Device Posture

Machine translated content

Disclaimer

Contents

Device Posture

February 16, 2024

El servicio Citrix Device Posture es una solución basada en la nube que ayuda a los administradores a cumplir ciertos requisitos que los dispositivos finales deben cumplir para acceder a los recursos de Citrix DaaS (aplicaciones y escritorios virtuales) o Citrix Secure Private Access (SaaS, aplicaciones web, TCP y UDP). Establecer la confianza en el dispositivo comprobando la postura del dispositivo es fundamental para implementar un acceso basado en la confianza cero. El servicio Device Posture aplica los principios de confianza cero en su red al comprobar el cumplimiento de los dispositivos finales (gestión, BYOD y postura de seguridad) antes de permitir que el usuario final inicie sesión.

Requisitos previos

- Requisitos de licencia: la concesión del servicio Citrix Device Posture forma parte de las licencias Citrix DaaS Premium, Citrix DaaS Premium Plus y Citrix Secure Private Access Advanced. Los clientes con otras licencias pueden adquirir un derecho a Device Posture Service como complemento. Para un complemento, los clientes deben comprar un SKU de autenticación adaptable independiente, pero no necesariamente tienen que implementarlo para usar el servicio Device Posture.
- Plataformas admitidas:
  - Windows (10 y 11)
  - macOS 13 Ventura
  - macOS 12 Monterrey
  - iOS
  - IGEL

> **Nota:**
>
> - Un dispositivo que se ejecuta en una plataforma no compatible se marca como no compatible de forma predeterminada. Puede cambiar la clasificación de **No conforme** a Inicio de **sesión denegado** en la ficha **Configuración** de la página Postura del dispositivo.
> - Un dispositivo que se ejecuta en una plataforma compatible, pero que no coincide con ninguna directiva de postura del dispositivo predefinida, se marca como no compatible de forma predeterminada. Puede cambiar la clasificación de **No conforme** a Inicio de **sesión denegado** en la ficha **Configuración** de la página Postura del dispositivo.
> - Para la compatibilidad con iOS en el servicio Device Posture, el cliente EPA está inte-

> grado como parte de la aplicación Citrix Workspace para iOS. Para obtener más información sobre las versiones, consulte la aplicación Citrix Workspace para iOS.
>
> – Para que IGEL OS sea compatible con el servicio Device Posture, el cliente EPA está integrado como parte del sistema operativo IGEL. Póngase en contacto con el equipo de soporte de IGEL para instalar el cliente EPA en los dispositivos IGEL.

- Cliente Citrix Device Posture (cliente EPA): una aplicación ligera que debe instalarse en el dispositivo terminal para ejecutar escaneos de postura del dispositivo. Esta aplicación no requiere derechos de administrador local para descargarla e instalarla en un endpoint.

  > **Nota:**
  >
  > Si utilizas una verificación del certificado del dispositivo, debes instalar el cliente de la EPA con derechos de administrador.

- Navegadores compatibles: Chrome, Edge y Firefox.
- Configuración del firewall: para permitir que el servicio Device Posture actualice los clientes EPA en un dispositivo final, el firewall/proxy debe configurarse para permitir los siguientes dominios:
  - `https://swa-ui-cdn-endpoint-prod.azureedge.net`
  - `https://productioniconstorage.blob.core.windows.net`
  - *.netscalergateway.net
  - *.nssvc.net
  - *.cloud.com
  - *.pendo.io
  - *.citrixworkspacesapi.net

Funciones en Tech Preview

- Servicio de postura del dispositivo con IGEL. Regístrese para obtener la vista previa mediante https://podio.com/webforms/29062020/2362942.
- Servicio de postura del dispositivo con iOS. Regístrese para obtener la vista previa mediante https://podio.com/webforms/28888524/2338366.
- Verificación de geolocalización y verificación de ubicación de red. Regístrese para obtener la vista previa mediante https://podio.com/webforms/29051759/2362665.
- Integración de CrowdStrike con el servicio Device Posture. Para obtener más información, consulta la integración de CrowdStrike con Device Posture - Preview.

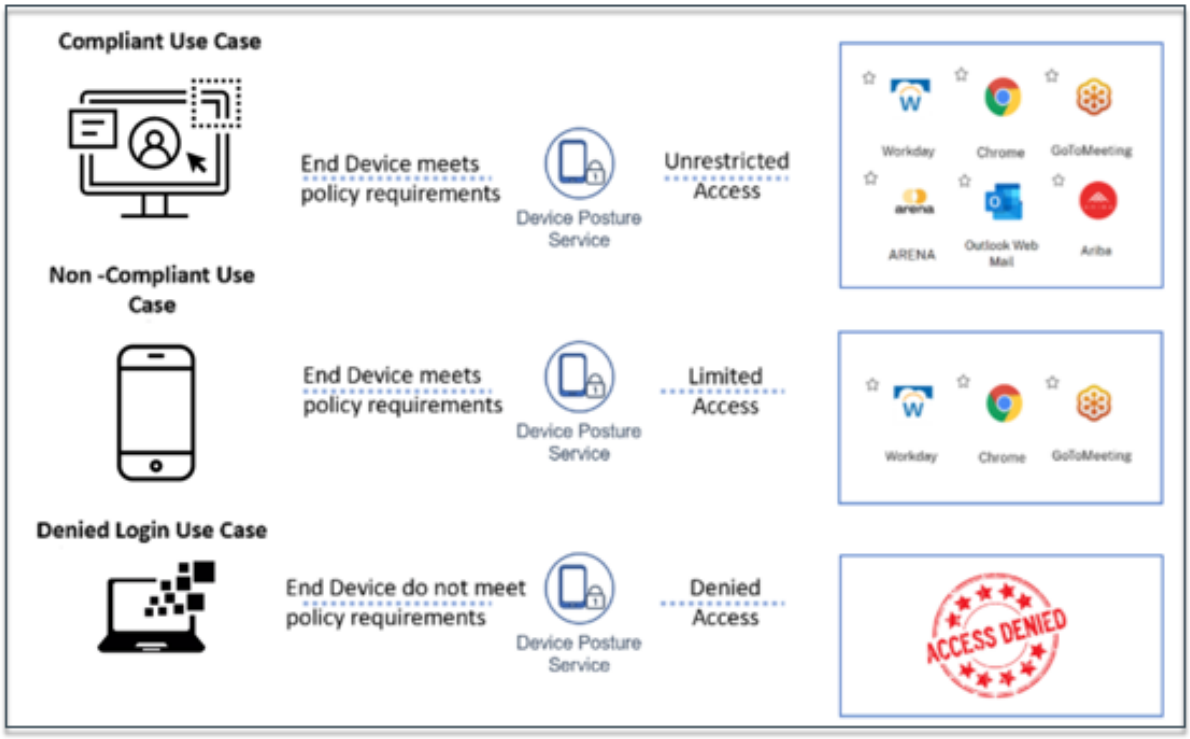
Funcionamiento

Los administradores pueden crear directivas de posición de los dispositivos para comprobar la posición de los dispositivos de punto final y determinar si se permite o se deniega el inicio de sesión en un dispositivo de punto final. Los dispositivos a los que se permite iniciar sesión se clasifican además como conformes o no conformes. Los usuarios pueden iniciar sesión desde un explorador web o la aplicación Citrix Workspace.

Las siguientes son las condiciones de alto nivel que se utilizan para clasificar un dispositivo como compatible, no compatible y de inicio de sesión denegado.

- **Dispositivos compatibles**: Dispositivo que cumple con los requisitos de directiva preconfigurados y que puede iniciar sesión en la red de la empresa con acceso total o sin restricciones a los recursos de Citrix Secure Private Access o a los recursos de Citrix DaaS.
- **Dispositivos no compatibles**: Dispositivo que cumple con los requisitos de directiva preconfigurados y que puede iniciar sesión en la red de la empresa con acceso parcial o restringido a los recursos de Citrix Secure Private Access o a los recursos de Citrix DaaS.
- **Inicio de sesión denegado:** Se deniega el inicio de sesión a un dispositivo que no cumpla con los requisitos de la directiva.

La clasificación de los dispositivos como **compatibles,**no conformes****y con inicio de **sesión denegado** se transfiere al servicio Citrix DaaS y Citrix Secure Private Access, que a su vez utiliza la clasificación de dispositivos para proporcionar capacidades de acceso inteligente.



> **Nota:**
>
> - Las directivas de Posición de dispositivo deben configurarse específicamente para cada plataforma. Por ejemplo, en macOS, un administrador puede permitir el acceso a los dispositivos que tienen una versión de sistema operativo específica. Del mismo modo, para Windows, el administrador puede configurar directivas para incluir un archivo de autorización específico, ajustes de registro, etc.
> - Los escaneos de la postura del dispositivo solo se realizan durante la autenticación previa o antes de iniciar sesión.
> - Para ver las definiciones de "conforme"e "no conforme", consulte Definiciones.

Escaneos compatibles con Postura del dispositivo

El servicio Citrix Device Posture admite los siguientes escaneos:

Windows	macOS	iOS	IGEL
Versión de la aplicación Citrix Workspace	Versión de la aplicación Citrix Workspace	Versión de la aplicación Citrix Workspace	-
Versión del sistema operativo	Versión del sistema operativo	Versión del sistema operativo	-
Archivo (existe, nombre de archivo y ruta)	Archivo (existe, nombre de archivo y ruta)	-	Archivo (existe, nombre de archivo y ruta)
Geolocalización	Geolocalización	-	-
Ubicación de red	Ubicación de red	-	-
Dirección MAC	Dirección MAC	-	-
Proceso (existe)	Proceso (existe)	-	-
Microsoft Endpoint Manager	Microsoft Endpoint Manager	-	-
CrowdStrike	CrowdStrike	-	-
Certificado del dispositivo	Certificado del dispositivo	-	-
Explorador web	Explorador web	-	-
Antivirus	Antivirus	-	-

Windows	macOS	iOS	IGEL
Registro no numérico (32 bits)	-	-	-
Registro no numérico (64 bits)	-	-	-
Registro numérico (32 bits)	-	-	-
Registro numérico (64 bits)	-	-	-
Tipo de instalación de Windows Update	-	-	-
Instalación de Windows Update, comprobación de la última actualización	-	-	-

> **Nota:**
>
> - Para la compatibilidad con iOS en el servicio Device Posture, el cliente EPA está integrado como parte de la aplicación Citrix Workspace para iOS. Para obtener más información sobre las versiones, consulte la aplicación Citrix Workspace para iOS.

Integración de terceros con la postura del dispositivo

Además de los escaneos nativos que ofrece el servicio Device Posture, el servicio también se puede integrar con las siguientes soluciones de terceros en Windows y macOS.

- Microsoft Intune. Para obtener más información, consulte Integración de Microsoft Intune con Device Posture.
- CrowdStrike. Para obtener más información, consulta la integración de CrowdStrike con Device Posture - Preview.

Configurar la postura del dispositivo

La postura del dispositivo es una combinación de directivas y reglas que un dispositivo debe cumplir para acceder a los recursos. Cada directiva se adjunta a una de las acciones, a saber: conforme, no conforme o inicio de sesión denegado. Además, cada directiva está asociada a una prioridad y la evaluación de la directiva se detiene si una directiva se considera verdadera y se toman las medidas correspondientes.

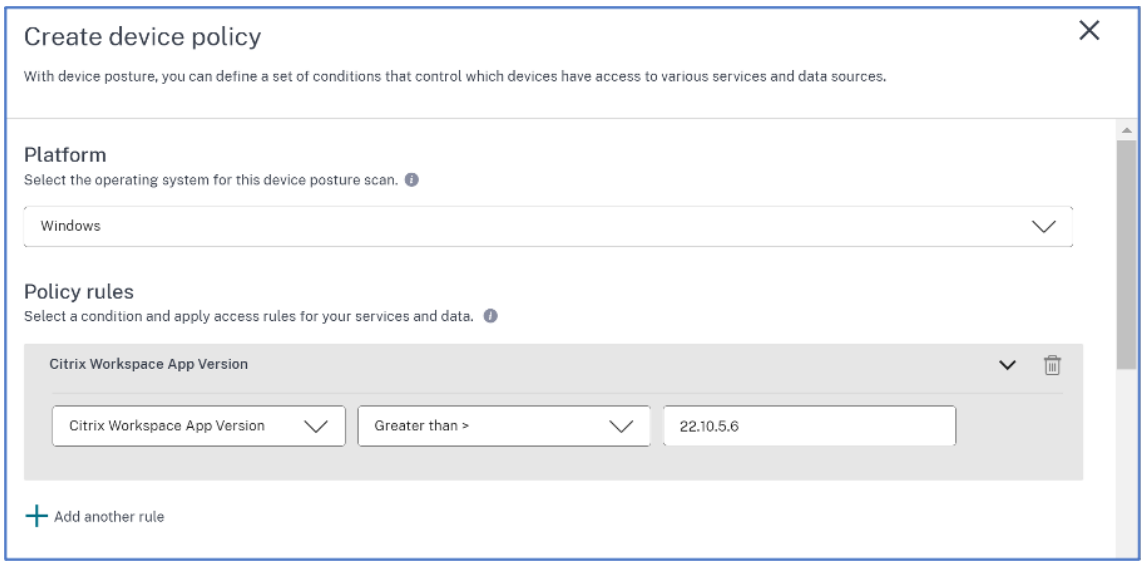
1. Inicie sesión en Citrix Cloud y, a continuación, seleccione **Administración de acceso e identidades** en el menú de tres líneas.
2. Haga clic en la ficha **Postura del dispositivo** y, a continuación, en **Administrar**.

