



# Device Posture

Machine translated content

## Disclaimer

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

## Contents

<b>Novedades</b>	<b>2</b>
<b>Device Posture Service en modo de prueba: Tech Preview</b>	<b>5</b>
<b>Integración de CrowdStrike con Device Posture</b>	<b>7</b>
<b>Integración de Microsoft Intune con Device Posture</b>	<b>11</b>
<b>Verificación del certificado del dispositivo con Device Posture Service</b>	<b>16</b>
<b>Imponga controles inteligentes en DaaS mediante Device Posture</b>	<b>19</b>
<b>Supervisión y solución de problemas</b>	<b>22</b>
<b>Registros de Device Posture</b>	<b>24</b>
<b>Administrar el cliente Citrix Endpoint Analysis para Device Posture Service</b>	<b>25</b>
<b>Reglamentación de datos</b>	<b>28</b>

## Novedades

June 19, 2024

### 29 de mayo de 2024

- **Disponibilidad de Device Posture Service en modo de prueba: Tech Preview**

Device Posture Service también está disponible en modo de prueba, en el que los administradores pueden probar Device Posture Service antes de habilitarlo en su entorno de producción. Esto permite a los administradores analizar el impacto de los escaneos de Device Posture en los dispositivos de los usuarios finales y después planificar su plan de acción en consecuencia antes de habilitarlos en producción. Para obtener más información, consulte [Device Posture Service en modo de prueba: Tech Preview](#).

- **Análisis periódico de dispositivos - Tech Preview**

Ahora puede habilitar el análisis periódico de los dispositivos Windows para las comprobaciones configuradas cada 30 minutos. Para obtener más información, consulte [Análisis periódico de dispositivos: Tech Preview](#).

### 14 de mayo de 2024

- **Omitir las comprobaciones de Device Posture**

Los administradores pueden permitir a los usuarios finales omitir las comprobaciones de Device Posture en sus dispositivos. Para obtener más información, consulte [Omitir las comprobaciones de Device Posture](#).

- **Panel de Device Posture**

El portal de Device Posture Service ahora tiene un panel de control para los registros de supervisión y solución de problemas. Los administradores ahora pueden usar este panel para supervisar y solucionar problemas. Para obtener más información, consulte [Registros de Device Posture](#).

- **Disponibilidad general de las comprobaciones de explorador y antivirus**

Las comprobaciones del explorador y del antivirus ya están disponibles de forma general. Para obtener más información, consulte [Escaneos compatibles con Device Posture](#).

- **Disponibilidad general de mensajes personalizados**

La opción de agregar mensajes personalizados cuando se deniega un acceso ahora está disponible de forma general. Para obtener más información, consulte [Mensajes personalizados para situaciones de acceso denegado](#).

## 26 de marzo de 2024

- **Soporte de URL de espacio de trabajo personalizadas**

Las URL personalizadas del espacio de trabajo ahora son compatibles con Device Posture Service. Puede usar una URL de tu propiedad además de la URL de cloud.com para acceder al espacio de trabajo. Asegúrese de permitir el acceso a citrix.com desde su red. Para obtener más información sobre los dominios personalizados, consulte [Configurar un dominio personalizado](#).

## 12 de febrero de 2024

- **Soporte para comprobaciones de explorador y antivirus - Tech Preview**

Device Posture Service ahora admite las comprobaciones del explorador y del antivirus. Para obtener más información, consulte [Escaneos compatibles con Device Posture](#).

## 23 de enero de 2024

- **Disponibilidad general de la verificación del certificado del dispositivo con Device Posture Service**

La verificación del certificado del dispositivo con Device Posture Service ya está disponible de forma general. Para obtener más información, consulte [Comprobación del certificado del dispositivo con Device Posture Service](#).

- **Funciones en Tech Preview de Device Posture Service**

Device Posture Service ahora admite las siguientes comprobaciones:

- Device Posture Service ahora es compatible con las plataformas IGEL.
- Device Posture Service ahora admite verificaciones de geolocalización y ubicación de red.

Para obtener más información, consulte [Device Posture](#).

## 11 de septiembre de 2023

- **Disponibilidad general de la integración de la Device Posture con Microsoft Intune**

La integración de la Device Posture con Microsoft Intune ya está disponible de forma general. Para obtener más información, consulte [Integración de Microsoft Intune con Device Posture](#).

### **30 de agosto de 2023**

- **Administrar Citrix Endpoint Analysis Client para Device Posture Service**

El cliente EPA se puede utilizar junto con NetScaler y Device Posture. Se requieren algunos cambios de configuración para administrar el cliente EPA cuando se usa con NetScaler y Device Posture. Para obtener más información, consulte [Administrar el servicio Citrix Endpoint Analysis Client for Device Posture](#).

