta de Citrix. Al aplicar la acción, se envía una notificación por correo electrónico al usuario. El usuario debe responder por correo electrónico sobre la legitimidad de su actividad.

**Determine qué acción quiere aplicar a sus usuarios:**

En función de la respuesta del usuario, puede determinar el siguiente curso de acción que quiere tomar. Puede aplicar una acción global como Agregar a la lista de seguimiento, Notificar a los administradores. También puede aplicar una acción específica de la fuente de datos, como Citrix Gateway-Lock user.

Si recibe una respuesta de que el usuario realizó la actividad denunciada, la actividad no es sospechosa y no es necesario que realice ninguna acción en la cuenta del usuario. El límite diario para enviar alertas de seguridad al usuario es de tres correos electrónicos.

Considere un usuario de Citrix Content Collaboration cuya puntuación de riesgo haya superado los 80 en una duración de 80 minutos. Puede alertar al usuario sobre este comportamiento inusual aplicando la acción **Solicitar respuesta del usuario final**. Se envía una alerta de seguridad al usuario desde el ID de correo electrónico `security-analytics@cloud.com`.

El correo electrónico contiene la siguiente información:

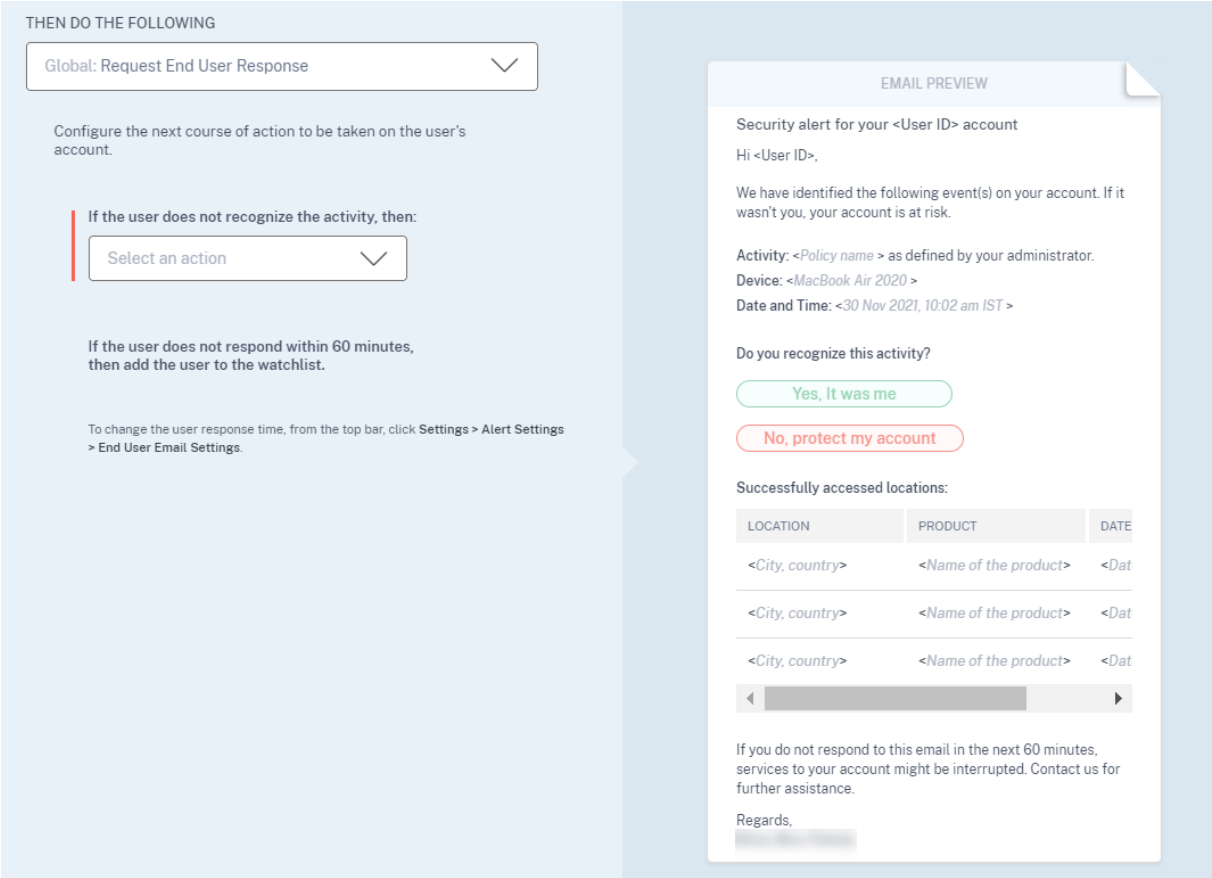
- Actividad del usuario que ha activado el indicador de riesgo
- Dispositivo del usuario
- Fecha y hora de la actividad del usuario
- Ubicaciones (ciudades y países) desde las que se accede correctamente a los productos o servicios. Si la ciudad o el país no están disponibles, el valor correspondiente se muestra como "Desconocido"

La acción **Solicitar respuesta del usuario final** se agrega a la cronología de riesgo del usuario.

Si el usuario no reconoce la actividad detectada en su cuenta de Citrix, Citrix Analytics aplica la acción que ha definido.

Si el usuario no envía su respuesta en el plazo de una hora desde la recepción del correo electrónico, Citrix Analytics lo agrega a la lista de seguimiento. Puede supervisar al usuario y su cuenta para detectar cualquier actividad sospechosa y tomar las medidas oportunas.

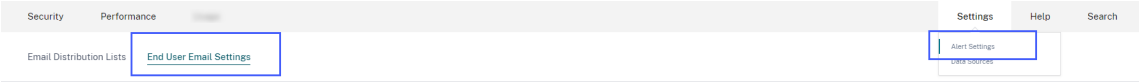
 




**¿Cómo configurar el tiempo de respuesta del usuario?** Puede configurar el tiempo de respuesta del usuario a su correo electrónico de alerta de seguridad. Si el usuario no responde a la actividad notificada dentro del período de tiempo especificado, se agrega a la lista de seguimiento para su supervisión.

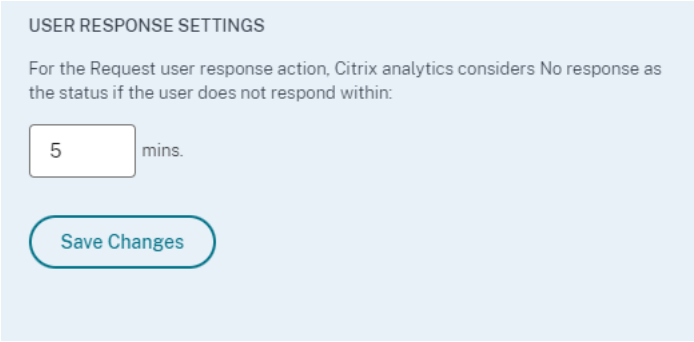
Siga los pasos para configurar el tiempo de respuesta del usuario:

1. Haga clic en **Configuración > Configuración de alertas > Configuración del correo electrónico del usuario final**.




2. En la página **Configuración del correo electrónico del usuario final**, introduzca el número de minutos en el cuadro de texto.

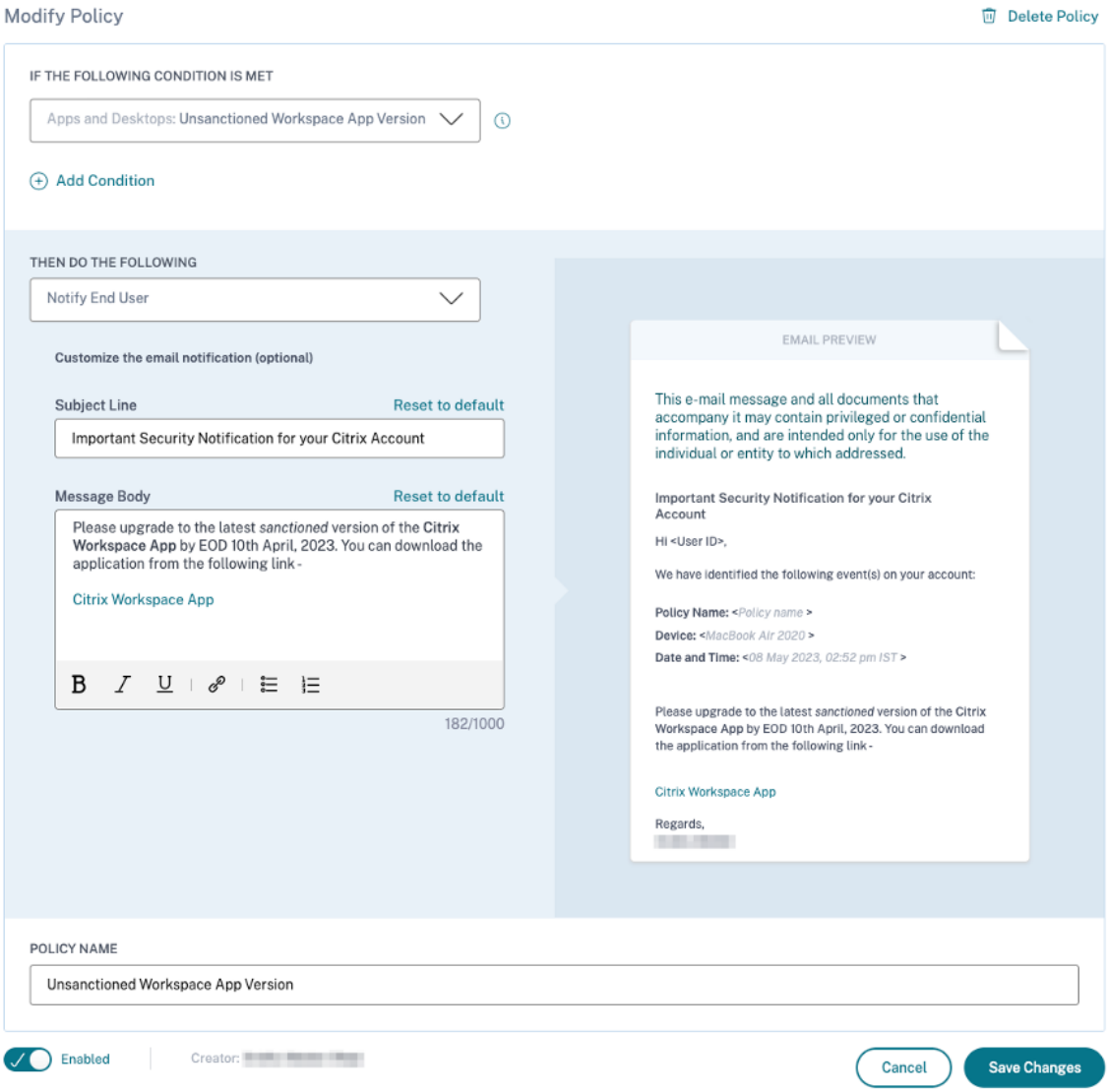



3. Haga clic en **Guardar cambios**.

También puede agregar un banner, un texto de encabezado y un texto de pie de página en el correo electrónico de alerta de seguridad para que parezca legítimo, atraiga la atención de los usuarios y aumente el tiempo de respuesta. Para obtener más información, consulte Configuración del correo electrónico del usuario final.

**Notificar al usuario final** **Notificar al usuario final** es una acción global mediante la cual puede enviar notificaciones por correo electrónico a los usuarios finales cuando se detecta un comportamiento inusual o sospechoso en sus cuentas de Citrix. El asunto del correo electrónico y el cuerpo del mensaje son personalizables. Cuando la acción se aplica después de activar una directiva, se envía una notificación por correo electrónico al usuario. No se solicita ninguna respuesta del usuario final y no se realizan acciones disruptivas en la cuenta del usuario.




Esta acción puede ayudar a resolver varios casos de uso de cumplimiento basados en un disparador de indicadores de riesgo integrado o personalizado. Con el asunto del correo electrónico y el cuerpo del mensaje personalizables, también es lo suficientemente flexible como para atender muchos casos de uso genéricos de notificación al usuario final, que no requieren una respuesta ni una acción disruptiva en la cuenta del usuario.

El correo electrónico contiene la siguiente información:

- Nombre de la directiva asociada a la acción.
- Dispositivo del usuario (si está disponible)
- Fecha y hora de la actividad del usuario

La notificación por correo electrónico al usuario final se envía desde el ID de correo electrónico

security-analytics@cloud.com.

> **Nota:**
>
> El límite diario de las directivas es de **tres** correos electrónicos por usuario. Una vez que se supera este umbral, la acción no se aplica y no se envía ninguna notificación por correo electrónico al usuario final. La acción está visible en la vista de cronología del usuario con el mensaje Se **ha alcanzado el límite diario de correo electrónico del usuario**.

La acción se añade al cronograma de riesgo del usuario. Sin embargo, no es una acción manual y no se puede aplicar a un usuario desde la vista de cronología.

**Personalización del contenido del correo electrónico del usuario** Anteriormente, los administradores de Citrix Analytics se ponían en contacto manualmente con los usuarios finales para proporcionarles instrucciones correctivas sobre la detección de actividades sospechosas, lo que suponía un proceso lento para cerrar un incidente.

La función **de personalización del contenido del correo electrónico del usuario final** se introduce para solicitar la respuesta del usuario final, notificar a los usuarios finales y correos electrónicos informativos. El correo electrónico de respuesta del usuario final busca la validación/respuesta del usuario; sin embargo, un correo electrónico informativo muestra el tipo de actividad sospechosa y qué tipo de acción correctiva ya se ha tomado. El correo electrónico de notificación al usuario final informa al usuario final sobre las infracciones de cumplimiento o las actividades sospechosas en su cuenta de Citrix sin solicitarle una respuesta.

Con la función **de personalización del contenido del correo electrónico del usuario final**, los administradores de Citrix Analytics pueden añadir un mensaje personalizado en la plantilla del cuerpo del correo electrónico informativo o de respuesta del usuario final de solicitud del usuario final o notificación. Con el editor de cuadros de texto enriquecido, un administrador puede modificar el contenido por directiva utilizando varias herramientas de edición, como negrita, cursiva, hipervínculo, etc.

> **Nota**
>
> La función Personalización del contenido del correo electrónico del usuario final solo está disponible para las acciones basadas en directivas y no para las acciones manuales.

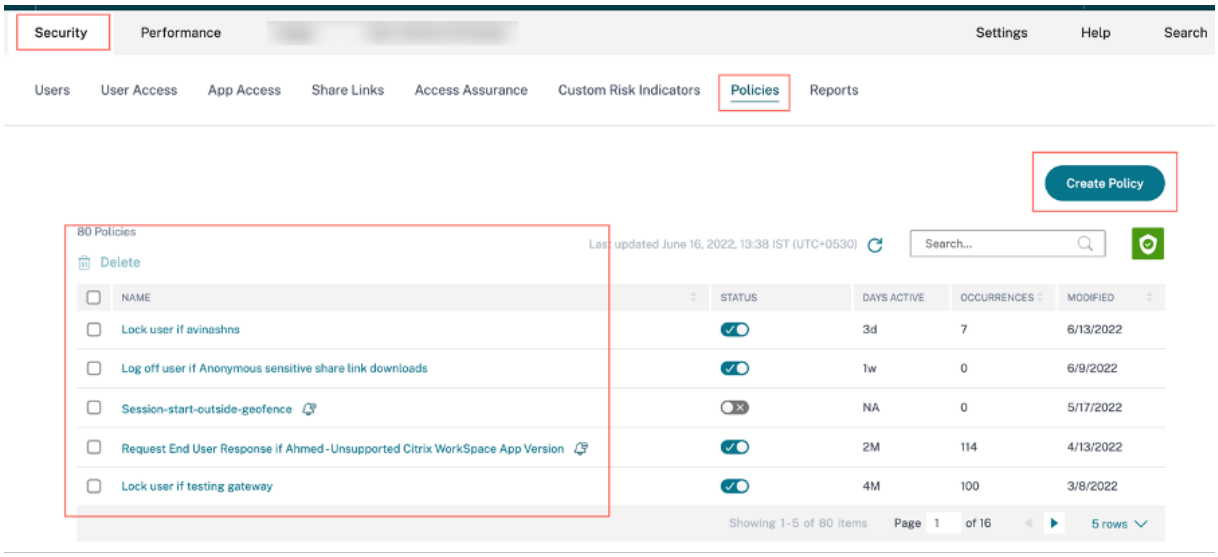
Puede personalizar el contenido de tres tipos de correos electrónicos:

- Solicitar correo electrónico de respuesta para el usuario final.
- Notificar correo electrónico al usuario final
- Correo electrónico enviado cuando se realiza alguna de las siguientes acciones del usuario final:
  - Acción de cierre de sesión en **Citrix Apps and Desktop**

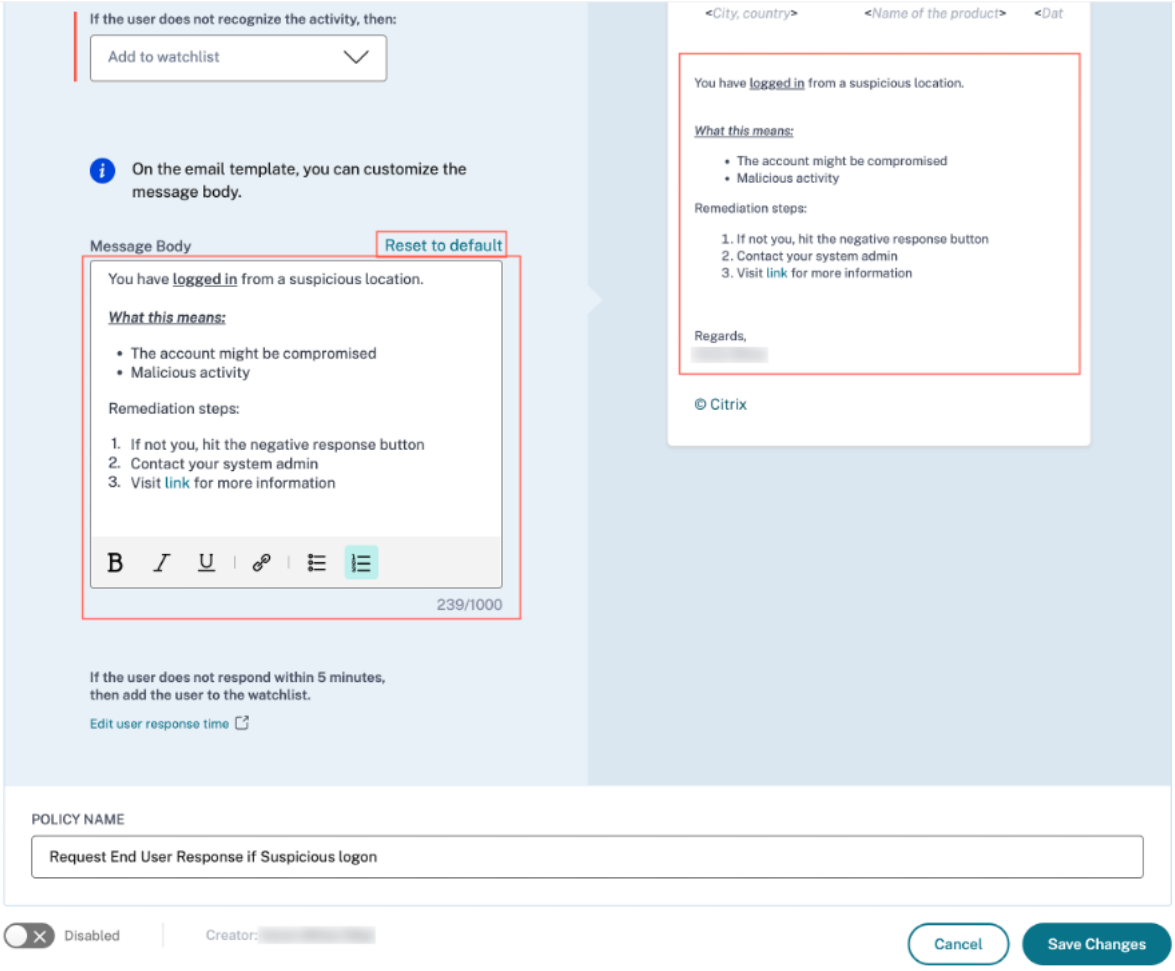
- Cerrar sesión y bloquear al usuario en **Citrix Gateway**

Puede ver la lista de directivas en **la ficha Seguridad > Directivas**.




Se puede ver el cuerpo del correo electrónico personalizado haciendo clic en la directiva existente o al crear una nueva directiva. En el panel derecho, puede obtener una vista previa del contenido actualizado del correo electrónico.




**Nota**

- El administrador puede establecer el contenido en la plantilla predeterminada haciendo clic en el enlace **Restablecer valores predeterminados**. El límite de caracteres para el cuerpo personalizado es de 1000.
- Para la acción **Notificar al usuario final**, el administrador también puede personalizar el campo **Línea de asunto**. Se puede restablecer a los valores predeterminados haciendo clic en el enlace **Restablecer valores predeterminados**. El límite de caracteres para el asunto del correo electrónico personalizado es de 500.

Haga clic en **Guardar cambios** para crear o actualizar la directiva. Cuando se activa la directiva, se envía la siguiente notificación por correo electrónico al usuario final:

- **Solicitar correo electrónico de respuesta del usuario final**: acción de directiva que envía un correo electrónico solicitando la respuesta del usuario.
- **Correo electrónico de notificación al usuario final**: notificación por correo electrónico que se envía a los usuarios finales informándoles de problemas de cumplimiento, actividades sospe-

chosas, etc. en su cuenta de Citrix.

- **Correo electrónico informativo: correo electrónico**informativo que se envía después de una acción del usuario final.

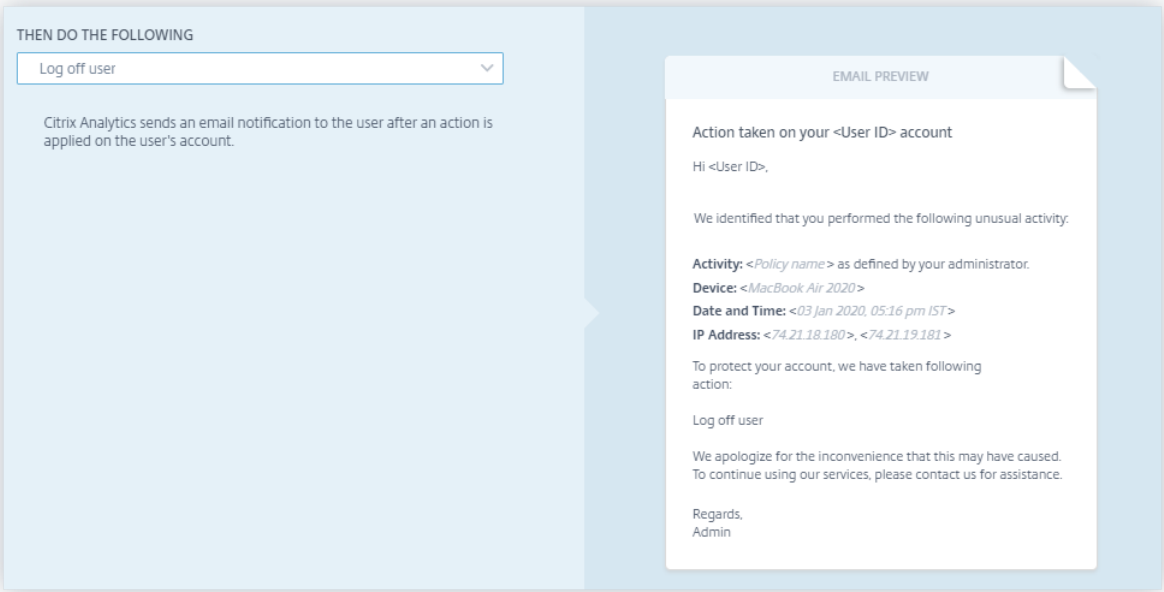
El usuario final puede leer el correo electrónico y completar las acciones de corrección según lo solicite el administrador.

> **Nota**
>
> El administrador con acceso de solo lectura no puede modificar/agregar el cuerpo del correo electrónico.

### Notificar al usuario después de aplicar la acción disruptiva

En este tipo de acción, puede aplicar una acción perjudicial como **Cerrar sesión del usuario y Bloquearusuario** en la cuenta del usuario cuando se detecta una actividad inusual. Cuando se aplica una acción a la cuenta del usuario, es posible que se interrumpan los servicios de su cuenta. En tales casos, el usuario debe ponerse en contacto con el administrador para poder acceder a su cuenta como antes.

Considere un usuario de Citrix Content Collaboration cuya puntuación de riesgo haya superado los 80 en una duración de 80 minutos. Puede cerrar la sesión del usuario. Una vez realizada esta tarea, el usuario no puede acceder a su cuenta y se envía una notificación por correo electrónico al usuario desde el ID de correo electrónico `security-analytics@cloud.com`. El correo electrónico contiene detalles del evento, como la actividad, el dispositivo, la fecha y la hora y la dirección IP. El usuario debe ponerse en contacto con el administrador para acceder a su cuenta como antes.



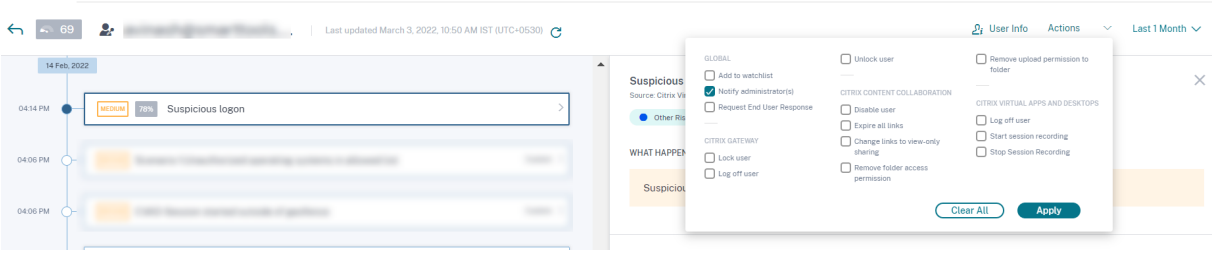

 

## Aplicar una acción manualmente

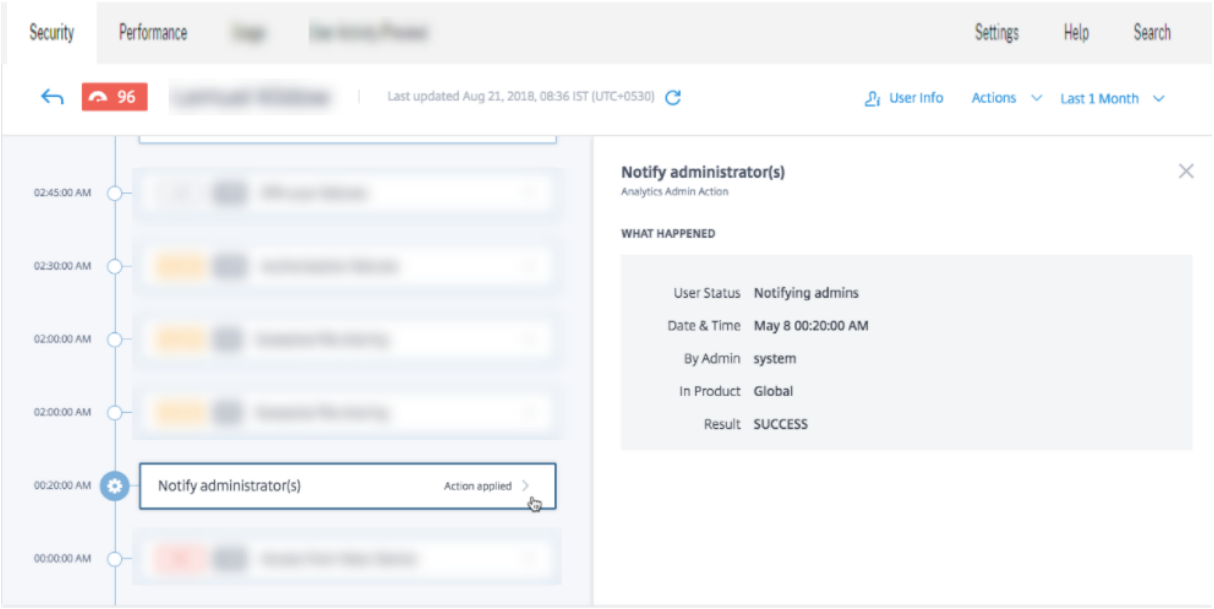
Piense en un usuario, Lemuel, que inicia sesión en una red mediante un dispositivo nuevo por primera vez. Para supervisar su cuenta, ya que su comportamiento es inusual, puede utilizar la acción **Notificar a los administradores**.

Para aplicar la acción manualmente al usuario, debe:

Navegue hasta el perfil de un usuario y seleccione el indicador de riesgo adecuado. En el menú **Acciones**, seleccione la acción **Notificar a los administradores** y haga clic en **Aplicar**.




Se envía una notificación por correo electrónico a todos los administradores o a los seleccionados para supervisar su cuenta. La acción aplicada se agrega a su línea de tiempo de riesgo y los detalles de la acción se muestran en el panel derecho de la página de línea de tiempo de riesgo.




**Notas**

- Si es administrador de Citrix Cloud con permisos de acceso total, de forma predeterminada, las notificaciones por correo electrónico están inhabilitadas para su cuenta de Citrix Cloud. Para recibir notificaciones por correo electrónico, habilítelo en su cuenta de Citrix Cloud. Para obtener más información, consulte Recibir notificaciones por correo electrónico.

> - Si es administrador de Citrix Cloud con permisos de acceso personalizados (solo lectura y acceso completo) para administrar Security Analytics, las notificaciones por correo electrónico están habilitadas para su cuenta de Citrix Cloud. Para dejar de recibir notificaciones por correo electrónico de Citrix Analytics, solicite al administrador de acceso total de Citrix Cloud que elimine su nombre de la lista de distribución de notificaciones a los administradores. Para obtener información sobre, consulte Lista de distribución de correo electrónico.

### Administrar directivas

Puede ver el panel Directivas para administrar todas las directivas creadas en Citrix Analytics para supervisar e identificar incoherencias en la red. En el panel de control Directivas, puede:

1. Ver la lista de directivas
2. Detalles de la directiva
   - Nombre de la directiva
   - Estado: habilitado o inhabilitado.
   - Duración de la directiva: Días que la directiva ha estado activa o inactiva.
   - Ocurrencias: Veces que se activa la directiva.
   - Modificada: Marca de tiempo, solo si se ha modificado la directiva.
3. Eliminar la directiva
   - Para eliminar una directiva, puede seleccionar la directiva que quiere eliminar y hacer clic en **Eliminar**.
   - O bien, puede hacer clic en el nombre de la directiva para dirigirse a la página Modificar directiva. Haga clic en **Eliminar directiva**. En el cuadro de diálogo, confirme su solicitud para eliminar la directiva.
4. Crear una directiva
5. Haga clic en el nombre de una directiva para ver más detalles. También puede modificar la directiva al hacer clic en su nombre. Otras modificaciones que se pueden hacer son las siguientes:
   - Cambia el nombre de la directiva.
   - Condiciones de la directiva.
   - Acciones que se van a aplicar.
   - Habilite o inhabilite la directiva.
   - Elimine la directiva.

> **Nota**
>
> - Si no quiere eliminar la directiva, puede optar por inhabilitarla.
> - Para volver a habilitar la directiva en el panel de directivas, haga lo siguiente:
>  - On the Policies dashboard, click the **Status** slider button and refresh the page. The **Status** slider button turns green.
>  - On the Modify Policy page, click the **Enabled** slider button on the bottom of the page.

### Modelos compatibles

Citrix Analytics admite los siguientes modos de directivas:

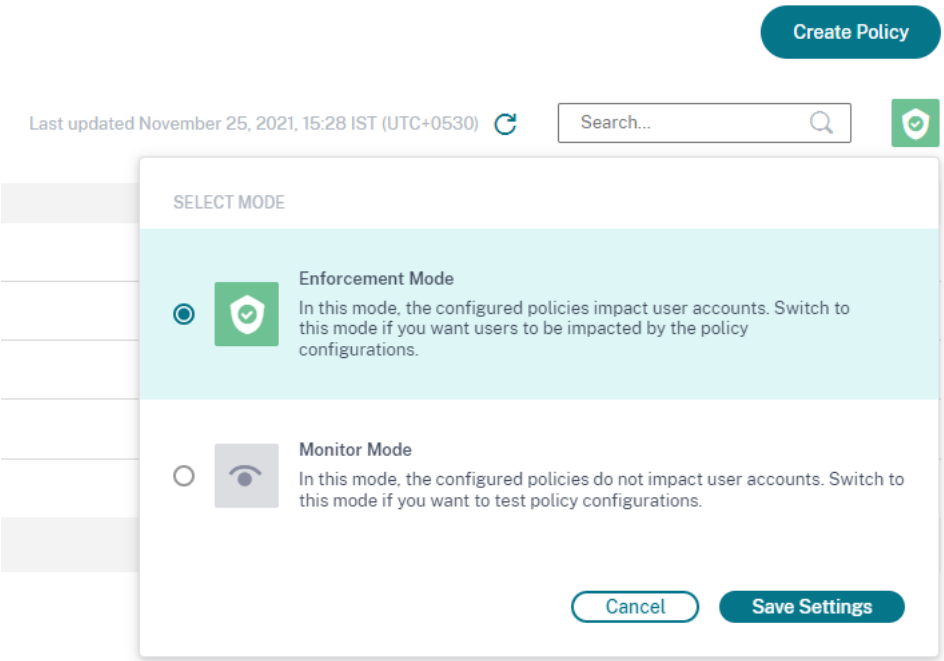
- **Modo de aplicación**: En este modo, las directivas configuradas afectan a las cuentas de usuario.
- **Modo de supervisión**: En este modo, las directivas configuradas no afectan a las cuentas de usuario. Puede establecer directivas en este modo si quiere probar cualquier configuración de directivas.

Siga las instrucciones siguientes para configurar los modos de las directivas:

1. Vaya a **Seguridad** > **Directivas**.
2. En la página **Directivas**, seleccione el icono de la esquina superior derecha que se muestra junto a la barra de **búsqueda**. Aparece la ventana **SELECCIONAR MODO**.
3. Selecciona el modo que prefieras y haga clic en **Guardar configuración**.

> **Nota**
>
> Las directivas predeterminadas creadas por Analytics están configuradas en modo de supervisión. Como resultado, las directivas existentes también heredan este modo. Puede evaluar el impacto de todas las directivas conjuntamente y, a continuación, cambiarlas al modo de aplicación.




### Búsqueda de directivas de autoservicio

En la página de búsqueda de autoservicio, puede ver los eventos de usuario que han cumplido las condiciones definidas en las directivas. La página también muestra las acciones aplicadas a estos eventos de usuario. Filtrar los eventos de usuario en función de las acciones aplicadas.

## Directivas e indicadores de riesgo personalizados preconfigurados

December 7, 2023

Citrix Analytics for Security proporciona una lista de indicadores de riesgo personalizados preconfigurados y una directiva para ayudarle a supervisar la seguridad de su infraestructura Citrix. Las condiciones de estos indicadores de riesgo personalizados preconfigurados y de la directiva ya están definidas de acuerdo con casos de riesgo de seguridad específicos, como usuarios comprometidos, amenazas internas y exfiltración de datos. También puede modificar estas condiciones preconfiguradas o agregar sus propias condiciones según sus requisitos de seguridad y utilizar los indicadores de riesgo personalizados para mitigar los riesgos.

Actualmente, los indicadores de riesgo personalizados preconfigurados están disponibles para los siguientes casos:

- Geocercas

- Acceso por primera vez

### Indicadores de riesgo personalizados preconfigurados para el caso de geocercas

Utilice los siguientes indicadores de riesgo personalizados preconfigurados para detectar eventos de usuarios desde fuera de las áreas geocercadas.

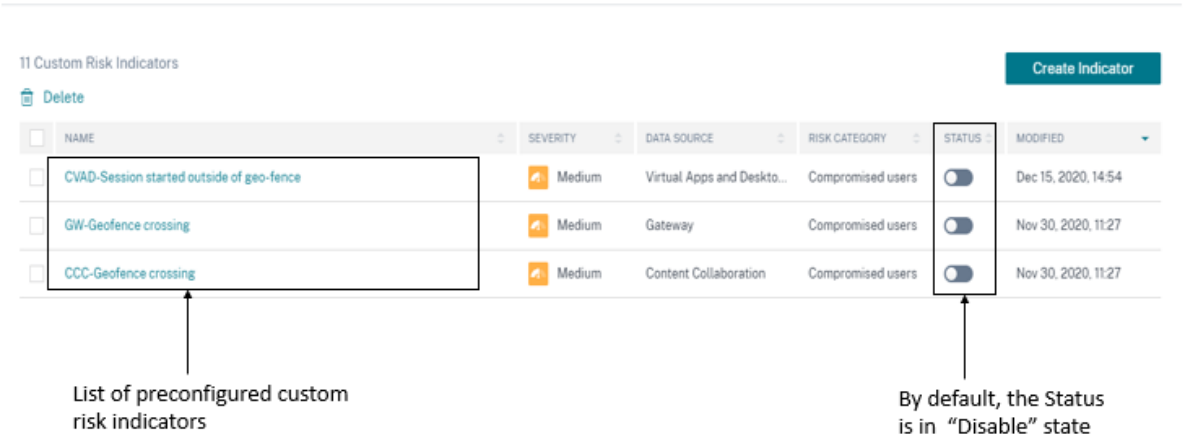
- Sesión CVAD iniciada fuera de la geocerca
- Cruce de geocercas GW

Los indicadores de riesgo personalizados preconfigurados se activan cada vez que los usuarios acceden a los productos Citrix desde fuera de su país de operación habitual o de la geocerca. De forma predeterminada, la geocerca se establece en "Estados Unidos". Puede establecer el país que necesite como geocerca.

> **Nota**
>
> La *sesión de CVAD iniciada fuera del indicador de riesgo de geocercado* está vinculada a la **configuración de geocercado** de la función Ubicación de Access Assurance. Por lo tanto, no se pueden modificar directamente los países geocercados en el estado del indicador de riesgo. Para actualizar los países geocercados en el indicador de riesgo, seleccione los países en la **configuración de geocercado del** panel de control de ubicación de Access Assurance. Para obtener más información, consulte el panel de control de ubicación de Access assurance.

Para ver los indicadores de riesgo personalizados preconfigurados, seleccione **Seguridad > Indicadores de riesgo personalizados**.

De forma predeterminada, los indicadores de riesgo personalizados preconfigurados están inhabilitados. Utilice el botón **STATUS** para activarlas.




En la tabla siguiente se describen los distintos indicadores de riesgo personalizados preconfigurados para geocercas.

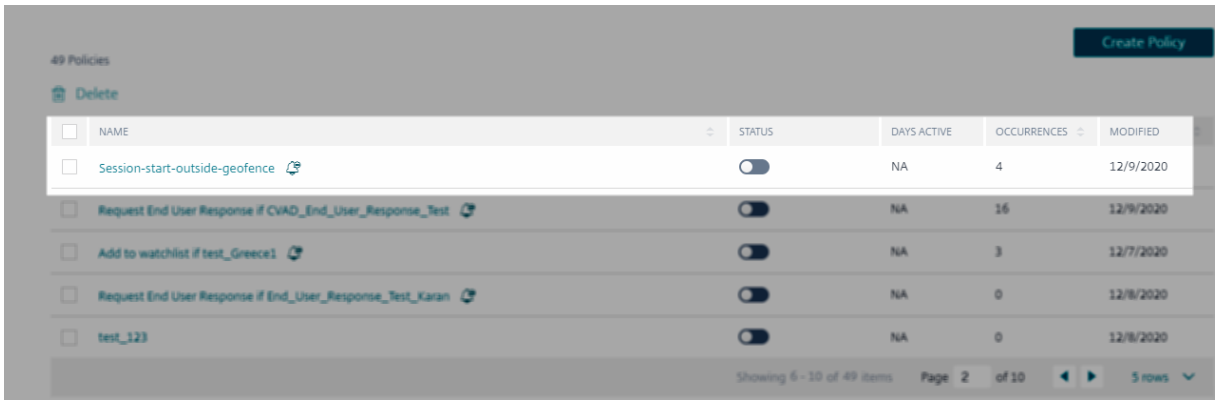
 

| Nombre del indicador de riesgo personalizado | Escenario | Condiciones del indicador personalizado | Origen de datos | Categoría de riesgo |
|---|---|---|---|---|
| Sesión CVAD iniciada fuera de la geocerca | El usuario ha iniciado una sesión virtual fuera de su país de operación | Tipo de evento = session.Logon Country! = “Estados Unidos” | Aplicación Citrix Workspace | Usuarios comprometidos |
| Cruce de geocercas GW | El usuario tiene una autenticación correcta desde fuera de su país de operación | Tipo de evento = “VPN_AI”Y país. = “Estados Unidos” | Citrix Gateway (local) | Usuarios comprometidos |

### Directiva preconfigurada para el caso de geocercas

Citrix proporciona una directiva preconfigurada que aplica la acción **Solicitar respuesta del usuario final** a una cuenta de usuario cada vez que el usuario inicia una sesión virtual desde fuera de su país de operación. El usuario recibe un correo electrónico y, en función de la respuesta del usuario, se toman las medidas adecuadas, como agregar el usuario a la lista de seguimiento o notificar al administrador para que tome medidas adicionales. Para obtener más información, consulte Solicitar la respuesta del usuario final.

Para ver la directiva preconfigurada, seleccione **Seguridad > Directivas**.




En la tabla siguiente se describe la directiva preconfigurada para geocercas.

| Nombre de directiva | Escenario | Condiciones de la directiva | Acción aplicada |
|---|---|---|---|
| Inicio de sesión fuera de la geocerca | Capacidad de un administrador para validar la legitimidad del usuario mediante la acción “Solicitar respuesta del usuario final”cuando el usuario inicia la sesión virtual fuera de su país de operación | Uso con indicador de riesgo personalizado preconfigurado: “La sesión de CVAD se inició fuera de la geocerca” | Solicitar respuesta del usuario final<br>En función de la siguiente respuesta del usuario, se aplica la acción correspondiente<br>Si el usuario no reconoce la actividad: **Agregar a la lista de seguimiento**<br>Si el usuario reconoce la actividad: **No es necesario realizar ninguna acción**<br>Si el usuario no responde en los 60 minutos siguientes a la recepción del correo electrónico: **Añádelo a la lista de seguimiento** |

> **Nota**
>
> La acción **Solicitar respuesta de usuario final** solo se admite en la región Estados Unidos. Por lo tanto, si su organización está incorporada a la región de la Unión Europea en Citrix Cloud, la directiva preconfigurada no se aplica a su cuenta. Para utilizar la directiva preconfigurada,

> modifique la directiva y seleccione otra acción de su elección.

### Cree su propia directiva con indicadores de riesgo personalizados preconfigurados para geocercas

También puede crear sus propias directivas con estos indicadores de riesgo personalizados preconfigurados y aplicar acciones como bloquear usuarios o cerrar la sesión de los usuarios cada vez que se activen los indicadores. Para obtener información sobre cómo crear directivas, consulte Configurar directivas y acciones.

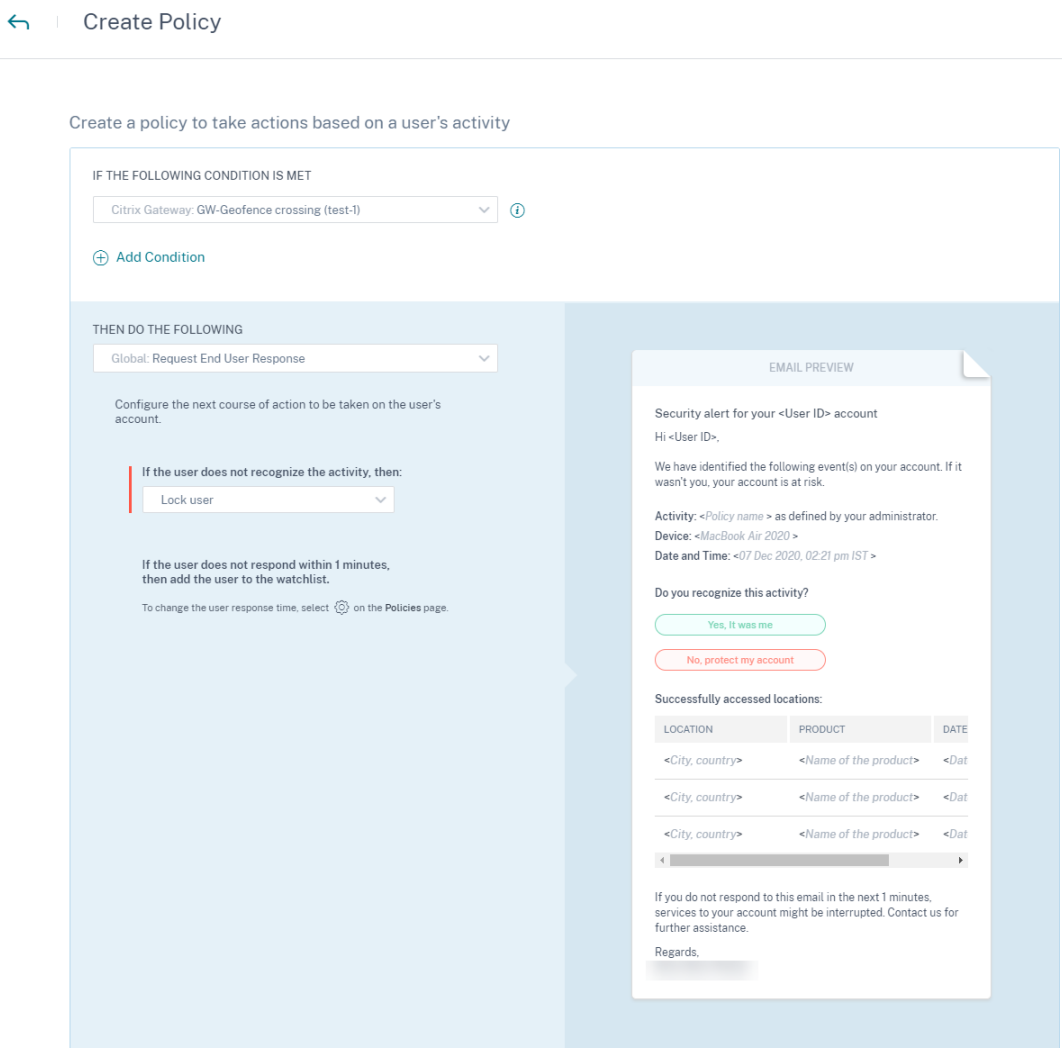
El siguiente ejemplo muestra una directiva que bloquea a los usuarios que intentan acceder a los servicios de Citrix desde fuera de los Estados Unidos. El acceso del usuario se bloquea si el usuario no reconoce su actividad de acceso.

**Estado**: cruce de geocerca GW

**Acción**: Solicitar respuesta del usuario final

**Acción siguiente**: Bloquear al usuario si el usuario no reconoce la actividad




> **Nota**
>
> La acción **Solicitar respuesta de usuario final** solo se admite en la región Estados Unidos. Por lo tanto, si su organización está integrada en la región Unión Europea, seleccione otra acción de su elección en lugar de la acción **Solicitar respuesta del usuario final**.

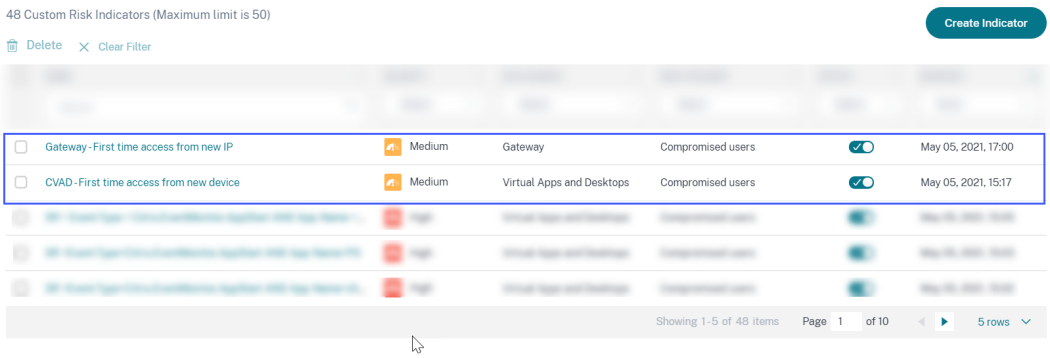
## Indicadores de riesgo personalizados preconfigurados para el primer caso de acceso

Utilice los siguientes indicadores de riesgo personalizados para detectar los eventos de usuario en los escenarios de acceso por primera vez:

- Acceso por primera vez al CVAD desde un nuevo dispositivo
- Acceso por primera vez a la puerta de enlace desde una nueva IP

De forma predeterminada, estos indicadores de riesgo personalizados preconfigurados están habilitados. Utilice el botón **STATUS** si quiere inhabilitarlos.




En la tabla siguiente se describen los indicadores de riesgo personalizados preconfigurados para el acceso por primera vez.

| Nombre del indicador personalizado | Escenario | Condiciones preconfiguradas | Origen de datos | Categoría de riesgo |
|---|---|---|---|---|
| Acceso por primera vez al CVAD desde un nuevo dispositivo | Cuando un usuario de la aplicación Citrix Workspace inicia sesión desde una de las siguientes opciones | Las condiciones siguientes están habilitadas de forma predeterminada | Citrix Virtual Apps and Desktops locales y Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service) | Usuarios comprometidos |
| | Un nuevo dispositivo | La primera vez que se trata de un nuevo ID de dispositivo. | | |

| Nombre del indicador personalizado | Escenario | Condiciones preconfiguradas | Origen de datos | Categoría de riesgo |
|---|---|---|---|---|
| | Un dispositivo existente que no se ha utilizado durante los últimos 90 días. | `Event-Type = "Session.Logon"AND Client-Type IN ("XA.Receiver.Windows", "XA.Receiver.Mac", "XA.Receiver.Chrome", "XA.Receiver.Android", "XA.Receiver.Linux", "XA.Receiver.iOS")` | | |
| Acceso por primera vez a la puerta de enlace desde una nueva IP | Cuando un usuario de Citrix Gateway firma correctamente una de las siguientes opciones | Las condiciones siguientes están habilitadas de forma predeterminada | Citrix Gateway | Usuarios comprometidos |
| | Una nueva dirección IP pública | La primera vez para una nueva IP de cliente | | |

| Nombre del indicador personalizado | Escenario | Condiciones preconfiguradas | Origen de datos | Categoría de riesgo |
|---|---|---|---|---|
| | Una dirección IP pública existente que no se ha utilizado durante los últimos 90 días. | `Event-Type = "Authentication"AND Status-Code = "Successful login"AND Client-IP-Type != "private"AND Access-Insight-Flags = 1` | | |

En la barra de condiciones, también puede agregar sus propias condiciones además de las condiciones preconfiguradas para identificar amenazas según sus necesidades.