   > **Nota:**
   >
   > - Los clientes del servicio Secure Private Access pueden hacer clic directamente en **Device Posture** en la barra de navegación izquierda de la interfaz de usuario del administrador.
   > - Para los usuarios nuevos, la página de inicio de Posición de dispositivo les pide que creen una directiva de Posición de dispositivo. La directiva de Posición de dispositivo debe configurarse de forma individual para cada plataforma. Una vez que haya creado una directiva de Posición de dispositivo, aparecerá en las plataformas correspondientes.
   > - Una directiva entra en vigor solo después de habilitar Posición de dispositivo. Para habilitar Postura del dispositivo, presione el botón **Postura del dispositivo está inhabilitad** de la esquina superior derecha para **habilitarla**.

3. Haga clic en **Crear directiva de dispositivos**.
4. En **Plataforma**, seleccione la plataforma para la que quiera aplicar una directiva. Puede cambiar la plataforma de Windows a macOS o viceversa, independientemente de la ficha que haya seleccionado en la página principal de Postura del dispositivo.
5. En **Reglas de directiva**, seleccione la comprobación que desee realizar como parte de la postura del dispositivo y seleccione las condiciones que deben coincidir.

   > **Nota:**
   >
   > - Para comprobar el certificado del dispositivo, asegúrese de que el certificado del emisor esté en el dispositivo. De lo contrario, puede importar un certificado de dispositivo mientras crea la directiva de postura del dispositivo o cargar el certificado desde **Configuración** en la página de inicio de Device Posture. Para obtener más información, consulte Importar el certificado de dispositivo al crear la directiva para el certificado de dispositivo y Cargar el certificado de dispositivo.
   > - Para la verificación del certificado del dispositivo, el cliente EPA del dispositivo final debe estar instalado con derechos administrativos.
   > - La verificación del certificado del dispositivo con el servicio Device Posture no admite la verificación de revocación de certificados.

6. Haga clic en **Agregar otra regla** para crear varias reglas. Se aplica una condición AND a varias reglas.



7. En **Resultado de directiva** basado en las condiciones que ha configurado, seleccione el tipo según el cual el análisis del dispositivo debe clasificar el dispositivo del usuario.

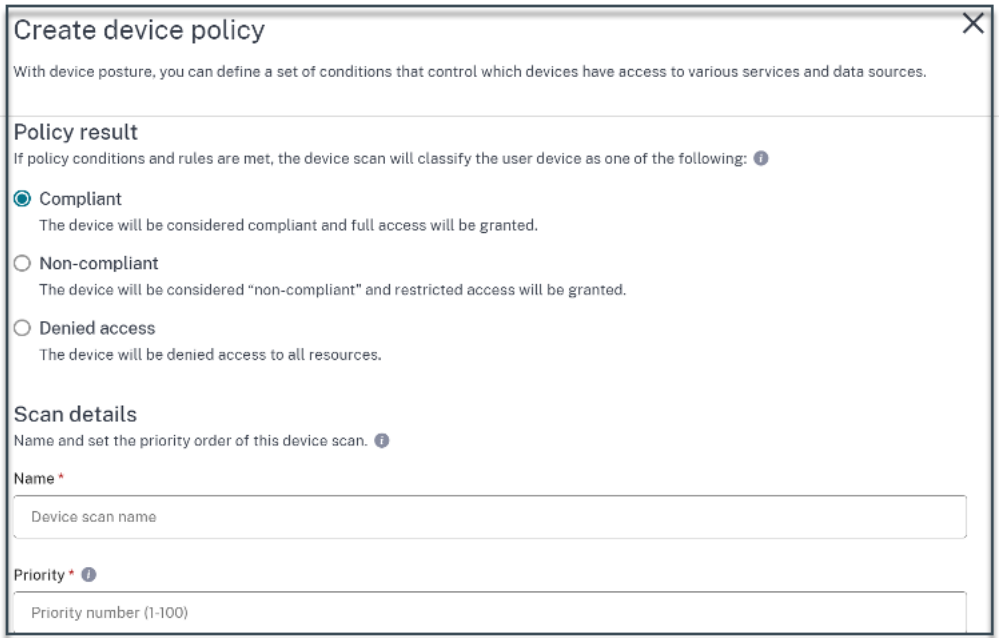
   - Conforme
   - No cumple
   - Acceso denegado

8. Introduzca un nombre para la directiva.

9. En **Prioridad**, introduzca el orden en que se deben evaluar las directivas.

   - Puede introducir un valor comprendido entre 1 y 100. Se recomienda configurar las directivas de denegación con mayor prioridad, seguidas de las no conformes y, por último, las conformes.
   - La prioridad con el valor más bajo tiene la preferencia más alta.
   - Solo las directivas que están habilitadas se evalúan en función de la prioridad.

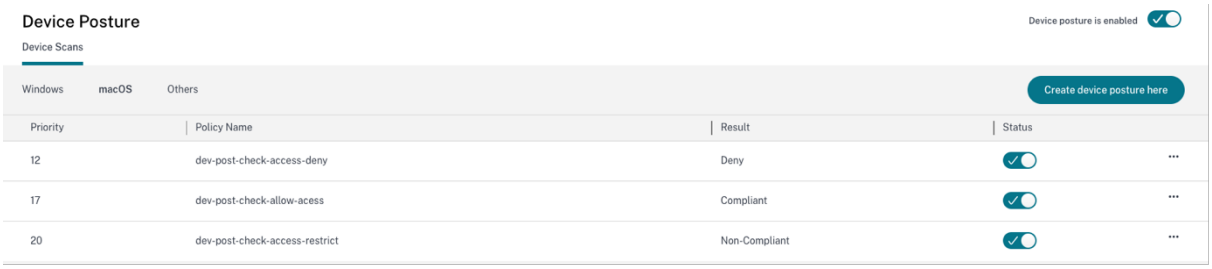
10. Haga clic en **Crear**.



> **Importante:**
>
> Debe **activar** el botón **Habilitar al crearse** para que las directivas de postura del dispositivo surtan efecto. Antes de habilitar las directivas, se recomienda que se asegure de que las directivas estén configuradas correctamente y que realice estas tareas en la configuración de prueba.

Modificar una directiva de Posición de dispositivo

Las directivas de postura del dispositivo configuradas se enumeran en la plataforma específica, en la página **Escaneos de dispositivos**. Puede buscar la directiva que quiere modificar desde esta página. También puede habilitar, inhabilitar o eliminar una directiva desde esta página.



Configurar el acceso contextual (acceso inteligente) mediante la postura del dispositivo

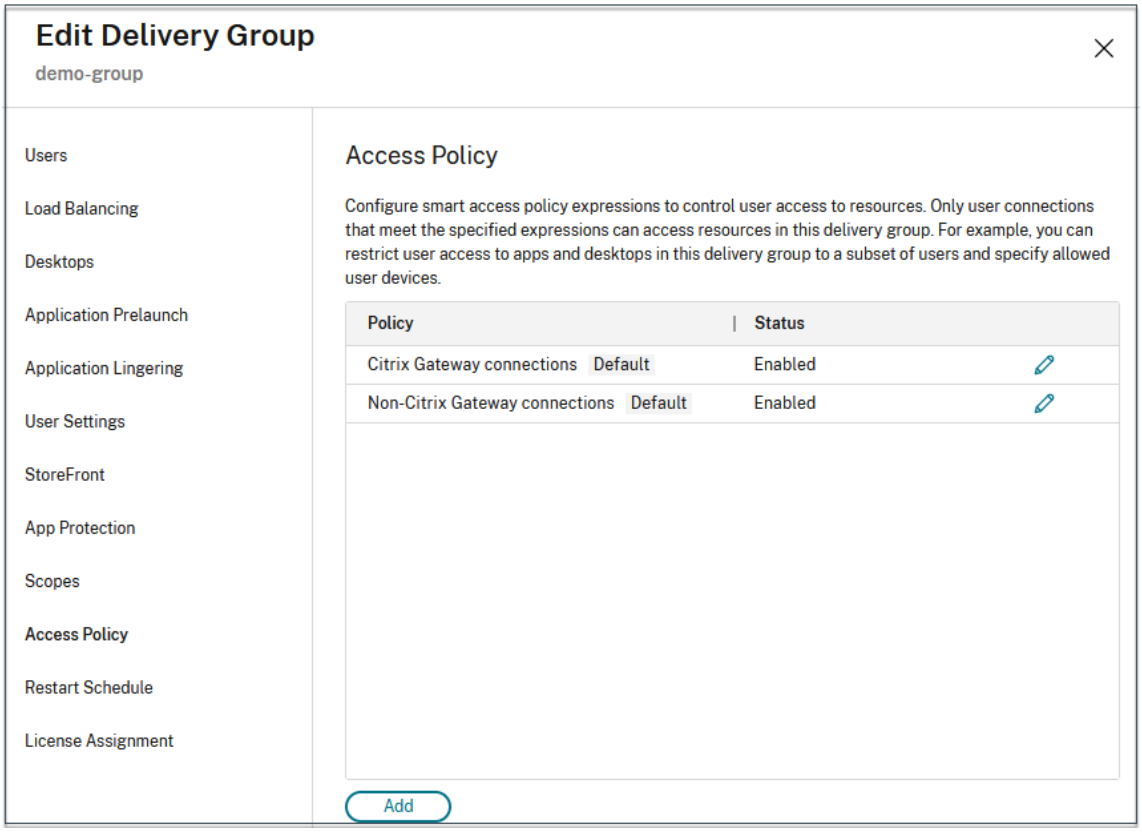
Tras la verificación de la postura del dispositivo, se le permite iniciar sesión y se clasifica como compatible o no compatible. Esta información está disponible como etiquetas para el servicio Citrix DaaS y el servicio Citrix Secure Private Access y se utiliza para proporcionar acceso contextual en función de

la posición del dispositivo. Por lo tanto, Citrix DaaS y Citrix Secure Private Access deben configurarse para aplicar el control de acceso mediante etiquetas de posición del dispositivo.

Configuración de Citrix DaaS con Device Posture mediante la nueva interfaz de usuario de Studio (versión preliminar)

Inscríbase para obtener la vista previa.

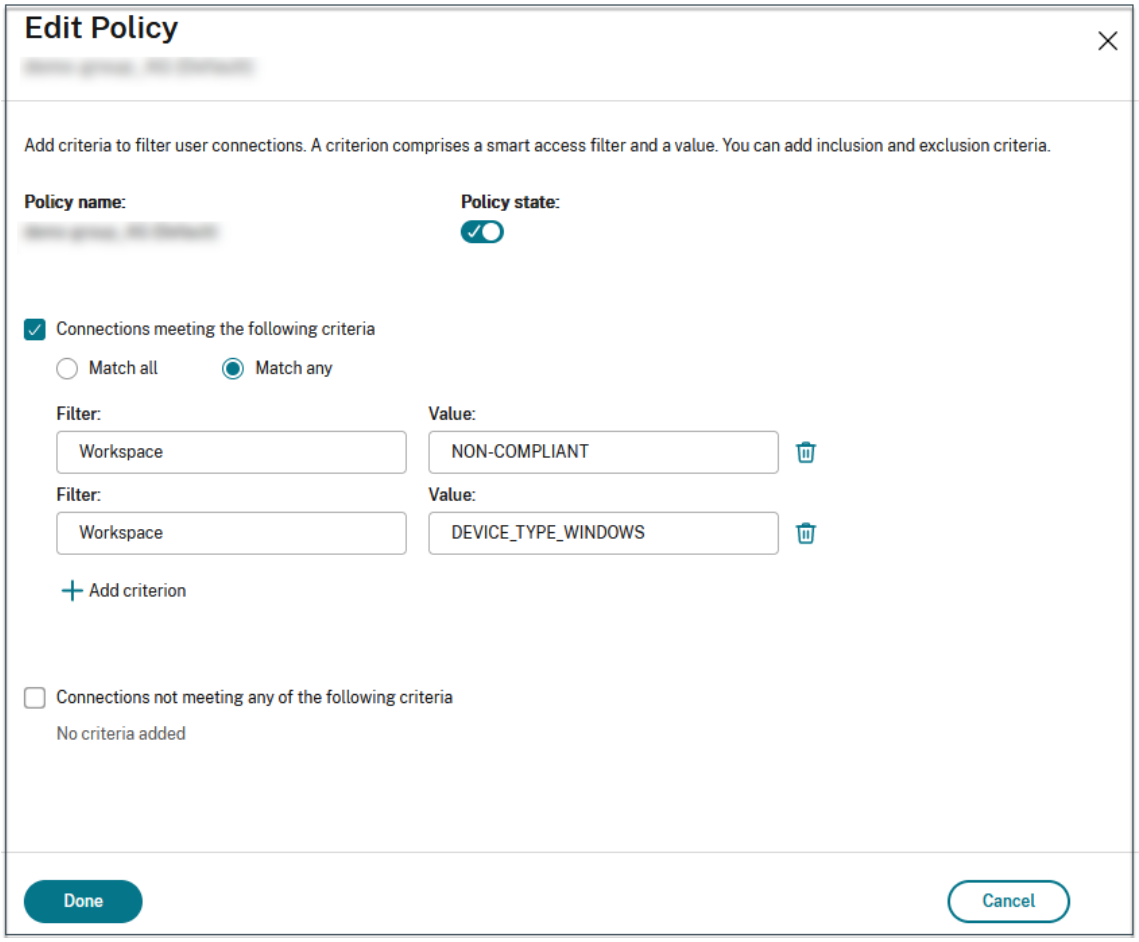
1. Inicie sesión en Citrix Cloud.
2. En el icono de **DaaS**, haga clic en **Administrar**.
3. Vaya a la sección **Grupos de entrega** en el menú de la izquierda.
4. Seleccione el grupo de entrega para el que quiere configurar el control de acceso en función de la postura del dispositivo y haga clic en **Modificar**.
5. En la página **Modificar grupo de entrega**, haga clic en **Directiva de acceso**.
6. Haga clic en el icono de edición de la fila de **conexiones de Citrix Gateway** para editar la política de conexiones de puerta de enlace.