### **28 de agosto de 2023**

- **Soporte de Device Posture Service en plataformas iOS - Tech Preview**

Device Posture Service ahora es compatible con las plataformas iOS. Para obtener más información, consulte [Device Posture](#).

### **22 de agosto de 2023**

- **Verificación del certificado del dispositivo con Citrix Device Posture Service - Tech Preview**

El servicio Citrix Device Posture ahora permite el acceso contextual (Smart Access) a los recursos de Citrix DaaS y Secure Private Access comprobando el certificado del dispositivo final con una entidad de certificación corporativa para determinar si se puede confiar en el dispositivo final. Para obtener más información, consulte [Comprobación del certificado del dispositivo con Device Posture Service](#).

### **17 de agosto de 2023**

- **Eventos de Device Posture en Citrix DaaS Monitor**

Los eventos de Device Posture Service y los registros de supervisión ahora se pueden buscar en DaaS Monitor. Para obtener más información, consulte [Eventos de Device Posture en Citrix DaaS Monitor](#).

### **23 de enero de 2023**

- **Device Posture Service**

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 obtener más información, consulte [Device Posture](#).

[AAUTH-90]

- **Integración de Microsoft Endpoint Manager con Device Posture**

Además de los escaneos nativos que ofrece Device Posture Service, Device Posture Service también se puede integrar con otras soluciones de terceros. Device Posture está integrado en Microsoft Endpoint Manager (MEM) en Windows y macOS. Para obtener más información, consulte [Integración de Microsoft Endpoint Manager con Device Posture](#).

[ACS-1399]

## Device Posture Service en modo de prueba: Tech Preview

June 19, 2024

Device Posture Service también está disponible en modo de prueba, en el que los administradores pueden probar Device Posture Service antes de habilitarlo en su entorno de producción. Esto permite a los administradores analizar el impacto de los escaneos de Device Posture en los dispositivos de los usuarios finales y después planificar su plan de acción en consecuencia antes de habilitarlos en producción. Device Posture Service en modo de prueba recopila datos de los dispositivos de los usuarios finales y los clasifica en tres categorías: compatibles, no conformes y denegados. Sin embargo, esta clasificación no impone ninguna acción en los dispositivos de los usuarios finales. En cambio, permite a los administradores evaluar sus entornos y mejorar la seguridad. Los administradores pueden ver estos datos en el panel de control de Device Posture. Los administradores también pueden inhabilitar el modo de prueba, si es necesario.