Por ejemplo, si quiere identificar los eventos de usuario de un país determinado, puede agregar la dimensión país junto con la condición preconfigurada:

- `Event-Type = "Session.Logon"AND Client-Type IN ("XA.Receiver.Windows", "XA.Receiver.Mac", "XA.Receiver.Chrome", "XA.Receiver.Android", "XA.Receiver.Linux", "XA.Receiver.iOS")AND Country = “United States”`
- `Event-Type = "Authentication"AND Status-Code = "Successful login" AND Client-IP-Type != "private"AND Access-Insight-Flags = 1 AND Country = “United States”`

## Configuración del correo electrónico del usuario final

December 7, 2023

La configuración del correo electrónico del usuario final controla la plantilla de correo electrónico asociada a la acción global Solicitar respuesta del usuario final. Aplica esta acción para obtener una

respuesta de los usuarios ante cualquier actividad inusual detectada en su cuenta. Los usuarios responden a través de los correos electrónicos que reciben de Citrix Analytics for Security.

Puede usar la configuración del correo electrónico para:

- Agregue un banner, un texto de encabezado y un texto de pie de página adecuados para atraer la atención del usuario y obtener su respuesta. También hace que su correo electrónico parezca más legítimo.
- Agregue la duración (en minutos) dentro del cual el usuario debe responder a su correo electrónico. Si el usuario no responde dentro del tiempo de respuesta, Citrix Analytics aplica la acción especificada al usuario.

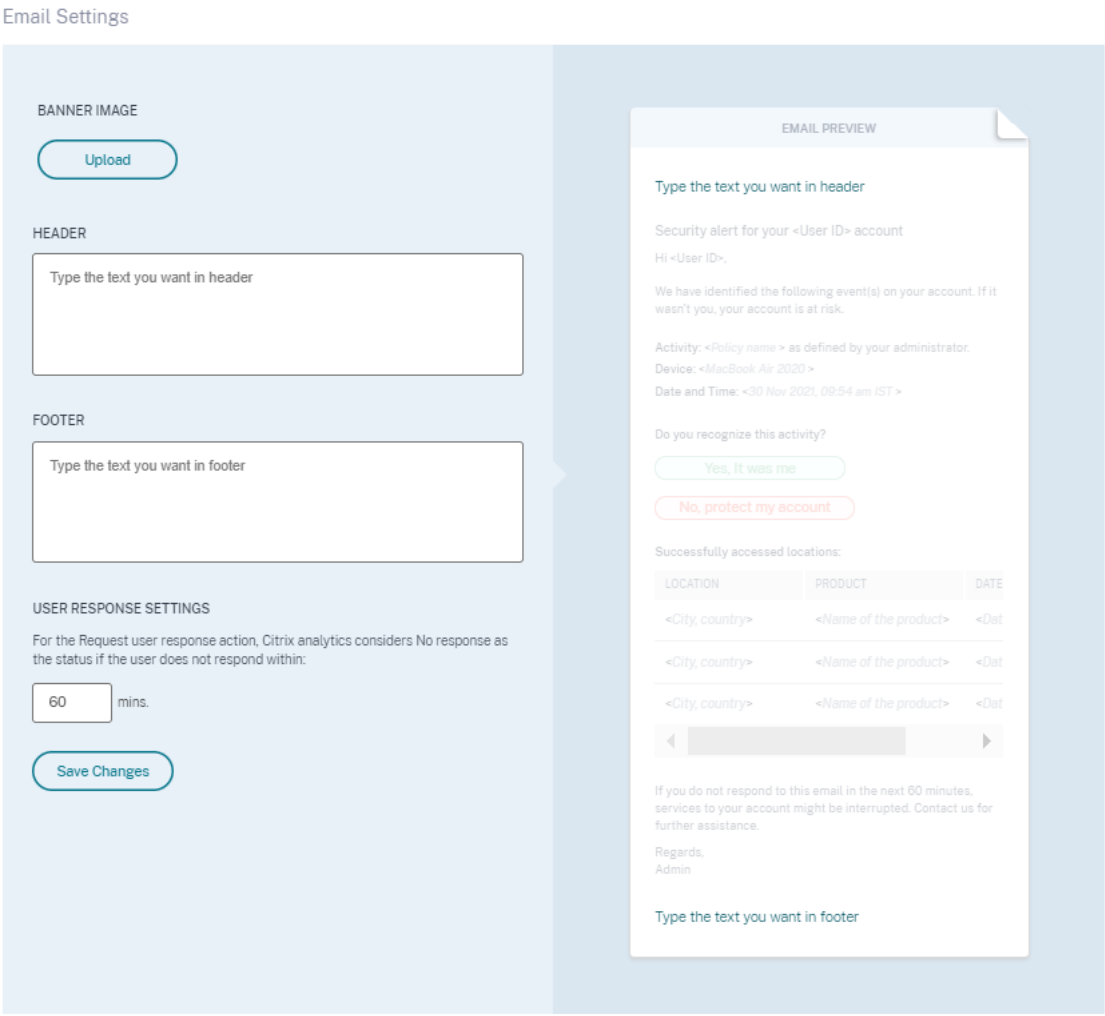
## Modificar la configuración de correo

Para modificar la configuración del correo electrónico:

1. En la barra superior, haga clic en **Configuración > Configuración de alertas > Configuración del correo electrónico del usuario final**.


2. Haga clic en Modificar para subir o navegar por una imagen de banner. Al subir un archivo de imagen, asegúrese de que la imagen cumpla con los siguientes requisitos:
   - Formatos compatibles: JPEG o PNG
   - Dimensiones máximas: 400* 100 píxeles
   - Tamaño máximo de archivo: 5 MB
3. Introduzca sus textos en los campos **HEADER** y **FOOTER**. Estos campos son opcionales.
4. Introduzca la hora en la configuración de respuesta del usuario.
5. Obtenga una vista previa del correo electrónico y haga clic en **Guardar cambios**.




## Configuración de correo electrónico de administrador

December 7, 2023

La página **Configuración del correo electrónico del administrador** le permite configurar los destinatarios de las listas de distribución personalizadas para las alertas del sistema. Esto garantiza que los administradores reciban alertas del sistema útiles para ellos.

La función de **configuración del correo electrónico del administrador** ofrece las siguientes funcionalidades:

Vea las alertas del sistema, las listas de distribución de correo electrónico que reciben la alerta, el último usuario que modificó la configuración de la alerta y la última fecha en que se modificó la alerta. Modifique la configuración de alertas. Cambie la lista de distribución de destino para varias alertas

del sistema.

### Modificar la configuración de alertas

Para modificar la configuración de alertas:

1. En la barra superior, haz clic en **Configuración > Configuración de alertas > Configuración del correo electrónico del administrador**.


2. Haga clic en la alerta cuya lista de distribución de correo electrónico desee modificar.
3. Seleccione las listas de distribución que deben recibir la alerta en la lista desplegable **Elija la lista de distribución de correo electrónico**.
   También puede crear su propia lista de distribución haciendo clic en **Crear lista de distribución de correo electrónico**. Para obtener más información, consulte Crear una lista de distribución de correo electrónico.
4. Haga clic en **Guardar cambios**.

## Lista de control

February 13, 2023

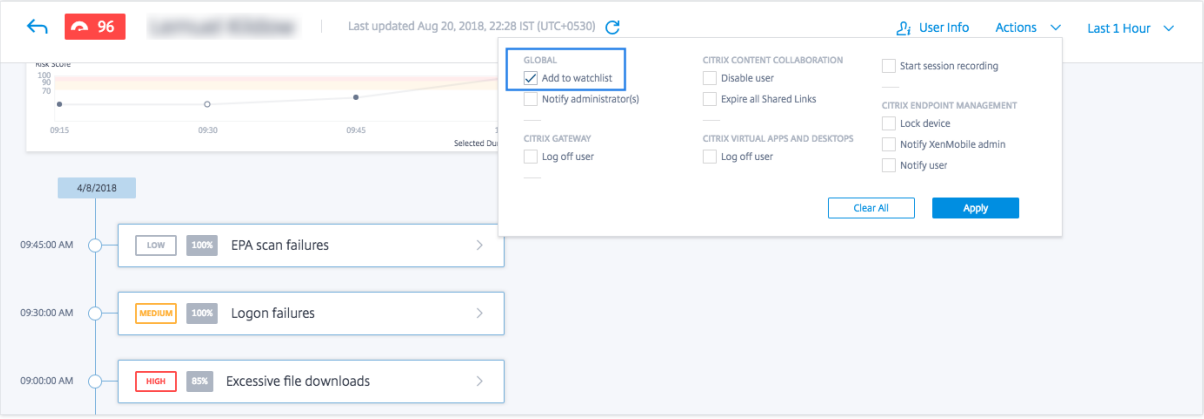
Use listas de seguimiento para monitorear la actividad de usuarios específicos en busca de posibles amenazas. Por ejemplo, puede supervisar a los usuarios que no trabajan a tiempo completo en su organización o a los usuarios que activan un indicador de riesgo específico con frecuencia.

### Cómo añadir un usuario a la lista de seguimiento

Puede añadir un usuario a la lista de seguimiento manualmente o puede definir políticas que, cuando se activen, añadan un usuario a la lista de seguimiento.

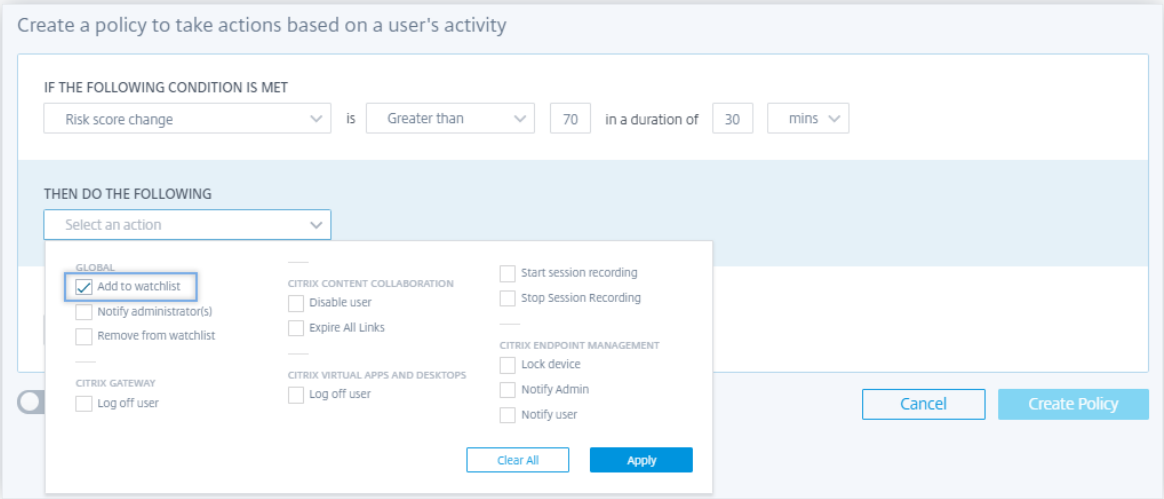
Para añadir un usuario a la lista de seguimiento manualmente, navega hasta el perfil del usuario en el cronograma de riesgos. A continuación, en el menú **Acciones**, selecciona **Añadir a la lista de seguimiento**. Haga clic en **Aplicar** y siga las instrucciones para ejecutar la acción.




Para añadir un usuario a la lista de seguimiento mediante políticas, cree una política con un conjunto de condiciones que deben cumplirse. Selecciona la acción **Añadir a la lista de seguimiento** . Cuando se cumplen las condiciones, el usuario se añade a la lista de seguimiento. Por ejemplo, puede añadir un usuario a la lista de seguimiento si el cambio en la puntuación de riesgo del usuario es superior a 70 en 30 minutos.

Para obtener más información sobre la creación de políticas, consulte Configurar políticas y acciones.



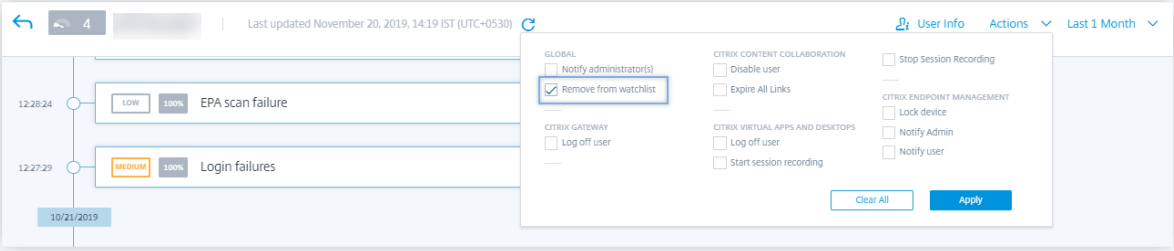

## Cómo eliminar a un usuario de la lista de seguimiento

Puede eliminar un usuario de la lista de seguimiento manualmente o puede definir políticas que, cuando se activen, eliminen a un usuario de la lista de seguimiento.

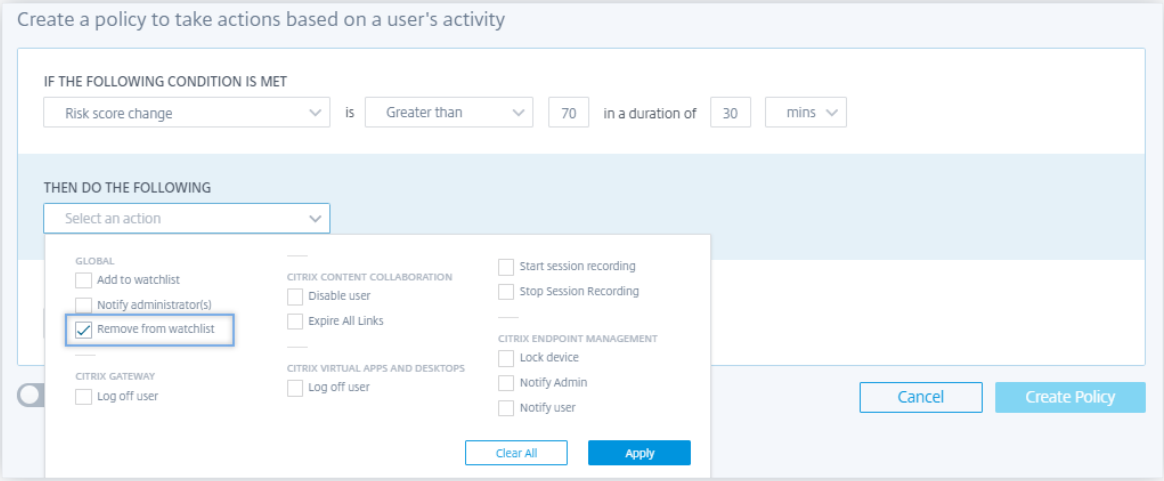
Para eliminar a un usuario de la lista de seguimiento manualmente, navega hasta el perfil del usuario en la cronología de riesgos. A continuación, en el menú **Acciones**, selecciona **Eliminar de la lista de seguimiento**. Haga clic en **Aplicar** y siga las instrucciones para ejecutar la acción.

> **Nota**
>
> Cuando un usuario esté en la lista de seguimiento y quieras eliminarlo, verás la opción **Eliminar de la lista de seguimiento** en el menú **Acciones** .




Para eliminar a un usuario de la lista de seguimiento mediante políticas, cree una política con un conjunto de condiciones que deben cumplirse. Selecciona la acción **Eliminar de la lista de seguimiento** . Cuando se cumplen las condiciones, el usuario se elimina de la lista de seguimiento. Por ejemplo, puede que desees eliminar a un usuario de la lista de seguimiento si el cambio en la puntuación de riesgo del usuario es inferior a 70 en 60 minutos. Para obtener más información sobre la creación de políticas, consulte Configurar políticas y acciones.




## Cómo monitorear a los usuarios en una lista de seguimiento

En el panel **Seguridad > Usuarios**, consulte lo siguiente:

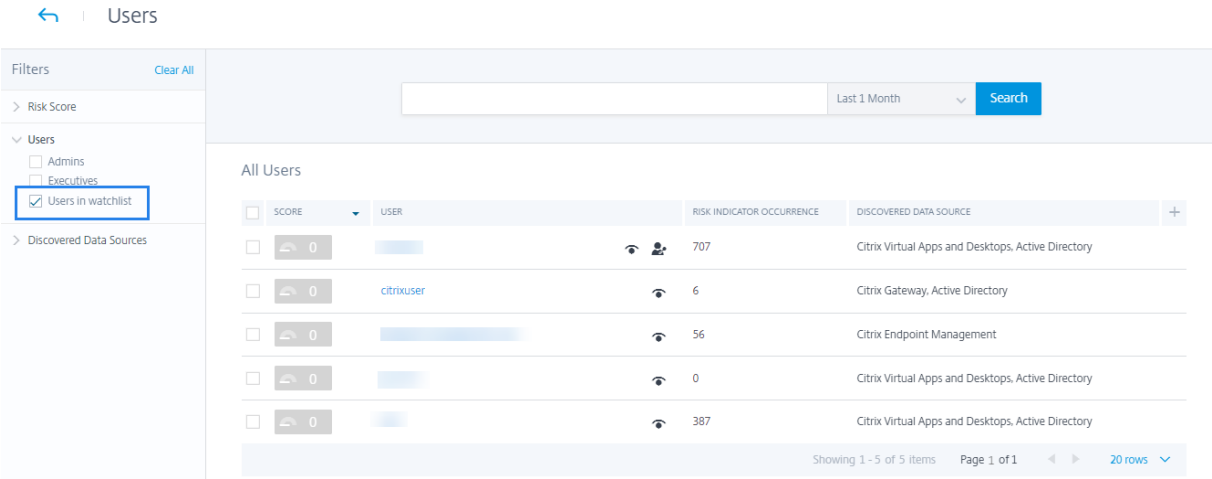
- Resumen del número de usuarios de la lista de seguimiento durante los últimos 13 meses. Haga clic en la casilla para ver la lista de todos los usuarios de la lista de seguimiento en el panel **Usuarios en la lista de seguimiento** .

- Los cinco usuarios principales de la lista de seguimiento figuran en función de la puntuación de riesgo. En el panel **Usuarios en la lista** de seguimiento, vea la puntuación de riesgo y las incidencias de los indicadores de riesgo junto con el nombre del usuario. Haga clic en **Ver más** para ver la lista de todos los usuarios de la lista de seguimiento de la página **Usuarios** .
- Los usuarios más riesgosos que están en la lista de seguimiento. En el panel **Usuarios de riesgo**, el icono en forma de «ojo» que aparece junto al usuario indica que el usuario está en la lista de seguimiento.

En la página **Usuarios**, consulta la lista de todos los usuarios de la lista de seguimiento. Vea detalles como la puntuación de riesgo, el número de indicadores de riesgo activados y las fuentes de datos asociadas de un usuario.

Usa el cuadro de búsqueda para buscar usuarios y los detalles de sus eventos. Seleccione el período de tiempo para ver las ocurrencias del indicador de riesgo para el período específico.




## Notificación por correo electrónico semanal

December 7, 2023

Citrix Analytics envía notificaciones semanales por correo electrónico en las que se resumen las exposiciones a los riesgos de seguridad en la infraestructura de TI de su organización. La notificación semanal lo mantiene al tanto e informado sobre los eventos de riesgo y sus ocurrencias en la semana anterior. Puede averiguar si algún evento requiere su atención o acciones sin iniciar sesión en Citrix Analytics. Esta información lo mantiene informado sobre lo que sucede en su dominio de seguridad de TI.

### Habilitar notificaciones por correo

- Si es administrador de Citrix Cloud con permiso de acceso completo o personalizado, las notificaciones por correo electrónico están inhabilitadas de forma predeterminada en su cuenta de Citrix Cloud. Para recibir notificaciones por correo electrónico de cualquier servicio de Citrix Cloud, como Citrix Analytics, habilite la opción de notificación en su Citrix Cloud. Para obtener más información, consulte Recibir notificaciones por correo electrónico. Las preferencias de notificación no están disponibles para los administradores que se agregan a través de Active Directory/Azure AD Groups.
- De forma predeterminada, las notificaciones por correo electrónico se envían a la lista predeterminada de administradores de seguridad de Citrix. Puede cambiar esto configurando los destinatarios de las listas de distribución personalizadas para las alertas semanales. Para obtener más información, consulta Configuración de correo electrónico de administrador.

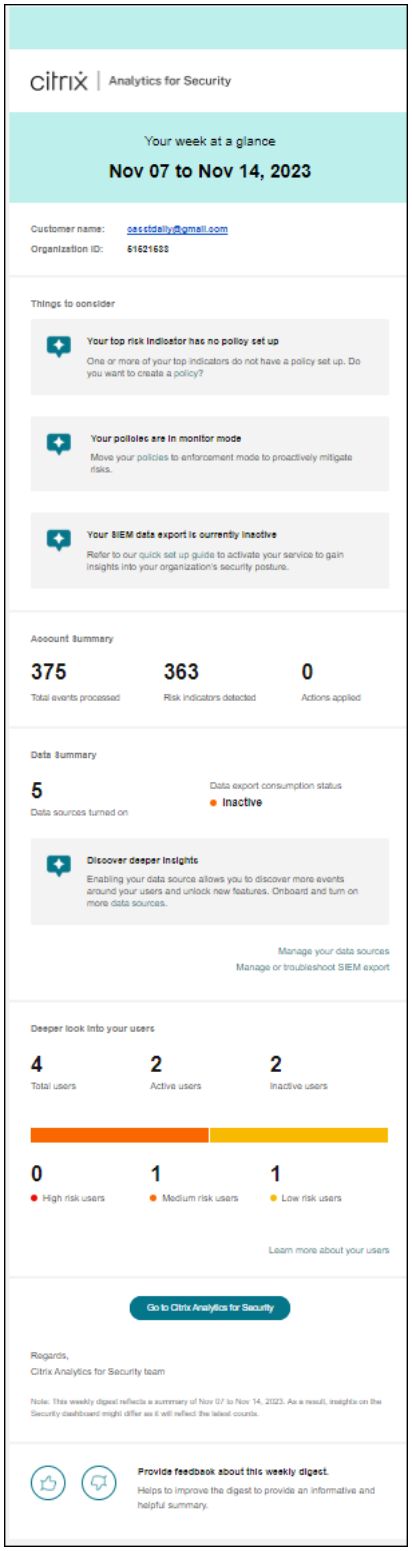
### ¿Cuándo recibe un correo electrónico de Citrix Analytics?

Todos los martes, Citrix Cloud le envía una notificación por correo electrónico desde donotreplynotifications@citrix.com.

La notificación por correo electrónico proporciona la siguiente información:

- Resumen del número total de eventos procesados, los indicadores de riesgo detectados y las acciones aplicadas
- Resumen del número total de fuentes de datos activas y del estado del consumo de exportación de datos
- Los tres principales indicadores de riesgo
- Las tres acciones principales tomadas en relación con los indicadores de riesgo
- Número total de usuarios activos y número total de usuarios riesgosos
- Cualquier evento o acción que requiera su atención



citrix | Analytics for Security

Your week at a glance

**Nov 07 to Nov 14, 2023**

Customer name: oesstdaily@gmail.com
Organization ID: 61621688

Things to consider

**Your top risk indicator has no policy set up**
One or more of your top indicators do not have a policy set up. Do you want to create a policy?

**Your policies are in monitor mode**
Move your policies to enforcement mode to proactively mitigate risks.

**Your SIEM data export is currently inactive**
Refer to our quick set up guide to activate your service to gain insights into your organization's security posture.

Account Summary

| 375 | 363 | 0 |
|---|---|---|
| Total events processed | Risk indicators detected | Actions applied |

Data Summary

5
Data sources turned on

Data export consumption status
Inactive

**Discover deeper insights**
Enabling your data source allows you to discover more events around your users and unlock new features. Onboard and turn on more data sources.

Manage your data sources
Manage or troubleshoot SIEM export

Deeper look into your users

| 4 | 2 | 2 |
|---|---|---|
| Total users | Active users | Inactive users |

| 0 | 1 | 1 |
|---|---|---|
| High risk users | Medium risk users | Low risk users |

Learn more about your users

Go to Citrix Analytics for Security

Regards,
Citrix Analytics for Security team

Note: This weekly digest reflects a summary of Nov 07 to Nov 14, 2023. As a result, insights on the Security dashboard might differ as it will reflect the latest counts.

**Provide feedback about this weekly digest.**
Helps to improve the digest to provide an informative and helpful summary.

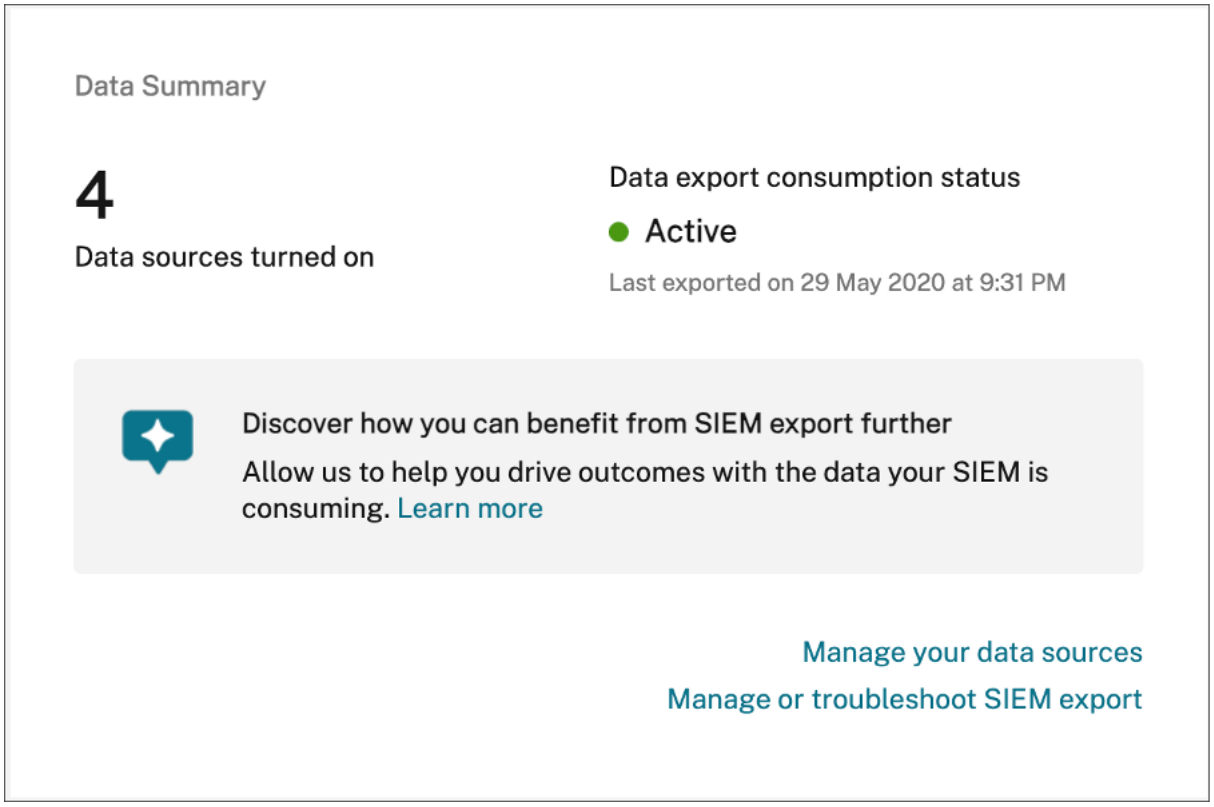
 

### Resumen de la cuenta

El correo electrónico semanal proporciona un resumen del número total de eventos procesados, los indicadores de riesgo detectados y las acciones aplicadas.


### Resumen de datos

El correo electrónico semanal también proporciona información sobre las fuentes de datos que se han activado, junto con el estado del consumo de exportación de datos.




Haga clic en **Administrar las fuentes de datos** en el correo electrónico para ver la página **Fuentes de datos** en Citrix Analytics. Puede incorporar la fuente de datos y activar el procesamiento de datos para permitir que Citrix Analytics permita el procesamiento de datos. Para obtener más información sobre cómo habilitar el análisis, consulte Habilitar el análisis en las fuentes de datos.

Haga clic en **Administrar o solucionar problemas de exportación de SIEM** para ver la página Exportaciones de datos en Citrix Analytics para solucionar problemas de su entorno y administrar la configuración de exportación de datos.

### Información a los usuarios

El correo electrónico semanal proporciona información sobre el número total de usuarios y usuarios que han actuado de manera arriesgada.

- **Número de usuarios de alto riesgo** : identificado en rojo. Representan una amenaza inmediata para la organización.
- **Número de riesgo medio** : identificado en naranja. Tienen varias infracciones graves en su cuenta durante la semana seleccionada y deben ser monitoreadas de cerca.
- **Número de usuarios de bajo riesgo** : identificado en amarillo. Tienen algunas infracciones graves en su cuenta, pero potencialmente no se consideran una amenaza.

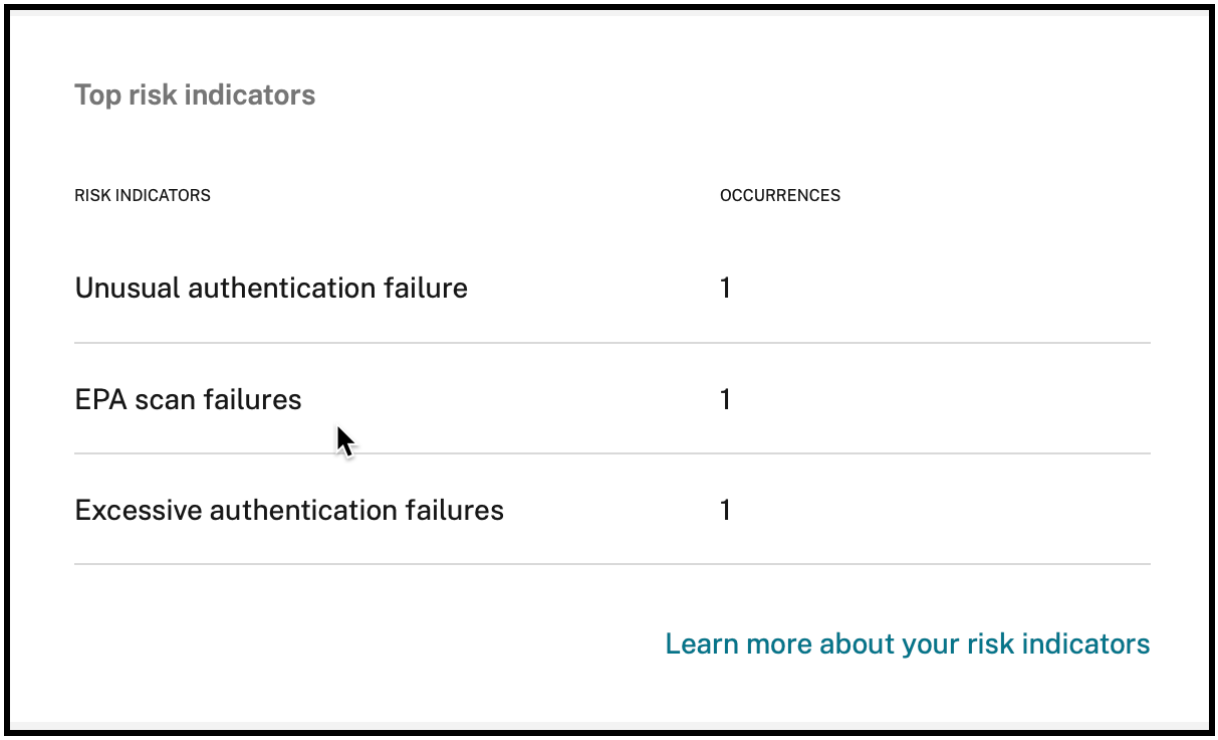

Para obtener más información, consulte Usuarios de riesgo.

Haga clic en **Más información sobre sus usuarios** para ver la página **Usuarios riesgosos** de Citrix Analytics. Puede obtener información más detallada sobre los usuarios activos y la categorización de riesgos.

### Principales indicadores de riesgo

El correo electrónico semanal proporciona información sobre los tres principales indicadores de riesgo y el número de incidencias de la semana seleccionada. Según el número de casos, se muestran los indicadores de riesgo predeterminados y personalizados para la semana seleccionada.



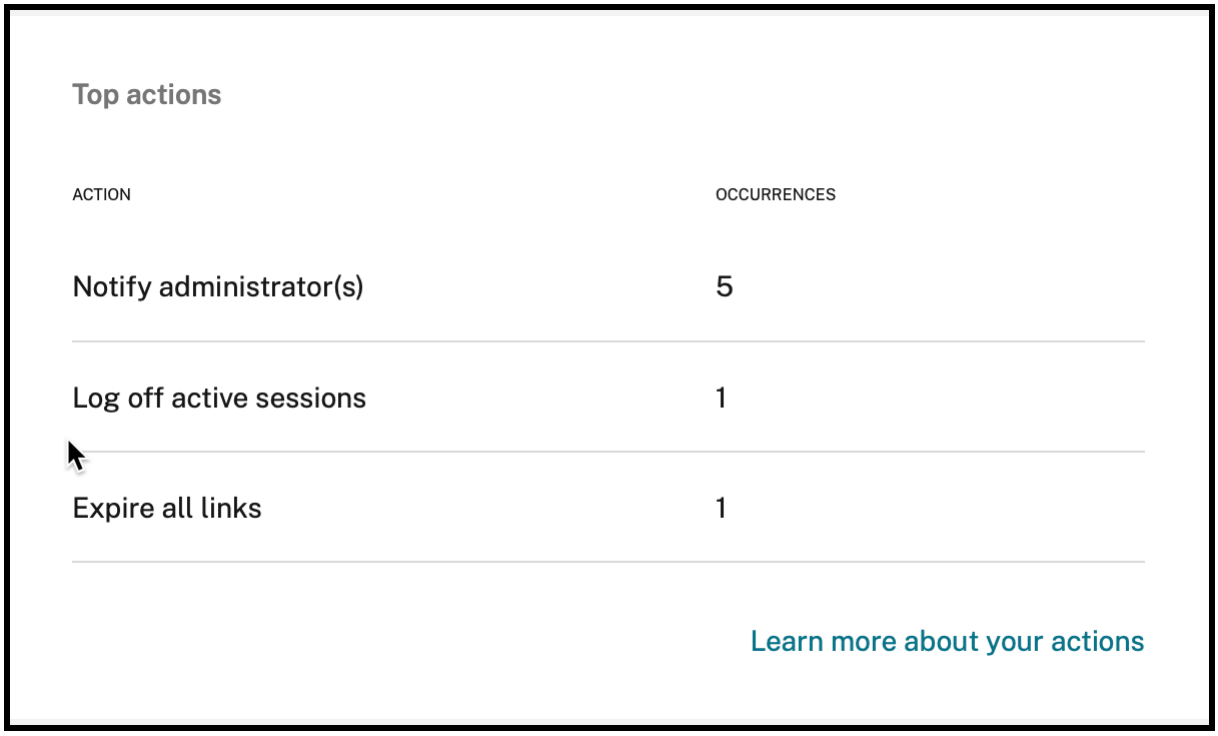

Para obtener más información, consulte los indicadores de riesgo.

Haga clic en **Más información sobre sus indicadores de riesgo** en el correo electrónico para ver la página de **descripción general de los indicadores de riesgo** en Citrix Analytics.

### Acciones principales

El correo electrónico semanal proporciona información sobre las tres acciones principales tomadas en respuesta a las amenazas sospechosas y anómalas que se produjeron la semana pasada. Según el número de ocurrencias, se muestran las acciones globales y las acciones de Citrix Gateway para la semana seleccionada.



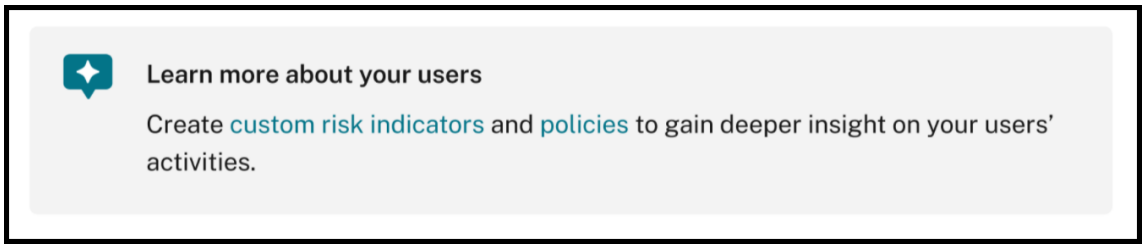

Para obtener más información sobre las acciones y la configuración de una acción, consulte Directivas y acciones.

Haga clic en **Más información sobre sus acciones** en el correo electrónico para ver la página **Acciones principales** de Citrix Analytics.

### ¿Qué medidas debe tomar después de recibir el correo electrónico?

Los correos electrónicos semanales le permiten averiguar si algún evento o acción requiere su atención.

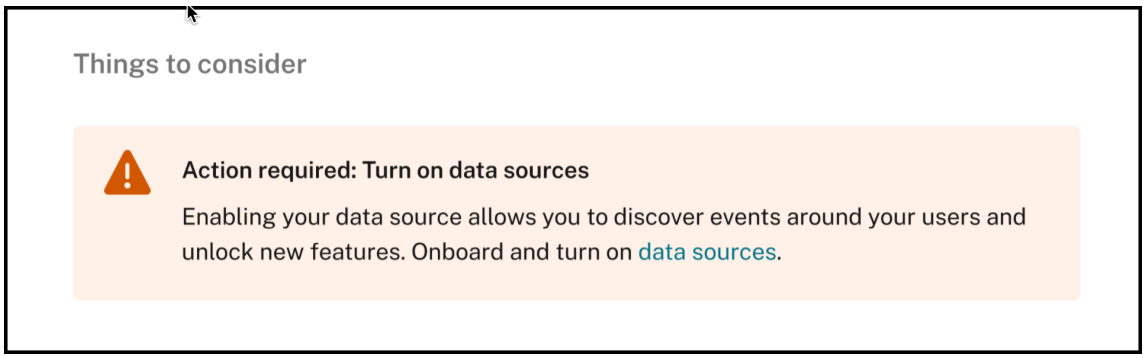
- Si no se ha detectado ningún indicador de riesgo durante la semana, recibirá el siguiente mensaje que le pide que cree más indicadores de riesgo personalizados.



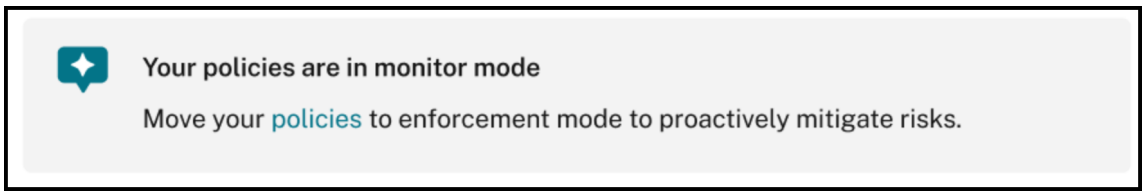

Puede iniciar sesión en Citrix Analytics para crear más indicadores de riesgo personalizados.

- Si ninguna de las fuentes de datos está activada en Security Analytics, aparecerá el siguiente mensaje en el que se le solicita que active el procesamiento de datos para las fuentes de datos.

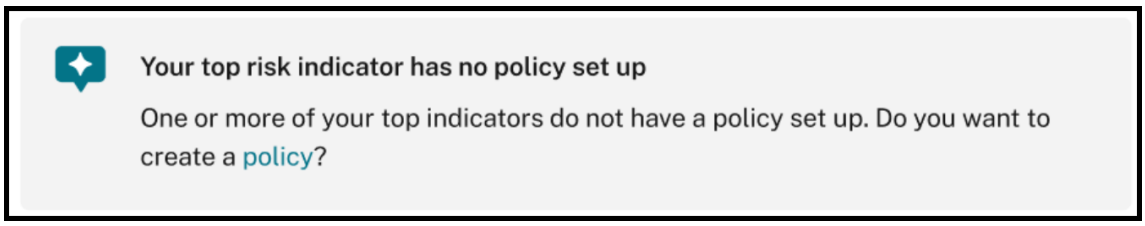
 



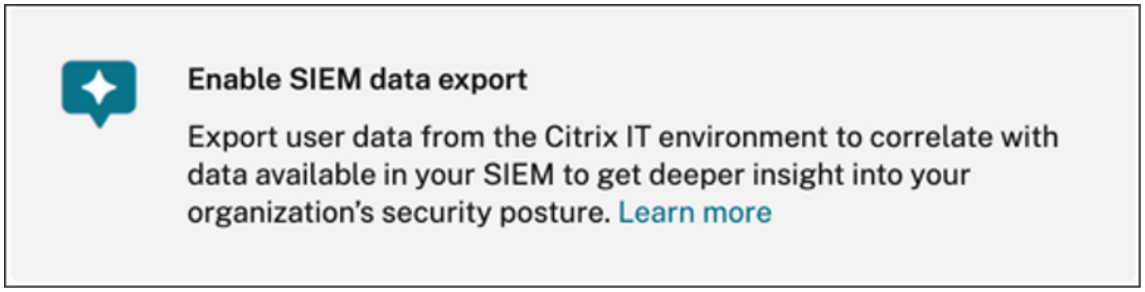

- Si ninguna de las directivas está en modo de supervisión, recibirá el siguiente mensaje que le pedirá que pase las directivas al modo de aplicación.




- Si no hay ninguna directiva establecida para ninguno de los tres indicadores de riesgo principales de la semana, recibirá el siguiente mensaje que le pide que cree una directiva.



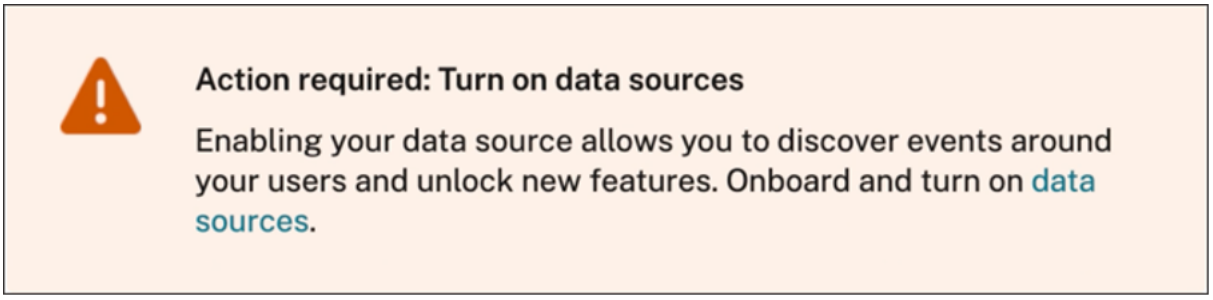

- Si no ha habilitado la **exportación de datos** para su arrendatario de Citrix Analytics, las siguientes recomendaciones le indican más detalles sobre nuestras opciones de **exportación de datos**, que le permiten exportar sus datos de Citrix a un entorno SIEM.




- Si el estado de consumo de la exportación de datos está inactivo, recibirá el siguiente mensaje que le pedirá que active su servicio.


> **Nota**
>
> La transmisión de datos solo se habilita cuando el procesamiento de datos está activado al menos para una fuente de datos. Si el procesamiento de datos está desactivado en todas las fuentes de datos, recibirá el siguiente mensaje de advertencia para habilitar la fuente de datos.




## Registros de auditoría

February 12, 2020

Un registro de auditoría describe la información de auditoría de los eventos generados en Citrix Analytics. Pueden ser eventos del sistema, como errores, o una pista de auditoría de acciones de configuración realizadas por el administrador de Citrix Analytics.

Cada vez que se agrega, elimina o actualiza una configuración, la información del evento se escribe en el registro de auditoría. Esta información es acerca de lo que se modificó, la hora en que se modificó y quién la modificó.

Puede ver la información del registro de auditoría de los últimos tres meses.

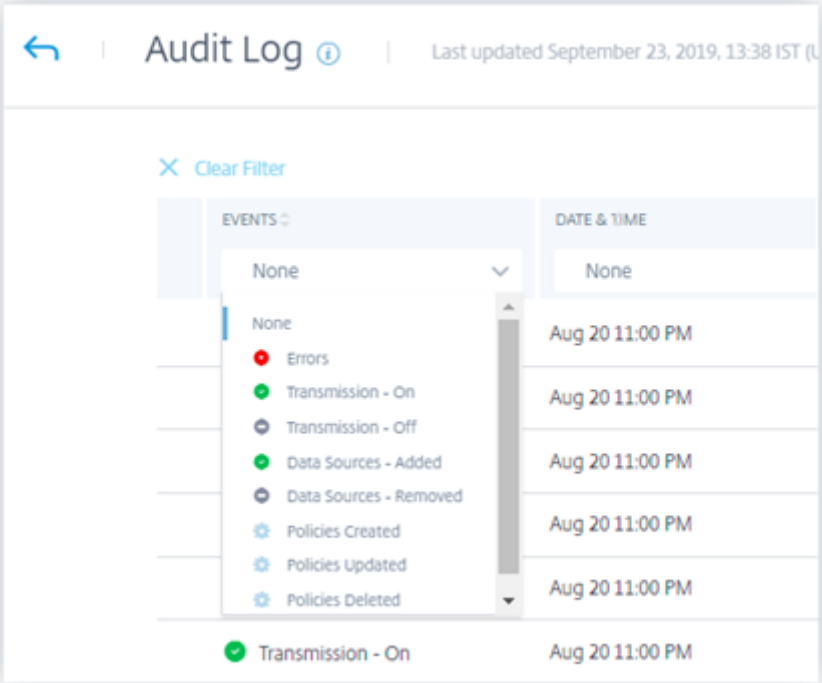
### Actividades que generan eventos de auditoría

Los siguientes eventos se registran en Citrix Analytics:

- Errores generados
- Transmisión encendida

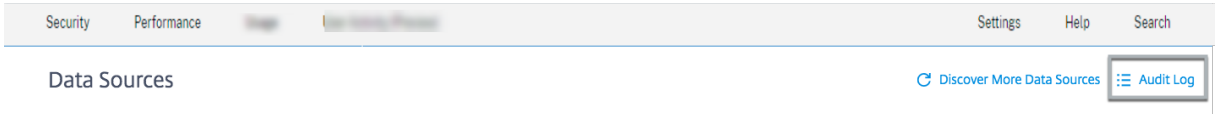
 

- Transmisión apagada
- Fuentes de datos agregadas
- Orígenes de datos eliminados
- Directivas creadas
- Directivas actualizadas
- Directivas eliminadas




## Cómo ver el registro de auditoría

Para ver los registros de auditoría, inicie sesión en Citrix Analytics. Vaya a **Configuración > Orígenes de datos**. En la página **Orígenes de datos**, haga clic en **Registro de auditoría** en la esquina superior derecha.




## Cómo utilizar el registro de auditoría

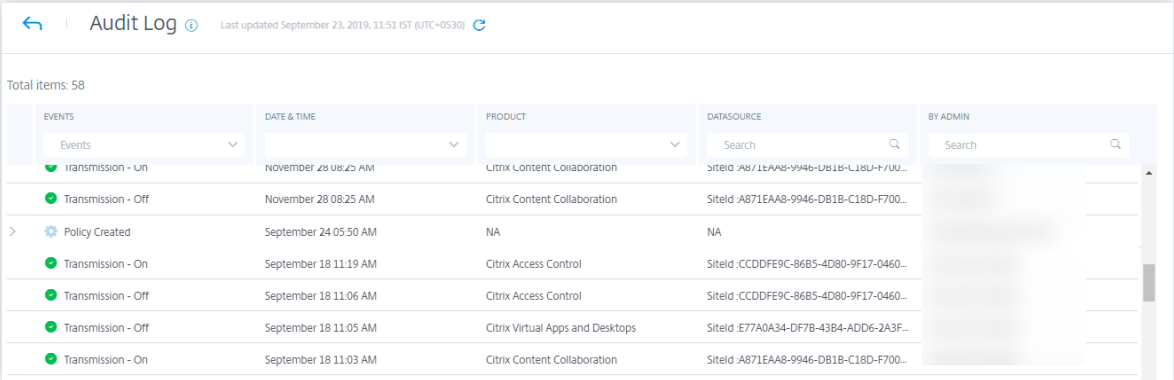
Puede utilizar el registro de auditoría para revisar y conocer cualquier evento en Citrix Analytics. Actualice la página **Registro de Auditoría** para obtener los datos de auditoría más recientes. La página

muestra la fecha y hora de la última actualización de los datos de auditoría.

Puede ver la siguiente información de auditoría en la página **Registro de auditoría**. También puede filtrar los datos de auditoría en función de estos campos.

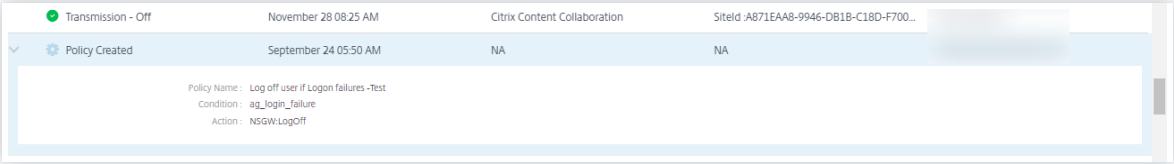
- **Eventos**. Los eventos pueden ser generados por el sistema o configuraciones aplicadas por el administrador en Citrix Analytics. Los eventos también pueden representar errores como la falta de aplicación de acciones o un origen de datos. De forma predeterminada, se muestran los registros de todos los eventos. Puede filtrar según el tipo de evento que quiera ver.
- **Fecha y hora**. Los datos y la hora en que se produjo el evento. Puede filtrar según el período para el que quiere ver el registro. Puede ver los eventos del día actual, los últimos siete días, los últimos 15 días, el último mes y los últimos tres meses.
- **Producto**. El producto para el que se generó el evento. Los eventos se generan en el producto y se agregan en Citrix Analytics donde se muestran. Puede filtrar el registro en función de uno o más productos.
- **Origen de datos**. Nombre de la instancia de producto asociada a la entrada de auditoría. Puede buscar cualquier origen de datos específico para ver sus datos de auditoría.
- **Por Admin**. El administrador de Citrix Analytics que realizó las actividades de administración. Puede buscar actividades realizadas por cualquier administrador específico.