   a) En la página Editar política, seleccione **Conexiones que cumplan los siguientes criterios.**

b) Seleccione **Coincidir con cualquiera** y, a continuación, haga clic en **Agregar criterio** .

c) Agregue criterios para todas las etiquetas de ubicación que configuró en Configurar ubicaciones de red: escriba **Workspace** para **Filter** y ****COMPLIANTo NONCOMPLIANT para **Value** .



Nota:

La sintaxis de las etiquetas de clasificación de dispositivos debe introducirse de la misma manera que se capturó anteriormente, es decir, en mayúsculas (**CONFORME** y **NO CONFORME**). De lo contrario, las directivas de postura del dispositivo no funcionan según lo previsto.

Además de las etiquetas de clasificación del dispositivo, el servicio Device Posture también devuelve la etiqueta del sistema operativo y la etiqueta de directiva de acceso asociadas al dispositivo. Las etiquetas del sistema operativo y las etiquetas de la directiva de acceso deben escribirse únicamente en mayúsculas.

- DEVICE_TYPE_WINDOWS
- DEVICE_TYPE_MAC

> - Nombre exacto de la directiva (en mayúsculas)

Configuración de Citrix Secure Private Access con Postura del dispositivo

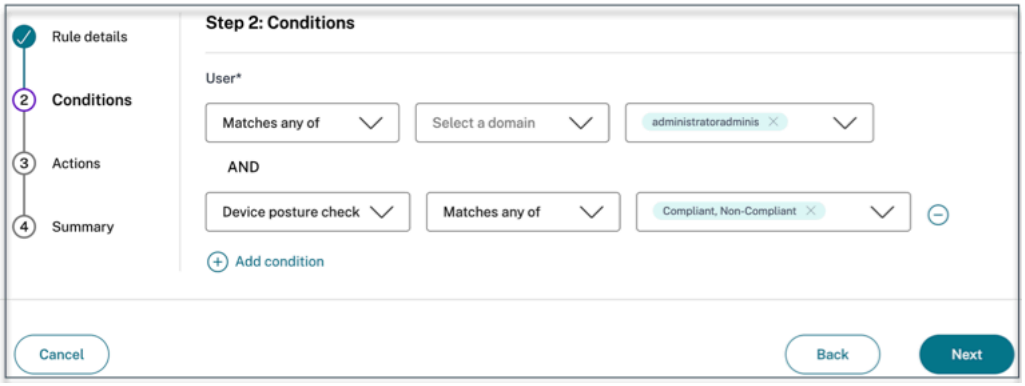
1. Inicie sesión en Citrix Cloud.
2. En el mosaico Acceso privado seguro, haga clic en **Administrar** .
3. Haga clic en **Directivas de acceso** en el menú de navegación de la izquierda y, a continuación, en **Crear directiva**.
4. Introduzca el nombre de la directiva y la descripción de la misma.
5. En **Aplicaciones**, seleccione la aplicación o el conjunto de aplicaciones en las que se debe aplicar esta directiva.
6. Haga clic en **Crear regla** para crear reglas para la directiva.
7. Introduzca el nombre de la regla y una breve descripción de la regla y, a continuación, haga clic en **Siguiente**.
8. Selecciona las condiciones de los usuarios. La condición de **usuario** es una condición obligatoria que debe cumplirse para conceder acceso a las aplicaciones a los usuarios.
9. Haga clic en **+** para agregar la condición de postura del dispositivo.
10. Seleccione **Verificación de postura del dispositivo** y la expresión lógica en el menú desplegable.
11. Introduzca uno de los siguientes valores en las etiquetas personalizadas:
    - Compatible : para dispositivos compatibles
    - No compatible : para dispositivos que no cumplen con las normas
12. Haga clic en **Siguiente**.
13. Seleccione las acciones que se deben aplicar en función de la evaluación de la condición y, a continuación, haga clic en **Siguiente**.

    La página de resumen muestra los detalles de la directiva.
14. Puede comprobar los detalles y hacer clic en **Finalizar**.

    Para obtener más información sobre la creación de directivas de acceso, consulte Configurar una directiva de acceso con varias reglas.

> **Nota:**
>
> Cualquier aplicación de Secure Private Access que no esté etiquetada como compatible o no compatible en la directiva de acceso se trata como la aplicación predeterminada y se puede acceder

> a ella en todos los terminales, independientemente de la posición del dispositivo.



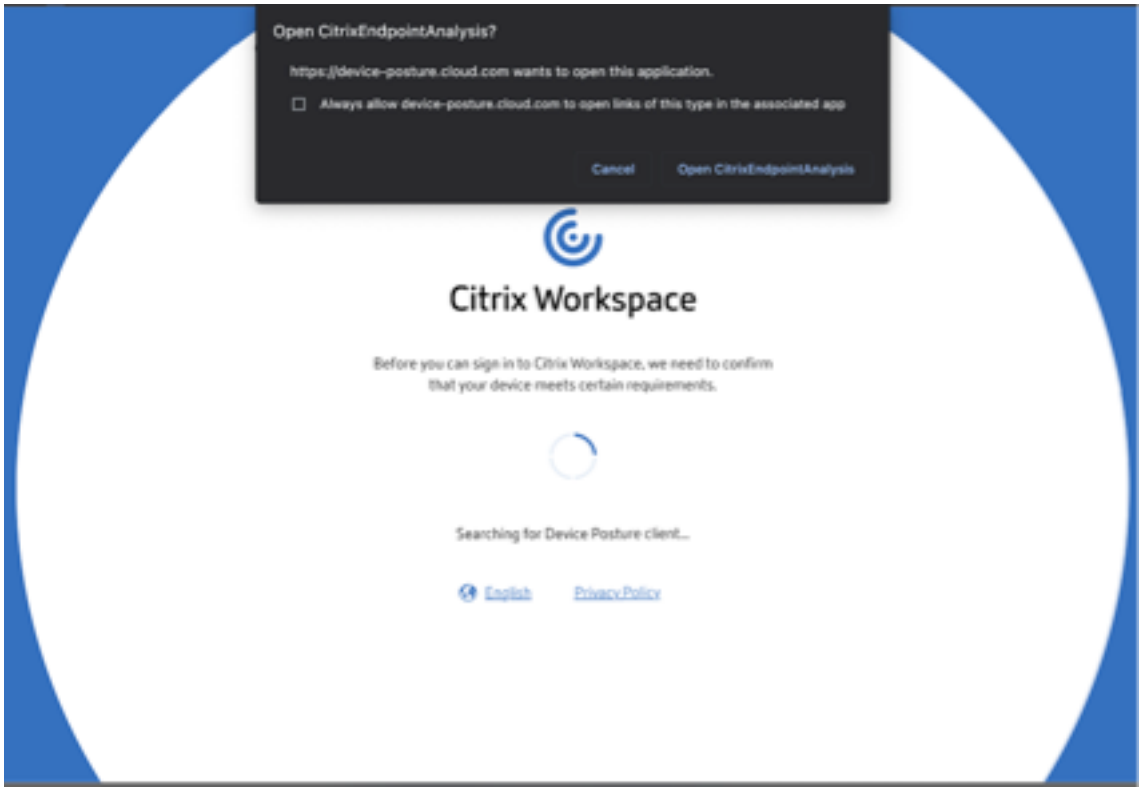
Flujo del usuario final

Una vez establecidas las directivas de postura del dispositivo y habilitada la postura del dispositivo, los siguientes son los flujos del usuario final en función de la forma en que el usuario final inicia sesión en Citrix Workspace.

Flujo de usuarios finales mediante acceso al explorador web

> **Nota:**
>
> El cliente macOS y el navegador Chrome se utilizan como ejemplo con fines ilustrativos. Las pantallas y las notificaciones varían según el cliente y el explorador web que utilice para acceder a la URL de Citrix Workspace.

- Cuando un usuario final inicia sesión en la URL de Citrix Workspace `https://<your-workspace-URL` a través de un explorador web, se le solicita que ejecute la aplicación Citrix Endpoint Analysis.



- Cuando el usuario final hace clic en **Abrir Citrix End Point Analysis**, el cliente de postura del dispositivo ejecuta y analiza los parámetros del punto final en función de los requisitos de la directiva de postura del dispositivo.
- Si el cliente de postura del dispositivo más reciente no está instalado en el terminal, se redirige a los usuarios a la página que muestra las opciones **Comprobar de nuevo** y **Descargar el cliente**. El usuario debe hacer clic en **Descargar cliente**.
- Si el último cliente de postura del dispositivo ya está instalado en el terminal, el usuario debe **volver a hacer clic en Comprobar.**

Flujo de usuarios finales a través de la aplicación Citrix Workspace

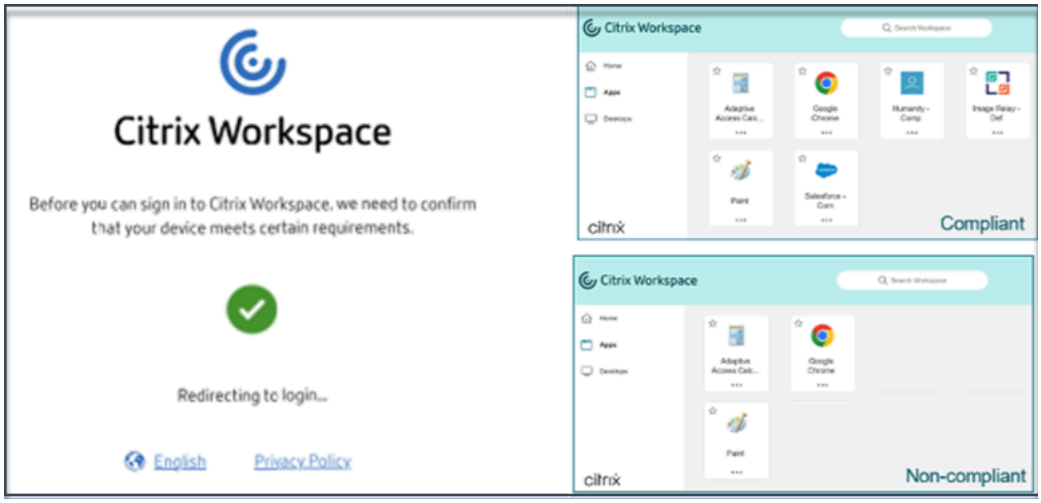
- Cuando un usuario final inicia sesión en la URL de Citrix Workspace `https://your-workspace-url` a través de la aplicación Citrix Workspace, el cliente de postura del dispositivo instalado en el extremo ejecuta y analiza los parámetros del punto final en función de los requisitos de la directiva de postura del dispositivo.
- Si el cliente de postura del dispositivo más reciente no está instalado en el terminal, se redirige a los usuarios a la página que muestra las opciones **Comprobar de nuevo** y **Descargar el cliente**. El usuario debe hacer clic en **Descargar cliente**.
- Si el último cliente de postura del dispositivo ya está instalado en el terminal, el usuario debe **volver a hacer clic en Comprobar.**

Flujo del usuario final: resultados de la postura del dispositivo

Según las condiciones de la directiva de postura del dispositivo, pueden darse tres posibilidades.