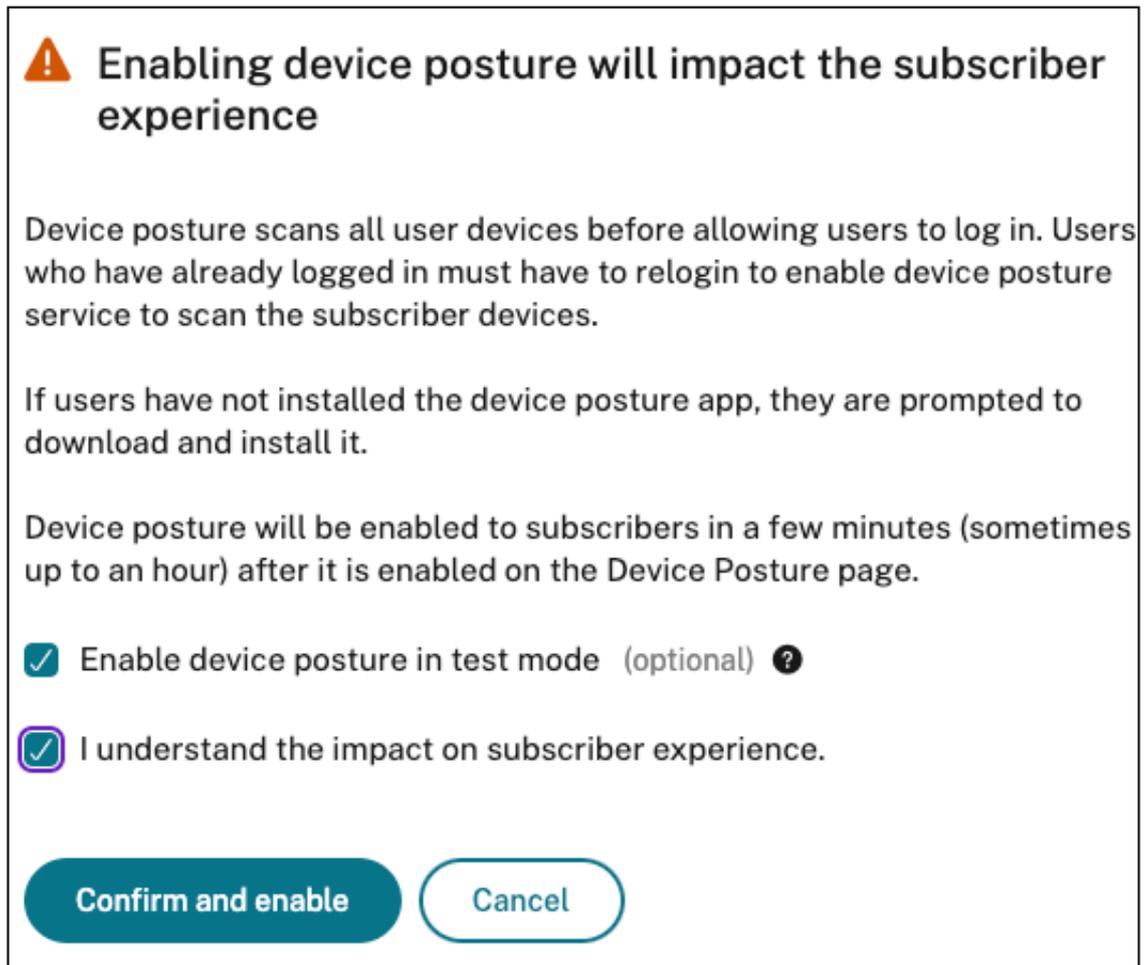
**Nota:**

El cliente EPA debe estar instalado en los dispositivos. En caso de que un dispositivo final no tenga instalado el cliente EPA, Device Posture Service presenta una página de descarga para que el usuario final descargue e instale el cliente, sin la cual el usuario final no puede iniciar sesión.

### Habilitar el modo de prueba

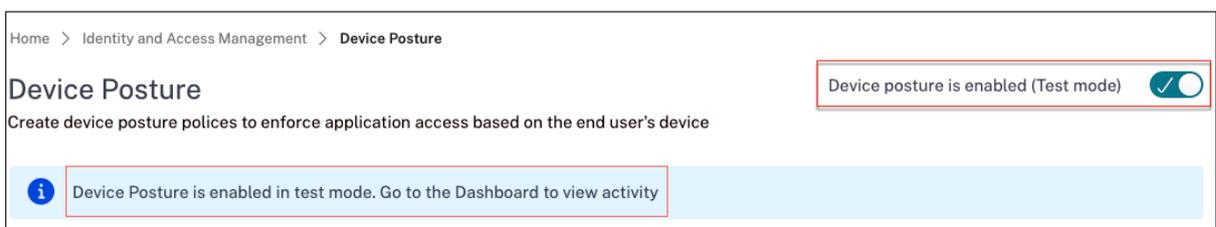
1. Inicie sesión en Citrix Cloud y después seleccione **Administración de acceso e identidades** en el menú de tres líneas.

2. Haga clic en la ficha **Device Posture** y después en **Administrar**.
3. Deslice el conmutador **Device Posture está inhabilitado** a la posición ACTIVAR.
4. En la ventana de confirmación, seleccione ambas casillas.



5. Haga clic en **confirmar y activar**.

Cuando Device Posture Service está activado en el modo de prueba, la página principal de Device Posture muestra una nota que confirma lo mismo.



Los administradores pueden configurar las directivas y reglas para los escaneos de postura de los dispositivos. Para obtener más información, consulte Configurar la Device Posture. Según los resultados

del escaneo, los dispositivos de los usuarios finales se clasifican como compatibles, no conformes y rechazados. Los administradores pueden ver estos datos en el panel de control.

### Ver las actividades del modo de prueba en el panel

1. Haga clic en la ficha **Panel de control** en la página Device Posture.  
El gráfico **Registros de diagnóstico** muestra el número de dispositivos clasificados como compatibles, no conformes y de inicio de sesión denegado.
2. Para ver los detalles, haga clic en el enlace **Ver más**.

#### Diagnóstico del modo de prueba

Los administradores pueden descargar los registros de supervisión desde la interfaz de usuario.

### Habilitar el modo de prueba en producción

Si Device Posture Service ya está habilitado en producción, lleve a cabo los siguientes pasos para habilitar el modo de prueba:

1. En la página de inicio, deslice el conmutador **Device Posture está habilitado** a la posición DESACTIVAR.
2. Seleccione **Comprendo que se inhabilitarán todas las comprobaciones de Device Posture**.
3. Haga clic en **Confirmar e inhabilitar**.
4. Ahora habilite Device Posture deslizando el conmutador **Device Posture está inhabilitado** para encenderlo.
5. En la ventana de confirmación, seleccione las dos opciones siguientes.
  - **Habilitar Device Posture en modo de prueba**
  - **Comprendo el impacto en la experiencia de los suscriptores**
6. Haga clic en **confirmar y activar**.

## Integración de CrowdStrike con Device Posture

June 19, 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 Device Posture 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 Virtual Apps and Desktops, 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.