Si el evento registrado se basó en una directiva, puede hacer clic en el icono de flecha para ver más detalles, como:

- Nombre de directiva
- La condición especificada
- La acción resultante




# Informes personalizados

June 18, 2024

Puede crear y programar informes personalizados mediante los eventos y la información disponibles en Citrix Analytics for Security. Los informes personalizados le ayudan a extraer información de interés específico y a organizar los datos gráficamente. Ayuda a analizar la seguridad de la fuente de datos de su elección a lo largo del tiempo.

Los informes personalizados admiten las siguientes fuentes de datos:

- Aplicaciones y escritorios
- Gateway
- Secure Private Access
- Secure Browser
- Directivas
- Indicadores de riesgo
- Puntuación de riesgo

## Campos compatibles en informes personalizados

Algunas fuentes de datos también están disponibles en la búsqueda de autoservicio. Para ver estos tipos de eventos y los campos compatibles, haga clic en las siguientes fuentes de datos.

- Aplicaciones y escritorios
- Gateway
- Secure Private Access
- Secure Browser
- Directivas

Las siguientes fuentes de datos solo están disponibles en los informes personalizados. En la tabla siguiente se enumeran los campos admitidos en los informes personalizados para las siguientes fuentes de datos:

- Indicadores de riesgo

- Puntuación de riesgo

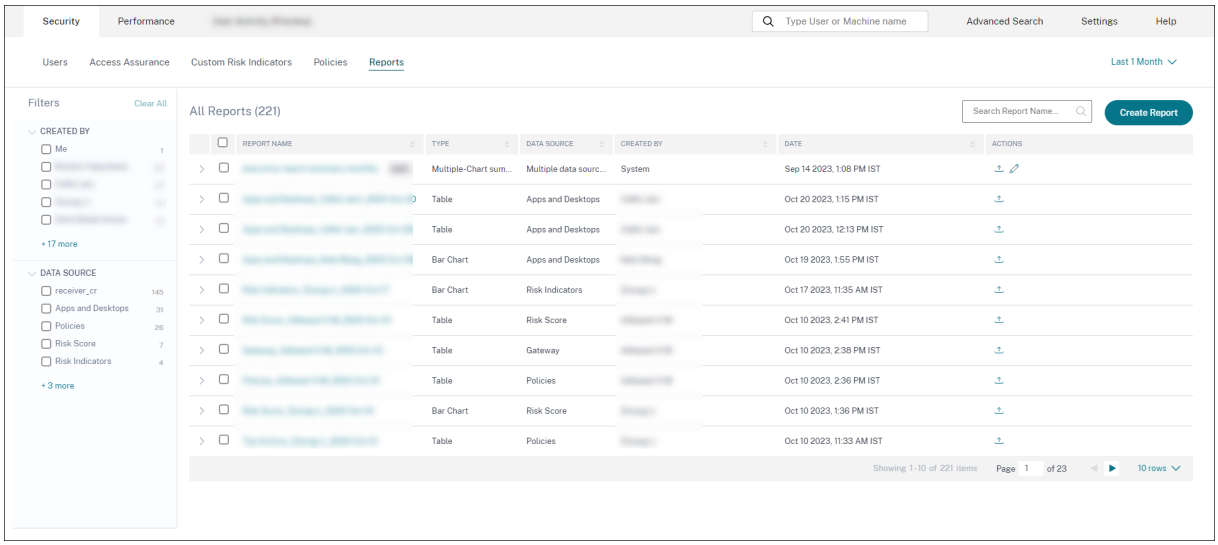
| Origen de datos | Dimensión | Descripción |
|---|---|---|
| Indicadores de riesgo | Categoría | Indica la categoría de los indicadores de riesgo. Los indicadores de riesgo se agrupan en una de cuatro categorías: puntos finales comprometidos, usuarios comprometidos, exfiltración de datos o amenazas internas. |
| | Nombre del indicador de riesgo | Nombre del indicador de riesgo. En el caso de un indicador de riesgo personalizado, el administrador define el nombre al crear el indicador. |
| | Gravedad | Indica la gravedad del riesgo. Puede ser bajo, medio o alto. |
| | User-Name | El nombre de usuario o dominio\nombre de usuario que se utiliza para iniciar sesión. |
| Puntuación de riesgo | Puntuación de riesgo | La puntuación de riesgo asignada al usuario. La puntuación de riesgo varía de 0 a 100 en función de la gravedad de la amenaza asociada a la actividad del usuario. |
| | User-Name | El nombre de usuario o dominio\nombre de usuario que se utiliza para iniciar sesión. |
| | Categoría de puntuación de riesgo | Según la puntuación de riesgo, un usuario arriesgado puede pertenecer a una de las siguientes categorías: riesgo alto, riesgo medio y riesgo bajo. |

## Informes

Puede realizar las siguientes acciones en los informes mediante esta vista:

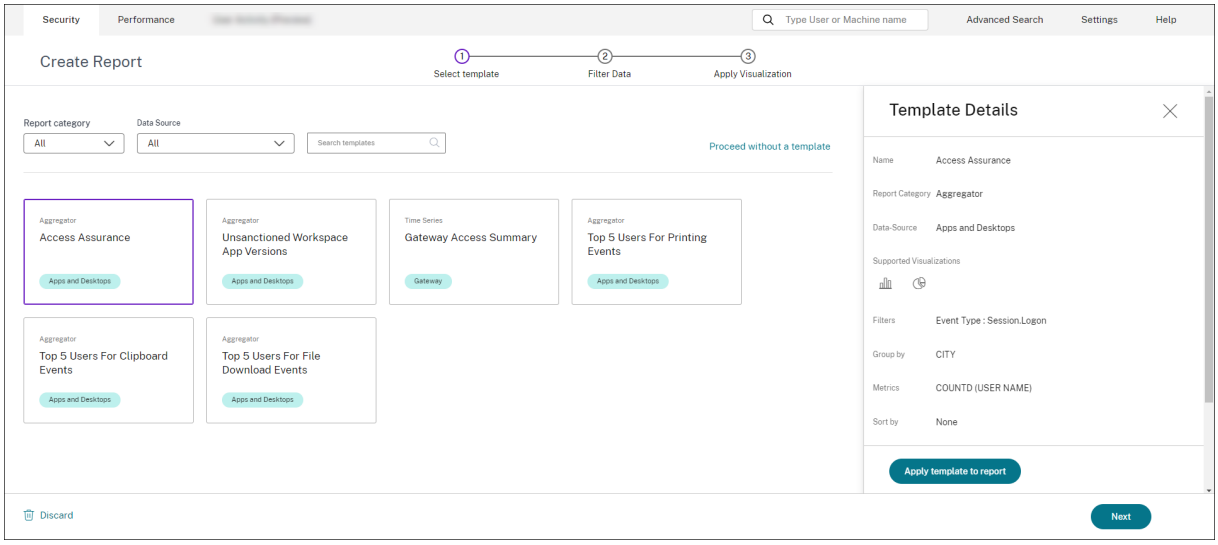
- Haga clic en **Crear informe** para crear un informe personalizado.
- Amplíe una fila para ver la vista previa de un informe personalizado existente.
- Haga clic en el nombre del informe para ver la visualización detallada del informe.
- Haga clic en el icono de exportación para exportar un informe personalizado existente en formato PDF.
- Haz clic en el icono de edición para modificar los informes que has creado.
- Haga clic en el icono de eliminación para eliminar los informes que ha creado.




## Crear un informe personalizado

Para crear un informe personalizado, haga clic en **Crear informes**. En la página **Crear informe**, puede elegir crear un informe personalizado con o sin plantillas.

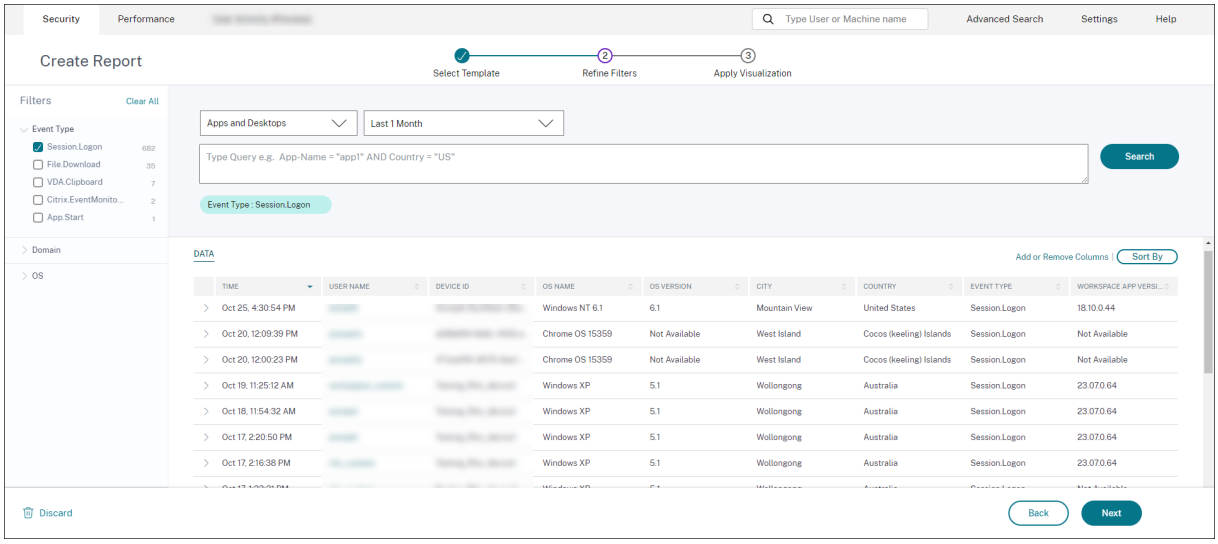
 




## Creación de un informe personalizado con plantillas

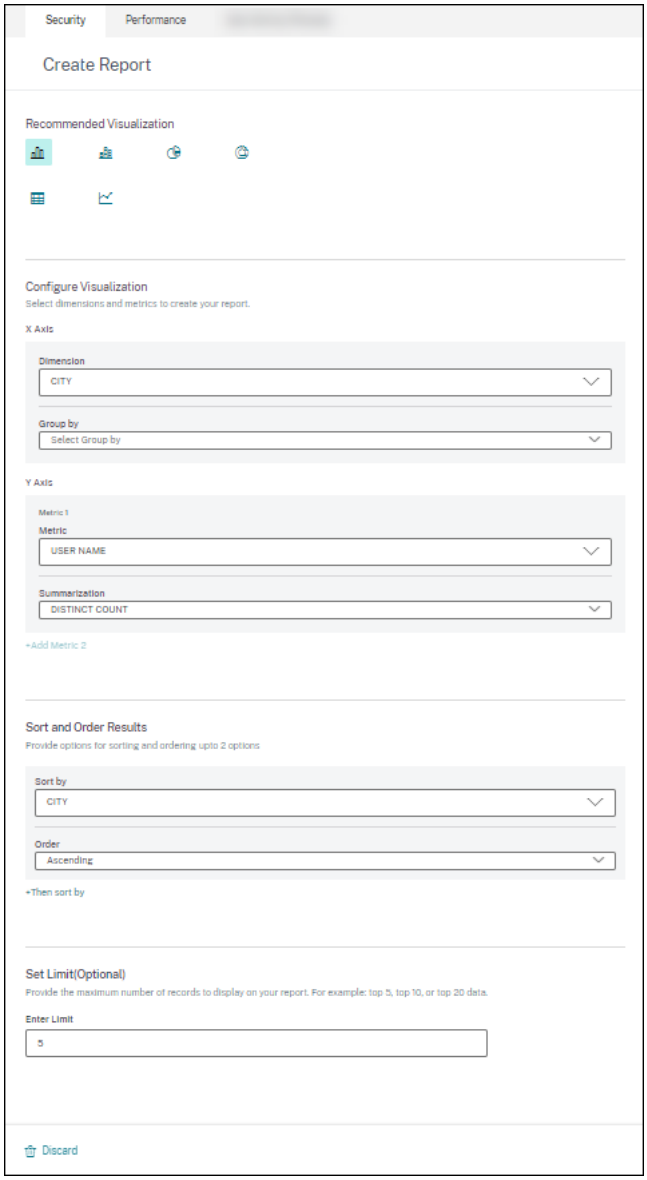
Para crear un informe personalizado con una plantilla:

1. **Seleccione una plantilla**: una vez que haga clic en una plantilla, los detalles de la plantilla se muestran a la derecha. Haga clic en **Aplicar plantilla al informe** para permitir que el informe utilice la plantilla seleccionada.
2. **Refinar filtros**: la página **Refinar filtros** muestra los filtros que estaban predefinidos para la plantilla que ha seleccionado. Realice los cambios necesarios y, a continuación, haga clic en **Siguiente**.




1. **Aplicar visualización**: seleccione una de las visualizaciones disponibles para mostrar el informe.



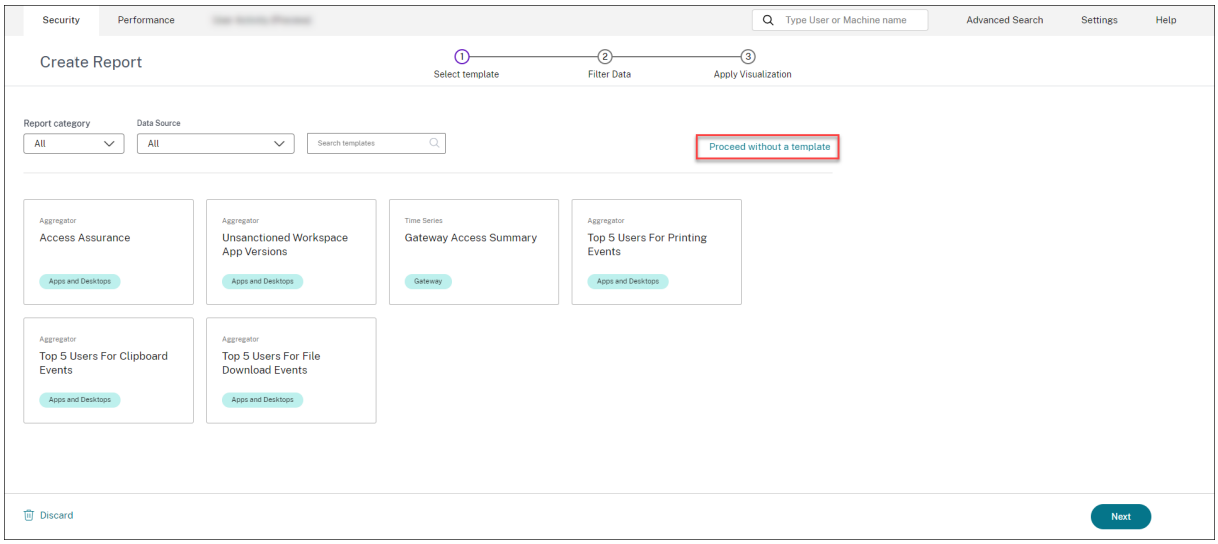

- **Gráfico de barras**: presenta los datos con barras rectangulares verticales con una altura proporcional a los valores. Se usa para comparar eventos.
- **Gráfico de columnas apiladas**: presenta los datos en forma de barras apiladas una sobre otra. Se usa para visualizar la suma total de datos en varias subcategorías.
- **Gráfico circular**: presenta los datos en forma circular. Se usa para visualizar el tamaño relativo de los datos o porcentajes.
- **Gráfico de anillos**: presenta los datos en forma de anillos. Se usa para visualizar el tamaño relativo de los datos o porcentajes. - **Tabla**: presenta los datos en forma de tabla. Se usa para visualizar tantas dimensiones como sea necesario.
- **Gráfico de líneas**: presenta datos con puntos conectados por segmentos en línea recta. Se utiliza para visualizar las tendencias de los datos durante un período de tiempo.

1. Ahora configure la visualización con los siguientes parámetros:
    - Dimensión del eje x
    - Métricas que se trazarán en el eje y
    - Resúmenes o agregaciones, como el promedio o el recuento, que se aplicarán a la métrica
    - Opciones de clasificación y pedido
    - Un límite opcional para el número máximo de registros que se mostrarán en el informe.

### Creación de un informe personalizado sin plantillas

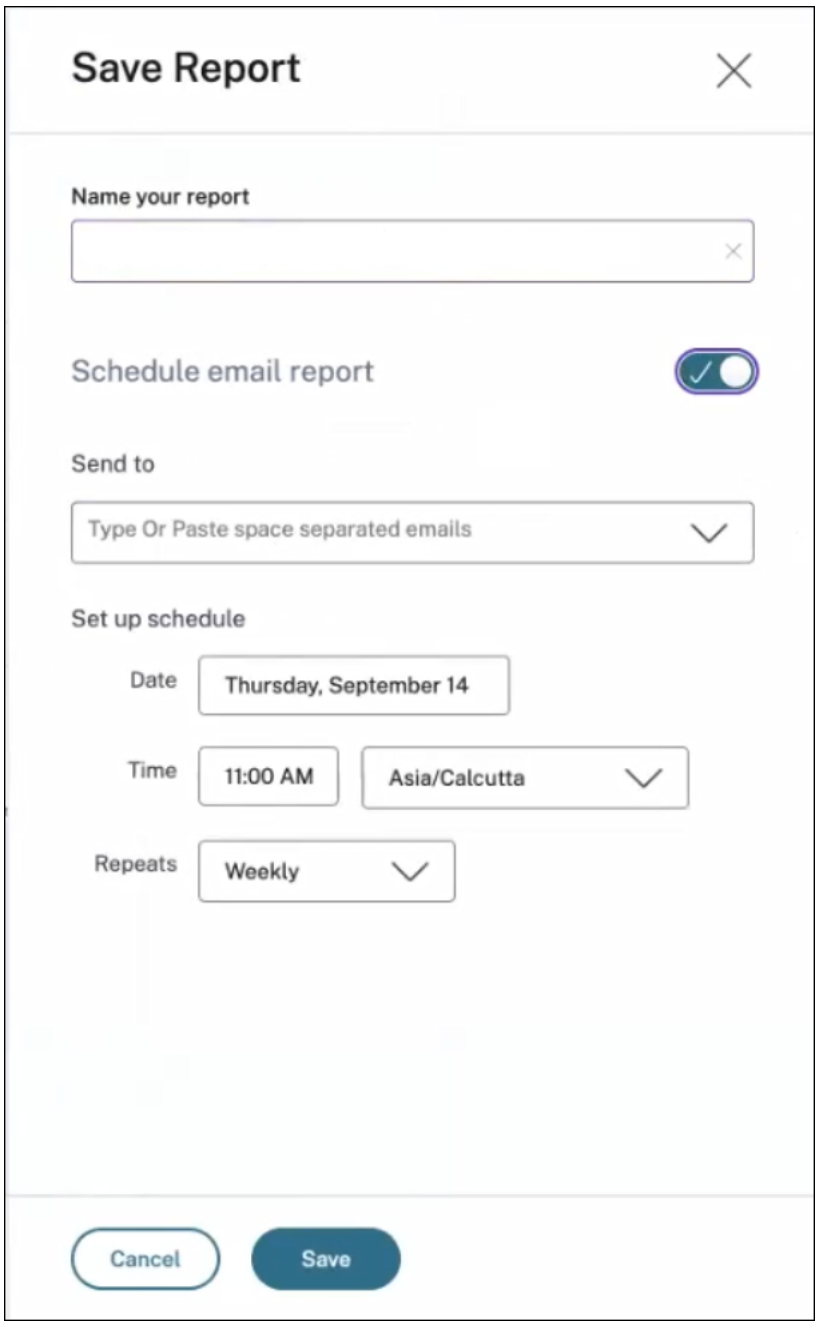
También puede crear un informe personalizado sin una plantilla predefinida. Haz clic en **Crear informe personalizado sin plantilla**. Seleccione una fuente de datos de la lista desplegable. Siga los pasos para definir los filtros, aplicar la visualización, guardar y programar el informe.




### Guardar un informe

1. Para guardar el informe, haga clic en **Guardar**. Especifique un título para su informe.
2. Puede programar el informe para enviar el informe por correo electrónico a los ID de correo electrónico y las listas de distribución especificados en una fecha y hora específicas o en un horario periódico.

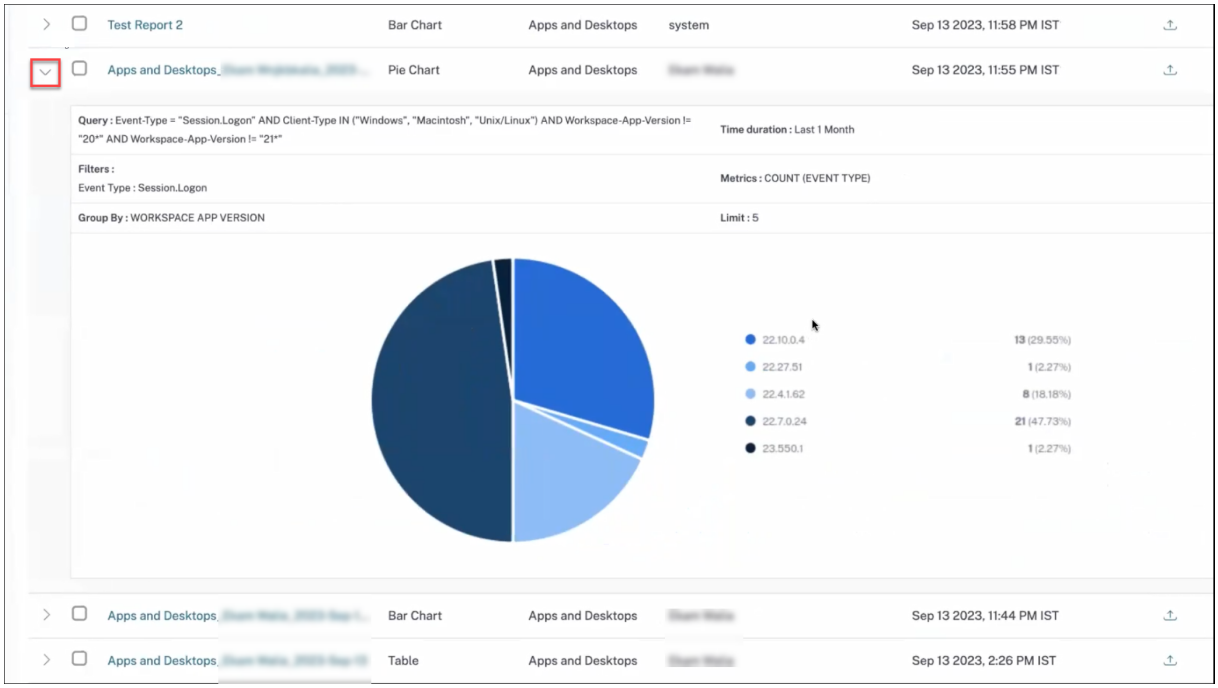
 




### Ver un informe

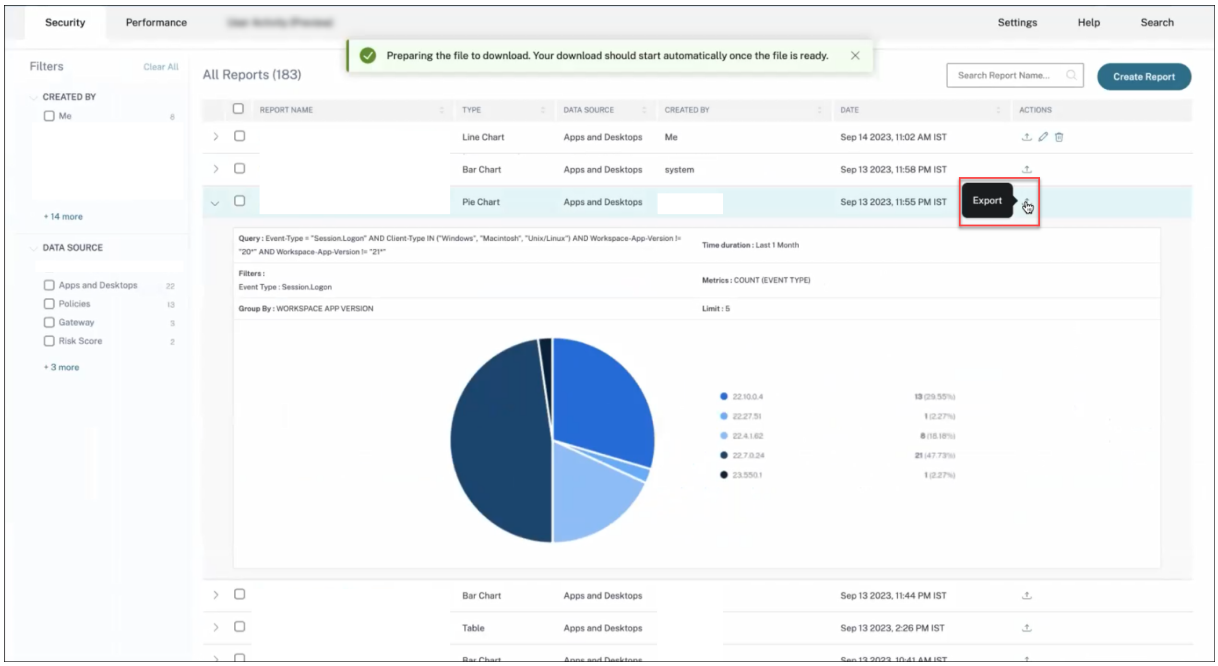
1. Después de crear y guardar un informe, puede verlo en la página **Informes**. También puede modificar o eliminar un informe guardado.
2. Haz clic en el botón desplegable para obtener una vista previa del informe.




## Exportar un informe

Haga clic en el icono de exportación para exportar el informe.

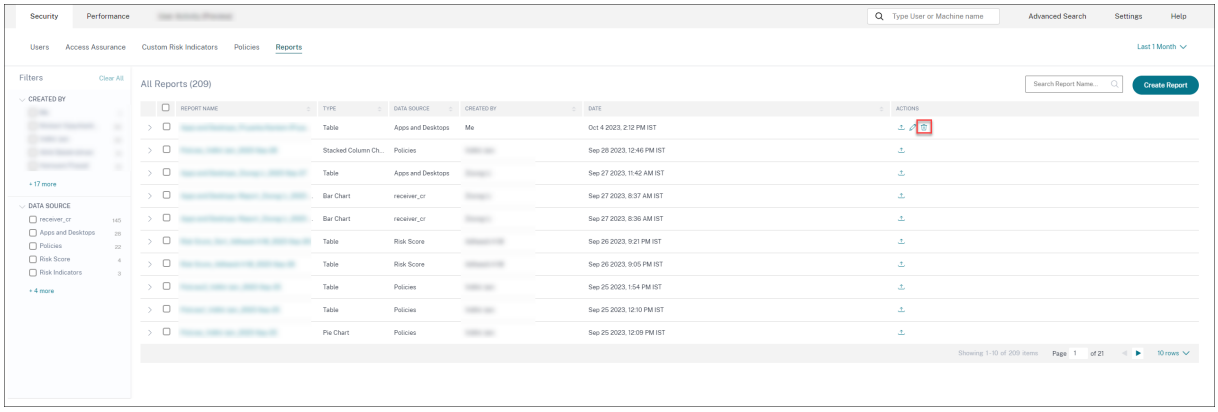



## Eliminar un informe

Haga clic en el icono de eliminación para eliminar el informe.

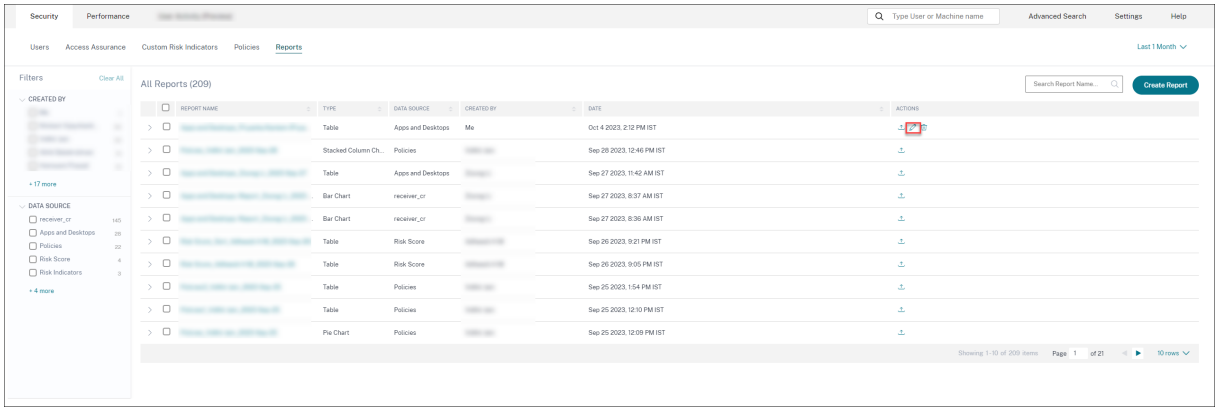
> Nota:
>
> Solo el usuario que crea el informe puede eliminarlo.




## Modificar un informe

Haga clic en el icono de modificación para modificar el informe.

> Nota:
>
> Solo el usuario que crea el informe puede modificarlo.



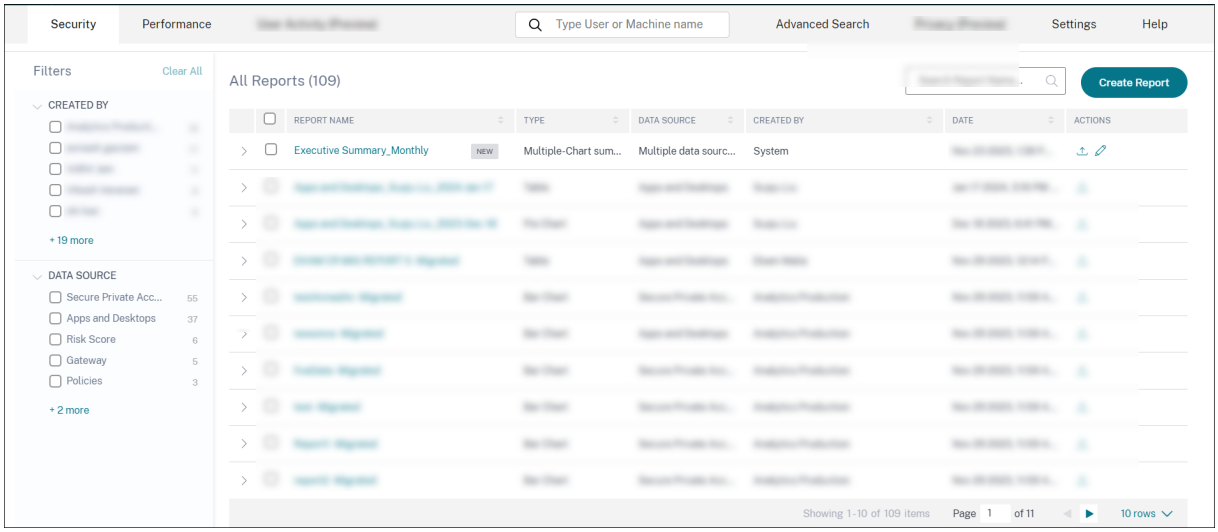

## Informe resumen ejecutivo

Puede programar una exportación automática por correo electrónico que contenga un PDF de un informe resumen ejecutivo creado previamente. El informe resumen ejecutivo es una colección de informes que muestran la estrategia de seguridad de su empresa de un solo vistazo durante el período de tiempo seleccionado para el público que usted elija.

Puede crear el informe de datos para las siguientes duraciones:

- Última hora
- Últimas 12 horas
- Último día
- Última semana
- Último 1 mes




### ¿Qué informes contiene?

El informe resumen ejecutivo contiene los siguientes informes:

- **Distribución del riesgo de los usuarios**: la distribución de los perfiles de riesgo alto, medio y bajo en función de su puntuación de riesgo calculada más alta en el período de tiempo seleccionado.
- Usuarios con mayor riesgo: los usuarios con mayor riesgo entre todos los usuarios ordenados por las puntuaciones de riesgo más altas para el período de tiempo seleccionado.
- **Ocurrencias de riesgo por categorías**: la visión integral de los tipos de exposiciones al riesgo y los riesgos críticos proporcionados por las categorías de riesgo que requieren una acción inmediata. Los indicadores de riesgo se agrupan en las siguientes categorías:
  - Usuarios comprometidos
  - Dispositivos de punto final comprometidos
  - Exfiltración de datos
  - Amenazas internas
- **Indicadores de riesgo**: los indicadores de riesgo activados para los usuarios durante el período de tiempo seleccionado.
- **Acciones**: las acciones aplicadas a los indicadores de riesgo activados para los usuarios durante el período de tiempo seleccionado.

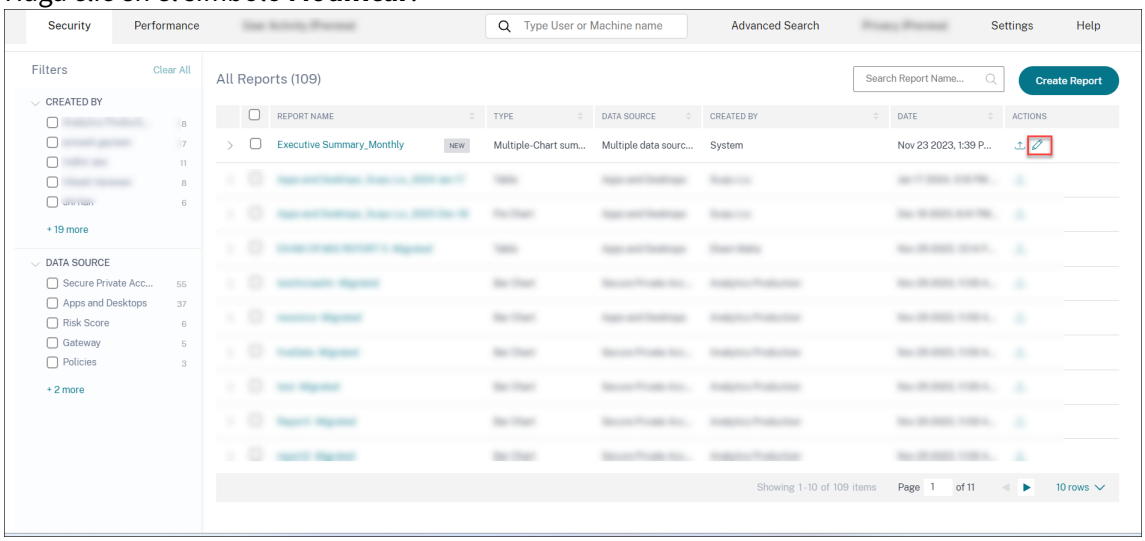
 

- **Directivas principales**: las cinco directivas principales que más se activaron en el período de tiempo seleccionado.
- **Acciones principales**: las cinco acciones principales que más se activaron en el período de tiempo seleccionado.
- **Indicadores de riesgo por gravedad**: indicadores de riesgo predeterminados y personalizados activados por los usuarios ordenados según la gravedad.
- **Indicadores de riesgo por total de ocurrencias**: indicadores de riesgo predeterminados y personalizados activados por los usuarios ordenados en función de las ocurrencias.

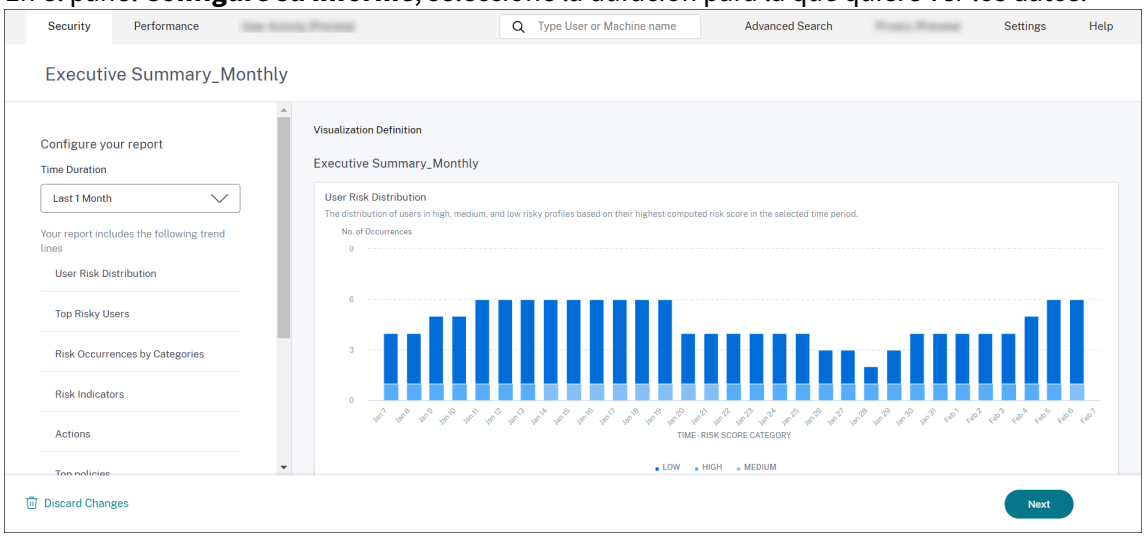
### Modificar un informe ejecutivo

Para modificar un informe ejecutivo, siga estos pasos:

1. Haga clic en el símbolo **Modificar**.




2. En el panel **Configure su informe**, seleccione la duración para la que quiere ver los datos.



3. Haga clic en **Siguiente**. Aparece el panel **Guardar informe**.

> **Nota:**
>
> Para descartar los cambios, haga clic en **Descartar cambios**.

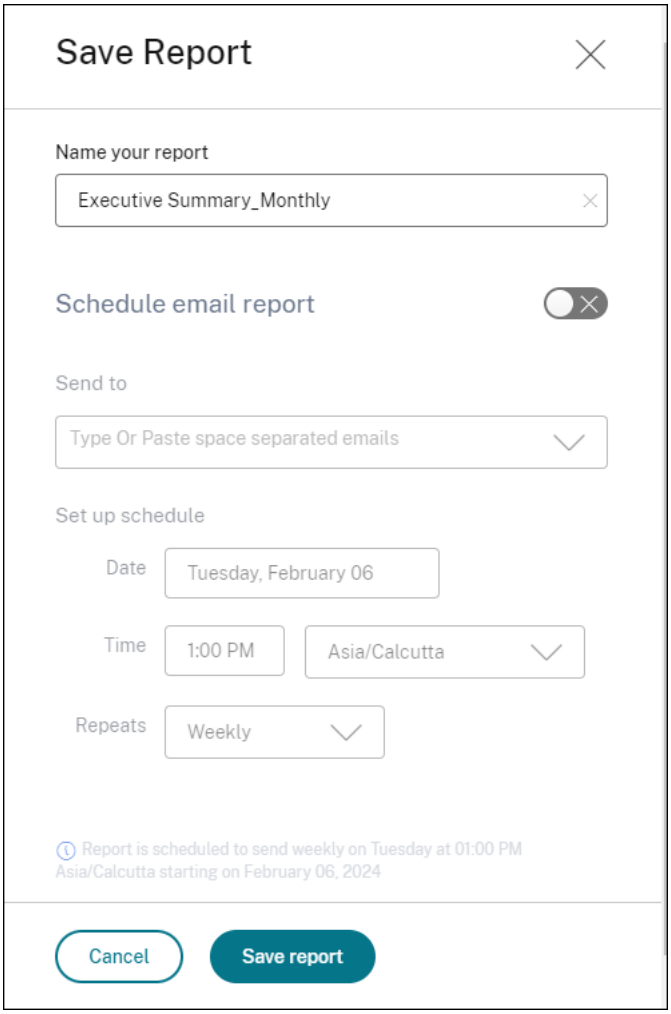
4. En el panel **Guardar informe**, introduzca los siguientes detalles:

   a) **Nombre de informe**: el nombre del informe ejecutivo.

   b) **Programar informe por correo electrónico**: active esta opción para programar el informe. La opción está desactivada de forma predeterminada.

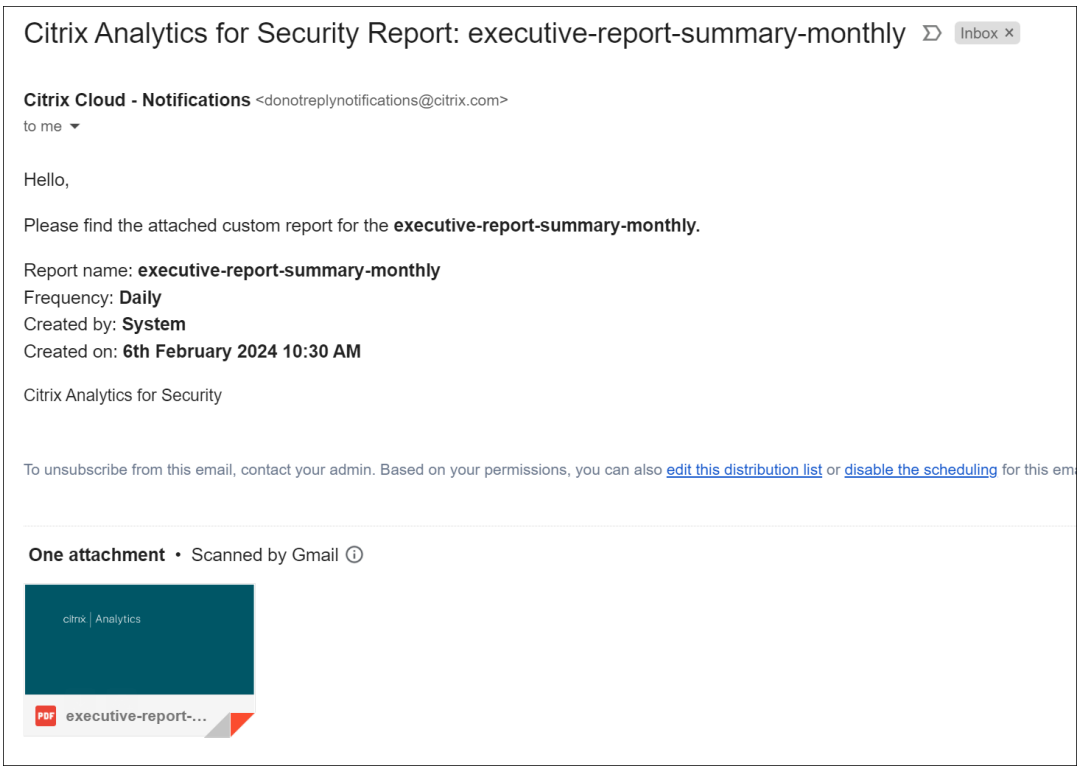
   c) **Enviar a**: seleccione una lista de distribución en el menú desplegable. También puede agregar una combinación de listas de distribución y direcciones de correo electrónico individuales. Para crear una lista de distribución personalizada, consulte Parámetros de correo electrónico de administrador.

   d) **Configurar programación**: seleccione la hora deseada en la que el informe se envía por primera vez a la audiencia seleccionada y la hora en que se repite.

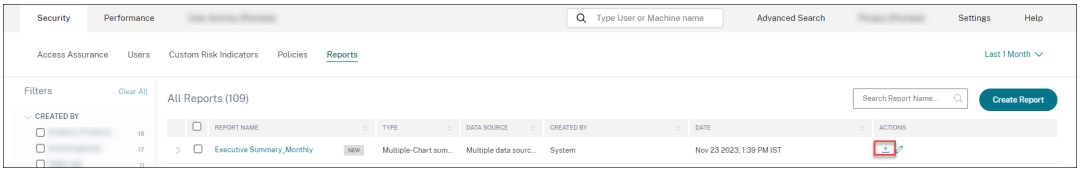


e) Haga clic en **Guardar informe**. A continuación, el informe se envía por correo electrónico a los destinatarios de la lista.

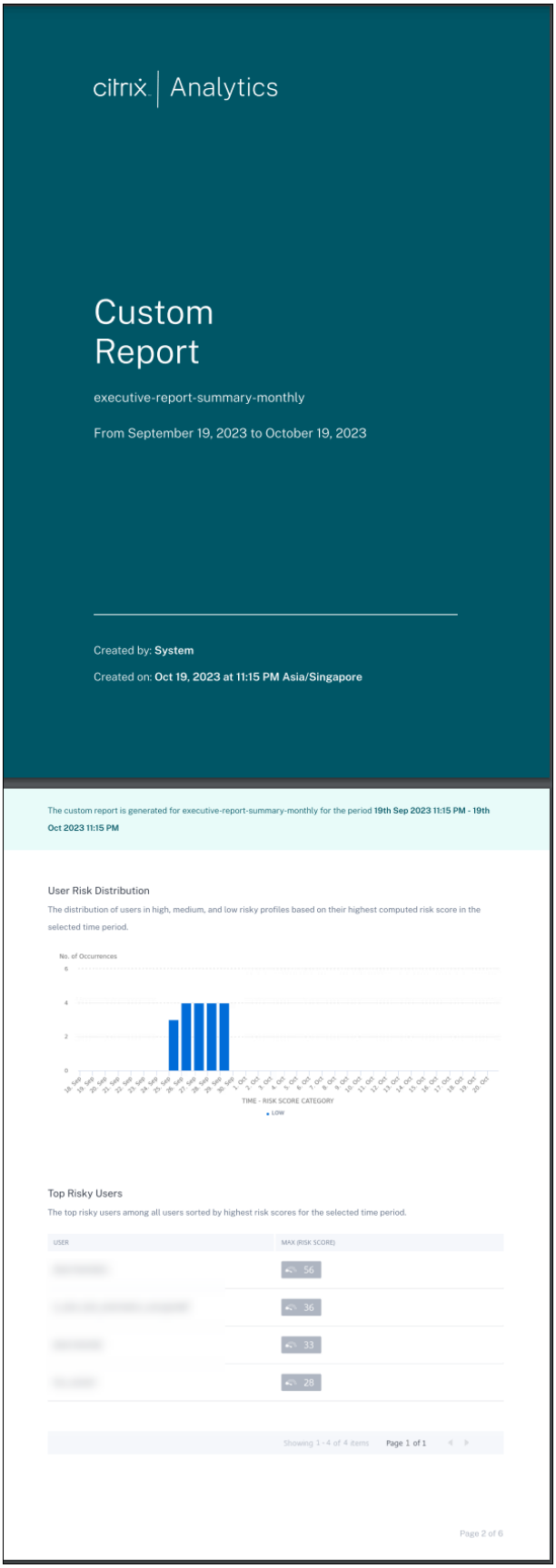



Como alternativa, puede exportar el informe ejecutivo en formato PDF con el símbolo **Exportar**.




La siguiente captura de pantalla muestra una salida PDF de ejemplo:



# Búsqueda de autoservicio

December 7, 2023

## ¿Qué es la búsqueda de autoservicio?

La función de búsqueda de autoservicio le permite buscar y filtrar los eventos de usuario recibidos de sus orígenes de datos. Puede explorar los eventos de usuario subyacentes y sus atributos. Estos eventos le ayudan a identificar cualquier problema de datos y solucionarlo. La página de búsqueda muestra varias facetas (dimensiones) y métricas de una fuente de datos. Puede definir la consulta de búsqueda y aplicar filtros para ver los eventos que coinciden con los criterios definidos. De forma predeterminada, la página de búsqueda de autoservicio muestra los eventos de usuario del último día.

Actualmente, la función de búsqueda de autoservicio está disponible para estos orígenes de datos:

- Authentication
- Gateway
- Secure Browser
- Secure Private Access
- Aplicaciones y escritorios
- Usuarios, máquinas y sesiones de rendimiento

Además, puede realizar búsquedas de autoservicio en los eventos que cumplen las directivas definidas. Para obtener más información, consulte Búsqueda de autoservicio de directivas.

## Cómo acceder a la búsqueda de autoservicio

Puede acceder a la búsqueda de autoservicio mediante las siguientes opciones:

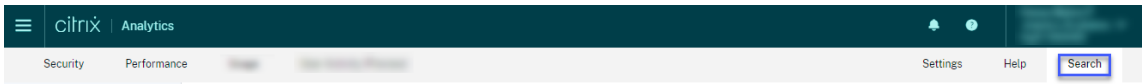
- **Barra superior**: haga clic en **Buscar** en la barra superior para ver todos los eventos de usuario del origen de datos seleccionado.
- **Cronología de riesgos en una página de perfil de usuario**: haga clic en **Búsqueda** de eventos para ver los eventos del usuario respectivo.

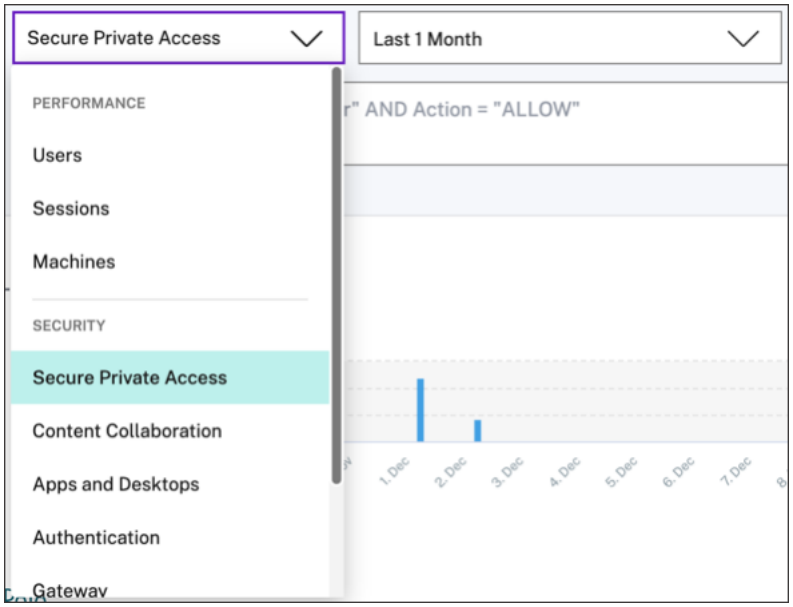
### Búsqueda de autoservicio desde la barra superior

Utilice esta opción para ir a la página de búsqueda de autoservicio desde cualquier lugar de la interfaz de usuario.