Si un punto final cumple con las condiciones de la directiva, por lo que el dispositivo se clasifica como;

- **Cumple con las normas**: El usuario final puede iniciar sesión con acceso sin restricciones a los recursos de Secure Private Access o Citrix DaaS.
- **No cumple**: El usuario final puede iniciar sesión con acceso restringido a los recursos de Secure Private Access o Citrix DaaS.



Si un punto final cumple las condiciones de la directiva, por lo que el dispositivo se clasifica como **Acceso denegado**, aparece el mensaje **Acceso denegado**.

Mensajes personalizados para escenarios de acceso denegado (versión preliminar) Los administradores tienen la opción de personalizar el mensaje que se muestra en el dispositivo final cuando se deniega el acceso.

Esta función está en versión preliminar. Regístrese para obtener la vista previa mediante https://podio.com/webforms/29219975/2385710.

Realice los siguientes pasos para agregar mensajes personalizados:

1. Navegue hasta la página **Postura del dispositivo > Escaneos** del dispositivo .
2. Haga clic en **Configuración**.

3. Haga clic en **Editary**, en el cuadro Mensaje , introduzca el mensaje que debe mostrarse en situaciones de acceso denegado. Puede introducir un máximo de 256 caracteres.
4. Haga clic **en Habilitar mensaje personalizado al guardar** para aplicar la opción de mostrar el mensaje personalizado. Si no selecciona esta casilla, el mensaje personalizado se crea pero no se muestra en los dispositivos en los escenarios de acceso denegado.

   Como alternativa, puede activar el interruptor de mensajes **personalizados** en la página de **configuración** para mostrar el mensaje en los dispositivos.
5. Haga clic en **Guardar**.

El mensaje que ha introducido aparece cada vez que se deniega el acceso al dispositivo final.

Supervise y solucione los eventos de postura del dispositivo

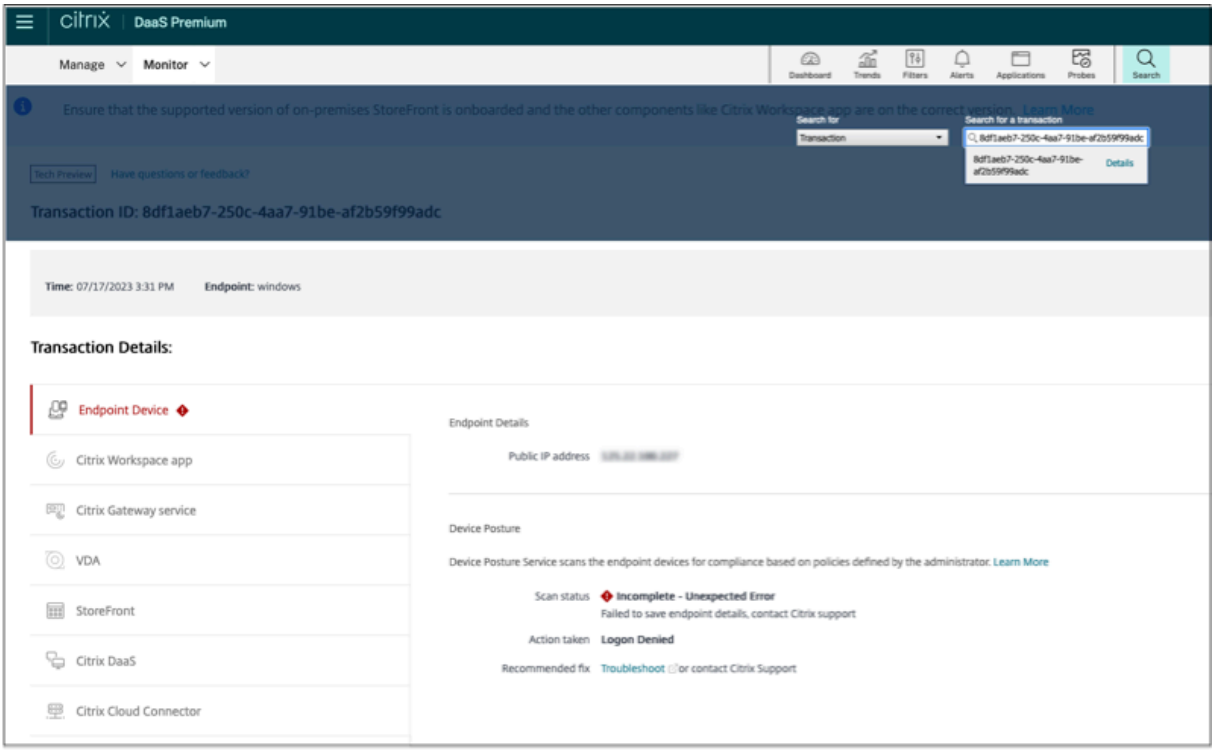
Los registros de eventos de postura del dispositivo se pueden ver en dos lugares:

- Monitor Citrix DaaS
- Panel de control de Citrix Secure Private Access

Eventos de postura del dispositivo en Citrix DaaS Monitor

Realice los siguientes pasos para ver los registros de eventos del servicio Device Posture.

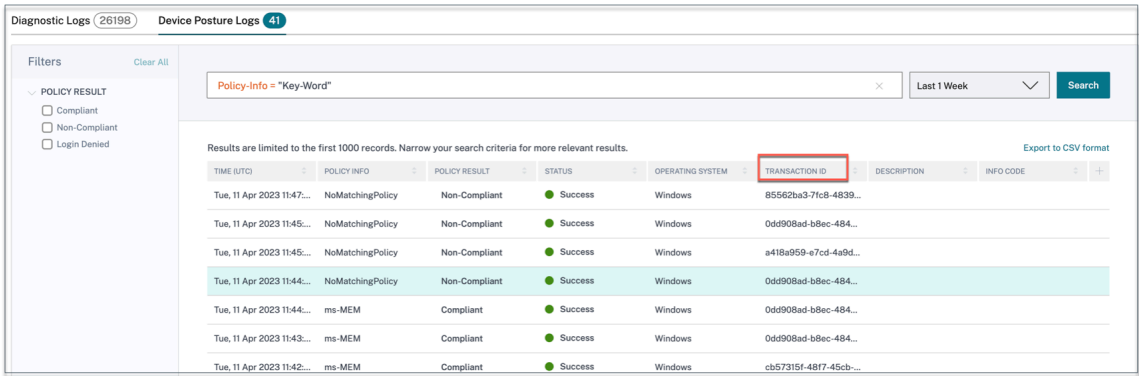
1. Copie el ID de transacción de la sesión fallida o de acceso denegado del dispositivo del usuario final.
2. Inicie sesión en Citrix Cloud.
3. En el mosaico DaaS, haga clic en **Administrar** y, a continuación, en la ficha **Supervisar**.
4. En la interfaz de usuario de Monitor, busque el ID de transacción de 32 dígitos y haga clic en **Detalles**.



Eventos de postura del dispositivo en el panel de Secure Private Access

Realice los siguientes pasos para ver los registros de eventos del servicio Device Posture.

1. Inicie sesión en Citrix Cloud.
2. En el mosaico Acceso privado seguro, haga clic en **Administrar** .
3. Vaya a la sección Panel de control en el menú de la izquierda.
4. Haga clic en el enlace **Ver más** del gráfico **Registros de diagnóstico** para ver los registros de eventos de postura del dispositivo.



- Los administradores pueden filtrar los registros en función del identificador de transacción del gráfico de **registros de diagnóstico**. El identificador de la transacción también se muestra al

usuario final cada vez que se deniega el acceso.

- Si hay un error o una falla en el escaneo, el servicio Device Posture muestra un ID de transacción. Este identificador de transacción está disponible en el panel del servicio Secure Private Access. Si los registros no ayudan a resolver el problema, los usuarios finales pueden compartir el ID de transacción con el soporte de Citrix para resolver el problema.

- Los registros de los clientes de Windows se encuentran en:
  - %localappdata%\Citrix\EPA\dpaCitrix.txt
  - %localappdata%\Citrix\EPA\epalib.txt
- Los registros de los clientes de macOS se encuentran en:
  - ~/Biblioteca/Aplicación Support/Citrix/EPAPlugin/EpaCloud.log
  - ~/Biblioteca/Application Support/Citrix/EPAPlugin/epaplugin.log

Registros de errores de postura del dispositivo

Los siguientes registros relacionados con el servicio Device Posture se pueden ver en el panel de control de Citrix Monitor y Secure Private Access. Para todos estos registros, se recomienda ponerse en contacto con el soporte de Citrix para obtener una solución.

- No se pudieron leer las directivas configuradas
- No se pudieron evaluar los escaneos de los terminales
- No se pudieron procesar las directivas/expresiones
- No se pudieron guardar los detalles del punto final
- No se pudieron procesar los resultados del escaneo de los puntos finales

Limitaciones conocidas

- Las URL de espacios de trabajo personalizadas no son compatibles con el servicio Device Posture.
- El tiempo necesario para activar o desactivar la función de postura del dispositivo después de activar o desactivar el botón de posicionamiento del dispositivo puede tardar entre unos minutos y una hora.
- Los cambios en la configuración de la postura del dispositivo no surtirán efecto inmediatamente. Los cambios pueden tardar unos 10 minutos en surtir efecto.
- Si ha activado la opción de continuidad del servicio en Citrix Workspace y Device Posture Service está inactivo, es posible que los usuarios no puedan iniciar sesión en Workspace. Esto se debe a que Citrix Workspace enumera las aplicaciones y los escritorios en función de la memoria caché local del dispositivo del usuario.
- Si ha configurado un token y una contraseña de larga duración en Citrix Workspace, el análisis de postura del dispositivo no funciona para esta configuración. Los dispositivos se escanean solo cuando los usuarios inician sesión en Citrix Workspace.
- Cada plataforma puede tener un máximo de 10 directivas y cada directiva puede tener un máximo de 10 reglas.
- El acceso basado en roles no es compatible con el servicio Device Posture.

Calidad del servicio

- Rendimiento: en condiciones ideales, el servicio Device Posture agrega 2 segundos adicionales de retraso durante el inicio de sesión. Este retraso puede aumentar en función de las configuraciones adicionales, como las integraciones de terceros, como Microsoft Intune.
- Resiliencia: el servicio Device Posture es muy resistente con varios POP para garantizar que no haya tiempo de inactividad.

Definiciones

Los términos compatible y no compatible en referencia al servicio Device Posture se definen de la siguiente manera.

- **Dispositivos compatibles**: Dispositivo que cumple con los requisitos de directiva preconfigurados y que puede iniciar sesión en la red de la empresa con acceso total o sin restricciones a los recursos de Citrix Secure Private Access o a los recursos de Citrix DaaS.
- **Dispositivos no compatibles**: Dispositivo que cumple con los requisitos de directiva preconfigurados y que puede iniciar sesión en la red de la empresa con acceso parcial o restringido a los recursos de Citrix Secure Private Access o a los recursos de Citrix DaaS.

Integración de CrowdStrike con Device Posture - Vista previa

February 16, 2024

La evaluación de confianza cero (ZTA) de CrowdStrike proporciona evaluaciones de la postura de seguridad mediante el cálculo de una puntuación de seguridad de ZTA de 1 a 100 para cada dispositivo final. Una puntuación ZTA más alta significa que la postura del dispositivo final es mejor.

Citrix Device Posture Service puede habilitar el acceso contextual (Smart Access) a los recursos de Citrix Desktop as a Service (DaaS) y Citrix Secure Private Access (SPA) mediante el uso de la puntuación ZTA de un dispositivo final.

Los administradores de Device Posture pueden usar la puntuación ZTA como parte de las directivas y clasificar los dispositivos finales como conformes, no conformes (acceso parcial) o incluso denegar el acceso. A su vez, las organizaciones pueden utilizar esta clasificación para proporcionar acceso contextual (Smart Access) a aplicaciones y escritorios virtuales, y a aplicaciones web y SaaS. Las directivas de puntuación ZTA son compatibles con las plataformas Windows y macOS.

Configurar la integración de CrowdStrike

La configuración de la integración de CrowdStrike es un proceso de dos pasos.