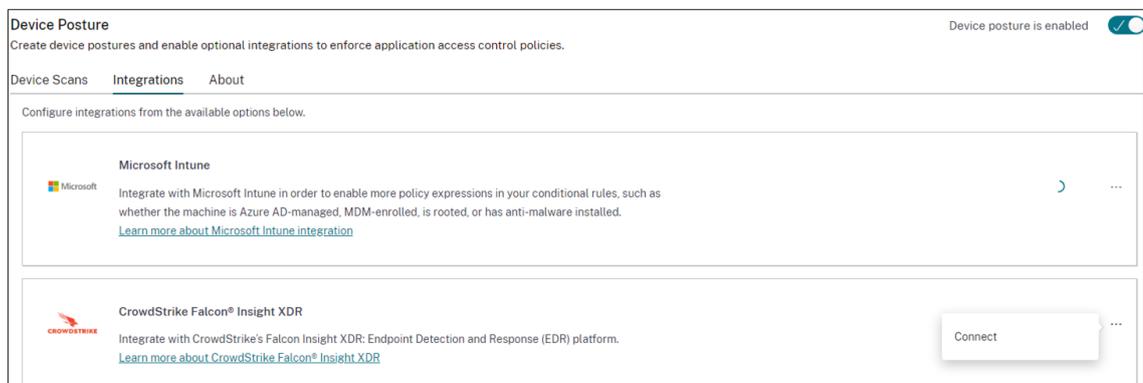
**Paso 1:** Establecer la confianza entre el servicio Citrix Device Posture y el servicio CrowdStrike ZTA. Se trata de una actividad que se realiza una sola vez.

**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 después seleccione **Administración de acceso e identidad** en el menú de hamburguesas.
2. Haga clic en la ficha **Device Posture** y después 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 después hacer clic en la ficha **Integraciones**.

4. Haga clic en el botón de puntos suspensivos del cuadro de CrowdStrike y después 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 después 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 configurado** a **Configurado**.

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

## Paso 2: Configure directivas de Device Posture

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 después en **Crear directiva de dispositivos**.

The screenshot shows a 'Create device policy' dialog box. At the top, it says 'With device posture, you can define a set of conditions that control which devices have access to various services and data sources.' Below this, there is a section 'Select the operating system for this device posture scan.' with a dropdown menu currently set to 'Windows'. Underneath is the 'Policy rules' section, which says 'Select a condition and apply access rules for your services and data.' A rule is added for 'CrowdStrike' with the condition 'Risk Score' 'Less than' '0-100'. There are buttons to 'Add qualifier' and 'Add another rule' at the bottom.

2. Seleccione la plataforma para la que se creó esta directiva.
3. En **Policy Rule**, seleccione **CrowdStrike**.
4. Para el calificador de **puntuación de riesgo**, seleccione la condición y después 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 Device Posture.

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**

Policy result  
If policy conditions and rules are met, the device scan will classify the user device as one of the following: ⓘ

**Compliant**  
The device will be considered compliant and full access will be granted.

**Non-compliant**  
The device will be considered "non-compliant" and restricted access will be granted.

**Denied access**  
The device will be denied access to all resources.

Scan details  
Name and set the priority order of this device scan. ⓘ

Name \*

Priority \* ⓘ

Enable when created

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 Device Posture Service 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

[Device Posture Service](#)

## Integración de Microsoft Intune con Device Posture

June 19, 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 Device Posture 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 Device Posture 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.

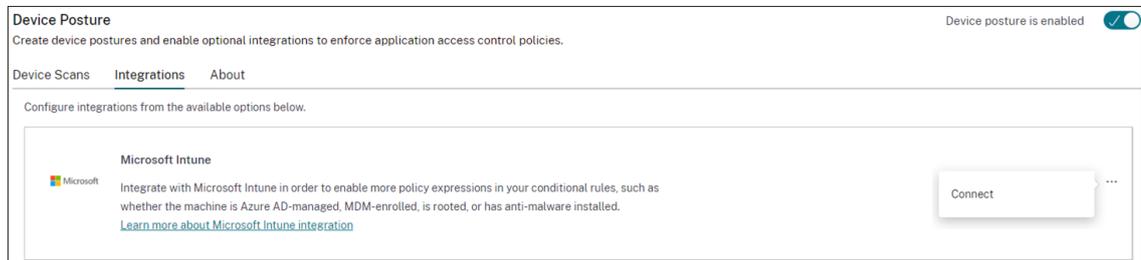
**Paso 1:** Integre la Device Posture con el servicio Microsoft Intune. Se trata de una actividad que se realiza una sola vez para establecer la confianza entre Device Posture y Microsoft Intune.

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

### Paso 1: Integrar la Device Posture 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 después haga clic en la ficha **Integraciones**.

- **Cientes 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 después en la ficha **Integraciones**.