1. Haga clic en **Buscar** para ver la página de autoservicio.




2. Seleccione el origen de datos y el período de tiempo para ver los eventos correspondientes.

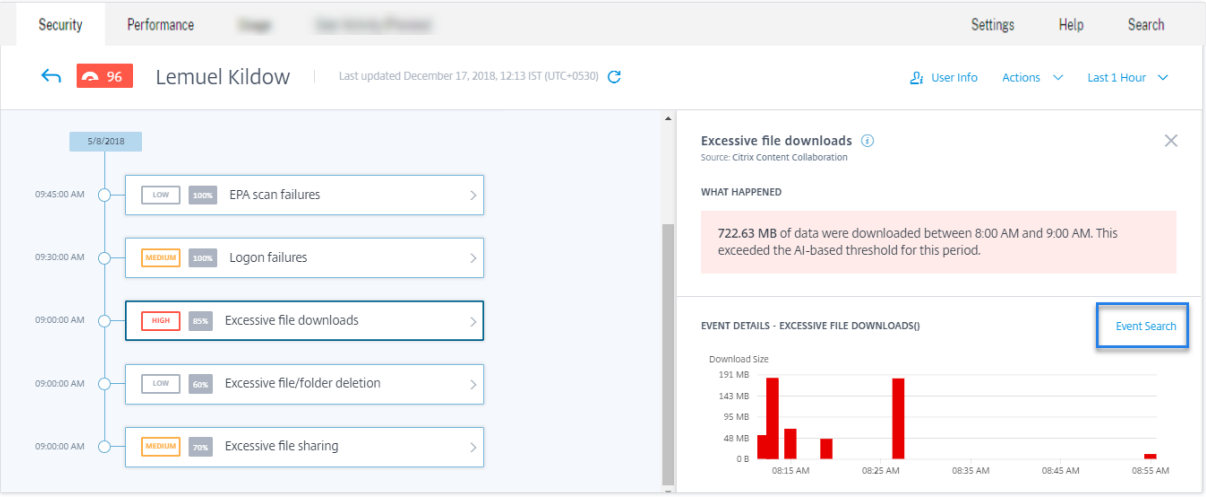



### Búsqueda de autoservicio desde el cronograma de riesgos del usuario

Utilice esta opción si quiere ver los eventos de usuario asociados a un indicador de riesgo.

Al seleccionar un indicador de riesgo del cronograma de un usuario, la sección de información del indicador de riesgo se muestra en el panel derecho. Haga clic en **Búsqueda de eventos** para explorar los eventos asociados al usuario y el origen de datos (para la que se activa el indicador de riesgo) en la página de búsqueda de autoservicio.




Para obtener más información sobre el cronograma de riesgo del usuario, consulte Cronología de riesgos.

## Cómo utilizar la búsqueda de autoservicio

Utilice las siguientes funciones de la página de búsqueda de autoservicio:

- Facetas para filtrar sus eventos.
- Cuadro de búsqueda para introducir la consulta y filtrar los eventos.
- Selector de tiempo para seleccionar el período de tiempo.
- Detalles del cronograma para ver los gráficos de eventos.
- Datos de eventos para ver los eventos.
- Expórtelo en formato CSV para descargar sus eventos de búsqueda en un archivo CSV.
- Exporta un resumen visual para descargar el informe de resumen visual de su consulta de búsqueda.
- Clasificación de varias columnas para ordenar los eventos por varias columnas.

### Usar facetas para filtrar eventos

Las facetas son el resumen de los puntos de datos que constituyen un evento. Las facetas varían según el origen de datos. Por ejemplo, las facetas del origen de datos de acceso privado seguro son la reputación, las acciones, la ubicación y el grupo de categorías. Mientras que las facetas de Apps y escritorios son el tipo de evento, el dominio y la plataforma.

Seleccione las facetas para filtrar los resultados de la búsqueda. Las facetas seleccionadas se muestran como fichas.

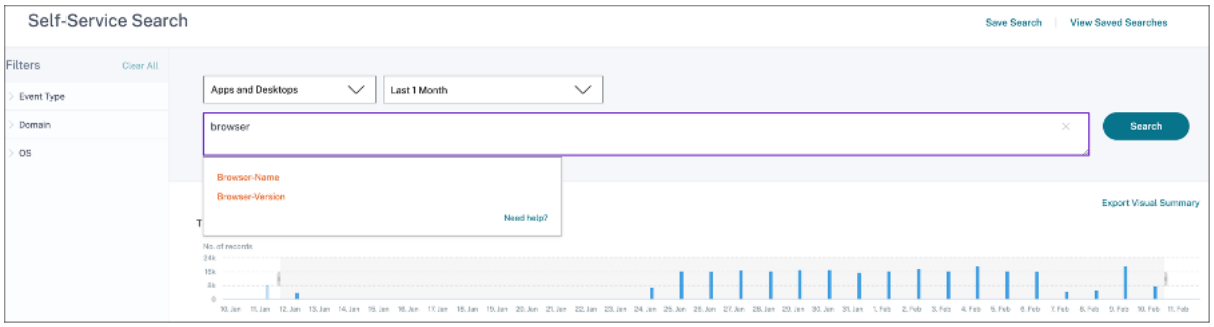
 

Para obtener más información sobre las facetas correspondientes a cada origen de datos, consulte el artículo de búsqueda de autoservicio para el origen de datos mencionado anteriormente en este artículo.

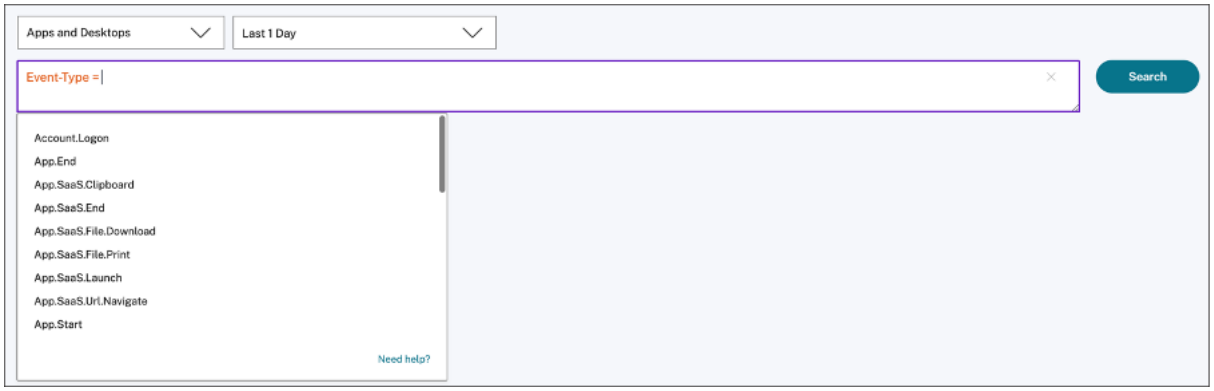
### Utilizar la consulta de búsqueda en el cuadro de búsqueda para filtrar eventos

Al colocar el cursor en el cuadro de búsqueda, el cuadro de búsqueda muestra una lista de dimensiones basada en los eventos del usuario. Estas dimensiones varían según el origen de datos. Utilice las dimensiones y los operadores válidos para definir los criterios de búsqueda y buscar los eventos necesarios.

Por ejemplo, en la búsqueda de autoservicio de Apps y escritorios, obtiene los siguientes valores para la dimensión `Browser`. Use la dimensión para escribir la consulta, seleccione el período de tiempo y, a continuación, haga clic en **Buscar**.




Al seleccionar determinadas dimensiones, como `Event-Type` y `Clipboard-Operation` junto con un operador válido, los valores de la dimensión se muestran automáticamente. Puede elegir un valor de las opciones sugeridas o introducir un valor nuevo según sus requisitos.




**Operadores compatibles en la consulta de búsqueda** Utilice los siguientes operadores en las consultas de búsqueda para refinar los resultados de la búsqueda.

| Operador | Descripción | Ejemplo | Resultado |
|---|---|---|---|
| | Asigne un valor a una dimensión de búsqueda. | User-Name: John | Muestra los eventos del usuario John. |
| = | Asigne un valor a una dimensión de búsqueda. | User-Name = John | Muestra los eventos del usuario John. |
| ~ | Busca eventos con valores similares. | User-Name ~ test | Muestra los eventos con nombres de usuario similares. |
| " " | Encierra valores separados por espacios. | User-Name = “John Smith” | Muestra los eventos del usuario John Smith. |
| < > | Búsqueda de valor relacional. | Volumen de datos > 100 | Muestra los eventos en los que el volumen de datos es superior a 100 GB. |
| AND | Buscar eventos en los que se cumplan las condiciones especificadas. | User-Name: John AND Data Volume > 100 | Muestra los eventos del usuario John en los que el volumen de datos es superior a 100 GB. |
| ! ~ | Comprueba los eventos del patrón coincidente que especifique. Este operador NOT LIKE devuelve los eventos que no contienen el patrón coincidente en ninguna parte de la cadena de eventos. | User-Name !~ John | Muestra los eventos de los usuarios excepto John, John Smith o cualquier otro usuario que contenga el nombre coincidente “John”. |

| Operador | Descripción | Ejemplo | Resultado |
|---|---|---|---|
| ! = | Comprueba los eventos de la cadena exacta que especifique. Este operador NOT EQUAL devuelve los eventos que no contienen la cadena exacta en ninguna parte de la cadena de eventos. | Country != USA | Muestra los eventos de los países excepto EE. UU. |
| * | Buscar eventos que coincidan con las cadenas especificadas. Actualmente, el operador * solo se admite con los siguientes operadores : , = y ! =. Los resultados de la búsqueda distinguen entre mayúsculas y min | User-Name = John* | Muestra los eventos de todos los nombres de usuario que empiezan por John. |
| | | User-Name = *John* | Muestra los eventos de todos los nombres de usuario que contienen John. |
| | | User-Name = *Smith | Muestra los eventos de todos los nombres de usuario que terminan en Smith. |
| | | Nombre de usuario: John* | Muestra los eventos de todos los nombres de usuario que empiezan por John. |
| | | Nombre de usuario: *John* | Muestra los eventos de todos los nombres de usuario que contienen John. |

| Operador | Descripción | Ejemplo | Resultado |
|---|---|---|---|
| | | Nombre de usuario: *Smith | Muestra los eventos de todos los nombres de usuario que terminan en Smith. |
| | | Nombre de usuario! = John* | Muestra los eventos de todos los nombres de usuario que no empiezan por John. |
| | | Nombre de usuario! = *Herrero | Muestra los eventos de todos los nombres de usuario que no terminan en Smith. |
| `IN` | Asigne varios valores a una dimensión de búsqueda para obtener los eventos relacionados con uno o varios valores. **Nota**: Actualmente, puede usar este operador con las siguientes dimensiones de Aplicaciones y escritorios: `Device ID`, `Domain`, `Event-Type` y `User-Name`. Este operador solo se aplica a los valores de cadena. | User-Name IN (John, Kevin) | Busca todos los eventos relacionados con John o Kevin. |

| Operador | Descripción | Ejemplo | Resultado |
|---|---|---|---|
| `NOT IN` | Asigne varios valores a una dimensión de búsqueda y busque los eventos que no contienen los valores especificados. **Nota**: Actualmente, puede usar este operador con las siguientes dimensiones de Aplicaciones y escritorios: `Device ID`, `Domain`, `Event-Type` y `User-Name`. Este operador solo se aplica a los valores de cadena. | User-Name NOT IN (John, Kevin) | Busca los eventos para todos los usuarios excepto John y Kevin. |
| `IS EMPTY` | Comprueba si hay un valor nulo o un valor vacío para una dimensión. Este operador solo funciona para dimensiones de tipo cadena como `App-Name`, `Browser` y `Country`. No funciona para dimensiones de tipo no cadena (número) como `Upload-File-Size`, `Download-File-Size` y `Client-IP`. | Country IS EMPTY | Busca eventos en los que el nombre del país no está disponible o está vacío (no especificado). |

| Operador | Descripción | Ejemplo | Resultado |
|---|---|---|---|
| `IS NOT EMPTY` | Comprueba si hay un valor no nulo o un valor específico para una dimensión. Este operador solo funciona para dimensiones de tipo cadena como `App-Name`, `Browser` y `Country`. No funciona para dimensiones de tipo no cadena (número) como `Upload-File-Size`, `Download-File-Size` y `Client-IP`. | Country IS NOT EMPTY | Busca eventos en los que el nombre del país esté disponible o especificado. |
| `OR` | Busca valores en los que una o ambas condiciones son verdaderas. | (User-Name = `John*` OR User-Name = `*Smith`) AND Event-Type = "Session.Logon" | Muestra eventos de `Session.Logon` para todos los nombres de usuario que comienzan por John o terminan por Smith. |

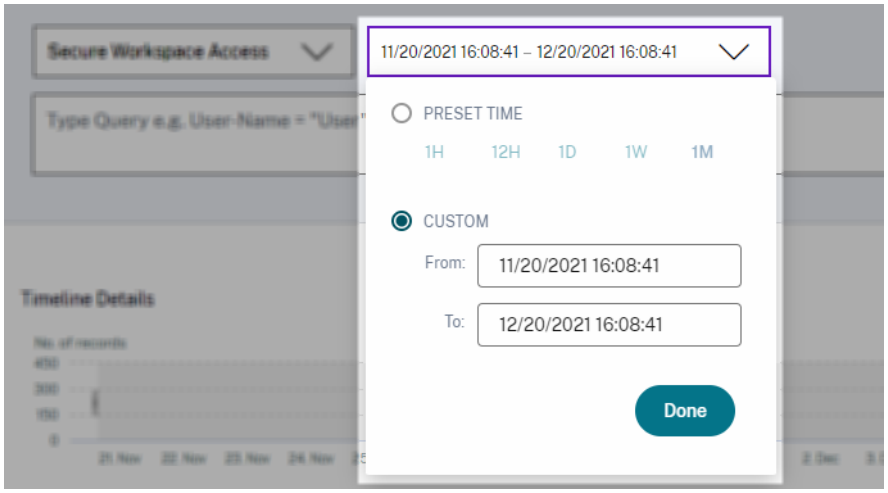
> **Nota**
>
> Para el operador **NOT EQUAL**, al introducir los valores de las dimensiones de la consulta, utilice los valores exactos disponibles en la página de búsqueda de autoservicio de un origen de datos. Los valores de cota distinguen entre mayúsculas y minúsculas

Para obtener más información sobre cómo especificar la consulta de búsqueda para el origen de datos, consulte el artículo de búsqueda de autoservicio del origen de datos mencionado anteriormente en este artículo.

### Seleccione la hora para ver el evento

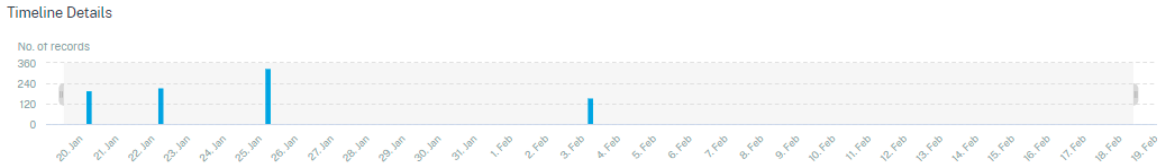
Seleccione una hora preestablecida o introduzca un intervalo de tiempo personalizado y haga clic en **Buscar** para ver los eventos.




### Ver los detalles del cronograma

La línea de tiempo proporciona una representación gráfica de los eventos del usuario durante el período de tiempo seleccionado. Mueva las barras de selección para elegir el intervalo de tiempo y ver los eventos correspondientes al intervalo de tiempo seleccionado.

En la ilustración se muestran los detalles del cronograma de los datos de acceso.

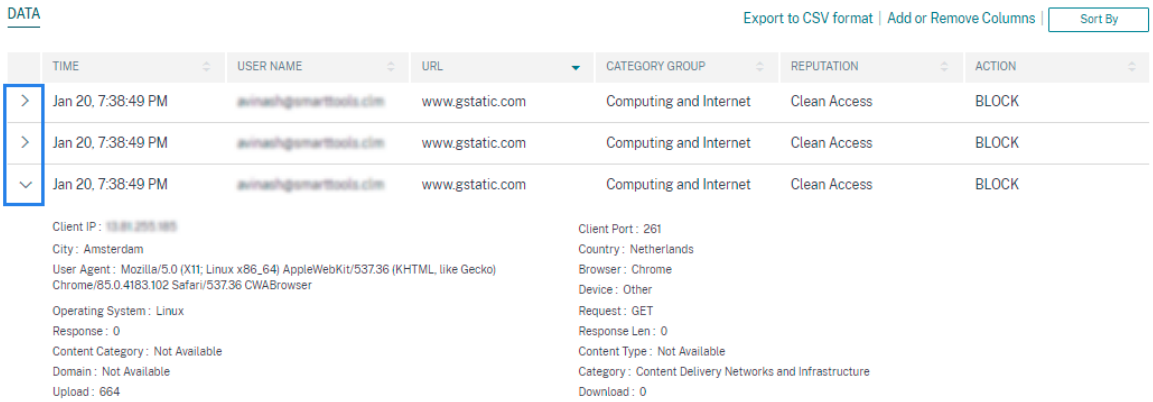



### Ver el evento

Puede ver la información detallada sobre el evento de usuario. En la tabla **DATOS**, haga clic en la flecha de cada columna para ver los detalles del evento de usuario.

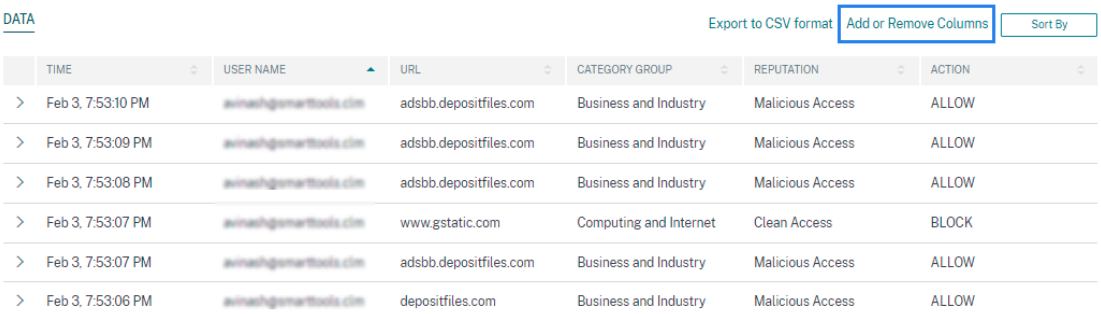
En la ilustración se muestran los detalles sobre los datos de acceso del usuario.



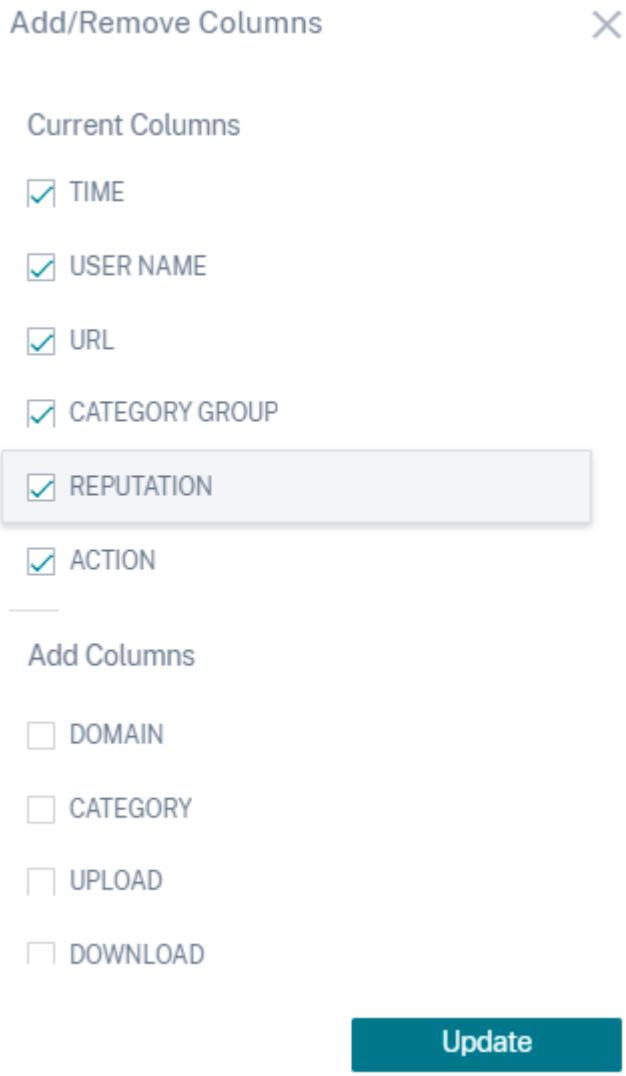

**Agregar o quitar columnas** Puede agregar o quitar columnas de la tabla de eventos para mostrar u ocultar los puntos de datos correspondientes. Haga lo siguiente:

1. Haga clic en **Agregar o quitar columnas**.



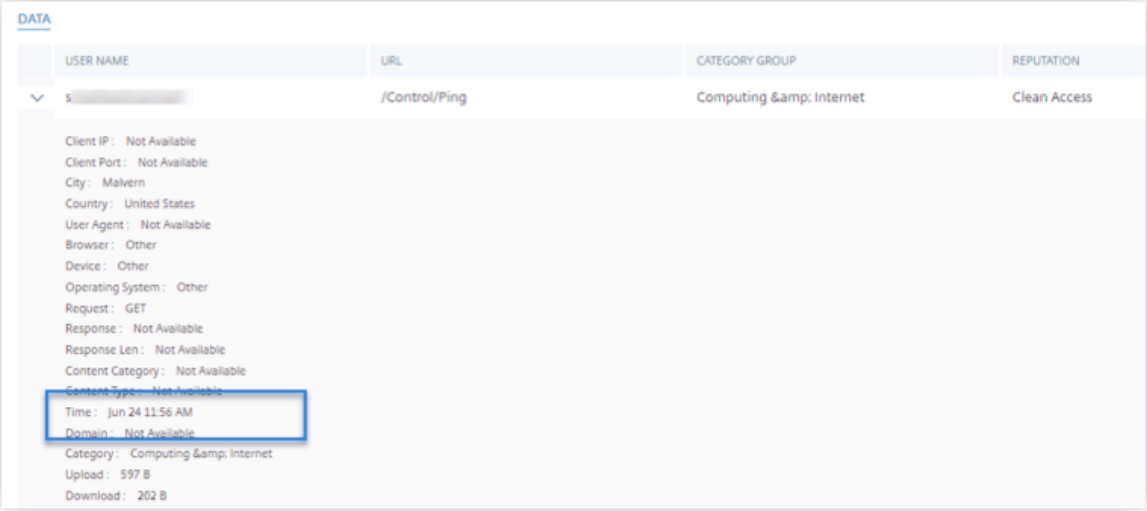

2. Seleccione o anule la selección de los elementos de datos de la lista y, a continuación, haga clic en **Actualizar**.



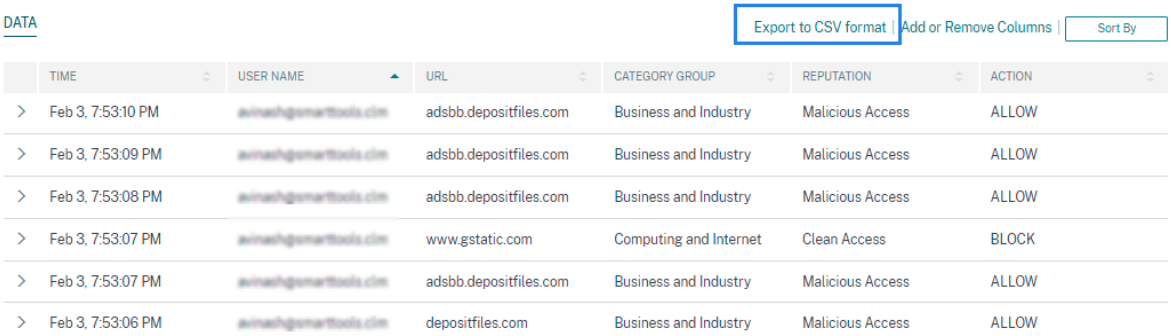

Si anula la selección de un punto de datos de la lista, la columna correspondiente se elimina de la tabla de eventos. Sin embargo, puede ver ese punto de datos expandiendo la fila de eventos de un usuario. Por ejemplo, si anula la selección del punto de datos **TIME** de la lista, la columna **TIME** se quita de la tabla de eventos. Para ver el registro de tiempo, expanda la fila de eventos de un usuario.




### Exportar los eventos a un archivo CSV

Exporta los resultados de la búsqueda a un archivo CSV y guárdalo como referencia. Haga clic en **Exportar a formato CSV** para exportar los eventos y descargar el archivo CSV generado. Puede exportar 100 000 filas mediante la función **Exportar a formato CSV**.




### Resumen visual de exportación

Puede descargar el informe resumido visual de su consulta de búsqueda y compartir una copia con otros usuarios, administradores o su equipo ejecutivo.

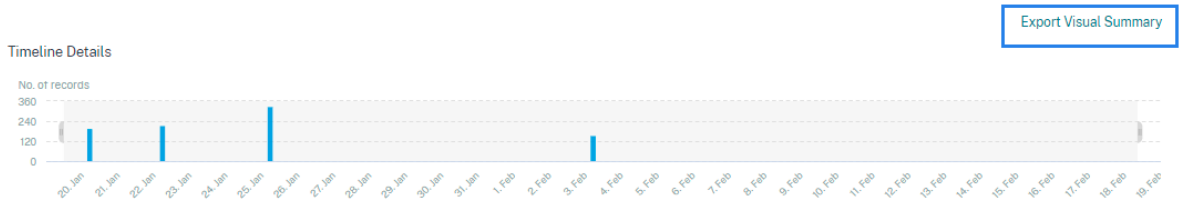
Haga clic en **Exportar resumen visual** para descargar el informe de resumen visual en formato PDF. El informe contiene la siguiente información:

- Consulta de búsqueda que ha especificado para los eventos del período de tiempo seleccionado.
- Las facetas (filtros) que ha aplicado a los eventos durante el período de tiempo seleccionado.

- El resumen visual, como los gráficos de línea de tiempo, gráficos de barras o gráficos de los eventos de búsqueda para el período de tiempo seleccionado.

Para una fuente de datos, puede descargar el informe de resumen visual solo si los datos se muestran en formatos visuales como gráficos de barras o detalles de línea de tiempo. De lo contrario, esta opción no está disponible. Por ejemplo, puede descargar el informe de resumen visual de los orígenes de datos, como Aplicaciones y escritorios, Sesiones, donde ve los datos como detalles de la línea de tiempo y gráficos de barras. Para los orígenes de datos como Usuarios y Equipos, los datos solo se ven en formato tabular. Por lo tanto, no se puede descargar ningún informe de resumen visual.

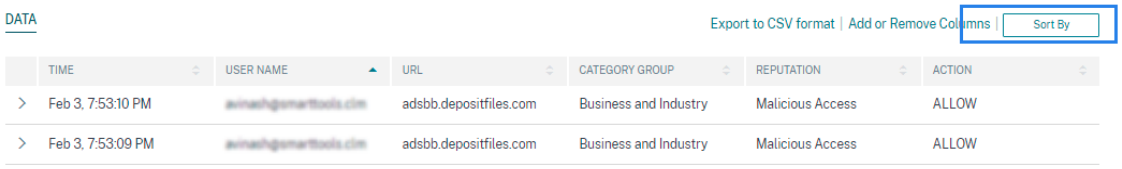



### Clasificación de varias columnas

La clasificación ayuda a organizar los datos y proporciona una mejor visibilidad. En la página de búsqueda de autoservicio, puede ordenar los eventos de usuario por una o varias columnas. Las columnas representan los valores de varios elementos de datos, como nombre de usuario, fecha y hora y URL. Estos elementos de datos varían según los orígenes de datos seleccionadas.

Para realizar una ordenación de varias columnas, haga lo siguiente:

1. Haga clic en **Ordenar por**.



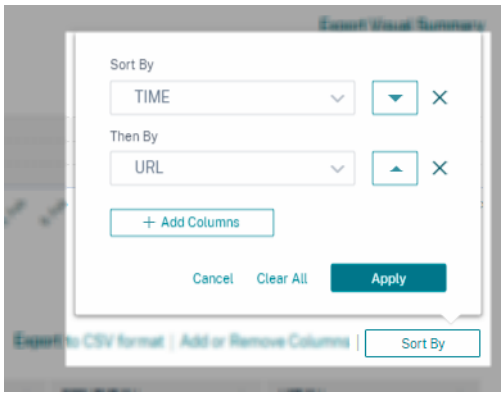

2. Seleccione una columna de la lista **Ordenar por**.
3. Seleccione el orden de clasificación: ascendente (flecha hacia arriba) o descendente (flecha abajo) para ordenar los eventos de la columna.
4. Haga clic en **+ Agregar columnas**.
5. Seleccione otra columna de la lista **Entonces por**.
6. Seleccione el orden de clasificación: ascendente (flecha hacia arriba) o descendente (flecha hacia abajo) para ordenar los eventos de la columna.

> **Nota**
>
> Puede agregar hasta seis columnas para realizar la ordenación.

7. Haga clic en **Aplicar**.
8. Si no quiere aplicar la configuración anterior, haga clic en **Cancelar**. Para quitar los valores de las columnas seleccionadas, haga clic en **Borrar todo**.

En el siguiente ejemplo se muestra una ordenación de varias columnas en los eventos Secure Private Access. Los eventos se ordenan por hora (en orden más reciente a más antiguo) y, a continuación, por URL (en orden alfabético).




Alternativamente, puede ordenar varias columnas con la tecla **Mayús**. Pulse la tecla **Mayús** y haga clic en los encabezados de columna para ordenar los eventos de usuario.

## Cómo guardar la búsqueda de autoservicio

Como administrador, puede guardar una consulta de autoservicio. Esta función ahorra el tiempo y el esfuerzo de volver a escribir la consulta que utiliza con frecuencia para el análisis o la solución de problemas. Las siguientes opciones se guardan con la consulta:

- Filtros de búsqueda aplicados
- Fuente de datos seleccionada y duración

Haga lo siguiente para guardar una consulta de autoservicio:

1. Seleccione el origen de datos y la duración necesarios.
2. Escriba una consulta en la barra de búsqueda.
3. Aplica los filtros necesarios.
4. Haga clic en **Guardar búsqueda**.
5. Especifique el nombre para guardar la consulta personalizada.

> **Nota**
>
> Asegúrese de que el nombre de la consulta sea exclusivo. De lo contrario, la consulta no se guarda.

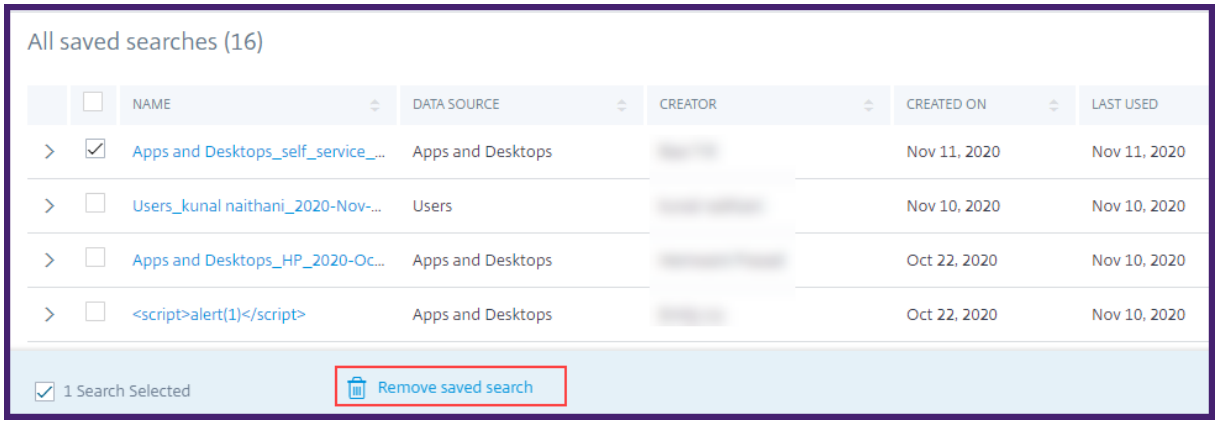
6. Active el botón **Programar informe por correo electrónico** si quiere enviar una copia del informe de consulta de búsqueda a sí mismo y a otros usuarios a intervalos regulares. Para obtener más información, consulte Programar un correo electrónico para una consulta de búsqueda.
7. Haga clic en **Guardar**.

**Para ver las búsquedas guardadas**:

1. Pulse **Ver búsquedas guardadas**.
2. Haga clic en el nombre de la consulta de búsqueda.

**Para eliminar una búsqueda guardada**:

1. Pulse **Ver búsquedas guardadas**.
2. Seleccione la consulta de búsqueda que ha guardado.
3. Haga clic en **Eliminar búsqueda guardada**.




**Para modificar una búsqueda guardada**:

1. Pulse **Ver búsquedas guardadas**.
2. Haga clic en el nombre de la consulta de búsqueda que ha guardado.
3. Modifique la consulta de búsqueda o la selección de facetas en función de su requisito.
4. Haga clic en **Actualizar búsqueda > Guardar** para actualizar y guardar la búsqueda modificada con el mismo nombre de consulta de búsqueda.

5. Si quiere guardar la búsqueda modificada con un nombre nuevo, haga clic en la flecha hacia abajo y haga clic en **Guardar como nueva búsqueda > Guardar como**.

Si reemplaza la búsqueda por un nuevo nombre, la búsqueda se guardará como una nueva entrada. Si conserva el nombre de búsqueda existente durante la sustitución, los datos de búsqueda modificados anulan los datos de búsqueda existentes.

> **Nota**
>
> - Solo el propietario de una consulta puede modificar o eliminar sus búsquedas guardadas.
> - Puede copiar la dirección de enlace de búsqueda guardada para compartirla con otro usuario.

## Programar un correo electrónico para una consulta de búsqueda

Puede enviarte una copia del informe de consultas de búsqueda a ti mismo y a otros usuarios a intervalos regulares configurando un calendario de entrega de correo electrónico.

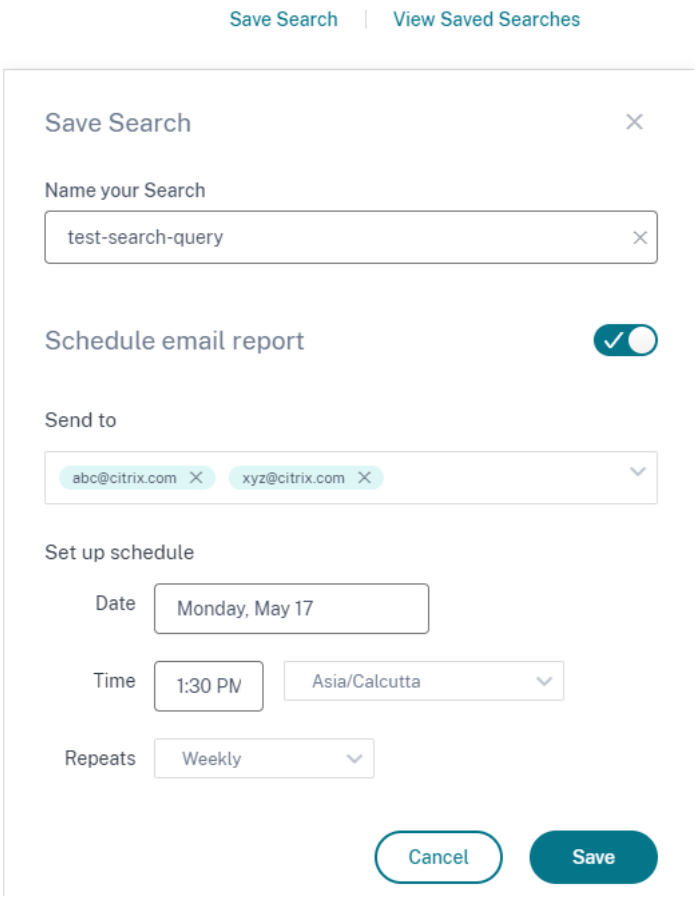
Esta opción solo está disponible si el informe de consulta de búsqueda contiene datos en formatos visuales como gráficos de barras o detalles de línea de tiempo. De lo contrario, no puede programar una entrega por correo electrónico. Por ejemplo, puede programar un correo electrónico para los orígenes de datos, como Aplicaciones y escritorios, Sesiones, donde verá los datos como detalles de la línea de tiempo y gráficos de barras. Para los orígenes de datos como Usuarios y Equipos, los datos solo se ven en formato tabular. Por lo tanto, no puede programar un correo electrónico.

### Programar un correo electrónico mientras se guarda una consulta de búsqueda

Al guardar una consulta de búsqueda, configura un calendario de entrega de correo electrónico de la siguiente manera:

1. En el cuadro de diálogo **Guardar búsqueda**, active el botón **Programar informe por correo electrónico**.




2. Introduce o pega las direcciones de correo electrónico de los destinatarios.

> **Nota**
>
> Los grupos de correo electrónico no son compatibles.

3. Establece la fecha y la hora de entrega del correo electrónico.
4. Seleccione la frecuencia de entrega: diaria, semanal o mensual.
5. Haga clic en **Guardar**.

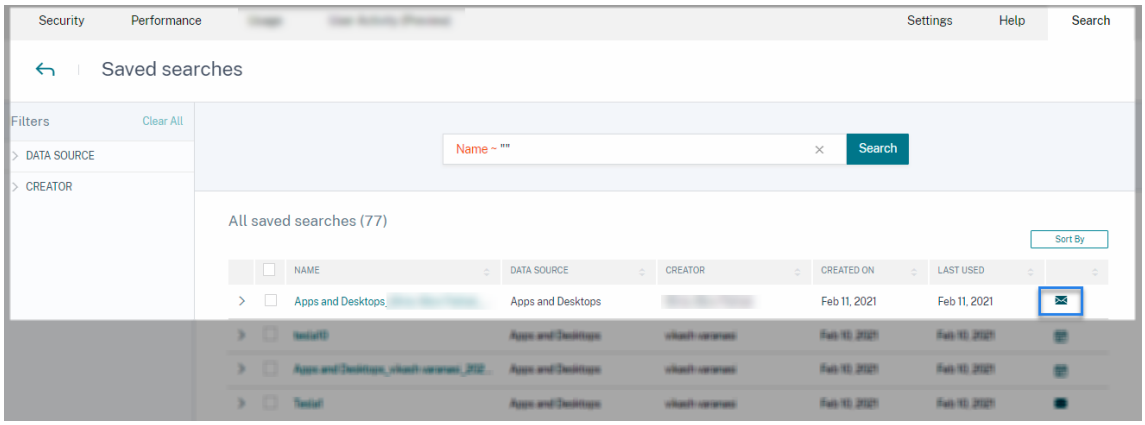
### Programar un correo electrónico para una consulta de búsqueda ya guardada

Si quiere configurar un calendario de entrega de correo electrónico para una consulta de búsqueda que guardaste anteriormente, haga lo siguiente:

1. Pulse **Ver búsquedas guardadas**.
2. Vaya a la consulta de búsqueda que ha creado. Haga clic en el icono **Enviar esta consulta por correo electrónico**.

> **Nota**
>
> Solo el propietario de una consulta puede programar la entrega por correo electrónico de su consulta de búsqueda guardada.




3. Active el botón **Programar informe por correo electrónico**.
4. Introduce o pega las direcciones de correo electrónico de los destinatarios.

> **Nota**
>
> Los grupos de correo electrónico no son compatibles.

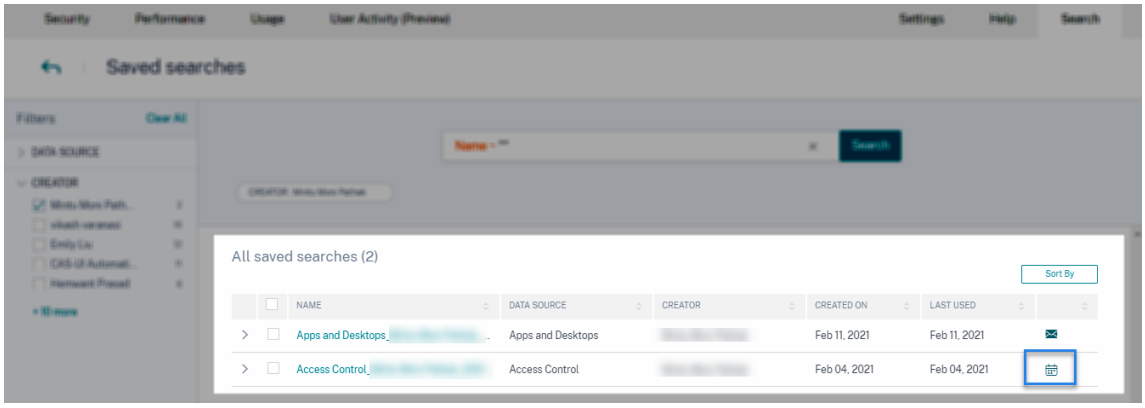
5. Establece la fecha y la hora de entrega del correo electrónico.
6. Seleccione la frecuencia de entrega: diaria, semanal o mensual.
7. Haga clic en **Guardar**.

### Detener un programa de entrega de correo electrónico para una consulta de búsqueda

1. Pulse **Ver búsquedas guardadas**.
2. Vaya a la consulta de búsqueda que ha creado. Haga clic en el icono **Ver calendario de entrega de correo electrónico**.

> **Nota**
>
> Solo el propietario de una consulta puede detener la programación de correo electrónico de su consulta de búsqueda guardada.




3. Desactive el botón **Programar informe por correo electrónico**.
4. Haga clic en **Guardar**.

### Contenido del correo electrónico

Los destinatarios reciben un correo electrónico de “Citrix Cloud - Notificaciones < donotreplynotifications@citrix.com >”sobre el informe de consultas de búsqueda. El informe se adjunta como documento PDF. El correo electrónico se envía a intervalos regulares definidos por usted en la configuración **Programar informe de correo electrónico**.

El informe de consultas de búsqueda contiene la siguiente información:

- Consulta de búsqueda que ha especificado para los eventos del período seleccionado.
- Las facetas (filtros) que ha aplicado a los eventos.
- El resumen visual, como los gráficos de línea de tiempo, gráficos de barras o gráficos de los eventos de búsqueda.

## Permisos para administradores de acceso total y acceso de solo lectura

- Si es administrador de Citrix Cloud con acceso completo, puede usar todas las funciones disponibles en la página **Buscar**.
- Si es administrador de Citrix Cloud con acceso de solo lectura, solo puede realizar las siguientes actividades en la página **Buscar**:
  - Para ver los resultados de la búsqueda, seleccione una fuente de datos y el período de tiempo.
  - Introduzca una consulta de búsqueda y consulte los resultados de la búsqueda.
  - Permite ver los resultados de búsqueda guardados de otros administradores.

- Exporte el resumen visual y descargue los resultados de la búsqueda en un archivo CSV.

Para obtener información sobre las funciones de administrador, consulte Administrar funciones de administrador para Citrix Analytics.

## Búsqueda de autoservicio de autenticación

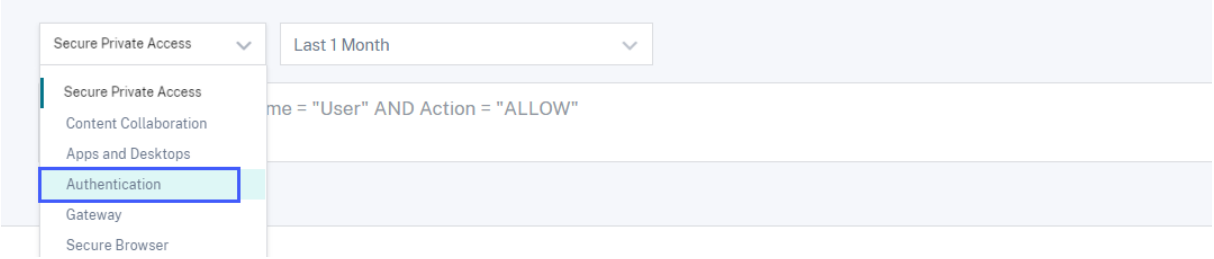
September 27, 2021

Utilice la búsqueda de autoservicio para obtener información sobre los detalles de autenticación de usuarios de Citrix Cloud de su empresa. Citrix Analytics for Security recibe los eventos de autenticación de usuarios del servicio Administración de identidades y accesos de Citrix Cloud. Los eventos de autenticación, como el inicio de sesión del usuario, el cierre de sesión del usuario y la actualización del cliente, se muestran en la página de búsqueda de autoservicio.

Para obtener más información sobre las funcionalidades de búsqueda, consulte **Búsqueda de autoservicio**.

### Seleccione el origen de datos de autenticación

Para ver los eventos de autenticación, seleccione **Autenticación** en la lista. De forma predeterminada, la página de autoservicio muestra los eventos del último día. También puede seleccionar el período de tiempo para el que quieres ver los eventos.

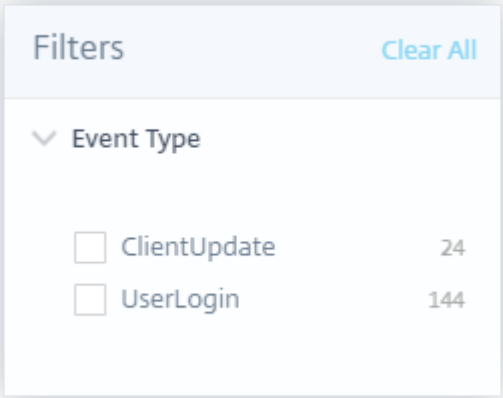



### Seleccione las facetas para filtrar los eventos

Utilice el filtro siguiente para los eventos de autenticación:

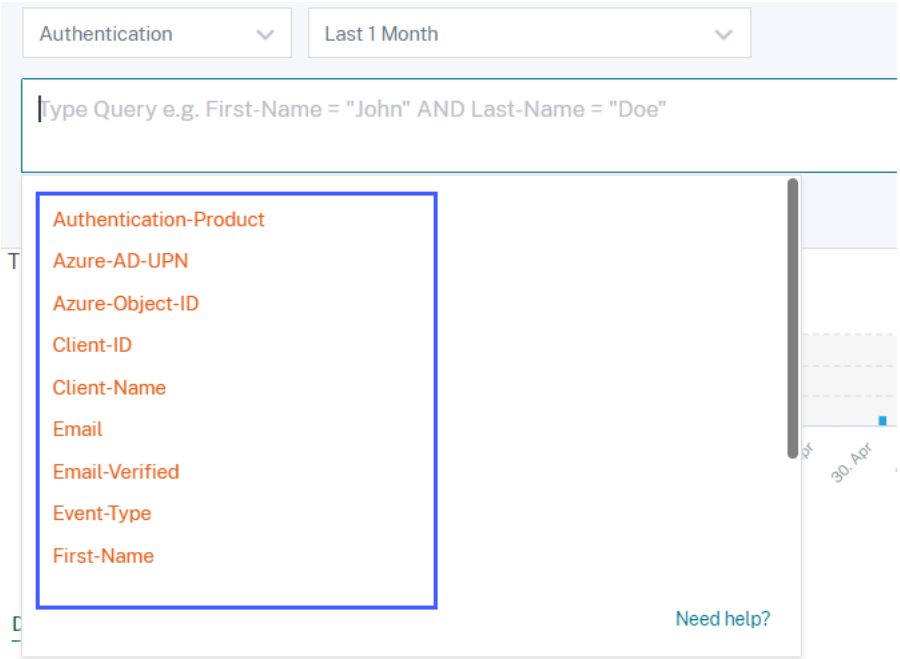
- **Tipo de evento**: busca eventos según los tipos de eventos de usuario, como inicio de sesión de usuario, cierre de sesión de usuario y actualización de clientes.




### Especificar consulta de búsqueda para filtrar eventos

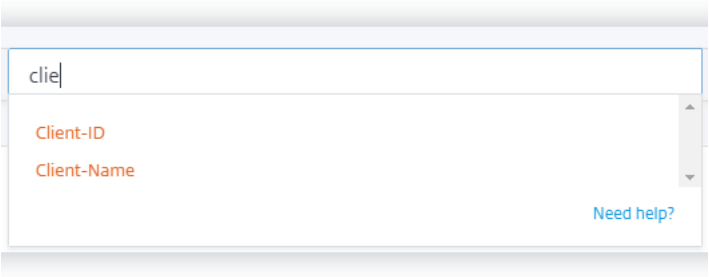
Sitúe el cursor en el cuadro de búsqueda para ver la lista de dimensiones de los eventos de autenticación. Utilice las dimensiones y los operadores para especificar la consulta y buscar los eventos necesarios.



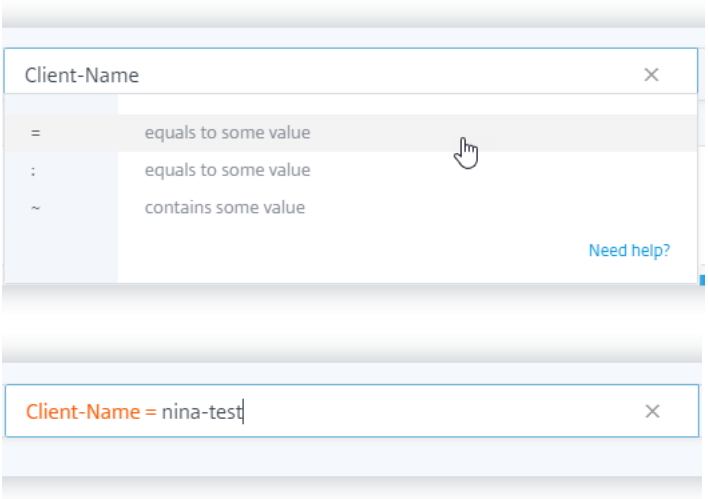

Por ejemplo, quiere ver los eventos de autenticación de un cliente “nina-test”con el estado del correo electrónico verificado.