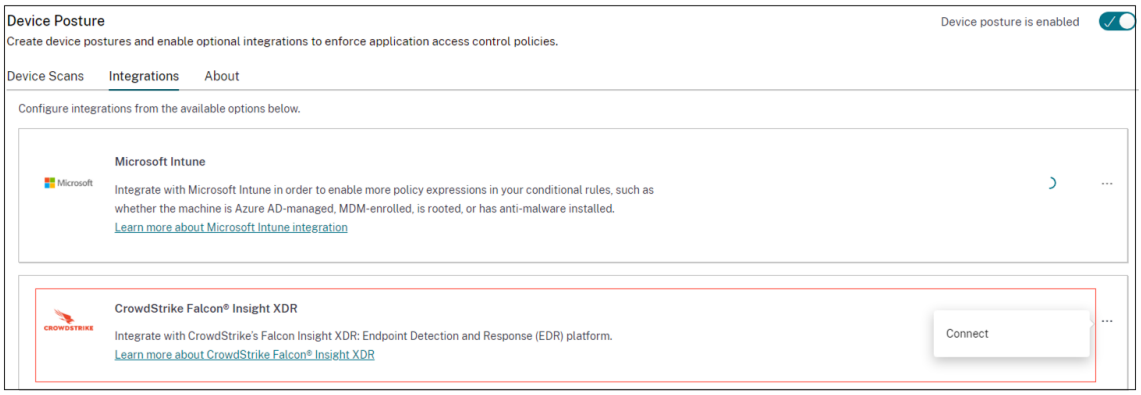
Paso 1: Establecer la confianza entre el servicio Citrix Device Posture y el servicio CrowdStrike ZTA. Se trata de una actividad que se realiza una sola vez.

Paso 2: Configure las directivas para utilizar la puntuación ZTA de CrowdStrike como regla para proporcionar un acceso inteligente a los recursos de Citrix DaaS y Citrix Secure Private Access.

Paso 1: Establecer la confianza entre el servicio Citrix Device Posture y el servicio CrowdStrike ZTA

Realice lo siguiente para establecer la confianza entre el servicio Citrix Device Posture y el servicio CrowdStrike ZTA.

1. Inicie sesión en Citrix Cloud y, a continuación, seleccione **Administración de acceso e identidad** en el menú de hamburguesas.
2. Haga clic en la ficha **Device Posture** y, a continuación, en **Administrar**.
3. Haga clic en la ficha **Integraciones**.



> **Nota:**
>
> Como alternativa, los clientes pueden ir a la opción **Device Posture** en el panel de navegación izquierdo de la GUI del servicio Secure Private Access y, a continuación, hacer clic en la ficha **Integraciones**.

4. Haga clic en el botón de puntos suspensivos del cuadro de CrowdStrike y, a continuación, haga clic en **Conectar**. Aparece el panel de integración de CrowdStrike Falcon Insight XDR.
5. Introduzca el ID de cliente y el secreto del cliente y, a continuación, haga clic en **Guardar**.

> **Nota:**
>
> - Puede obtener el ID de cliente y el secreto de cliente de la API de ZTA en el portal de CrowdStrike (**Soporte y recursos > Clientes y claves de la API**).
> - Asegúrese de seleccionar la **evaluación de confianza cero** y los ámbitos de **host** con permisos de lectura para establecer la confianza.

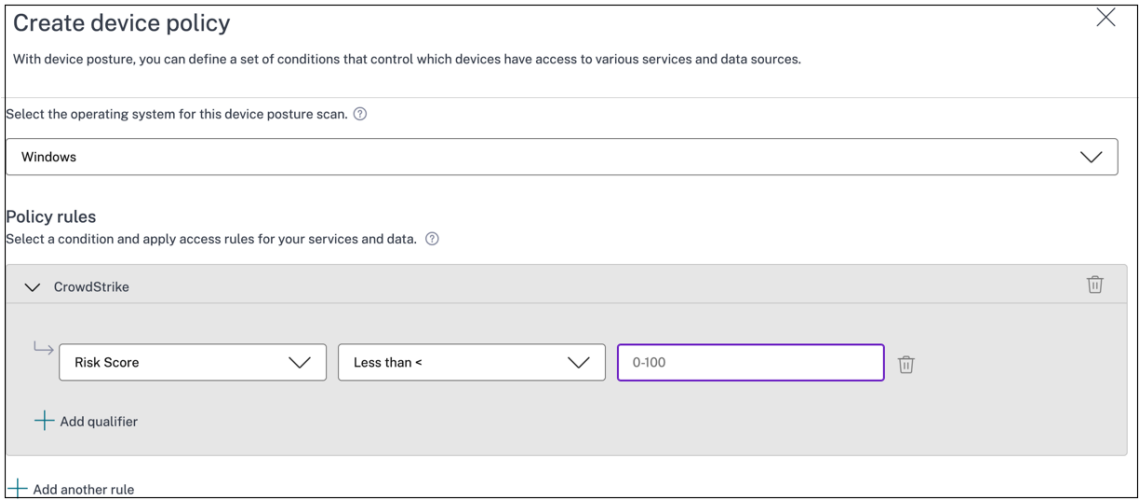
La integración se considera exitosa después de que el estado cambie de **No configuradoa Configurado**.

Si la integración no se realiza correctamente, el estado aparece como **Pendiente**. Debe hacer clic en el botón de puntos suspensivos y, a continuación, en **Reconectar**.

Paso 2: Configure directivas de Posición de dispositivo

Realice lo siguiente para configurar directivas que utilicen la puntuación ZTA de CrowdStrike como regla para proporcionar un acceso inteligente a los recursos de Citrix DaaS y Citrix Secure Private Access.

1. Haga clic en la ficha **Escaneos de dispositivos** y, a continuación, en **Crear directiva de dispositivos**.

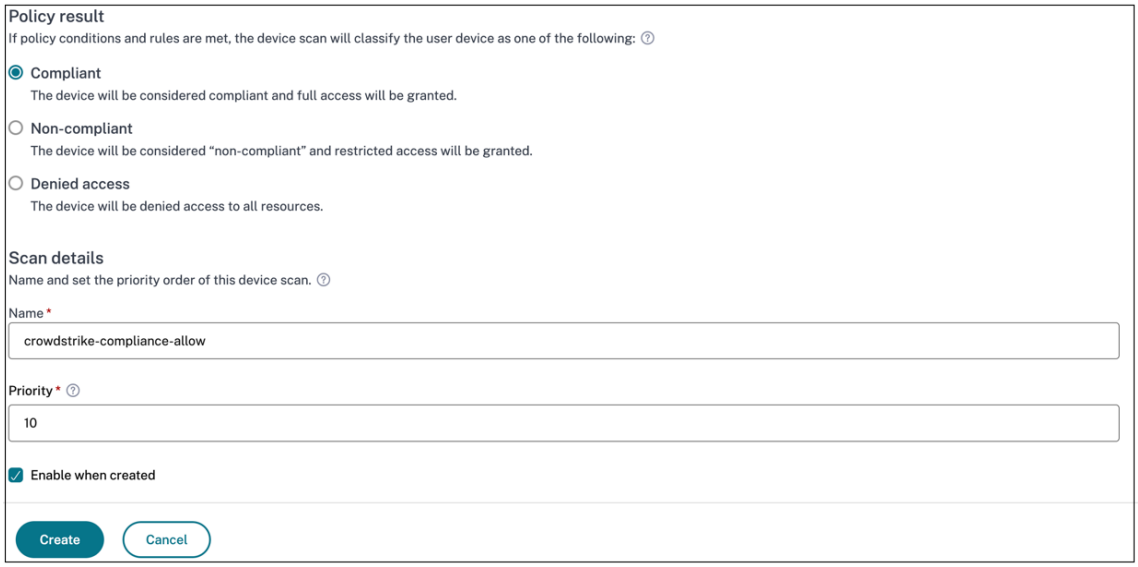


2. Seleccione la plataforma para la que se creó esta directiva.
3. En **Policy Rule**, selecciona **CrowdStrike**.
4. Para el calificador de **puntuación de riesgo**, seleccione la condición y, a continuación, introduzca la puntuación de riesgo.
5. Haga clic en **+** para agregar un calificador que compruebe si el sensor CrowdStrike Falcon está funcionando.

   > **Nota:**
   >
   > Puede usar esta regla con otras reglas que configure para Postura del dispositivo.

6. En **Resultado de la directiva** basado en las condiciones que haya configurado, seleccione una de las siguientes opciones.

   - **Conforme**
   - **No cumple**
   - **Inicio de sesión denegado**



7. Introduzca el nombre de la directiva y defina la prioridad.
8. Haga clic en **Crear**.

Definiciones

Los términos compatible y no conforme en referencia al servicio Device Posture se definen de la siguiente manera.

- Dispositivos compatibles: Dispositivo que cumple con los requisitos de directiva preconfigurados y que puede iniciar sesión en la red de la empresa con acceso total o sin restricciones a los recursos de Citrix Secure Private Access o a los recursos de Citrix DaaS.
- Dispositivos no compatibles: Dispositivo que cumple con los requisitos de directiva preconfigurados y que puede iniciar sesión en la red de la empresa con acceso parcial o restringido a los recursos de Citrix Secure Private Access o a los recursos de Citrix DaaS.

Referencias

Servicio de postura del dispositivo

Integración de Microsoft Intune con Device Posture

February 16, 2024

Microsoft Intune clasifica el dispositivo de un usuario como compatible o registrado en función de su configuración de directivas. Durante el inicio de sesión del usuario en Citrix Workspace, la postura del dispositivo puede comprobar con Microsoft Intune el estado del dispositivo del usuario y utilizar esta información para clasificar los dispositivos de Citrix Cloud como compatibles, no conformes (acceso parcial) o incluso denegar el acceso a la página de inicio de sesión del usuario. Los servicios como Citrix DaaS y Citrix Secure Private Access, a su vez, utilizan la clasificación de los dispositivos según Postura del dispositivo para proporcionar acceso contextual (Smart Access) a aplicaciones y escritorios virtuales y a aplicaciones SaaS y web, respectivamente.

Para configurar la integración de Microsoft Intune

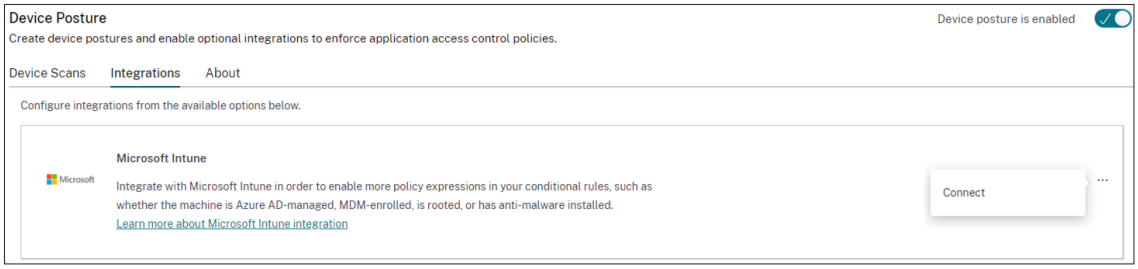
La configuración de la integración de Intune es un proceso de dos pasos.

Paso 1: Integre la postura del dispositivo con el servicio Microsoft Intune. Se trata de una actividad que se realiza una sola vez para establecer la confianza entre Device Posture y Microsoft Intune.

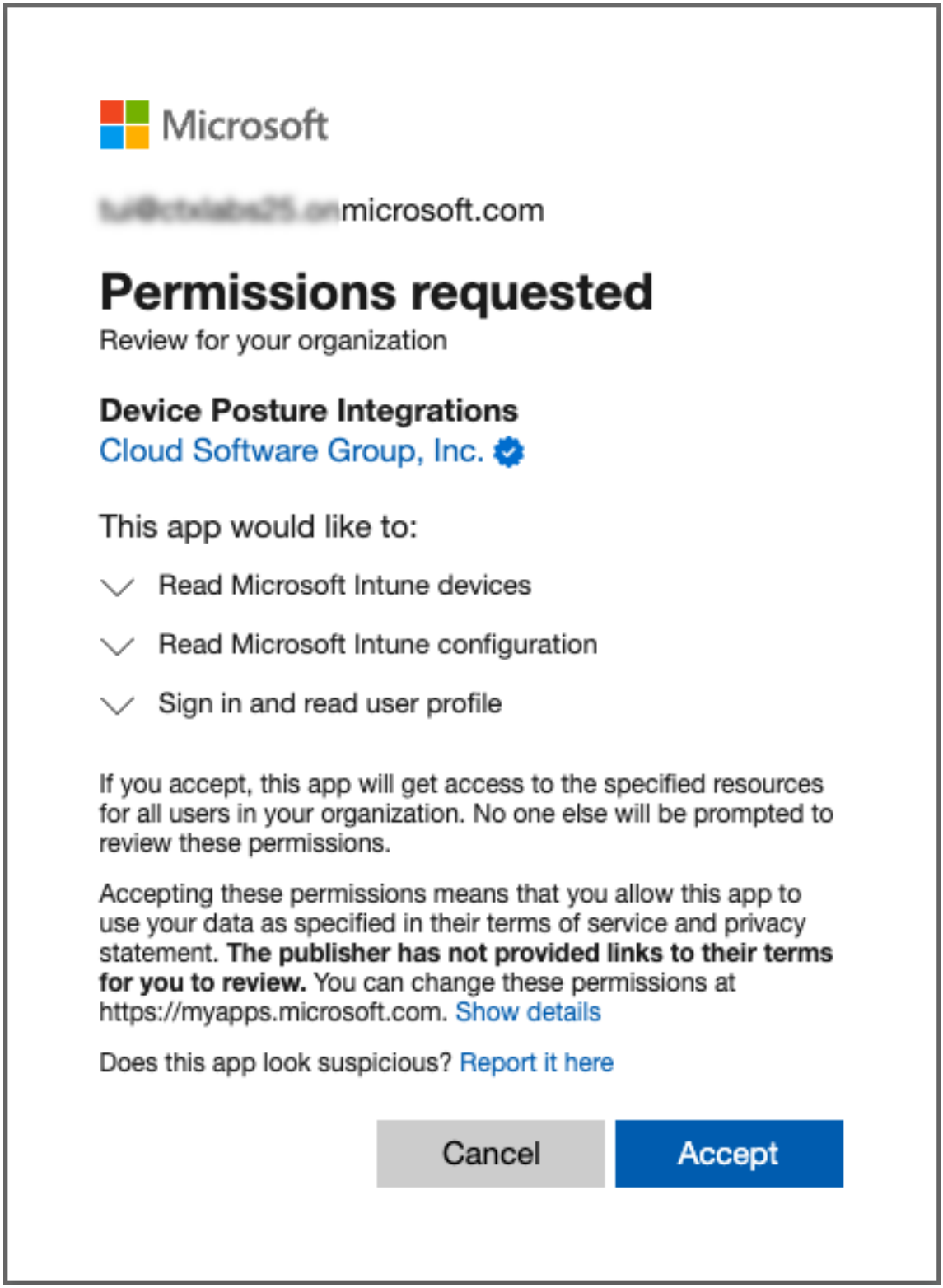
Paso 2: Configure las directivas para usar la información de Microsoft Intune.