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



tu@ctelabs25.onmicrosoft.com

## Permissions requested

Review for your organization

### Device Posture Integrations

Cloud Software Group, Inc. 

This app would like to:

- ✓ Read Microsoft Intune devices
- ✓ Read Microsoft Intune configuration
- ✓ Sign in and read user profile

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. **The publisher has not provided links to their terms for you to review.** You can change these permissions at <https://myapps.microsoft.com>. [Show details](#)

Does this app look suspicious? [Report it here](#)

En la siguiente tabla se enumeran los permisos de la API de Microsoft Intune para la integración con Device Posture Service.

## Device Posture

---

Nombre de API	Valor de la reclamación	Nombre del permiso	Tipo
Microsoft Graph	DeviceManagementManagedDevices.ReadAll	Microsoft Intune	Aplicación
Microsoft Graph	DeviceManagementServiceConfig.Read.All	Microsoft Intune	Aplicación

---

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

Si la integración no se realiza correctamente, el estado aparece como **Pendiente**. Debe hacer clic en los **puntos suspensivos** y después en **Reconectar**.

### Paso 2: Configure directivas de Device Posture

1. Haga clic en la ficha **Escaneos de dispositivos** y después en **Crear directiva de dispositivos**.

### Create device policy

✕

With device posture, you can define a set of conditions that control which devices have access to various services and data sources.

---

**Platform**  
Select the operating system for this device posture scan. ⓘ

Windows
▾

---

**Policy rules**  
Select a condition and apply access rules for your services and data. ⓘ

▾ Microsoft Intune
🗑️

Matches all of
▾

Compliant
Managed
▾

+ Add another rule

---

**Policy result**  
If policy conditions and rules are met, the device scan will classify the user device as one of the following: ⓘ

**Compliant**  
The device will be considered compliant and full access will be granted.

**Non-compliant**  
The device will be considered “non-compliant” and restricted access will be granted.

**Denied access**  
The device will be denied access to all resources.

---

**Scan details**  
Name and set the priority order of this device scan. ⓘ

Create

Cancel

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 después 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 Device Posture.

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 Device Posture](#).