1. Introduzca “cliente”en el cuadro de búsqueda para obtener las dimensiones relacionadas.

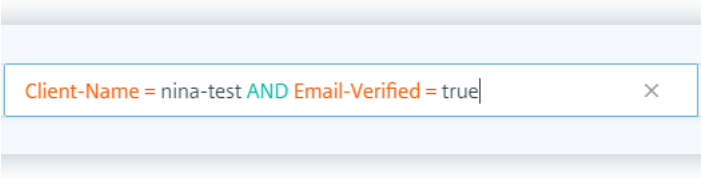
 




2. Seleccione **Nombre del cliente** y, a continuación, especifique el valor “nina-test”con el operador igual.




3. Seleccione el operador **AND y**, a continuación, seleccione la dimensión **Verificado por correo electrónico** . Asigne el valor “true”a **Email-Verified** mediante el operador igual. El valor “true” indica que se ha verificado el correo electrónico del usuario.




4. Seleccione el período de tiempo y haga clic en **Buscar** para ver los eventos en la tabla **DATA**.

## Búsqueda de autoservicio para Gateway

September 27, 2021

Utilice la función de búsqueda de autoservicio para obtener información sobre los eventos de usuario recibidos del origen de datos de Citrix Gateway. Cuando los usuarios acceden a sus recursos de red,

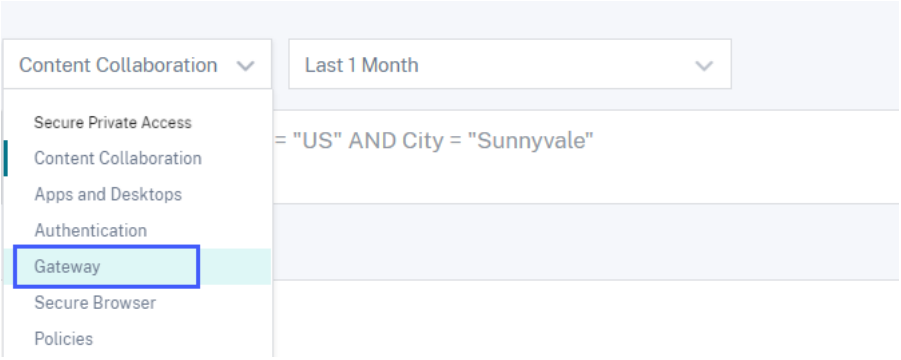
 

como servidores de archivos, aplicaciones y sitios web a través de Citrix Gateway, se generan eventos para cada conexión de usuario. Algunos ejemplos de eventos de usuario son, por ejemplo, etapa de autenticación, tipo de autorización y código de sesión VPN. Citrix Analytics for Security recibe estos eventos y los muestra en la página de búsqueda de autoservicio. Puede ver los usuarios y sus datos de acceso.

Para obtener más información sobre las funcionalidades de búsqueda, consulte **Búsqueda de autoservicio**.

### Seleccione el origen de datos de Gateway

Para ver los eventos de Gateway, seleccione **Gateway** en la lista. De forma predeterminada, la página de autoservicio muestra los eventos del último día. También puede seleccionar el período de tiempo para el que quieres ver los eventos.

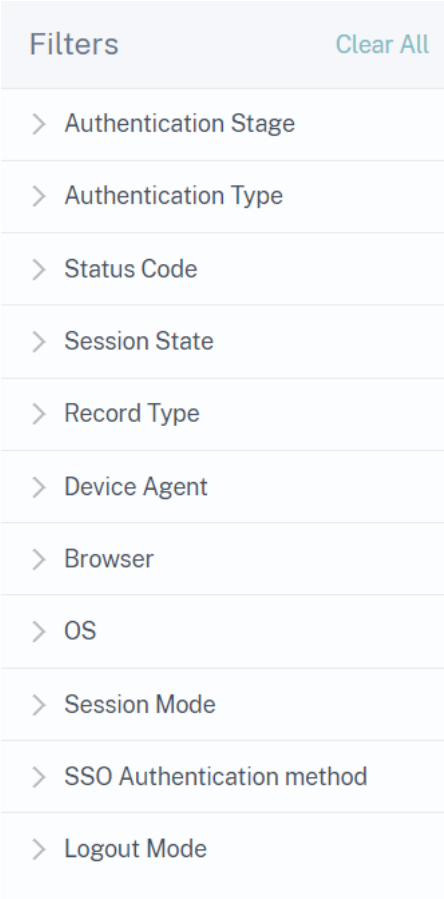



> **Nota**
>
> De forma alternativa, puede acceder a la página Búsqueda de autoservicio de puerta de enlace desde el panel **Seguridad** > **Usuarios** > **Resumen de acceso** . En casos de inicio de sesión satisfactorio, puede acceder a los datos mediante el código de estado. Para obtener más información, consulte el panel Resumen de acceso .

### Utilizar las facetas para filtrar eventos

Las facetas se clasifican en función de los eventos recibidos del origen de datos. Utilice las siguientes facetas para filtrar los eventos:




- **Fase de autenticación**: busque eventos en función de las diferentes etapas de la autenticación del cliente, como primaria, secundaria y terciaria.
- **Tipo de autenticación**: busca eventos basados en los tipos de autenticación del cliente, como Local, RADIUS, LDAP, TACACS, autenticación de certificados de cliente, incluida la autenticación con tarjeta inteligente.
- **Device Agent**: Busque eventos basados en los dispositivos cliente como iPhone, iPad, Windows Mobile.
- **Tipo de registro**: busca eventos según los tipos de registros VPN. Los siguientes tipos de registros VPN están disponibles:

| Tipo de registro | Descripción |
|---|---|
| VPN_AI | Filtra los eventos de usuario relacionados con la autenticación. |
| VPN_IF | Filtra los eventos de usuario relacionados con el archivo ICA. |
| VN_ST | Filtra los eventos de usuario relacionados con el cierre de sesión. |

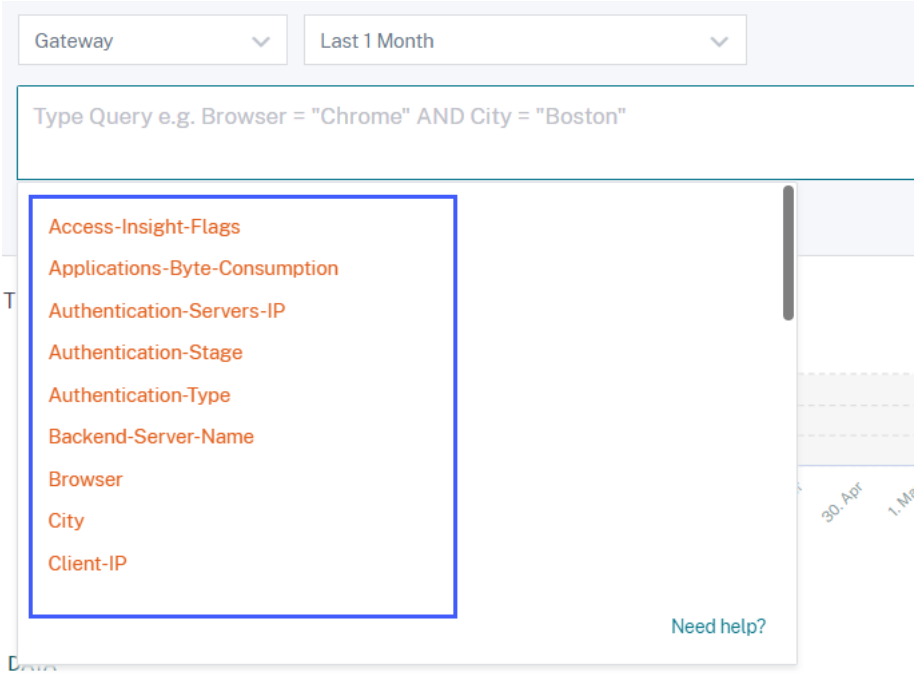
 

- **Explorador**: Busque eventos basados en los exploradores como Internet Explorer, Chrome, Firefox, Safari.
- **SO**: busca eventos basados en los sistemas operativos del cliente como Windows, Mac, Linux, Android, iOS.
- **Código de estado**: busca eventos basados en los códigos de estado de VPN, como error de respuesta de redirección SSL, error de autorización, error de inicio de sesión único.
- **Estado de la sesión**: busca eventos según los estados de la sesión VPN, como el estado del cliente, el estado de autorización, el estado de SSO y la actualización del ancho de banda de la aplicación.
- **Modo de sesión**: busca eventos basados en los modos de sesión VPN, como Túnel completo, Proxy ICA, Clientless.
- **Método de autenticación de SSO**: busca eventos basados en diferentes métodos de autenticación de inicio de sesión único, como básico, resumen, NTLM, Kerberos, AG básico, SSO basado en formularios.
- **Modo de cierre de sesión**: Busque eventos basados en los modos de cierre de sesión VPN, tales como cierre de sesión de error interno, cierre de sesión de tiempo de espera de sesión, cierre de sesión iniciado por el usuario, sesión de administrador terminada.

### Especificar consulta de búsqueda para filtrar eventos

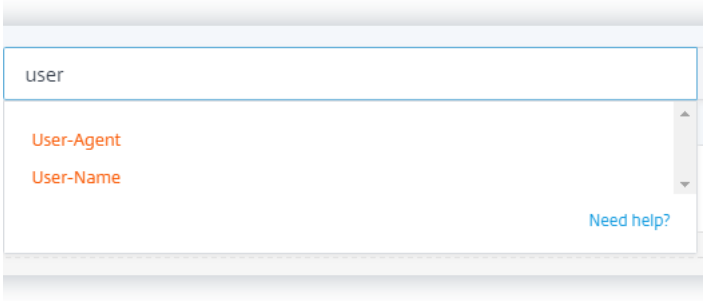
Sitúe el cursor en el cuadro de búsqueda para ver la lista de dimensiones de los eventos de Gateway. Utilice las dimensiones y los operadores para especificar la consulta y buscar los eventos necesarios.

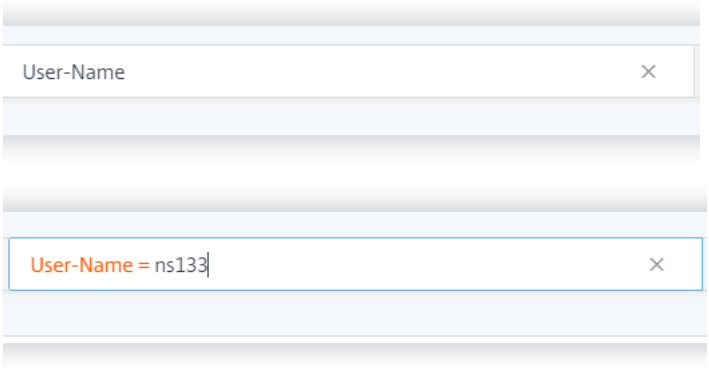



Por ejemplo, quiere ver los eventos de un usuario "ns133"en el que el código de estado de la VPN es "inicio de sesión correcto".

1. Introduzca "usuario"en el cuadro de búsqueda para elegir la dimensión relacionada.



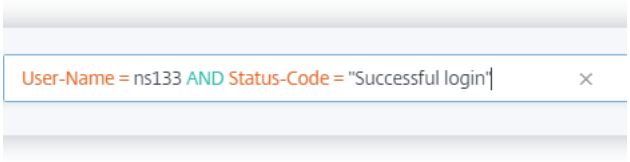

2. Seleccione **Nombre de usuario** e introduzca el valor "ns133"con el operador igual.



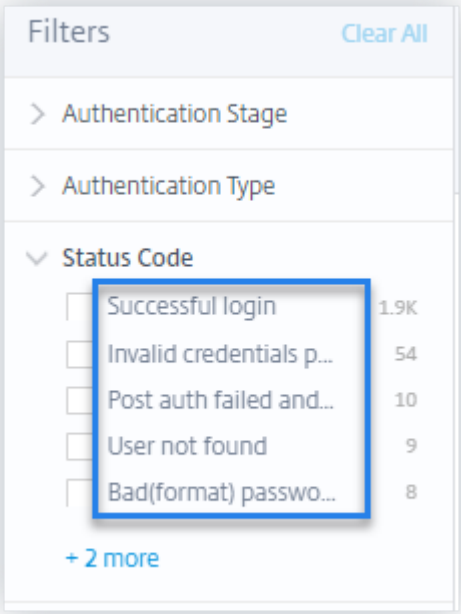

3. Seleccione el operador **AND y**, a continuación, seleccione la dimensión **Código de estado** . In-

troduzca la cadena “Inicio de sesión satisfactorio”para **Código de estado** con el operador igual.




Para identificar los posibles valores de cadena de **código de estado**, expanda la lista de filtros **Código de estado** y utilice el nombre del filtro como cadena en la consulta de búsqueda.




4. Seleccione el período de tiempo y haga clic en **Buscar** para ver los eventos en la tabla **DATA**.

## Valores admitidos para su consulta de búsqueda

Introduzca los siguientes valores para las dimensiones para definir la consulta de búsqueda.

### Indicadores de Access-Insight

Indica el estado de la sesión VPN. Introduzca uno de los valores de marca siguientes:

| Estado de sesión VPN | Valor de bandera |
|---|---|
| Autentificación previa | 2 |

| Estado de sesión VPN | Valor de bandera |
|---|---|
| Último o último estado de la autenticación nFactor (multifactor) | 1 |
| Post autenticación | 4 |

> **Nota**
>
> Este indicador solo se aplica a los estados de sesión VPN anteriores para los eventos de autenticación. Para todos los demás eventos, el valor de la bandera es cero.

#### Consumo de bytes de aplicaciones

Para la `Applications-Byte-Consumption` dimensión, introduzca el siguiente valor:

| Valor | Tipo | Descripción |
|---|---|---|
| Ejemplos: `40`, `100` | Número | Datos (en bytes) consumidos por la aplicación que está utilizando. |

#### IP de servidores de autenticación

Para la `Authentication-Servers-IP` dimensión, introduzca el siguiente valor:

| Valor | Tipo | Descripción |
|---|---|---|
| Ejemplo:`10.xxx.xx.xx` | Cadena | Dirección IP del servidor de autenticación. |

#### Fase de autenticación

Para la `Authentication-Stage` dimensión, introduzca el siguiente valor:

| Valor | Tipo | Descripción |
|---|---|---|
| `Primary`, `Secondary`, o `Tertiary` | Cadena | Diferentes etapas de la autenticación de clientes. |

**Tipo de autenticación**

Para la `Authentication-Type` dimensión, introduzca el siguiente valor:

| Valor | Tipo | Descripción |
|---|---|---|
| `LDAP`,`SAML`, `Local`, `Radius`, `TACACS`, `SAMLIDP`, o `OTP`. | Cadena | Autentica a tus usuarios mediante uno de los métodos disponibles. |

**Nombre del servidor backend**

Para la `Backend-Server-Name` dimensión, introduzca el siguiente valor:

| Valor | Tipo | Descripción |
|---|---|---|
| Ejemplo:`10.xxx.xxx.xx` | Cadena | Dirección IP del servidor back-end. |

**Explorador web**

Para la `Browser` dimensión, introduzca el siguiente valor:

| Valor | Tipo | Descripción |
|---|---|---|
| `PN Agent`, `Edge`, `Firefox`, `Chrome`, o `Safari`. | Cadena | Explorador utilizado. |

**Ciudad**

Para la `City` dimensión, introduzca el siguiente valor:

| Valor | Tipo | Descripción |
|---|---|---|
| Ejemplos: `Boston`, `Beijing` | Cadena | Ciudad desde la que el usuario ha iniciado sesión. |

**Cliente-IP**

Para la `Client-IP` dimensión, introduzca el siguiente valor:

| Valor | Tipo | Descripción |
|---|---|---|
| Ejemplo:`10.xxx.xxx.xx` | Cadena | Dirección IP del dispositivo del usuario. |

**Tipo de IP de cliente**

Para la `Client-IP-Type` dimensión, introduzca el siguiente valor:

| Valor | Tipo | Descripción |
|---|---|---|
| público, privado | Cadena | Indica si la dirección IP del usuario es pública o privada. |

> **Nota**
>
> Los valores distinguen entre mayúsculas y minúsculas Introduzca los valores en minúsculas.

**Cliente-puerto**

Para la `Client-Port` dimensión, introduzca el siguiente valor:

| Valor | Tipo | Descripción |
|---|---|---|
| Ejemplo:`45334` | Número | Número de puerto del dispositivo de usuario. |

**País**

Para la `Country` dimensión, introduzca el siguiente valor:

| Valor | Tipo | Descripción |
|---|---|---|
| Ejemplos: `United States`, `India` | Cadena | País desde el que el usuario ha iniciado sesión. |

> **Nota**
>
> Encierra el valor dentro de “”si el valor contiene espacios. **Ejemplo**: País = “Estados Unidos”.

#### Tipo de Evento

Para la `Event-Type` dimensión, introduzca el siguiente valor:

| Valor | Tipo | Descripción |
|---|---|---|
| Autenticación, archivo ICA, cierre de sesión | Cadena | Tipo de eventos de usuario. |

#### FQDN de puerta de enlace

Para la `Gateway-FQDN` dimensión, introduzca el siguiente valor:

| Valor | Tipo | Descripción |
|---|---|---|
| Ejemplo:`Gateway-test` | Cadena | Nombre de dominio de su Citrix Gateway. |

#### IP de puerta de enlace

Para la `Gateway-IP` dimensión, introduzca el siguiente valor:

| Valor | Tipo | Descripción |
|---|---|---|
| Ejemplo:`10.xxx.xxx.xx` | Cadena | Dirección IP de su Citrix Gateway. |

#### Puerto de puerta de enlace

Para la `Gateway-Port` dimensión, introduzca el siguiente valor:

| Valor | Tipo | Descripción |
|---|---|---|
| Ejemplo:`443` | Cadena | Número de puerto de Citrix Gateway. |

#### Modo de cierre de sesión

Para la `Logout-Mode` dimensión, introduzca el siguiente valor:

| Valor | Tipo | Descripción |
|---|---|---|
| `"Internal error"`, `"Inactive time out"`, `"User initiated logout"`, o `"Administrator killed session"`. | Cadena | Motivo del tiempo de espera o de la finalización de la sesión VPN. |

> **Nota**
>
> Encierra el valor dentro de “”si el valor contiene espacios. **Ejemplo**: Modo de cierre de sesión = `"Internal error"`.

#### IP de NetScaler

Para la `NetScaler-IP` dimensión, introduzca el siguiente valor:

| Valor | Tipo | Descripción |
|---|---|---|
| Ejemplo:`10.xxx.xx.xx` | Cadena | Dirección IP del dispositivo Citrix ADC. |

#### SO

Para la `OS` dimensión, introduzca el siguiente valor:

| Valor | Tipo | Descripción |
|---|---|---|
| Ejemplos: `MAC_OS`, `WINDOWS` | Cadena | Sistema operativo del dispositivo del usuario. |

#### Tipo de registro

Para la `Record Type` dimensión, introduzca el siguiente valor:

| Valor | Tipo | Descripción |
|---|---|---|
| VPN_AI | Cadena | Indica los eventos de usuario relacionados con la autenticación. |
| VPN_IF | Cadena | Indica los eventos de usuario relacionados con el archivo ICA. |
| VPN_ST | Cadena | Indica sucesos de usuario relacionados con el cierre de sesión. |

**Método de autenticación SSO**

Para la SSO-Authentication-Method dimensión, introduzca el siguiente valor:

| Valor | Tipo | Descripción |
|---|---|---|
| NSAUTH_BEARER, NSAUTH_FORM, NSAUTH_CITRIXAGBASIC, NSAUTH_NEGOTIATE, NSAUTH_NTLM, o NSAUTH_BASIC. | Cadena | Distintos métodos de autenticación de inicio de sesión único. |

**IP del servidor**

Para la Server-IP dimensión, introduzca el siguiente valor:

| Valor | Tipo | Descripción |
|---|---|---|
| Ejemplo:10.xx.xxx.xx | Cadena | Dirección IP del servidor back-end. |

**Puerto de servidor**

Para la Server-Port dimensión, introduzca el siguiente valor:

| Valor | Tipo | Descripción |
| --- | --- | --- |
| Ejemplo:`47054` | Número | Número de puerto del servidor back-end. |

**Estado de sesión**

Para la `Session-State` dimensión, introduzca el siguiente valor:

| Valor | Tipo | Descripción |
| --- | --- | --- |
| `"Set Client State"`, `"Authorization State"`, `"SSO State"`, y `"Application Bandwidth Update"` | Cadena | El estado de la sesión VPN. |

> **Nota**
>
> Encierra el valor dentro de “”si el valor contiene espacios. **Ejemplo**: Estado de sesión = `"Set Client State"`.

**Código de estado**

Para la `Status-Code` dimensión, introduzca el siguiente valor:

| Valor | Tipo | Descripción |
| --- | --- | --- |
| `"Successful login"`, `"Invalid credentials passed"`„ `"Post auth failed and connection quarantined"`, `"Login not permitted"`, `"Maximum login failures reached"` | Cadena | El código de estado de la VPN. |

> **Nota**
>
> Encierra el valor dentro de “”si el valor contiene espacios. **Ejemplo**: Código de sesión = `"Successful login"`.

#### Agente de usuario

Para la `User-Agent` dimensión, introduzca el siguiente valor:

| Valor | Tipo | Descripción |
|---|---|---|
| `IPHONE`, `IPAD`, o `WINPHONE` | Cadena | El agente o el dispositivo utilizado para acceder a la VPN. |

#### ID de sesión VPN

Para la `VPN-Session-ID` dimensión, introduzca el siguiente valor:

| Valor | Tipo | Descripción |
|---|---|---|
| `c2c290c61dfe4e07247bde1e02b42a12` | Cadena | ID de sesión asignado por el servidor para la sesión VPN de un usuario. |

#### Modo sesión VPN

Para la `VPN-Session-Mode` dimensión, introduzca el siguiente valor:

| Valor | Tipo | Descripción |
|---|---|---|
| `"Full Tunnel"`, `"ICA Proxy"`, o `Clientless` | Cadena | Diferentes modos de la sesión VPN de un usuario. |

> **Nota**
>
> Encierra el valor dentro de “”si el valor contiene espacios. **Ejemplo**: Código de sesión = `"Full Tunnel"`.

# Búsqueda de directivas de autoservicio

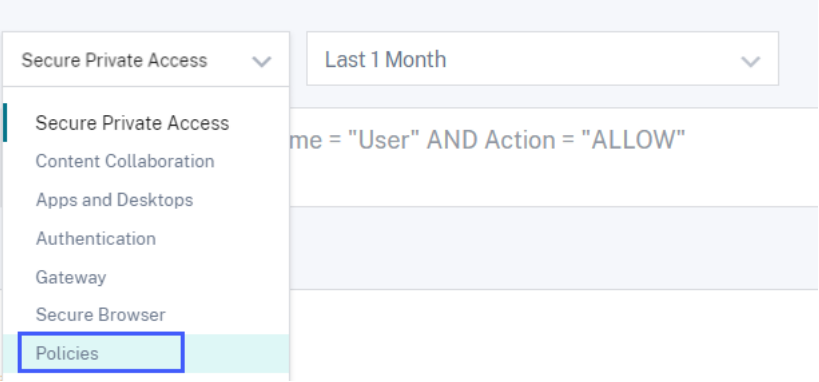
May 9, 2022

Citrix Analytics for Security le permite crear directivas y aplicar acciones en caso de sucesos inusuales o sospechosos en las cuentas de usuario. Cuando los eventos de usuario cumplen las directivas definidas, las acciones se aplican automáticamente en las cuentas de usuario para aislar la amenaza y evitar que se produzcan futuros eventos anómalos. Mediante la búsqueda de autoservicio, puede ver los eventos de usuario que han cumplido las directivas definidas y ver las acciones aplicadas en estos eventos anómalos.

Para obtener más información sobre las funcionalidades de búsqueda, consulte **Búsqueda de autoservicio**.

## Seleccione el conjunto de datos Policies

Para ver los eventos relacionados con las directivas definidas, seleccione **Directivas** de la lista. De forma predeterminada, la página de autoservicio muestra los eventos del último día. También puede seleccionar el período de tiempo para el que quiere ver los eventos.



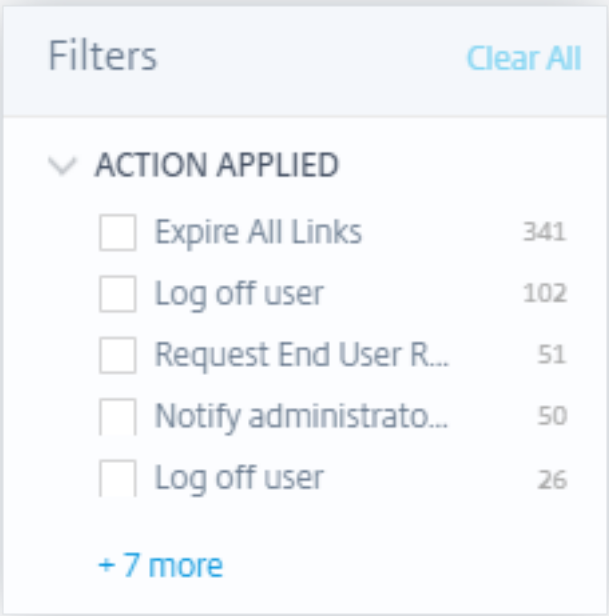

> **Nota**
>
> También puede acceder a la página Búsqueda de autoservicio de directivas desde el panel **Seguridad** > **Usuarios** > **Directivas y acciones** . Seleccione una directiva en el panel de control para ver los eventos de usuario relacionados con la directiva. Para obtener más información, consulte el panel Directivas y acciones .

## Seleccione las facetas para filtrar los eventos

La lista de facetas muestra las acciones aplicadas en los eventos de usuario. Seleccione las acciones aplicadas de la lista de facetas y visualice los eventos en función de las acciones aplicadas. Para

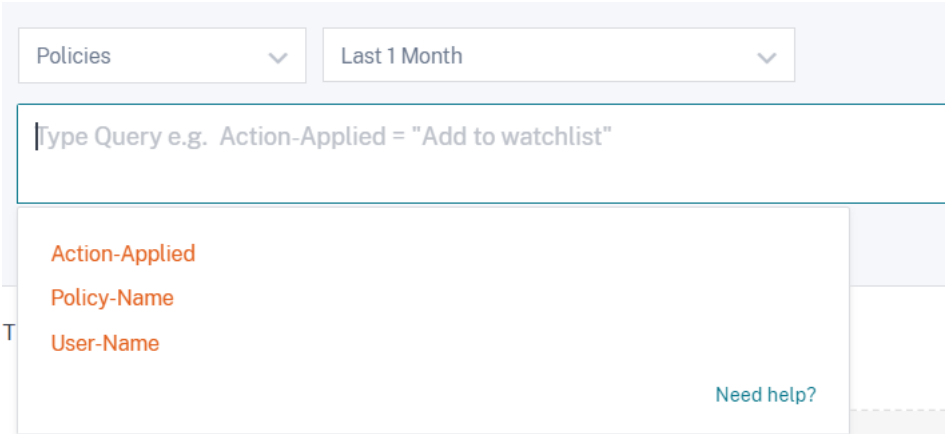
 

obtener más información sobre las acciones que puede aplicar al configurar directivas, consulte ¿Qué son las acciones?




### Especificar consulta de búsqueda para filtrar eventos

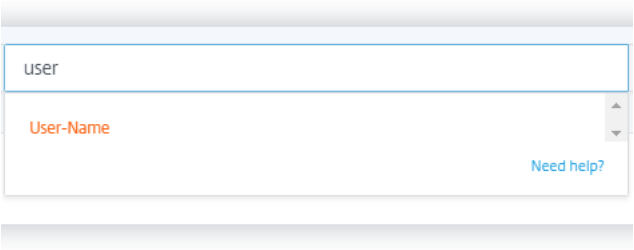
Sitúe el cursor en el cuadro de búsqueda para ver la lista de dimensiones de los eventos relacionados con las directivas. Utilice las dimensiones y los operadores para especificar la consulta y buscar los eventos necesarios.



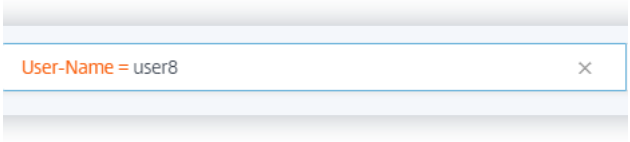

Por ejemplo, quiere ver los eventos anómalos de un usuario “usuario8”donde la acción aplicada a esos eventos es “Inhabilitar usuario”. “

1. Introduzca “user”en el cuadro de búsqueda para obtener las dimensiones relacionadas.

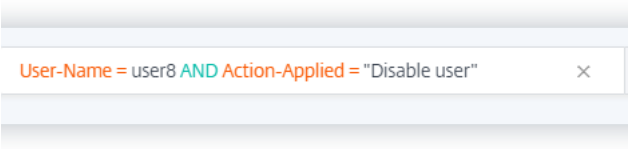



2. Seleccione **Nombre de usuario** e introduzca el valor “usuario8”con el operador igual.



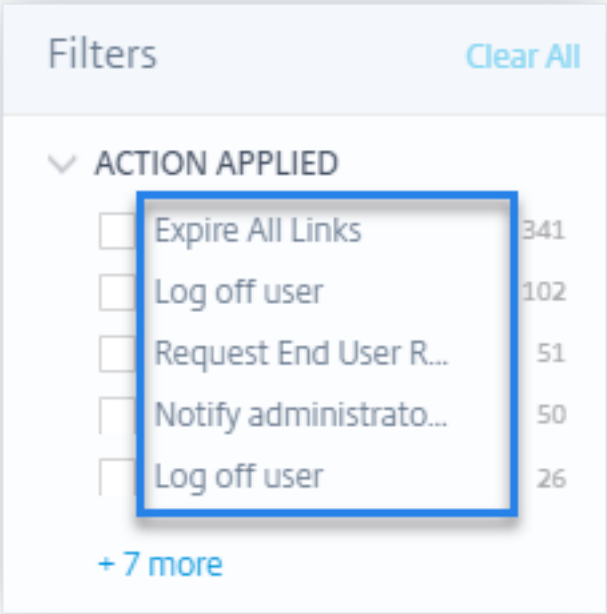

3. Seleccione el operador **AND y**, a continuación, seleccione la dimensión **Aplicada por acción** . Introduzca la cadena “Inhabilitar usuario”para **Acción aplicada** mediante el operador igual.

> **Nota**
>
> Si el valor de cadena contiene dos o más palabras, debe incluirse con el operador “” . Por ejemplo “ `Disable user`”, “Detener grabación de sesiones”.




Para identificar los posibles valores de cadena para **Acción aplicada**, expanda la lista de facetas y utilice el nombre del filtro como cadena en la consulta de búsqueda.




4. Seleccione el período de tiempo y haga clic en **Buscar** para ver los eventos en la tabla **DATA**.

## Búsqueda de autoservicio para aislamiento remoto de navegadores (Secure Browser)

December 7, 2023

Utilice la búsqueda de autoservicio para obtener información sobre las sesiones de navegación de los usuarios de Citrix Workspace que utilizan Citrix Remote Browser Isolation Service. Citrix Remote Browser Isolation es un servicio en la nube que proporciona una experiencia de navegación por Internet segura sin comprometer la seguridad de la red corporativa. Cuando los usuarios acceden a las aplicaciones web mediante Remote Browser Isolation, se generan eventos como la conexión de sesión, el inicio de la sesión, las aplicaciones publicadas y las aplicaciones eliminadas para cada conexión de usuario. Citrix Analytics for Security recibe estos eventos y los muestra en la página de autoservicio. Puede hacer un seguimiento de los usuarios y sus sesiones de navegación.

Para obtener más información sobre las funcionalidades de búsqueda, consulte **Búsqueda de autoservicio**.

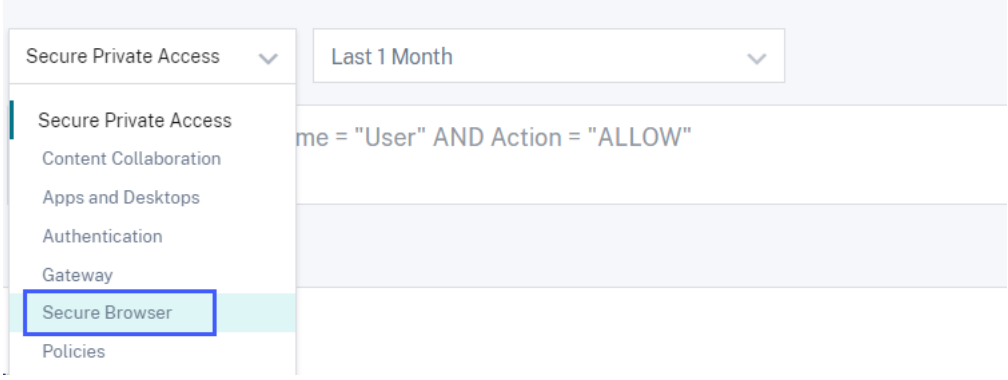
 

### Requisito previo

Para recibir eventos de Remote Browser Isolation, habilite el **seguimiento de nombres de host** en Remote Browser Isolation para registrar los nombres de host de las sesiones de usuario. Esta información se envía a Citrix Analytics for Security. Para obtener más información, consulte Administrar sesiones de Remote Browser Isolation publicadas.

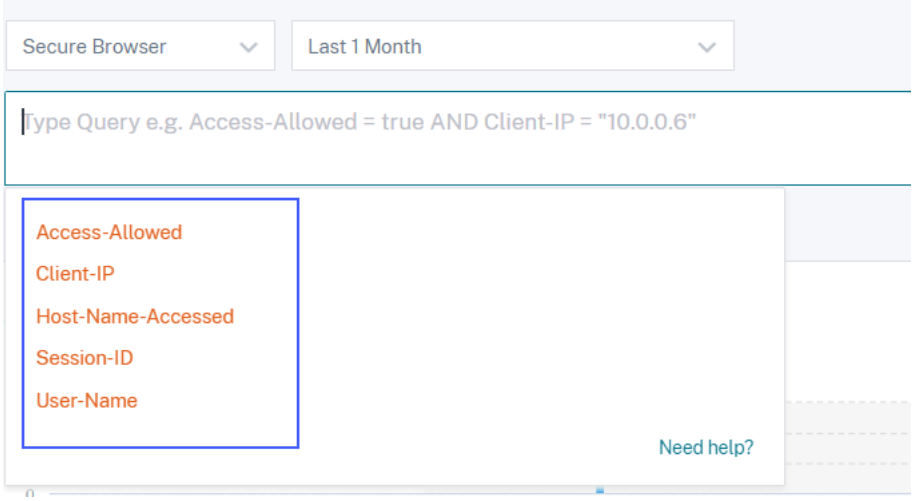
### Seleccione el origen de datos de Remote Browser Isolation

Para ver los eventos de Remote Browser Isolation, seleccione **Remote Browser Isolation** en la lista. De forma predeterminada, la página de autoservicio muestra los eventos del último día. También puede seleccionar el período de tiempo para el que quiere ver los eventos.




### Especificar consulta de búsqueda para filtrar eventos

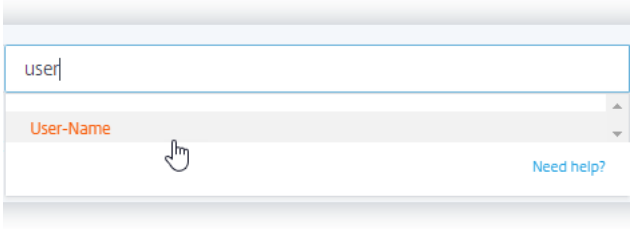
Coloque el cursor en el cuadro de búsqueda para ver la lista de dimensiones de los eventos de Remote Browser Isolation. Utilice las dimensiones y los operadores para especificar la consulta y buscar los eventos necesarios.



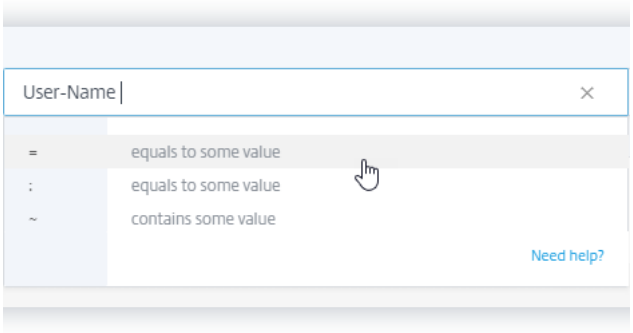

 

Por ejemplo, quiere ver los detalles del evento de navegación de un usuario “aa”que tiene permiso para acceder a varios servicios de host, como google.com, amazon.com.

1. Introduzca “user”en el cuadro de búsqueda para ver las dimensiones relacionadas.




2. Haga clic en **Nombre de usuario** e introduzca el valor “aa”con el operador igual.




3. Seleccione el operador **AND** y la dimensión **Allow-Access** . Asigne el valor “true”a **Allow-Access** mediante el operador igual. El valor “true”indica que el usuario puede acceder a los servicios host.




4. Seleccione el período de tiempo y haga clic en **Buscar** para ver los eventos en la tabla **DATA**.

## Ver detalles de eventos de usuario

Puede ver los siguientes datos recibidos de Remote Browser Isolation Service:

- **Hora**: fecha y hora en que se produjo el evento de usuario.
- **Nombre de usuario**: usuario que inició el evento.
- **ID de sesión**: número exclusivo asignado a la sesión de usuario.
- **IP del cliente**: dirección IP del dispositivo del usuario.
- **Nombre de host**: servicio host al que accede el usuario a través de la red.

- **Permitir acceso**: el usuario tiene permitido o denegado el acceso al servicio host.

## Búsqueda de autoservicio para Secure Private Access

April 12, 2024

Utilice la búsqueda de autoservicio para obtener información sobre los eventos de acceso de los usuarios de Citrix Cloud de su organización. Ejemplos de eventos de acceso son la categoría de url, la categoría de contenido, los exploradores y los dispositivos. Citrix Analytics for Security recibe estos eventos del servicio Secure Private Access y los muestra en la búsqueda de autoservicio. Puede hacer un seguimiento de los usuarios y sus datos de acceso.

Para obtener más información sobre las funcionalidades de búsqueda, consulte **Búsqueda de autoservicio**.

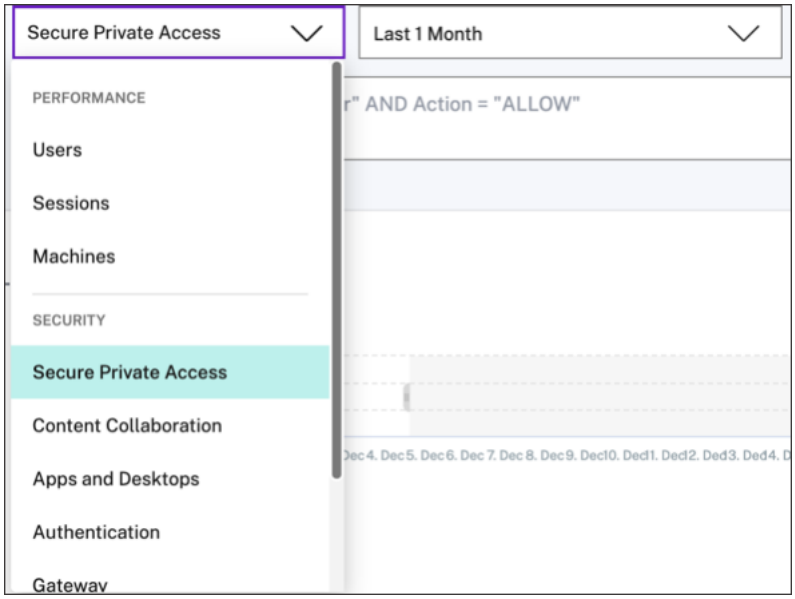
> **Nota:**
>
> Estas prestaciones de Citrix Analytics for Security se ven afectadas debido a que Secure Private Access ha dejado de utilizar el filtrado web basado en categorías:
>
> 1. Los campos de datos como el grupo de categorías, la categoría y la reputación de las URL ya no están disponibles en el panel de seguridad de Citrix Analytics.
> 2. El indicador de acceso a sitios web de riesgo, que se basa en los mismos datos, también se ha retirado y no se activa para los clientes.
> 3. Los indicadores de riesgo personalizados existentes que utilicen los campos de datos (categoría, grupo, categoría y reputación de las URL) y sus directivas asociadas ya no se activan.

Para obtener más información sobre la retirada en Secure Private Access, consulte Funciones retiradas.

### Seleccione la fuente de datos de acceso privado seguro

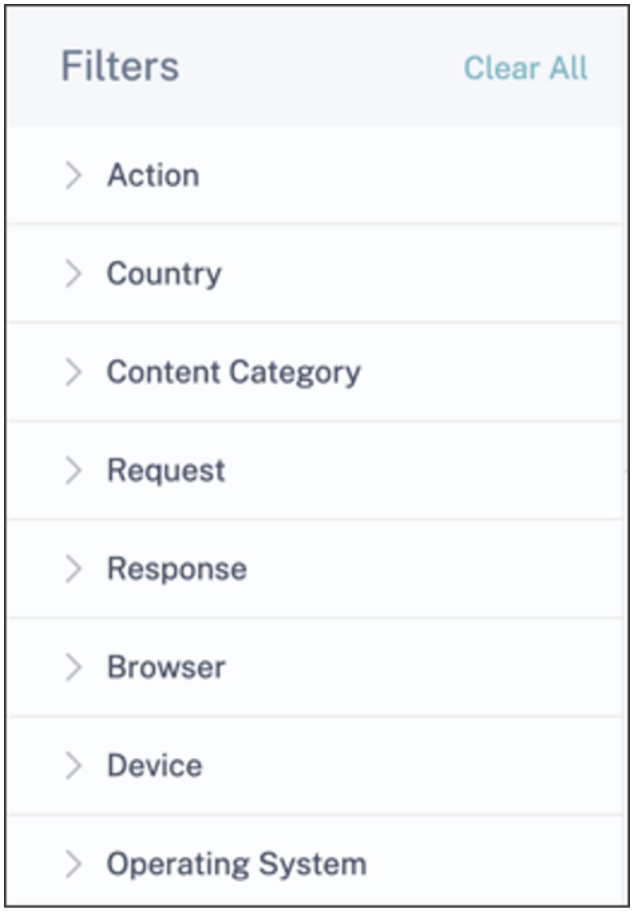
Para ver los eventos de acceso privado seguro, seleccione **Acceso privado seguro** en la lista. De forma predeterminada, la página de autoservicio muestra los eventos del último día. También puede seleccionar el período de tiempo para el que quiere ver los eventos.




### Seleccione las facetas para filtrar los eventos

Use las siguientes facetas que están asociadas a los eventos de acceso privado seguro.

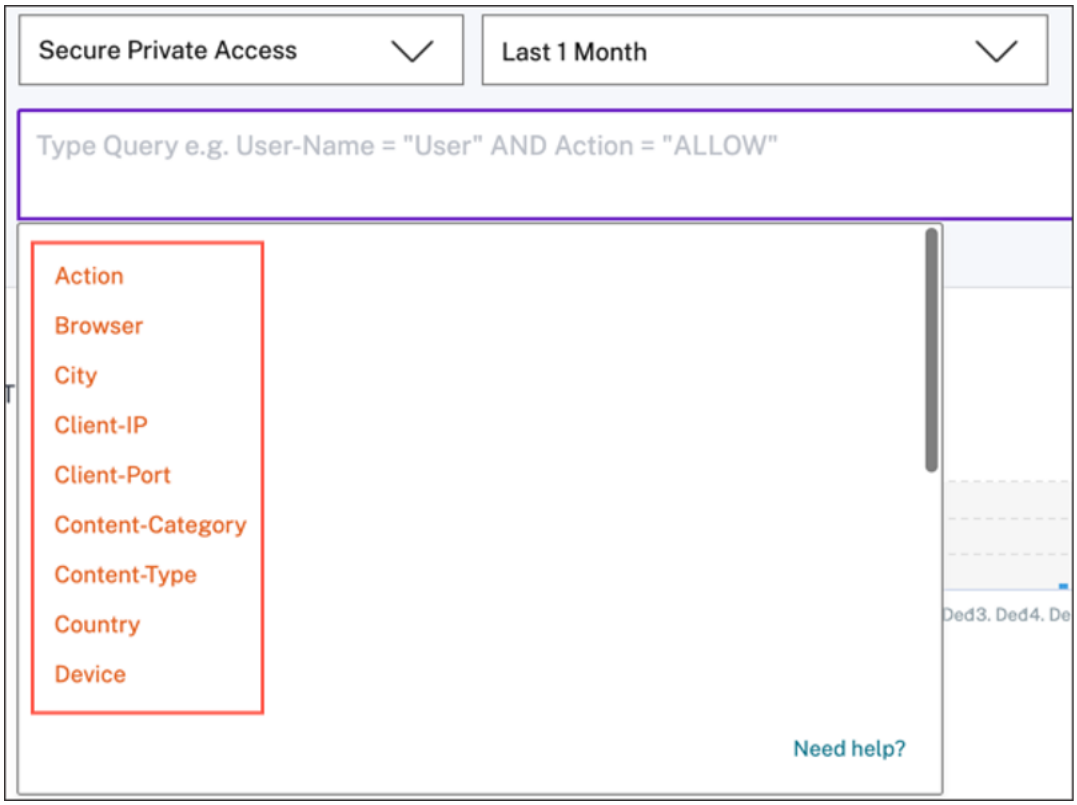


- **Acción**: busca eventos en función de las acciones realizadas en las aplicaciones de los usuarios, como permitir, bloquear y redirigir.
- **País**: Busca eventos en función de las ubicaciones de acceso de los usuarios.
- **Categoría de contenido**: busca eventos en función de las categorías de contenido a las que se accede, como aplicación, imagen y texto.
- **Solicitud**: busca eventos basados en los métodos HTTP como GET, POST, PUT, DELETE.
- **Respuesta**: busca eventos en función de la respuesta HTTP.
- **Explorador**: busca eventos en función de los exploradores utilizados por los usuarios.
- **Dispositivo**: busca eventos en función de los dispositivos utilizados, como teléfonos Android, iPhones, MacBook.
- **Sistema operativo**: Busque eventos basados en los sistemas operativos instalados en los dispositivos.

### Especificar consulta de búsqueda para filtrar eventos

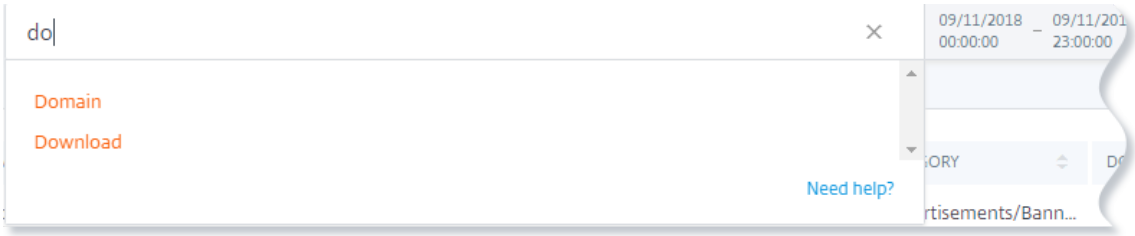
Coloque el cursor en el cuadro de búsqueda para ver la lista de dimensiones de los eventos de acceso privado seguro. Utilice las dimensiones y los operadores para especificar la consulta y buscar los eventos necesarios.



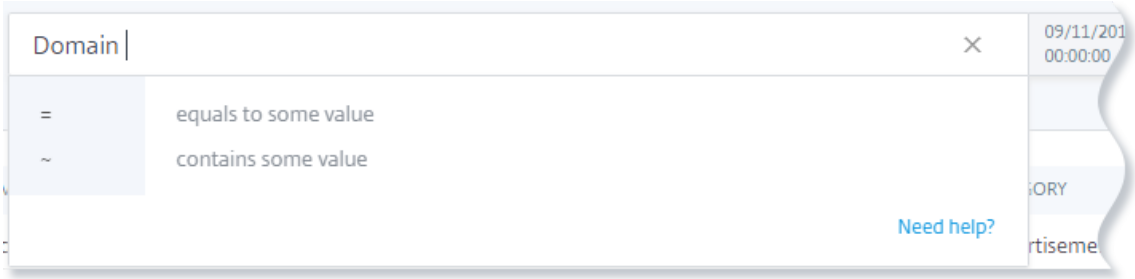

 

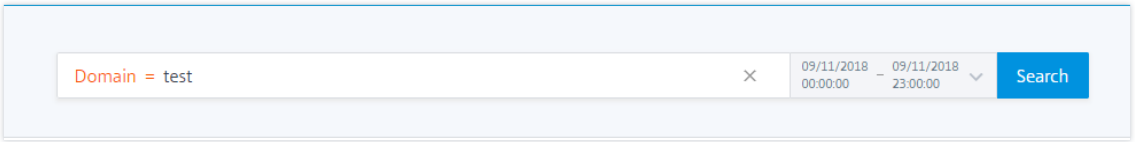
Por ejemplo, quiere ver los dominios de prueba en los que el volumen de descarga de datos supera los 2.000 bytes. Especifique la consulta de búsqueda de la siguiente manera:

1. Introduce “do”en el cuadro de búsqueda para obtener las sugerencias relacionadas.

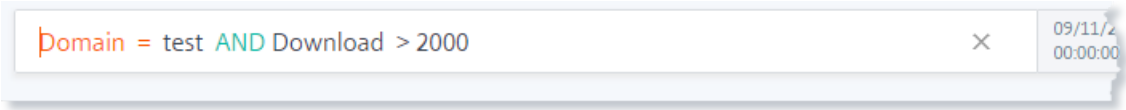



2. Haga clic en **Dominio** y, a continuación, especifique el valor “test”con el operador igual.




3. Utilice el operador **AND y**, a continuación, seleccione la dimensión **Descargar** . Seleccione el operador **>** e introduzca el volumen de descarga en bytes.