Paso 1: Integrar la postura del dispositivo con Microsoft Intune

1. Para acceder a la ficha **Integraciones**, utilice uno de los métodos siguientes:
   - Acceda a la URL https://device-posture-config.cloud.com en su explorador web y, a continuación, haga clic en la ficha **Integraciones**.
   - Clientes de Secure Private Access: En la GUI de Secure Private Access, en el panel de navegación del lado izquierdo, haga clic en **Device Posture** y, a continuación, en la ficha **Integraciones**.



2. Haga clic en el botón de **puntos suspensivos** y, a continuación, en **Conectar**. Se redirige al administrador a Azure AD para autenticarse.



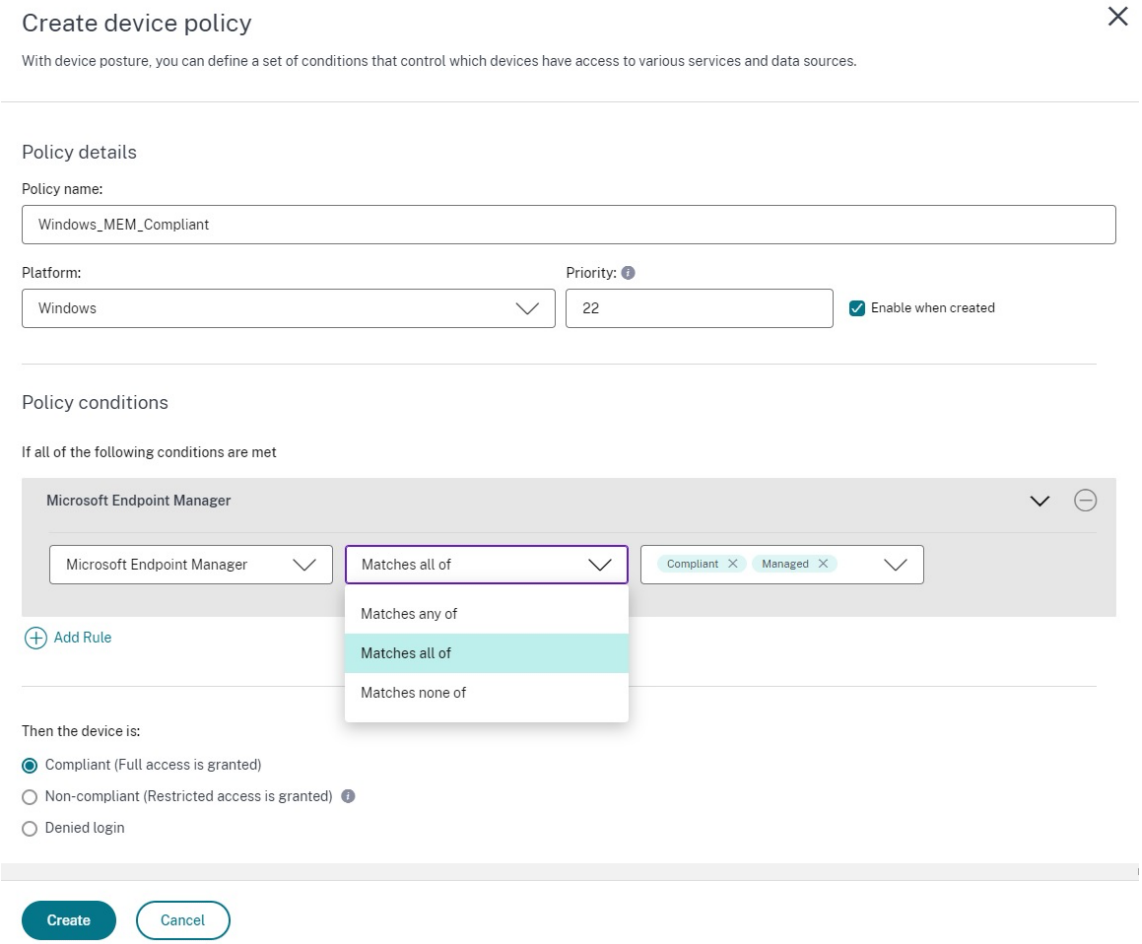
Cuando el estado de integración cambie de **No configurado** a **Configurado**, los administradores pueden crear una directiva de Posición de dispositivo.

Si la integración no se realiza correctamente, el estado aparece como **Pendiente**. Debe hacer clic en

los **puntos suspensivos** y, a continuación, en **Reconectar**.

Paso 2: Configure directivas de Posición de dispositivo

1. Haga clic en la ficha **Escaneos de dispositivos** y, a continuación, en **Crear directiva de dispositivos**.



2. Introduzca el nombre de la directiva y defina la prioridad.
3. Seleccione la plataforma para la que se creó esta directiva.
4. En **Seleccionar regla**, seleccione **Microsoft Endpoint Manager**.
5. Seleccione una condición y, a continuación, seleccione las etiquetas MEM que quiera cotejar.
   - **Para cotejar "cualquiera"**, se aplica una condición OR.
   - **Para cotejar "todo"**, se aplica la condición AND.

> **Nota:**
>
> Puede usar esta regla con otras reglas que configure para Postura del dispositivo.

6. En **Entonces, el dispositivo está:** según las condiciones que haya configurado, seleccione una de las siguientes opciones.
   - **Conforme (se concede acceso completo)**
   - **No conforme (se concede un acceso restringido)**
   - **Inicio de sesión denegado**

Para obtener más información sobre la creación de una directiva, consulte Configurar la directiva de postura del dispositivo.

Verificación del certificado del dispositivo con el servicio Device Posture

February 16, 2024

Para configurar las comprobaciones de certificados de dispositivos con el servicio Device Posture, los administradores deben importar un certificado de emisor desde su dispositivo. Una vez que haya un certificado de emisor válido en el servicio Device Posture, los administradores pueden utilizar las comprobaciones de certificados del dispositivo como parte de las directivas de postura del dispositivo.

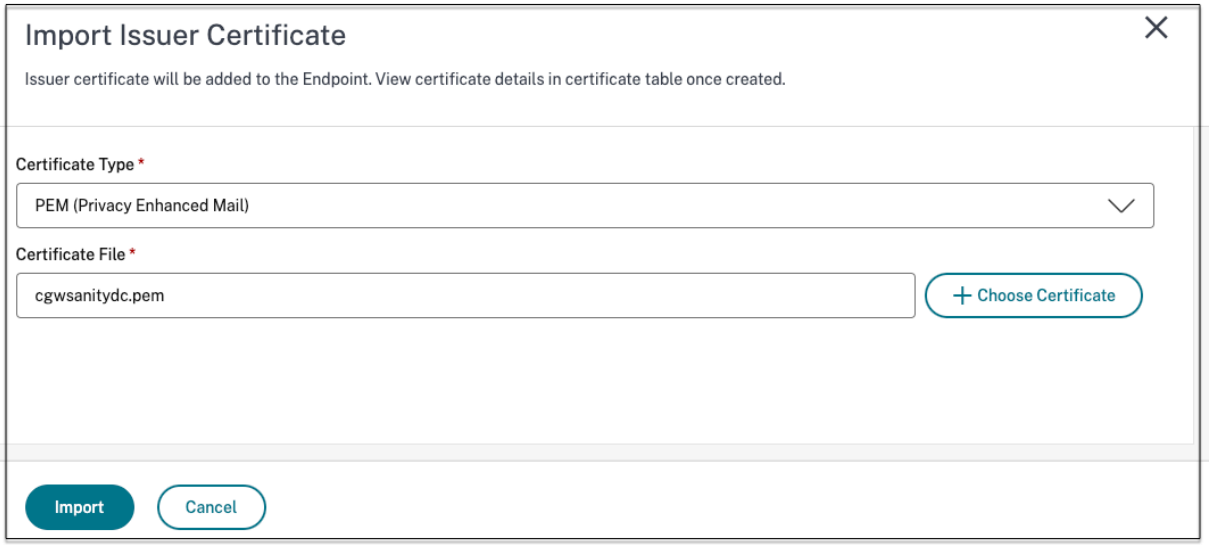
> **Puntos a tener en cuenta:**
>
> - El servicio Device Posture solo admite el tipo de certificado de emisor PEM.
> - Para comprobar el certificado del dispositivo en Windows, el cliente EPA del dispositivo final debe estar instalado con derechos administrativos. Para otras comprobaciones, no necesita los derechos administrativos locales. Para obtener más información sobre los escaneos compatibles, consulte Escaneos compatibles con la postura del dispositivo.
> - Para instalar el cliente EPA con derechos administrativos en Windows, ejecute el siguiente comando en la ubicación en la que se descarga el complemento del cliente EPA.
>
>  ```
>  msiexec /i epasetup.msi
>  ```
>
> - La verificación del certificado del dispositivo con el servicio Device Posture no admite la verificación de revocación del certificado.
> - Si un certificado de dispositivo está firmado por un certificado intermedio, debe cargar la cadena completa que contiene los certificados raíz e intermedio en un único archivo PEM.
>
>  ```
>  Example: chain.pem
>  ```



```
2
3 -----BEGIN CERTIFICATE-----
4 ****************************
5 -----END CERTIFICATE-----
6 -----BEGIN CERTIFICATE-----
7 ****************************
8 -----END CERTIFICATE
```

Cargar certificado de dispositivo

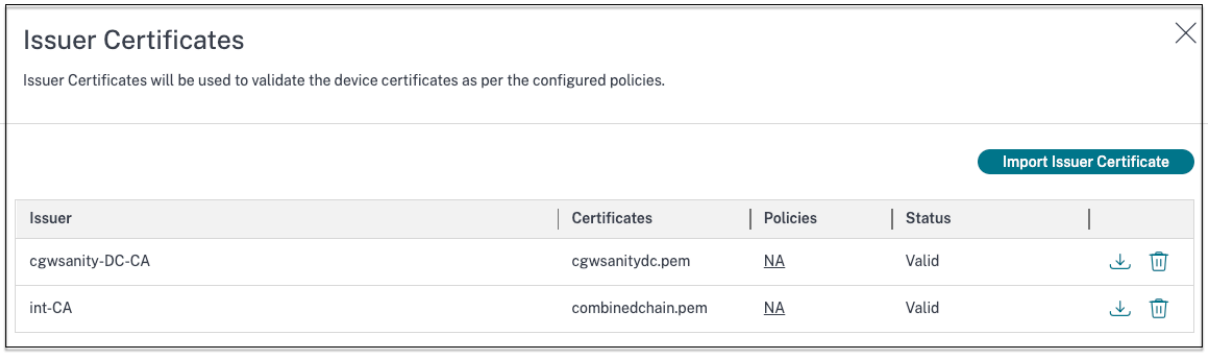
1. Haga clic en **Configuración** en la página de inicio de Device Posture.
2. Haga clic en **Administrar**y, a continuación, en **Importar certificado de emisión**.
3. En **Tipo de certificado**, seleccione el tipo de certificado. Solo se admite el tipo PEM.
4. En **Archivo de certificado**, haga clic en **Elegir certificado** para seleccionar el certificado del emisor.
5. Haga clic en **Abrir**y, a continuación, en **Importar**.