## Verificación del certificado del dispositivo con Device Posture Service

June 19, 2024

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

### Puntos a tener en cuenta:

- Device Posture Service 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 Device Posture](#).
- 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 Device Posture Service 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.

```
1 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 **Parámetros** en la página de inicio de Device Posture.
2. Haga clic en **Administrary**, 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**, a continuación, en **Importar**.

### Import Issuer Certificate

✕

Issuer certificate will be added to the Endpoint. View certificate details in certificate table once created.

---

**Certificate Type \***

PEM (Privacy Enhanced Mail)
▾

**Certificate File \***

cgwsanitydc.pem

+ Choose Certificate

Import

Cancel

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

## Ver certificados importados

1. Haga clic en **Parámetros** 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.

### Issuer Certificates

✕

Issuer Certificates will be used to validate the device certificates as per the configured policies.

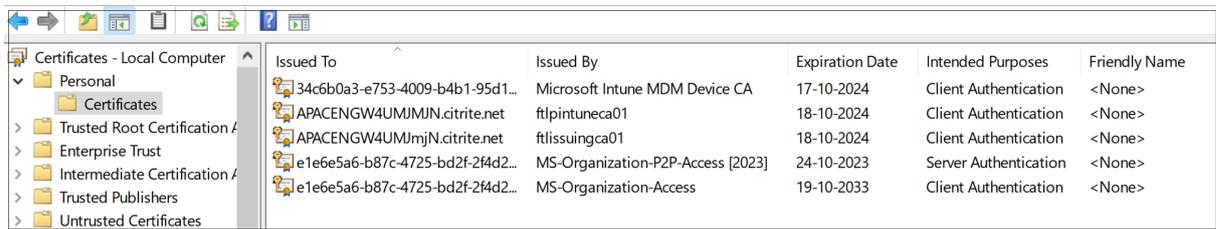
Import Issuer Certificate

Issuer	Certificates	Policies	Status	
cgwsanity-DC-CA	cgwsanitydc.pem	NA	Valid	<span style="font-size: 0.8em; color: #666;">↓</span> <span style="font-size: 0.8em; color: #666;">🗑️</span>
int-CA	combinedchain.pem	NA	Valid	<span style="font-size: 0.8em; color: #666;">↓</span> <span style="font-size: 0.8em; color: #666;">🗑️</span>

## 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.

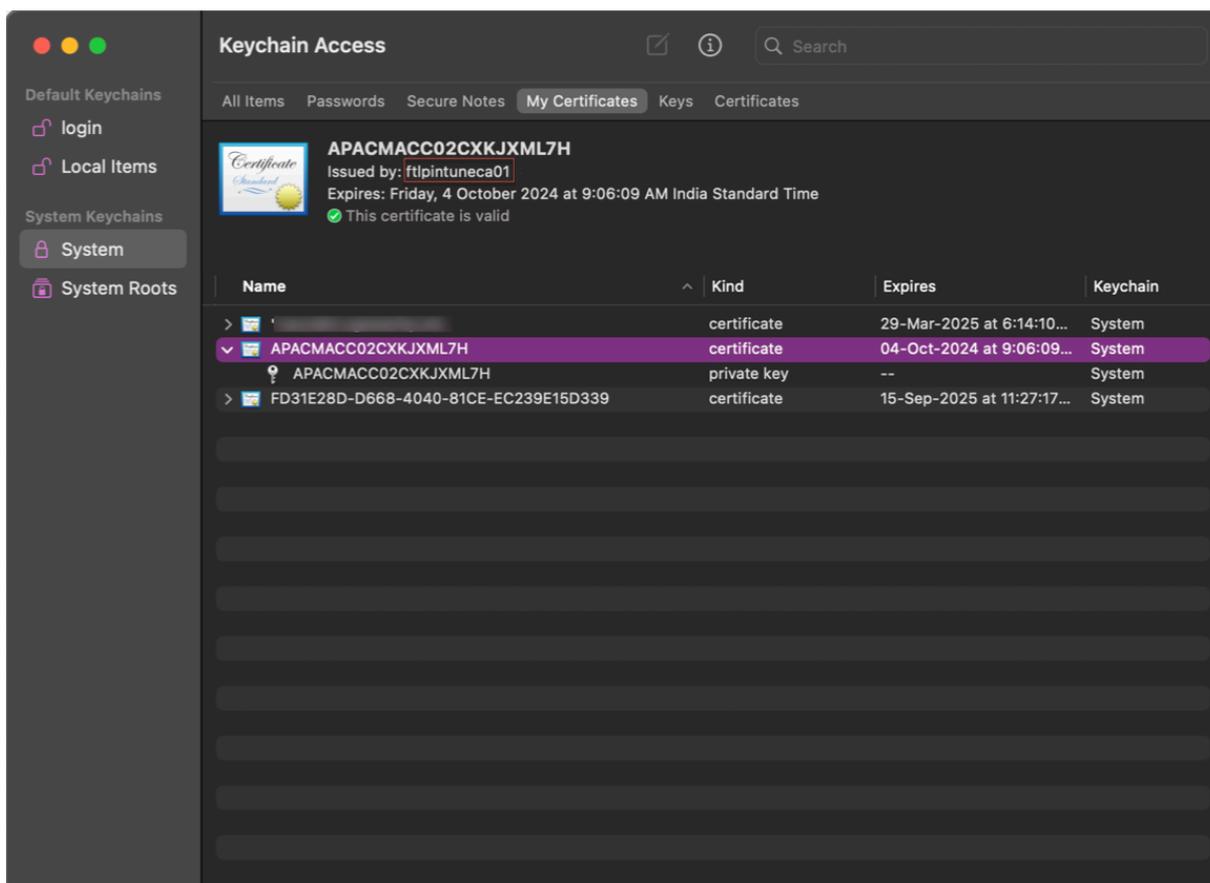


Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
34c6b0a3-e753-4009-b4b1-95d1...	Microsoft Intune MDM Device CA	17-10-2024	Client Authentication	<None>
APACENGW4UMJMjN.citrite.net	ftlpintuneca01	18-10-2024	Client Authentication	<None>
APACENGW4UMJMjN.citrite.net	ftlissuingca01	18-10-2024	Client Authentication	<None>
e1e6e5a6-b87c-4725-bd2f-2f4d2...	MS-Organization-P2P-Access [2023]	24-10-2023	Server Authentication	<None>
e1e6e5a6-b87c-4725-bd2f-2f4d2...	MS-Organization-Access	19-10-2033	Client Authentication	<None>

### macOS:

1. Abra **Keychain Access** y después 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**, a continuación, haga clic en **Guardar**.

**Edit Setting**  
Client clipboard redirection

Allowed  
This setting will be allowed.

Prohibited  
This setting will be prohibited.

**Description**  
 Allow or prevent the clipboard on the client device to be mapped to the clipboard on the server. By default, clipboard redirection is allowed.  
 To prevent cut-and-paste data transfer between a session and the local clipboard, select 'Prohibited'. Users can still cut and paste data between applications running in a session.  
 After allowing this setting, configure the maximum allowed bandwidth the clipboard can consume in a client connection using the Clipboard redirection bandwidth limit setting or the Bandwidth limit for clipboard redirection channel as percent of total session bandwidth setting.

**Related settings**  
 Clipboard redirection bandwidth limit, Clipboard redirection bandwidth limit percent

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

**Create Policy**

Summary

Filters: 0 selected  View selected only

Filter ↓	Value
<input type="checkbox"/> > Delivery Group	
<input type="checkbox"/> > Delivery Group type	
<input type="checkbox"/> > Organizational Unit (OU)	
<input type="checkbox"/> > Tag	
<b>Filters for user settings only</b>	