4. Seleccione el período de tiempo y haga clic en **Buscar** para ver los eventos en la tabla **DATA**.

## Búsqueda de autoservicio de aplicaciones y escritorios

February 12, 2024

Utilice la búsqueda automática para obtener información sobre los eventos de usuario recibidos de la fuente de datos Citrix Virtual Apps and Desktops y de la fuente de datos Citrix DaaS (anteriormente, el Citrix Virtual Apps and Desktops Service). Cuando los usuarios usan aplicaciones virtuales o escritorios virtuales, se generan eventos correspondientes a sus actividades y acciones. Ejemplos de eventos

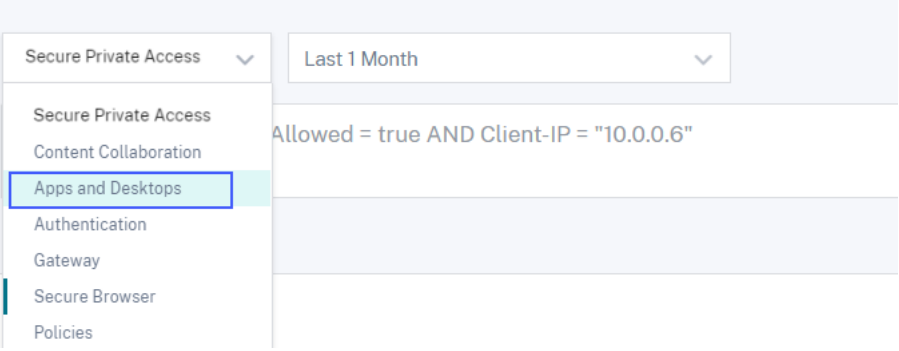
 

de usuario son la descarga de archivos, el inicio de sesión de la cuenta y el inicio de la aplicación. Citrix Analytics for Security recibe estos eventos de usuario y los muestra en la página de autoservicio. Puede hacer un seguimiento de los usuarios y sus actividades.

Para obtener más información sobre las funcionalidades de búsqueda, consulte **Búsqueda de autoservicio**.

### Seleccione la fuente de datos de Apps and Desktops

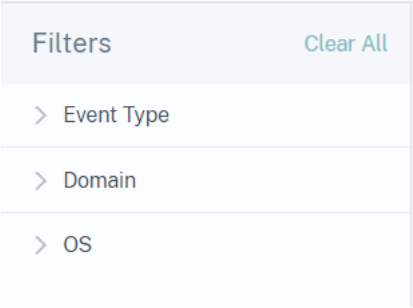
Para ver los eventos de Citrix Virtual Apps and Desktops o Citrix DaaS, seleccione **Aplicaciones y escritorios** de la lista. De forma predeterminada, la página de autoservicio muestra los eventos del último día. También puede seleccionar el período de tiempo para el que quiere ver los eventos.




De forma predeterminada, la página de autoservicio muestra los eventos del último mes. La página también proporciona varias facetas y un cuadro de búsqueda para filtrar y centrarse en los eventos necesarios.

### Seleccione las facetas para filtrar los eventos

Use las siguientes facetas que están asociadas a los eventos de Apps and Desktops.



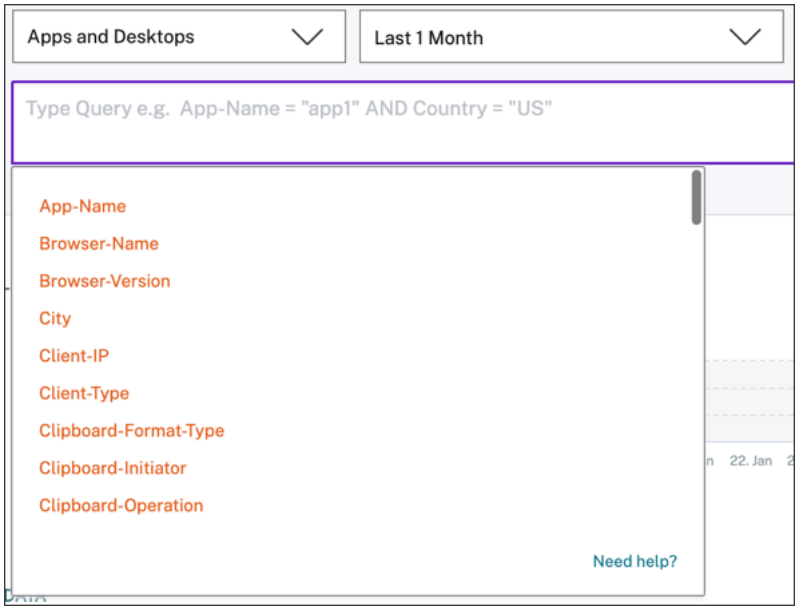

- **Tipo de evento**: Busca eventos según el tipo de evento, como el inicio de sesión de la cuenta, el cierre de la aplicación y el final de la sesión.
- **Dominio**: Busque eventos basados en dominios como citrate.net.

- **SO**: busca eventos basados en los sistemas operativos como Chrome, iOS y Windows utilizados en el dispositivo del usuario. Seleccione el nombre y las versiones del sistema operativo para filtrar los eventos. Para obtener más información sobre las versiones del sistema operativo, consulte Valores admitidos para la consulta de búsqueda.

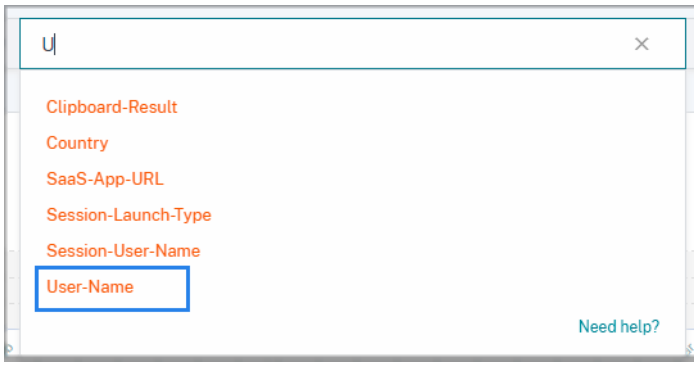
### Especificar consulta de búsqueda para filtrar eventos

Coloque el cursor en el cuadro de búsqueda para ver la lista de dimensiones de los eventos de Apps y escritorios. Utilice las dimensiones y los operadores para especificar la consulta y buscar los eventos necesarios.




Por ejemplo, quiere buscar eventos para el usuario “John Doe”que utiliza el sistema operativo Windows.

1. Introduce “U”en el cuadro de búsqueda para obtener las sugerencias relacionadas.




2. Haga clic en **Nombre de usuario** e introduzca el valor “John”con el operador igual.


3. Seleccione el operador **AND** y la dimensión del **nombre del SO**. Asigne el valor "Windows 7"con el operador igual.

```
User-Name = "John" AND OS-Name = "Windows 7"
```

4. Seleccione el período de tiempo y haga clic en **Buscar** para ver los eventos basados en la tabla **DATOS**.

## Tipos de eventos y campos compatibles

Los siguientes campos están disponibles para todos los tipos de eventos, excepto VDA.print:

- City
- Client IP
- País
- ID de dispositivo
- Nombre del sistema operativo
- Versión de SO
- Información adicional del sistema operativo
- Hora
- Nombre de usuario
- Versión de la aplicación Workspace
- Estado de la aplicación Workspace

En la siguiente tabla se describen los tipos de eventos disponibles para la fuente de datos de Apps and Desktops y los campos específicos de cada tipo de evento.

| Valor | Descripción | Campos |
| --- | --- | --- |
| `Account.Logon` | Se activa al iniciar sesión en Store a través de la aplicación Citrix Workspace. **Nota**: Account.Logon no está disponible para el cliente HTML5. | Compruebe los campos comunes tal y como se ha descrito anteriormente. |
| `Session.Logon` | Se activa cuando inicias sesión en tu sesión virtual. | Directivas de protección de aplicaciones, dominio, tipo de inicio de sesión, nombre de servidor de sesión, nombre de usuario de sesión |
| `Session.End` | Se activa al finalizar la sesión virtual. | Dominio, tipo de inicio de sesión, nombre de servidor de sesión, nombre de usuario de sesión |
| `App.Start` | Se activa al iniciar una sesión de aplicación virtual. **Nota**: Este tipo de evento no se aplica cuando la aplicación se inicia dentro de la sesión de escritorio. | Nombre de la aplicación, dominio, tipo de inicio de sesión, nombre del servidor de sesión, nombre de usuario de la sesión |
| `App.End` | Se activa al finalizar una sesión de aplicación virtual. **Nota**: Este tipo de evento no se aplica cuando la aplicación se inicia dentro de la sesión de escritorio. | Nombre de la aplicación, dominio, tipo de inicio de sesión, nombre del servidor de sesión, nombre de usuario de la sesión |

| Valor | Descripción | Campos |
| --- | --- | --- |
| `File.Download` | Se activa cuando un usuario copia un archivo de una sesión virtual remota al dispositivo cliente. No se activa cuando las transferencias de archivos se realizan dentro de las sesiones virtuales. **Nota**: Este tipo de evento solo se envía cuando el servidor permite la redirección de archivos (consulte la configuración de redireccionamiento de archivos para obtener más información) y la preferencia de **acceso a archivos** del espacio de trabajo del cliente está establecida en **Lectura y escritura**. | Dominio, tipo de dispositivo de descarga, nombre del archivo de descarga, ruta del archivo de descarga, tamaño del archivo de descarga, nombre del servidor de sesión, nombre de usuario de la sesión |

| Valor | Descripción | Campos |
| --- | --- | --- |
| `Printing` | Se activa al imprimir un archivo con la sesión iniciada por la aplicación Citrix Workspace a través de una impresora cliente. **Nota**: La aplicación Citrix Workspace tiene dos limitaciones técnicas que afectan a los eventos de impresión. En primer lugar, la telemetría del nombre del documento impreso no se incluye en el evento de impresión debido a un problema conocido en todas las variantes de la plataforma. En segundo lugar, la telemetría del tamaño del archivo impreso no se incluye en el evento de impresión para Windows debido a otra limitación técnica conocida. Para recopilar estos conjuntos de datos (nombre de archivo/tamaño de archivo), utilice el evento VDA.print. Para obtener más información, consulte Habilitar la telemetría de impresión para Citrix DaaS. | Nombre del navegador, versión del navegador, dominio, nombre de impresora, formato de archivo de impresión, tamaño del archivo de impresión, nombre del servidor de sesión, nombre de usuario de la sesión |
| `AppProtection.ScreenCapture` | Se activa cuando un usuario intenta capturar una captura de pantalla mientras se encuentra en una sesión protegida. **Nota**: Para obtener más información, consulte Protección de aplicaciones. | Títulos de aplicaciones protegidas, nombre de la herramienta de captura de pantalla, ruta de la herramienta de captura de pantalla |

| Valor | Descripción | Campos |
| --- | --- | --- |
| `App.SaaS.Launch` | Se activa cuando la aplicación Citrix Workspace inicia una aplicación SaaS en Citrix Enterprise Browser. | Nombre del navegador, versión del navegador, nombre de la aplicación SaaS, URL de la aplicación SaaS |
| `App.SaaS.End` | Se activa cuando la aplicación Citrix Workspace cierra una aplicación SaaS en Citrix Enterprise Browser. | Nombre del navegador, versión del navegador, URL de la aplicación SaaS |
| `App.SaaS.Clipboard` | Se activa cuando se realiza una operación de portapapeles en Citrix Enterprise Browser. | Nombre del navegador, versión del navegador, tamaño del formato de detalles del portapapeles, tipo de formato de detalles del portapapeles, iniciador de detalles del portapapeles, resultado de los detalles del portapapeles, funcionamiento del portapapeles, URL de la aplicación SaaS |
| `App.SaaS.File.Download` | Se activa cuando se descarga un archivo en Citrix Enterprise Browser. | Nombre del navegador, versión del navegador, tipo de dispositivo de descarga, ruta del archivo de descarga, tamaño del archivo de descarga |
| `App.SaaS.File.Print` | Se activa cuando se inicia la impresión en Citrix Enterprise Browser. | Nombre del navegador, versión del navegador, nombre del archivo de impresión, nombre de la aplicación SaaS, URL de la aplicación SaaS |
| `App.SaaS.Url.Navigate` | Se activa cuando Citrix Enterprise Browser navega por una URL. | Nombre del navegador, versión del navegador, nombre de la aplicación SaaS, URL de la aplicación SaaS |

| Valor | Descripción | Campos |
| --- | --- | --- |
| `Citrix.EventMonitor.AppStart` | Se activa cuando una aplicación agregada a la lista de monitoreo de aplicaciones del servidor de grabación de sesiones se inicia dentro de una sesión de escritorio virtual. | Nombre de la aplicación |
| `Citrix.EventMonitor.AppEnd` | Se activa cuando una aplicación agregada a la lista de monitoreo de aplicacionesdel servidor de grabación de sesiones se detiene dentro de una sesión de escritorio virtual. | Nombre de la aplicación |
| `Citrix.EventMonitor.Clipboard` | Se activa cuando se ha realizado una acción del portapapeles dentro de una grabación de sesión. | Tipo de formato de datos del portapapeles, nombre del proceso, título de la ventana |
| `Citrix.EventMonitor.FileTransfer` | Se activa cuando un usuario transfiere un archivo entre una sesión de escritorio virtual y la máquina del usuario. | Tamaño del archivo, dirección de operación (de host a cliente, de cliente a host), ruta de origen, ruta de destino |
| `Citrix.EventMonitor.RegistryChange` | Se activa cuando se realiza una operación de registro. Las posibles operaciones de registro son crear, eliminar, cambiar el nombre, establecer valor y eliminar valor. | Operación de registro, nombre de registro, ruta de registro, ID de proceso, ruta del archivo de proceso |
| `Citrix.EventMonitor.SessionEnd` | Se activa cuando finaliza la grabación de una sesión. | Descripción |
| `Citrix.EventMonitor.SessionLaunch` | Se activa cuando se inicia la grabación de una sesión. | Tipo de grabación de sesión |
| `Citrix.EventMonitor.TopMost` | Se activa cuando cambia la ventana superior. | Nombre de la aplicación |
| `Citrix.EventMonitor.IdleStart` | Se activa cuando la sesión queda inactiva. | Compruebe los campos comunes tal y como se ha descrito anteriormente. |

| Valor | Descripción | Campos |
| --- | --- | --- |
| `Citrix.EventMonitor.IdleEnd` | Se activa cuando finaliza la sesión inactiva. | Compruebe los campos comunes tal y como se ha descrito anteriormente. |
| `Citrix.EventMonitor.WebBrowsing` | Se activa cuando el usuario interactúa con las páginas web de los navegadores dentro de una sesión de escritorio virtual. | Nombre de la aplicación, URL |
| `Citrix.EventMonitor.FileCreate` | Se activa cuando se crea un archivo o una carpeta en una sesión de escritorio virtual dentro de la ruta del sistema de archivos supervisado. | Nombre de archivo, ruta de archivo, tamaño de archivo |
| `Citrix.EventMonitor.FileRename` | Se activa cuando se cambia el nombre de un archivo o una carpeta en una sesión de escritorio virtual dentro de la ruta del sistema de archivos supervisado. | Compruebe los campos comunes tal y como se ha descrito anteriormente. |
| `Citrix.EventMonitor.FileMove` | Se activa cuando un archivo o una carpeta de la ruta del sistema de archivos supervisado se mueve en una sesión de escritorio virtual o entre los hosts de sesión (VDA) y los dispositivos cliente. | Compruebe los campos comunes tal y como se ha descrito anteriormente. |
| `Citrix.EventMonitor.FileDelete` | Se activa cuando se elimina un archivo o una carpeta dentro de la ruta del sistema de archivos supervisado en una sesión de escritorio virtual. | Nombre de archivo, ruta de archivo, tamaño de archivo |
| `Citrix.EventMonitor.CDMUSBDriveAttach` | Se activa cuando se inserta un dispositivo de almacenamiento masivo USB mapeado por asignación de unidades de cliente (CDM) en un cliente desde el que se conecta la sesión virtual de aplicaciones y escritorio. | Compruebe los campos comunes tal y como se ha descrito anteriormente. |

| Valor | Descripción | Campos |
| --- | --- | --- |
| `Citrix.EventMonitor.GenericUSBDriveAttach` | Se activa cuando se inserta un dispositivo de almacenamiento masivo USB redirigido genérico en un cliente desde el que se conectan las aplicaciones virtuales y la sesión de escritorio. | Compruebe los campos comunes tal y como se ha descrito anteriormente. |
| `Citrix.EventMonitor.RDPConnection` | Se activa cuando un usuario crea una conexión de escritorio remoto en una máquina VDA. | IP de destino, ID de proceso |
| `Citrix.EventMonitor.UserAccountModification` | Activa todo tipo de operaciones con cuentas de usuario, como la creación, activación, inhabilitación, eliminación, cambios de nombre y modificación de contraseñas. | Descripción, nombre de usuario objetivo |
| `VDA.Print` | Se activa cuando se inicia un trabajo de impresión en Aplicaciones y escritorios. **Nota**: Este evento solo se aplica a la fuente de datos DaaS de Citrix. Para obtener más información, consulte Habilitar la telemetría de impresión para Citrix DaaS. | Nombre de usuario del documento, nombre de máquina, nombre del archivo de impresión, tamaño del archivo de impresión, nombre de la impresora, hora, número total de copias impresas, total de páginas impresas |
| `VDA.Clipboard` | Se activa cuando se realiza una operación de portapapeles en aplicaciones y escritorios. **Nota**: Este evento solo se aplica a la fuente de datos DaaS de Citrix. Para obtener más información, consulte Habilitar la telemetría del portapapeles para Citrix DaaS. | Tipo de formato de portapapeles, funcionamiento del portapapeles, dirección de funcionamiento del portapapeles, operación permitida del portapapeles, tamaño del portapapeles, nombre de máquina |

> **Nota**
>
> Todos los eventos de grabación de sesiones requieren que la política para registrar sus eventos esté habilitada en el servidor de grabación de sesiones. Para obtener más información, consulte Crear una directiva de detección de eventos personalizada.

### Valores admitidos para su consulta de búsqueda

Introduzca los siguientes valores para las dimensiones para definir la consulta de búsqueda.

| Dimensión | Valor | Tipo | Descripción |
|---|---|---|---|
| `App-Name` | Sesiones de aplicación o escritorio.<br><br>Ejemplos de sesiones de aplicación: Una sesión sin el nombre de la comunidad `#Cloud - Excel 2016` y una sesión con el nombre de la comunidad: `XA65PROD#Concur`<br>Ejemplos de sesiones de escritorio: Una sesión sin el nombre de la comunidad `#SINXIAP0616 $S1-1` y una sesión con el nombre de la comunidad: `XA65PROD# SINXIAP0616 $S1 -1` | Cadena | Nombre de una aplicación o escritorio iniciados. |
| `App-Protection-Policies` | Ejemplo:`AntiScreenCaptureEnabled` | Cadena | Directivas de protección de aplicaciones activas para la sesión. |

| Dimensión | Valor | Tipo | Descripción |
|---|---|---|---|
| `Browser-Name` | Ejemplo: Google Chrome, Citrix Enterprise Browser, Microsoft Edge, FIREFOX, SAFARI | Cadena | Nombre del explorador web |
| `Browser-Version` | Ejemplo: 80.0.3987.122, 101.0.9999.0 | Cadena | Versión del explorador web |
| `City` | Ejemplos: Santa Clara, Houston, Chicago | Cadena | Nombre de ciudad de un usuario. |
| `Client-IP` | Una dirección IP. Ejemplo: 10.10.10.10 | Cadena | Dirección IP del dispositivo de punto final del usuario. |
| `Client-Type` | Android, Windows, Macintosh, Chrome, HTML5, Unix/Linux, iOS, grabación de sesiones, monitor | Cadena | Indica los diferentes tipos de aplicaciones Citrix Workspace en función de los sistemas operativos o la fuente de datos original. |
| `Clipboard-Format-Type` | Ejemplos: texto, html, CF_UNICODETEXT | Cadena | Formato de datos copiado en el portapapeles. |
| `Clipboard-Initiator` | Ejemplos: teclado, menú contextual, javascript | Cadena | Indica cómo se ha iniciado la operación del portapapeles. **Nota**: Solo son compatibles con las aplicaciones SaaS. |

| Dimensión | Valor | Tipo | Descripción |
|---|---|---|---|
| `Clipboard-Operation` | Copiar, cortar, pegar o colocar | Cadena | Indica qué operación del portapapeles se realiza. **Nota**: La operación de **colocar** indica que los datos se están colocando en el portapapeles. Esto no garantiza que el cliente haya pegado o utilizado los datos del portapapeles. Esta operación solo se admite para el evento VDA.Clipboard. |
| `Clipboard-Operation-Direction` | De cliente a anfitrión, de anfitrión a cliente | Cadena | Indica la dirección del funcionamiento del portapapeles. **Nota**: Solo es compatible con el funcionamiento del portapapeles de Apps and Desktop (Citrix DaaS). |
| `Clipboard-Operation-Permitted` | Permitido o denegado | Cadena | Indica si la operación del portapapeles está permitida en Apps and Desktop Session. **Nota**: Solo es compatible con el funcionamiento del portapapeles de Apps and Desktop (Citrix DaaS). |
| `Clipboard-Result` | Éxito o bloqueado | Cadena | Indica el resultado de la operación del portapapeles. **Nota**: Solo son compatibles con las aplicaciones SaaS. |

| Dimensión | Valor | Tipo | Descripción |
|---|---|---|---|
| `Clipboard-Size` | Ejemplos: 10, 20 | Número | Tamaño de los datos (en bytes) almacenados actualmente en el portapapeles. |
| `Country` | Ejemplos: EE. UU., India | Cadena | Nombre del país de un usuario. |
| `Description` | **Para eventos `Citrix.EventMonitor.UserAccountModification`**: Se creó una cuenta de usuario, se habilitó una cuenta de usuario y se intentó restablecer la contraseña de una cuenta. | Cadena | Describe el estado de modificación de la cuenta de usuario, por ejemplo, si la cuenta se creó, se eliminó, se le cambió el nombre o se intentó restablecer la contraseña. |
| | **Para eventos `Citrix.EventMonitor.SessionEnd`**: Unknown, Logoff, Rollover, Trigger e Incomplete | | Describe el motivo del fin de la grabación de la sesión. |
| `Destination-IP` | Ejemplo: 10.60.110.xxx | Cadena | Dirección IP del escritorio remoto. |
| `Destination-Path` | Ejemplo: \H$\Desktop\Folder\ejemplo.txt | Cadena | La ruta final del archivo una vez finalizada la transferencia. |
| `Device-ID` | Ejemplo: cb781185-18ad-4f45-b75f | Cadena | Identificador de dispositivo utilizado para licencias, nombre de cliente o identificador de hardware del sistema operativo. |

| Dimensión | Valor | Tipo | Descripción |
| --- | --- | --- | --- |
| `Domain` | Ejemplo: example.com | Estructura | Nombre de dominio de un servidor que envió una solicitud. |
| `Download-Device-Type` | Ejemplos: descargas por USB, unidad de disco duro, unidad remota, crom o navegador. | Cadena | Tipo de dispositivo al que se descarga o transfiere el archivo. |
| `Download-File-Format` | Ejemplo: txt, PDF, xlsx, docx | Cadena | El formato del archivo descargado. |
| `Download-File-Name` | Ejemplo: example-file.txt | Cadena | Nombre del archivo descargado. |
| `Download-File-Path` | Ejemplo: C:\Users\admin\Desktop | Cadena | Ruta del archivo descargado. |
| `Download-File-Size` | Ejemplo: 8.05 | Número | Tamaño del archivo descargado en kilobytes. |

| Dimensión | Valor | Tipo | Descripción |
|---|---|---|---|
| Event-Type | Account.Logon, Session.Logon, Session.End, App.Start, App.End, File.Download, Printing, AppProtection.ScreenCapture, App.SaaS.Launch, App.SaaS.End, App.SaaS.Clipboard, App.SaaS.File.Download, App.SaaS.File.Print, App.SaaS.Url.Navigate, Citrix.EventMonitor.AppStart, Citrix.EventMonitor.AppEnd, Citrix.EventMonitor.TopMost, Citrix.EventMonitor.WebBrowsing, Citrix.EventMonitor.FileCreate, Citrix.EventMonitor.FileRename, Citrix.EventMonitor.FileMove, Citrix.EventMonitor.FileDelete, Citrix.EventMonitor.CDMUSBDriveAttach, Citrix.EventMonitor.GenericUSBDriveAttach, Citrix.EventMonitor.RDPConnection, Citrix.EventMonitor.UserAccountModification, VDA.Print, VDA.Clipboard, Citrix.EventMonitor.RegistryChange, Citrix.EventMonitor.SessionLaunch, Citrix.EventMonitor.SessionEnd, | Cadena | Para obtener más información, consulte Tipos de eventos y campos admitidos. |

| Dimensión | Valor | Tipo | Descripción |
|---|---|---|---|
| `Jail-Broken` | Sí o no | Cadena | Indica si el dispositivo está rooteado o no. **Nota**: Si esta dimensión está ausente, el dispositivo no está rooteado. Esta clave se aplica a la aplicación Citrix Workspace para dispositivos iOS y Android. |
| `Operation-Direction` | De host a cliente/de cliente a host | Cadena | Indica la dirección de la transferencia del archivo. |
| `OS-Extra-Info` | Ejemplo: 20G80, Service Pack 1, 19043 | Cadena | Indica la información adicional del sistema operativo, como los números de compilación, los service packs y los parches. |
| `OS-Name` | Ejemplo: macOS 11, Windows 7, Android 8.1, Windows 10 Enterprise | Cadena | Indica el nombre del sistema operativo. |
| `OS-Version` | Ejemplo: 11.5.1, 14.7.1, 2009 | Cadena | Indica la versión del sistema operativo |
| `Print-File-Format` | Ejemplos: PDF, PS, DOCX | Cadena | Formato del archivo impreso. |
| `Print-File-Name` | Ejemplo: example-file.pdf | Cadena | Nombre del archivo impreso. |
| `Print-File-Size` | Ejemplos: 10, 20 | Cadena | Tamaño del archivo impreso en bytes. |
| `Printer-Name` | Ejemplo: testprinter-1 | Cadena | Nombre de la impresora utilizada. |

| Dimensión | Valor | Tipo | Descripción |
|---|---|---|---|
| `Process-ID` | Ejemplo: 11248 | Cadena | Hace referencia al identificador del proceso que se utiliza para identificar el proceso específico que realiza dos acciones: **crear un proceso nuevo** y establecer **una conexión de escritorio remoto**. Actualmente, Process-ID solo está asociado al evento Citrix.EventMonitor.rdpConnection. |
| `Protected-App-Titles` | Ejemplo: Escritorio de administración - Citrix Workspace | Cadena | Nombre de la aplicación que se ejecuta en la sesión protegida. |
| `Registry-Name` | Nombre del registro modificado | Cadena | El nombre del registro que se modificó. |
| `Registry-Operation` | Cambiar nombre, crear, eliminar, setValue, DeleteValue | Cadena | Indica qué operación de registro se ha realizado. |
| `Registry-Path` | Ruta del registro modificado | Cadena | La ruta del registro que se modificó. |
| `SaaS-App-Name` | Ejemplo: Workday | Cadena | Nombre de la aplicación SaaS. |
| `SaaS-App-URL` | Ejemplo:`https://xyz.com\|String` | Cadena | URL de la aplicación SaaS o URL de gateway o proxy. **Nota**: La URL de gateway/proxy aparece en el evento app.saas.launch cuando la aplicación SaaS se inicia inicialmente. |

| Dimensión | Valor | Tipo | Descripción |
|---|---|---|---|
| Screen-Capture-Tool-Name | Ejemplo: ScreenShotTool.exe | Cadena | Nombre de la herramienta de captura de pantalla. |
| Screen-Capture-Tool-Path | Ejemplo: c:\Program files (x86)\ ScreenContent Client | Cadena | Ruta de la herramienta de captura de pantalla. |
| Session-Launch-Type | Aplicación o escritorio | Cadena | Indica si la sesión iniciada es de tipo aplicación o escritorio. |
| Session-Recording-Type | Grabación tradicional/Grabación solo de eventos | Cadena | Indica el tipo de grabación de la sesión iniciada. |
| Session-Server-Name | Ejemplos: escritorio hospedado, VDA-1 en la nube | Cadena | Nombre de la aplicación o el escritorio conectado como recibido de un servidor. |
| Session-User-Name | Ejemplos: usuario demo, usuario de prueba | Cadena | Nombre de usuario recibido del servidor. |
| Source-Path | Ejemplo: C:\Users\admin\Desktop\ejemplo.txt | Cadena | La ruta inicial del archivo antes de transferirlo. |
| Target-User-Name | Ejemplos: user01 | Cadena | Actualmente, el nombre de usuario de destino solo se usa para el evento Citrix.EventMonitor.UserAccountModif en el que se modificó la cuenta de usuario. |
| Total-Copies-Printed | Ejemplos: 1, 2 | Número | Número total de copias impresas por el usuario. |
| Total-Pages-Printed | Ejemplos: 1,2 | Número | Número total de páginas del documento impresas por el usuario. |

| Dimensión | Valor | Tipo | Descripción |
|---|---|---|---|
| `User-Name` | nombre de usuario o Dominio\ nombre de usuario | Cadena | El nombre de usuario o dominio\ nombre de usuario. Se utiliza para iniciar sesión en StoreFront Si el inicio de sesión de StoreFront no se realiza a través de la aplicación Citrix Workspace para HTML5 o Chrome, este valor es el mismo que el recibido del servidor. |
| `VDA-Name` | Ejemplo: TSVDA-19-01.xd.local | Cadena | Indica el nombre de la máquina VDA. |
| `Window-Title` | Ejemplo: Administrador - 01 Símbolo del sistema | Cadena | Indica el título de la ventana en la que se realizó la operación de portapapeles. |
| `Workspace-App-Version` | Ejemplo: 20.8.0.3 (2008) | Cadena | La aplicación Citrix Workspace o la versión de Citrix Receiver están instaladas en el dispositivo del usuario y se utilizan para iniciar aplicaciones virtuales remotas y sesiones de escritorio. |

| Dimensión | Valor | Tipo | Descripción |
| --- | --- | --- | --- |
| `Workspace-App-Status` | Compatible o no compatible | Cadena | Indica si Citrix Analytics for Security admite o no la versión instalada de la aplicación Citrix Workspace o Citrix Receiver en el dispositivo del usuario. Pase el mouse sobre **No compatible** cuando la aplicación Workspace no sea compatible. Aparece una ventana emergente con un enlace para ver la lista de versiones compatibles. Cuando una versión de la aplicación Workspace se acerca al estado de no compatible, aparece un encabezado en la página de búsqueda de autoservicio con una lista de las versiones compatibles disponibles a las que puede iniciar una actualización. |

**Formato de nomenclatura del sistema operativo**

Citrix Analytics recibe los detalles del sistema operativo (SO) de un dispositivo de usuario y los traduce en nombre del sistema operativo, versión del sistema operativo e información adicional del sistema operativo.

- **Nombre del sistema operativo** indica el nombre del sistema operativo.
- **Versión de SO** indica el ID de versión o la versión de lanzamiento del sistema operativo.
- **Información adicional del sistema operativo** indica la información adicional del sistema operativo, como números de compilación, service packs y parches.

En la tabla siguiente se proporcionan algunos ejemplos del formato de numeración de versiones de los sistemas operativos.

| Nombre del sistema operativo | Versión de SO | Información adicional del sistema operativo |
|---|---|---|
| macOS 11 | 11.5.1 | 20G80 |
| iOS 14 | 14.7.1 | No disponible |
| Windows 10 Enterprise | 2009 | 19043 |
| Windows 7 | 6.1 | Service Pack 1 |
| Android 8.1 | 8.1.0 | No disponible |

> **Notas**
>
> - Para obtener los detalles del sistema operativo de Mac versión 11.x o posterior, la versión de cliente recomendada es la aplicación Citrix Workspace para Mac 2108 o posterior.
> - Los detalles del sistema operativo de Windows 10 no están disponibles actualmente.

## Solución de problemas de seguridad y rendimiento de Citrix Analytics

December 7, 2023

En esta sección se explica cómo resolver los siguientes problemas que pueden surgir al utilizar Citrix Analytics for Security.

- Verificar a los usuarios anónimos como usuarios legítimos.
- Solucionar problemas de transmisión de eventos desde un origen de datos.
- Active eventos de Virtual Apps and Desktops, eventos SaaS y verificación de la transmisión de eventos a Citrix Analytics for Security.
- Elservidor de grabación de sesiones no se puede conectar.
- Problemas de configuración con el complemento Citrix Analytics para Splunk

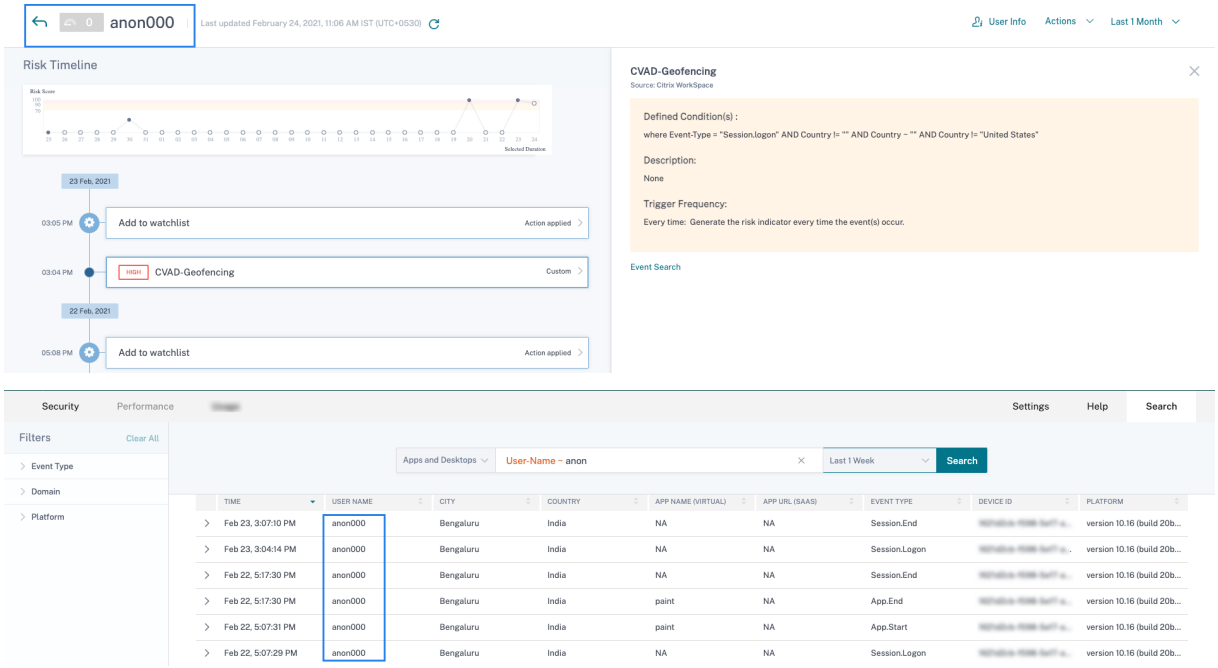
 

# Comprobar que los usuarios anónimos son usuarios legítimos

August 23, 2022

Como administrador, puede observar que algunos usuarios de Citrix Virtual Apps and Desktops y Citrix DaaS (anteriormente Citrix Virtual Apps and Desktops Service) se muestran como anónimos en Citrix Analytics for Security. Estos usuarios se identifican como usuarios descubiertos. Sin embargo, sus nombres de usuario aparecen como anonXYZ (donde "XYZ"representa un número de tres dígitos) en las siguientes páginas:

- Usuarios
- Cronología del usuario
- Usuarios con riesgos
- Búsqueda de autoservicio de la fuente de datos de Apps y escritorios




Cuando consulte a estos usuarios, es posible que quiera saber:

- ¿Quiénes son estos usuarios?
- ¿Son estos usuarios legítimos o de naturaleza maliciosa?
- ¿Cómo verificarlas?
- ¿Qué acciones debo aplicar para estos usuarios?

Puede ver usuarios anónimos en su entorno de TI de Citrix en los siguientes escenarios:

- Cuando un usuario utiliza una aplicación de explorador segura publicada
- Cuando un usuario utiliza un almacén no autenticado

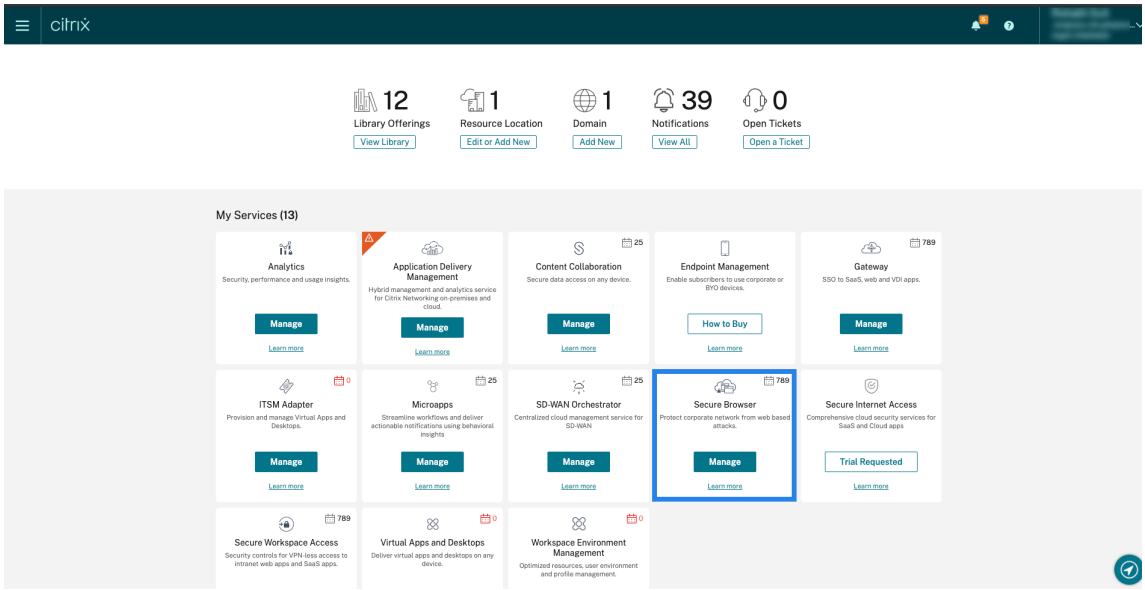
### Usuario que usa aplicaciones de explorador seguras publicadas

Las aplicaciones de explorador seguro son aplicaciones web que se publican mediante Citrix Secure Browser Service. Estas aplicaciones aíslan sus eventos de navegación web y protegen su red corporativa de los ataques basados en el explorador. Para obtener más información, consulte Secure Browser Service.

Las aplicaciones de explorador seguras utilizan la capacidad de sesión anónima de Citrix DaaS.

Para comprobar si Secure Browser está configurado en su cuenta de Citrix Cloud:

1. Inicie sesión en Citrix Cloud.
2. En la tarjeta **Secure Browser**, haga clic en **Administrar**.




3. En la página **Administrar**, compruebe si hay aplicaciones de explorador seguras publicadas.

Si un usuario accede a un almacén de StoreFront a través de sitios de Citrix Receiver para Web mediante un explorador web y utiliza las aplicaciones de explorador seguras publicadas, la identidad del usuario se oculta. Por lo tanto, Citrix Analytics muestra al usuario como anónimo.

Si un usuario accede a un almacén de StoreFront a través de una aplicación Citrix Receiver o Citrix Workspace que está instalada en su dispositivo y utiliza las aplicaciones de explorador seguras publicadas, Citrix Analytics muestra al usuario como el nombre de usuario especificado en StoreFront.

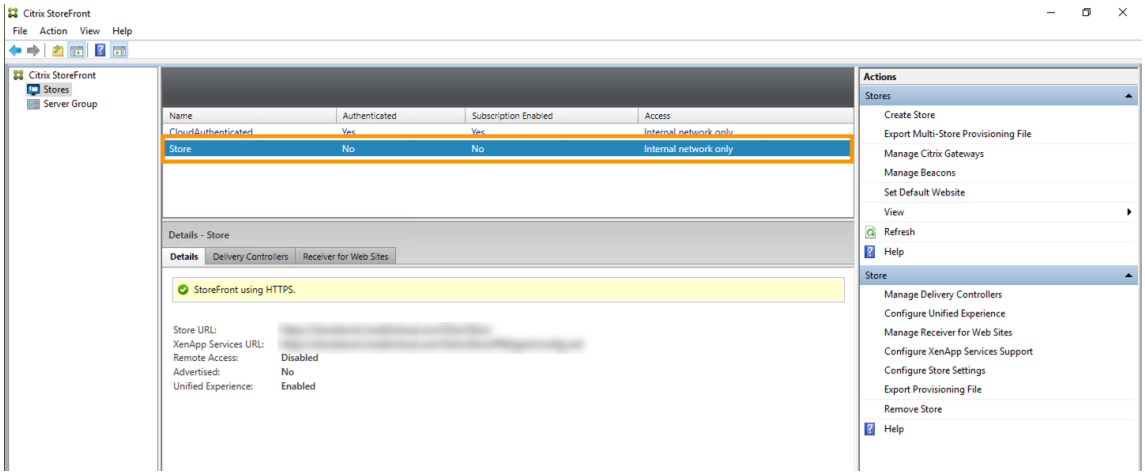
Por lo tanto, puede considerar al usuario como un usuario legítimo de su organización. No necesita aplicar ninguna acción si no se asocia ningún comportamiento de riesgo con el usuario.

### Usuario que usa un almacén no autenticado

El almacén no autenticado es una función de Citrix StoreFront y se aplica a los almacenes administrados por el cliente. Esta función admite el acceso de usuarios no autenticados (anónimos).

Para verificar si su organización tiene un almacén sin autenticar:

1. Abra Citrix Studio.
2. Haga clic en **Almacenes**.
3. Para sus almacenes, compruebe el estado de autenticación en la columna Autenticado.




Si un almacén no está autenticado y el usuario accede a ese almacén no autenticado, la identidad del usuario permanece anónima. Por lo tanto, Citrix Analytics muestra al usuario como anónimo. Puede considerar a este usuario como un usuario legítimo de su organización. No necesita aplicar ninguna acción si no se asocia ningún comportamiento de riesgo con el usuario.

# Solucionar problemas de transmisión de eventos desde un origen de datos

April 12, 2024

Esta sección le ayuda a solucionar problemas de transmisión de datos en Citrix Analytics for Security. Cuando una fuente de datos no transmite los eventos de los usuarios con precisión, puede encontrar problemas como la no detección de usuarios y los indicadores de riesgo.

## Lista de comprobación

| Secuencia | Cheques |
|---|---|
| 1 | ¿Tiene el derecho correcto para usar Security Analytics? |
| 2 | ¿La fuente de datos se admite en su región de origen? |
| 3 | ¿Su entorno cumple con todos los requisitos del sistema? |
| 4 | ¿Se detectan todas los orígenes de datos y se habilita el procesamiento de datos en Analytics? |
| 5 | ¿Las actividades de los usuarios en la fuente de datos transmiten eventos de forma precisa a Analytics? |
| 6 | ¿Los eventos de escritorios y aplicaciones virtuales se transmiten a Analytics? |
| 7 | ¿Los eventos de los usuarios aparecen en la página de búsqueda de autoservicio de Analytics? |
| 8 | ¿Analytics descubre a los usuarios? |

### Comprobación 1: ¿Tiene el derecho correcto para utilizar Security Analytics?

Citrix Analytics for Security es una oferta basada en suscripción. Para obtener más información, consulte Introducción.

### Comprobación 2: ¿se admite la fuente de datos en su región de origen?

Citrix Analytics for Security se admite en las siguientes regiones de origen:

- Estados Unidos (EE. UU.)
- Unión Europea (UE)
- Sur de Asia Pacífico (APS)

Según la ubicación de su organización, puede incorporarse a Citrix Cloud en una de las regiones de origen.

Sin embargo, ciertos orígenes de datos no se admiten en todas las regiones de origen. Los [orígenes de datos]((/en-us/security-analytics/data-sources.html) son los productos desde los que Citrix Analytics for Security recibe los eventos de los usuarios.

Si su organización se incorpora a Citrix Cloud en una región de origen donde no se admite una fuente de datos, no obtendrá eventos de usuario de la fuente de datos.

Use la siguiente tabla para ver los orígenes de datos y las regiones en las que se admiten.

| Origen de datos | Apoyado en la región de EE. UU. | Apoyado en la región de la UE | Se admite en la región APS |
|---|---|---|---|
| Citrix Endpoint Management | Sí | Sí | Sí |
| Citrix Gateway (local) | Sí | Sí | Sí |
| Proveedor de identidades Citrix | Sí | Sí | Sí |
| Citrix Secure Browser | Sí | Sí | Sí |
| Citrix Secure Private Access | Sí | No | No |
| Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service) | Sí | Sí | Sí |
| Citrix Virtual Apps and Desktops local | Sí | Sí | Sí |
| Microsoft Active Directory | Sí | Sí | Sí |
| Microsoft Graph Security | Sí | Sí | Sí |

### Comprobación 3: ¿Su entorno cumple con todos los requisitos del sistema?

Citrix Analytics puede tardar unos minutos en recibir los eventos de usuario de los orígenes de datos. Si no ve ningún evento de usuario en las tarjetas de sitio de origen de datos, asegúrese de que el entorno cumpla con los requisitos previos y los requisitos del sistema.

#### Requisitos previos

1. Todas sus suscripciones a Citrix Cloud deben estar activas. En la página de Citrix Cloud, asegúrese de que todos los servicios de Citrix Cloud estén activos.
2. Si usa local Citrix Virtual Apps and Desktops, debe agregar sus sitios a Citrix Workspace y configurar la agregación de sitios. Citrix Analytics descubre automáticamente los sitios agregados a Citrix Workspace. Para obtener más información, consulte Agregación de escritorios y aplicaciones virtuales locales en espacios de trabajo.
3. Si utiliza una implementación de StoreFront para sus sitios, configure los servidores de StoreFront para permitir que la aplicación Citrix Workspace envíe eventos de usuario a Citrix Analytics. Asegúrese de que la versión de StoreFront sea 1906 o posterior. Si no configura el servidor StoreFront, Citrix Analytics no recibe eventos de usuario de las instalaciones locales Citrix Virtual Apps and Desktops. Para configurar la implementación de StoreFront, consulte el artículo del servicio Citrix Analytics en la documentación de StoreFront.
4. Los usuarios de Citrix Virtual Apps and Desktops y Citrix DaaS los usuarios deben usar la versión especificada de las aplicaciones Citrix Workspace o Citrix Receiver en sus puntos finales. De lo contrario, Analytics no recibe los eventos del usuario de los puntos finales del usuario. La lista de versiones compatibles de la aplicación Citrix Workspace o Citrix Receiver está disponible en Citrix Virtual Apps and Desktops y en el origen de datos de Citrix DaaS.
5. Para recibir los eventos de los usuarios de una sesión de Secure Browser publicada, habilite la configuración de **seguimiento de nombres de host** en Secure Browser. De forma predeterminada, esta configuración está inhabilitada. Para obtener más información, consulte Administrar exploradores seguros publicados.
6. Incorpore sus orígenes de datos como se menciona en los siguientes artículos:
   - Origen de datos de Citrix Endpoint Management
   - Origen de datos de Citrix Gateway
   - Origen de datos de Citrix Secure Private Access
   - Origen de datos de Citrix Virtual Apps and Desktops y Citrix DaaS
   - Integración Microsoft Active Directory
   - Integración de Microsoft Graph Security

### Comprobación 4: ¿Se detectan todas los orígenes de datos y se habilita el procesamiento de datos en Analytics?

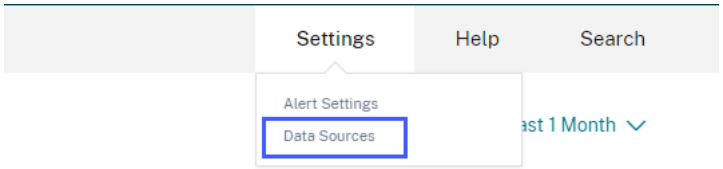
Asegúrese de que se descubran todos sus orígenes de datos y de que haya habilitado el procesamiento de datos para ellos. Si no habilita el procesamiento de datos para una fuente de datos, los usuarios que utilizan la fuente de datos no se detectan. Esta situación puede crear un riesgo potencial para la seguridad.

Habilitar el procesamiento de datos garantiza que Citrix Analytics procese los eventos de los usuarios. Los eventos se envían a Citrix Analytics solo cuando los usuarios utilizan activamente la fuente de datos.

> **Nota**
>
> Citrix Analytics no extrae datos de su entorno de forma activa.

**Para detectar sus orígenes de datos y habilitar el análisis, haga lo siguiente:**

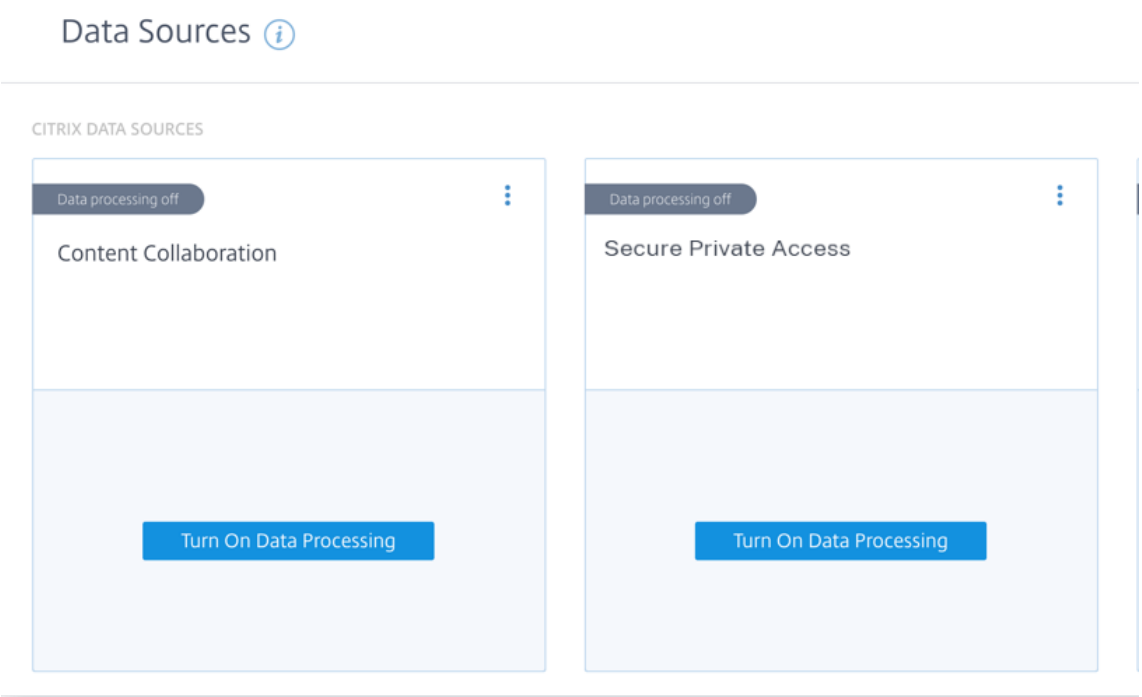
1. Haga clic en **Configuración** > **Orígenes de datos** > **Seguridad** para ver los orígenes de datos descubiertas. Citrix Analytics descubre automáticamente las fuentes de datos a las que se ha suscrito a su cuenta de Citrix Cloud.