El certificado seleccionado aparece en **Configuración > Certificados del emisor**. Puede importar varios certificados.

Ver certificados importados

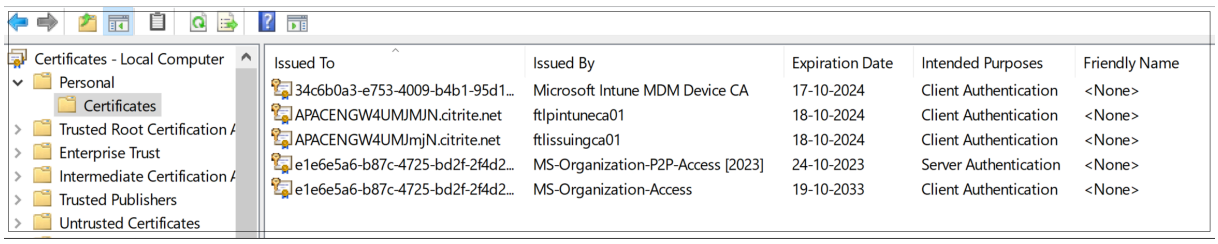
1. Haga clic en **Configuración** en la página de inicio de Device Posture.
2. En **Certificados de emisor**, haga clic en **Administrar**.
3. La página de certificados de emisor muestra los certificados de emisor importados.



Instale el certificado de dispositivo en el dispositivo final

Windows:

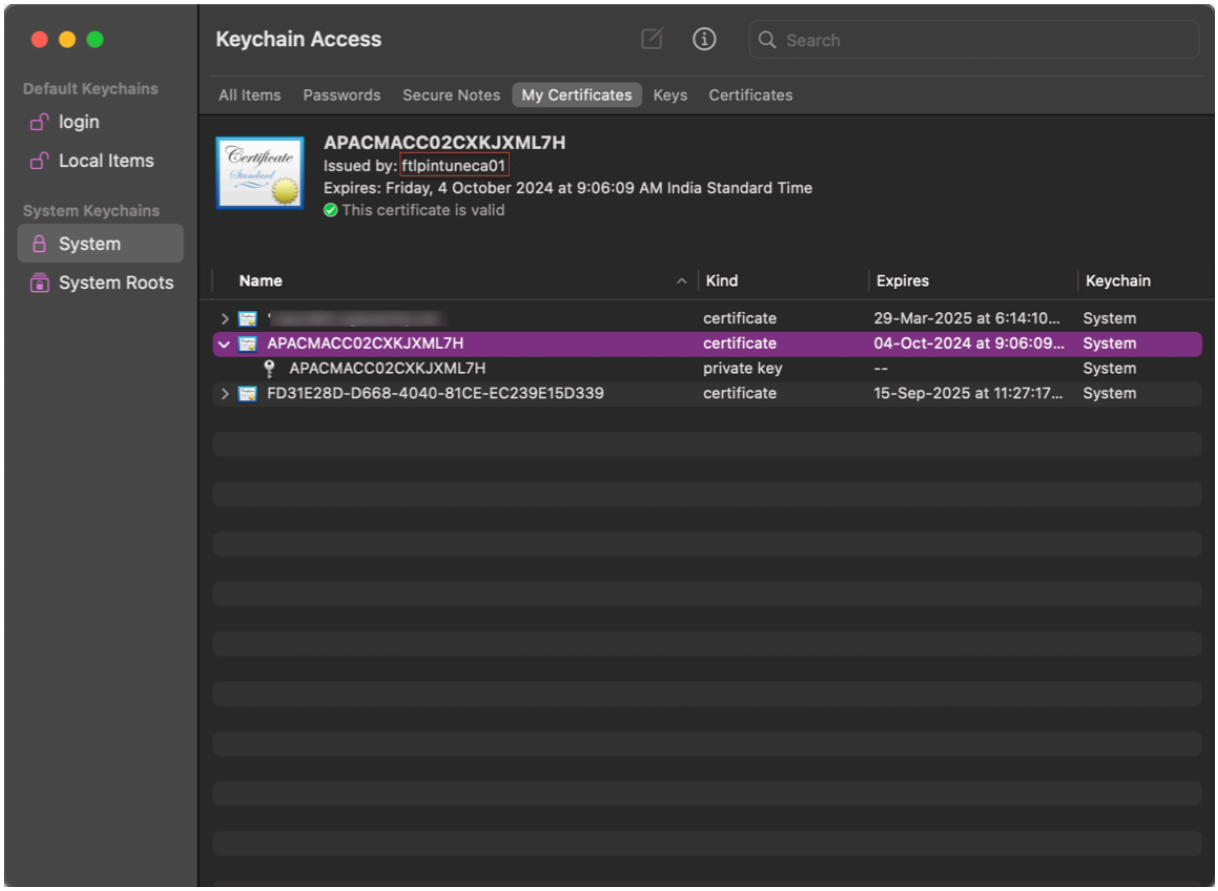
1. En el menú **Inicio**, abra el **Administrador de certificados de equipo**.
2. Asegúrese de que el certificado esté instalado en `Certificates - Local Computer\Personal\Certificates`.
   - Los **fines previstos** deben incluir la **autenticación del cliente**.
   - La columna **Emitido por** debe coincidir con el nombre del emisor configurado en la GUI del administrador.



macOS:

1. Abra **Keychain Access** y, a continuación, seleccione **Sistema**.
2. Haga clic en **Archivo > Importar elementos** para importar el certificado.

   El campo **Emitido por** debe mostrar el nombre del emisor del certificado.



Imponga controles inteligentes en DaaS mediante Device Posture

February 16, 2024

Puede aplicar controles inteligentes al acceder a los recursos de Citrix Desktop as a Service (DaaS) a través del servicio Citrix Device Posture.

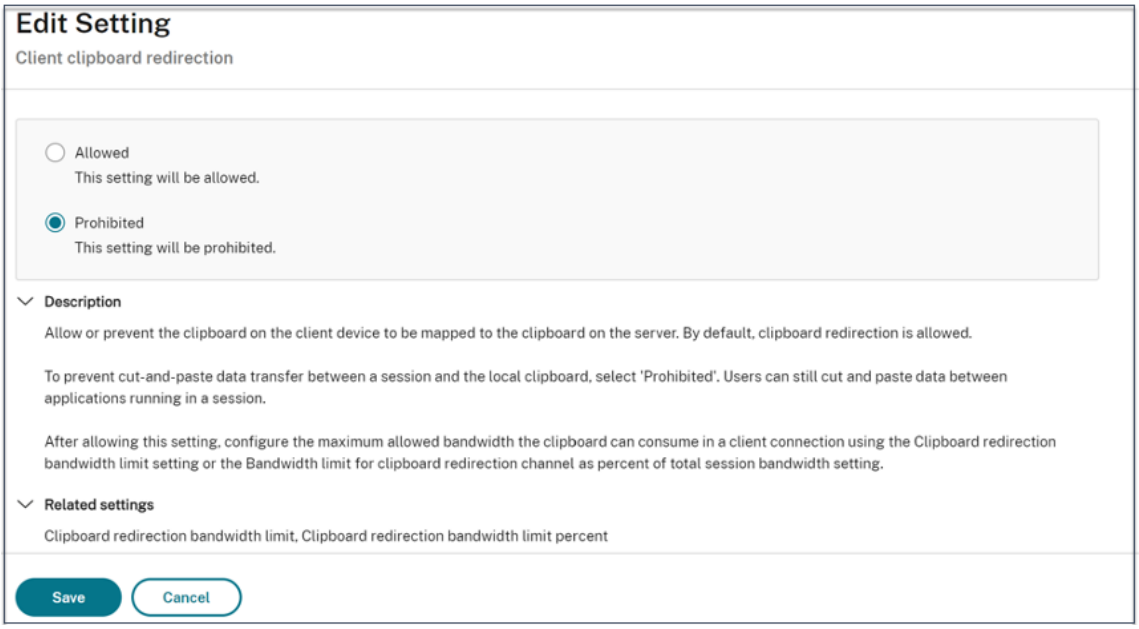
> **Nota:**
>
> Esta no es una configuración exhaustiva, sino un ejemplo de cómo usar Device Posture para configurar las directivas de Studio.

En este ejemplo, se crea una directiva para inhabilitar la función de copiar y pegar en los recursos de Citrix DaaS mediante las etiquetas del servicio Device Posture (COMPLIANT y NON-COMPLIANT).

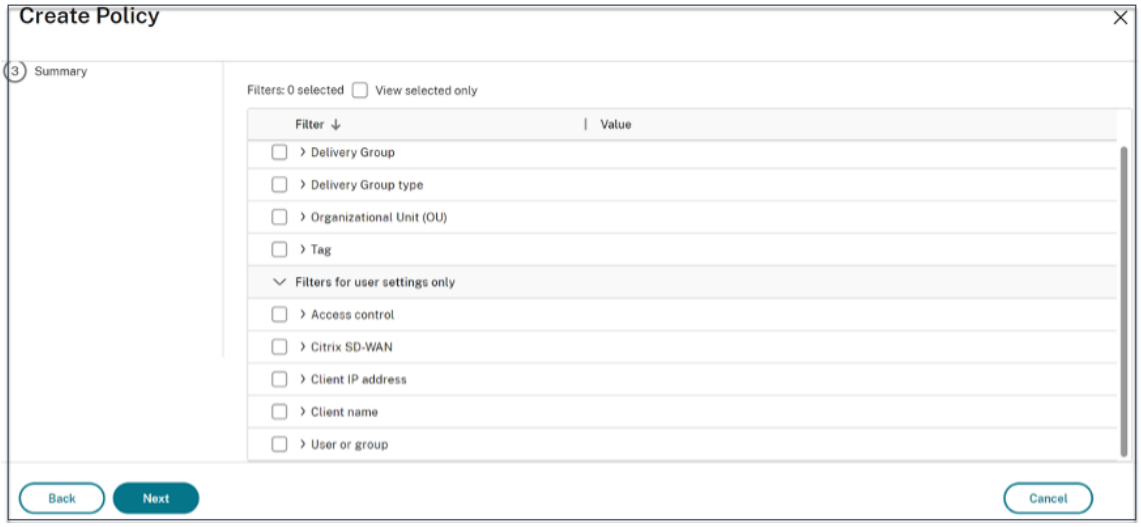
Para inhabilitar la función de copiar y pegar para los usuarios que provienen de un dispositivo NO COMPATIBLE en Citrix DaaS, lleve a cabo los siguientes pasos:

1. En la página de configuración de Citrix DaaS, haga clic en la ficha **Administrar**.

2. Haga clic en la ficha **Directivas**.
3. Seleccione **Crear directiva**.
4. En **Seleccionar configuración**, seleccione **Redirección del portapapeles del cliente**.
5. En **Editar configuración**, seleccione **Prohibido**y, a continuación, haga clic en **Guardar**.

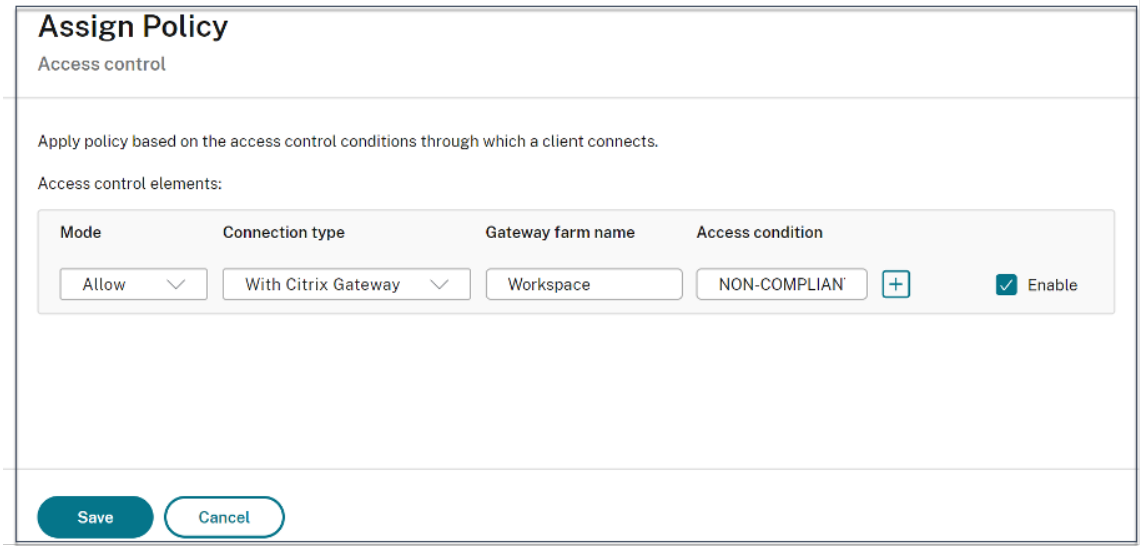


6. En la página **Usuarios y máquinas**, haga clic en **Usuarios y equipos filtrados y**, a continuación, asigne esta directiva a **Control de acceso**.
7. Vaya a **Filtrar solo para la configuración de usuario** y seleccione **Control de acceso**.