<input type="checkbox"/> > Access control	
<input type="checkbox"/> > Citrix SD-WAN	
<input type="checkbox"/> > Client IP address	
<input type="checkbox"/> > Client name	
<input type="checkbox"/> > User or group	

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

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

**Assign Policy**  
Access control

Apply policy based on the access control conditions through which a client connects.

Access control elements:

Mode	Connection type	Gateway farm name	Access condition
Allow	With Citrix Gateway	Workspace	NON-COMPLIAN

Enable

Save Cancel

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.

## Supervisión y solución de problemas

June 19, 2024

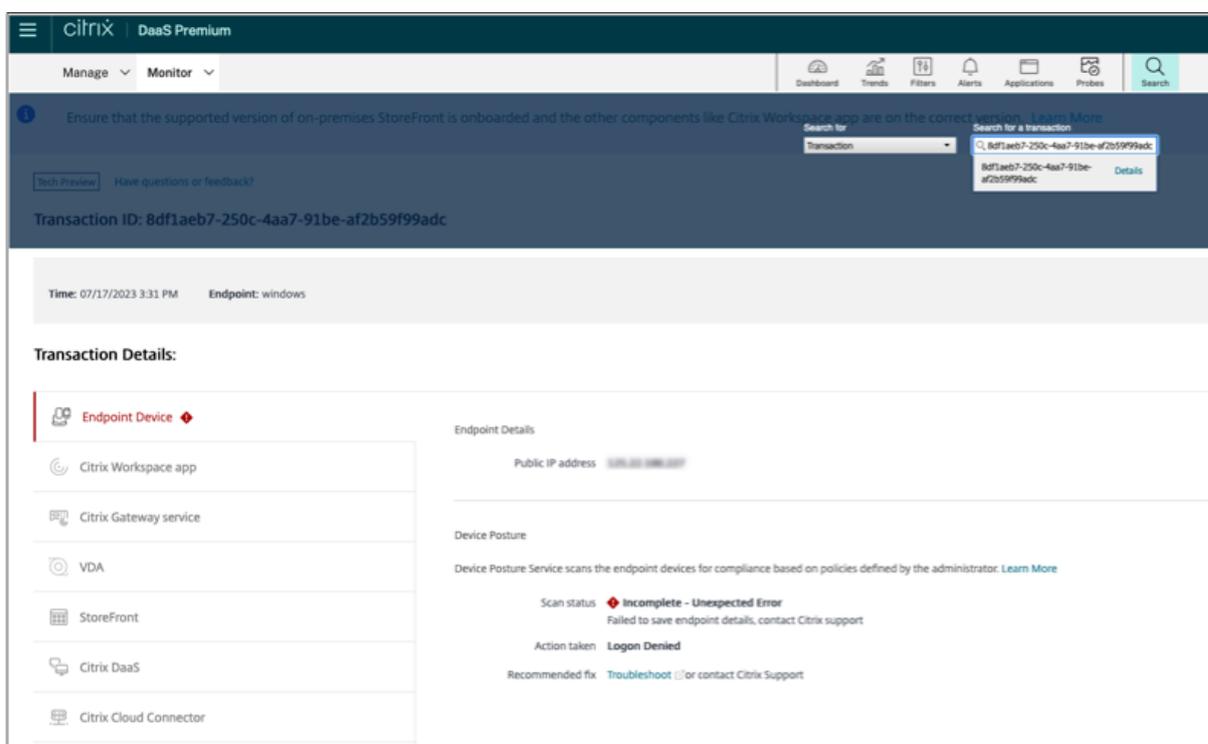
Los registros de eventos de Device Posture se pueden ver en dos lugares:

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

### Eventos de Device Posture en Citrix DaaS Monitor

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

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 después en la ficha **Supervisar**.  
En la interfaz de usuario del monitor, busque el identificador de transacción de 32 dígitos y haga clic en **Detalles**.



## Eventos de Device Posture en el panel de Secure Private Access

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

1. Inicie sesión en Citrix Cloud.
2. En el mosaico Secure Private Access, haga clic en **Administrar** y después en **Panel de control**.
3. Haga clic en el enlace **Ver más** del gráfico **Registros de diagnóstico** para ver los registros de eventos de Device Posture.

TIME (UTC)	POLICY INFO	POLICY RESULT	STATUS	OPERATING SYSTEM	TRANSACTION ID	DESCRIPTION	INFO CODE
Tue, 11 Apr 2023 11:47:...	NoMatchingPolicy	Non-Compliant	Success	Windows	85562ba3-71c8-4839...		
Tue, 11 Apr 2023 11:45:...	NoMatchingPolicy	Non-Compliant	Success	Windows	0dd908ad-b8ec-484...		
Tue, 11 Apr 2023 11:45:...	NoMatchingPolicy	Non-Compliant	Success	Windows	a418a959-e7cd-4a9d...		
Tue, 11 Apr 2023 11:44:...	NoMatchingPolicy	Non-Compliant	Success	Windows	0dd908ad-b8ec-484...		
Tue, 11 Apr 2023 11:44:...	ms-MEM	Compliant	Success	Windows	0dd908ad-b8ec-484...		
Tue, 11 Apr 2023 11:43:...	ms-MEM	Compliant	Success	Windows	0dd908ad-b8ec-484...		
Tue, 11 Apr 2023 11:42:...	ms-MEM	Compliant	Success	Windows	cb57315f-48f7-45cb...		

- 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, Device Posture Service 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 Citrix Support 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/EPAPugin/EpaCloud.log
  - ~/Biblioteca/Application Support/Citrix/EPAPugin/epapugin.log

## Registros de errores de Device Posture

Los siguientes registros relacionados con Device Posture Service 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 Citrix Support 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

## Registros de Device Posture

June 19, 2024

Puede utilizar el panel del portal de Device Posture Service para supervisar y solucionar problemas. Para ver el panel de Device Posture Service, haga clic en la ficha **Panel de control** de la página de inicio de Device Posture. La sección **Registro y solución de problemas** muestra los registros de diagnóstico relacionados con Device Posture Service. Puede hacer clic en el enlace **Ver más** para ver los detalles de los registros. Puede refinar la búsqueda en función de los resultados de la directiva (**Compatible**, **No compatible** e **Inicio de sesión denegado**).

Home > Identity and Access Management > Device Posture

Device Posture Device posture is enabled