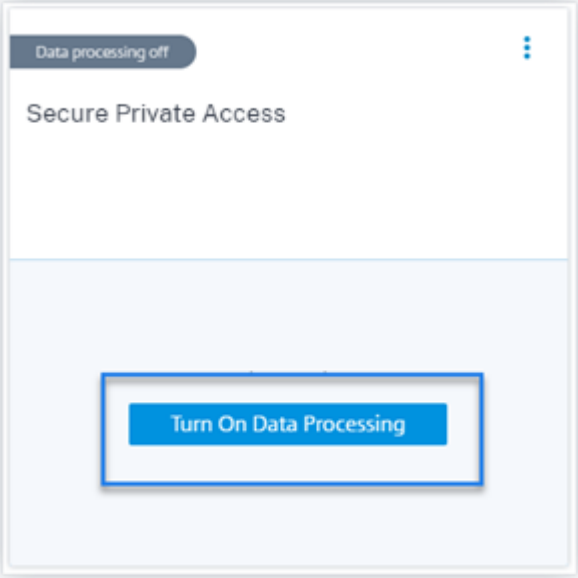

2. En la página **Orígenes de datos**, los orígenes de datos descubiertas aparecen como tarjetas de sitio. De forma predeterminada, el procesamiento de datos está desactivado.

> **Importante**
>
> Citrix Analytics procesa sus datos después de haber dado su consentimiento.




3. Haga clic **en Activar procesamiento de datos** en la tarjeta del sitio para la que quiere que Citrix Analytics procese los eventos. Por ejemplo, en la tarjeta del sitio Citrix Secure Private Access, haga clic **en Activar procesamiento de datos**.




4. Después de activar el procesamiento de datos, Citrix Analytics procesa los eventos del origen de datos. El estado de la tarjeta del sitio cambia a Procesamiento de datos. Puede ver el número de usuarios y los eventos recibidos en función del período de tiempo seleccionado.


5. Para todas los orígenes de datos detectadas, siga los pasos especificados en Introducción para habilitar el análisis.

### Comprobación 5: ¿Las actividades de los usuarios en la fuente de datos transmiten eventos de forma precisa a Analytics?

Citrix Analytics recibe eventos de usuario de los orígenes de datos cuando los usuarios utilizan activamente los orígenes de datos. Los usuarios deben realizar algunas actividades en la fuente de datos para generar eventos. Por ejemplo, para recibir eventos de la fuente de datos de Apps and Desktops, los usuarios de Apps and Desktops deben compartir, cargar o descargar algunos archivos.

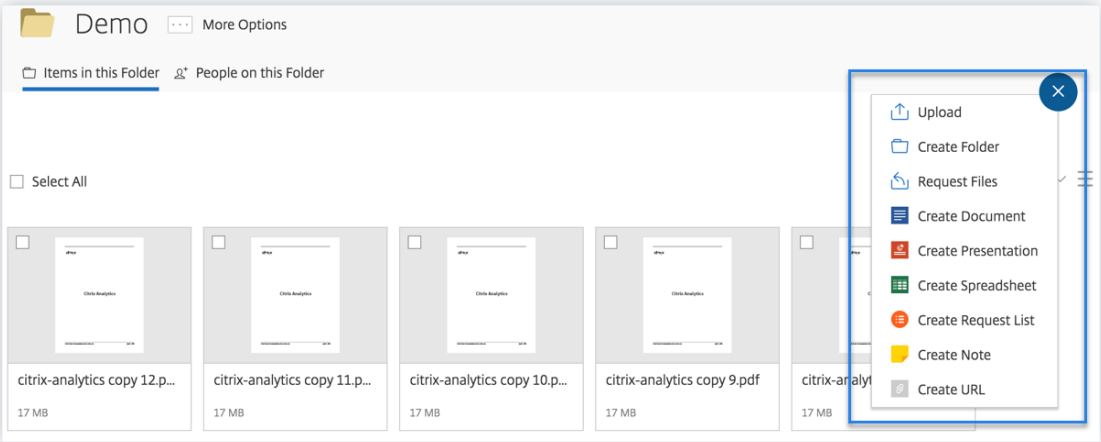
> **Nota**
>
> Citrix Analytics no extrae datos de su entorno de forma activa.

Si no ve ningún evento de usuario en Citrix Analytics para su fuente de datos, hay una alta probabilidad de que los usuarios no estén activos en ese momento.

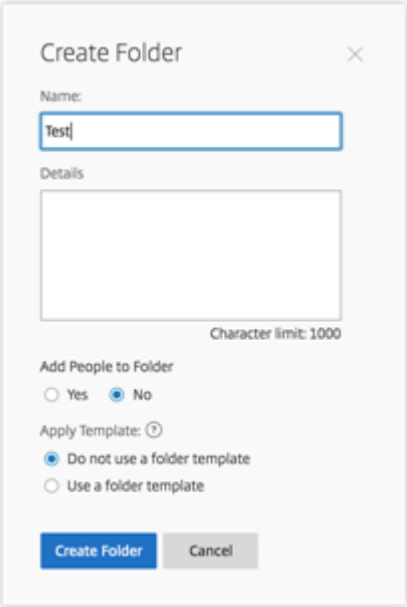
Para comprobar que Citrix Analytics recibe correctamente los eventos del usuario, lleve a cabo la siguiente actividad. Esta actividad utiliza la fuente de datos de Citrix Apps and Desktops. Puede realizar una actividad similar con otros productos Citrix (orígenes de datos) en función de su suscripción.

1. Inicie sesión en el servicio Citrix Apps and Desktops.
2. Realice algunas actividades habituales de usuario, como crear carpetas, descargar archivos, cargar archivos o eliminar archivos.

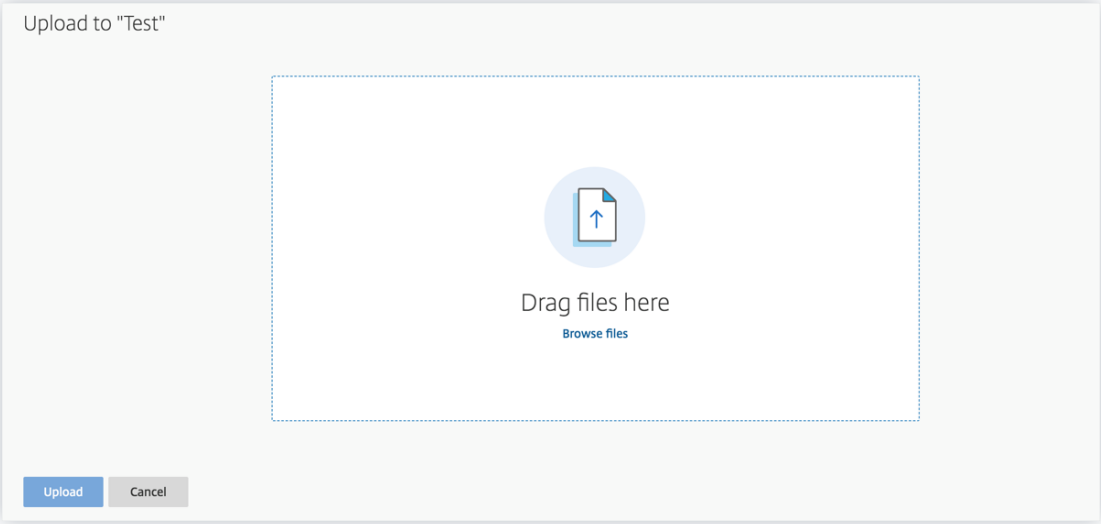



3. Por ejemplo, cree una carpeta de prueba.

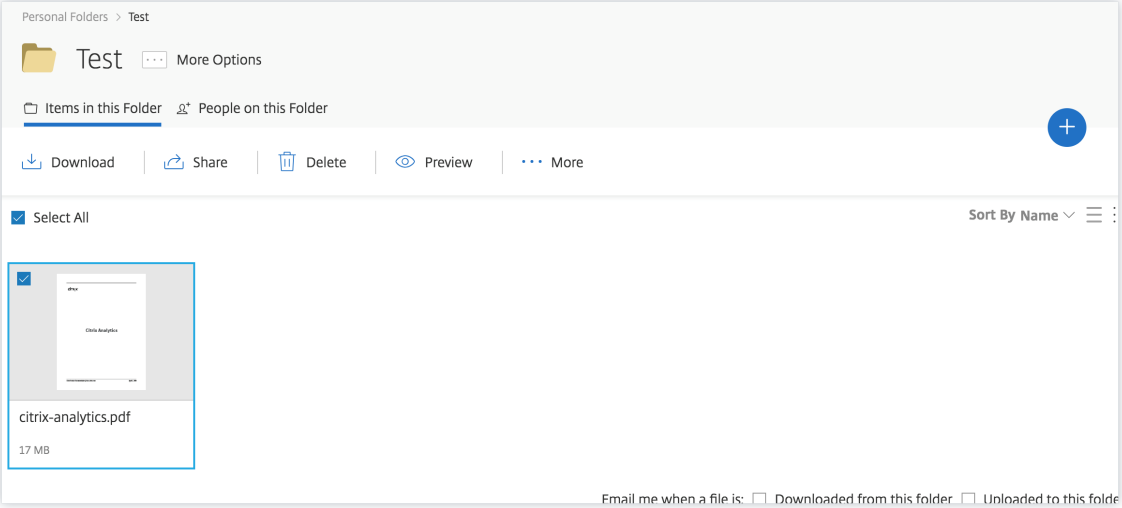



4. Sube algunos archivos locales.

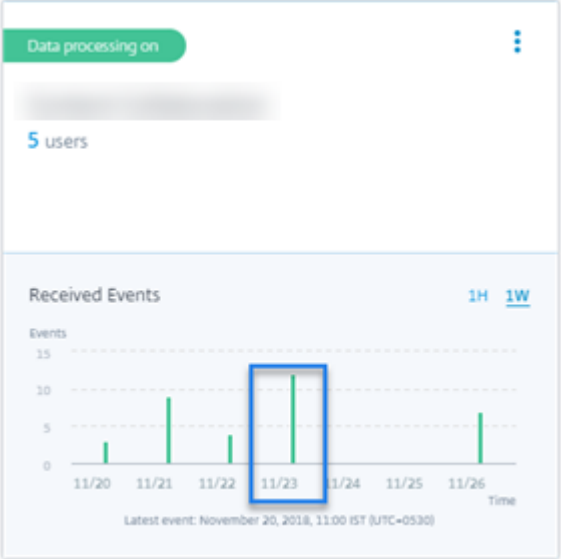



5. Elimina algunos archivos de la carpeta.




6. Vuelva a Citrix Analytics y consulte la tarjeta lateral de **Apps and Desktops** en la página Fuente de datos. Citrix Analytics recibe los eventos de usuario de la fuente de datos de Apps and Desktops y los muestra en la tarjeta del sitio.




### Comprobación 6: ¿se transmiten los eventos de escritorios y aplicaciones virtuales a Analytics?

Algunas versiones de la aplicación Citrix Workspace o del cliente Citrix Receiver no pueden enviar eventos de usuario a Citrix Analytics. Cuando los usuarios inician aplicaciones y escritorios virtuales a través de estos clientes, Citrix Analytics no detecta a los usuarios hasta que realizan los eventos compatibles.

Por ejemplo, la aplicación Citrix Workspace para Linux 2006 o posterior no envía los eventos de ***inicio de la aplicación SaaSy finalización de la aplicación SaaS*** a Citrix Analytics. Un usuario que lanza una aplicación SaaS mediante la aplicación Citrix Workspace para Linux no se detecta en Citrix Analytics.

#### Eventos admitidos

Consulte la siguiente tabla para comprobar los eventos de usuario admitidos por cada versión de cliente.

- **Sí**. El cliente envía el evento a Citrix Analytics.
- **No**: el cliente no envía el evento a Citrix Analytics.
- **NA**- El evento no es aplicable al cliente.

| Evento | Aplicación Workspace para Windows 1907 o posterior | Aplicación Workspace para Mac 1910.2 o una versión posterior | Aplicación Workspace para Linux 2006 o posterior | Aplicación Workspace para Android: la última versión disponible en Google Play | La última versión de la aplicación Workspace para iOS está disponible en Apple App Store | Aplicación Workspace para Chrome: la versión más reciente está disponible en Chrome Web Store | Aplicación Workspace para HTML5 2007 o posterior |
|---|---|---|---|---|---|---|---|
| Inicio de sesión de cuenta | Sí | Sí | Sí | Sí | Sí | No | No |
| Inicio de sesión | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| Inicio de sesiones | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| Fin de sesión | Sí | Sí | Sí | Sí | Sí | Sí | Sí |
| Inicio de aplicación | Sí | Sí | Sí | No | Sí | Sí | Sí |
| Cierre de aplicación | Sí | Sí | Sí | No | Sí | Sí | Sí |
| Descarga de archivos | Sí | Sí | Sí | No | No | Sí | Sí |
| Impresión | No | Sí | Sí | No | No | Sí | Sí |
| Lanzamiento de aplicaciones SaaS | Sí | Sí | No | No | No | No | No |

| Evento | Aplicación Workspace para Windows 1907 o posterior | Aplicación Workspace para Mac 1910.2 o una versión posterior | Aplicación Workspace para Linux 2006 o posterior | Aplicación Workspace para Android: la última versión disponible en Google Play | La última versión de la aplicación Workspace para iOS está disponible en Apple App Store | Aplicación Workspace para Chrome: la versión más reciente está disponible en Chrome Web Store | Aplicación Workspace para HTML5 2007 o posterior |
|---|---|---|---|---|---|---|---|
| Fin de la aplicación SaaS | Sí | Sí | No | No | No | No | No |
| Navegación URL de aplicaciones SaaS | Sí | Sí | No | No | No | No | No |
| Acceso al portapapeles de aplicaciones SaaS | Sí | Sí | No | No | No | No | No |
| Descarga de archivos de aplicaciones SaaS | Sí | Sí | No | No | No | No | No |

| Evento | Aplicación Workspace para Windows 1907 o posterior | Aplicación Workspace para Mac 1910.2 o una versión posterior | Aplicación Workspace para Linux 2006 o posterior | Aplicación Workspace para Android: la última versión disponible en Google Play | La última versión de la aplicación Workspace para iOS está disponible en Apple App Store | Aplicación Workspace para Chrome: la versión más reciente está disponible en Chrome Web Store | Aplicación Workspace para HTML5 2007 o posterior |
|---|---|---|---|---|---|---|---|
| Impresión de archivos de aplicaciones SaaS | Sí | Sí | No | No | No | No | No |

Según el estado de transmisión del evento, es posible que se produzcan los siguientes problemas:

- Cuando los usuarios se conectan a Citrix Virtual Apps and Desktops o Citrix DaaS con los clientes, es posible que no los descubran en Citrix Analytics hasta que realicen un evento (actividad) compatible. Por ejemplo, considere dos eventos de usuario: Inicio de aplicaciones e Inicio de aplicaciones SaaS. Un usuario que usa la aplicación Citrix Workspace para iOS, Citrix Analytics recibe el evento App Start pero no el evento SaaS App Launch. Por lo tanto, cuando el usuario inicia cualquier aplicación virtual, el evento Inicio de la aplicación se transmite a Citrix Analytics y se descubre al usuario. Sin embargo, si el usuario inicia una aplicación SaaS, Citrix Analytics no recibe el evento SaaS App Launch y no se descubre al usuario. Para obtener información sobre los usuarios detectados, consulte Usuarios descubiertos.
- Los eventos marcados como **No** en la tabla no aparecen en la página de búsqueda de autoservicio. Para obtener información sobre cómo utilizar la página de autoservicio, consulte Acerca de la búsqueda de autoservicio.

**Recomendación**

Para obtener los máximos beneficios de Analytics, Citrix recomienda lo siguiente:

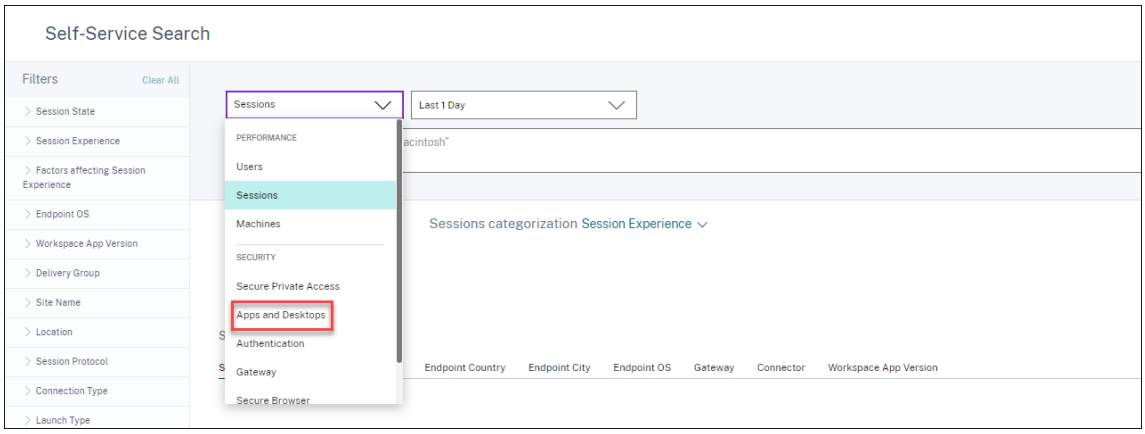
- **Usuario de Windows**: Conéctese a Citrix Virtual Apps and Desktops y Citrix DaaS con la aplicación Citrix Workspace para Windows 1907 o posterior.
- **Usuario de Mac**: Conéctese a su Citrix Virtual Apps and Desktops y Citrix DaaS mediante la aplicación Citrix Workspace para Mac 1910.2 o posterior.

### Comprobación 7: ¿Los eventos de los usuarios aparecen en la página de búsqueda de autoservicio de Analytics?

Realice esta comprobación final para asegurarse de que los eventos se transmiten con precisión a Citrix Analytics.

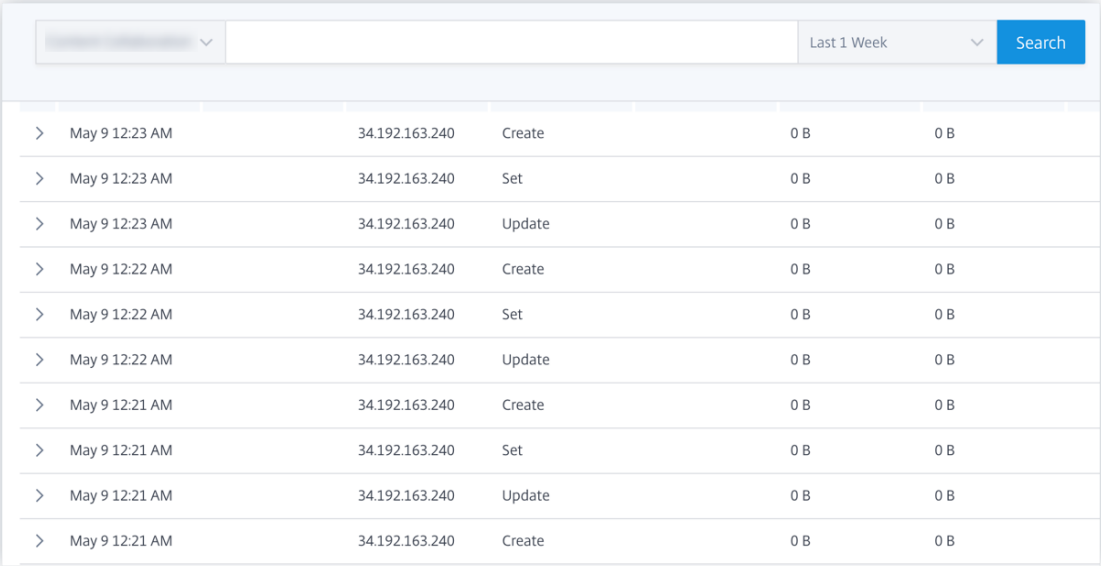
1. En la barra superior, haz clic en **Búsqueda avanzada** para ir a la página de búsqueda de autoservicio.


2. Seleccione la fuente de datos para ver la página de búsqueda correspondiente y los eventos.




3. Para ver los datos asociados a los eventos de Apps and Desktops, seleccione **Apps and Desktops** en la lista, seleccione el período de tiempo y, a continuación, haga clic en **Buscar**.




Para obtener más información, consulte Búsqueda de autoservicio.

### Comprobación 8: ¿Analytics descubre a los usuarios?

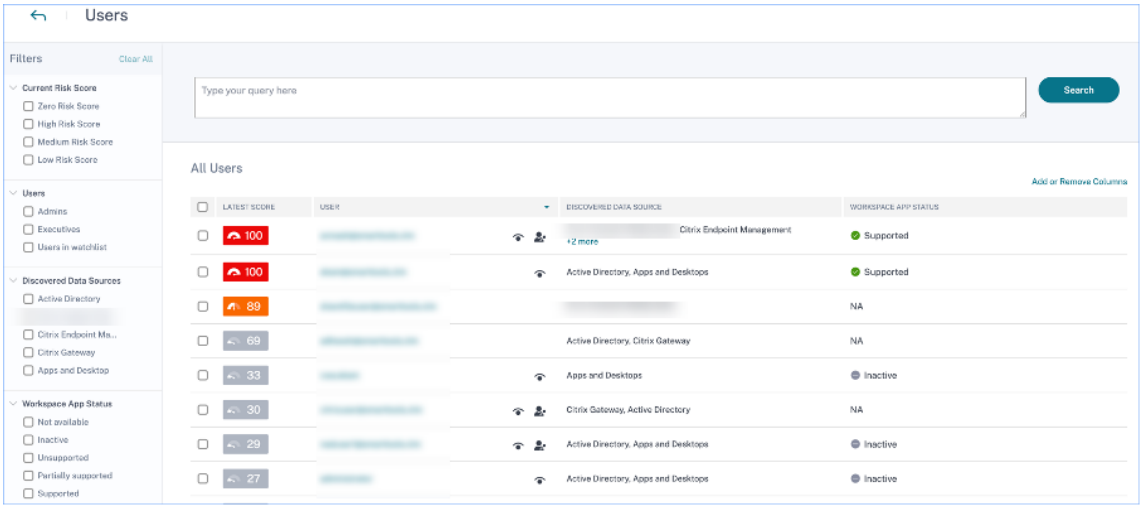
Cuando los eventos comienzan a fluir a Citrix Analytics, los usuarios que generan los eventos se detectan y se muestran en el panel **Usuarios**. Este proceso suele tardar unos minutos antes de que puedas verlos en el panel de control.

1. Haga clic en el enlace **Usuarios descubiertos** en el panel **Usuarios** para ver la lista completa de los usuarios detectados por Citrix Analytics.


2. La página **Usuarios** muestra la lista de todos los usuarios descubiertos en los últimos 31 días. Seleccione el período de tiempo para ver las ocurrencias del indicador de riesgo.

> **Nota:**
>
> Si intenta establecer un valor superior a 31 días, el sistema mostrará un mensaje de error que indica: **Intervalo de fechas no válido. El intervalo máximo permitido entre la fecha de inicio y la de finalización es de 31 días**.




Si los eventos se transmiten correctamente, el entorno de Citrix Analytics funciona según lo esperado. Los indicadores de riesgo se generan cuando se detectan anomalías.

## Desencadenar eventos de Virtual Apps and Desktops y SaaS, y verificar la transmisión de eventos

April 12, 2024

En esta sección se describen los procedimientos para activar eventos de aplicaciones y escritorios, eventos de SaaS, y para comprobar que Citrix Analytics for Security recibe estos eventos de usuario de forma activa.

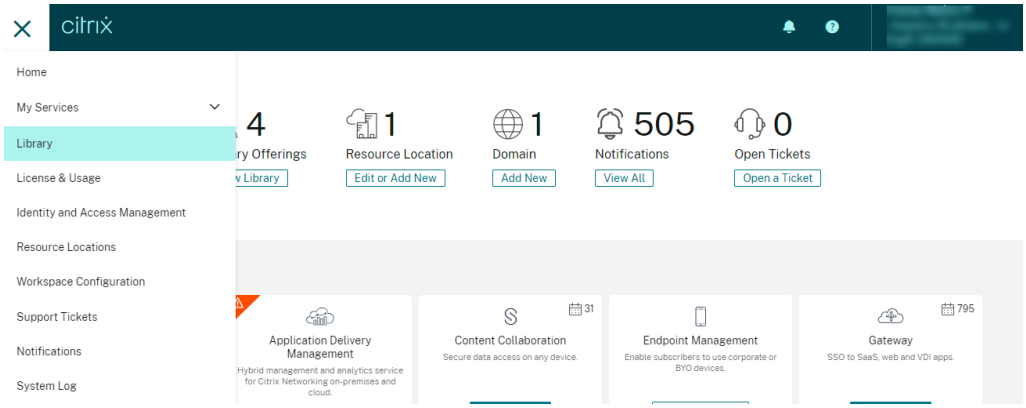
### Requisitos previos

- Si usa local Citrix Virtual Apps and Desktops, incorpore sus sitios locales en Citrix Analytics y habilite el procesamiento de datos desde la tarjeta del sitio. Si utiliza Citrix DaaS (anteriormente el Citrix Virtual Apps and Desktops Service), habilite el procesamiento de datos directamente desde la tarjeta del sitio. Para obtener más información, consulte Origen de datos de Citrix Virtual Apps and Desktops y Citrix DaaS.
- Use las versiones correctas de la aplicación Citrix Workspace o Citrix Receiver en los dispositivos de punto final de los usuarios para que los eventos se envíen con precisión a Citrix Analytics. Para obtener más información, consulte Origen de datos de Citrix Virtual Apps and Desktops y Citrix DaaS.
- Antes de desencadenar el evento de impresión desde el escritorio virtual, asegúrese de que una impresora esté configurada y aprovisionada en su entorno de aplicaciones y escritorios. Para

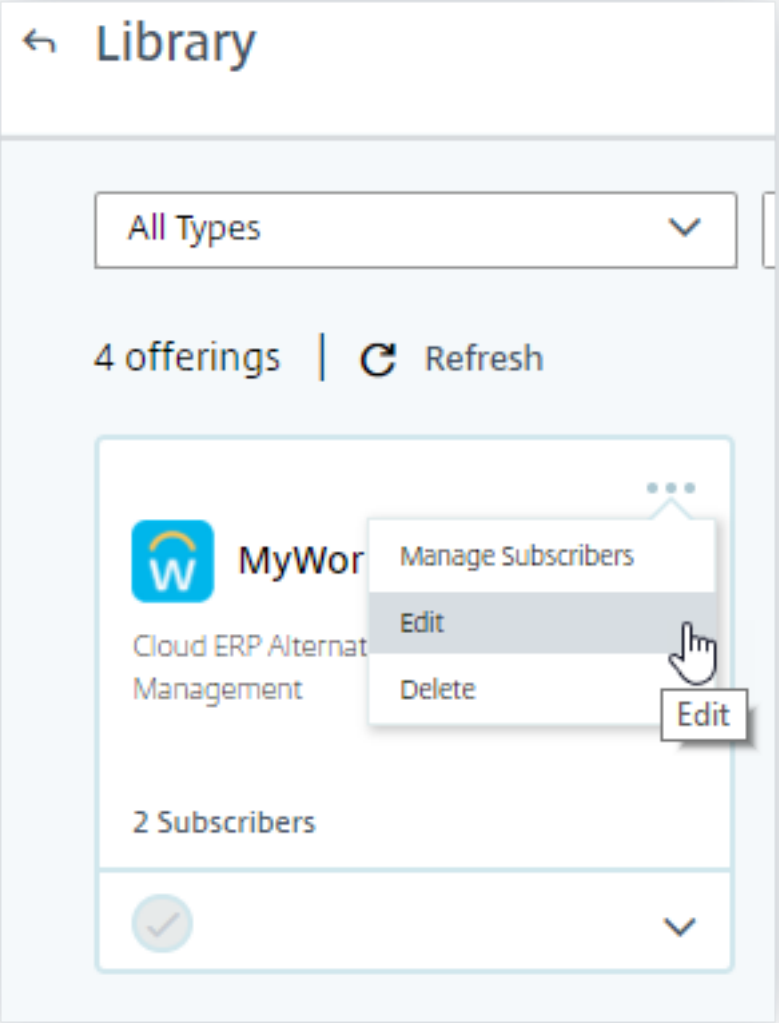
obtener más información sobre la administración de una impresora, consulte Imprimir.

- Para activar los eventos SaaS, como el lanzamiento de aplicaciones SaaS, la navegación URL de aplicaciones SaaS, la descarga de archivos de aplicaciones SaaS, debe usar una aplicación SaaS configurada desde Workspace. Las aplicaciones SaaS más utilizadas incluyen Salesforce, Workday, Concur y GoTo Meeting.
  - Si no hay aplicaciones SaaS configuradas, debe configurar y publicar una aplicación SaaS. Para obtener más información, consulte Compatibilidad con aplicaciones de software como servicio. Al configurar una aplicación SaaS, asegúrese de que las siguientes opciones de seguridad estén inhabilitadas:
    * Restringir acceso al portapapeles
    * Restringir impresión
    * Restringir navegación
    * Limitar la descarga
  - Si quiere utilizar una aplicación SaaS ya configurada desde su Workspace para desencadenar los eventos, asegúrese de que las opciones de seguridad mejoradas especificadas estén inhabilitadas para la aplicación SaaS:
    1. Vaya a su cuenta de Citrix Cloud y seleccione **Biblioteca**.

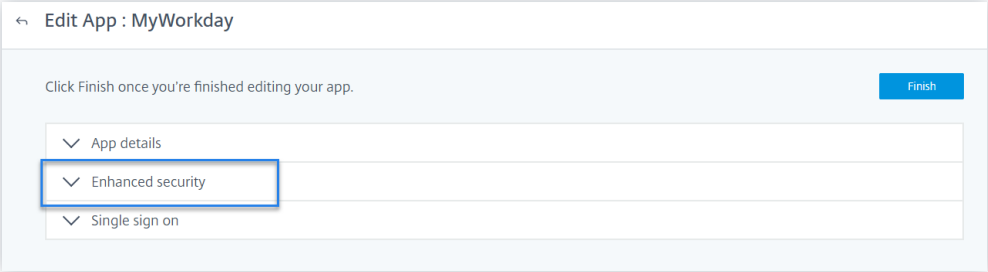



    2. En la página **Biblioteca**, identifique la aplicación SaaS que quiere usar para verificar los eventos. Por ejemplo, Workday.
    3. Haga clic en los puntos suspensivos y seleccione **Modificar**.

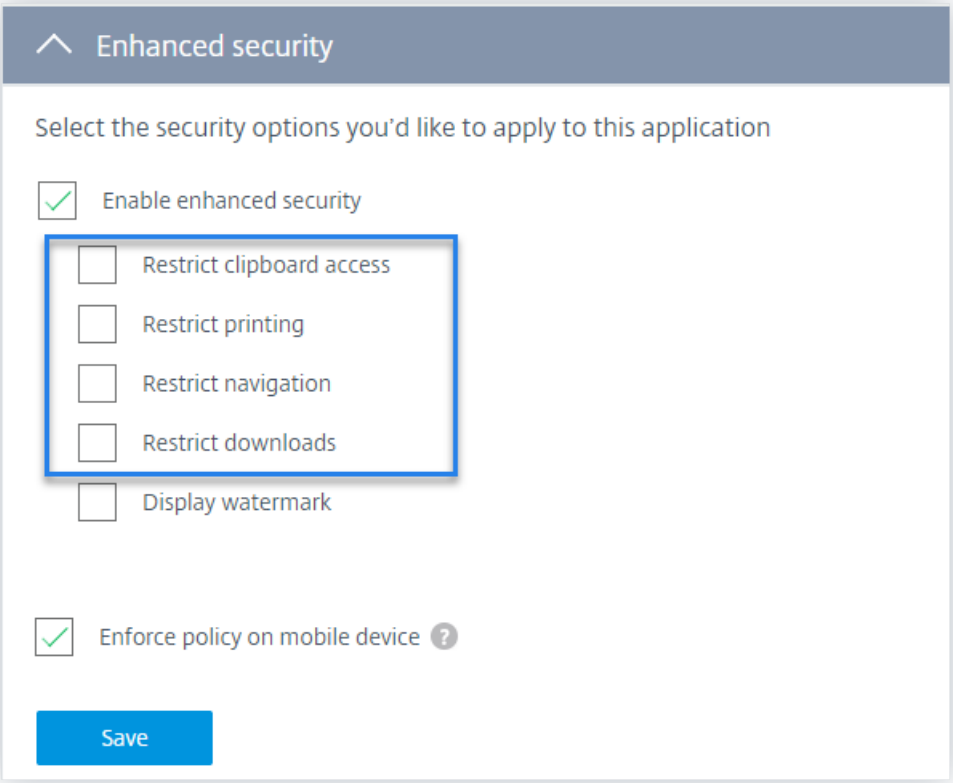



4. En la página **Modificar aplicación**, haga clic en la flecha hacia abajo para Seguridad mejorada.




5. Asegúrese de que las siguientes opciones de seguridad no estén seleccionadas.




## Problema conocido

Algunas versiones de la aplicación Citrix Workspace y Citrix Receiver no pueden enviar algunos eventos a Citrix Analytics. Por lo tanto, Citrix Analytics no puede proporcionar información ni generar indicadores de riesgo para estos eventos. Para obtener más información sobre el problema y su solución alternativa, consulte el problema conocido: CAS-16151.

## Procedimiento

Realice los siguientes pasos en secuencia para desencadenar los eventos en su entorno de Apps and Desktops y comprobar que Citrix Analytics for Security recibe estos eventos de forma activa.

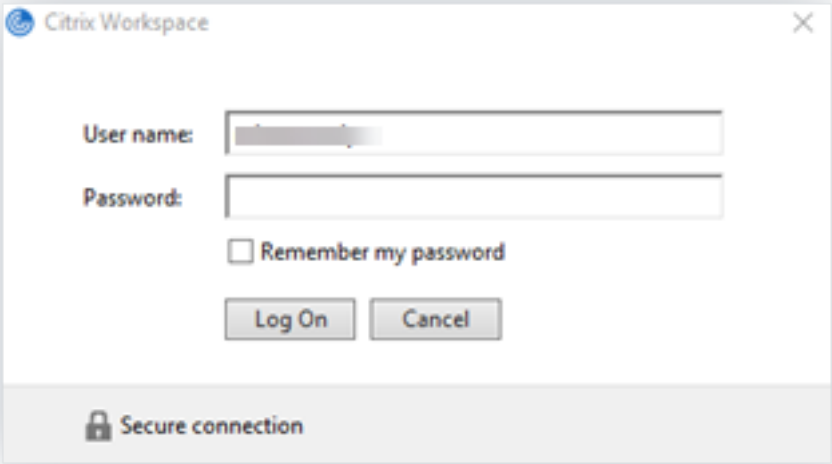
> **Nota**
>
> - Es posible que los eventos tarden algún tiempo en llegar a Citrix Analytics. Actualice la página de Citrix Analytics si no ve los eventos desencadenados.
> - Para desencadenar los eventos SaaS, este procedimiento utiliza la aplicación Workday como ejemplo. Puede usar cualquier aplicación SaaS configurada desde su Workspace

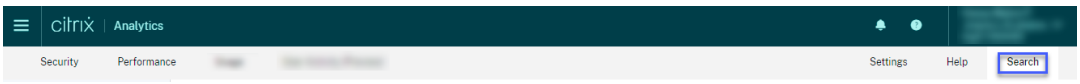
> para desencadenar los eventos SaaS.

- **Inicio de sesión de cuenta**

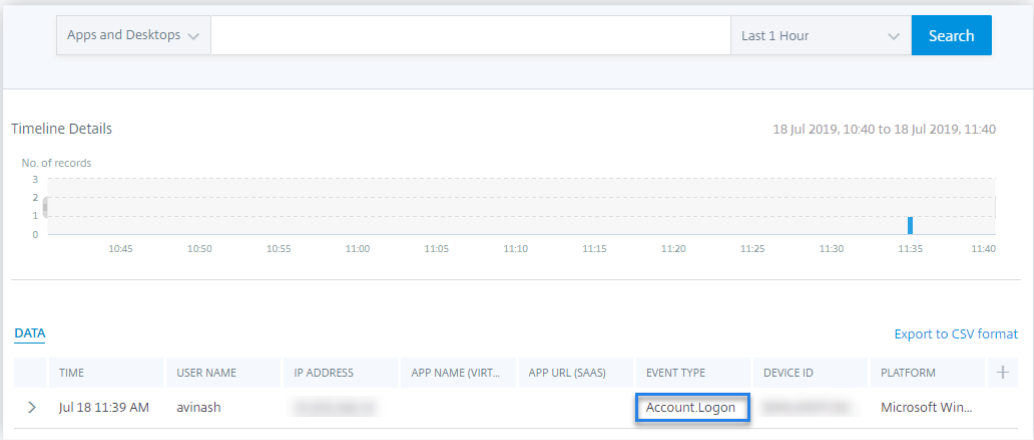
  1. Inicie la aplicación Citrix Workspace o Citrix Receiver para acceder a Workspace o StoreFront.
  2. Introduzca sus credenciales para iniciar sesión en la aplicación Citrix Workspace o en Citrix Receiver.




  3. Vaya a Citrix Analytics.
  4. Haga clic en **Buscar** y seleccione **Aplicaciones y escritorios** en la lista.



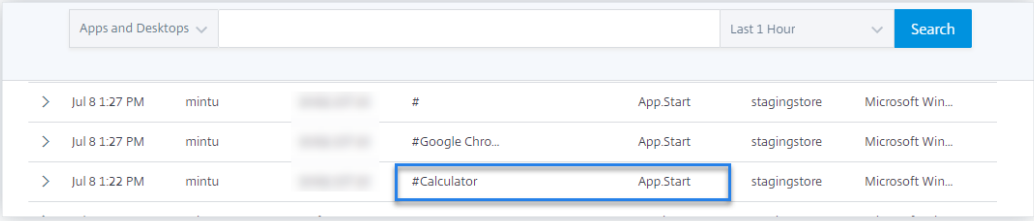

  5. En la página de búsqueda, consulte los datos del evento **Account.Logon**. Expanda la fila para ver los detalles del evento.



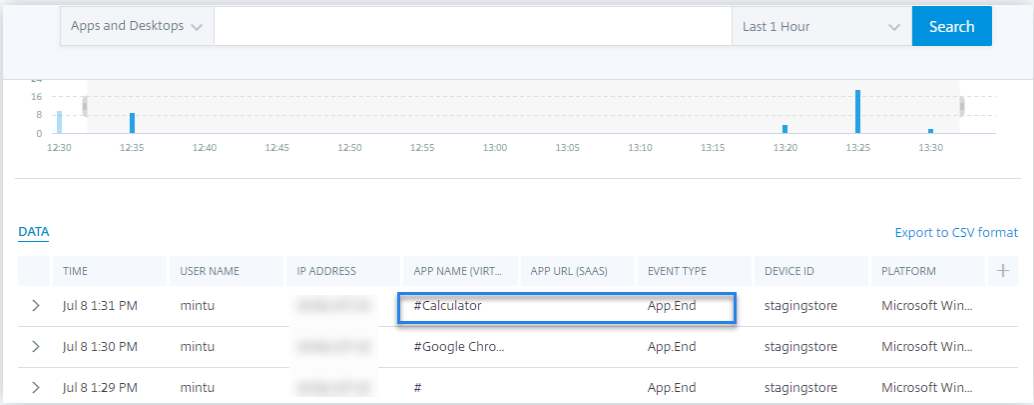
- **Inicio de aplicación**

  1. Inicie la aplicación Citrix Workspace o Citrix Receiver para acceder a Workspace o StoreFront.
  2. Inicie una aplicación como la calculadora.
  3. Vaya a Citrix Analytics.
  4. Haga clic en **Buscar** y seleccione **Aplicaciones y escritorios**.
  5. En la página de búsqueda, consulte los datos de los datos del evento **App.Start**. Expanda la fila para ver los detalles del evento.




- **Cierre de aplicación**

  1. Cierre la calculadora que ya ha lanzado en su Workspace o StoreFront.
  2. Vaya a Citrix Analytics.
  3. Haga clic en **Buscar** y seleccione **Aplicaciones y escritorios**.
  4. En la página de búsqueda, consulte los datos de los datos del evento **App.End**. Expanda la fila para ver los detalles del evento.

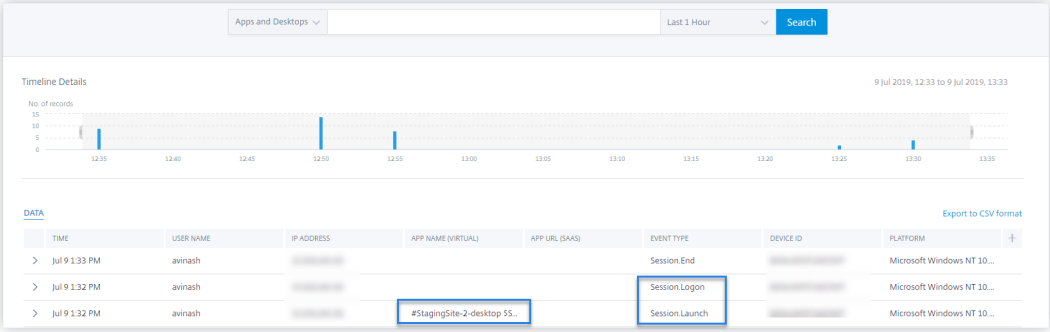



- **Inicio de sesión e inicio de sesión**

  1. Inicie la aplicación Citrix Workspace o Citrix Receiver para acceder a Workspace o StoreFront.

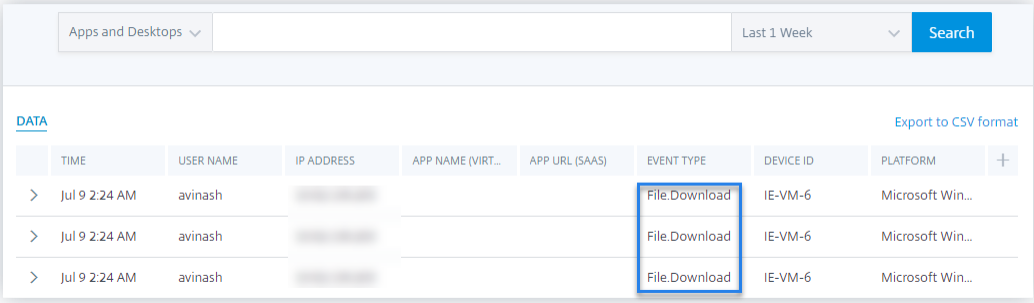
 

2. Inicie su escritorio virtual.
3. Vaya a Citrix Analytics.
4. Haga clic en **Buscar** y seleccione **Aplicaciones y escritorios**.
5. En la página de búsqueda, consulte los datos de los eventos **Session.Logon** y **Session.Launch**. Expanda la fila para ver los detalles del evento.




- **Descarga de archivos**

1. Inicie la aplicación Citrix Workspace o Citrix Receiver para acceder a Workspace o StoreFront.
2. Inicie su escritorio virtual.
3. Copie un archivo del escritorio virtual en el equipo local.
4. Vaya a Citrix Analytics.
5. Haga clic en **Buscar** y seleccione **Aplicaciones y escritorios**.
6. En la página de búsqueda, consulte los datos del evento **File.Download**. Expanda la fila para ver los detalles del evento.

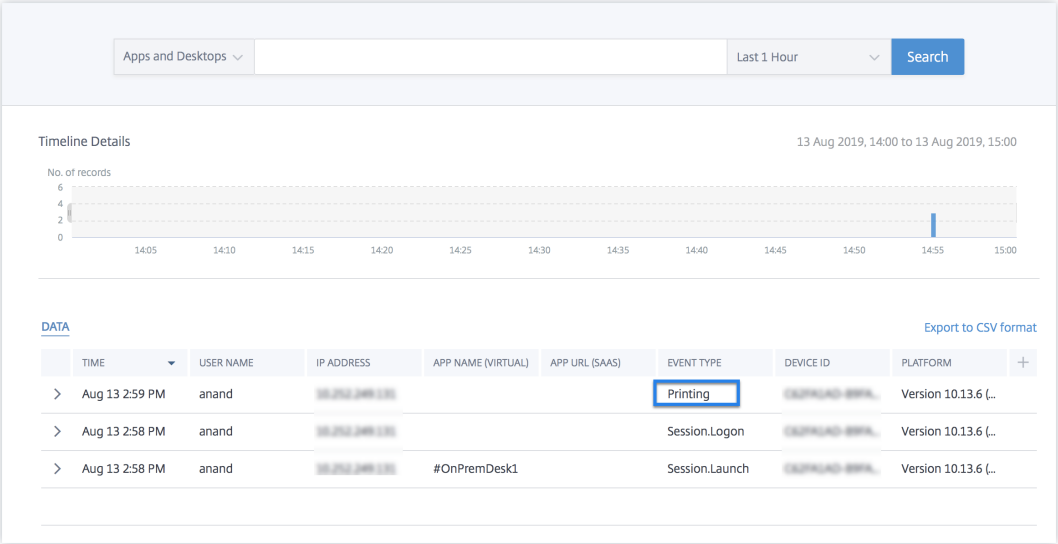



- **Impresión**

1. Inicie la aplicación Citrix Workspace o Citrix Receiver para acceder a Workspace.
2. Inicie su escritorio virtual.

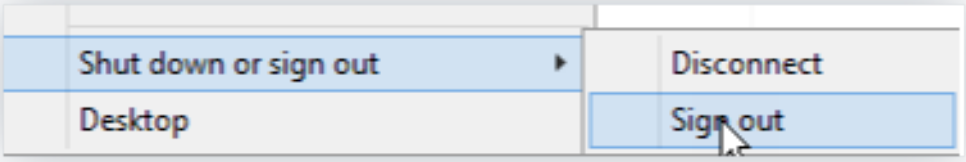
 

3. Imprima un documento con una impresora que esté configurada con su escritorio virtual.
4. Vaya a Citrix Analytics.
5. Haga clic en **Buscar** y seleccione **Aplicaciones y escritorios**.
6. En la página Buscar, consulte los datos del evento **Printing**. Expanda la fila para ver los detalles del evento.



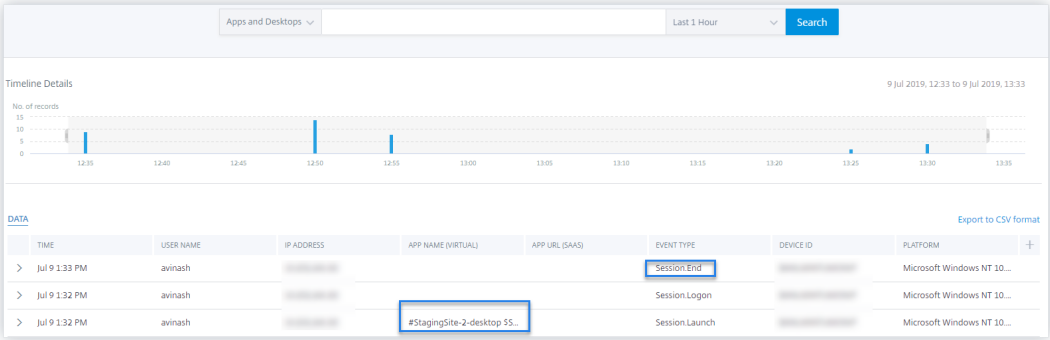

- **Fin de sesión**

1. Cierre sesión en su escritorio virtual. Por ejemplo, si usa un escritorio virtual de Windows, seleccione la opción **Cerrar sesión**.




2. Vaya a Citrix Analytics.
3. Haga clic en **Buscar** y seleccione **Aplicaciones y escritorios**.
4. En la página de búsqueda, consulte los datos del evento **Session.End**. Expanda la fila para ver los detalles del evento.

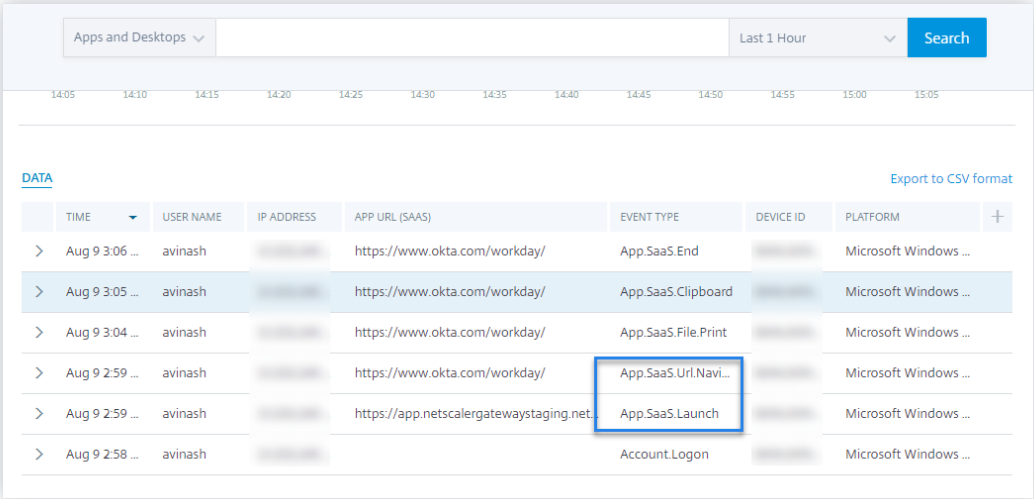



- **Lanzamiento de aplicaciones SaaS y navegación URL de aplicaciones SaaS**

  1. Inicie la aplicación Citrix Workspace o Citrix Receiver para acceder a Workspace o StoreFront.
  2. Inicie una aplicación SaaS como Workday y espere hasta que se cargue la página de Workday. Navegue por las páginas web de Workday.