8. En la página **Asignar directiva**, deje la configuración predeterminada para el **modo y eltipo de conexión**.

En **Nombre de comunidad de Gateway**, escriba **Espacio de trabajo** y, en **Condición de acceso**, escriba **NO COMPATIBLE**.



9. Introduzca un nombre para la directiva. Considere la posibilidad de asignar un nombre a la directiva en función de a quién o a qué afecta, por ejemplo, *acceso restringido al portapapeles para dispositivos no compatibles*. Si lo desea, puede proporcionar una descripción.
10. Haz clic en **Finalizar.**

> **Nota:**
>
> La directiva está inhabilitada de forma predeterminada. Al habilitar la directiva, se puede aplicar inmediatamente a los usuarios que inicien sesión. Si se inhabilita, la directiva no se aplica. Si necesita establecer la prioridad de una directiva o agregar configuraciones en otro momento, puede inhabilitar la directiva hasta que esté listo para aplicarla.

Cómo validar una configuración de directiva

Valide sus directivas para asegurarse de que funcionan según lo previsto antes de implementarlas ampliamente. En el ejemplo de configuración:

- Para los usuarios que provienen de un dispositivo final COMPATIBLE, los recursos de Citrix DaaS deben enumerarse sin las restricciones de copiar y pegar.
- Para los usuarios que provienen de un dispositivo final NO COMPATIBLE, los recursos de Citrix DaaS se deben enumerar con las restricciones de copiar y pegar.

Registros de postura del dispositivo

February 16, 2024

El panel del servicio Secure Private Access captura los registros de postura del dispositivo, además de los registros relacionados con las aplicaciones SaaS/Web y TCP/UDP.

Para ver los registros de postura del dispositivo, haga clic en la pestaña **Registros de postura del dispositivo** . Puede refinar la búsqueda en función de los resultados de la política (**compatible, no compatible e inicio de sesión denegado**).

Para obtener más información, consulte Registros de diagnóstico.

Administrar el cliente Citrix Endpoint Analysis para el servicio Device Posture

February 16, 2024

El servicio Citrix Device Posture es una solución basada en la nube que ayuda a los administradores a cumplir ciertos requisitos que los dispositivos finales deben cumplir para acceder a los recursos de Citrix DaaS (aplicaciones y escritorios virtuales) o Citrix Secure Private Access (SaaS, aplicaciones web, TCP y UDP).

Para ejecutar escaneos de postura del dispositivo en un dispositivo final, debe instalar el cliente Citrix EndPoint Analysis (EPA), que es una aplicación ligera, en ese dispositivo. El servicio Device Posture siempre se ejecuta con la última versión del cliente EPA publicada por Citrix.

Instalación del cliente EPA

Durante el tiempo de ejecución, el servicio Device Posture solicita al usuario final que descargue e instale el cliente EPA durante el tiempo de ejecución. Para obtener más información, consulte Flujo de usuario final.
Por lo general, un cliente de la EPA no requiere derechos de administrador local para descargar e instalar en un punto final. Sin embargo, para ejecutar escaneos de verificación de certificados de dispositivos en un dispositivo final, el cliente EPA debe estar instalado con acceso de administrador. Para obtener más información sobre la instalación del cliente EPA con acceso de administrador, consulte Instalar el certificado del dispositivo en el dispositivo final.

Actualización del cliente EPA para Windows

Cuando se publica una nueva versión del cliente EPA, los clientes EPA para Windows se actualizan de forma predeterminada después de la primera instalación. La actualización automática garantiza que los dispositivos de los usuarios finales siempre se ejecuten en la versión más reciente del cliente EPA que sea compatible con el servicio Device Posture. Para la actualización automática, el cliente EPA debe haberse instalado con acceso de administrador.

> **Nota:**
>
> La actualización automática se encuentra actualmente en versión preliminar. Regístrese para obtener la vista previa mediante https://podio.com/webforms/29214695/2384946.

Distribución del cliente de la EPA

Los clientes de la EPA se pueden distribuir mediante el servicio de configuración global de aplicaciones (GACS) o la EPA integrada con el instalador de la aplicación Citrix Workspace, o mediante herramientas de implementación de software.

- **Cliente EPA integrado con la aplicación Citrix Workspace (versión preliminar):**el cliente EPA también está integrado con la aplicación Citrix Workspace. Esta integración elimina la necesidad de que los usuarios finales instalen el cliente EPA después de instalar la aplicación Citrix Workspace.
  - Si un dispositivo final ya tiene un cliente EPA instalado y el usuario final instala la aplicación Citrix Workspace, el cliente EPA integrado no está instalado en ese dispositivo. El cliente de la EPA existente se utiliza para comprobar la postura del dispositivo.
  - Del mismo modo, si el usuario final desinstala la aplicación Citrix Workspace, el cliente EPA integrado también se elimina del dispositivo de forma predeterminada. Sin embargo, si el cliente EPA no se instaló como parte de la instalación integrada de la aplicación Citrix Workspace, el cliente EPA existente se conserva en el dispositivo.

> **Nota:**
>
> - La integración del cliente EPA con la aplicación Citrix Workspace solo se admite en la plataforma Windows y está en versión preliminar. Regístrese para obtener la vista previa mediante https://podio.com/webforms/29219973/2385708.

- **Distribuya el cliente mediante GACS**: GACS es una solución proporcionada por Citrix para gestionar la distribución de agentes del lado del cliente (complementos). El servicio de actualización automática disponible en GACS garantiza que los dispositivos finales estén en las últimas versiones de la EPA sin la intervención del usuario final. Para obtener más información sobre el GACS, consulte ¿Cómo utilizar el servicio de configuración global de aplicaciones?

> **Nota:**
>
> - El GACS solo es compatible con los dispositivos Windows para la distribución del cliente EPA.
> - Para administrar un cliente EPA a través de GACS, instale la aplicación Citrix Workspace (CWA) en los dispositivos finales.
> - Si CWA se instala con privilegios de administrador en un dispositivo de usuario final, GACS instala el cliente EPA con los mismos privilegios de administrador.
> - Si CWA se instala con privilegios de usuario en un dispositivo de usuario final, GACS instala el cliente EPA con los mismos privilegios de usuario.

Distribuya el cliente mediante herramientas de implementación de software: los administradores pueden distribuir el cliente EPA más reciente a través de herramientas de implementación de software como Microsoft SCCM.

Administre el cliente EPA cuando se utilice con NetScaler y Device Posture

El cliente EPA se puede utilizar junto con NetScaler y Device Posture en las siguientes implementaciones:

- Autenticación adaptativa basada en NetScaler con EPA
- Gateway local basado en NetScaler con EPA

El servicio Device Posture envía la última versión del cliente EPA a los dispositivos finales. Sin embargo, en NetScaler, los administradores pueden configurar el siguiente control de versiones para los escaneos EPA en los servidores virtuales de puerta de enlace:

- **Siempre**: el cliente EPA del dispositivo final y NetScaler deben tener la misma versión.
- **Esencial**: la versión del cliente EPA del dispositivo final debe estar dentro del rango configurado en NetScaler.
- **Nunca**: el dispositivo final puede tener cualquier versión del cliente EPA.

Para obtener más información, consulte Comportamientos de los complementos.

Consideraciones al utilizar el cliente EPA con NetScaler y Device Posture

Cuando se utiliza un cliente EPA junto con Device Posture Service y NetScaler, puede haber situaciones en las que el dispositivo final ejecute la última versión del cliente EPA mientras que NetScaler utilice una versión diferente del cliente EPA. Esto podría provocar una discordancia entre la versión del cliente EPA en NetScaler y el dispositivo final. Como resultado, NetScaler puede solicitar al usuario final que instale la versión de cliente EPA que está presente en NetScaler. Para evitar este conflicto, recomendamos los siguientes cambios de configuración:

- Si ha configurado EPA con autenticación adaptativa o con autenticación local o servidor virtual de puerta de enlace, se recomienda inhabilitar el control de versiones del cliente EPA en NetScaler. Esto se hace para garantizar que el servicio GACS o Device Posture no envíe la última versión del cliente EPA a los dispositivos finales.
- El control de versión de la EPA se puede configurar en **Nunca** mediante la CLI o la GUI. Estos cambios de configuración son compatibles con NetScaler 13.x y versiones posteriores.
  - CLI: utilice los comandos de la CLI para la autenticación adaptativa y el servidor virtual de autenticación local.
  - GUI: utilice la GUI para el servidor virtual de puerta de enlace local. Para obtener más información, consulte Control de la actualización de los clientes de Citrix Secure Access.

Ejemplos de comandos CLI:

```
add rewrite action <rewrite_action_name> insert_http_header Plugin-Upgrade ""epa_win:Never;epa_mac:Always;epa_linux:Always;vpn_win:Never;vpn_mac:Always;vpn_linux:Always;""

add rewrite policy <rewrite_action_policy> "HTTP.REQ.URL.CONTAINS("pluginlist.xml")" <rewrite_action_name>

bind authentication vserver <Authentication_Vserver_Name> -policy <rewrite_action_policy> -priority 10 -type RESPONSE
<!--NeedCopy-->
```

Reglamentación de datos

February 16, 2024

En este tema se proporciona información sobre la recopilación, el almacenamiento y la retención de registros por parte de Device Posture Service. Todos los términos en mayúsculas que no estén definidos en lassecciones Definiciones llevan el significado especificado en elAcuerdo de servicios para usuarios finales de Citrix.

Residencia de datos

Los datos del contenido de los clientes de Citrix Device Posture residen en los servicios de la nube de AWS y Azure. Se replican en las siguientes regiones para garantizar su disponibilidad y redundancia:

- AWS
  - Este de EE. UU.

  - India occidental
  - Europa (Fráncfort)

- Azure
  - Oeste de EE. UU.
  - Europa occidental
  - Asia (Singapur)
  - Centro Sur de EE. UU.

Estos son los diferentes destinos de la configuración del servicio, los registros de tiempo de ejecución y los eventos.

- Servicio Splunk para la supervisión del sistema y los registros de depuración, solo en la ubicación de EE. UU.
- Citrix Analytics Service para ver los registros de diagnóstico y acceso de usuarios, consulte Gobierno de datos de Citrix Analytics Service para obtener más información.
- Servicio de registros del sistema de Citrix Cloud para registros de auditoría de administradores. Para obtener más información, consulte Consideraciones geográficas y manejo de registros y contenido del cliente de Citrix Cloud Services.

Recopilación de datos

Citrix Device Posture Service permite a los administradores del cliente configurar el servicio a través de la interfaz de usuario de Device Posture. El siguiente contenido del cliente se recopila en función de la configuración de la directiva de postura del dispositivo y de la plataforma:

- Versión del sistema operativo
- Versión de la aplicación Citrix Workspace
- Direcciones MAC
- Procesos en ejecución
- Certificado de dispositivo
- Detalles del Registro
- Detalles de la actualización de instalación de Windows
- Detalles de la última actualización de Windows
- Sistema de archivos: nombres de archivos, hashes de archivos y hora de modificación
- Nombre del dominio

Para los registros de tiempo de ejecución recopilados por los componentes del servicio, la información clave consiste en lo siguiente:

- ID de cliente/arrendatario
- ID de dispositivo (identificador único generado por Citrix)

- Salida del escaneo de Device Posture
- Dirección IP pública del dispositivo de punto final

Transmisión de datos

Citrix Device Posture Service envía registros a destinos protegidos por la seguridad de la capa de transporte.

Control de datos

Citrix Device Posture Service no ofrece actualmente opciones para que los clientes desactiven el envío de registros o impidan que el contenido de los clientes se replique a nivel mundial.

Retención de datos

Según la directiva de retención de datos de Citrix Cloud, los datos de configuración del cliente se purgan del servicio 90 días después del vencimiento de la suscripción.

Los destinos de registro mantienen su directiva de retención de datos específica del servicio.

- Para obtener más información, consulte Gobierno de datos para conocer la directiva de retención de los registros de Analytics.
- Los registros de Splunk se archivan y, finalmente, se eliminan después de 90 días.

Exportación de datos

Hay diferentes opciones de exportación de datos para diferentes tipos de registros.

- Se puede acceder a los registros de auditoría del administrador desde la consola Registro del sistema de Citrix Cloud.
- Los registros de diagnóstico de Device Posture Service del dispositivo se pueden exportar desde el panel de Citrix Analytics Service o de Secure Private Access Service como un archivo CSV.

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, incluidos los registros que miden el rendimiento, la estabilidad, el uso, la seguridad y el soporte.

- Los servicios significan que los servicios de Citrix Cloud descritos anteriormente para los fines de Citrix Analytics.