Create device posture policies to enforce application access based on the end user's device

Dashboard Device Scans Integrations

Last 1 Week

Logging and Troubleshooting

D diagnostic Logs ⓘ

Device Posture ⓘ



Compliant	162
Non-Compliant	113
Login Denied	122

See more

### Nota:

Los registros de Device Posture también se capturan en el panel del servicio Secure Private Access. Para ver los registros de Device Posture, haga clic en la ficha **Registros de Device Posture**. Puede refinar la búsqueda en función de los resultados de la directiva (**compatible**, **no com-**

patible e inicio de sesión denegado). Para obtener más información, consulte [Registros de diagnóstico](#).

## Administrar el cliente Citrix Endpoint Analysis para Device Posture Service

June 19, 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 Device Posture en un dispositivo final, debe instalar el cliente Citrix Endpoint Analysis (EPA), que es una aplicación ligera, en ese dispositivo. Device Posture Service siempre se ejecuta con la última versión del cliente EPA publicada por Citrix.

### Instalación del cliente EPA

Durante el tiempo de ejecución, Device Posture Service 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 de un cliente de la 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 Device Posture Service. Para la actualización automática, el cliente EPA debe haberse instalado con acceso de administrador.

**Nota:**

La actualización automática está en versión preliminar. Regístrese para obtener la Tech Preview 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.

- **Instalador de clientes EPA integrado con la aplicación Citrix Workspace:** El instalador de clientes EPA está integrado con la aplicación Citrix Workspace 2402 LTSR para Windows. Esta integración elimina la necesidad de que los usuarios finales instalen el cliente EPA por separado después de instalar la aplicación Citrix Workspace.

Para instalar el cliente EPA como parte de la aplicación Citrix Workspace, utilice la opción de la línea de comandos `InstallePAClient`. Por ejemplo, `./CitrixworkspaceApp.exe InstallePAClient`.

**Nota:**

- La instalación del cliente EPA como parte de la aplicación Citrix Workspace está inhabilitada de forma predeterminada. Debe habilitarse explícitamente mediante la opción de línea de comandos `InstallePAClient`.
- Si un dispositivo final ya tiene un cliente EPA instalado y el usuario final instala la aplicación Citrix Workspace, se actualiza el cliente EPA existente.
- Si un 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.
- El instalador del cliente EPA integrado con la aplicación Citrix Workspace también se puede usar con NetScaler. Para obtener más información, consulte [Administrar el cliente EPA cuando se usa con NetScaler](#) y Device Posture.

- **Distribuya el cliente mediante GACS:** GACS es una solución proporcionada por Citrix para administrar 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 usar 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

Device Posture Service 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:

```
1 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;""
2
3 add rewrite policy <rewrite_action_policy> "HTTP.REQ.URL.CONTAINS("
  pluginlist.xml)" <rewrite_action_name>
4
5 bind authentication vserver <Authentication_Vserver_Name> -policy <
  rewrite_action_policy> -priority 10 -type RESPONSE
6 <!--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 las secciones [Definiciones](#) llevan el significado especificado en el [Acuerdo 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.



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).