     > **Nota**
     >
     > Asegúrese de que la opción **Restringir navegación** esté inhabilitada en la sección Seguridad mejorada. Para obtener más información, consulte **Requisitos previos**.

  3. Vaya a Citrix Analytics.
  4. Haga clic en **Buscar** y seleccione **Aplicaciones y escritorios**.
  5. En la página de **búsqueda**, consulte los datos de los eventos **App.SaaS.Launch** y **App.SaaS.URL.Navigation**. Expanda la fila para ver los detalles del evento.



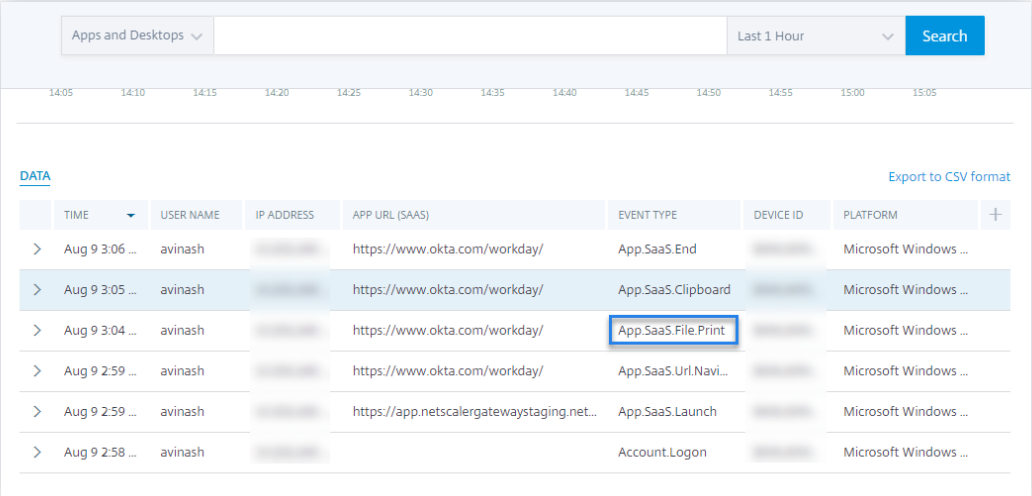

- **Impresión de archivos de aplicaciones SaaS**

  1. Imprima la página de Workday que está viendo actualmente.

> **Nota**
>
> Asegúrese de que la opción **Restringir impresión** esté inhabilitada en la sección Seguridad mejorada. Para obtener más información, consulte los **requisitos previos**.

2. Vaya a Citrix Analytics.
3. Haga clic en **Buscar** y seleccione **Aplicaciones y escritorios**.
4. En la página de búsqueda, consulte los datos del evento **App.SaaS.File.Print**. Expanda la fila para ver los detalles del evento.



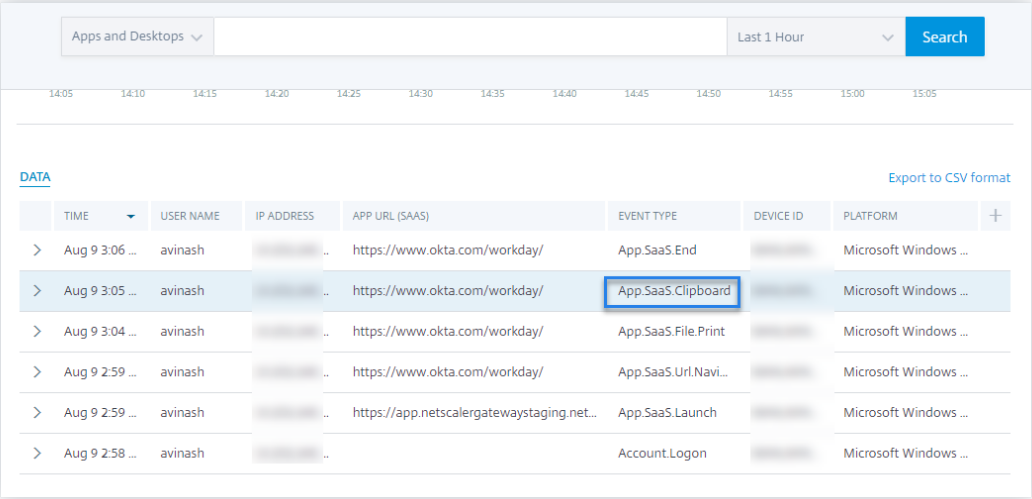

- **Acceso al portapapeles de aplicaciones SaaS**

1. En la página de Workday, copie texto en el portapapeles del sistema.

> **Nota**
>
> Asegúrese de que la opción **Restringir acceso al portapapeles** esté inhabilitada en la sección Seguridad mejorada. Para obtener más información, consulte los **requisitos previos**.

2. Vaya a Citrix Analytics.
3. Haga clic en **Buscar** y seleccione **Aplicaciones y escritorios**.
4. En la página de búsqueda, consulte los datos del evento **App.SaaS.Clipboard**. Expanda la fila para ver los detalles del evento.

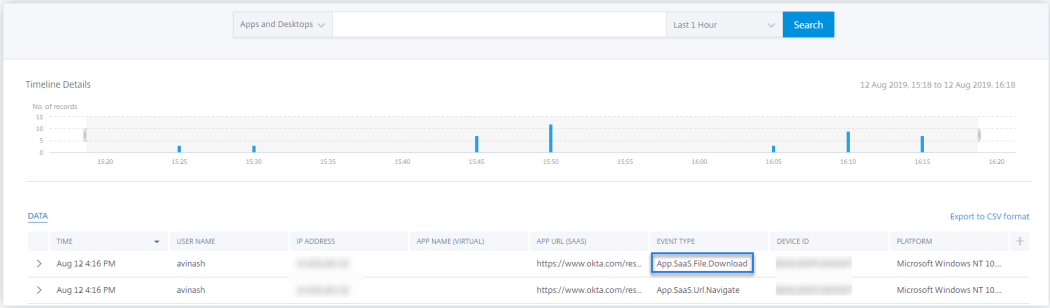



- **Descarga de archivos de aplicaciones SaaS**

  1. En la página Workday, busque un documento público, como un documento técnico, y descargue el documento.

     > **Nota**
     >
     > Asegúrese de que la opción **Restringir descargas** esté inhabilitada en la sección Seguridad mejorada. Para obtener más información, consulte los **requisitos previos**.

  2. Vaya a Citrix Analytics.
  3. Haga clic en Buscar y seleccione **Aplicaciones y escritorios**.
  4. En la página Buscar, consulte los datos del evento **App.SaaS.file.download**. Expanda la fila para ver los detalles del evento.

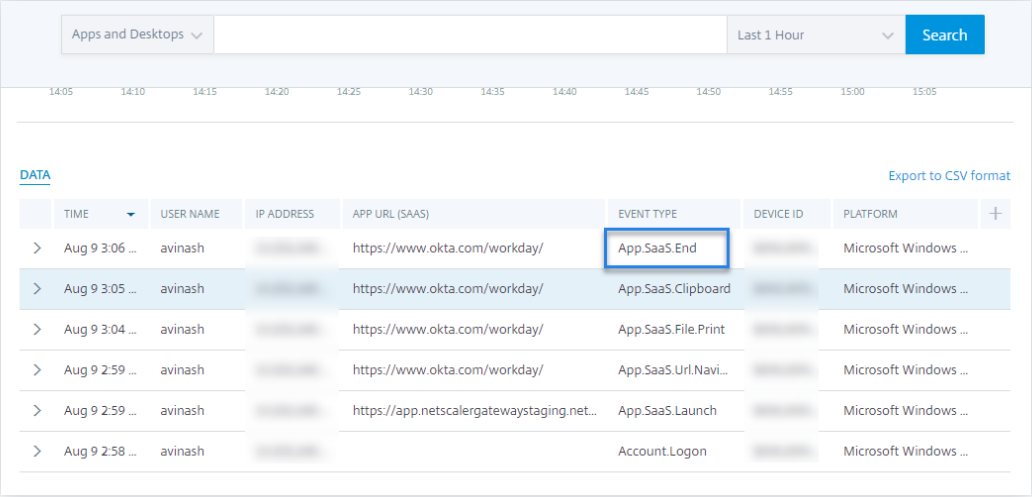



- **Fin de la aplicación SaaS**

  1. Cierre la página de Workday.
  2. Vaya a Citrix Analytics.
  3. Haga clic en **Buscar** y seleccione **Aplicaciones y escritorios**.

4. En la página de búsqueda, consulte los datos del evento **App.SaaS.End**. Expanda la fila para ver los detalles del evento.




- **VDA.Print**

  **Requisitos previos**

  Antes de desencadenar el evento de impresión, consulte Habilitar la telemetría de impresión para Citrix DaaS.

  Para activar un evento de impresión, realice las siguientes acciones:

  1. Abra un documento de texto con un bloc de notas o cualquier otra aplicación en la que se permita imprimir.
  2. Haga clic en **Archivo > Imprimir** o presione **Ctrl + P**.
  3. En Seleccionar impresora, elija su impresora, haga clic en **Aplicar** y, a continuación, imprima.

- **VDA.Clipboard**

  **Requisitos previos**

  Antes de activar el evento de impresión, consulte Habilitar la telemetría del portapapeles para Citrix DaaS.

  Para activar un evento de portapapeles, realice las siguientes acciones:

  1. Abra un documento de texto con un bloc de notas o cualquier editor de texto.
  2. Seleccione el contenido que quiere copiar.
  3. Haga clic con el botón secundario en copiar o presione Ctrl+C.

# No se han recibido eventos de usuario de la versión de la aplicación Citrix Workspace compatible

July 12, 2022

Si no ve ningún evento de un usuario que utiliza una versión de la aplicación Citrix Workspace admitida por Citrix Analytics, el problema podría estar en una de las siguientes situaciones:

- Configurar StoreFront
- Requisito de lanzamiento web

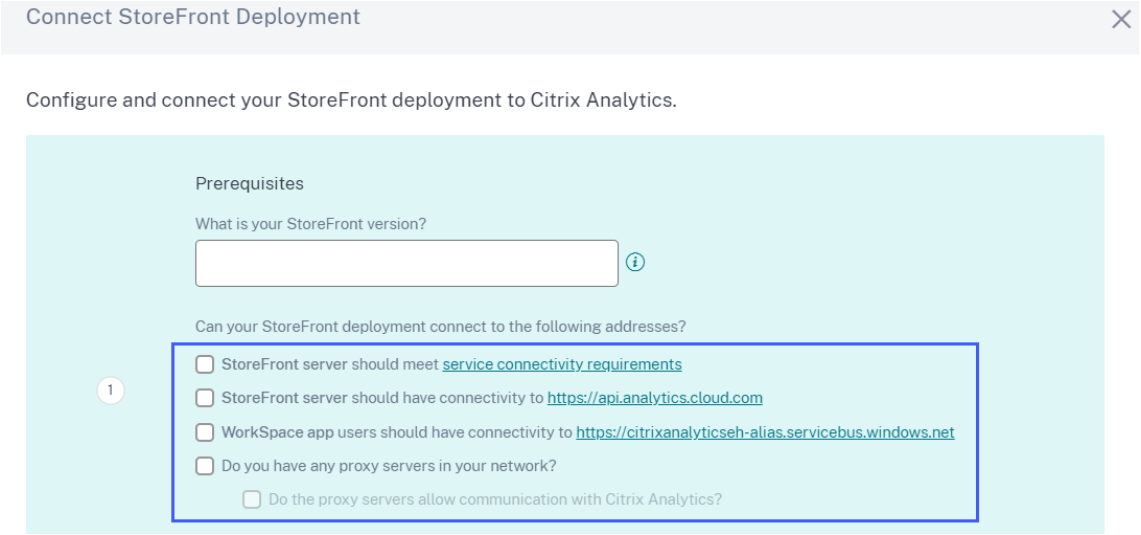
## Configurar StoreFront

Si una implementación de StoreFront está conectada a Citrix Analytics, compruebe la **marca de tiempo Última actualización**. La hora debe actualizarse al menos una vez a la semana si los usuarios acceden activamente a StoreFront. Las actualizaciones frecuentes indican una conexión correcta entre la implementación de StoreFront y Citrix Analytics. De lo contrario, hay algunos problemas de conectividad.

Compruebe los siguientes requisitos de conectividad:

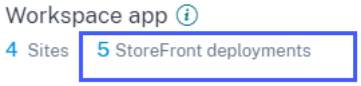
- El servidor StoreFront debe cumplir los requisitos del sistema y de conectividad.
- El servidor StoreFront debe poder conectarse a `https://api.analytics.cloud.com`
- Los usuarios de la aplicación Workspace deben poder conectarse a `https://citrixanalyticseh-alias.servicebus.windows.net`
- El servidor proxy debe permitir la conexión al concentrador de eventos de Citrix Analytics:
  - **Región de los Estados Unidos**: `https://citrixanalyticseh-alias.servicebus.windows.net/`
  - **Región de la Unión Europea**: `https://citrixanalyticseheu-alias.servicebus.windows.net/`
  - **Región Asia Pacífico Sur**: `https://citrixanalyticsehaps-alias.servicebus.windows.net/`

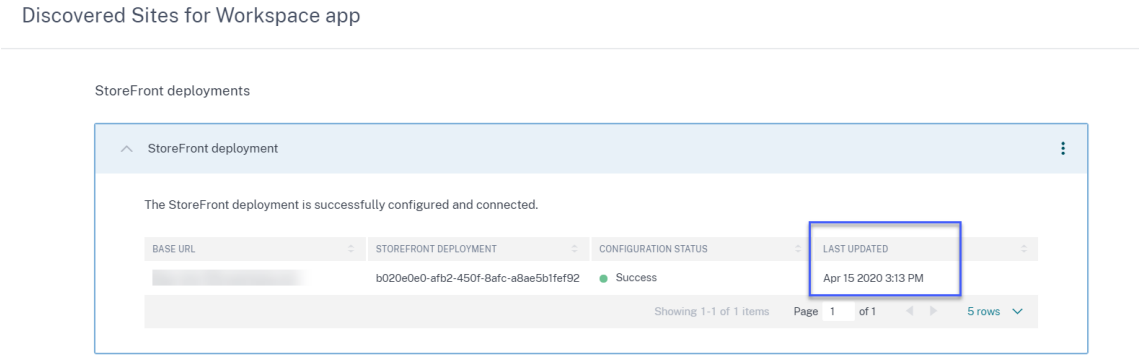



Para comprobar la hora de la última actualización:

1. Haga clic en **Configuración > Orígenes de datos**.
2. En la tarjeta del sitio de la aplicación Workspace, haga clic en el número de servidores StoreFront conectados.




3. En la implementación de StoreFront, compruebe la hora de la última actualización.




Si la última marca de tiempo actualizada no se actualiza con frecuencia incluso después de cumplir los requisitos de conectividad, vuelva a configurar StoreFront. Para obtener más información, consulte Incorporar sitios de Virtual Apps and Desktops mediante StoreFront.

### Requisito de lanzamiento web

Un usuario puede iniciar aplicaciones y escritorios virtuales de una de las siguientes formas:

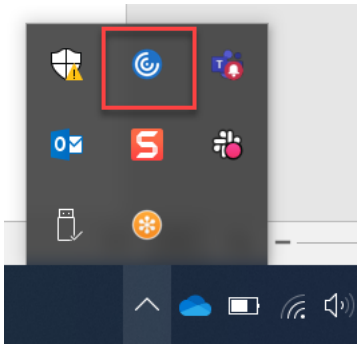
- Acceda a Citrix Store o Citrix Workspace a través de la aplicación Citrix Workspace. Este enfoque se denomina lanzamiento nativo.
- Abra la URL de Citrix Store o la URL de Citrix Workspace en un explorador web. Haga clic en una aplicación o en un escritorio virtual para descargar el archivo ICA correspondiente. A continuación, abra el archivo ICA mediante un explorador web para iniciar la aplicación o el escritorio virtual. Este enfoque se denomina lanzamiento web.

Para el lanzamiento web, asegúrese de que el dispositivo del usuario debe tener uno de los siguientes clientes según el sistema operativo del dispositivo.

| Cliente | Versión | Build |
|---|---|---|
| Aplicación Citrix Workspace para Windows | 2006.1 o posterior | 20.6.0.38 o posterior |
| Aplicación Citrix Workspace para Mac | 2006 o posterior | 20.06.0.7 o posterior |

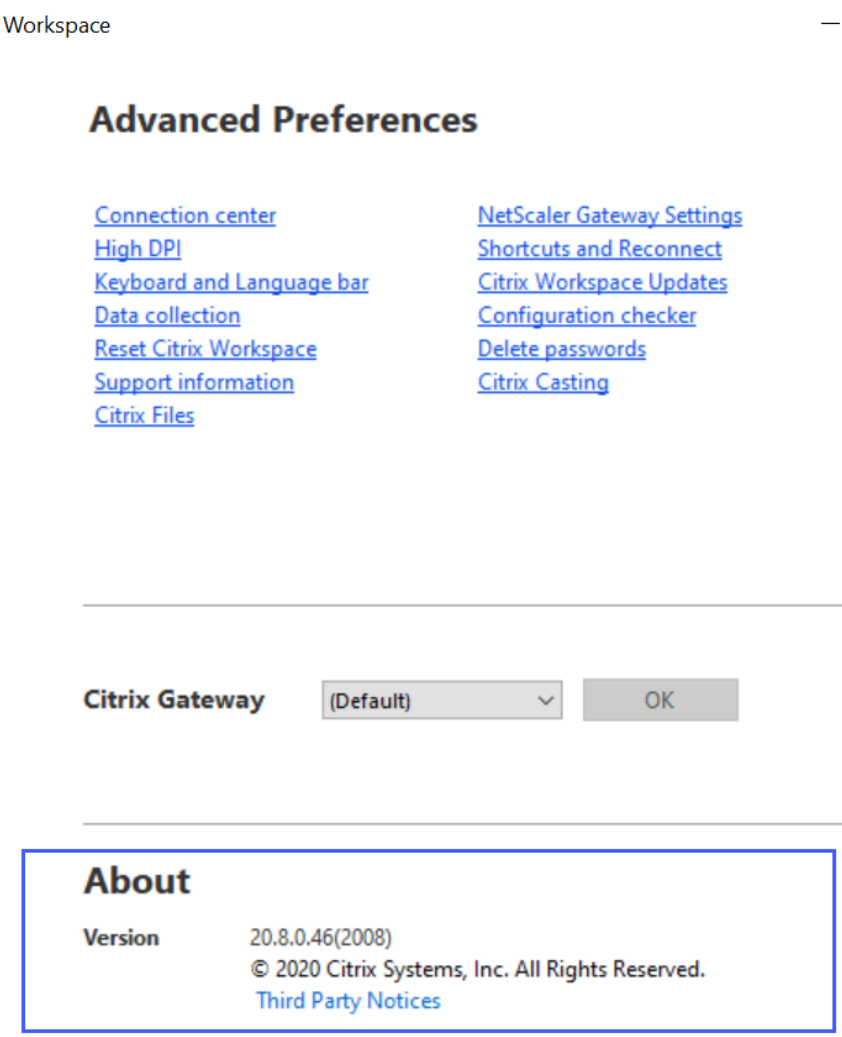
Para comprobar la versión de la aplicación Citrix Workspace:

1. En el equipo local del usuario, haga clic con el botón derecho en el icono de la aplicación Citrix Workspace.



2. Haga clic en **Preferencias avanzadas** y marque la sección **Acerca** de para ver la versión.




## El servidor de grabación de sesiones configurado no se conecta

July 12, 2022

El servidor de grabación de sesiones no se conecta a Citrix Analytics después de la configuración. Por lo tanto, no ve el Servidor configurado en la tarjeta del sitio **Session Recording**.

Para solucionar este problema, haga lo siguiente:

1. En el servidor de Grabación de sesiones configurado, ejecute el siguiente comando de PowerShell para comprobar la identificación del equipo cliente (CMID).

```
Get-WmiObject -class SoftwareLicensingService | select
    Clientmachineid
```

2. Si el CMID está vacío, agregue los siguientes archivos de registro en las rutas especificadas.

| Nombre en el Registro | Ruta del Registro | Tipo de clave | Valor |
|---|---|---|---|
| AuditorUniqueID | Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\SmartAuditor\Server\ | Cadena | Introduzca su UUID. |
| EnableCASUseAuditorUniqueID | Computer/HKEY_LOCAL_MACHINE/SOFTWARE/Citrix/SmartAuditor/Server/ | REG_DWORD | 1 |

3. Reinicie estos servicios:
   - Servicio Citrix Session Recording Analytics
   - Administrador de almacenamiento de grabación de sesiones de Citrix

## No se puede conectar el servidor StoreFront con Citrix Analytics

January 4, 2023

Después de importar los valores de configuración de Citrix Analytics a su servidor StoreFront, el servidor StoreFront no se conecta a Citrix Analytics.

Para obtener información sobre cómo importar los valores de configuración a un servidor StoreFront, consulte Incorporar sitios de Virtual Apps and Desktops mediante StoreFront.

El Asistente de incorporación de CAS ayuda a comprobar y solucionar los problemas descritos en este artículo. Para obtener más información, consulte Asistente de incorporación de Citrix Analytics Service (CAS).

Para solucionar el problema, haga lo siguiente:

1. En el servidor StoreFront, haga ping a los puntos finales específicos de la región de Citrix Analytics para probar la conectividad entre el servidor StoreFront y el servidor Citrix Analytics. Además, asegúrese de que se cumplan los requisitos previos.

> **Nota**
>
> En su servidor StoreFront, puede probar la conectividad haciendo ping directamente a los puntos finales específicos de la región o abriendo un explorador web y accediendo a los puntos finales específicos de la región.

2. Habilite el registro detallado en el servidor StoreFront para rastrear los registros. Para obtener más información sobre el registro detallado, consulte el artículo CTX139592.
3. Abra el Administrador de Internet Information Services (IIS) y compruebe lo siguiente:
   - Si el sitio de StoreFront se encuentra en el sitio predeterminado de IIS, IIS reinicia el sitio de StoreFront.
   - Si el sitio de StoreFront está en otros controladores o no está en el sitio predeterminado, abra la ventana de comandos y escriba `iisreset`.
4. Ejecute el siguiente comando para importar la configuración de Citrix Analytics:

```
Import-STFCasConfiguration -Path "configuration file path"
```

5. Ejecute el siguiente comando para verificar la configuración importada:

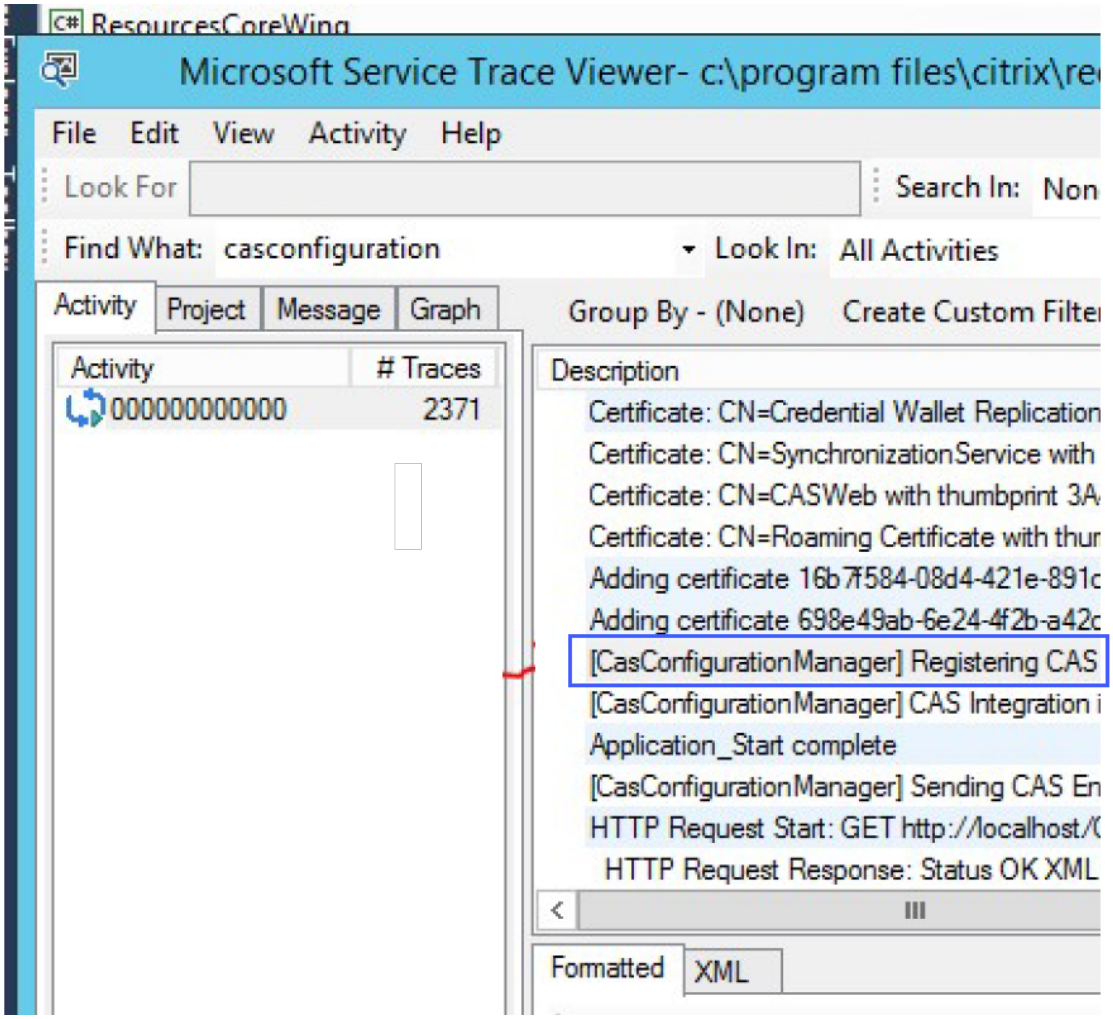
```
Get-STFCasConfiguration
```

6. Si el sitio de StoreFront se encuentra en otros controladores o no está en el sitio predeterminado, abra la ventana de comandos. Escriba `iisreset` para permitir que el sitio de StoreFront lea la configuración de Citrix Analytics.
7. Obtenga los archivos de registro detallados de StoreFront en la siguiente ubicación:

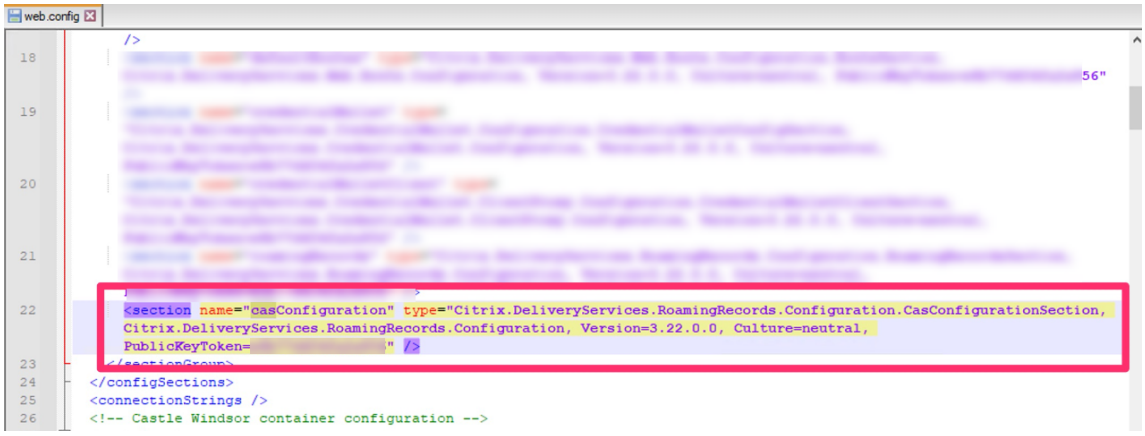
```
C:\Program Files\Citrix\Receiver StoreFront\Admin\trace
```

   En la ubicación mencionada anteriormente, puede encontrar varios archivos svclog que se pueden abrir en Event Viewer.
8. Use Microsoft Service Trace Viewer para abrir los siguientes registros:
   - Registros de StoreFront
   - Registros detallados de sitios móviles
9. En los registros, asegúrese de que las secciones **CasConfigurationManager** y la información del servidor Citrix Analytics estén disponibles.




10. Si las secciones CasConfigurationManager no están disponibles, abra el archivo web.config para el sitio móvil que se encuentra en `roaming site\folder`.
11. En el archivo `web.config`, busque la sección **casConfiguration** y asegúrese de que la información del servidor Citrix Analytics esté disponible.




12. En las máquinas Windows Server en las que esté instalado el servidor StoreFront, asegúrese de

lo siguiente:

- El cliente de TLS 1.2 está habilitado.
- Al menos uno de los siguientes conjuntos de cifrado está habilitado:
  - `TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384`
  - `TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256`
  - `TLS_DHE_RSA_WITH_AES_256_GCM_SHA384`
  - `TLS_DHE_RSA_WITH_AES_128_GCM_SHA256`

Para obtener información sobre cómo configurar el orden del conjunto de cifrado TLS, consulte la documentación de Microsoft.

13. Si utiliza máquinas con Windows Server 2012, asegúrese de que Diffie-Hellman Exchange (ECDHE/DHE) esté habilitado.
14. Asegúrese de que las máquinas Windows Server en las que está instalado el servidor StoreFront deben contener la configuración del registro mencionada en la documentación de Microsoft.

> **IMPORTANTE**
>
> Actualice los conjuntos de cifrado TLS/SSL mediante la directiva de grupo. No modifique manualmente los conjuntos de cifrado TLS/SSL. Para obtener más información sobre cómo usar la directiva de grupo, consulte la documentación de Microsoft.

Por ejemplo, la siguiente configuración del registro debe estar disponible en su equipo con Windows Server:

**Cliente TLS 1.2:**

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
    SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]
"Enabled"=dword:00000001
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
    SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]
"DisabledByDefault"=dword:00000000
```

**KEA de Diffie-Hellman:**

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
    SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\Diffie-Hellman
    ]
"Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
    SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\ECDH]
"Enabled"=dword:ffffffff
```

**Cifrados AES-128/AES-256:**

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
    SecurityProviders\SCHANNEL\Ciphers\AES 128/128]
"Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
    SecurityProviders\SCHANNEL\Ciphers\AES 256/256]
"Enabled"=dword:ffffffff
```

**Funciones hash SHA256/SHA384:**

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
    SecurityProviders\SCHANNEL\Hashes\SHA256]
"Enabled"=dword:ffffffff
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\
    SecurityProviders\SCHANNEL\Hashes\SHA384]
"Enabled"=dword:ffffffff
```

# Preguntas frecuentes

November 17, 2023

## Origen de datos

### ¿Qué es un origen de datos?

Los orígenes de datos son productos y servicios de Citrix que envían datos a Citrix Analytics.

Más información: Orígenes de datos

### ¿Cómo agrego un origen de datos?

Después de iniciar sesión en Citrix Analytics, en la pantalla de **bienvenida**, seleccione **Comenzar** para agregar un origen de datos a Citrix Analytics. Como alternativa, también puede agregar un origen de datos desde **Parámetros > Orígenes de datos**.

## Agente de Citrix ADM

### ¿Cuáles son los requisitos mínimos de recursos para instalar un agente en un hipervisor local?

8 GB de RAM, 4 CPU virtuales, 120 GB de almacenamiento, 1 interfaz de red virtual, 1 Gbps de rendimiento

**¿Tengo que asignar un disco adicional al agente de Citrix ADM durante el aprovisionamiento?**

No, no es necesario agregar un disco adicional. El agente solo se usa como intermediario entre Citrix Analytics y las instancias del centro de datos de su empresa. No almacena datos de inventario o análisis que requieran un disco adicional.

**¿Cuáles son las credenciales predeterminadas para iniciar sesión en un agente?**

Las credenciales predeterminadas para iniciar sesión en el agente son `nsrecover`/`nsroot`. Esto iniciará sesión en el intérprete de comandos del agente.

**¿Cómo cambio la configuración de red de un agente si he introducido un valor incorrecto?**

Inicie sesión en la consola del agente del hipervisor y acceda a la línea de comandos del shell con las credenciales `nsrecover`/`nsroot` y, a continuación, ejecute el comando `networkconfig`.

**¿Por qué necesito una URL de servicio y un código de activación?**

El agente utiliza la URL del servicio para localizar el servicio y el código de activación para registrar el agente en el servicio.

**¿Cómo puedo volver a introducir la URL del servicio si la he escrito incorrectamente en la consola del agente?**

Inicie sesión en el intérprete de comandos del agente con las credenciales `nsrecover`/`nsroot` y, a continuación, escriba: `deployment_type.py`. Este script le permite volver a introducir la URL del servicio y el código de activación.

**¿Cómo puedo obtener un nuevo código de activación?**

Puede obtener un nuevo código de activación del servicio Citrix ADM. Inicie sesión en el servicio Citrix ADM y vaya a **Redes > Agentes**. En la página **Agentes**, en la lista **Seleccionar acción**, seleccione **Generar código de activación**.

**¿Puedo reutilizar mi código de activación con varios agentes?**

No, no puede.

#### ¿Cuántos agentes de Citrix ADM debo instalar?

La cantidad de agentes depende de la cantidad de instancias administradas en un centro de datos y del rendimiento total. Citrix recomienda instalar al menos un agente por cada centro de datos.

#### ¿Cómo instalo varios agentes de Citrix ADM?

En la página Fuentes de datos, haga clic en el signo más (+) situado junto a Citrix Gateway y siga las instrucciones para instalar otro agente.

Como alternativa, puede acceder a la GUI de Citrix ADM y navegar a Redes > Agentes y hacer clic en **Configurar agente** para instalar varios agentes.

#### ¿Puedo instalar dos agentes en una configuración de alta disponibilidad?

No, no puede.

#### ¿Qué hago si falla el registro de mi agente?

- Asegúrese de que su agente tenga acceso a Internet (configure DNS).
- Asegúrese de haber copiado el código de activación correctamente.
- Asegúrese de haber introducido correctamente la URL del servicio.
- Asegúrese de tener abiertos los puertos necesarios.

#### El registro se ha realizado correctamente, pero ¿cómo puedo saber si el agente funciona correctamente?

Puede hacer lo siguiente para comprobar si el agente funciona correctamente:

- Una vez que el agente se haya registrado correctamente, acceda a Citrix ADM y vaya a **Redes > Agentes**. Puede ver los agentes descubiertos en esta página. Si el agente funciona correctamente, el estado se indica con un icono verde. Si no se está ejecutando, el estado se indica con un icono rojo.
- Inicie sesión en el intérprete de comandos del agente y ejecute los siguientes comandos: `ps -ax | grep mas` y `ps -ax | grep ulfd`. Asegúrese de que se estén ejecutando los siguientes procesos.

```
> shell
bash-3.2# ps -ax | grep mas
  550  ??  I      0:00.55 /usr/local/bin/python /mps/mas_hb_monit.py (python2.7)
 3027  ??  Is     0:04.65 ./mas_control --daemon --pidfile=/var/run/controld.pid
 3167  ??  I      0:00.90 ./mas_sysop CONTROL_IPC_SOCK=/tmp/mps/ipc_sockets/mps_control_sock
 3172  ??  I      5:48.09 ./mas_event CONTROL_IPC_SOCK=/tmp/mps/ipc_sockets/mps_control_sock
 3184  ??  I      0:52.81 ./mas_service CONTROL_IPC_SOCK=/tmp/mps/ipc_sockets/mps_control_sock
 3210  ??  I     17:01.36 ./mas_afdecoder CONTROL_IPC_SOCK=/tmp/mps/ipc_sockets/mps_control_sock
 3221  ??  I      0:49.17 ./mas_cloudagent CONTROL_IPC_SOCK=/tmp/mps/ipc_sockets/mps_control_sock
81383   0  Is     0:00.46 mas_cli
81580   0  S+     0:00.00 grep mas
bash-3.2# ps -ax | grep ulfd
 2834  ??  S      0:25.49 /var/mps/telemetry/ulfd/bin/nsulfd
 2835  ??  I      0:00.00 logger -i -t nsulfd -p local7.info
 2975  ??  S      0:01.41 /usr/local/bin/python -u /var/mps/telemetry/ulfd/bin/nsaad.py (python2.7)
81657   0  S+     0:00.00 grep ulfd
bash-3.2#
```

- Si alguno de los procesos no se está ejecutando, ejecute el comando **masd restart**. Es posible que tarde algún tiempo en iniciar todos los demonios (aproximadamente 1 minuto).
- Asegúrese de que `agent.conf` se haya creado en `/mpsconfig` después del registro correcto del agente.

## Incorporación de instancias de Citrix Gateway

### Las instancias de Citrix Gateway se agregan a Citrix Analytics, pero ¿cómo puedo saber si Analytics está habilitada en el agente?

Puede comprobar si el análisis está habilitado en el agente mediante el indicador de shell del agente. Si los análisis se habilitan correctamente en el agente, el parámetro `turnOnEvent` se establecería en `Y` en el archivo `/mpsconfig/telemetry_cloud.conf`.

Inicie sesión en el intérprete de comandos del agente y ejecute el siguiente comando: cat `/mpsconfig/telemetry_cloud.conf` y verifique el valor del parámetro `turnOnEvent`.

```
bash-3.2# cat /mpsconfig/telemetry_cloud.conf
{
"storage_account" : "casstoragebulkstaging",
"blobname" : "ns-mas-nwfaq2pzeena5pv2oi5mrhhlmmmyrf7n",
"blob_token" : "se=2018-03-29T06:03:21Z&sv=2015-12-11&si=_default&sr=c&sig=eAyPO
4516PPVr8Z6eVOOE4FvQ0HIvu7jVSW6NHBCtxE=",
"eventhub_sas" : "SharedAccessSignature sr=https://ehstaging.servicebus.windows.
net/ehgeneral/publishers/citrix691796.ns.mas.70380659-3fc3-462e-ba5b-cbc5d62f457
5/messages?api-version=2014-01&sig=WjUQcpqwX3eETMWr+x1a9sSbxeY8gPO8SktgTmguerw=&
se=1522303402&skn=dirsvc_send",
"expires" : 0,
"eventhub_endpoint" : "https://ehstaging.servicebus.windows.net/ehgeneral/publis
hers/citrix691796.ns.mas.70380659-3FC3-462E-BA5B-CBC5D62F4575/messages?api-versi
on=2014-01",
"turnOnEvent" : "Y",
"tenant" : "citrix691796",
"agent_id" : "dbb2b943-3b18-46c9-8c7e-70e206f5b3a0"
}
bash-3.2#
```

**He cerrado accidentalmente el asistente de incorporación de Citrix Gateway. ¿Tengo que iniciar mi configuración desde el principio?**

No. Citrix Analytics guarda el progreso y muestra la configuración incompleta como un mosaico en la página **Orígenes de datos > Parámetros**. Haga clic en **Continuar configuración** para completar la configuración.

## Incorporación del sitio de Virtual Apps and Desktops

**¿Cómo desactivo el procesamiento de datos?**

Si desea inhabilitar temporalmente el procesamiento de datos de su sitio a Citrix Analytics, simplemente haga clic en la tarjeta **Sitio** y, a continuación, haga clic en **Desactivar el procesamiento de datos**.

**Cuando agrego mi sitio a Workspace y hago clic en "Probar STA", la prueba falla. ¿Qué debo hacer?**

Es posible que haya un problema de conectividad entre Citrix Gateway y Cloud Connectors. Para solucionar problemas, consulte CTX232517 en el Knowledge Center de soporte de Citrix.

## ¿Dónde puedo obtener ayuda con Citrix Analytics?

Puede hacer preguntas y ponerse en contacto con expertos de Citrix Analytics en el foro de debate de Citrix Analytics en https://discussions.citrix.com/forum/1710-citrix-analytics/.

Para participar en el foro, debe iniciar sesión con su ID de Citrix.

## Garantía de acceso —Geolocalización

**¿Cómo obtiene Analytics los detalles de geolocalización?**

Citrix Analytics usa la dirección IP del dispositivo desde el que se inicia el cliente de Workspace. Citrix Analytics aprovecha un proveedor de datos de geolocalización IP de terceros para derivar la ubicación de un usuario a partir de su dirección IP. Cuando inicia sesión, resuelve su ubicación (dirección IPv4) en un país o ciudad, y la asignación se actualiza periódicamente. Las organizaciones pueden usar estas ubicaciones definidas por países para monitorear los patrones de acceso desde donde no hacen negocios.

#### ¿Cuál es el nivel de precisión para derivar la ubicación de un usuario?

Citrix Analytics aprovecha un proveedor de datos de geolocalización IP de terceros para derivar la ubicación de un usuario a partir de su dirección IP. Los servicios GeoIP pueden resolver en la ciudad o ubicación correcta la mayor parte del tiempo, pero las búsquedas de GeoIP nunca son completamente precisas. A veces, la ubicación que se muestra a un usuario puede ser diferente de su ubicación precisa de acceso.

Según la documentación de IP GeoPoint, el nivel de cobertura es de aproximadamente el 99,99% de las direcciones IP asignadas en todo el mundo (direcciones IP enrutables IPv4). En términos de precisión de ubicación, acompaña a cada uno de los campos de ubicación esenciales (país, estado, ciudad, código postal) con un factor de confianza.

#### ¿En qué casos es inexacta la determinación de la ubicación?

La precisión de los datos de geolocalización depende de cómo se conecte el dispositivo a Internet. Un dispositivo puede conectarse a Internet a través de:

- Puertas de enlace móviles
- VPN o servicio de alojamiento
- Servidor proxy o anonimizador regional o internacional

En tales casos, los datos de geolocalización no son precisos, independientemente de que se utilice el software del proveedor de geolocalización IP.

#### ¿Cuáles son las versiones compatibles de la aplicación Citrix Workspace?

Hay versiones mínimas de la aplicación Citrix Workspace necesarias para que el sistema operativo envíe el atributo de **dirección IP** a Citrix Analytics for Security. Consulte la tabla de matriz o las ubicaciones identificadas como no disponibles para obtener más información.

#### ¿En qué casos no recibimos los detalles geológicos?

Para ver los detalles de geolocalización, consulte la sección Ubicaciones identificadas como no disponibles para obtener más información.

#### ¿Qué servicio de geolocalización utiliza Citrix Analytics para informar de la ubicación de un usuario? ¿Cómo informar de una ubicación incorrecta para una IP?

Citrix Analytics utiliza los servicios de geolocalización basados en archivos de Neustar para proporcionar datos de geolocalización para los accesos entrantes. Tiene una página de corrección de IP

pública que se puede utilizar para enviar una solicitud de corrección por cuenta propia. Una vez que se envía una solicitud de corrección, Neustar revisa la solicitud para verificar su precisión y la procesa.

El proveedor de GeoIP ayuda a mostrar la información más precisa posible. Desafortunadamente, puede haber casos en los que los datos de GeoIP sean inexactos debido a la naturaleza innata de GeoIP.

## Glosario de términos

September 11, 2024

- **Acciones**: respuestas de bucle cerrado a eventos sospechosos. Se aplican acciones para evitar que ocurran eventos anómalos en el futuro. Obtenga más información.
- **Agente de seguridad de acceso a la nube (CASB)**: punto de aplicación de la directiva de seguridad local o basado en la nube ubicado entre los consumidores de servicios en la nube y los proveedores de servicios Los CASB combinan e interponen directivas de seguridad empresarial a medida que se accede a los recursos basados en la nube. También ayudan a las organizaciones a ampliar los controles de seguridad de su infraestructura local a la nube.
- **Citrix ADC (Application Delivery Controller)**: Dispositivo de red que vive en un centro de datos, ubicado estratégicamente entre el firewall y uno o más servidores de aplicaciones. Maneja el equilibrio de carga entre servidores y optimiza el rendimiento y la seguridad del usuario final para las aplicaciones empresariales. Obtenga más información.
- **Citrix ADM (Application Delivery Management)**: Solución centralizada de administración, análisis y orquestación de redes. Desde una única plataforma, los administradores pueden ver, automatizar y administrar los servicios de red para arquitecturas de aplicaciones escalables. Obtenga más información.
- **Agente de Citrix ADM**: Proxy que permite la comunicación entre Citrix ADM y las instancias administradas en un centro de datos. Obtenga más información.
- **Citrix Analytics**: Servicio en la nube que recopila datos en servicios y productos (locales y en la nube) y genera información procesable, lo que permite a los administradores gestionar de forma proactiva las amenazas a la seguridad de los usuarios y las aplicaciones, mejorar el rendimiento de las aplicaciones y admitir operaciones continuas. Obtenga más información.
- **Citrix Cloud**: plataforma que se conecta a los recursos a través de Citrix Cloud Connector en cualquier nube o infraestructura (local, nube pública, nube privada o nube híbrida). Obtenga más información.

- **Citrix Gateway**: Solución de acceso remoto consolidada que consolida la infraestructura de acceso remoto para proporcionar un inicio de sesión único en todas las aplicaciones, ya sea en un centro de datos, en la nube o entregadas como SaaS. Más información.
- **Citrix Hypervisor**: Plataforma de administración de virtualización optimizada para infraestructuras de virtualización de aplicaciones, escritorios y servidores. Obtenga más información.
- **Aplicación Citrix Workspace** (anteriormente conocida como Citrix Receiver): Software cliente que proporciona un acceso seguro y sin problemas a las aplicaciones, escritorios y datos desde cualquier dispositivo, incluidos smartphones, tabletas, PC y Mac. Obtenga más información.
- **DLP (Prevención de pérdida de datos)**: Solución que describe un conjunto de tecnologías y técnicas de inspección para clasificar la información contenida en un objeto, como un archivo, correo electrónico, paquete, aplicación o un almacén de datos. Además, el objeto también puede estar en almacenamiento, en uso o en una red. Las herramientas de DLP pueden aplicar directivas de forma dinámica, como registrar, informar, clasificar, reubicar, etiquetar y cifrar. Las herramientas de DLP también pueden aplicar protecciones de administración de derechos de datos empresariales. Obtenga más información.
- **DNS (Sistema de nombres de dominio)**: Servicio de red que se utiliza para localizar nombres de dominio de Internet y traducirlos a direcciones de protocolo de Internet (IP). El DNS mapea los nombres de sitios web que los usuarios proporcionan, a sus direcciones IP correspondientes que proporcionan las máquinas, para ubicar un sitio web independientemente de la ubicación física de las entidades.
- **Procesamiento de datos**: Método de procesamiento de datos desde una fuente de datos a Citrix Analytics. Obtenga más información.
- **Origen de datos**: Producto o servicio que envía datos a Citrix Analytics. Un origen de datos puede ser interno o externo. [Más información]/en-us/citrix-analytics/data-sources.html).
- **Exportación de datos**: Producto o servicio que recibe datos de Citrix Analytics y proporciona información. Obtenga más información.
- **Usuarios descubiertos**: Total de usuarios de una organización que utilizan orígenes de datos. Obtenga más información.
- **FQDN (nombre de dominio completo)**: Nombre de dominio completo para el acceso interno (StoreFront) y externo (Citrix ADC).
- **Aprendizaje automático**: Tipo de tecnología de análisis de datos que extrae conocimiento sin programarse explícitamente para hacerlo. Los datos de una amplia variedad de fuentes potenciales, como aplicaciones, sensores, redes, dispositivos y dispositivos, se introducen en un sistema de aprendizaje automático. El sistema utiliza los datos y aplica algoritmos para construir su propia lógica para resolver un problema, obtener información o hacer una predicción.

- **Microsoft Graph Security**: puerta de enlace que conecta la seguridad del cliente y los datos organizativos Proporciona alertas y opciones de corrección fáciles de revisar cuando se debe tomar una medida. Obtenga más información.
- **Análisis de rendimiento**: servicio que proporciona visibilidad de los detalles de las sesiones de los usuarios en toda la organización. Obtenga más información.
- **Directiva**: Conjunto de condiciones que deben cumplirse para que una acción se aplique en el perfil de riesgo de un usuario. Obtenga más información.
- **Indicador de riesgo**: Métrica que proporciona información sobre el nivel de exposición a un riesgo empresarial que la organización tiene en un momento dado. Obtenga más información.
- **Puntuación de riesgo**: Valor dinámico que indica el nivel agregado de riesgo que un usuario o una entidad representa para una infraestructura de TI durante un período de supervisión predeterminado. Obtenga más información.
- **Cronograma de riesgo**: Registro del comportamiento de riesgo de un usuario o una entidad que permite a los administradores investigar un perfil de riesgo y comprender el uso de datos, el uso del dispositivo, el uso de la aplicación y el uso de la ubicación. Obtenga más información.
- **Usuario con riesgos**: Usuario que ha actuado de manera arriesgada o ha presentado un comportamiento con riesgos. Obtenga más información.
- **Análisis de seguridad**: Análisis avanzado de datos que se utilizan para lograr resultados de seguridad convincentes, como la supervisión de la seguridad y la búsqueda de amenazas. Obtenga más información.
- **Secure Private Access**: Servicio que proporciona integración de inicio de sesión único, acceso remoto e inspección de contenido en una única solución para el control de acceso de extremo a extremo. Obtenga más información.
- **Splunk**: software SIEM (Administración de eventos e información de seguridad) que recibe datos inteligentes de Citrix Analytics y proporciona información sobre los posibles riesgos empresariales. Obtenga más información.
- **UBA (Análisis del comportamiento del usuario)**: Proceso de referencia de la actividad y el comportamiento de los usuarios en combinación con el análisis de grupos de pares, para detectar posibles intrusiones y actividades maliciosas.
- Lista de**seguimiento: lista**de usuarios o entidades a los que los administradores quieren supervisar en busca de actividades sospechosas. Obtenga más información.